UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de calidad de servicio en redes de computadoras para servicios de voz sobre IP

TESIS

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A N

García Sánchez Sergio Ivanhoe

Hernández Rodríguez Celina

DIRECTOR DE TESIS

Marcos Antonio López Hernández

Ciudad Universitaria, Cd. Mx., 2016

ÍNDICE

4. MECANISMOS DE CALIDAD EN OTRAS REDES

5. CONFIGURACIÓN DE LA RED Y LOS SERVICIOS DE VoIP

6. IMPLEMENTACIÓN DE LA CALIDAD DE SERVICIO

7. RESULTADOS

8. BIBLIOGRAFÍA

Agradecimientos

Principalmente agradezco a Dios por brindarme la salud, la fortaleza y la paciencia que me llevaron a nunca rendirme en esta travesía; por poner en mi camino a personas que han sabido guiarme, apoyarme, comprenderme, darme lecciones y motivarme a lo largo de mi vida.

Gracias a la UNAM, especialmente a la Facultad de Ingeniería, por darme la oportunidad de ocupar un lugar en sus aulas ya que con ello logré absorber todo el conocimiento que mis profesores pudieron transmitirme dentro y fuera de las mismas.

Agradezco a mis padres por el amor que me han dado, por la educación y los valores que me han inculcado; la oportunidad que me han brindado para elegir la carrera que a mi juicio me llenaría de dicha y felicidad; por permitirme vivir uno de los sueños más anhelados en mi vida y que sin su apoyo, motivación y esfuerzo no lo habría podido realizar: ir de intercambio a Francia. De manera especial agradezco a mi madre por todos los desvelos soportados, las atenciones dedicadas, los consejos transmitidos y el amor incondicional que me ha tenido desde que nací. Agradezco a mi padre particularmente por la sabiduría otorgada, el apoyo económico que hasta hoy me proporciona y el ejemplo que he adoptado como modelo a seguir y que me ha llevado hasta donde me encuentro actualmente. Gracias a ambos.

A mis hermanas, Yess, July y Viri, porque sin todas las risas y momentos de paz que siempre forman parte de nuestros días me habría vuelto loca. Gracias por ser como son y por quererme como me quieren. Las amo.

Gracias Serch por invitarme a formar parte de este proyecto y por hacer de este periodo de trabajo uno muy agradable y lleno de diversión. Porque logramos congeniar y sacar adelante esta tesis pese a las diferentes visiones que teníamos.

A mis amigos, a los cuales no puedo nombrar porque de hacerlo mi agradecimiento sería muy extenso. Afortunadamente cuento personas en mi vida que engloban todo lo que la palabra "amistad" implica y esta tesis también va para ustedes amigos, ya que fueron un pilar importante a lo largo de todas mis etapas formativas. ¡Los adoro!

Especialmente quiero agradecer a mi asesor de tesis, el profesor Marcos Antonio López Hernández, por guiar este trabajo profesional, por sus consejos, su apoyo, sus enseñanzas, explicaciones, su tiempo invertido en nosotros, su tolerancia y, sobre todo, por acogernos como si fuéramos integrantes extras de su familia. Porque todo el conocimiento que me ha transmitido es la herramienta más importante que me ha podido dar.

Celina Hernández Rodríguez

Agradezco con mucha sinceridad el apoyo de nuestro profesor Marcos Antonio López porque sin su ayuda esto no hubiera sido posible, gracias por compartirnos su conocimiento y por hacer que este trabajo fuera algo muy agradable e interesante de realizar.

Asimismo quiero agradecer a mi compañera Celina Hernández por su interminable paciencia y determinación, así como por proveer un enfoque distinto que me hizo darme cuenta de la importancia del trabajo en equipo.

Gracias a ambos por poner de su esfuerzo y de su tiempo para que esto fuera posible.

Sergio García Sánchez

Implementación de calidad de servicio en redes de computadoras para servicios de voz sobre IP

Objetivo general

Definir el concepto de calidad de servicio en redes de datos, así como el contexto en el que se usa y revisar conceptos importantes relativos a la calidad de servicio para poder describir los mecanismos de calidad de servicio (QoS) en servicios de voz para redes de computadoras, así como su implementación; identificar también las diferencias, ventajas y desventajas entre cada mecanismo de calidad de servicio y ver cómo el tráfico de voz y de datos es afectado por los mismos, y finalmente comprobar la efectividad de los mecanismos de calidad de servicio aplicados en un esquema de red específico, donde transcurre tráfico de voz y de datos de forma simultánea.

Objetivos específicos

- Implementar una red que soporte transmisión de datos y de voz, mediante la configuración de routers, switches y teléfonos de VoIP.
- Configurar mecanismos de calidad de servicio diversos y analizar los resultados obtenidos mediante el software 'WireShark'.
- Simular un entorno de red con la ayuda del software generador de tráfico 'NetScan'.
- Configurar diversos parámetros para agregar QoS al sistema de red propuesto.
- Aplicar mecanismos de calidad de servicio sobre un enlace con baja tasa de transmisión y analizar las diferencias.

Definición del problema

Cuando iniciaba el internet, en las redes de computadoras se transmitían datos correspondientes a aplicaciones de textos, bases de datos, archivos binarios, entre otros archivos; actualmente los paquetes de datos que se transmiten incluyen también los de otras aplicaciones de tiempo real como voz y video digitalizados. Anteriormente las aplicaciones como voz y video se transmitían por redes separadas de las redes de datos. Había redes para cada aplicación: voz, datos y videoconferencia.

Actualmente todas las aplicaciones se transmiten en la misma red; esto ha requerido implementar mecanismos para dar preferencia de transmisión a las aplicaciones sensibles a retardos, esto se conoce como *calidad de servicio*. Las redes que transmiten simultáneamente paquetes correspondientes a aplicaciones de datos, voz y video se conocen como ***redes convergentes***.

Los requerimientos de una red para los paquetes de estas últimas aplicaciones son diferentes y pueden llegar a presentar diversas dificultades, en su mayoría en lo referente a la calidad de servicio, ya que dichas aplicaciones son muy sensibles a retardos, pérdida de paquetes y otros fenómenos como el ***jitter***. Si bien las redes de datos no son algo nuevo, afrontar el reto de mejorar la calidad de servicio es un tema todavía presente por lo que este trabajo se enfocará en el estudio y aplicación de los mecanismos de calidad de servicio ya que sin estos mecanismos, las aplicaciones de voz y/o video no funcionarían aceptablemente.

Resultados esperados

Se esperan realizar los siguientes puntos:

- Implementar calidad de servicio en una red experimental simple y comparar los resultados con aquellos en los que no se implementa la calidad de servicio.
- Lograr tener una transferencia de voz en tiempo real en condiciones de calidad óptima.
- Reducir los valores de parámetros como porcentaje de pérdidas, retrasos y valor promedio del jitter, cuando se está aplicando calidad de servicio.
- Proporcionar calidad de servicio a la voz, evitando afectaciones a otro tipo de tráfico (ICMP y HTTP), en el caso de existir una saturación de la red.
- Conseguir un desempeño óptimo para una llamada VoIP establecida sobre un enlace con baja tasa de transmisión, para así poder aplicar las configuraciones de QoS en enlaces con un ancho de banda mayor.

Introducción a la calidad de servicio

La calidad de servicio no es un concepto nuevo en redes de datos, sin embargo, es un concepto que ha adquirido gran importancia en los últimos tiempos, debido a las crecientes necesidades de los usuarios por formar parte de una red que ofrezca servicios múltiples, como la telefonía, el internet, el correo electrónico; por lo que es de vital importancia dar a conocer qué significa la calidad de servicio y cómo puede aplicarse en los servicios o tecnologías que se usan en la actualidad.

> ***"Existen aplicaciones (y clientes) que exigen a la red, garantías más sólidas de desempeño. Con los mecanismos de calidad del servicio, la red puede honrar las garantías de desempeño que hace incluso cuando hay picos de tráfico, a costa de rechazar algunas solicitudes."***
>
> ***Tanenbaum[1]***

Sistemas de voz sobre IP

Uno de los actuales avances tecnológicos en el área de las telecomunicaciones es el conocido como 'Voice over IP' o VoIP. Esta tecnología consiste en realizar llamadas telefónicas sobre una red de transmisión de datos en lugar de hacerlas sobre la red telefónica tradicional.

Las señales provenientes de llamadas analógicas o digitales son convertidas a paquetes de datos, para su transporte en las redes de datos como cualquier otro paquete, por ejemplo de correo electrónico o de una página web. Esto permite utilizar las redes de datos, que son más económicas, y con ello dejar de depender del proveedor de servicios de la red telefónica pública. Un ejemplo de esta tecnología es el popular servicio *Skype* que puede incluso ser gratuito.

La VoIP tiene un gran número de ventajas sobre el sistema telefónico tradicional. Las empresas y particulares están migrando a la tecnología de VoIP, debido a los beneficios que ésta ofrece, entre ellos el costo, ya que los usuarios pueden implementar su sistema telefónico directamente en su red interna y eliminar el costo por la renta del servicio.

Existen varias formas de integrar este servicio pues es muy versátil, ya que depende de dónde, cómo y de qué manera se han de realizar las llamadas, como se aprecia en la figura 1.1. Ya sea desde el hogar, el trabajo o en una red corporativa, la forma en que se hacen las llamadas varía

[1] **Tanenbaum Andrew; Wetherall David, 2012, Redes de computadoras, Pearson Education, 5ª edición, México, p. 347.**

de acuerdo al tipo de servicio de VoIP que se use. La telefonía ***IP*** incluye el conjunto completo de servicios habilitados por VoIP, como la interconexión de teléfonos para comunicaciones; servicios relacionados como facturación y planes de marcación; y funciones básicas que pueden incluir conferencias, transferencia de llamadas, reenvío de llamadas y llamada en espera.

> ***"Con el incremento de la cantidad de personas que trabajan de forma remota, las empresas tienen una creciente necesidad de conectar a la gente, de forma segura, confiable y ecónomica".***
>
> ***Allan Johnson[2]***

Algunas empresas temen migrar su servicio de telefonía analógico hacia la telefonía IP debido al gasto que implicaría comprar equipos terminales telefónicos digitales. Sin embargo, este gasto puede simplificarse al hacer uso de adaptadores de teléfonos analógicos (ATA).

Además, se puede contar con un ***softphone*** para realizar llamadas a otros softphones o a otros teléfonos convencionales usando VoIP. Un ejemplo popular de softphone en la actualidad es Skype, que también cuenta con el servicio de videoconferencias, otro servicio que debe su implementación a VoIP.

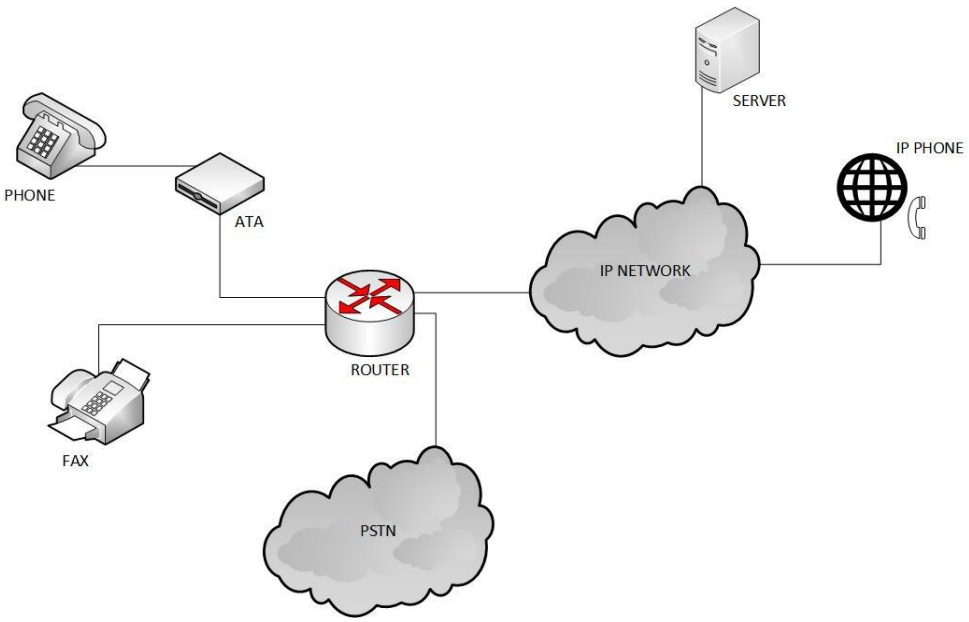

Figura 1.1. Red VoIP.

[2] *With the growing number of teleworkers, enterprises have an increasing need for secure, reliable and cost-effective ways to connect people.*

Johnson Allan, 2009, 31 days before your CCNA exam, Cisco Press, 2nd edition, USA, p. 7.

Algunas ventajas de VoIP son las siguientes:

- Reduce los gastos de desplazamiento mediante el uso de videoconferencias y conferencias en tiempo real.
- La administración y configuración del sistema son más flexibles.
- Permite que los dispositivos sean móviles.
- El costo de los gastos telefónicos se disminuye debido al uso de internet o de la red privada de la empresa.
- Se utiliza una sola red para voz y datos.
- Con VoIP se puede realizar una llamada desde cualquier lugar en dónde haya conectividad a internet. Esto es una ventaja para las personas que suelen viajar mucho.
- Flexibilidad y portabilidad del servicio mediante softphones.
- Permite las comunicaciones unificadas.

Sin embargo, se pueden tener las desventajas que se indican a continuación:

- Retraso en la llegada de paquetes o incluso pérdida de paquetes de información.
- Aunque es raro, VoIP es susceptible a virus, gusanos y hacking.
- El servicio en una red privada es mucho más eficiente que en una red pública como el internet, ya que en una red privada se puede gestionar el servicio y tratamiento de los paquetes según las necesidades de la empresa.

En los siguientes temas se verá con mayor profundidad algunos elementos contemplados en el funcionamiento de VoIP.

Como se ha mencionado en los párrafos anteriores, se encuentra presente el despliegue de las comunicaciones unificadas, mismo que toma relevancia porque actualmente es necesaria la integración de un sistema que sea capaz de proveer servicios de última generación, como los siguientes:

- Telefonía.
- Conferencias de voz y video.
- Servicios de mensajería y correo electrónico.
- Dispositivos móviles.
- Trabajo de forma remota.
- Combinación de audio y video.
- Presencia.

Estos servicios tienen un alto impacto debido a que, en primer lugar extienden el área de cobertura de una red, en segundo, brindan mayor libertad porque los servicios integrados

facilitan la comunicación desde diversos enfoques, y por último, tienen un costo menor al que se tendría al contratar cada uno de los servicios por separado.

De igual manera, ofrecen una mejor administración y mantenimiento, e integran diversas herramientas, con la finalidad de que la comunicación siempre esté disponible, sin importar la vía que se esté ocupando.

En general, la eficacia de las comunicaciones unificadas es que permiten la presencia del usuario, lo cual es un elemento indispensable cuando se requiere conectividad con alguien en específico, y una retroalimentación rápida dentro de la red, que a su vez mejora la colaboración entre usuarios.

Calidad de servicio (Quality of Service)

La calidad de servicio, también conocida como Quality of Service (QoS) es un tema de relevancia para cualquier red, y un problema a resolver en la gestión de ésta. Cada usuario, ya sea una persona o empresa, necesita cierto nivel de calidad en lo que al envío y recepción de su información se refiere. Pueden existir prioridades y clasificaciones de todo tipo, todo depende del enfoque que el cliente/usuario desee recibir, y de los servicios y aplicaciones que estén en curso.

En redes, donde existe una limitante como es el ancho de banda, se puede tener una saturación debida a la alta demanda en la trasferencia de datos. La red se ve obligada a descartar paquetes o a retrasarlos, afectando la veracidad de la información que fue transmitida, el tiempo de arribo de ésta e incluso, la pérdida total de la información enviada. Para evitar esto se recurre a mecanismos de implementación de calidad y servicio en las redes, que como se ha mencionado antes, depende del enfoque que el cliente requiera.

La popularidad de la telefonía IP se ha incrementado gracias al reaprovechamiento de los recursos y la disminución en el costo de las llamadas, al hacer uso de una red interna o el internet. Sin embargo, sin mecanismos de QoS, la calidad en VoIP es frágil en comparación con la calidad obtenida en los sistemas telefónicos tradicionales. Los problemas de calidad suelen ser abundantes, y la mayoría de las veces, inherentes a la utilización de la red.

A pesar de las limitaciones que se tienen en la actualidad, existen técnicas que ayudan a la solución de algunos de los principales problemas, en lo relativo a la calidad de servicio (QoS) de una red VoIP, como son la latencia[3], la perdida de paquetes, el jitter y el eco.

[3] Puede definirse a la latencia como la suma de los retardos que existen en la red.

Algunas recomendaciones previas a la aplicación de mecanismos de QoS son las siguientes:

- Delegar los niveles de servicio a diferentes grupos, como clientes o departamentos de una empresa.
- Priorizar los servicios de red que se ofrecen a grupos o aplicaciones específicos.
- Descubrir y eliminar áreas de cuello de botella de la red y otros tipos de congestión.
- Supervisar el rendimiento de la red y proporcionar estadísticas de rendimiento.
- Regular el ancho de banda.

Modelos de servicio dentro de QoS

Existen 3 modelos de servicio dentro de la calidad de servicio, los cuales se enlistan a continuación:

- **Best effort.** En el modelo de *mejor esfuerzo*, no se aplica calidad de servicio a los paquetes, por lo que no existe prioridad alguna para cada uno de ellos, además de que no se garantiza la entrega de los mismos. En este modelo todos los paquetes tienen la misma importancia al ser enviados; de hecho es el que se usa en la actualidad en la mayoría de las redes existentes.
- **Integrated services.** Los *servicios integrados* proveen alta calidad de servicio a los paquetes que se transmiten sobre la red. Dentro de este esquema existe lo que se conoce como ancho de banda reservado, que es un canal preferencial para cierto tipo de usuarios, así como servicios y aplicaciones. Utilizando este esquema la capacidad no siempre está disponible, pero se crea un canal exclusivo cuando se tiene que usar un enlace de transmisión, es decir, se encarga de que se tengan los recursos de red necesarios para la transmisión. También recibe el nombre de *reservación de recursos*.
- **Differentiated services.** Los *servicios diferenciados* no son necesariamente los que proveen la mejor calidad de servicio en una red, ya que no está garantizada la entrega de paquetes, pero su ventaja es que son escalables, es decir, que tienen la capacidad de adaptarse, reaccionar o aumentar de tamaño, sin perder calidad en los servicios que ofrecen, ya que el tráfico es separado en diferentes clases, cada una con una calidad de servicio asignada respecto a su importancia. Estas clases que se mencionan pueden designarse según el criterio deseado por el cliente o usuario.

Este último es el enfoque que se utilizará en este trabajo para implementar la calidad de servicio.

Reservación de recursos (IntServ)

La reservación de recursos no es otra cosa que los servicios integrados. En estos se maneja el control completo de punto a punto de un canal con un ancho de banda determinado específicamente para funciones que ocupan muchos recursos, como aplicaciones de video o audio de altísima calidad.

La calidad aquí es el punto más importante ya que no pueden haber fluctuaciones de calidad en el contenido, por lo que su instalación, configuración, uso y/o alquiler son generalmente de alto costo y no todos pueden acceder a este servicio, lo que crea una brecha entre los usuarios y/o clientes.

Si bien la reservación de recursos es la mejor forma para garantizar la entrega de datos de todo tipo, es la más cara y solamente pueden acceder a ella las empresas o usuarios que tengan alto poder adquisitivo, y que saquen provecho de las ventajas que ésta proporciona.

Servicios diferenciados (DiffServ)

Como ya se mencionó, dentro de las redes de datos existen diferentes niveles de servicio según los requerimientos que se tengan, lo que estos servicios diferenciados ofrecen es simplemente una prioridad o exclusividad en lo referente al tráfico de datos. Cada paquete de información pertenece intrínsecamente a una clase, lo que lo asocia directamente a cierta calidad de servicio. La escalabilidad es una cualidad importante en los servicios diferenciados.

Para entender un poco mejor el esquema de los servicios diferenciados se procederá a explicar sus componentes.

- **Differentiated Services Code Point (DSCP).** Es un valor dentro del encabezado IP que se usa para asignar una calidad.

Modelo de clases

Como ya se mencionó, dentro del flujo de información en la red existen diferentes clases de tráfico. Independientemente de las necesidades de los usuarios hay algunas clases que tienen prioridad sobre otras, simplemente por la forma en que funcionan o se requieren.

Una clase se crea para poder aglomerar o juntar todos los paquetes que tengan el mismo destino o finalidad, y que compartan características de uso o funcionamiento. Ejemplos de lo anterior son los siguientes:

- Voz.
- Video.
- Transacciones bancarias/Trámites en línea.
- Señalización.
- Enrutamiento.
- Correo electrónico.

La tabla 1.1 muestra los modelos de clases que existen y cuál conviene usar con base a los servicios y aplicaciones que se tengan.

<table>
<tr><th>Modelo de 3 clases</th><th>Modelo de 5 clases</th><th>Modelo de 8 clases</th><th>Modelo base</th></tr>
<tr><td rowspan="3">Tráfico de alta prioridad</td><td rowspan="2">Tráfico en tiempo real</td><td>Voz</td><td>Voz</td></tr>
<tr><td rowspan="2">Video</td><td>Videoconferencia</td></tr>
<tr><td>Streaming video</td></tr>
<tr><td>Señalización</td><td>Señalización</td><td>Señalización</td></tr>
<tr><td rowspan="5">Datos críticos</td><td rowspan="5">Datos críticos</td><td rowspan="2">Control de red</td><td>Enrutamiento</td></tr>
<tr><td>Administración de la red</td></tr>
<tr><td rowspan="2">Datos críticos</td><td>Datos críticos</td></tr>
<tr><td>Transaccional</td></tr>
<tr><td>Datos masivos</td><td>Datos masivos</td></tr>
<tr><td rowspan="2">Mejor esfuerzo</td><td>Mejor esfuerzo</td><td>Mejor esfuerzo</td><td>Mejor esfuerzo</td></tr>
<tr><td>Scavenger (sobrantes)</td><td>Scavenger</td><td>Scavenger</td></tr>
</table>

Tabla 1.1. Modelos de clases existentes.

En la tabla anterior puede apreciarse que, dependiendo del modelo que se escoja, se tiene un esquema de separación de tráfico grande o pequeño, mismo que puede aplicarse a una red determinada con características específicas.

Recomendaciones para la aplicación de QoS

Como ya se mencionó, la estructura que tiene un sistema influye directamente en cómo se aplicarán los mecanismos de calidad de servicio. En la tabla 1.2 puede verse que Cisco maneja un esquema de mecanismos según los servicios requeridos. En este caso se maneja voz, datos, señalización y enrutamiento.

Aplicación	Recomendaciones
Enrutamiento	***Rate-based queuing + RED***
Voz	***CAC +Priority queuing***
Videoconferencia	CAC + Rate-based queuing + *WRED*
Streaming video	CAC + Rate-based queuing + WRED
Datos críticos	Rate-based queuing + WRED
Señalización	**Rate-based queuing + RED**
Datos transaccionales	Rate-based queuing + WRED
Administración de la red	Rate-based queuing + RED
Datos masivos	Rate-based queuing + WRED
Scavenger/Sobrantes	No bandwitdth guarantee + RED
Mejor esfuerzo	**Rate-based queuing + RED**

Tabla 1.2. Esquema de mecanismos de calidad de servicio de Cisco.

Congestión en la red

La congestión en una red se presenta cuando la tasa de transmisión con la que los paquetes arriban a una interfaz excede el límite con el que ésta puede recibirlos, lo que crea un cuello de botella que dificulta, retrasa, limita y descarta paquetes como forma de compensación para poder seguir transmitiendo.

Existen varias formas en la que una interfaz puede quedar a merced de una tasa de transmisión mayor de paquetes que la propia, ya sea por exceso de tráfico, por errores en la configuración de la misma o por la capacidad del enlace.

Cuando hay exceso de paquetes se produce un fenómeno llamado ***tail drop***, mismo que hace que se eliminen dichos paquetes conforme van llegando; evitar la congestión engloba una serie mecanismos de QoS que sirven para que no se produzca el descarte de paquetes. Algunos de esos mecanismos son los siguientes:

- RED. Random Early Detection.
- WRED. Weighted Random Early Detection.

RED

Este mecanismo evita que se produzca el descarte de paquetes que llegan a una interfaz, de la siguiente manera: elimina paquetes de forma aleatoria antes de que se produzca el descarte masivo.

Aquí no existe una diferenciación entre tipos de flujos, es decir, se hace de forma aleatoria. RED es recomendado cuando se trabaja con flujos de tráfico TCP ya que estos disminuyen el tráfico una vez que se ha comenzado a usar RED, mientras que los otros flujos no lo hacen.

RED basa su funcionamiento en dos valores o cotas, mínimo y máximo; cuando hay menos paquetes en la cola de lo que está marcado como umbral mínimo, no pasa nada; cuando se excede el umbral máximo se descartan todos los paquetes; cuando el valor de la cola se encuentra entre umbrales se descartan paquetes de forma aleatoria.

