Implementación de un sistema ToIP con foco especial en los aspectos de QoS - calidad de servicio.

Nicolás Andrés Guillén Echegaray

Sistemas de Comunicación

Tutor/a de TF
Javier Jordán Parra

Profesor/a responsable de la asignatura
Carlos Monzo Sánchez

12/06/2023

Universitat Oberta de Catalunya

Ficha del Trabajo Final

Título del trabajo:	Implementación de una solución de ToIP con foco especial en los aspectos de QoS - calidad de servicio.
Nombre del autor/a:	Nicolás Andrés Guillén Echegaray
Nombre del Tutor/a de TF:	Javier Jordán Parra
Nombre del/de la PRA:	Carlos Monzo Sánchez
Fecha de entrega:	06/2023
Titulación o programa:	Máster Universitario en Ingeniería de Telecomunicación
Área del Trabajo Final:	Sistemas de comunicación
Idioma del trabajo:	Castellano
Palabras clave	VoIP, ToIP, QoS, TCP/IP, caudal

Resumen del Trabajo

Los métodos de comunicación se han ido adaptando a los avances tecnológicos surgidos durante el paso del tiempo. Entre ellos la telefonía, que en las últimas décadas ha sufrido diversos cambios. A mediados de los 90's comienza a usarse de forma masiva la telefonía mediante los protocolos de Internet y TCP/IP.

La telefonía IP trabaja convirtiendo llamadas, faxes y más información en señales digitales que viajan en redes IP. Se identifican dos términos sinónimos, la VoIP (Voice over Internet Protocol) y ToIP (Telephony over Internet Protocol). La VoIP se entiende como la comunicación entre dos terminales mediante IP. La ToIP engloba los servicios telefónicos y su infraestructura de paquetes de datos, con el propósito de asegurar la calidad de los servicios.

La calidad de la comunicación se determina por varios parámetros. La selección del códec, la gestión de la pérdida de paquetes, el retardo, el jitter e incluso el propio diseño de la red. Por tanto, los criterios de la calidad del servicio, QoS (Quality of Service) dependerán del conjunto de estos parámetros y la percepción subjetiva de los usuarios. Cada cliente tendrá unas demandas en función de sus necesidades, donde el proveedor del servicio deberá adaptar su oferta y que esta se asemeje lo más próximo posible a los valores asegurados QoS.

Para poder comparar los diferentes mecanismos, cómo afectan los parámetros en la comunicación y las medidas obtenidas se realizará un despliegue simulando un

escenario real de telefonía sobre IP, donde se podrá comprobar qué parámetros y mecanismos se usan para gestionar la QoS.

Abstract

The methods of communication have been adapting to technological advances that have emerged over time. Among them is telephony, which has undergone various changes in recent decades. In the mid-90s, telephony began to be widely used through Internet protocols and TCP/IP.

IP telephony works by converting calls, faxes, and other information into digital signals that travel over IP networks. Two synonymous terms are identified: VoIP (Voice over Internet Protocol) and ToIP (Telephony over Internet Protocol). VoIP refers to communication between two terminals using IP. ToIP encompasses telephone services and their data packet infrastructure, with the purpose of ensuring service quality.

The quality of communication is determined by various parameters, including codec selection, packet loss management, delay, jitter, and even network design itself. Therefore, the criteria for quality of service (QoS) will depend on the combination of these parameters and the subjective perception of users. Each customer will have specific demands based on their needs, and the service provider must adapt their offering to closely match the assured QoS values.

In order to compare different mechanisms, understand how parameters affect communication, and obtain measurements, a deployment will be conducted to simulate a real IP telephony scenario. This will allow testing how service quality is affected under different circumstances.

Índice

Lista de Figuras

Lista de Tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

En todo tipo de corporaciones la comunicación es parte del proceso, y un pilar básico del éxito. Esta puede ser interna, entre los trabajadores que componen la empresa, como externa, proveedores y clientes. Las relaciones se basan en la comunicación, existiendo en la actualidad diversos canales. Entre estos está la telefonía, la comunicación por voz en entornos de telefonía fija.

La infraestructura de telefonía debe estar correctamente planteada, teniendo en cuenta las necesidades actuales y futuras. Debe ser lo más homogénea posible, flexible y con posibilidad de realizar escalabilidad. Para cubrir estas necesidades en la actualidad se plantean sistemas de comunicación de telefonía basados en VoIP (*Voice over Internet Protocol*). Implementar estos sistemas permiten a las corporaciones avanzar y mejorar sus comunicaciones. Además, fomenta el proceso de digitalización.

El avance en la tecnología ha provocado que durante las últimas décadas sea más habitual la implementación de estos sistemas VoIP. La sustitución de la red de cobre por la de fibra óptica permite aprovechar las ventajas que esta ofrece. La voz se digitaliza y empaqueta para que viaje mediante la red de datos, junto a ella se añaden diversos servicios de telefonía, tales como llamadas en conferencia, retrollamada, bloqueo de spam, estructuras complejas como las de un *Call Center*, etc. Entre estos, se produce una colección de datos valiosos para poder interpretar la calidad del servicio.

En la actualidad dada la convivencia de estos sistemas VoIP con el resto de las comunicaciones que viajan por la red es necesario controlar la calidad del servicio. Para resolver los posibles inconvenientes se implementa un control de la calidad de servicio. QoS (*Quality of Service*) es el acrónimo que hace referencia a los mecanismos utilizados para priorizar los paquetes de datos que viajan por la red. En cuanto a la ToIP (*Telephony over Internet Protocol*) estos mecanismos de calidad del servicio son muy importantes para poder garantizar una experiencia de usuario correcta. Mediante la configuración de la red, routing del tráfico IP, se clasifica el tráfico y se dan diferentes prioridades para poder gestionar el ancho de banda.

1.2. Objetivos del Trabajo

El objetivo fundamental de este trabajo es analizar la QoS en un sistema ToIP, estudiar los mecanismos que se implementan con el objetivo de cumplir los requisitos para garantizar la calidad del servicio. Para ello, se analizarán diversas publicaciones de fabricantes, recomendaciones y estándares, escritos de revistas y artículos científicos publicados.

Además, se pretende implementar un sistema de comunicación de una empresa, asemejándose a lo más real posible. Se realizarán pruebas del sistema forzando diferentes estados de la red para poder hallar diferencias y concluir con un análisis de los parámetros de QoS asociados a estas pruebas.