WRED

Funciona de forma parecida a RED, pero además brinda la opción de poder decidir qué tipo de tráfico es el que se va a descartar; esta prioridad se basa en la precedencia IP o DSCP
WRED descarta los flujos de tráfico que no son IP antes que los que sí lo son. No es recomendada su aplicación dentro de VoIP, por la sensibilidad intrínseca que tienen los paquetes de voz para con los retardos.

Conceptos importantes

En esta sección se analizarán conceptos básicos y quizás sencillos, pero importantes para la comprensión de conceptos posteriores.

Digitalización

El término digitalizar hace referencia a la acción de convertir una señal analógica en una digital, para ello consta de varios pasos en los que el audio (la voz en este caso) es convertido.
La digitalización se compone de los siguientes pasos:

- Muestreo. Consiste en tomar muestras cada cierto intervalo de tiempo dentro del ***rango dinámico*** previamente definido. Debe tenerse una frecuencia de muestreo que permita que no se deteriore la señal pero que tampoco tenga valores en exceso. Siempre hay que tener en cuenta el teorema de Nyquist[4].
- Cuantización. En esta parte lo que se hace es convertir los valores analógicos a digitales, para que cada valor análogo tenga su correspondiente en digital, es decir, asociar a cada valor de tiempo un nivel de amplitud correspondiente. Para esto puede haber truncamientos, o redondeos de un valor hacia el nivel al que más se acerque. El número de niveles de cuantización dependerá directamente del número de bits considerados durante la cuantización.
- Codificación. Por último se debe representar numéricamente con un código establecido o estándar, siendo el binario el más común.

El objetivo de la digitalización es poder procesar el audio a una mayor velocidad y con menor ancho de banda en comparación con lo que se tendría de forma analógica, ya que las señales analógicas requieren más ancho de banda.

[4] **Teorema de Nyquist-Shannon**. Establece que la frecuencia a la que se muestrea una señal debe ser, como mínimo, el doble de la frecuencia máxima de la señal analógica.

En la figura 2.1 puede verse el proceso de digitalización de una señal análoga.

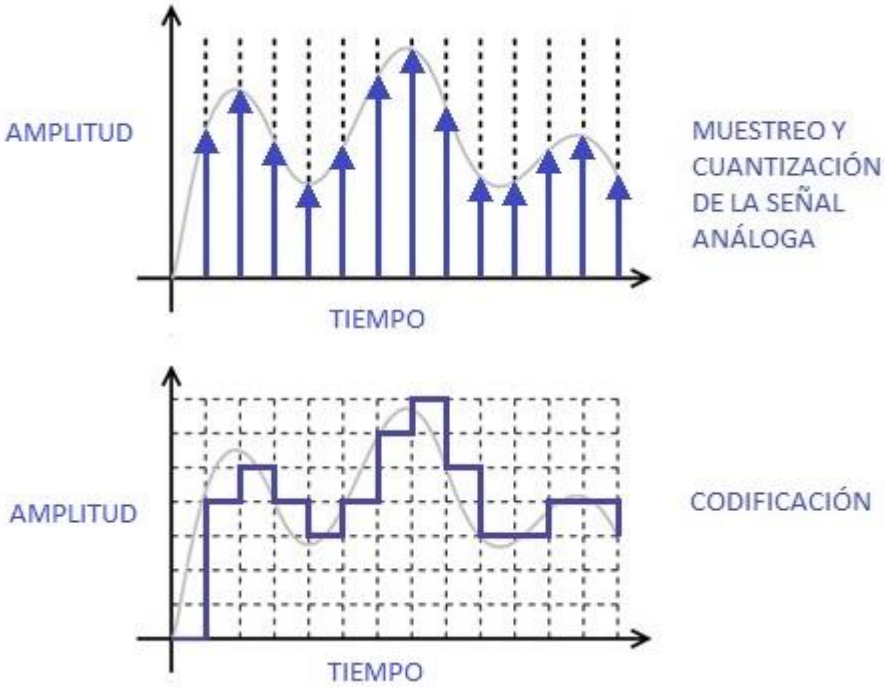

Figura 2.1. Digitalización de una señal análoga.

Compresión

La compresión consiste en la reducción de la cantidad de datos a transmitir, sin alterar la información que contiene. Esto es de interés ya que se suele tener una tasa de transmisión fija, por lo que la compresión puede resultar conveniente. Para realizar la compresión de las señales se usan complejos algoritmos de compresión. Existen dos tipos de compresión:

- Compresión sin pérdidas: en esencia se transmite toda la información, pero se elimina la información redundante.
- Compresión con pérdidas: se desprecia cierta información considerada irrelevante para el oído humano basándose en la acústica. Este tipo de compresión puede producir pérdida de calidad en el resultado final.

Ambos métodos tienen ventajas y desventajas propias. La compresión sin perdidas es adecuada si se requiere que la información origen arribe de manera fidedigna, afectando la ***relación de compresión***. La compresión con pérdidas tiene una alta relación de compresión pero se disminuye drásticamente la calidad y la información puede perder su transparencia.

En compresión, la señal puede ser codificada utilizando esquemas de tasa de transferencia constantes (**CBR**) o variables (**VBR**).

En el caso de CBR, siempre se necesita la misma cantidad de bytes para almacenar un intervalo determinado de tiempo. Es útil si se tiene un ancho de banda limitado y se quiere que la transmisión en tiempo real ocupe una porción de ancho de banda. En telefonía y aplicaciones de voz suele ser utilizado ya que ofrece tráfico de baja latencia con características a la entrega predecibles.

En VBR, la tasa se ajusta de acuerdo a las demandas de la señal, ya que diferentes partes de la información requieren más bits que otras, por ejemplo, un silencio requiere menos bits. Con VBR se puede tener un codificador más eficiente ya que mantiene un contenido con calidad constante.

A pesar de sus ventajas, VBR tiene dos inconvenientes principales: en primer lugar, hablando de una calidad específica, no hay ninguna garantía acerca de la **tasa de bits media** final. En segundo lugar, para algunas aplicaciones en tiempo real como voz sobre IP, lo que cuenta es **la tasa de bits máxima**, la cual debe ser lo suficientemente baja para el canal de comunicación.

En la figura 2.2 se observa cómo varían las tasas de transmisión según la aplicación o uso que se encuentre presente, como por ejemplo la música.

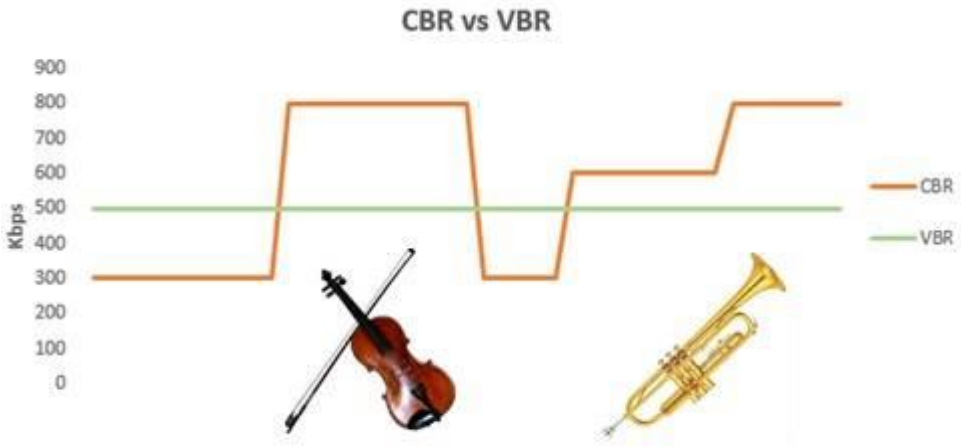

Figura 2.2. Tasas de transferencia.

Códecs

El nombre códec viene de ***coder-decoder***; es un programa, aplicación, circuito o dispositivo que puede convertir o transformar un flujo de datos y viceversa. También hacen compresión y descompresión de datos según se requiera. Los estándares de codificación son definidos por la ***ITU***.

Es importante considerar el uso de códecs en aplicaciones como voz sobre IP ya que afectan el comportamiento de dichas aplicaciones directamente. Los códecs tienen especial relevancia en enlaces de baja tasa de transmisión, pues se aseguran de no desperdiciar el ancho de banda disponible.

Existen muchos estándares de codificación dentro de las telecomunicaciones, algunos de los más usados para la telefonía son el G.711 y el G.729.

Estándar G.711

Sirve para codificar audio con una tasa de 64 kbps, es decir, toma 64000 muestras de la señal de audio en un segundo, después convierte cada pequeña muestra de información digital y la comprime para poder ser transmitida; tiene muy pocas pérdidas. Funciona mediante la modulación de pulsos codificados (PCM).

Con este esquema de codificación, la voz digitalizada puede distribuirse directamente por la red pública conmutada ***PSTN*** o hacia una central telefónica ***PBX***. Una ventaja de usar este estándar es que mejora la relación señal a ruido ***SNR***. Existen 2 tipos dentro de este esquema de codificación:

- Ley μ. Se usa en América del Norte y Japón.
- Ley A. Se usa en Europa y el resto del mundo.

Estándar G.729

Utiliza un método conocido como ***CS-ACELP***, mismo que codifica la voz con una tasa de 8 kbps, lo que se traduce en 8000 muestras por segundo, es el más utilizado, tiene el balance perfecto entre calidad de sonido y eficiencia en el uso de banda ancha.

En la tabla 2.1 se muestran las ventajas y desventajas de cada uno de los tipos de anexos que existen en el estándar de codificación G.729.

Tipo	Anexo	Tasa	Ventajas	Desventajas
G.729a	A	8 kbps	Menos procesamiento	Menor calidad de voz
G.729b	B	8 kbps	Soporta ***VAD*** y ***CNG***	Mayor procesamiento
G.729ab	AB	8 kbps	Combina los dos anteriores	
G.729d	D	6.4 kbps	Más rapidez	Peor calidad de voz
G.729e	E	11.8 kbps	Mejor calidad de voz	Más lentitud

Tabla 2.1. Ventajas y desventajas de los distintos tipos de anexos del estándar G.729.

Debe mencionarse que con este estándar en particular no existe confiabilidad a la hora de transmitir audio, música, tonos ***DTMF***, señales de módem ni fax, por lo que generalmente se recurre al estándar G.711 cuando se van a utilizar estas aplicaciones, pero es importante destacar que sigue siendo de amplio uso para la compresión de datos de audio cuando lo que se requiere es un uso mínimo del ancho de banda.

La figura 2.3 muestra los estándares de codificación utilizados en paquetes de voz.

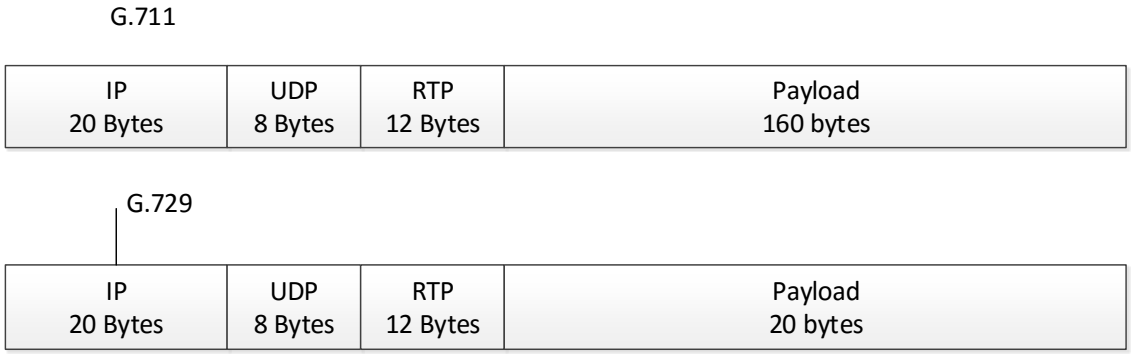

Figura 2.3. Modelos de paquetes de voz con los estándares G.711 y G.729, respectivamente.

Protocolo RTP y RTCP

El protocolo ***RTP*** está situado en la capa de aplicación del ***modelo OSI***; éste funciona sobre el protocolo ***UDP*** en la capa de sesión del modelo OSI como se ilustra en la figura 2.4. El protocolo RTP añade la identificación del ***payload***, el orden, el momento de salida de los paquetes (para detectar las pérdidas de paquetes, la existencia de desorden a la llegada de su destino, el retraso y el jitter).

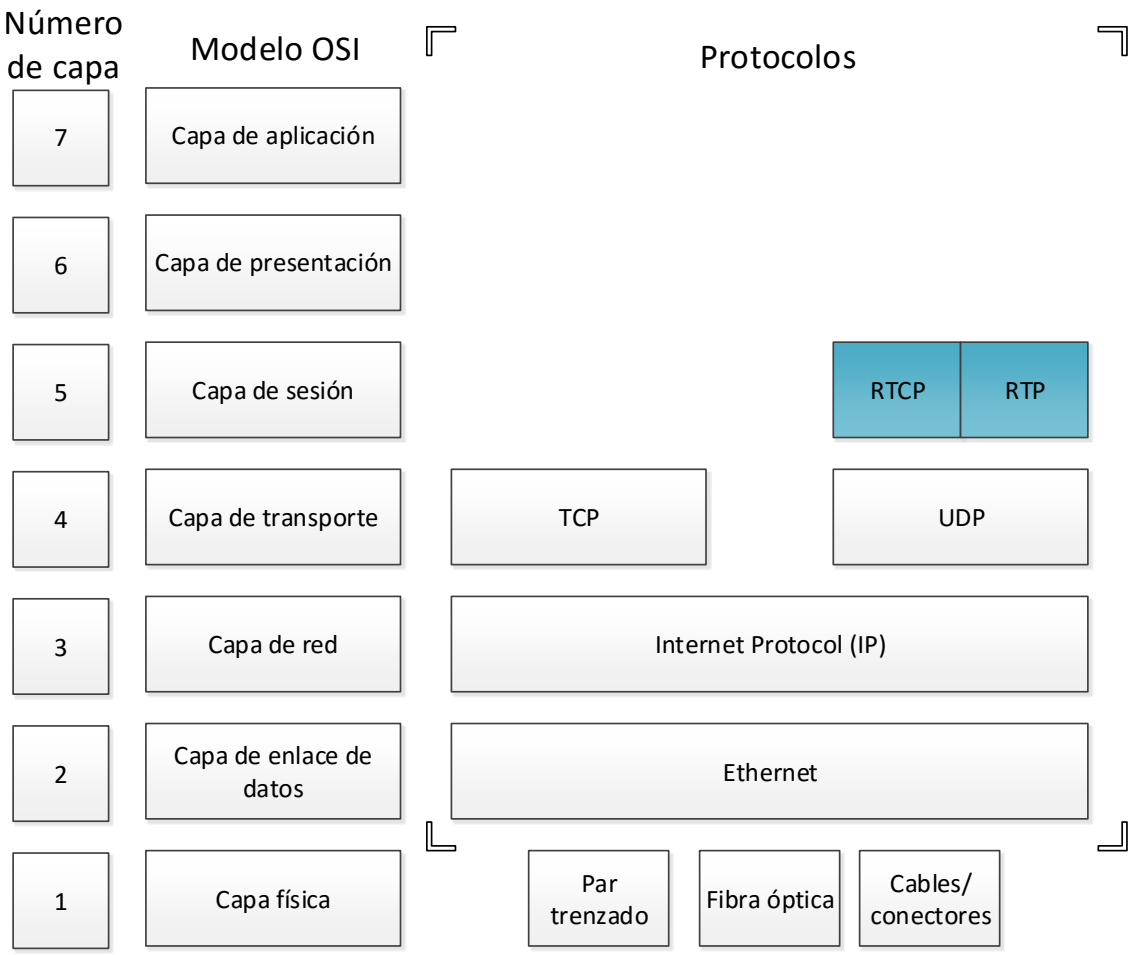

Figura 2.4. Protocolo RTP Y RTCP en el modelo OSI.

En la figura 2.5 se muestra el diagrama de un paquete de voz montado en una trama de capa 3, donde se pueden observar los protocolos IP, UDP y RTP contenidos, así como la carga útil del paquete.

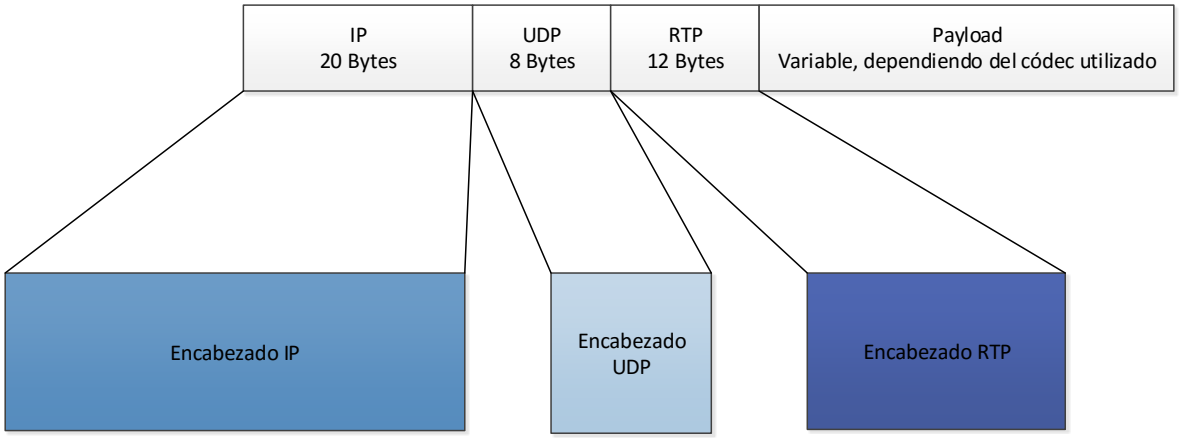

Figura 2.5. Paquete de voz sobre IP.

Los tamaños de los encabezados así como sus campos pueden observarse individualmente en las figuras 2.6, 2.7 y 2.8 respectivamente, para un mejor entendimiento de tamaño de los encabezados de cada protocolo:

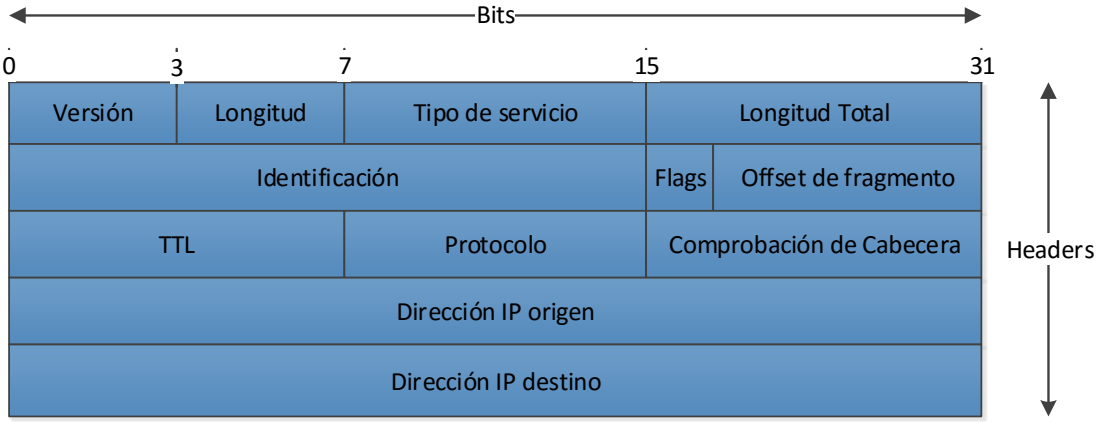

Figura 2.6. Encabezado IP.

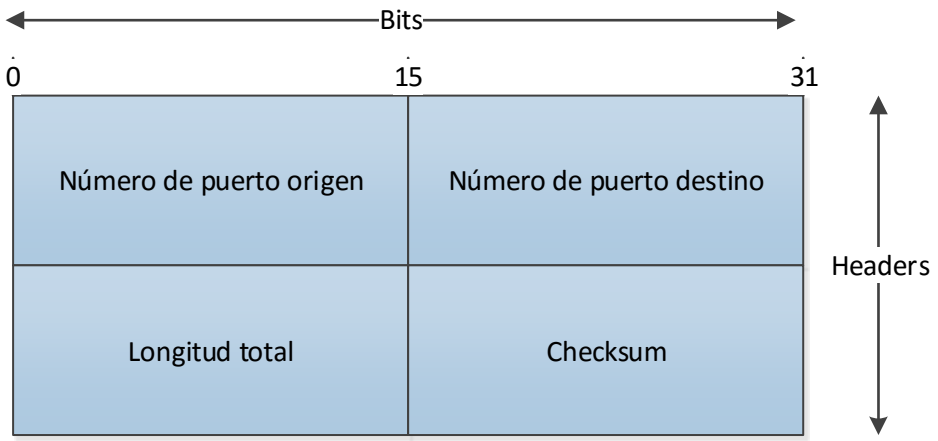

Figura 2.7. Encabezado UDP.

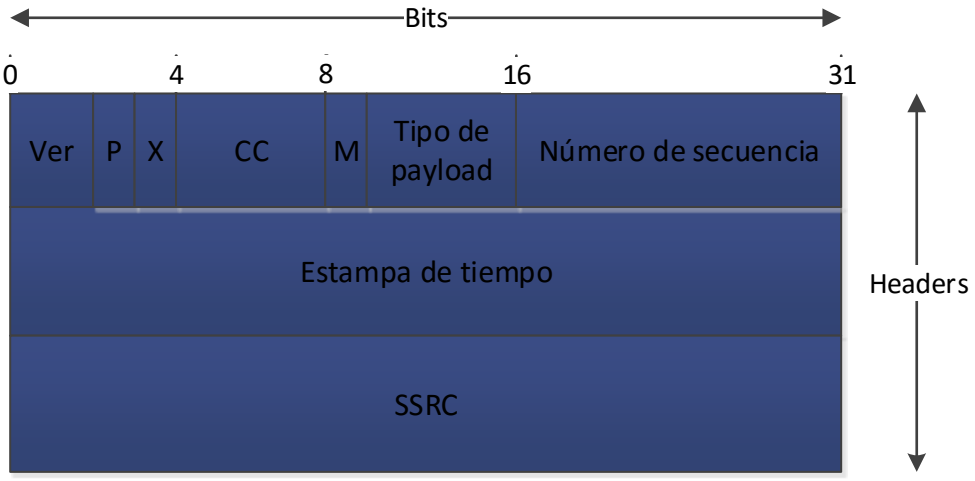

Figura 2.8. Encabezado RTP.

En la capa de red se agregan encabezados a la trama; un encabezado importante para la calidad de servicio es el Type of Service o también conocido como ToS, el cual fue empleado originalmente para clasificar y priorizar a los diferentes tipos de tráfico existentes en una red.

Dentro del encabezado IP, que se muestra en la figura 2.6, se puede ver el campo conocido como ToS, mismo que se menciona a continuación debido a su importancia dentro de QoS. Los paquetes IP tienen el campo ToS para marcar paquetes en un byte de espacio, que se divide en 3 bits para la precedencia IP, 2 para la parte de ECN (Explicit Congestion Notification), y el resto para la compatibilidad ToS-DSCP.

El modelo DiffServ mantiene el byte ToS bajo el nombre de Differentiated Service (DS), aunque con un formato diferente, el cual se presenta enseguida.

Campo ToS/DSCP

El campo DSCP utiliza los ocho bits que fueron anteriormente utilizados por el byte ToS para asegurar la compatibilidad entre protocolos así como entre equipos, mismos que puede apreciarse en la figura 2.9.

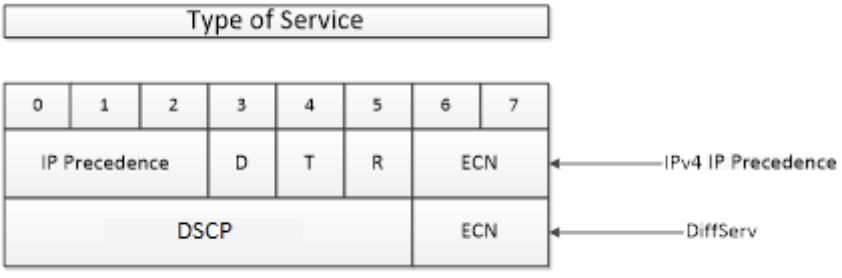

Figura 2.9. Campo Type of Service/DSCP.

Relacionado con el campo DSCP, se encuentran los siguientes conceptos:

- **Behavior Aggregate (BA).** Es un conjunto de paquetes con el mismo valor DSCP que se dirigen a una misma dirección.
- **Per Hop Behavior (PHB).** Es el comportamiento que se aplica y se presenta en un BA, mismo que puede ser modificado mediante diversas técnicas o mecanismos de condicionamiento.

La tabla 2.2 muestra donde pueden observarse los valores que toma el campo DSCP según el tipo de PHB que use, así como la aplicación para la que está reservado el servicio.

Bits	Valor	Clase	PHB	Aplicación
0-2	000	0	Default	Servicio Best effort
0-2	101	5	Expedited Forwarding (EF)	Servicio con poco retraso
0-2	001 010 011 100	1-4	Assured Forwarding (AF)	Servicio con ancho de banda garantizado
0-2	110 111	6-7	Internetwork & Network Control	Tráfico de control y protocolos de enrutamiento
3-5	000	N/A	Class Selector	Compatibilidad con dispositivos que no usen el campo DSCP

Tabla 2.2. Tipos de PHB dentro del campo DSCP.