Por tanto, los objetivos serán los siguientes:

- Análisis de un sistema ToIP, diferencias entre VoIP y ToIP, e impactos de QoS en estos sistemas.
- Estudio de TCP/IP, cómo se adaptado a los cambios para poder garantizar una QoS.
- Estudio de los mecanismos QoS en la red.
- Implementación de un entorno de simulación de un sistema de comunicaciones VoIP. Aplicación de los mecanismos para garantizar QoS. Pruebas con diferentes configuraciones en la red para obtener diversos resultados.
- Análisis de los resultados obtenidos.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

En cuanto a los objetivos relacionados con la sostenibilidad, se considera que el proyecto tiene un impacto considerablemente positivo, pues la conmutación de circuitos implicaba mayor cantidad de cableado, sistemas y coste. El consumo energético en un sistema de comunicación por IP es alto, mantener una temperatura óptima de las máquinas implicadas es esencial. Sin embargo, es mucho más efectivo que años atrás con los sistemas analógicos, donde el mantenimiento tiene un alto coste y habitualmente el consumo de energía es mucho mayor. Por ello, los sistemas VoIP proponen una alternativa más asequible y limpia, podrían encuadrarse el proyecto con la ODS 7 “*Affordable and clean energy*”.

Otra ODS con la que este proyecto se alinea es la 9 “*Industry, innovation and infraestructure*” pues mediante el uso de IP y no de circuitos conmutados se obtiene mayor flexibilidad, mayores capacidades de servicio, mejor integración con otros sistemas de comunicación y mayor escalabilidad. Se adapta a la actual

oferta de últimas tecnologías de red, la infraestructura es más económica pues se basa en la red de internet y no en las líneas telefónicas. Corporaciones de tamaño más reducido pueden obtener herramientas que tienen la misma calidad que las que usan las altas corporaciones, dado su menor costo, permitiendo el desarrollo de entornos más sostenibles e inclusivos. Permite llegar a zonas con menos recursos, donde se carece de telefonía tradicional. Entre otros aspectos positivos.

El uso de la VoIP está pensado para que sea ético y legítimo. Las oportunidades que aporta son de escala mundial, usado por la gran mayoría de empresas y entidades al tratarse de un sistema más económico que los tradicionales de telefonía. Sin embargo, como cualquier tecnología depende de cómo se use, dándose posibles casos de SPAM y *vishing*. Por ello, dada las posibilidades de uso positivo que puede aportar se considera un gran alineamiento con las ODS de comportamiento ético y responsabilidad social.

Respecto a la diversidad y los derechos humanos, el uso de sistemas de este tipo puede tener un impacto positivo. El hecho de que fomente el trabajo en remoto genera variedad de oportunidades a personas que puedan tener grandes barreras de entrada, como por el género, la orientación sexual o la raza. La educación, el emprendimiento y en general la comunicación en equipo son más accesibles usando esta tecnología.

1.4. Enfoque y método seguido

Los primeros pasos del trabajo irán orientados en obtener documentación relacionada con el tema principal, la VoIP, ToIP y QoS. Se analizará dicha documentación, descartando las que no tengan la suficiente calidad y claridad en los contenidos. En paralelo a la selección de los contenidos válidos se hará una revisión de la tecnología actual en estos sistemas. Se definirán los objetivos, trazará una planificación del trabajo y se definirá el estado del arte del proyecto. Se localizarán los parámetros clave de QoS, los mecanismos en redes TCP/IP aplicables, se detallarán los protocolos VoIP y ToIP con especial atención al impacto de los mecanismos que impactan en QoS.

Una vez consolidada la base teórica, se realizará una implementación de un entorno de pruebas. En él se comprobará la afectación de las diferentes configuraciones posibles y cómo estas afectan en las métricas de QoS. Se analizarán los resultados comparando los diferentes casos para ver la correlación con las propuestas de buenas prácticas que buscan asegurar la calidad del servicio.

De esta forma se desarrolla un proyecto fundamentado en la teoría y con demostración práctica de los impactos posibles en la calidad del servicio en sistemas de comunicación de telefonía fija mediante VoIP.

1.5. Planificación del trabajo

- PEC1: La primera entrega implica la definición del tema, la estructuración de la memoria y la planificación de los objetivos. En este caso el proyecto se orienta al análisis de la QoS en cuanto la telefonía fija sobre IP. Se determina el alcance del trabajo, se estructura la memoria con una estrategia y enfoque adecuados para alcanzar los objetivos deseados. Por tanto, se realiza la planificación necesaria para llevar a cabo el trabajo mediante un diagrama de Gantt.
- PEC2: En esta etapa, se establece la conexión entre el tema elegido y la documentación seleccionada donde se definen los conceptos relacionados, y se elabora el estado del arte del proyecto. Para ello se hace una introducción con los comienzos de la telefonía fija, el impacto de internet y TCP/IP, la adaptación de estos protocolos para que se pueda garantizar de alguna forma la calidad de las llamadas. Esta fase implica recopilar información sobre la situación actual del área de investigación específica y realizar una búsqueda bibliográfica exhaustiva de los recursos relacionados con el proyecto en cuestión, se ha optado por incluir no solo información de revistas, libros y webs, sino también contenido de los principales fabricantes de soluciones VoIP.
- PEC3: Análisis de configuraciones de impacto en QoS y diseño del entorno de pruebas. Implementación del entorno de pruebas. Creación de una estructura ToIP en la que se permita realizar cambios sobre el caudal de la red para comprobar los diferentes efectos sobre la calidad del servicio. Obtención de resultados de dichos experimentos. Conclusiones y relación entre los resultados obtenidos y las recomendaciones para asegurar QoS.
- PEC4: Puesta en común de los puntos desarrollados previamente, producción de la memoria final. Unificar el trabajo realizado documentando correctamente cada explicación dada en el transcurso del proyecto.
- PEC5: Defensa del Trabajo de Fin de Máster. Realización de una presentación en formato diapositivas, junto a una grabación donde se exponga el trabajo. Por último, defensa ante el tribunal.