Requerimientos de ancho de banda para aplicaciones de voz

Como ya se ha indicado, se utiliza el protocolo RTP para el envío de paquetes de voz sobre una red de datos. Este protocolo a su vez se monta sobre UDP, el que a su vez se monta sobre IP, para así viajar en la LAN sobre Ethernet. El ancho de banda requerido dependerá del ***overhead*** que genere la transmisión de estos paquetes, del estándar de codificación utilizado y el tamaño de la ventana de transmisión.

La selección del codificador-decodificador correcto determina ciertos factores en el tratamiento de la señal tales como la calidad vocal, la tasa de bits, el poder del cálculo, y el retraso de la señal. Entre más muestras sean encapsuladas el ancho de banda se irá reduciendo,

lo que impactaría de dos maneras muy significativas: en el retraso variable y en la ruptura de tramas.

La trama Ethernet consta de varios bits organizados en campos definidos dependiendo del tipo de trama, ya sea Ethernet IEEE 802.3 o Ethernet V2. En este caso, se considera la trama Ethernet V2 que se muestra en la figura 2.10. Se puede observar que la carga útil o payload es de 18 bytes.

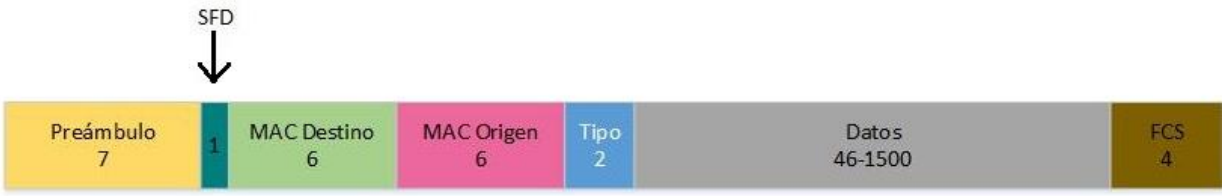

Figura 2.10. Trama Ethernet V2.

A continuación se muestra el cálculo del ancho de banda necesario para la transmisión de los paquetes de voz utilizando el estándar G.729:

- Se requiere el cálculo del payload[5] de los paquetes de voz determinados por la ventana de transmisión o tamaño de muestra, que suele ser de 20 ms por defecto.

$$Bytes_{muestra} = \frac{Tamaño\ de\ la\ muestra * BW\ del\ estándar}{8}$$

  El estándar G.729 utiliza un ancho de banda de 8 kbps por lo cual generaría un payload de voz de 20 bytes.

$$Bytes_{muestra} = \frac{20\ [ms] * 8\ [kbps]}{8} = 20\ bytes$$

- De acuerdo a la figura 2.3, se tienen 40 bytes de cabecera en la capa 3. Usando la fórmula anterior y haciendo las siguientes consideraciones se puede obtener el tamaño completo de la trama Ethernet y el ancho de banda requerido por llamada[6].

$$BW_{llamada} = (payload\ de\ voz + headers\ 3 + headers\ 2) * (packet\ ratio) * 8$$

[5] Fórmula para calcular el número de bytes encapsulados en una muestra de 20 ms de tamaño.
[6] Fórmula para calcular el ancho de banda requerido por la llamada.
El término *ancho de banda* hace referencia al usado en redes de datos e informática para determinar la capacidad y recursos de un sistema de red en bps; no debe confundirse con el *ancho de banda análogo* usado como parámetro en señales análogas, mismo que se expresa en Hz, con el que guarda relación.
Wallace Kevin, 2011, Implementing Cisco Unified Communications Voice over IP and QoS (Foundation Learning Guide), Cisco Press, 4th edition, USA, p. 130, 134.

$$BW_{llamada} = (20 + 40 + 18)\ [bytes] * \left(\frac{1}{20\ [ms]}\right) * 8\ [bits] = 31.2\ kbps$$

Realizando el mismo procedimiento se obtiene el ancho de banda requerido por llamada utilizando un estándar G.711.

$$BW_{llamada} = (160 + 40 + 18)\ [bytes] * \left(\frac{1}{20\ [ms]}\right) * 8\ [bits] = 87.2\ kbps$$

Retraso, pérdida de paquetes y jitter

La telefonía sobre internet o también llamada voz sobre IP requiere de mecanismos de calidad de servicio que ayuden a contrarrestar los daños ocasionados por el jitter, el retraso y la pérdida de paquetes.

> ***"Las redes IP deben proveer un número adecuado de servicios para soportar adecuadamente la transmisión de voz usando VoIP. Los administradores y arquitectos de red logran este nivel de servicio mediante la gestión del retraso, la variación en retraso, el aprovisionamiento del ancho de banda y la pérdida de paquetes, con técnicas QoS".***
>
> ***Kevin Wallace[7]***

RETRASO

El ***delay*** o retraso es el tiempo que tardan en llegar los paquetes de voz del transmisor al receptor, el cual es producido por la distancia que tienen que recorrer los paquetes para llegar de un punto a otro, además de retrasos producidos en la codificación y compresión, como puede verse en la figura 2.11.

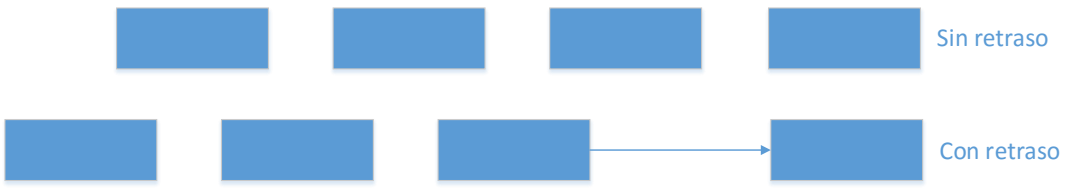

Figura 2.11. Retraso de paquetes.

Cisco define dos tipos de retardos: los retardos fijos y los retardos variables.

[7] *IP networks must provide a number of services to adequately support voice transmission using VoIP. Network administrators and architects achieve this service level by managing delay, delay variation (jitter), bandwidth provisioning, and packet loss parameters with QoS techniques.*
Wallace Kevin, 2011, Implementing Cisco Unified Communications Voice over IP and QoS (Foundation Learning Guide), Cisco Press, 4th edition, USA, p. 567.

- Los retardos fijos son intrínsecos de todas las conexiones y por lo tanto son predecibles en la mayoría de los casos, por ejemplo el retardo de serialización y el retardo de propagación.
- Los retardos variables cambian dependiendo de otras circunstancias, por ejemplo el retraso de encolamiento debido a la congestión de la red.

La norma G.114 de la ITU es la recomendada para tomar en cuenta el retraso óptimo en VoIP; según dicha recomendación un retraso de 0 a 150 milisegundos es aceptable para la mayoría de los casos y hasta 400 milisegundos para algunas aplicaciones con menos restricciones; valores mayores a 400 ms se consideran inaceptables[8].

Es importante recalcar que este cálculo de retardo en la norma sólo toma en cuenta la comunicación en un sentido y no la comunicación de ida y vuelta, como se utiliza en la telefonía sobre IP. Cisco considera razonable un retraso de 200 a 250 milisegundos tomando en cuenta los retardos variables y fijos[9].

PÉRDIDA DE PAQUETES

La pérdida de paquetes no es otra cosa que el descarte o la eliminación de los elementos que no se encuentran listos cuando se tiene que hacer una transmisión u ordenación de los paquetes; afecta mucho la comunicación ya que la telefonía sobre IP al transmitirse mediante el protocolo UDP y en tiempo real, no permite la retransmisión de paquetes, por lo tanto al haber un porcentaje alto de pérdidas, el usuario recibirá los mensajes entrecortados, afectando la coherencia de todo el mensaje.

Los paquetes de voz llegan a perderse cuando la red es inestable o se encuentra congestionada como puede se ilustra en la figura 2.12, asimismo se presentan pérdidas cuando existe mucha variación en retraso o jitter, ya que los paquetes llegan demasiado tarde para ser corregidos en lo referente al jitter. Como respuesta, el receptor notará la existencia de surcos o brincos en el audio por no estar todos los paquetes presentes al momento de la reproducción.

Tomando en cuenta la norma G.114 nuevamente, el porcentaje de pérdidas no deberá exceder al 1%. Puede que esta cifra parezca muy pequeña al principio pero si se considera que pueden haber pérdidas en cada tramo del sistema, este valor asegura que se transmita la cantidad

[8] **Norma G.114 de la ITU. One-way transmission time.**
[9] **Wallace Kevin, 2011, Implementing Cisco Unified Communications Voice over IP and QoS (Foundation Learning Guide), Cisco Press, 4th edition, USA, p. 261.**

necesario de información sin que haya problema en las comunicaciones.

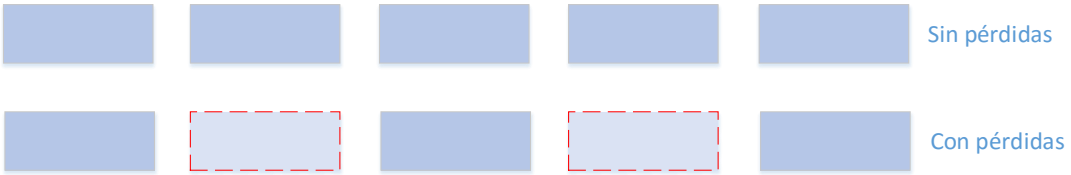

Figura 2.12. Pérdida de paquetes.

JITTER

El jitter se define como la variación en el retardo de los paquetes para llegar a su destino. En los sistemas de VoIP el transmisor genera una secuencia de paquetes de voz espaciados uniformemente, pero debido al tráfico en la red, los paquetes no llegan al receptor con el mismo espaciamiento de manera uniforme; a algunos paquetes les toma más tiempo llegar a su destino que a otros. Es de suma importancia que el receptor reciba los paquetes de voz espaciados uniformemente para lograr una buena calidad de voz.

Los sistemas de VoIP en los que los paquetes de voz tengan retardos de hasta 400 ms, como por ejemplo un enlace vía satélite, aunque incómodos, son tolerables por los usuarios, pero no sucede así con el jitter, es decir, con la variación del retardo de llegada de los paquetes, ya que cuando es grande, la voz se percibe entrecortada.

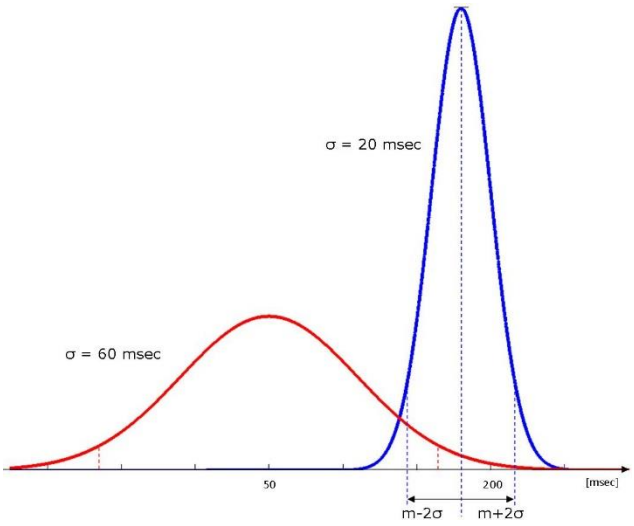

Figura 2.13. Tipos de jitter en un flujo de paquetes.

En la figura 2.13 se muestran dos casos diferentes en la forma que los paquetes llegan a su destino. En la distribución de llegada de paquetes en azul, los paquetes tardan en promedio 180 ms en llegar a su destino, la mayoría de los paquetes llegan entre 140 y 220 ms (± 2σ). En

el caso de la distribución en rojo, el promedio de llegada de los paquetes a su destino es menor, 50 ms, pero la variación del retardo en que llegan (jitter) es mayor.

Dicho de otra forma, en el caso azul se tiene una distribución aguda porque los valores de retraso son más estables y se encuentran más cercanos a la media, mientras que en el caso rojo la distribución es más suave porque los valores de retraso distan mucho de la media, de ahí que el caso rojo presente más jitter.

Según el fabricante Cisco, el jitter en sistemas de VoIP debe ser menor a 30 ms[10]. Si el valor es menor a 30 ms el jitter puede ser compensado de manera apropiada, si no, debe ser minimizado.

Un método empleado para disminuir el efecto del jitter es la utilización del dejitter-***buffer***, aunque éste afecta el retraso total de la comunicación porque se deben amortiguar todos los retrasos y después mandarlos al DSP como se ve en la figura 2.14. El dejitter-buffer consiste en la creación de una fila o almacén para recibir los paquetes y repartirlos con un ligero retraso. Si un paquete no está en el búfer cuando sea necesario se descarta. Típicamente el retraso añadido por el dejitter-buffer es de 10 a 30 milisegundos.

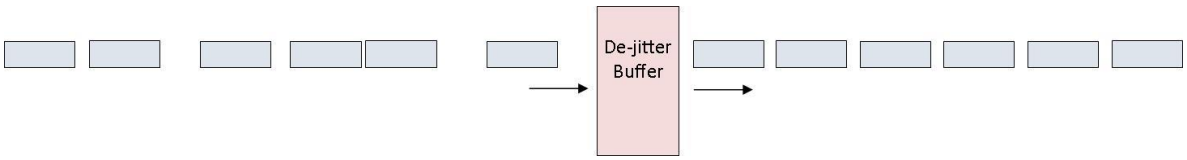

Figura 2.14. Funcionamiento del dejitter-buffer.

[10] **Tim Szigeti; et al, 2013, End-to-End QoS Network Design (Quality of Service for Rich-Media & Cloud Networks), Cisco Press, 2nd edition, USA, p.5.**

Señalización

La señalización es una de las partes más importantes que deben tomarse en cuenta cuando se trabaja con voz sobre IP, ya que para que se realice la llamada primero debe haberse formado un enlace sobre el cual la llamada ha de desarrollarse. La señalización se considera como tráfico de alta prioridad, por lo que esto debe tomarse en cuenta en el momento en que vayan a definirse las clases de tráfico con las cuales se trabajará.

La señalización, así como los demás tipos de tráfico, tiene asignado un valor predeterminado, mismo que puede observarse en la tabla 2.3.

Aplicación	Precedencia IP	PHB	DSCP	CoS
Enrutamiento	6	CS6	48	6
Voz	5	EF	46	5
Videoconferencia	4	AF41	34	4
Streaming video	4	CS4	32	4
Datos críticos	3	AF31	26	3
Señalización	**3**	**CS3**	**24**	**3**
Datos transaccionales	2	AF21	18	2
Administración de la red	2	CS2	16	2
Datos masivos	1	AF11	10	1
Scavenger/Sobrantes	1	CS1	8	1
Mejor esfuerzo	0	0	0	0

Tabla 2.3. Asignación de prioridades según el tipo de tráfico.

Continuando con la señalización, debe hacerse la aclaración de que en el pasado Cisco definía la señalización con un PHB con un parámetro de *AF31*, pero después se hizo el cambio a *CS3*, por lo que varía el PHB según el equipo telefónico que se use.

Para las mediciones realizadas en este trabajo se hizo una modificación del PHB *CS3* al PHB *AF31* durante el proceso de configuración, con el cual las llamadas que se realizaron entraron sin ningún problema, como puede verse en la sección posterior de resultados.

Mecanismos de calidad en servicios diferenciados

Los mecanismos de calidad de servicio son esquemas usados para brindar una forma de manifestar qué tipos de tráfico o servicios llevan más importancia sobre otros. Para ello, cada método aplica su comportamiento sobre el tráfico que cruza una interfaz, con lo que el tráfico es afectado de alguna manera por el tipo de mecanismo aplicado.

> ***"QoS ofrece técnicas utilizadas en la red para priorizar un tráfico determinado respecto a otros. El aspecto más importante de transportar tráfico de voz en una red de datos es mantener un nivel de QoS adecuado. Los paquetes de voz deben ser entregados lo más rápido posible con mínima fluctuación, pocas pérdidas y mínimo retraso".***
>
> ***Ernesto Ariganello[11]***

Existen muchos tipos de mecanismos de calidad de servicio dependiendo del tipo de red sobre el cual se esté desplegando el mecanismo, así como del funcionamiento propio de la red; algunos de estos mecanismos son configuraciones. Entre los que se ocuparon en este trabajo durante el proceso de configuración se encuentran los siguientes:

- Clasificación.
- Marcado.
- ***Policing***.
- ***Shaping***.
- Encolamiento.
- Fragmentación.
- Intercalado.

Enseguida se explica con más detalle en qué consiste el trabajo de cada uno de ellos, así como la parte del proceso en la que deben situarse, ya que no todos los métodos de calidad de servicio pueden aplicarse directamente.

Entender el funcionamiento de los mecanismos de calidad ayuda a aplicarlos apropiadamente bajo el entorno correcto, y asegura que funcione no solamente el mecanismo sino que también el tráfico adecuado se administre de forma conveniente para el usuario y se obtengan los resultados esperados.

[11] **Ariganello Ernesto; Barrientos Sevilla Enrique, 2010, Redes Cisco, CCNP a fondo (Guía de estudio para profesionales), AlfaOmega, 1ª edición, México, p. 443.**

Clasificación de tráfico (Classification)

La idea principal de clasificar el tráfico consiste en identificar y marcar los paquetes que entran a un sistema según las aplicaciones o el uso que se le va a dar a cada tipo de paquete, con lo que se tiene que se puede clasificar mediante diversos criterios, como por ejemplo:

- DSCP.
- Precedencia IP.
- Dirección fuente.
- Dirección destino.

Una de las ventajas de clasificar el tráfico que entra a una interfaz es que puede dirigirse hacia cierto destino o aplicación, es decir, se canaliza directamente con alguna funcionalidad del sistema con lo que fomenta la eficiencia del mismo.

Clasificar también sirve para asignar una credibilidad o certeza cuando exista conexión con un dispositivo que necesite basarse en un valor para asignar alguna prioridad; este caso se presenta cuando existe desconfianza sobre los dispositivos vecinos que se tengan, además puede llegar a ver una reclasificación de paquetes cuando no exista dicha confianza.

Una de las herramientas que se usan para la clasificación es el Modular QoS CLI (MQC).

Modular QoS CLI (MQC)

MQC es una herramienta que proporciona ***modularidad*** en la configuración de la calidad de servicio. Esta utilidad ofrece la facilidad de definir la configuración mediante la interfaz de la línea de comandos, lo que permite que el administrador defina los parámetros de los mecanismos de la calidad de servicio de una forma clara y directa.

Marcado de tráfico (Marking)

El marcado de tráfico o ***marking***, mismo que también se conoce como coloreado de paquetes, es denotar o contrastar un tipo de tráfico con respecto a otros. En esta parte lo que se hace es fijar los valores del paquete en la parte DSCP o precedencia IP de acuerdo a la clase a la que el paquete pertenezca.

También sirve para identificar el seguimiento que se le ha de dar al paquete entrante, pues a partir del valor con que el paquete fue marcado se determina el uso o trato que éste recibirá en etapas posteriores.

Policing

El uso de policing se da para condicionar o limitar la entrada de un flujo de paquetes a la interfaz de un sistema, asimismo controla las congestiones que puedan haber en la red y puede asignarse cierto ancho de banda a cada tarea.

Condicionar el tráfico mediante policing sirve para que ese tráfico sea restringido a un porcentaje del ancho de banda total, mostrado en la figura 3.1. La aplicación de *traffic policing*, como también se le conoce, puede ser en la entrada o salida de una interfaz.

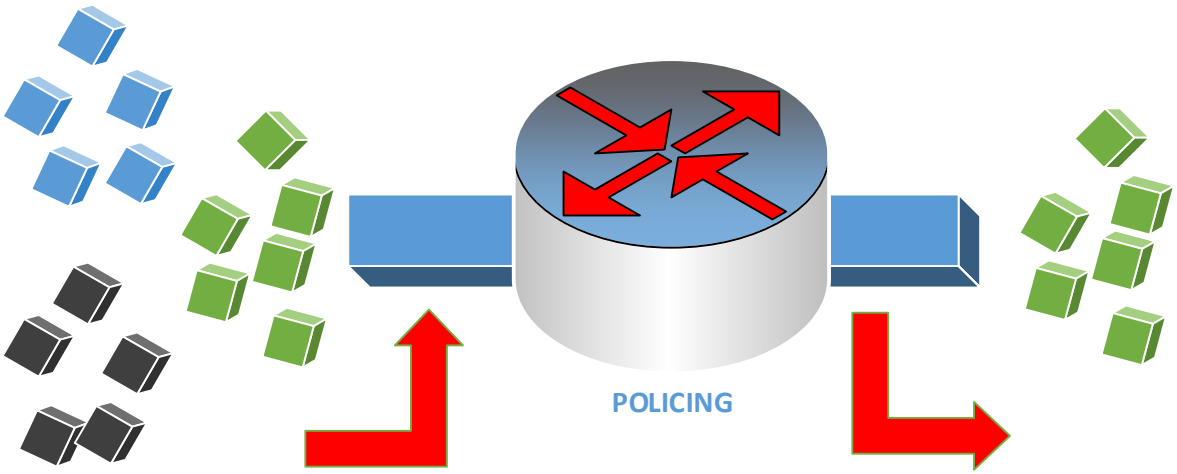

Figura 3.1. Policing.

Una de las herramientas que se usan para la aplicación de traffic policing es Class-Based Policing, mismo que se basa en la utilización de clases de tráfico creadas previamente y las toma para aplicaciones posteriores.

Shaping

Uno de los mecanismos o herramientas que se usa en los servicios diferenciados para brindar calidad de servicio es el denominado ***traffic shaping***. Mientras que con traffic policing se busca salvaguardar el ancho de banda existente, lo que se hace con shaping es suavizar o atenuar las diferencias en la tasa de transmisión que puedan haber en una red, limitándolas a un valor determinado.

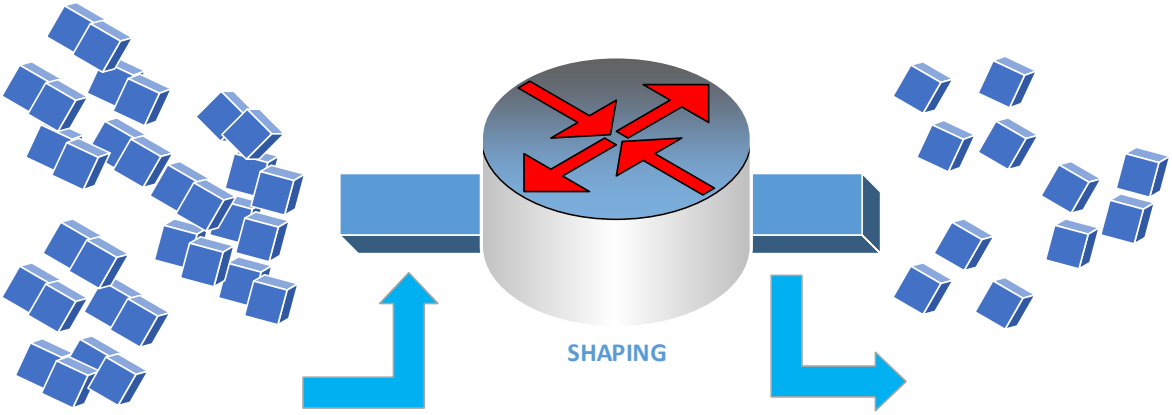

Figura 3.2. Shaping.

Traffic shaping funciona controlando el flujo de salida en una interfaz para ajustar la tasa de transmisión al valor que corresponda y se asegura de que el tráfico cumpla con las restricciones que se tengan para cada sección, de la forma que muestra la figura 3.2. Asimismo se encarga de colocar en un búfer los paquetes en exceso que existan en ese momento con el fin de conservar la tasa fijada, por lo que se reduce la congestión.

Comparación entre policing y shaping

Es importante mencionar que en comparación con policing, traffic shaping presenta ciertas ventajas, una de ellas es que la traffic shaping encola paquetes en un búfer cuando hay tráfico en exceso.

En la tabla 3.1 pueden apreciarse las ventajas y desventajas de un método con respecto al otro.

Policing	Shaping
Puede aplicarse en la entrada y salida de una interfaz	Solamente puede aplicarse en la salida de una interfaz
Los paquetes no contemplados son descartados, lo que causa una retransmisión TCP	Los paquetes no contemplados se almacenan, lo que disminuye las retransmisiones TCP pero aumenta el retardo
Permite el marcado de tráfico	No permite el marcado de tráfico
Usa menos búfers	Es compatible con Frame Relay

Tabla 3.1. Ventajas y desventajas de policing y shaping.

Como puede verse en la tabla 3.1, policing presenta una ventaja muy importante por sobre shaping, la repercusión que existe en la retransmisión; para este estudio se está trabajando con voz en el protocolo UDP, donde la retransmisión de paquetes TCP es irrelevante porque los paquetes de voz llegarían fuera de tiempo y perjudicial ya que los paquetes retransmitidos no tendrían coherencia con el resto de los paquetes enviados.

La aplicación de shaping además añade un retraso variable, el cual genera jitter, una razón más para preferir policing por sobre este. Como último punto, se tiene la figura 3.3, donde puede observarse el funcionamiento de policing sobre el tráfico.

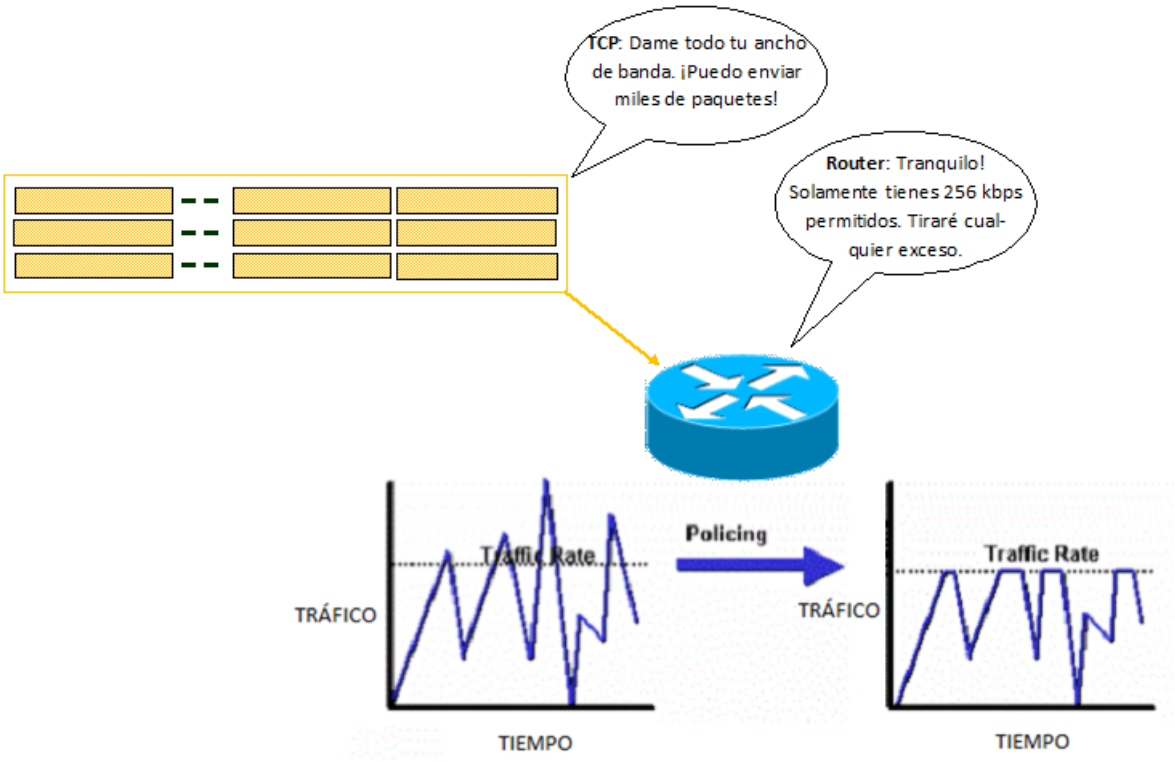

Figura 3.3. Variación de la ventana de transmisión con policing.

Cuando se usa policing, se descartan los paquetes excedentes pero también se reduce el tamaño de la ventana de transmisión, que está variando, mientras que con shaping se mantiene una ventana de transmisión estable.

Ventana de transmisión

Dentro del protocolo TCP existe algo que se conoce como ***windowing***, dicho concepto se basa en la idea de que al momento de transmitir se crea una ventana deslizante, misma que va aumentando de tamaño hasta alcanzar su máximo; el tamaño de la ventana define cuanto se ha de enviar entre el emisor y el receptor antes de recibir una notificación de llegada por parte del receptor y es un proceso dinámico establecido entre los dispositivos terminales que mantienen la conexión.

Colas (Queuing)

Para la implementación de la calidad del servicio se tiene que considerar el tipo de colas que se está manejando en el medio. Las colas determinan en qué orden van a salir los paquetes del búfer debido a diversos factores como peso o prioridad.

- **FIFO (First-In First-Out)**

  Es el mecanismo más sencillo. Los paquetes se almacenan en el búfer cuando existe congestión en la red y cuando se va liberando el medio permite el envío de los paquetes manteniendo el orden de llegada al búfer.

  FIFO es utilizado por defecto en productos Cisco cuando los enlaces son superiores a T1 (1.544 Mbps). La desventaja de este algoritmo es que está limitado a la capacidad del búfer en momentos de congestión. Es por ello que no es recomendable para QoS.

- **PQ (Priority Queueing)**

  Este algoritmo da prioridad estricta al tráfico importante, es decir, asegura que el tráfico prioritario reciba un servicio rápido en cada punto de la red gracias a la clasificación de los paquetes en cuatro colas: alta, media, normal y baja prioridad.

  A pesar de darle prioridad a los paquetes, no se cuenta con una garantía del ancho de banda para éstos.

- **CQ (Custom Queueing)**

  En este caso, el tráfico se clasifica en varias colas teniendo un límite de colas configurables. Los límites de las colas se calculan en base al tamaño medio de los paquetes, la unidad de transmisión máxima (MTU) y el porcentaje de ancho de banda mínimo garantizado que se asignará a cada cola.

  El ancho de banda del medio será compartido equitativamente, lo que no permite proporcionar una prioridad en el servicio. La configuración de las colas es relativamente complicada.

- **WFQ (Weighted Fair Queueing)**

  A diferencia de los mecanismos anteriores, WFQ es adaptativo, lo cual indica que se ajusta a los cambios producidos en la red. Esto permite que proporcione un tiempo de respuesta rápido. Se organiza el tráfico en tiempo real poniéndolo al principio de una

cola y, mediante el DSCP y la precedencia IP, clasifica los paquetes en colas independientes. Mediante el peso se determina cuántos paquetes son atendidos a la vez. No es escalable dentro de una gran red.

Con este elemento no se puede dar una garantía del ancho de banda al tráfico ni una prioridad a los servicios. Cisco utiliza WFQ por defecto en enlaces inferiores a T1 (1.544 Mbps).

- **CBWFQ (Class-Based WFQ)**

  Se utiliza MQC para organizar el tráfico en clases. Estas clases se colocan en colas con un determinado ancho de banda reservado o en una cola sin reservas por defecto. CBWFQ permite el uso de listas de control de acceso y protocolos o nombres de interfaz de entrada para definir cómo se clasifica el tráfico, proporcionando de este modo una amplia variedad de clasificaciones.

  En este mecanismo no se puede asignar una prioridad a los servicios. Con CBWFQ se pueden generar hasta 64 clases discretas en una misma política de servicio.

- **PQ-WFQ (Priority Queue WFQ)**

  Es también conocido como Prioridad IP RTP. Una única interfaz de comandos se utiliza para proporcionar el servicio de prioridad a todos los paquetes UDP destinados a cualquier número de puertos dentro de un rango especificado. Asigna prioridad a los paquetes RTP. Todo el tráfico restante es tratado con WFQ.

  El tráfico RTCP no tiene prioridad con este mecanismo. Bajo este escenario no se tiene la capacidad de garantizar el ancho de banda.

- **LLQ (Low Latency Queueing)**

  Antes conocido como PQ-CBWFQ. Es un contexto en el que se permite asignar las clases a ciertas colas configuradas con prioridad, ancho de banda reservado o sin reservas por defecto. En el siguiente tema se desarrolla este importante mecanismo de colas.

En la siguiente figura se puede observar generalmente cómo funciona el sistema de colas o encolamiento.

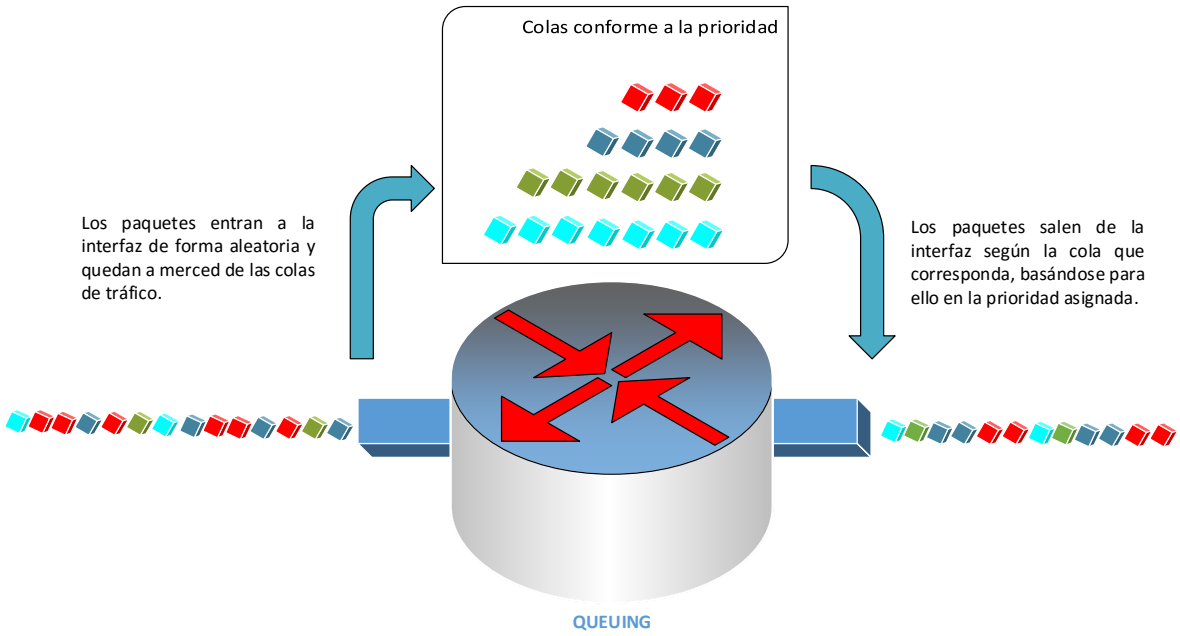

Figura 3.4. Colas de tráfico.

LLQ (Low Latency Queueing)

LLQ es una herramienta de Cisco que sirve para dar prioridad a determinada clase de tráfico. Las clases que han de priorizarse se definen mediante el ajuste de un porcentaje del ancho de banda, mismo que sirve de guía a LLQ a la hora de hacer el envío y el almacenamiento de los paquetes que llegan a cierta interfaz.

Dentro del LLQ hay dos características o puntos principales que se toman en cuenta cuando se está configurando:

- Prioridad. La prioridad se usará para ubicar una clase de alta prioridad y asignarle el ancho de banda especificado.
- Ancho de banda. El ancho de banda se usa para indicar el volumen que tendrá dicha clase, ya sea indicándole un valor directamente o mediante el uso de un porcentaje; la asignación directa de un valor para el ancho de banda sirve para limitar que una clase no rebase dicho parámetro pero a la vez limita a la clase cuando se tenga un ancho de banda mayor, pues esta se quedará enganchada a ese valor.

Además de los parámetros anteriores, también se puede resolver qué pasará con el ancho de banda restante, en caso de que se presente esta situación. El ancho de banda restante puede dividirse equitativamente entre las clases existentes, reservarse para una clase en exclusiva o no ser utilizado en absoluto, eso dependerá de las necesidades que se tengan con respecto al ancho de banda.

Como último punto, la prioridad de una clase puede asociarse directamente a la aplicación de policing, ya que ha de estar contenida en el mismo, por lo que se aprecia que LLQ facilita la determinación de la importancia de cada clase de tráfico.

LFI (Link Fragmentation and Interleaving)

La fragmentación e intercalado de las tramas es quizá uno de los mecanismos de calidad más útiles que puedan existir en este entorno, pues su funcionamiento parte de una idea muy simple: partir las tramas grandes y alternarlas con las pequeñas, de esta forma las tramas grandes que son divididos permiten que las tramas de menor tamaño también crucen una interfaz pues no la acaparan toda con su tamaño.

LFI es un mecanismo de capa 2, donde las tramas son divididas en fragmentos pequeños e iguales en tamaño y posteriormente enviados junto con las demás tramas, como se ilustra en la figura 3.5.

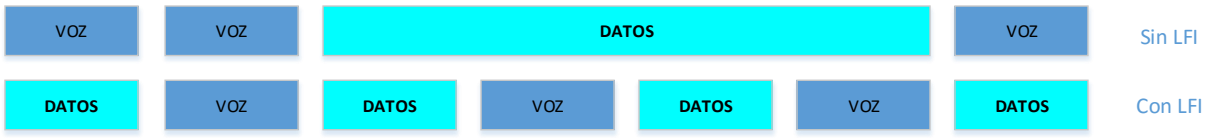

Figura 3.5. Fragmentación e intercalado de paquetes.

En la figura anterior puede apreciarse el funcionamiento de LFI con más detalle, aunque en la realidad no es tan simple, pues el router que recibe las tramas fragmentadas debe reincorporarlas nuevamente en una sola entidad, lo que gasta procesamiento y tiempo. También debe indicarse que LFI solamente funciona sobre una interfaz Multilink o Frame Relay previamente configurada.

En la fragmentación e intercalado se pueden establecer los siguientes parámetros:

- La interfaz Multilink a la que se está aplicando el mecanismo.
- El tamaño de los fragmentos que se tomarán basado en la fórmula para calcular el retraso por serialización.

La ventaja más importante de LFI es que puede reducir el retraso y el jitter en enlaces lentos con la partición que hace, característica de vital importancia para las llamadas telefónicas. LFI cobra importancia especial en este caso pues como se mencionó está dirigido a enlaces WAN con una tasa baja, menores a 768 kbps.

Retraso por serialización

Este es un retraso inherente a todos los sistemas debido a que todos presentan un retardo cuando se tienen que enviar los paquetes de un lado a otro. Este retraso está en función directa con la tasa del enlace y el tamaño del paquete. La siguiente fórmula[12] sirve para calcular el retraso por serialización.

$$Retraso\ por\ serialización\ (ms) = \frac{Tamaño\ del\ paquete\ (Bytes) * 8}{Tasa\ del\ enlace\ (kbps)}$$

Ya que el retraso unidireccional permitido en una red de VoIP es de 150 ms, Cisco recomienda que el retraso por serialización sea menor a 20 ms en un enlace. El retraso por serialización está directamente relacionado con el tamaño que el fragmento ha de tener cuando se utiliza LFI, mismo que se muestra en la siguiente fórmula[13].

$$Fragmento\ (Bytes) = \left(\frac{Tasa\ del\ enlace\ (kbps)}{8\ bits}\right) * (Retraso\ por\ serialización\ (ms))$$

MLS QoS Trust

Dentro de la configuración de un switch se encuentra un concepto llamado *mls qos trust*, este concepto hace referencia al grado de confianza que el switch debe tener cuando existe tráfico entrando en una interfaz que se encuentra conectada a un dispositivo dado.

Cisco tiene configurado por defecto que no exista confianza alguna para el tráfico que se menciona. Este concepto puede activarse mediante la línea de comandos del switch de la siguiente manera; se presentan dos situaciones cuando éste es activado:

[12] *Fórmula para calcular el retraso por serialización, en ms.*
*Serialization Delay (in seconds) = [(Packet Size in Bytes) * 8] / (Link Speed in bps)*

[13] *Fórmula para calcular el tamaño de un paquete, en bytes.*
*Fragment Size (in bytes) = [(Link Speed in bps) / 8 bits] * Serialization Delay (in sec)*
Wallace Kevin, 2011, Implementing Cisco Unified Communications Voice over IP and QoS (Foundation Learning Guide), Cisco Press, 4th edition, USA, p. 627-629.

- Si se activa el comando con la opción *pass-through dscp*, el valor DSCP original se queda adherido al paquete y se transmite tal cual al dejar la interfaz.
- Si no se activa el comando con esta opción, el valor DSCP se sobrescribe con base a un mapeo de CoS a DSCP predeterminado, donde se le asigna un valor establecido por Cisco según el tráfico que se tenga.

Al activar esta mejora de Cisco también se habilita ***CDP* trusted boundary**, que permite la opción de confiar cuando un teléfono de Cisco se ha conectado al puerto, si no hay ninguno conectado, se omite ese comando.

Comparación entre los mecanismos

En la tabla 3.2 se hace una comparación de las ventajas o desventajas, según el caso que aplique, que presenta un mecanismo con respecto a otro, así como una breve descripción de su funcionamiento.

Mecanismo de calidad de servicio	Descripción breve de su funcionamiento	Ventajas	Desventajas
Clasificación	Crea una clase para cada tipo de tráfico	Ordena un flujo de tráfico en clases o conjuntos	Se tiene que crear una clase para cada tipo de tráfico
Marcado	Marca cada clase con un valor dado	Asigna un valor a cada clase para su uso posterior	El valor asignado se queda adherido a la clase de tráfico
Policing	Condiciona el paso de cada clase de tráfico	Restringe el paso de clases no permitidas	Deben definirse para cada sistema según sus necesidades
Shaping	Controla el flujo de tráfico	Atenúa las diferencias que puedan existir en tasas de transmisión	Añade jitter y retraso a las comunicaciones existentes
LLQ	Determina el ancho de banda para cada clase	Establece y mantiene un ancho de banda en las clases definidas	Puede llegar a limitar el ancho de banda de ciertas aplicaciones
LFI	Fragmenta las tramas grandes y las alterna con las de menor tamaño	Permite el intercalado de tramas grandes y pequeñas	Las tramas que fueron segmentadas deben volver a integrarse
MLS QoS Trust	Confía en los parámetros de QoS de dispositivos vecinos	Mejora el desempeño de QoS al confiar en los dispositivos adyacentes	Solamente funciona con productos de la línea de Cisco

Tabla 3.2. Ventajas y desventajas de los mecanismos de QoS.

Implementación de mecanismos de calidad en otras redes

En las siguientes páginas se explicará un poco sobre los mecanismos de calidad de servicio existentes en otros esquemas de red, mismos que aunque tienen la misma funcionalidad para las clases de tráfico analizadas, no necesariamente funcionan de igual forma que en una red WAN como la que se plantea para este estudio.

Además se analizarán ventajas y desventajas de cada red con respecto a las otras redes mencionadas en este escrito. Se contemplan los principales esquemas de red: Ethernet, Frame Relay, MPLS y WiFi.

Ethernet

Como bien se sabe, las redes Ethernet basan su funcionamiento en el estándar 802.3, el cual ha ido evolucionando a través de los años, pues se han ido agregando nuevas versiones del mismo. En general, puede decirse que Ethernet es un estándar que se encarga de especificar qué características o rasgos se requieren para que el cableado, la señalización de la capa física y la parte referente a las tramas de la capa de enlace de datos funcionen en conjunto.

802.1q, mejor conocido como dot1q, es un estándar se encarga de normalizar o sistematizar las redes para que estas puedan funcionar entre sí, sin que exista problema alguno. Este estándar también puede llegar a conocerse como ***trunking***, ya que se utiliza para la creación de enlaces troncales donde transcurre tráfico de diferentes vlans, previamente etiquetadas.

Asociado a este mismo estándar se encuentra el estándar 802.1p, que se presenta a continuación, debido a que es el encargado de lo referente a la calidad de servicio para redes Ethernet.

IEEE 802.1p

La recomendación IEEE 802.1p es una extensión del estándar IEEE 802.1Q, ambos trabajan simultáneamente. El estándar 802.1Q especifica una etiqueta que se añade a la trama ***MAC*** de Ethernet.

Cuando la etiqueta del protocolo de identificación tiene el valor 0x8100, significa que la trama lleva la etiqueta IEEE 802.1q/802.1p. La etiqueta VLAN tiene cuatro partes:

- ID Tag (16 bits). Generalmente 0x8100.
- Prioridad (3 bits).
- Indicador de formato canónico (1 bit).
- VLAN ID (12 bits).

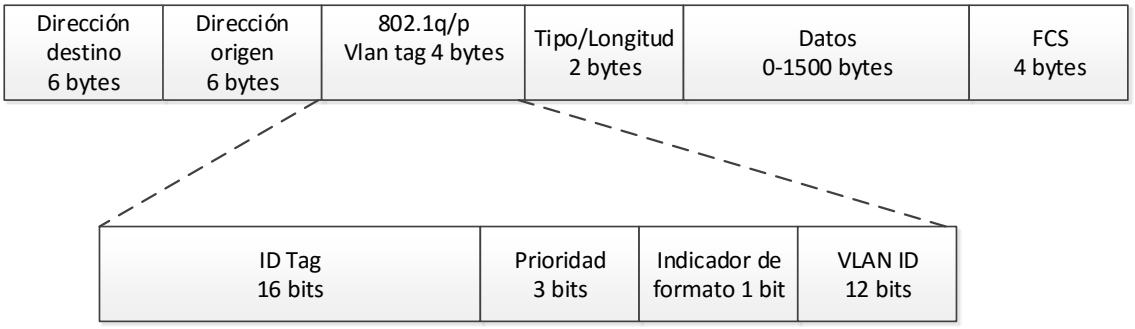

Figura 4.1. Estándar IEEE 802.1p.

Ya que el campo de prioridad no fue definido y usado en el estándar 802.1q, este campo es definido en el 802.1p. Esta extensión de la IEEE permite a los switches de capa 2 priorizar en el control de acceso al medio (MAC) y ofrecer suministros para filtrar el tráfico ***Multicast*** y asegurar que no se prolifere sobre las redes de conmutación. La figura 4.1 hace un análisis de los componentes del estándar 802.1p.

En la tabla 4.1 se aprecia que el encabezado 802.1p se compone de un campo de 3 bits que indica la prioridad, lleva uno de ocho valores de prioridad que corresponden a uno de ocho posibles niveles de servicio y su alcance se limita a la subred en la que se generaron.

Valor	Función
7	El tráfico podría ir a redes críticas como RIP y OSPF
5,6	Es para aplicaciones con retraso sensible, como video y voz en tiempo real
1-4	Es para aplicaciones de carga controlada con contenido multimedia en streaming
0	Usado por default cuando ningún otro valor fue dado.

Tabla 4.1. Valores asignados al tipo de tráfico según su prioridad.

Frame Relay

Es una red pública de conmutación de paquetes utilizada en servicios de transmisión a alta velocidad que permite la interconexión de redes de área local separadas geográficamente, a un costo menor que al interconectarlas mediante enlaces dedicados.

En ***Frame Relay*** se comparte la capacidad con sus clientes para poder así reducir los costos. El proveedor del servicio compromete un ancho de banda al cliente, sin embargo el cliente puede transmitir datos a una tasa superior a la contratada siempre y cuando no exista congestión en la red. FR es una red NBMA (Non-Broadcast Multiple Access), lo cual quiere decir que no permite mensajes tipo ***broadcast*** en la red.

Frame Relay maneja enlaces multipunto y punto a punto gracias al manejo de circuitos virtuales (VC), los cuales son una comunicación interna de FR entre localidades. Estos circuitos suelen ser privados (***PVC***) o conmutados (***SVC***). Los SVC se generan bajo demanda, es decir, si un ***DTE*** o equipo terminal conectado a FR requiere hacer una transmisión se genera un SVC que se convierte en PVC durante la transferencia y al finalizar ésta se elimina. Generalmente el PVC, como su nombre lo dice, permanece como si se tratase de un enlace dedicado permanente.

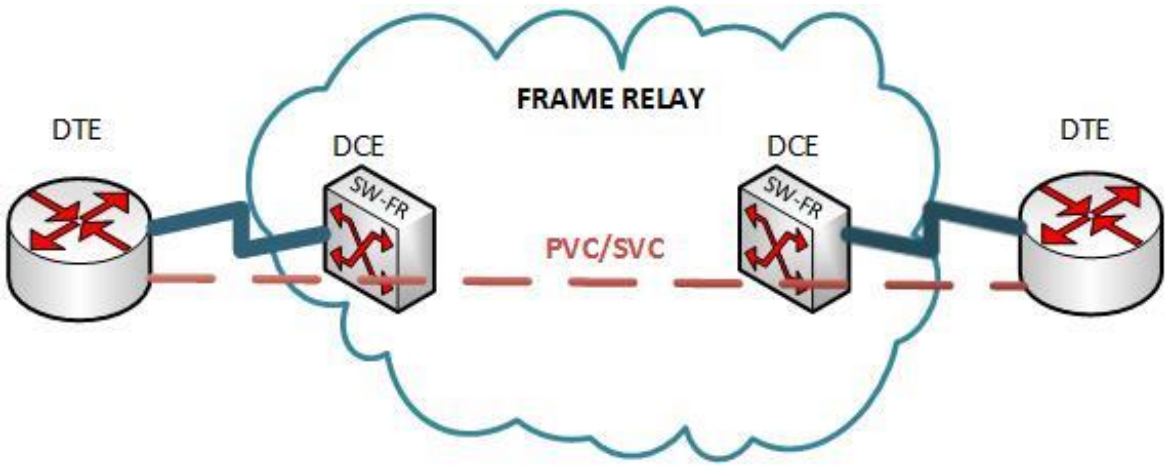

Figura 4.2. Esquema de red Frame Relay.

Los ***DCE*** o switches FR se encargan de manejar un ***CIR*** o tasa del circuito virtual dentro de la red FR, además de actuar al presentarse una congestión, marcando los encabezados DE (Discard Eligible), FECN (Forward Explicit Congestion Notification) o BECN (Backward Explicit Congestion Notification) dependiendo el caso, mismos que se localizan en la figura 4.3.