	Nombre	Inicio	Terminado
1	Selección tema del proyecto	20/02/23 8:00	28/02/23 17:00
2	PEC 1	1/03/23 8:00	12/03/23 17:00
3	PEC 2	13/03/23 8:00	26/03/23 17:00
4	**PEC 3**	**27/03/23 ...**	**19/05/23 17:00**
5	Implementación entorno de	27/03/23 7:00	20/04/23 17:00
6	Pruebas y obtención de res	21/04/23 7:00	11/05/23 17:00
7	Análisis de resultados	12/05/23 7:00	19/05/23 17:00
8	PEC 4	20/05/23 7:00	12/06/23 17:00
9	**PEC 5**	**13/06/23 ...**	**22/06/23 17:00**
10	Presentación	13/06/23 7:00	16/06/23 17:00
11	Grabación	17/06/23 7:00	18/06/23 7:00
12	Defensa ante tribunal	19/06/23 7:00	22/06/23 17:00

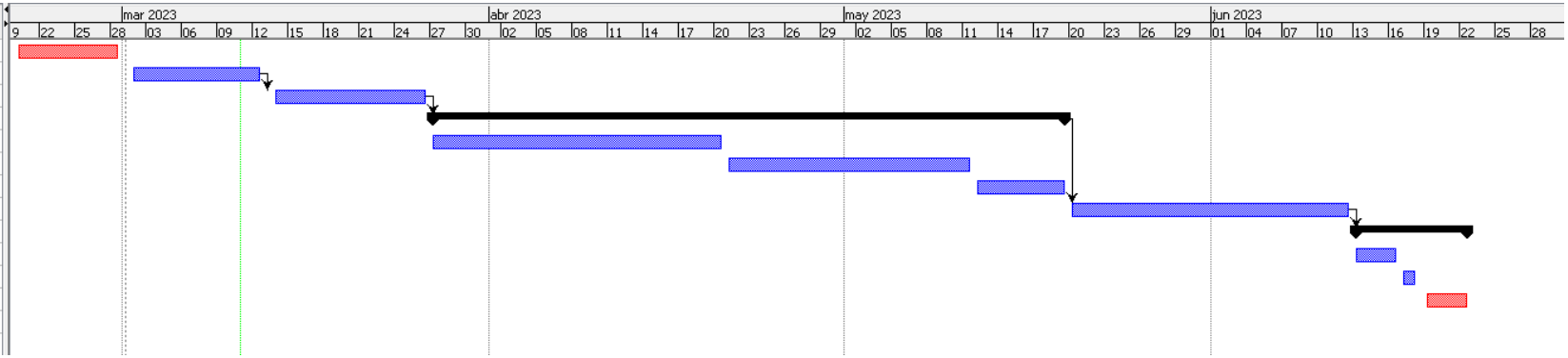


Ilustración 1. Diagrama de Gantt sobre la planificación del trabajo

1.6. Breve sumario de productos obtenidos

Con el desarrollo de este proyecto se pretende dejar un sumario del concepto QoS aplicado a la ToIP. Un análisis a las recomendaciones que se realizan al respecto de la materia, junto a unas pruebas en una maqueta de un sistema de telefonía fija. En esta maqueta se harán diferentes pruebas según las recomendaciones para ver en qué ocasiones es conveniente usar unas u otras.
De esta forma los contenidos aquí presentes pueden orientar a quien esté interesado en controlar la calidad de servicio de un sistema de telefonía fija.

Este estudio se centra en el análisis detallado de la calidad de servicio en sistemas de telefonía sobre IP, considerando diferentes entornos de red. Se evalúan las capacidades de QoS en una red de área local, en una red MPLS y se discute la posibilidad de implementar QoS en Internet, que por su naturaleza "best effort" plantea desafíos adicionales.

Se implementa un entorno de pruebas real, destacando la configuración íntegra de un switch conectado a un entorno de maquetas donde hay implementada una centralita telefónica. En ella se registran diversos terminales con los que se han hecho pruebas para demostrar los conceptos más importantes en este tipo de configuraciones y conseguir una gestión eficiente del tráfico de voz y priorización de paquetes en la red.

Los resultados obtenidos demuestran la importancia de implementar mecanismos de QoS adecuados para garantizar un rendimiento óptimo de los servicios de telefonía sobre IP en cada entorno específico. Una guía detallada con conceptos básicos y avanzados de este campo. De esta forma los contenidos aquí presentes pueden orientar a quien esté interesado en controlar la calidad de servicio de un sistema de telefonía fija.

1.7. Breve descripción de otros capítulos de la memoria

En primer lugar, se realizará una introducción a la tecnología y los aspectos teóricos mediante el desarrollo del estado del arte. Con ello se pretende guiar al lector por los inicios de los sistemas de telefonía hasta la actualidad, asociando este desarrollo al impacto en la calidad del servicio. En esta introducción se plantean las diferencias entre ToIP y VoIP indicando los elementos que la componen. Una idea inicial de QoS y algunos aspectos sobre los protocolos y mecanismos implicados en los sistemas de telefonía IP.

Seguido a esta introducción se desarrollan bajo el título de “Resultados” los conceptos clave del campo de estudio. Primero se define cómo se mide la calidad de servicio, los parámetros objetivos y subjetivos para enmarcar cómo de buena es la comunicación. Los parámetros que afectan a esta calidad como son el *jitter,* el retardo y la pérdida de paquetes. El concepto de MOS y la calidad de experiencia del usuario. El segundo apartado dentro de este capítulo

principal, se explican los mecanismos que existen para realizar un marcado y clasificación de los paquetes en función de la prioridad que estos deben tener en caso de ser tráfico en tiempo real (como la voz). Seguidamente vienen 3 capítulos donde según el tipo de red se relacionado y se dan posibles soluciones para clasificar y tratar el tráfico de manera diferente según las etiquetas que este lleve.

Y para finalizar y demostrar gran parte de los conceptos tratados, se implementa en un entorno real (mediante terminales físicos) diferentes casos y analizan los datos recopilados. Se han incluido en el anexo, para no empeorar la lectura, cierta información relevante.

Las conclusiones obtenidas mencionan la importancia de implementar QoS en los sistemas de tiempo real, concretamente en el caso de la VoIP.

2. Estado del arte

2.1 Introducción histórica

Los sistemas de comunicación de telefonía fija alcanzaron su pleno desarrollo durante finales del siglo XX. Las redes de telefonía pasaron de ser particulares a municipales para comenzar a crecer de manera exponencial, tanto en expansión como en complejidad. [1]

La conectividad en estos despliegues se soportaba principalmente sobre líneas metálicas de cables de cobre. Para agregar nuevas líneas se realizaba mediante un par de hilos de cobre que conectaban al cliente con la central telefónica, conocido como bucle de abonado. Por lo que el servicio de voz (línea fija) se basaba en RTC (Red Telefónica Conmutada) o RDSI (Red Digital de Servicios integrados). Las compañías telefónicas habían realizado una gran inversión para desplegar este tipo de red y proveer el servicio de voz.