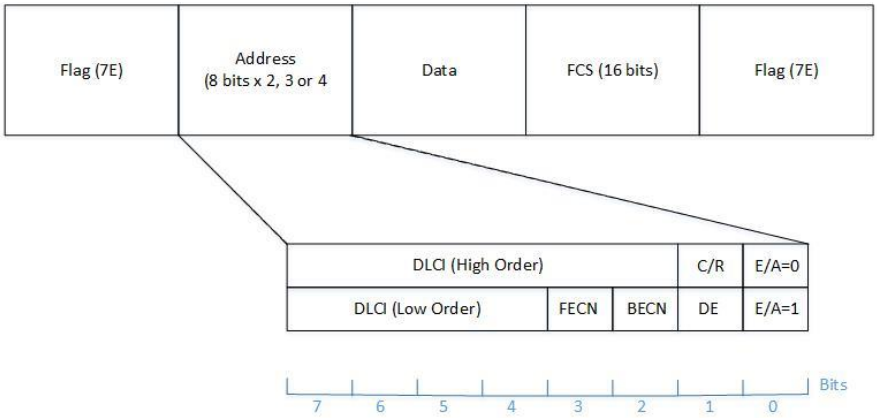

Figura 4.3. Encabezado del encapsulado Frame Relay.

- DE. Cuando existe una congestión, las tramas que tengan marcado este campo con un "1" serán las primeras en ser descartadas. La asignación de prioridades es a consideración del cliente.
- FECN. Los switches FR se encargan de marcar el campo FECN de las tramas del DTE que se están transmitiendo a una tasa superior al CIR acordado, para informarle al DTE receptor que debe solicitarle al DTE transmisor un ajuste en la ventana de transmisión.
- BECN. Este campo es marcado en las tramas de vuelta enviadas por el DTE receptor para solicitarle al DTE transmisor que disminuya la tasa con la que está transmitiendo.

El proceso anterior puede contemplarse en la figura 4.4.

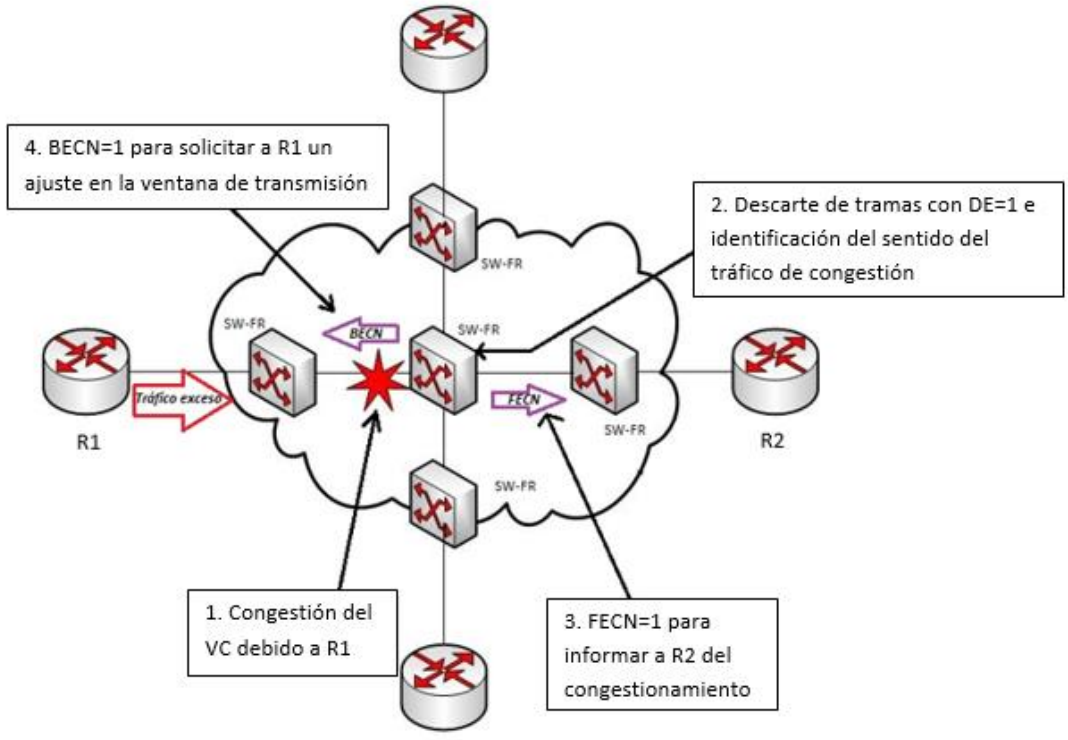

Figura 4.4. Funcionamiento de Frame Relay.

Gracias al identificador ***DLCI*** de PVC se puede hacer un mapeo de la red ya se manual o mediante los mensajes ***IARP***. Los switches FR se comunican con los DTE mediante el protocolo ***LMI***, con ello se ayuda a que el DTE tenga conocimiento de los acontecimientos que se presentan dentro de la nube Frame Relay como caídas de los circuitos virtuales, bloqueos, etc.

IMPLEMENTACIÓN DE QoS EN FRAME RELAY.

Para garantizar QoS sobre la red Frame Relay se pueden tomar en cuenta los siguientes métodos para conseguirlo:

- Dar una prioridad estricta al tráfico de voz.
- ***Frame Relay Traffic Shaping.***
- Fragmentación FRF.12.

Prioridad estricta al tráfico de voz

Para darle prioridad al tráfico de voz sobre los demás tipos de paquetes se recurre a los mecanismos de colas ya mencionadas anteriormente. En los siguientes 2 casos se observa las colas óptimas para la implementación de prioridad sobre los paquetes de voz.

- **Prioridad IP RTP:** Se crea una cola de prioridad estricta (PQ) en el PVC para un conjunto de flujos de paquetes RTP que pertenecen a un rango de puertos destino UDP. Una vez que los routers DTE reconocen este tráfico UDP lo colocan en la cola PQ estricta, lo transmiten hasta que la cola PQ quedé vacía y proceden a enviar los otros tráficos conforme a WFQ. El tráfico de voz tendrá prioridad siempre y cuando exista congestión en la red, de no presentarse, se utilizará WFQ por defecto, al igual que se observa en la figura 4.5.

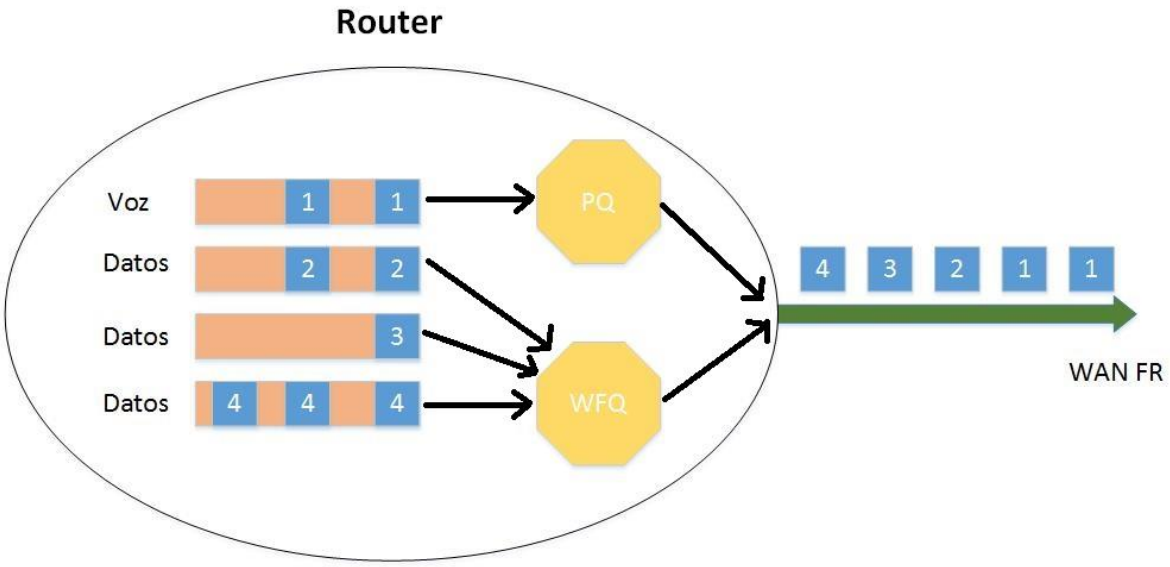

Figura 4.5. Funcionamiento de la prioridad IP RTP.

- **LLQ:** Ya se ha mencionado anteriormente el funcionamiento de LLQ. Para Frame Relay, las colas se configuran en función de cada PVC. Cada PVC tiene una PQ y un número asignado de colas equitativas (FQ). La figura 4.6 muestra éste proceso con más detalle.

Figura 4.6. Funcionamiento de LLQ en Frame Relay.

Para la configuración de LLQ es necesario calcular un nuevo ancho de banda con base a la siguiente expresión y la cabecera de capa 2, dependiendo de, si sólo se está utilizando Frame Relay o si se incluye FRF.12.

$$BW_{llamada} = (payload\ de\ voz + headers\ 3 + headers\ 2) * (packet\ ratio) * 8$$

CONFIGURACIÓN DE LLQ EN FRAME RELAY

Dentro de la política se configuran todas aquellas instrucciones que se van a efectuar ante cada tipo de tráfico procedente de una clase en específico. Es el mismo procedimiento y los mismos comandos, los que se aplicarán en el caso de este trabajo.

- Se crea la clase.
- Se crea la política.
- Se asocia a una interfaz en el sentido requerido.

La diferencia existe en las condiciones previas configuradas para el tipo de red que se trabaja.

Frame Relay Traffic Shaping

En la figura 4.4 se muestra el proceso de QoS aplicados en la red. FRTS permite eliminar los cuellos de botella mediante la modificación de parámetros útiles en la gestión de la congestión de tráfico de red. Algunos términos importantes son los siguientes:

- *Tasa de información comprometida (CIR):* Es la tasa de transferencia de datos que el proveedor de servicio garantiza para los PVC. Esta tasa es fijada por el proveedor pero es configurada por el usuario del router.
- *Ráfaga comprometida (Bc):* Número máximo de bits de la red Frame Relay, que se compromete a transferir a través de un Tc.
- *Exceso de ráfaga (Be):* Número máximo de bits no comprometidos que el switch FR intenta transferir más allá del CIR sobre el Tc.
- *Intervalo de medición de tasa comprometida (Tc):* Intervalo de tiempo durante el cual se transmiten los bits Bc o (Bc+Be) son transmitidos. Tc se calcula como Tc= Bc/CIR. El valor de Tc es calculado después de ser configurados los valores de Bc y CIR. Tc no puede exceder los 125 ms.

CONFIGURACIÓN DE FRAME RELAY TRAFFIC-SHAPING

Una vez teniendo la configuración correcta y funcional de los routers en red Frame Relay, se configura en el puerto serial directamente conectado a la WAN FR los siguientes comandos para aplicar FRTS:

- **frame-relay traffic-shaping:** Este comando permite habilitar FRTS para la interfaz. Cada DLCI bajo esta interfaz serial es catalogada ya sea con los parámetros de traffic shaping definidos por el usuario o por defecto. El usuario puede definir estos parámetros de dos maneras:
    - Utilizando el comando **class** *class_name* se creará una clase bajo la configuración **frame-relay interface-dlci** *number* o;
    - Utilizando el comando **frame-relay** *class* se creará una clase bajo la interfaz serial.

Nota. Bajo la configuración del DLCI se configura ***VoFR*** utilizando el comando **vofr** *cisco.*

En el modo de configuración del router, se configurarán los parámetros FRTS para un específico DLCI mediante el siguiente comando:

- **map-class frame-relay** *class_name:* Bajo esta configuración se determinan los parámetros de FRTS utilizando varias reglas, a continuación se muestran los comandos para editar los valores de las variables mencionadas en este trabajo y aquellos que afectan directamente al tráfico de voz:
    - **frame-relay cir** *bps*
    - **frame-relay bc** *bits*
    - **frame-relay be** *bits*
    - **frame-relay voice bandwidth** *bps:* Determina cuanto ancho de banda está reservado para una class map Frame Relay.

Fragmentación FRF.12

Se utiliza FRF.12 en los enlaces de baja tasa de transmisión (menos de 768 kbps). El tamaño de los fragmentos se ajusta para que los paquetes de voz no sean fragmentados y no experimenten un retraso de serialización superior a 20 ms. Se establece el tamaño de la fragmentación con base a la tasa del puerto que tenga el valor más bajo del enlace. Cualquier PVC que comparta la misma interfaz física con otros PVC tiene que configurar la fragmentación con el tamaño utilizado por el PVC de voz.

Para determinar el valor del tamaño de la fragmentación se recurre a la siguiente expresión[14]:

$$Tamaño_{Fragmentación}\ [bytes] = Tasa_{Enlace}[bytes] * Retardo_{Serialización}\ [s]$$

CONFIGURACIÓN DE FRAGMENTACIÓN FRF.12

- **map-class frame-relay** *class_name*
  - **frame-relay fragment** *fragment_size*

Multi-Protocol Layer Switching (MPLS)

Es un protocolo cuya función se puede asociar a una unión de capa 2 con capa 3 del modelo OSI, para efectos prácticos. Esta tecnología se desarrolló para dar solución a los problemas que surgen en la conmutación de paquetes basada en IP, por ejemplo:

- Todos los routers de una red necesitan conocer todos los posibles direccionamientos destino. De lo contrario puede existir un ***black hole.***
- En las redes actuales se puede sobre-utilizar una interfaz debido al protocolo interno del enrutamiento configurado.

MPLS consiste en una conmutación basada en etiquetas cuyo objetivo es llevar la velocidad de capa 2 a capa 3. En la figura 4.7 se observan dichas etiquetas, mismas que permiten a los routers tomar decisiones en el momento basándose en el contenido de éstas, evitando la búsqueda de la IP destino dentro de las tablas de ruteo. Gracias a ello se puede ganar velocidad al enfocar las funciones de capa 2 con las de capa 3.

En la red MPLS se cuenta con unos equipos denominados ***LSR***, los cuales se encuentran a la entrada de la red. Al recibir la información de ruteo con la información de los prefijos que otros routers vecinos son capaces de alcanzar, ellos asignan a cada prefijo una etiqueta que es anunciada internamente en la red MPLS.

Con ello, cada router LSR tendrá 2 etiquetas asociadas a cada prefijo,

- La etiqueta de recepción e identificación del prefijo.
- La etiqueta de envío e identificación de interfaz de salida.

[14] Véase la página 40.

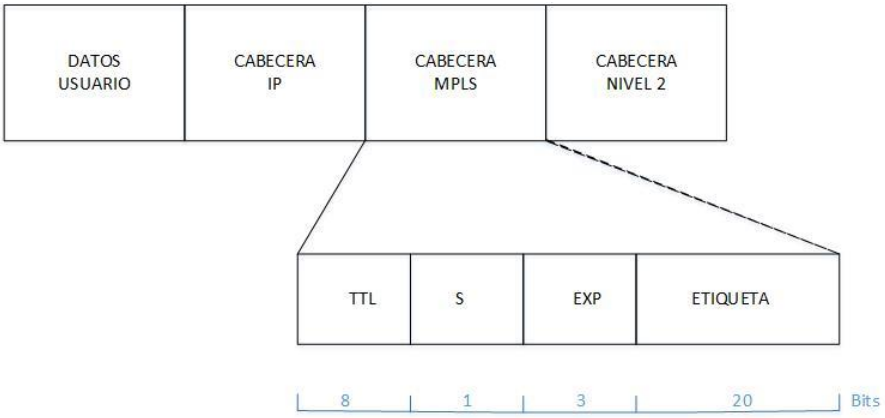

Figura 4.7. Etiqueta identificadora en Multi-Protocol Layer Switching.

Cuando el paquete llega al ***LER***, éste elimina la etiqueta y se envía el paquete en formato IP tradicional hacia su destino. Una ejemplificación de una red MPLS se muestra en la figura 4.8.

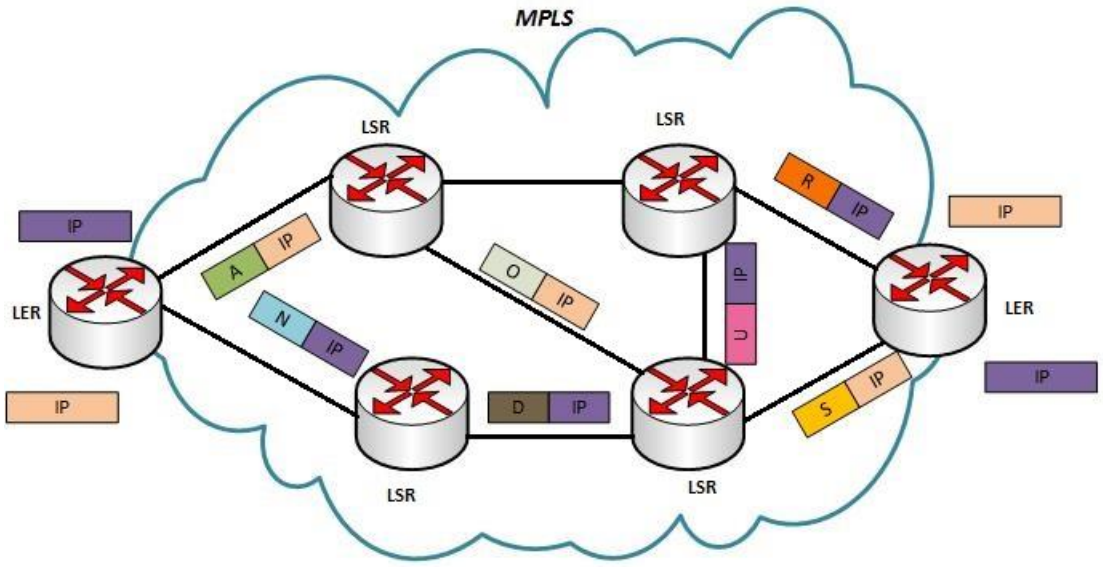

Figura 4.8. Red Multi-Protocol Layer Switching.

IMPLEMENTACIÓN DE QOS EN MPLS

Para la implementación de QoS se toma en cuenta que en el encabezado MPLS existe un campo llamado EXP (Experimental) y pese al nombre, éste es utilizado exclusivamente para QoS de la misma manera como son utilizados en el encabezado IP los 3 bits destinados para la precedencia IP. El campo EXP copiará los primeros 3 bits del DSCP (es decir, IP Precedence) y en cada salto y cambió de etiqueta, no se modificarán estos valores.

Al igual como los LSR de la red revisan la etiqueta para saber cómo enrutarla de manera óptima mediante la capacidad de efectuar ***traffic engineering***, los LSR necesitan solamente mirar el contenido de EXP del encabezado MPLS para determinar cómo tratar a cada paquete.

Al igual que en las redes IP, se puede implementar LLQ, CBWFQ, WRED, policing y shaping en MPLS basándose en el campo EXP. Los comandos de configuración dependerán de si se está montando sobre una red Frame Relay, ATM, etc. Ya que se recuerda que se trata de un multi-protocolo.

Wi-Fi

WiFi es una tecnología LAN inalámbrica creada por ***Wi-Fi Alliance***, que fundamenta su funcionamiento en el estándar 802.11; se basa en el uso de un dispositivo conocido como ***access point***, el cual es capaz de conectarse a diferentes dispositivos compatibles con dicha tecnología, lo que les permite acceder a Internet. Se muestra su logotipo en la figura 4.9.

Figura 4.9. Logotipo de Wi-Fi.

Esta tecnología se ha vuelto parte esencial de lo que es la conexión a Internet actualmente, pues todos o la mayoría de los dispositivos inteligentes soportan Wi-Fi y lo usan como principal medio de acceso a la red. Debido al exponencial crecimiento de esta forma de comunicación se consideró la intervención de calidad de servicio sobre las redes inalámbricas.

Lo primero que hay que pensar cuando se habla de redes inalámbricas es que funcionan de manera muy diferente, enseguida se destacan algunas diferencias:

- Tasa de transmisión. Es mucho más lenta ya que existen muchas pérdidas en el medio y también por la forma en que los datos se envían.
- Saturación. La afluencia de dispositivos suele ser mayor.
- Difícil de abastecer. El ancho de banda es limitado.

Tomando en cuenta estas características, se creó el estándar 802.11e para hiciera frente a las crecientes necesidades de este sistema de transmisión, permitiendo la priorización de diferentes flujos de trabajo entre equipos o dispositivos. Este estándar se encarga de controlar

el flujo que va desde el punto de acceso hasta los aplicativos finales en forma de ondas de radio y es ahí donde aplica la calidad de servicio, como puede verse en la figura 4.10.

Wi-Fi habilita los puntos de acceso para dar prioridad a cierto tipo de tráfico mediante la aplicación del módulo ***HCF*** que está compuesto de dos mecanismos de acción:

- ***EDCA.*** También conocido como ***EDCF***, se encarga de la priorización de los datos, pues introduce el concepto de categorías de tráfico, definiendo ocho niveles de tráfico de prioridad, de forma similar a como se hace dentro del modelo de servicios diferenciados. Incluye elementos de DCF como ***CSMA/CA***. En este mecanismo se introducen cuatro categorías de acceso, como puede apreciarse en la tabla 4.2, mismos que a su vez se encuentran dentro del estándar 802.1d.

Prioridad	Prioridad 802.1d	Categoría de acceso	Tipo de tráfico
Baja	0	0	Best effort
Baja	1	0	Best effort
Baja	2	0	Best effort
Baja	3	1	Streaming video
Media	4	2	Video
Media	5	2	Video
Alta	6	3	Voice
Alta	7	3	Voice

Tabla 4.2. Prioridades existentes dentro del estándar 802.1d.

- ***HCCA.*** Atiende y soporta el tráfico parametrizado, como se haría dentro del modelo de servicios integrados. Este mecanismo es mucho más complejo que el anterior ya que aquí la calidad de servicio debe definirse con precisión, pues los parámetros deben ser descritos con antelación (tasa, ruido, potencia) para que las estaciones tengan la prioridad apropiada.

En general, la calidad de servicios en redes inalámbricas puede resumirse en los tres pasos siguientes:

- Se tienen 3 dispositivos cualesquiera (un teléfono, una tableta y una computadora) con categorías de tráfico alta, media y baja, respectivamente, que requieren enviar datos inalámbricamente. Se envía un paquete al punto de acceso, mismo que identifica los dispositivos.
- Después del reconocimiento, se produce un periodo de tiempo arbitrario antes de que los dispositivos envíen los datos, según su nivel de prioridad, que es más corto para aquellos que tienen mayor prioridad.

- El dispositivo de mayor prioridad, en este caso el teléfono, comienza a contar antes de empezar a transmitir, al igual que la tableta y la computadora, pero estas últimas suspenden su cuenta cuando el teléfono comienza a enviar sus paquetes.

Con lo anterior, puede verse que este mecanismo funciona mediante un sistema de encolamiento que se basa en la prioridad que cada servicio o estación de transmisión lleve adscrito, mismo que puede verse con mayor claridad en la figura 4.10.

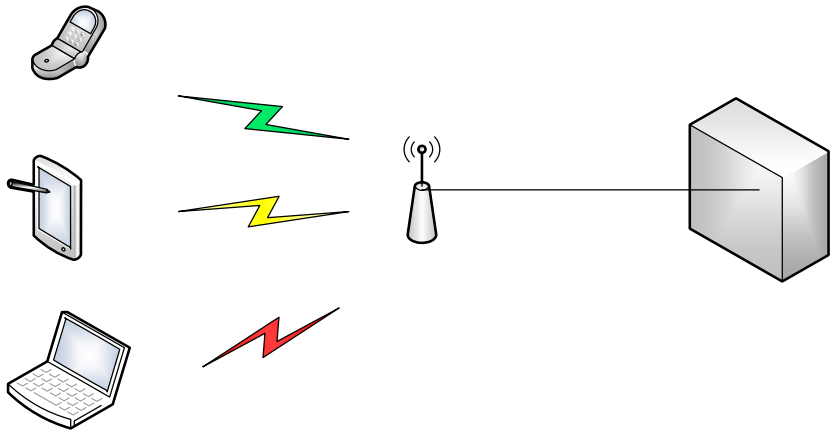

Figura 4.10. Esquema de conexión de una red inalámbrica.

Adicionalmente, el estándar 802.11e añade una funcionalidad denominada *Tiempo de vida máximo del* ***MSDU***, que especifica el tiempo máximo que un paquete puede estar en la capa MAC antes de descartarse, muy útil para aplicaciones en tiempo real como la voz o el video.

En Cisco, ya se usa este esquema de calidad de servicio en nuevos sistemas WLAN, especialmente en aplicaciones para telefonía IP, mismo que se conoce como ***QBSS*** y que forma parte del estándar 802.11e.

WMM

WMM es un nuevo esquema que define características de calidad de servicio, además de gestión de energía; incluye también técnicas y protocolos pertenecientes a 802.11e, más específicamente de EDCA.

Ejemplos de la evolución que WMM presenta, es que la mayoría de los puntos de acceso y los dispositivos actuales ya cuentan con certificación por parte de Wi-Fi Alliance, así como muchas de las aplicaciones de reciente creación. En WMM ya no es obligatorio el uso de HCCA y además es compatible con dispositivos que no cuentan con dicha certificación, pues facilita la interoperabilidad de esquemas y versiones distintas.

En WMM los paquetes son etiquetados en la parte de su cabecera DSCP, por lo que es compatible con el esquema de calidad de servicio tradicional para redes no inalámbricas; dentro de WMM se definen las siguientes categorías de acceso, así como el tipo de tráfico al que corresponde.

Categoría de acceso	Tipo de tráfico
Background WMM	Aplicaciones de menor importancia
Best effort WMM	Aplicaciones con baja importancia
Video WMM	Video
Voz WMM	Voz

Tabla 4.3. Categorías de tráfico dentro de WMM.

En la tabla 4.3 puede notarse que existe una categoría que se llama best effort; dicha categoría se usa para integrar a los dispositivos y servicios que no cuentan con certificación WMM.

Finalmente, puede concluirse que WMM ofrece una gama de ventajas para el usuario, como la interoperabilidad de esquemas y fabricantes, la disponibilidad para incluirse en nuevos dispositivos, la compatibilidad con el estándar 802.11e, la popularidad que está ganando, el despliegue que tiene actualmente y desde luego su adaptabilidad.

Configuración de la red y los servicios de VoIP

Se configuró una red WAN donde se interconectan dos redes LAN tal y como se muestra en la figura 5.1. Se nombraron a las redes LAN como México y Monterrey con la finalidad de representar las redes de dos ciudades separadas.

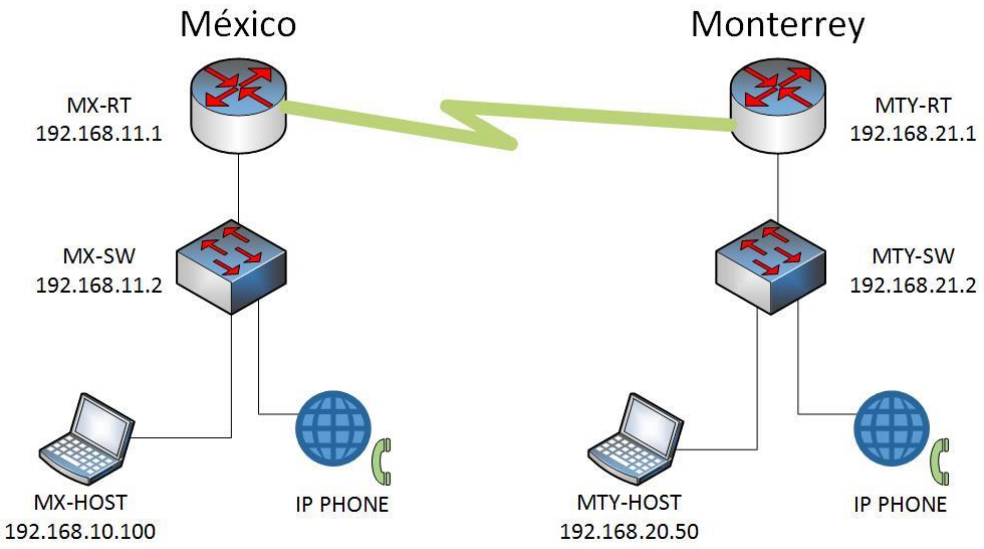

Figura 5.1. Esquema de conexión de la red

Para este trabajo se requirió considerar la transferencia de datos y voz en forma simultánea para representar un entorno real de comunicación, lo que se logró mediante el uso de un software generador de tráfico y de un par de teléfonos Cisco VoIP, los cuales se enlistan en la tabla 5.1, así como el direccionamiento usado que se observa en las tablas 5.2 y 5.3.

Equipo	Nombre del equipo	Modelo del equipo
Router	MX-RT	Cisco 2811
Switch	MX-SW	Cisco 3550
Teléfono	MX-Phone	Cisco 7911
Router	MTY-RT	Cisco 2811
Switch	MTY-SW	Cisco 3550
Teléfono	MTY-Phone	Cisco 7911

Tabla 5.1. Modelos utilizados en el estudio.

Ubicación	Dirección IP
MX-HOST	192.168.10.100
MTY-HOST	192.168.20.50

Tabla 5.2. Direccionamiento de las computadoras.

Nombre del equipo	Direccionamiento
MX-RT	192.168.11.1

MX-SW	192.168.11.2
MX-Phone	192.168.10.129
MTY-RT	192.168.21.1
MTY-SW	192.168.21.2
MTY-Phone	192.168.20.129

Tabla 5.3. Direccionamiento de routers, switches y teléfonos.

CONFIGURACIÓN DEL ACCESO REMOTO (TELNET)

Para tener un manejo más práctico de los dispositivos y su configuración, se decidió configurar telnet en cada uno de ellos para tener un acceso remoto a la interfaz de línea de comandos mediante una IP asociada a la vlan nativa respectiva a cada dispositivo. Por cuestiones de seguridad se ingresó una contraseña tanto para telnet como para acceder al modo privilegiado. La tabla 5.4 indica la configuración hecha en cada equipo.

MX-SW	**MTY-SW**
Switch>enable Switch#configure terminal Switch(config)# hostname MX-SW MX-SW(config)#interface Vlan 1 MX-SW (config-if)#ip address 192.168.11.2 255.255.255.0 MX-SW(config-if)#exit MX-SW(config)#enable password FacIng MX-SW(config)#line vty 0 4 MX-SW(config-line)#password UNAMredes MX-SW(config-line)#exit	Switch>enable Switch#configure terminal Switch(config)# hostname MTY-SW MTY-SW(config)#interface Vlan 1 MTY-SW(config-if)#ip address 192.168.21.2 255.255.255.0 MTY-SW(config-if)#exit MTY-SW(config)# enable password FacIng MTY-SW(config)#line vty 0 4 MTY-SW(config-line)#password UNAMredes MTY-SW(config-line)#exit
MX-RT	**MTY-RT**
Router>enable Router#configure terminal Router(config)#hostname MX-RT MX-RT(config)#interface FastEthernet0/0.1 MX-RT(config-subif)#encapsulation dot1Q 1 native MX-RT(config-subif)#ip address 192.168.11.1 255.255.255.0 MX-RT(config-subif)#exit MX-RT(config)#enable password FacIng MX-RT(config)#line vty 0 4 MX-RT(config-line)#password UNAMredes MX-RT(config-line)#exit	Router>enable Router#configure terminal Router(config)#hostname MTY-RT MTY-RT(config)#interface FastEthernet0/0.1 MTY-RT(config-subif)#encapsulation dot1Q 1 native MTY-RT(config-subif)#ip address 192.168.21.1 255.255.255.0 MTY-RT(config-subif)#exit MTY-RT(config)#enable password FacIng MTY-RT(config)#line vty 0 4 MTY-RT(config-line)#password UNAMredes MTY-RT(config-line)#exit

Tabla 5.4. Configuración del acceso remoto en los equipos.

CONFIGURACIÓN DE LOS SWITCHES

Con la red conectada físicamente se configuraron dos VLANs en ambos switches, mismas que se señalan en la tabla 5.5.

VLAN	Tipo	Descripción
2	DATOS	Es por donde viajarán los segmentos TCP.
10	VOZ	Es por donde viajarán los datagramas UDP (Voz).

Tabla 5.5. VLANs requeridas.

Después, para la conexión entre router y switch se configuró un puerto en modo troncal con encapsulamiento dot1Q de la IEEE, así como dos puertos espejo para poder monitorear el enlace entre el switch y el router, de la forma que se muestra en la tabla 5.6.

MÉXICO	MONTERREY
MX-SW(config)#vlan 2 MX-SW(config-vlan)#name DATOS MX-SW(config-vlan)#vlan 10 MX-SW(config-vlan)#name VOZ MX-SW(config-vlan)#exit MX-SW(config)#interface range fastEthernet 0/1-5 MX-SW(config-if-range)#switchport mode access MX-SW(config-if-range)#switchport access vlan 2 MX-SW(config-if-range)#switchport voice vlan 10 MX-SW(config-if-range)#no shutdown MX-SW(config)#interface FastEthernet0/23 MX-SW(config-if)#switchport trunk encapsulation dot1q MX-SW(config-if)#switchport mode trunk MX-SW(config-if)#no shutdown MX-SW(config)#monitor session 1 source interface FastEthernet0/23 MX-SW(config)#monitor session 1 destination interface FastEthernet0/24	MTY-SW(config)#vlan 2 MTY-SW (config-vlan)#name DATOS MTY-SW (config-vlan)#vlan 10 MTY-SW (config-vlan)#name VOZ MTY-SW (config-vlan)#exit MTY-SW (config)#interface range fastEthernet 0/1-5 MTY-SW (config-if-range)#switchport mode access MTY-SW (config-if-range)#switchport access vlan 2 MTY-SW (config-if-range)#switchport voice vlan 10 MTY-SW (config-if-range)#no shutdown MTY-SW (config)#interface FastEthernet0/23 MTY-SW (config-if)#switchport trunk encapsulation dot1q MTY-SW (config-if)#switchport mode trunk MTY-SW (config-if)#no shutdown MTY-SW(config)#monitor session 1 source interface FastEthernet0/23 MTY-SW(config)#monitor session 1 destination interface FastEthernet0/24

Tabla 5.6. Configuración de las VLANs en los switches.

CONFIGURACIÓN DE LOS ROUTERS

Conexión serial

Se realizó una conexión serial con cables DB60-V.35 (DTE) y DB60-V.35 (DCE) para enlazar los routers. Con una conexión de tipo serial se puede configurar el enlace de los equipos y a la vez simular un enlace tradicional entre dos ciudades, propio de una red WAN. La tasa de transmisión para esta red es de 128 kbps. Se configuraron en los routers los parámetros referentes a un enlace serial así como las rutas estáticas para la comunicación entre las LANs y VLANs.

Se decidió configurar el puerto serial 0/1/0 del router México como DCE. Debido a esto se indicó la tasa de transmisión en esta interfaz como se en la tabla 5.7.

MÉXICO	MONTERREY
MX-RT(config)#interface serial 0/1/0 MX-RT(config-if)#description link Puerto DCE	MTY-RT(config)#interface serial 0/0/0 MTY-RT(config-if)#description Puerto DTE

MX-RT(config-if)#ip address 192.168.40.1 255.255.255.0 MX-RT(config-if)#no shutdown MX-RT(config-if)#clock rate 128000	MTY-RT(config-if)#ip address 192.168.40.2 255.255.255.0 MTY-RT(config-if)#no shutdown

Tabla 5.7. Configuración del enlace serial.

Default gateway

Para que el router pueda diferenciar las VLANs es necesario indicar un ***default gateway*** para cada una de ellas. Se puede observar en la tabla 5.8, que se crearon subredes para optimizar la utilización de direcciones IP, mismas que se asociaron a las subinterfaces mediante un default gateway.

MÉXICO	MONTERREY
MX-RT(config)# interface FastEthernet0/0 MX-RT(config-if)#no shutdown MX-RT(config-if)# interface FastEthernet0/0.2 MX-RT(config-subif)#encapsulation dot1Q 2 MX-RT(config-subif)#ip address 192.168.10.126 255.255.255.128 MX-RT(config-subif)# interface FastEthernet0/0.10 MX-RT(config-subif)#encapsulation dot1Q 10 MX-RT(config-subif)#ip address 192.168.10.254 255.255.255.128	MTY-RT(config)# interface FastEthernet0/0 MTY-RT(config-if)#no shutdown MTY-RT(config-if)# interface FastEthernet0/0.2 MTY-RT(config-subif)#encapsulation dot1Q 2 MTY-RT(config-subif)#ip address 192.168.20.126 255.255.255.128 MTY-RT(config-subif)# interface FastEthernet0/0.10 MTY-RT(config-subif)#encapsulation dot1Q 10 MTY-RT(config-subif)#ip address 192.168.20.254 255.255.255.128

Tabla 5.8. Configuración del default gateway.

Rutas estáticas

Diferenciar las VLANs no es lo único que un router requiere ya que también necesita la información necesaria para poder enviar un paquete a su destino, es decir, se necesita configurar una ruta estática o un protocolo dinámico para indicárle cuál es el camino a seguir para llegar a la red de interés. Se decidió crear rutas estáticas utilizando la interfaz de salida del router, cuya configuración se encuentra en la tabla 5.9.

MÉXICO	MONTERREY
MX-RT(config)#ip route 192.168.20.0 255.255.255.255 192.168.40.2 MX-RT(config)#ip route 192.168.21.0 255.255.255.255 192.168.40.2	MTY-RT(config)#ip route 192.168.10.0 255.255.255.255 192.168.40.1 MTY-RT(config)#ip route 192.168.11.0 255.255.255.255 192.168.40.1

Tabla 5.9. Configuración de las rutas estáticas.

DHCP (Dynamic Host Configuration Protocol)

Se indicó que el router funcione como DHCP para la VLAN 10. La configuración se muestra con los siguientes comandos de la tabla 5.10.

MÉXICO	MONTERREY
MX-RT(config)#ip dhcp excluded-address 192.168.10.128 MX-RT(config)#ip dhcp pool VOZ MX-RT(dhcp-config)#network 192.168.10.128 255.255.255.128 MX-RT(dhcp-config)#default-router 192.168.10.254 MX-RT(dhcp-config)#option 150 ip 192.168.10.254	MTY-SW(config)#ip dhcp excluded-address 192.168.20.128 MTY-SW(config)#ip dhcp pool VOZ MTY-SW(dhcp-config)#network 192.168.20.128 255.255.255.128 MTY-SW(dhcp-config)#default-router 192.168.20.254 MTY-SW(dhcp-config)#option 150 ip 192.168.20.254

Tabla 5.10. Configuración del servidor DHCP.

CONFIGURACIÓN DE LOS SERVICIOS DE VOIP

Call Manager

Para la configuración de los servicios de voz se indicaron las extensiones pertenecientes a cada teléfono así como el número máximo de teléfonos IP para las redes respectivas. Con estas configuraciones se puso habilitar la comunicación de los teléfonos. Como puede verse en la tabla 5.11, se asignaron 2 extensiones a ambos teléfonos.

MÉXICO	MONTERREY
MX-RT(config)#dial-peer voice 9 voip MX-RT(config-dial-peer)#destination-pattern 2... MX-RT(config-dial-peer)#session target ipv4:192.168.40.2 MX-RT(config)#telephony-service MX-RT(config-telephony)#ip source-address 192.168.10.254 port 2000 MX-RT(config-telephony)#max-ephones 5 MX-RT(config-telephony)#max-dn 5 MX-RT(config-telephony)#auto assign 1 to 5 MX-RT(config-telephony)#exit MX-RT(config)#ephone-dn 1 MX-RT(config-ephone-dn)#number 1101 MX-RT(config-ephone-dn)#ephone-dn 2 MX-RT(config-ephone-dn)#number 1102	MTY-RT(config)#dial-peer voice 9 voip MTY-RT(config-dial-peer)#destination-pattern 1... MTY-RT(config-dial-peer)#session target ipv4:192.168.40.1 MTY-RT(config)#telephony-service MTY-RT(config-telephony)#ip source-address 192.168.20.254 port 2000 MTY-RT(config-telephony)#max-ephones 5 MTY-RT(config-telephony)#max-dn 5 MTY-RT(config-telephony)#auto assign 1 to 5 MTY-RT(config-telephony)#exit MTY-RT(config)#ephone-dn 1 MTY-RT(config-ephone-dn)#number 2101 MTY-RT(config-ephone-dn)#ephone-dn 2 MX-RT(config-ephone-dn)#number 2102

Tabla 5.11. Configuración de los servicios telefónicos.

Implementación de la calidad de servicio

Enseguida se muestran todos los comandos e instrucciones dadas a los dispositivos (routers y switches) para la configuración de la calidad de servicio mediante los mecanismos explicados en las secciones anteriores. Se muestran dichas configuraciones por etapas ya que es así como se fueron aplicando en la práctica.

Configuración de la clasificación de tráfico (Classification) y Policing

Utilizando MQC se pudieron configurar los mecanismos de policing y se utilizó Class-Based para la clasificación de los paquetes. En este caso, se clasificaron los datos en tres tipos mediante el uso de listas de acceso específicas para cada clase.

MX-RT	MTY-RT
MX-RT(config)#access-list 100 permit ip any any precedence 5	MTY-RT(config)#access-list 100 permit ip any any precedence 5
MX-RT(config)#access-list 100 permit ip any any dscp ef	MTY-RT(config)#access-list 100 permit ip any any dscp ef
MX-RT(config)#access-list 101 permit tcp any any eq telnet	MTY-RT(config)#access-list 101 permit tcp any any eq telnet
MX-RT(config)#access-list 101 permit icmp any any	MTY-RT(config)#access-list 101 permit icmp any any
MX-RT(config)#access-list 102 permit ip any any dscp cs3	MTY-RT(config)#access-list 102 permit ip any any dscp cs3
MX-RT(config)#access-list 102 permit ip any any dscp af31	MTY-RT(config)#access-list 102 permit ip any any dscp af31
MX-RT(config)#class-map SIGNAL	MTY-RT(config)#class-map SIGNAL
MX-RT(config-cmap)#match access-group 102	MTY-RT(config-cmap)#match access-group 102
MX-RT(config-cmap)#class-map VOZ	MTY-RT(config-cmap)#class-map VOZ
MX-RT(config-cmap)#match access-group 100	MTY-RT(config-cmap)#match access-group 100
MX-RT(config-cmap)#class-map DATOS	MTY-RT(config-cmap)#class-map DATOS
MX-RT(config-cmap)#match access-group 101	MTY-RT(config-cmap)#match access-group 101

Tabla 6.1. Configuración de la clasificación de tráfico y Policing.

Se puede notar en la tabla 6.1, que se asignó un grupo de listas de acceso a cada clase. Las clases que se crearon se encargan de clasificar los paquetes que coinciden con el grupo de listas de acceso asociadas para posteriormente, aplicarles una política; también se muestran algunas marcas de DSCP.

El comportamiento de reenvío asignado a un DSCP se denomina comportamiento por salto (PHB). El PHB define la precedencia de reenvío que un paquete marcado recibe en relación con otro tráfico del sistema con Diffserv.

El grupo 100 de las listas de acceso creadas se encarga de clasificar en capa 3 los paquetes de voz mediante un DSCP con un PHB de reenvío acelerado (EF), asegurando que cualquier tipo de tráfico con reenvíos EF tenga la máxima prioridad. Asimismo clasifica a nivel de capa 3 los

paquetes con una precedencia crítica, es decir, con un valor de 5 en el campo ToS del encabezado IP. Estas listas de acceso están agrupadas dentro de la clase VOZ, ya que son los paquetes de ésta a los que se les dará preferencia.

En la clase SIGNAL se clasificaron los paquetes de señalización mediante el grupo de listas de acceso 102, utilizando un DSCP con un PHB de reenvío asegurado (AF), con ello se asegura un cierto ancho de banda y espacio en el búfer para la señalización (AF31). Por otra parte, dentro de este grupo de listas de acceso se hace uso del selector de clase 3 para clasificar los paquetes de señalización en versiones actualizadas del IOS.

Finalmente, mediante el grupo 101 de listas de acceso, se clasificaron los paquetes de datos trabajados en este proyecto de tipo ICMP y TCP.

Configuración de LLQ (Low Latency Queuing)

MX-RT	MTY-RT
MX-RT(config)#policy-map POLIVOZ MX-RT(config-pmap)#class VOZ MX-RT(config-pmap-c)#bandwidth percent 40 MX-RT(config-pmap-c)#class DATOS MX-RT(config-pmap-c)#bandwidth percent 20 MX-RT(config-pmap-c)#class SIGNAL MX-RT(config-pmap-c)#bandwidth percent 10 MX-RT(config-pmap-c)#exit MX-RT(config-pmap)#exit MX-RT(config)# interface Serial0/1/0 MX-RT(config-if)#service-policy output POLIVOZ	MTY-RT(config)#policy-map POLIVOZ MTY-RT(config-pmap)#class VOZ MTY-RT(config-pmap-c)#bandwidth percent 40 MTY-RT(config-pmap-c)#class DATOS MTY-RT(config-pmap-c)#bandwidth percent 20 MTY-RT(config-pmap-c)#class SIGNAL MTY-RT(config-pmap-c)#bandwidth percent 10 MTY-RT(config-pmap-c)#exit MTY-RT(config-pmap)#exit MTY-RT(config)# interface Serial0/0/0 MTY-RT(config-if)#service-policy output POLIVOZ

Tabla 6.2. Configuración de Low Latency Queuing.

Después de crear las clases se requiere asociarlas a una política donde se especifique cómo se van a tratar los paquetes de cada clase, que puede verse en la tabla 6.2.

Gracias a LLQ, se está brindando una estricta cola de prioridad a CB-WFQ para garantizar un ancho de banda a las clases de alta prioridad, teniendo:

- 40% del ancho de banda disponible para la voz.
- 20% del ancho de banda disponible para los datos.
- 10% del ancho de banda disponible para la señalización.

Al definir la política se procede a asignarla en el puerto serial que conecta ambas LAN en la dirección de salida (output), para así poder filtrar, clasificar y aplicar la política antes de ser enviados a través del enlace serial hacia su destino.

Configuración de MLP (Multilink Protocol)

Para la implementación de Multilink es necesario cambiar el protocolo Ethernet de HDLC a PPP. Es por ello que se crea una interfaz lógica Multilink para tratar indirectamente la interfaz serial a las conveniencias requeridas. Directamente se ven afectadas las rutas estáticas durante el proceso por lo que hay que especificarlas mediante la interfaz Multilink cuando ésta se encuentre activa, como se hizo en la tabla 6.3.

MX-RT	MTY-RT
MX-RT(config)#interface serial 0/1/0 MX-RT(config-if)#encapsulation ppp MX-RT(config-if)#no ip address MX-RT(config-if)#ppp multilink MX-RT(config-if)#ppp multilink group 1 MX-RT(config-if)#shutdown MX-RT(config-if)#exit MX-RT(config)#interface multilink 1 MX-RT(config-if)#ip address 192.168.40.1 255.255.255.0 MX-RT(config-if)#ppp multilink MX-RT(config-if)#ppp multilink group 1 MX-RT(config-if)#no shutdown MX-RT(config-if)#exit MX-RT(config)#ip route 192.168.20.0 255.255.255.255 multilink 1 MX-RT(config)#ip route 192.168.21.0 255.255.255.255 multilink 1	MTY-RT(config)#interface serial 0/0/0 MTY-RT(config-if)#encapsulation ppp MTY-RT(config-if)#no ip address MTY-RT(config-if)#ppp multilink MTY-RT(config-if)#ppp multilink group 1 MTY-RT(config-if)#shutdown MTY-RT(config-if)#exit MTY-RT(config)#interface multilink 1 MTY-RT(config-if)#ip address 192.168.40.2 255.255.255.0 MTY-RT(config-if)#ppp multilink MTY-RT(config-if)#ppp multilink group 1 MTY-RT(config-if)#no shutdown MTY-RT(config-if)#exit MTY-RT(config)#ip route 192.168.10.0 255.255.255.255 multilink 1 MTY-RT(config)#ip route 192.168.11.0 255.255.255.255 multilink 1

Tabla 6.3. Configuración de Multilink Protocol.

Al tener la interfaz virtual Multilink activa se configuró ésta como un grupo Multilink para formar una colección de interfaces que se ligan a la configuración de Multilink PPP y así agruparlas. Este punto no es necesario para este caso, pero se utilizó por cuestiones didácticas. Como se ha mencionado, al retirar la dirección IP de la interfaz serial, las rutas estáticas se vieron afectadas, por lo que se solucionó el enrutamiento al reconfigurarlas mediante la interfaz Multilink.

Configuración de LFI (Link Fragmentation and Interleaving)

LFI trabaja sobre una interfaz Multilink. Este mecanismo de QoS es uno de los más eficientes y recurridos en la práctica.

MX-RT	MTY-RT
MX-RT(config)#interface serial 0/1/0 MX-RT(config-if)#no service-policy output POLIVOZ MX-RT(config-if)#interface multilink 1 MX-RT(config-if)#ppp multilink interleave MX-RT(config-if)#ppp multilink fragment delay 10 MX-RT(config-if)#service-policy output POLIVOZ	MTY-RT(config)#interface serial 0/0/0 MTY-RT(config-if)#no service-policy output POLIVOZ MTY-RT(config-if)#interface multilink 1 MTY-RT(config-if)#ppp multilink interleave MTY-RT(config-if)#ppp multilink fragment delay 10 MTY-RT(config-if)#service-policy output POLIVOZ

Tabla 6.4. Configuración de Link Fragmentation and Interleaving.

Se puede observar en la tabla 6.4, el LFI configurado en la interfaz Multilink y para incrementar la eficiencia en QoS, se asoció el policing junto con LLQ a la interfaz Multilink para obtener un mejor desempeño de la red.