En las redes de telefonía tradicional la comunicación se establece a través de un conjunto de nodos interconectados entre sí, donde la central pública es la encargada de establecer la conexión entre los abonados. En los primeros años de la telefonía fija esta conmutación era manual, el llamante establecía la llamada con una operadora de la central pública y manualmente un operario conectaba con el otro extremo. Dada la limitación manual en zonas donde había un alto número de llamadas, se desarrolló la conmutación electromecánica, donde las centrales tenían la capacidad de establecer una conexión directa entre dos dispositivos de comunicación a través de un camino físico dedicado.

Para que la central supiera a dónde se quería llamar era necesario indicarlo de alguna manera, este proceso se conoce como señalización. La ITU-T se encargó de recomendar los sistemas de señalización con el objetivo de ser usados en las comunicaciones internacionales. En la señalización en redes de conmutación analógica se identifican dos grupos [2]:

- Señalización usuario a red (abonado): Cómo el usuario final se comunica con la PSTN. Se realiza mediante el uso de DTMF (*Dual Tone Multi-Frequency*). Donde cada tecla del dial del teléfono es la suma de dos tonos. Estos tonos se decodifican en los conmutadores para identificar el número marcado y encaminarlo al destino.
- Señalización interna de la red (troncal): Cómo se comunican los conmutadores internos de la red. En este caso se usan técnicas de multi frecuencia.

Con el avance de la tecnología y el desarrollo de la digitalización de las comunicaciones la conmutación de circuitos analógica avanza a una conmutación digital. Este cambio se ve impulsado gracias a la digitalización de la voz, donde la señal de voz analógica se muestrea, cuantifica y codifica para obtener un resultado de unos y ceros. Todas las

técnicas de muestreo utilizan el teorema de Nyquist, el cual establece que, si se muestrea a dos veces la frecuencia más alta en una onda acústica, se logra una transmisión de voz de buena calidad. La modulación más utilizada en telefonía es la PCM (*Pulse Code Modulation*), el proceso es el siguiente:

- Las formas de onda analógicas pasan a través de un filtro de frecuencia de voz para eliminar todo lo que sea mayor a 4000 Hz. Ya que la gran mayoría de información en una señal de voz se concentra entre los 300 Hz y 3400 Hz, conservando un margen de salvaguarda.
- Utilizando el teorema de Nyquist, es necesario muestrear a 8000 muestras por segundo para lograr una transmisión de voz de buena calidad.
- Después de que se muestrea la forma de onda, se convierte en una forma digital discreta. Esta muestra se representa por un código que indica la amplitud de la forma de onda en el instante en que se tomó la muestra. La forma de PCM de telefonía utiliza ocho bits para el código y un método de compresión logarítmica que asigna más bits a las señales de menor amplitud.

Si se multiplican las 8000 muestras por segundo por los 8 bit se obtienen los 64000 bits (64kbps) por segundo necesarios para el transporte de los paquetes de voz en telefonía.

La Red Digital de Servicios Integrados (RDSI) es una red que facilita conexiones digitales extremo a extremo entre los terminales conectados a ella (teléfono, fax, datos, etc.) para proporcionar una amplia gama de servicios, tanto de voz como de datos, a la que los usuarios acceden a través de un conjunto de interfaces normalizadas definidas por el ITU-T. En los primeros años, los medios de transmisión y conmutación son digitales excepto el bucle de abonado. Incorpora un nuevo concepto de conmutación, la conmutación de paquetes. [3]

La conmutación de paquetes es una técnica de transmisión de datos en redes de computadoras que divide los datos en paquetes y los envía individualmente a través de la red hacia su destino. Cada paquete incluye información de control, como la dirección de origen y destino, y el tamaño del paquete. Los terminales pueden dividir la información a enviar en varios paquetes que se encaminan de manera independientemente. La transmisión no se apodera del canal por largos períodos de tiempo, sino que divide lo que se desea enviar en porciones. Inicialmente estaba pensada exclusivamente el transporte de datos, pero se acabó adaptando su uso para la voz.

Ilustración 2. Conmutación de paquetes vs Conmutación de circuitos [4]

En la conmutación de paquetes el estándar X.25 fue el primero que se definió por la ITU-T procurando una norma internacional para protocolos de acceso a redes de comunicación. Constituye la primera red de conmutación de paquetes. A los años, y tras diversas modificaciones de X.25, surge una técnica simplificada de conmutación de paquetes para el transporte de información de datos. Frame Relay, simplifica el proceso ya que elimina ciertas funciones para dotar de mayor velocidad, representa la evolución de la red X.25. En 1988 se propuso la recomendación I.121 para utilizar ATM (*Asynchronous Transfer Mode*), como tecnología base para liderar un proyecto donde una gran red albergue a otras redes en el transporte de paquetes de datos. En él se definen un conjunto total de protocolos de comunicación, permitiendo aumentar más la velocidad de conmutación (entre otras ventajas) [5].

Con la intención de intercambiar información en texto, mediante un proyecto académico y de investigación militar estadounidense nace Internet. En 1995 se eliminan las restricciones y comienza su uso comercial, lo cual supuso una revolución mundial en las telecomunicaciones.

Con el avance de la tecnología, mayor potencia de cálculo en los procesadores, y la continua demanda de mayor ancho de banda, el despliegue de estas líneas se sustituye de RTB (módems a 56 Kbps) por RDSI (módems a 64 o 128 Kbps) y posteriormente xDSL. Permitiendo un mayor ancho de banda, sin embargo, esta capacidad se quedó pequeña. La red no era capaz de soportar tal cantidad de exigencias, la tendencia estaba clara, los sistemas de comunicación usarían internet. Se adoptan por tanto los estándares de este [6].

El conjunto de protocolos TCP/IP permite que computadoras de todos los tamaños, de muchos proveedores de computadoras diferentes, que ejecutan sistemas operativos totalmente diferentes, se comuniquen entre sí. Los protocolos de red normalmente se desarrollan en capas y cada una es responsable de una faceta diferente de las comunicaciones. Un conjunto de protocolos, como TCP/IP, es la combinación de diferentes protocolos en varias capas [7]. Se compone de 4:

- Capa de enlace o acceso al medio. Maneja el hardware de la interfaz de red física.

- Capa de red o de internet. es el protocolo de la capa de red que se utiliza para enrutar los paquetes de datos a través de una red. Cada dispositivo en una red tiene una dirección IP única que se utiliza para enrutar los paquetes de datos.
- Capa de transporte. proporciona un flujo de datos entre dos hosts, para la capa de aplicación anterior. En el conjunto de protocolos TCP/IP hay dos protocolos de transporte muy diferentes: TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagramas de usuario).
- Capa de aplicación. Maneja los detalles de la aplicación en particular.