Configuración de MLS Qos Trust

MX-SW	MTY-SW
MX-SW(config)#interface FastEthernet0/1 MX-SW(config-if)#mls qos trust device cisco-phone MX-SW(config-if)#mls qos trust dscp	MTY-SW(config)#interface FastEthernet0/1 MTY-SW(config-if)#mls qos trust device cisco-phone MTY-SW(config-if)#mls qos trust dscp

Tabla 6.5. Configuración de MLS QoS Trust.

Con los comandos de MLS mostrados en la tabla 6.5 se asegura que el dispositivo confíe en cualquier teléfono Cisco conectado a la interfaz determinada. De esta manera, los teléfonos Cisco enviarán sus paquetes con un DSCP=5 y el switch confiará en este valor y lo dejará pasar sin cambiar el valor del DSCP.

Este método no es el camino más recomendable de QoS, ya que de ser un teléfono IP de otra marca, y si se tuviera únicamente configurado el comando *mls qos trust device cisco-phone,* el switch dudaría de los paquetes marcados con DSCP=5 que enviaría el dispositivo y por no tratarse de un producto Cisco, cambiaría el DSCP=0.

Resultados

En este esquema de red, el congestionamiento se concentra en la parte del enlace serial; esto se debe a que aquí se encuentra la tasa de transmisión más lenta de todo el enlace, pues en los demás enlaces del sistema se tiene una tasa correspondiente a la de un enlace FastEthernet, equivalente a 100 Mbps.

Esta reducción en el ancho de banda produce un cuello de botella que hace que los paquetes que en tramos anteriores habían circulado sin problema empiecen a colisionar y hayan pérdidas en el sistema, es por ello que es un buen lugar para aplicar mecanismos de calidad de servicio, ya que en los demás segmentos no se requieren.

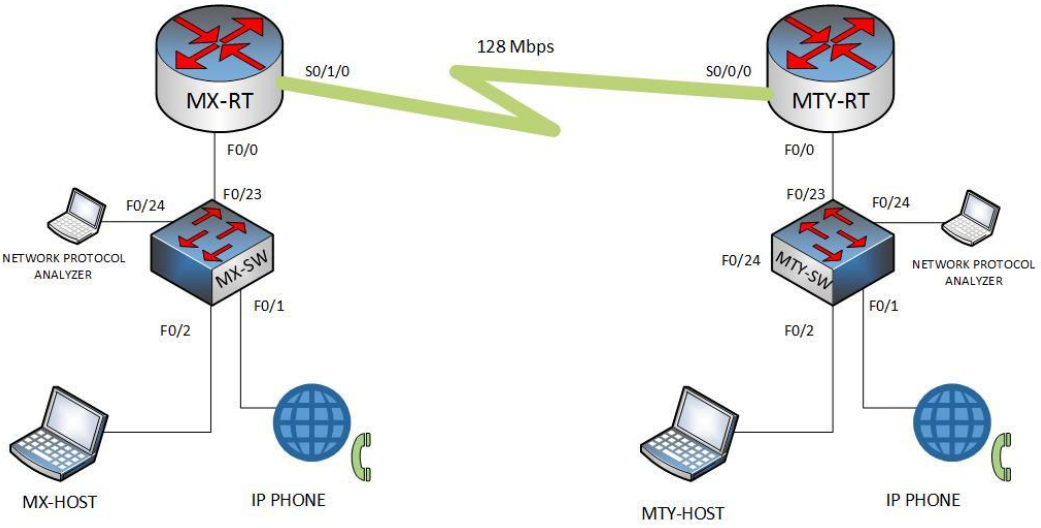

Figura 7.1. Conexión de la red

El enlace serial de baja tasa que se maneja en este trabajo ocasiona dificultades y complicaciones en la transmisión de la información entre LANs. El caso de implementación de QoS que mejor resolvió los problemas en la red fue el que incluye LLQ, LFI y Class-Based.

La combinación que se tiene de estos mecanismos arroja un trabajo en conjunto que controla de manera óptima el cómo va a pasar la información a través del serial para poder explotarlo sin que se tengan desperdicios o perdida de la información.

En los casos FIFO y WFQ no se pudo tener un aprovechamiento del canal apropiado para el manejo de todo tipo de tráfico ya que no se puede jerarquizar el tráfico a conveniencia del cliente. Estas deducciones se obtuvieron del resultado de las pruebas realizadas en los siguietes apartados.

Análisis de resultados

Utilizando un generador de tráfico (NetScan) instalado en las computadoras MX-HOST y MTY-HOST, se crearon paquetes HTTP para todos los casos. Adicionalmente se realizó un comparativo con tráfico ICMP para el caso con LFI. Éstos se generaron cada 20 ms durante 1 min, es decir, se transfirieron 3000 paquetes/min. Al ser la voz muestreada de igual forma cada 20 ms, se transfirieron 3000 paquetes/min, teniendo un total de 6000 paquetes/min de información.

Las mediciones fueron realizadas con ayuda del analizador de red WireShark en los puertos indicados en la figura 7.1. Estos puertos son espejos de los puertos troncales entre los switches y los routers por lo cual permitirán analizar cómo fue tratada la información a través del enlace serial.

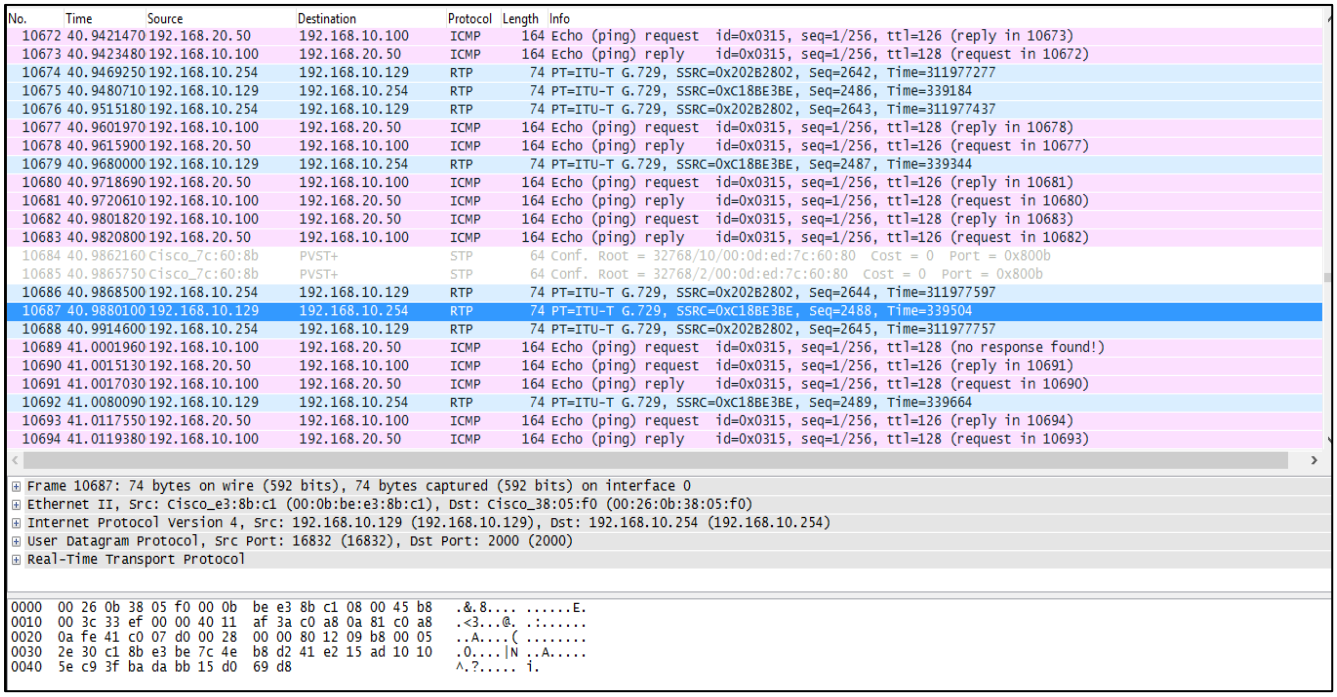

Figura 7.2. Monitoreo de puerto troncal MX-SW.

En la figura 7.2, se muestra para su análisis, uno de los resultados arrojados por WireShark y así entender cómo fueron interpretados los datos; también pueden apreciarse muchos parámetros generales como número de paquete, hora de arribo, IP fuente, IP destino, protocolo, tamaño del paquete e información sobre el paquete, por ejemplo, el códec utilizado en el caso de los RTP y la secuencia del paquete.

Al seleccionar un paquete se puede observar información específica de éste, como la trama Ethernet, los protocolos encapsulados, e incluso la ubicación de cada campo en la trama y el contenido en hexadecimal. También se entregan los puertos utilizados y el DSCP que cuenta el paquete, éste último es de gran relevancia para éste trabajo, que se aprecia en la figura 7.3.

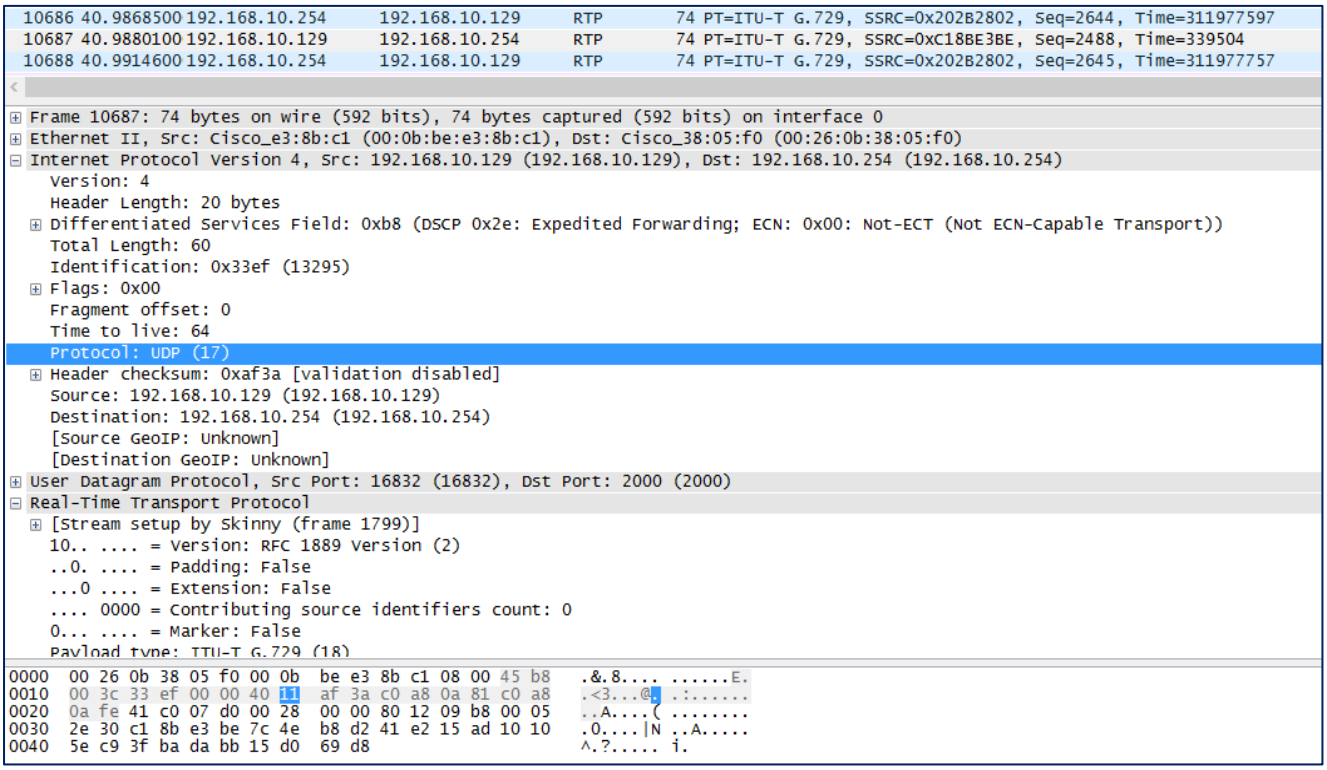

Figura 7.3. Detalles del paquete RTP.

El cálculo del jitter promedio lo arroja WireShark, así como el valor del retraso máximo, total de paquetes RTP y las pérdidas de los paquetes de voz.

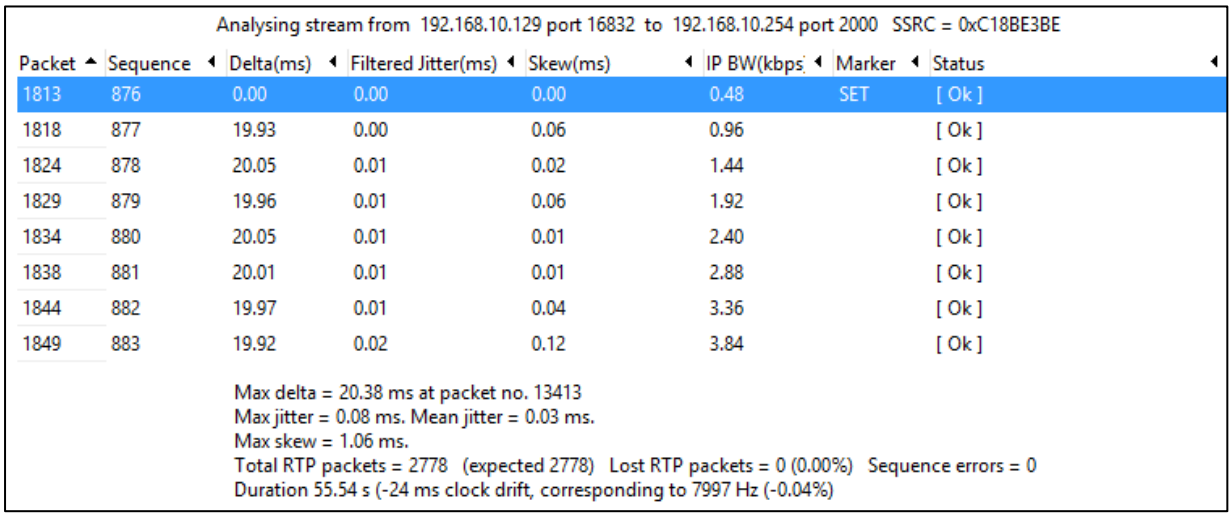

Figura 7.4. Análisis de jitter de voz en la prueba.

En la figura 7.4 el analizador de red proporciona algunos de los elementos para determinar que puede estar fallando en la red cuando se necesite y verificar cuál es el comportamiento de ésta.

Tráfico de señalización

Además del tráfico medido anteriormente, por el enlace serial también circula el tráfico de señalización, mismo que es capaz de apreciarse en WireShark mediante los paquetes de tipo Skinny, que se muestran en la figura 7.5.

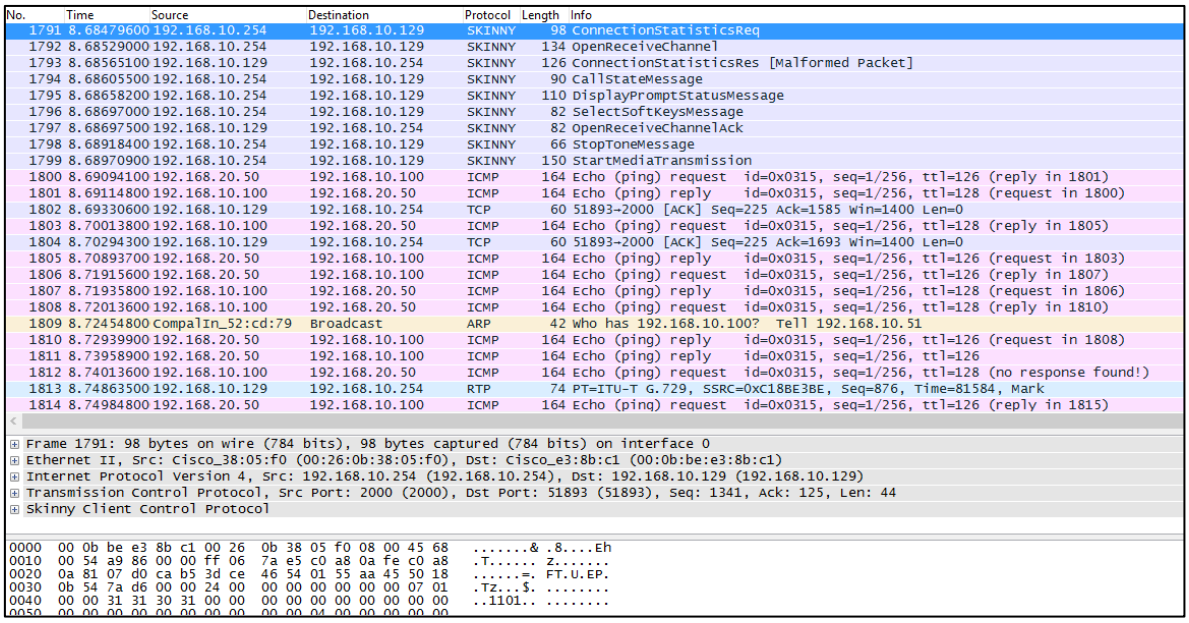

Figura 7.5. Tráfico de señalización.

A continuación se procede a la muestra de los resultados y su interpretación para cada caso.

Caso 1. FIFO

Para este primer contexto se utilizó FIFO como método de encolamiento para la transmisión de los paquetes que el router va recibiendo y que posteriormente enviará a su destino.

Teniendo en cuenta el resultado de la ecuación[15] para el ancho de banda requerido sin la implementación de mecanismos QoS, se procede a calcular el ancho de banda requerido para los datos en las mismas condiciones, con la finalidad de obtener el valor del ancho de banda total requerido para la transmisión de la información en este escenario.

$$BW_{Datos} = (payload\ de\ datos + headers\ 2) * \left(\frac{1}{20\ [ms]}\right) * 8$$

$$BW_{150} = (150 + 18)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 67.2\ kbps$$

$$BW_{300} = (300 + 18)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = \ 127.2\ kbps$$

[15] Véase la página 25.

$$BW_{1500} = (1500 + 18)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 607.2\ kbps$$

MÉXICO								
QoS	**Bytes**	**BW DATOS (kbps)**	**BW VOZ (kbps)**	**BW TOTAL (kbps)**	**% BW requerido del enlace**	**Jitter VOZ (ms)**	**Pérdida paquetes de voz (%)**	**Protocolo**
FIFO 100	150	67.2	31.2	98.4	76.875	0.117	0	TCP/HTTP
FIFO 100	300	127.2	31.2	158.4	123.75	3.493	51.5	TCP/HTTP
FIFO 100	1500	607.2	31.2	638.4	498.75	No entró la llamada	No entró la llamada	TCP/HTTP
MONTERREY								
FIFO 100	150	67.2	31.2	98.4	76.875	0.125	0	TCP/HTTP
FIFO 100	300	127.2	31.2	158.4	123.75	3.568	50.3	TCP/HTTP
FIFO 100	1500	607.2	31.2	638.4	498.75	No entró la llamada	No entró la llamada	TCP/HTTP

Tabla 7.1. Resultados del primer escenario.

Los resultados entre Monterrey y México son muy similares ya que se generó el tráfico en ambas direcciones con un flujo simétrico. Este comportamiento se observa en todos los casos.

Se puede observar que en este caso en donde se tiene implementada la cola FIFO con un búfer de 100 paquetes se obtuvieron muchas deficiencias en la llamada tanto visibles como audibles. En la tabla 7.1 se puede observar que al incrementar el tamaño de los paquetes de datos, éstos se van perdiendo hasta llegar al punto en donde la llamada ya no tiene la oportunidad de ser enlazada.

El jitter se mantuvo en un valor muy bajo con paquetes de 150 bytes debido a que el ancho de banda soporta el envío de voz y datos en tiempo real y el búfer es suficiente para que no existan perdidas. Al duplicar el tamaño del paquete ya se presenta una pérdida considerable de un poco más de la mitad de los paquetes y de manera audible se escucha como la voz se torna entrecortada y muy atrasada. El búfer ya no es suficiente.

Al tomarse más tiempo para poder transmitir un paquete pesado comienzan a descartarse los paquetes de voz debido a la lenta liberación del búfer.

Es por ello que la llamada ni siquiera puedo enlazarse cuando los paquetes de 1500 bytes toman lugar en el búfer. Recordando que la transmisión se configuró para que se enviará un paquete de 1500 bytes cada 20 ms, y en ambos flujos de Tx, por lo que el ancho de banda del enlace serial está saturado y puede observarse en la columna de BW.

Caso 2. WFQ

Para el segundo escenario se usó WFQ como método de calidad de servicio. Como puede verse en la tabla 7.2, ya se empiezan a presentar diferencias en los parámetros comparándolo con el caso anterior.

MÉXICO								
QoS	**Bytes**	**BW DATOS (kbps)**	**BW VOZ (kbps)**	**BW TOTAL (kbps)**	**% BW requerido del enlace**	**Jitter VOZ (ms)**	**Pérdida paquetes de voz (%)**	**Protocolo**
WFQ	150	67.2	31.2	98.4	76.875	0.127	0	TCP/HTTP
WFQ	300	127.2	31.2	158.4	123.75	16.798	0	TCP/HTTP
WFQ	1500	607.2	31.2	638.4	498.75	28.213	0	TCP/HTTP
MONTERREY								
WFQ	150	67.2	31.2	98.4	76.875	0.121	0	TCP/HTTP
WFQ	300	127.2	31.2	158.4	123.75	16.840	0	TCP/HTTP
WFQ	1500	607.2	31.2	638.4	498.75	28.230	0	TCP/HTTP

Tabla 7.2. Resultados del segundo escenario.

Este mecanismo utiliza un algoritmo que ubica los paquetes en colas independientes con base a su peso.

Puede observarse un cambio positivo en las perdidas de los paquetes de voz si se compara con la tabla 7.1 del caso previo, ya que al tener colas independientes al peso de los paquetes, éstos pudieron salir sin problema del búfer. El problema se tuvo en el incremento del jitter debido al aumento del tamaño de los paquetes HTTP provocando una saturación en el ancho de banda del serial que terminó por retardar la llamada. De manera audible la conversación era clara pero no llegaba en tiempo real.

Cabe recordar que en la red de este trabajo sólo se ocupó una llamada por lo que al incrementar el número de llamadas se tendría un jitter aún más grande, así como la posibilidad de no completar la llamada satisfactoriamente.

Caso 3. LFI

Para el último escenario se ocupó LFI como método de calidad de servicio, mismo que se desplegó sobre una interfaz Multilink, previamente configurada en ambos routers.

Para este caso se tiene un nuevo cálculo del ancho de banda requerido por cada llamada como por los datos.

$$BW_{Datos} = (payload\ de\ datos + headers\ 2) * \left(\frac{1}{20\ [ms]}\right) * 8$$

$$BW_{150} = (150 + 13)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 65.2\ Kbps$$

$$BW_{300} = (300 + 13)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 125.2\ Kbps$$

$$BW_{1500} = (1500 + 13)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 605.2\ Kbps$$

$$BW_{por\ llamada} = (payload\ de\ datos + headers\ 3 + headers\ 2) * \left(\frac{1}{20\ [ms]}\right) * 8$$

$$BW_{por\ llamada} = (20 + 40 + 13)[bytes] * \left(\frac{1}{20\ [ms]}\right) * 8[bits] = 29.2\ Kbps$$

La ventaja que se tiene en este caso es que a pesar de contar con un cálculo de los anchos de banda requeridos, se pueden asignar prioridades o un valor de ancho de banda fijo para el tratamiento de las clases. En este trabajo se aplicó una política para que el ancho de banda requerido por la voz se reservara siempre para ésta y así no tener ningún paquete de voz perdido y el menor número posible de paquetes de datos perdidos.

MEXICO								
QoS	**Bytes**	**BW DATOS (kbps)**	**BW VOZ (kbps)**	**BW TOTAL (kbps)**	**% BW requerido del enlace**	**Jitter VOZ (ms)**	**Pérdida paquetes de voz (%)**	**Protocolo**
LFI	150	65.2	29.2	94.4	73.75	0.102	0	TCP/HTTP
LFI	300	125.2	29.2	154.4	120.625	5.277	0	TCP/HTTP
LFI	1500	605.2	29.2	634.4	495.625	5.957	0	TCP/HTTP
MONTERREY								
LFI	150	65.2	29.2	94.4	73.75	0.121	0	TCP/HTTP
LFI	300	125.2	29.2	154.4	120.625	7.502	0	TCP/HTTP
LFI	1500	605.2	29.2	634.4	495.625	7.289	0	TCP/HTTP

Tabla 7.3. Resultados del tercer escenario.

En este caso se observan en la tabla 7.3, valores de jitter muy bajos y porcentajes nulos de pérdida, mismos que se repiten cuando se cambia el tamaño del paquete enviado.

Ha de entenderse que el porcentaje de pérdidas se ha reducido, como en el caso anterior, debido a que comienza a hacerse presente el uso de mecanismos de calidad de servicio, fragmentación e intercalado en este caso. Los paquetes que en casos anteriores se habían perdido por ser muy

grandes, se fragmentan y se intercalan con los paquetes de menor tamaño por lo que el porcentaje de pérdida es cero debido a que ahora se envían todos.

Respecto al jitter, puede verse que no se tiene el menor que se ha presentado comparado con los casos anteriores ya que en el primer caso aunque el jitter es más bajo, hay una pérdida de paquetes significativa mientras que en el tercero la pérdida es nula, situación donde se refleja que el uso de fragmentación e intercalado de paquetes mejora considerablemente la eficiencia del sistema.

Si se pone atención en los valores de jitter de este caso puede notarse el aumento del mismo, situación que refleja el flujo de tráfico que también va en aumento cuando se cambia el tamaño de los paquetes a uno mayor. De otra manera el valor del jitter es correcto porque se tuvo poco tráfico al principio y a partir de ahí comienza a incrementarse. Por último, se hace énfasis en que es el mejor mecanismo de calidad de servicio porque si se compara con los anteriores presenta ventajas contra ambos:

- Comparando contra el caso 1 (FIFO). Hay mayor jitter debido a que la pérdida de paquetes está siendo compensada con la variación en retraso, dado que no están habiendo pérdidas en absoluto.
- Comparando contra el caso 2 (WFQ). Se conserva el porcentaje de pérdidas nulo y se reduce el jitter aún más.

Caso adicional. LFI con tráfico ICMP

Este caso se hizo para corroborar los resultados del funcionamiento de la fragmentación e intercalado del caso anterior, haciendo una variación en el tipo de tráfico utilizado, ICMP para este escenario.

MEXICO								
QoS	**Bytes**	**BW DATOS (kbps)**	**BW VOZ (kbps)**	**BW TOTAL (kbps)**	**% BW requerido del enlace**	**Jitter VOZ (ms)**	**Pérdida paquetes de voz (%)**	**Protocolo**
LFI	150	65.2	29.2	94.4	73.75	7.450947	0	UDP/ICMP
LFI	300	125.2	29.2	154.4	120.625	5.437919	0	UDP/ICMP
LFI	1500	605.2	29.2	634.4	495.625	5.906746	0	UDP/ICMP
MONTERREY								
LFI	150	65.2	29.2	94.4	73.75	7.18219	0	UDP/ICMP
LFI	300	125.2	29.2	154.4	120.625	7.567264	0	UDP/ICMP
LFI	1500	605.2	29.2	634.4	495.625	7.203629	0	UDP/ICMP

Tabla 7.4. Resultados del escenario adicional.

Como se aprecia en la tabla 7.4, los valores del jitter promedio y porcentaje de pérdidas se acercan bastante a los del tercer escenario debido a que se repiten las condiciones y características del mismo.

Al usar MLP LFI, también se está usando CBWFQ junto con PQ y se está dando prioridad a la voz, evitando las perdidas y teniendo un jitter bajo. Puede compararse con el caso 2 donde solamente se usa WFQ, pero con una mejor eficiencia.

Revisando los valores de este escenario se confirma que LFI está aplicándose de forma correcta para ambos casos, pues se obtuvieron los valores esperados con anterioridad.

En la figura 7.6, se muestra una comparación de los mecanismos de calidad y servicio en sus diferentes modalidades, corroborando de manera visual que los mejores casos se llevaron a cabo con LFI con un jitter considerablemente bajo y sin pérdidas. Asimismo se observa el caso en el que no se establece la llamada con FIFO y con una transferencia de datos de 1500 bytes.

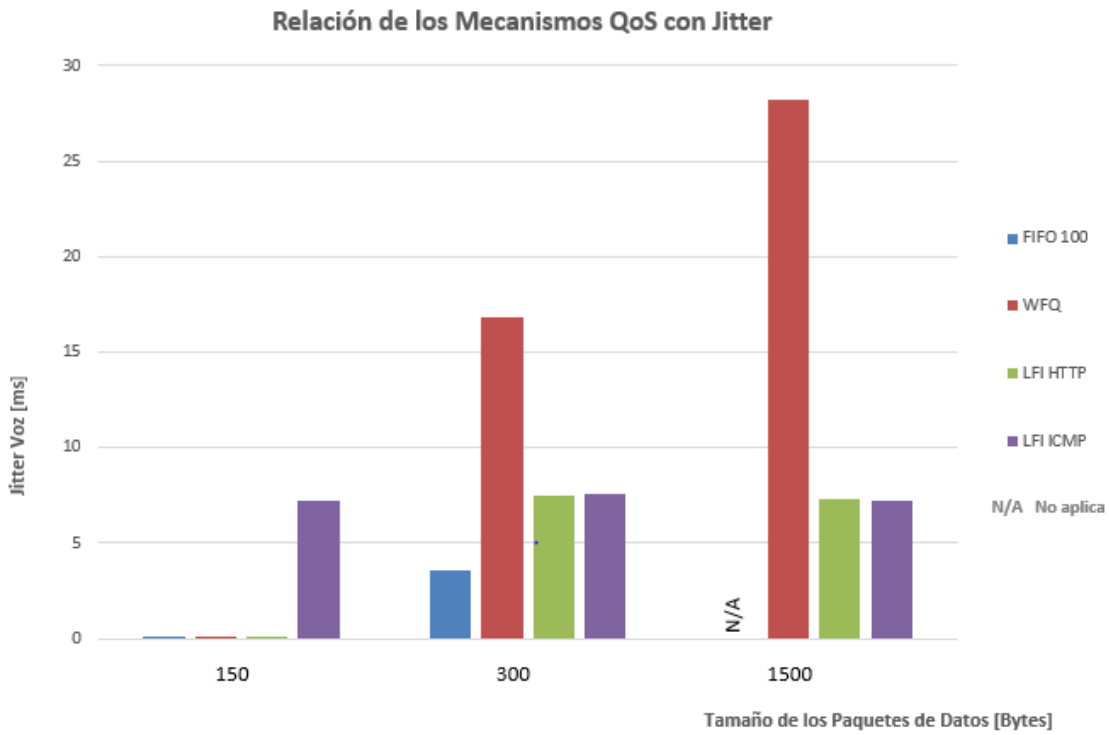

Figura 7.6. Comportamiento del jitter con los mecanismos de QoS. Mediciones en México.

Conclusiones

Después de analizar cada uno de los escenarios sobre los que se hicieron pruebas, se llegó a diversas conclusiones, que se expresarán a continuación con la finalidad de cerrar o ultimar puntos que se han hecho a lo largo de todo el trabajo.

Sobre los mecanismos de calidad:

- FIFO no puede considerarse un método de calidad de servicio ya que, si bien tiene un funcionamiento específico, no hace un tratamiento específico de los paquetes.
- WFQ es un buen mecanismo de calidad, pues proporciona cierta ventaja al momento de hacer la diferenciación de tipos de tráfico y agruparlas en colas independientes. Contribuye de forma positiva a la mejora del proceso de la voz, aunque no necesariamente sea el mejor método desde la perspectiva de este trabajo.
- LFI. Es el mejor mecanismo de calidad de servicio para el esquema de red presentado sobre la interfaz virtual Multilink, dado que los valores que presenta en cuestión de pérdidas, retrasos y jitter son los más adecuados para la transmisión de la voz.

Sobre los parámetros del sistema:

- La pérdida de paquetes se presentó con gran impacto en el caso de FIFO, pues se descartaban muchos paquetes excedentes, lo cual perjudicaba enormemente el tratamiento que la voz recibía, ya que hacía ininteligible todo lo que se transmitía de un lado del canal hacía el otro.
- El retardo de paquetes, al igual que la pérdida de los paquetes, se presentó como una enorme dificultad desde el principio, ya que era un parámetro con el que se tenía que lidiar siempre sin importar el mecanismo de calidad aplicado, pues como se mencionó, algunos retrasos son inherentes a los dispositivos de transmisión.
- El jitter fue el parámetro en el que se esperaban más cambios al aplicar la calidad, pues sin duda es el que más repercute al entendimiento de la voz en un medio de comunicación, en este caso, el enlace serial. Pudo observarse que en los valores obtenidos mediante las pruebas, el jitter respondía de la forma que se esperó para todos los casos: bajo para FIFO ya que había muchas pérdidas en su lugar, alto en WFQ porque había muchos retrasos y el sistema era algo inestable por el funcionamiento de las colas y bajo en LFI ya que se compensó porque no hubo pérdidas.
- Las pérdidas de paquetes de otro tipo de tráfico no fueron considerables ya que LFI logró evitarlos, así como el jitter de datos.

Sobre la calidad percibida por el usuario:

- Con FIFO no existía como tal el concepto de calidad de servicio, pues el tratamiento que recibía la voz y los datos era pésimo, la voz sonaba muy atrasada, se cortaba, presentaba saltos e inclusive se escuchaba el canal completamente vacío.
- Con WFQ la percepción de la voz mejoró notablemente pues los retrasos se redujeron, la voz sonaba más clara, los saltos en el audio disminuyeron y las pérdidas se hicieron casi nulas.
- Con LFI la calidad del audio fue óptima ya que como se mencionó anteriormente en el análisis de resultados, la voz se escuchaba en tiempo y forma, sin saltos, retrasos ni pérdidas.

Sobre la configuración implementada:

- El uso de MQC facilitó la configuración de los mecanismos de calidad de servicio debido a que permite definir una clase de tráfico, crear una política de tráfico, y que se asocie la política de tráfico a una interfaz. Es importante tener presente que no es un mecanismo de QoS, sino una herramienta que Cisco implementó para facilitar la configuración de QoS.
- Verificar el firmware y modelo del dispositivo antes de comenzar con las configuraciones ayudó ya que es importante para tener presente qué comandos y servicios soporta. De no contar con el firmware apropiado para el propósito, se deberá recurrir con el proveedor Cisco para solicitarle la actualización correspondiente.

Sobre el software utilizado:

- NetScan demostró ser una herramienta eficiente para la generación de paquetes de todo tipo, pues pueden modificarse ampliamente los parámetros que los paquetes han de contener.
- WireShark cumplió con el objetivo de analizar el tráfico en las interfaces debido a que se lograron precisar los parámetros definidos desde el inicio (pérdidas, retrasos y jitter) y además se pudieron vislumbrar parámetros adicionales (tráfico de señalización, de control y de gestión de la red en general).

Sobre el sistema en general:

- La disposición de los equipos ayudó considerablemente a estudiar el análisis mediante el uso del software, ya que su linealidad o arquitectura hizo más sencillo aislar la parte del sistema que tenía que ser revisada en ese momento.

- La simetría que el sistema aporta también permitió hacer suposiciones que al final resultaron correctas, como el hecho de que los valores de pérdidas, retrasos y jitter resultaron similares para los casos de México y Monterrey, así como la cantidad de paquetes transmitidos y la calidad de las llamadas.
- QoS es recomendado aplicarlo sobre un sistema cuando se presenten enlaces de baja tasa de transmisión. Sin importar el tipo de red a configurar, los mecanismos de QoS tienen en esencia la misma estructura y comandos.

Referencias

LIBROS

1) **Wallace Kevin, 2011, Implementing Cisco Unified Communications Voice over IP and QoS (Foundation Learning Guide), Cisco Press, 4th edition, USA.**

Capítulos: 1. Introducing voice gateways (1-161).
2. Configuring basic voice over IP (165-294).
7. Introducing Quality of Service (567-604).
8. Configuring QoS mechanisms (607-673).

2) **Odom Wendell, 2013, Cisco CCENT/CCNA ICND1 100-101 (Official Cert Guide), Cisco Press, 1st edition, USA.**

Capítulos: 3. Fundamentals of WANs (67-86).
4. Fundamentals of IPv4 addressing and routing (89-115).
5. Fundamentals of TCP/IP transport and applications (117-135).
8. Configuring Ethernet switching (199-229).
9. Implementing Ethernet virtual LANs (235-260).
15. Installing Cisco routers (403-421).
18. Configuring and verifying host connectivity (493-523).
22. Basic IPv4 access control lists (599-621).
23. Advanced IPv4 ACLs and device security (623-651).

3) **Odom Wendell, 2013, Cisco CCENT/CCNA ICND2 200-101 (Official Cert Guide), Cisco Press, 1st edition, USA.**

Capítulos: 12. Implementing point to point WANs. (359-386).
13. Understanding Frame Relay concepts (389-406).
15. Identifying other types of WANs (445-463).
20. Managing IOS files (579-601).

4) **Ariganello Ernesto; Barrientos Sevilla Enrique, 2010, Redes Cisco, CCNP a fondo (Guía de estudio para profesionales), AlfaOmega, 1ª edición, México.**

Capítulos: 11. Redes virtuales (321-329).
17. Telefonía IP (435-452).
20. Redes inalámbricas (479-495).
25. MPLS (563-601).
35. Implementaciones VoIP (763-789).
36. Calidad de servicio (791-802).
38. Administración de colas y congestión (821-837).
39. Manipulación del tráfico y del enlace (841-846).

5) **Tanenbaum Andrew; Wetherall David, 2012, Redes de computadoras, Pearson Education, 5ª edición, México.**

Secciones: 1.1. Usos de las redes de computadoras (2-12).
3.1 Cuestiones de diseño de la capa de enlace de datos (168-174).
4.3 Ethernet (240-255).
4.4 Redes inalámbricas (257-267).
5.4 Calidad de servicio (347-361).

6.3 Control de congestión (455-462).
6.4 Los protocolos de transporte de internet: UDP (464-469).
6.5 Los protocolos de transporte de internet: TCP (474-499).

6) **Empson Scott, 2013, CCNA Routing and Switching (Portable Command Guide), Cisco Press, 3rd edition, USA.**

Capítulos:
6. Configuring a Cisco router (45-55).
7. Static routing (57-61).
11. Configuring a switch (91-97).
12. VLANs (101-104).
22. Remote connectivity using Telnet or SSH (195-198).
23. Verifying end to end connectivity (199-201).
28. DHCP (227-231).
29. Configuring serial encapsulation: HDLC and PPP (233-237).
33. Managing traffic using access control lists (257-267).

7) **Cloara Jeremy; Valentine Michael, 2012, CCNA Voice 640-461 (Official Cert Guide), Cisco Press, 2nd edition, USA.**

Capítulos:
1. Traditional voice versus unified voice (3-25).
2. Understanding the pieces of Cisco Unified Communications (27-46).
3. Understanding the Cisco IP phone concepts and registration (49-67).
4. Getting familiar with CME administration (69-79).
13. Voicemail integration with Cisco Unity Connection (343-375).
14. Enabling Cisco Unified Presence Support (377-394).

8) **Johnson Allan, 2009, 31 days before your CCNA exam, Cisco Press, 2nd edition, USA.**

Secciones:
Day 31. Networking devices, components and diagrams (1-12).
Day 30. Network models and applications (13-19).
Day 29. Data flow from end to end (21-29).
Day 24. Switching technologies and VLAN concepts (71-85).
Day 23. VLAN and trunking configuration and troubleshooting (87-95).
Day 20. Host addressing, DHCP and DNS (123-134).
Day 17. Connecting and booting routers (161-166).
Day 16. Basic router configuration and verification (167-177).
Day 15. Managing Cisco IOS and configuration files (179-189).
Day 14. Static, default and RIP routing (191-209).
Day 10. Wireless standards, components and security (253-259).
Day 7. ACL concepts and configurations (279-288).
Day 3. PPP configuration and troubleshooting (329-336).

TESIS

- ***Joskowicz José. Voz, video y telefonía sobre IP, tesis (licenciatura en Ingeniería Eléctrica), Uruguay, Universidad de la República, Instituto de Ingeniería Eléctrica, 2013, 93 pp.***
- ***Jaime Hernández Joel-Martínez Santiago Edson. Proceso de integración de la red de VoIP en la torre central de telecomunicaciones de México, tesis (licenciatura en Ingeniería Eléctrica-Electrónica), México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2010, 90 pp.***
- ***Arana Mondragón Juan Manuel-Meza Mejía Iselín. Implantación de calidad de servicio en redes inalámbricas Wi-Fi, tesina (licenciatura en Informática), México, Escuela Superior de Ingeniería Mecánica y Eléctrica, Unidad Culhuacán, 2009, 259 pp.***

NORMAS Y ESTÁNDARES

- **G.114. One-way transmission time.**
- **G.711. Pulse Code Modulation (PCM) of voice frequencies.**
- **G.729. Coding of speech at 8 kbit/s using CS-ACELP.**
- **802.3. Local Area Networks (LAN) Protocols.**
- **802.1p. LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization.**
- **802.1q. Bridges and bridged networks.**
- **802.11e. MAC Enhancements for Quality of Service.**

MESOGRAFÍA

http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html [Consultado el 22 de agosto de 2015]

http://www.cisco.com/cisco/web/support/LA/102/1027/1027043_Designing_VoIP_over_ISDN.pdf [Consultado el 10 de noviembre de 2015]

http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html [Consultado el 26 de agosto de 2015]

http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html#wp1029087 [Consultado el 12 de septiembre de 2015]

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html#wp17641 [Consultado el 27 de noviembre de 2015]

http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/12156-voip-ov-fr-qos.html#topic4 [Consultado el 3 de febrero de 2016]

http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/14073-fr-traffic.html [Consultado el 3 de febrero de 2016]

http://www.cisco.com/cisco/web/support/LA/107/1075/1075610_qos_mqc_ps6922_TSD_Products_Configuration_Guide_Chapter.pdf [Consultado el 10 de octubre de 2015]

http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html [Consultado el 12 de febrero de 2016]

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/mplsqos.html [Consultado el 12 de febrero de 016]

http://www.docs.oracle.com/cd/E19957-01/820-2981/ipqos-intro-50/index.html [Consultado el 10 de enero de 2016]

http://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP.pdf [Consultado el 14 de octubre de 2015]

http://www.jupiter.utm.mx/~tesis_dig/10141.pdf [Consultado el 21 de diciembre de 2015]

http://www.udb.edu.sv/udb/archivo/guia/electronica-ingenieria/fundamentos-de-voz-sobre-ip-y-calidad-de-servicio/2015/i/guia8.pdf [Consultado el 15 de agosto de 2015]

http://www.voip-info.org/wiki/view/What+is+VOIP [Consultado el 10 de agosto de 2015]

Glosario

Access point. Punto de acceso. Terminal de red que brinda conectividad de red a dispositivos inalámbricos mediante ondas de radio.

ARP. Address Resolution Protocol. Protocolo de resolución de direcciones. Se encarga de encontrar una dirección MAC asociada a una dirección IP dada.

Bandwidth. Ancho de banda. Expresado también como BW por sus siglas en inglés, es la cantidad de datos que se puede transmitir en una conexión de red en un tiempo determinado, se expresa en bps.

Black hole. Agujero negro. Se refiere a lugares en la red donde el tráfico entrante o saliente se descarta en silencio, sin informar a la fuente que los datos no llegaron a su destinatario.

Broadcast. Tipo de tráfico cuyo envío se realiza de forma masiva a un bloque de direcciones.

Búfer. Fila o hilera de almacenamiento temporal, de paquetes para este caso.

CAC. Call Admission Control. Control de admisión de llamadas. Se encarga de que solamente un número determinado de llamadas simultáneas sean admitidas a la red.

CDP. Cisco Discovery Protocol. Protocolo de Cisco que sirve para dar a conocer información sobre los dispositivos vecinos, así como algunos de los parámetros que estos ocupan.

CIR. Commited Information Rate. Tasa de información comprometida.

Codificación. Proceso en el cual una muestra es representada por una sucesión de números o valores.

CNG. Comfort Noise Generator. Algoritmo que genera una señal de ruido cuando no hay ruido presente en el canal. Funciona en conjunto con el algoritmo ***VAD***.

Coder. Codificador.

CS-ACELP. Conjugate Structure Algebraic Code Excited Linear Prediction. Algoritmo perteneciente al estándar de codificación G.729.

CSMA/CA. Carrier Sense Multiple Access with Collision Avoidance. Sistema de control de acceso a redes que permite que múltiples estaciones utilicen un mismo medio de transmisión.

Decoder. Decodificador.

Default gateway. Puerta de enlace predeterminada.

Delay. Retraso o retardo.

DCE. Data Communication Equipment. Equipo de comunicación de datos. Cualquier equipo proveedor de servicio en una red.

DTE. Data Terminal Equipment. Equipo terminal de datos. Cualquier equipo receptor o emisor de datos que se encuentre al final de una conexión.

DiffServ. Servicios diferenciados.

DLCI. Data Link Connection Identifier. Identificador de conexión de enlace de datos.

DSP. Procesador digital de señales.

DTMF. Dual Tone Multi Frequency. Marcación por tonos. Es un sistema que se usa sobre líneas analógicas, y que sirve para la señalización entre equipos telefónicos.

EDCA. Enhanced Distributed Channel Access. Acceso mejorado al canal distribuido.

EDCF. Enhanced Distribution Coordination Function. Función mejorada de coordinación de distribución.

Frame Relay Traffic Shaping. Conformación de tráfico Frame Relay.

Frame Relay. Tecnología de conmutación de paquetes para redes distantes.

HCCA. ***HCF*** Controlled Channel Access. Acceso híbrido al canal controlado.

HCF. Hybrid Coordination Function. Función híbrida de coordiniación.

Header. Encabezado o etiqueta identificadora del paquete.

IARP. Inverse ***ARP***. ARP inverso. Funciona al contrario del protocolo ARP.

IP. Internet Protocol. Protocolo de Internet.

ITU. International Telecommunications Union. Unión Internacional de Telecomunicaciones. Institución de la ONU, encargada de regular las telecomunicaciones a nivel internacional.

Jitter. Fluctuación.

LER. Label Edge Router. Router etiquetador de borde.

LMI. Local Management Interface. Interfaz de gestión local. Es un estándar de señalización usado entre routers y switches Frame Relay.

LSR. Label Switch Router. Switch etiquetador de borde.

MAC. Medium Access Control. Control de acceso al medio.

Marking. Marcado de tráfico. Mecanismo de DiffServ que consiste en colorear los paquetes que cruzan una interfaz.

Modelo OSI. Es un modelo de referencia para la arquitectura de red, que divide la comunicación en siete niveles. Define cómo se comunica y trabaja cada nivel con los niveles inmediatamente superiores e inferiores.

Modularidad. Es la propiedad que tiene un sistema de dividirse y poder analizarse en partes y no como un todo, lo que facilita el estudio de algún segmento en específico.

MPLS. Multi-Protocol Label Switching. Protocolo de conmutación entre capa 2 y 3.

MSDU. ***MAC*** Service Data Unit. Unidad de servicio de datos de la capa MAC.

Multicast. Tráfico multicast. Envío de tráfico a múltiples destinos simultáneamente.

Overhead. Excedente. Se le llama así al gasto extra que excede el ancho de banda, mismo que es producido por la información adicional.

Payload. Carga útil del paquete. Para este caso será la voz digitalizada procesada por el códec.

PBX. Private Branch Exchange. Central telefónica privada.

Policing. Políticas o reglas de tráfico. Mecanismo de DiffServ que consiste en una política de restricción que regula el envío de paquetes.

Priority queuing. Encolamiento por prioridad. Conocido más ampliamente como LLQ.

PSTN. Public Switched Telephone Network. Red telefónica conmutada.

PVC. Private Virtual Circuit. Circuito virtual privado.

QBSS. QoS Basic Service Set. Extensión del estándar 802.11e.

QoS. Quality of Service. Calidad de servicio.

Rango dinámico. La relación de un máximo nivel especificado de un parámetro, al valor perceptible mínimo del mismo.

Rate-based queuing. Conocido más ampliamente como CBWFQ.

Redes convergentes. Las redes convergentes o redes de multiservicio se refieren a la integración de los servicios de voz, datos y video sobre una sola red.

Relación de compresión. Parámetro que indica en qué proporción ha sido comprimida la información en razón con su valor sin comprimir.

RTP. Real-Time Transfer Protocol. Protocolo de transferencia en tiempo real.

Shaping. Ver ***Traffic shaping.***

SNR. Signal to Noise Ratio. Relación señal a ruido.

Stream. Flujo de datos o información.

Softphone. Es un servicio telefónico mediante software que se basa en el uso de telefonía de voz sobre IP.

SVC. Switched Virtual Circuit. Circuit virtual conmutado.

Tail drop. Recorte/eliminación de paquetes sobrantes en un búfer. Algoritmo de gestión de tráfico implementado en equipos de enrutamiento que ayuda a mejorar la congestión de red.

Tasa de bits máxima. Tasa de transferencia de datos máxima.

Tasa de bits media. Tasa de transferencia de datos promedio.

Traffic engineering. Ingeniería de tráfico. Herramienta de MPLS que sirve para optimizar el tráfico de la red.

Traffic shaping. Conformación de tráfico. Mecanismo de DiffServ que permite tener un mejor control sobre el flujo de tráfico. También se le conoce como shaping.

Trunking. Enlace troncal. Se usa para transmitir tráfico de diferentes ***vlans*** en un mismo enlace mediante etiquetas previamente asignadas.

UDP. User Datagram Protocol. Protocolo de datagramas de usuario.

Vlans. Virtual LANs. Redes virtuales de área local.

VAD. Voice Activity Detection. Detección de actividad de voz. Algoritmo de voz que detecta intervalos de silencio.

Wi-Fi. Estándar de transmisión en redes inalámbricas.

Wi-Fi Alliance. Institución creadora de Wi-Fi.

WMM. Wi-Fi Multimedia. Esquema de calidad de servicio para Wi-Fi.

Windowing. Ventana deslizante. Proceso de transmisión perteneciente al protocolo TCP.

Índice de figuras y tablas

FIGURAS

TABLAS