El uso de los protocolos TCP/IP incrementaba exponencialmente, a principios de los 2000 surgió el concepto *All-IP*, porque las operadoras de telefonía fija se dieron cuenta que basando todos los servicios en IP conseguirían menores costes de operación y mantenimiento en la red troncal. Mediante la estandarización del conjunto de protocolos se fue estableciendo un mayor abanico de posibilidades sobre IP.

El uso de la red de datos era mayor que el de la red de telefonía, la necesidad de la adaptación de la red era un hecho a principios del siglo XXI. Con la llegada de la fibra óptica se termina de dar prácticamente por terminada la era de la Red Telefónica Pública Conmutada. Un ejemplo de ello es el reciente cierre de las últimas centrales de cobre por parte de Telefónica en España [8].

Por lo tanto, la comunicación por telefonía fija se transforma. Pasa de transportar la voz por un canal (establecido únicamente durante la llamada), con una tasa de cambio de información garantizada, a transportar la voz digitalizada y probablemente comprimida dentro de datagramas IP.

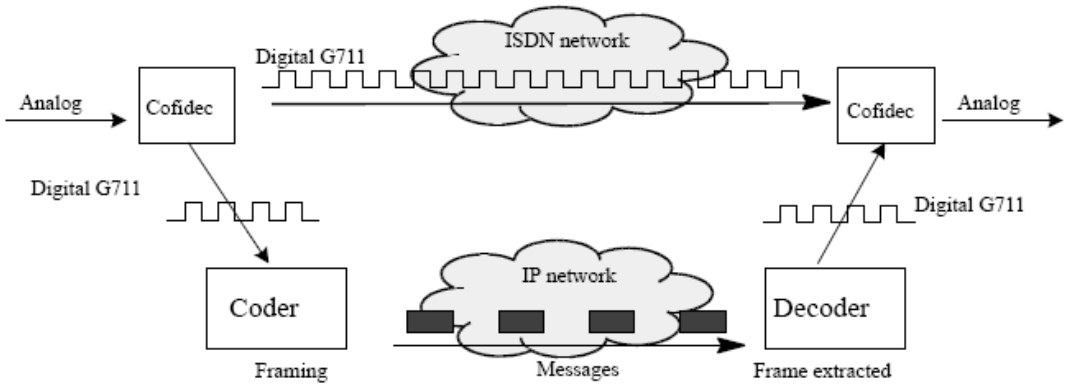


Ilustración 3. 8AL91007USAJ - Ed. 01 - March 2019 - IP-PCX Networks pág 30

2.2 ToIP y VoIP

Se define la VoIP como el concepto más amplio de telefonía en internet, es la posibilidad de transportar conversaciones telefónicas en paquetes IP. Por tanto, no se refiere a ningún mecanismo en concreto de los que existen. Entre los protocolos para implementar VoIP se encuentran: SIP, H.323, RTP, SDP, etc. Es la forma más común de referirse a este tipo de

comunicaciones. Sin embargo, el concepto de la ToIP hace referencia a los servicios posibles de la voz de telefonía fija que viaja a través de IP, recoge las técnicas que permiten la transmisión de teléfono a teléfono. Por ello se relaciona con el uso de una centralita telefónica.

2.2.1 PBX

PBX o PABX hace referencia al término inglés *Private Branch Exchange* que en castellano sería Ramal Privado de Conmutación Automática, o más bien Central Privada Automática. Permite usar una o varias líneas telefónicas con un grupo de usuarios, el administrador del sistema puede controlar como compartir las líneas exteriores que comunican con la PBX. Estas líneas reciben el nombre de troncales. En los sistemas de conmutación de circuitos esta PBX daba los servicios de telefonía privados al administrador (corporación, edificio, etc.). Con el avance de la tecnología en las PBX algunos fabricantes implementan mejoras mediante el uso de tarjetas hardware que se conectaban a la PBX. Entre estas mejoras se incluía la opción de manejar terminales IP.

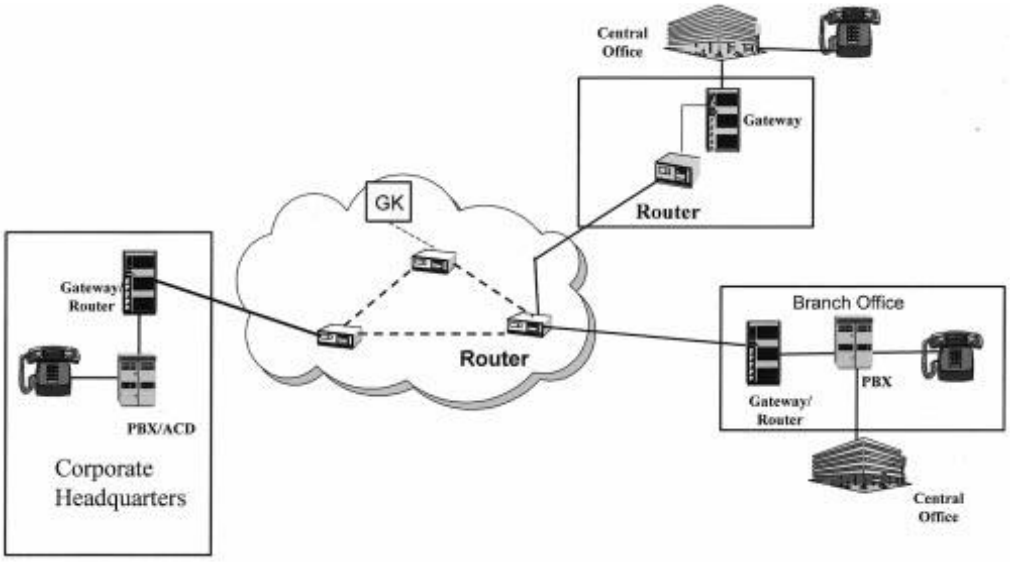


Ilustración 4. Voice Over Internet Protocol (VoIP) [9]

Muchas de estas líneas telefónicas se han ido sustituyendo por encaminamientos IP. La PBX puede convivir con los dos sistemas, para comunicarse entre ellos surge el concepto de *trunking*, donde la PBX encamina las llamadas por un enlace u otro en función si se dirige a teléfonos IP o analógicos. Las PBX digitales admiten líneas troncales digitales y analógicas. Tiene un directorio con los terminales conectados a ella y su dirección IP, en caso de que la llamada sea externa sobre IP se encamina mediante un *gateway* VoIP [10].

Las centralitas actuales son directamente PBX IP, pudiendo estas estar alojadas en la nube del propio proveedor de servicios sin necesidad de adquirir el hardware te la PBX como tal. Implementan *Trunk SIP* (troncales SIP) y en caso de ser necesario mediante conversores tipo ATA (adaptador para teléfonos analógicos) es posible conectar teléfonos analógicos. Un ATA tiene un conector RJ11 y un RJ45. Por un lado habla con el teléfono analógico y por el otro opera en modo digital con la red de voz IP.

La centralita se encuentra entre los terminales de voz y las líneas de comunicación externas. Es el punto central del sistema, tiene conexión con los terminales de la red corporativa, el router de la entidad y el *gateway*.

2.2.2 Gateway

Un Media Gateway en un sistema de VoIP es un dispositivo que se utiliza para convertir los datos de voz analógicos en paquetes de datos digitales que se pueden transmitir a través de una red IP. En otras palabras, el Media Gateway es un dispositivo que interconecta una red telefónica tradicional (PSTN) con una red de voz sobre IP (VoIP). [9]

Además de la conversión de la señal de voz, el Media Gateway también puede proporcionar funciones adicionales como la gestión de llamadas, el enrutamiento de llamadas e incluso la gestión de calidad de servicio (QoS) para garantizar una buena calidad de voz durante las llamadas.

2.2.3 Protocolos de señalización

Los sistemas están definidos mediante protocolos de señalización estándares, desde los circuitos conmutados se emplea un intercambio de información para realizar un control de las llamadas y los equipos involucrados, en la conmutación de paquetes han existido diversos formatos, pero hoy el más común es el uso del protocolo SIP.

H.323 fue el primer protocolo abierto de telefonía IP. Surgió como una evolución de otros protocolos de videoconferencia y telecomunicaciones. Se definen tres componentes principales: *Terminal* (dispositivo llamante o llamado), el *Gatekeeper* (controlador del ancho de banda, permisos y traducción de direcciones) y el *Gateway*. [11]

Como complemento a ambos, SIP y H.323, se desarrolló el protocolo MEGACO. Es un protocolo usado para controlar y gestionar *media gateways*. utiliza un modelo de control centralizado, en el que un controlador central MEGACO gestiona múltiples *gateways*.

El protocolo SIP está recogido en la RFC 3261 donde se define cómo establecer, modificar o finalizar una sesión entre dos extremos o más. Se utilizan los protocolos UDP, RTP y RTCP para el transporte. El flujo de mensajes básico en SIP sería el siguiente:

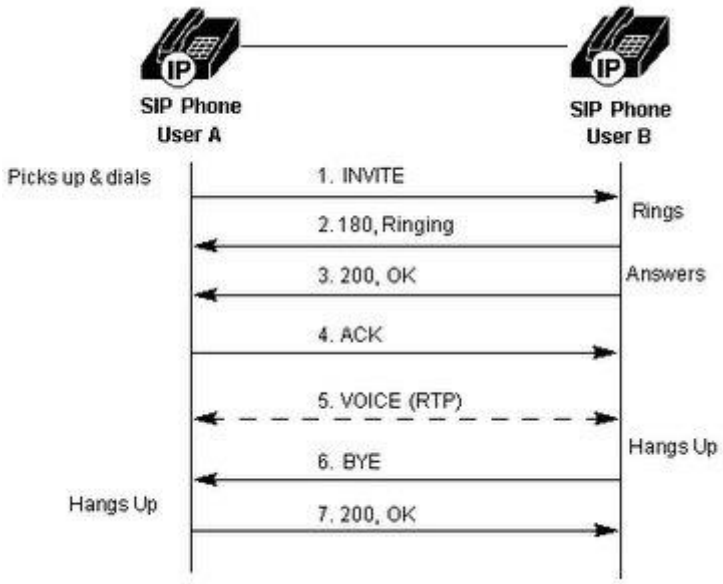


Ilustración 5. Flujo básico SIP [12]

2.2.4 Códecs

Los códecs son una parte integral en el desarrollo de VoIP, ya que son responsables de la conversión de la señal de voz en audio a datos digitales codificados. Un códec es un software capaz de codificar una forma de onda (analógica) generada en el lado del remitente en una cadena de bits que, al decodificarse en el extremo remoto, será lo más similar posible a la forma de onda original. La selección del códec afecta al ancho de banda consumido, a la tasa de bits, al tamaño de la trama, y sobre todo a la calidad de la voz, como se detallará más adelante todo ello conlleva una variación de parámetros objetivos que afectan la concepción de la calidad. En la siguiente tabla se muestran los códecs más habituales:

Tabla 1. Comparativa códecs [9]

Codec	**Algorithm**	***Frame Size/ Lookahead***	**Usual Rate**	**Comments**
G.711	PCM	0.125 ms/0	64 Kb/s	Universal use
G.722		0.125 ms/1.5 ms	48, 56 or 64 Kb/s	Wideband coder
G.726	ADPCM	0.125 ms/0	32 Kb/s	High quality, low complexity
G.728	LD-CELP	0.625 ms/0	16 Kb/s	High quality in tandem; Recommended for cable
G.729(A)	CS-ACELP	10 ms/5 ms	8 Kb/s	Widespread use
G.729e	Hybrid CELP	10 ms/5 ms	11.8 Kb/s	High quality/complexity; Recommended for cable
G.723.1(6.3)	MPC-MLQ	30 ms/7.5 ms	6.3 Kb/s	Video conferencing origin
G.723.1(5.3)	ACELP	30 ms/7.5 ms	5.3 Kb/s	Video conferencing origin
IS-127	RCELP	20 ms/5ms	Var. 4.2 Kb/s avg.	
AMR	ACELP	20 ms	Var. 4.75-12.2 Kb	Compatible w. No. Amer. & Japanese digital cellular, WCDMA (not CDMA2000); Nokia IPR

2.3 QoS

Para realizar una migración satisfactoria es necesario que las redes IP cumplan con las mismas expectativas que había en la red telefónica conmutada. En esta red había un canal dedicado con un ancho de banda exclusivo para esa comunicación.

El objetivo es intentar conseguir al menos la misma calidad que en las redes conmutadas, para ello se debe tener en cuenta cada sistema implicado en la comunicación: el hardware y software de los teléfonos IP, ciclos de CPU, memoria, y los recursos de la red. Es importante asegurar que haya suficiente ancho de banda disponible para ambos flujos de tráfico, independientemente del estado de las demás conexiones en la red (incluso si la conexión a Internet está siendo ampliamente utilizada). Son muchos los factores que determinan la calidad de la voz, desde la selección del códec, el control del eco, la pérdida de paquetes, el retardo, el *jitter*, y el diseño de la propia red. La complejidad y la interacción dinámica entre los procesos y las condiciones del sistema bajo el que se ejecutan estos procesos hacen que la detección y el diagnóstico de los problemas en el entorno IP sean poco triviales [13].

El retardo que puede tener un paquete desde el emisor hasta el receptor puede ser un problema, ya que si es muy elevado la percepción de los participantes sería como estar en dos conversaciones a la vez. Para compensar la variación de este retardo (jitter) se almacena la información en un búfer y así reducir el efecto de dicho *jitter*. Aunque si el tamaño del retardo excede al del búfer se producirán pérdidas de paquetes nuevamente.

Las pérdidas de paquetes producen cortes y saltos en la llamada, algunos algoritmos pueden codificar de tal manera que reducen estas pérdidas y las hacen imperceptibles. Pero no es posible disimular grandes pérdidas en cortos periodos de tiempo.

Existen diferentes tipos de códecs que permiten digitalizar la voz. Para medir la calidad que estos aportan se utiliza una media subjetiva de un gran número de oyentes. Este parámetro se denomina MOS, *Mean Opinion Score.* En los tests se varían diferentes características de la comunicación como el efecto del ruido ambiente, el efecto de la degradación del canal (pérdida de paquetes) y los efectos producidos por la interconexión con otras redes de transporte territoriales e inalámbricas. Se debe tener en cuenta que la codificación debe producirse lo más cercana al orador y la descodificación lo más próxima al oyente. La concatenación de codificadores degrada la calidad de la comunicación.

Para un buen funcionamiento en una red IP se debe comenzar por realizar una provisión eficiente antes de aplicar mecanismos complejos de QoS. Si los enlaces no se encuentran ocupados a más de un 30%, no es necesario el uso de estos. Sin embargo, esto no siempre es posible en zonas donde el ancho de banda es muy ajustado.

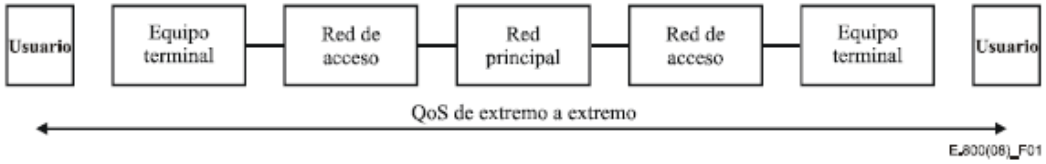


Ilustración 6. Esquema de contribuciones a la QoS de extremo a extremo

Por tanto, la QoS de extremo a extremo depende de los sistemas implicados. Por definición del concepto es una medida “del grado de satisfacción de un usuario de un servicio”. Lo cual implica la calidad del funcionamiento de la red y la calidad del funcionamiento independiente de la red.

Este proyecto se centra en un análisis de la red de acceso mediante una implementación de un sistema ToIP en una red LAN. Se da por hecho que los proveedores de red cumplen con unos requisitos de QoS en sus servicios y que no son de la índole de los usuarios finales. Por ello para demostrar los efectos sobre la calidad del servicio las pruebas se centrarán en situaciones que sufre la red interna y no la que ofrece el proveedor.

2.4 Redes TCP/IP

El principal problema durante el desarrollo de las redes era decantarse por cuál usar. Al ir surgiendo estas en paralelo, existían diversos motivos para arriesgarse a invertir en los nuevos sistemas o avanzar en los ya implementados. Con la conmutación de circuitos se opta por una decisión de comunicación que garantiza que la red dispone de recursos, sin embargo, sumamente ineficiente si hablamos de servicios de datos. Los datos se generan a ráfagas y con un canal reservado durante toda la comunicación habría momentos de un tiempo considerable que se desaprovecharía el canal. Por otro lado, la decisión de la conmutación de paquetes, donde la información se divide en paquetes más pequeños que se envían de forma independiente por la red, sin reserva de recursos, generando problemas como retardos, pérdidas y *jitter*.

Finalmente se optó por implementar la conmutación de paquetes como tecnología de transporte por excelencia. Concretamente El protocolo IP junto al TCP. Sin embargo, IP no se pensó para el transporte de información multimedia, ni para transporte de paquetes en tiempo real. Por ello, para complementar el servicio *best effort* que ofrece el protocolo se deben implementar mecanismos que permitan un control de la calidad del servicio.

2.4.1 Protocolos implicados

Las aplicaciones típicas de Internet utilizan TCP/IP, mientras que VoIP utiliza RTP/UDP/IP. Aunque IP es un protocolo de comunicaciones de red sin conexión y *best effort* (mejor esfuerzo), TCP es un protocolo de transporte confiable que utiliza confirmaciones y

retransmisiones para garantizar la recepción de los paquetes. Usados juntos, TCP/IP es una suite de protocolos de comunicaciones de red confiable y orientado a la conexión. [7]

TCP/IP no es adecuado para usar en comunicaciones en tiempo real, como una conversación por voz. Las confirmaciones de paquetes ocasionarían un gran retardo en las llamadas. Para ello se usa UDP junto a RTP, de esta forma se permite el transporte de paquetes en tiempo real. RTP no reserva recursos y no garantiza la calidad del servicio. Como complemento surge el RTCP, un protocolo que se utiliza para la proporcionar información de control de calidad y estadísticas sobre la transmisión.

Si el protocolo RTP es el portador del contenido de voz (y vídeo), el responsable de establecer la sesión es el protocolo SIP. *Session Initiation Protocol* es un protocolo que usa TCP/IP basado en HTTP (transferencia de hipertexto), se encarga de establecer, modificar y finalizar las sesiones. Surgió de la necesidad de que la telefonía fuese un servicio más de internet. Por ello su sintaxis se asemeja a la de protocolos usados en otros servicios, como el correo electrónico. Funciona mediante transacciones, un extremo realiza peticiones (considerado cliente) y el otro las recibe (considerado servidor). Ambos extremos poseen la capacidad de ser cliente y servidor, pues envían y reciben peticiones indistintamente. En este intercambio negocian los parámetros de la comunicación entre los dos extremos, lo que se llama el protocolo de señalización. Otro protocolo de señalización es el H.323, el cual paulatinamente está siendo sustituido por el SIP debido a su simplicidad, escalabilidad, compatibilidad y seguridad mejorada. Aunque sigue siendo compatible con sistemas VoIP, los principales fabricantes, como Cisco [14] dejan de dar soporte en algunos de sus productos, o 3CX que afirma que el protocolo está cayendo en desuso ya que los fabricantes de teléfonos (dispositivos *endpoint*) optan por SIP [15].

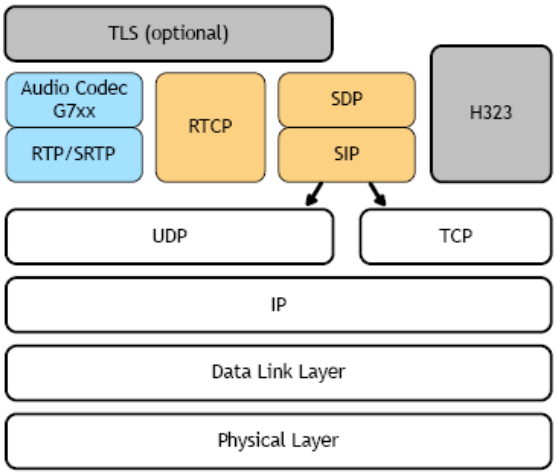


Ilustración 7. SIP modelo OSI

2.4.2 Mecanismos

Ya que las redes IP soportan voz y datos, se han desarrollado mecanismos para dar preferencia a la transmisión de paquetes de voz sobre los paquetes de datos y para

separar ambos flujos. La IETF (*Internet Engineering Task Force*) publicó mediante RFC los modelos para garantizar QoS.

Best Effort, IntServ y *DiffServ* son tres modelos de servicio que se utilizan para gestionar el tráfico de red y garantizar la calidad de servicio en diferentes tipos de aplicaciones de red.

- *Best Effort*: Es un modelo de servicio básico que se utiliza en la mayoría de las redes IP. En este modelo, los paquetes se envían de forma no prioritaria y sin garantía de entrega o retardo. La red hace todo lo posible para enviar los paquetes, pero no garantiza su llegada ni su tiempo de entrega. Por tanto, no es un modelo que podamos considerar si el objetivo es garantizar la calidad de servicio.
- *IntServ*: El modelo de servicios integrados está basado en flujos. Los routers de la red utilizan el protocolo RSVP (*Resource Reservation Protocol*) para reservar recursos de red específicos para una aplicación determinada. Esto garantiza que los paquetes de la aplicación tengan prioridad sobre otros paquetes y se entreguen con una calidad de servicio garantizada. Se implementa en capa 4, la capa de transporte.
  En cada uno de los flujos de datos se reservan recursos y se notifica al origen que se puede garantizar la calidad del servicio solicitada. Los dispositivos de red garantizan y gestionan los recursos de cada flujo. Por tanto, es un modelo determinista, ya que garantiza la QoS si esta es posible. [16]
  Este modelo tiene la desventaja de que los routers deben realizar gran cantidad de gestiones para garantizar los flujos, se requiere de un mayor consumo, lo cual empeora a mayor tamaño de la red. Sin embargo, en redes más pequeñas garantiza la QoS.
- *DiffServ*: A raíz de la desventaja del modelo *IntServ*, para gestionar con mayor agilidad los recursos surge un modelo de servicio que se utiliza para clasificar y priorizar el tráfico de red en diferentes clases de servicio (CoS). En este modelo, los paquetes se clasifican según su tipo y se les asigna un nivel de prioridad. Los routers de la red utilizan esta información de prioridad para gestionar el tráfico y garantizar que los paquetes con prioridad más alta tengan un mejor rendimiento y se entreguen antes que los paquetes con prioridad más baja. El marcado del tipo de tráfico se realiza mediante el campo DSCP que se encuentra en la cabecera de los paquetes IP y se utiliza para definir la clase de servicio a la que pertenece el paquete. El campo DSCP consta de 6 bits en el encabezado de los paquetes IP, lo que permite 64 posibles valores diferentes. Se implementa en la capa 3, la capa de red. Las políticas de servicio de red pueden ser específicas para un dominio QoS completo, parte del dominio o incluso locales a un solo nodo.
  No se realiza una reserva previa, por tanto, no proporciona un QoS determinista, pero sí garantías estadísticas mediante la definición de políticas de tratamiento en los enlaces [17].

Tabla 2. Comparativa Best Effort, IntServ y DiffServ

	Best Effort	**IntServ**	**DiffServ**
Garantías	No	Determinista	Estadística
Unidad de gestión	No	Flujo de datos	Tipo de tráfico
Escalabilidad	Grande	Pequeña	Regular
Reserva de recursos	No	Cada nodo iniciado por app	Cada nodo previamente configurado
Zona	Toda la red	*End-to-end*	Orientado a dominio

Otro mecanismo, en este caso para capa 2, es el que se define dentro del estándar IEEE802.1Q, el IEEE 802.1p. Este se utiliza en la capa de enlace de datos para etiquetar los paquetes de red con un valor de prioridad y, de esta manera, garantizar que los paquetes se entreguen en orden y con la prioridad adecuada en la red. Mediante 3 bits se indica el tipo de tráfico y por tanto la prioridad que requiere.

Tabla 3. 802.1p Tipos de tráfico

Prioridad	**Tipo de tráfico**
0	Mejor esfuerzo *(Best Effort)*
1	Segundo plano
2	Reservado
3	Esfuerzo excelente
4	Carga controlada
5	Vídeo
6	Voz
7	Control de red

3. Resultados

La calidad de servicio engloba a todas las descripciones o medidas del rendimiento del tráfico en una red de computadoras y otras redes de telecomunicación, comprende los requerimientos en una conexión para controlar el tráfico y garantizar el rendimiento de aplicaciones críticas. Asegurar una calidad del servicio es una necesidad para cualquier proveedor o cliente. En concreto para la telefonía IP fija se puede analizar en tramos, ya que como vimos en la Ilustración 6, el recorrido de la voz en una conversación telefónica actualmente atraviesa diferentes equipos y protocolos los cuales pueden afectar a la calidad de esta. Además, en la misma red conviven diferentes tipos de tráficos, a lo que principalmente era una red de datos se le sumó la voz y luego el vídeo. Todos ellos consumen ancho de banda y requieren de un trato diferente en función de las necesidades del cliente.

3.1 Cómo se mide la QoS

Para medir la calidad en una llamada se parte de dos premisas: la sensación de los usuarios de la calidad y las medidas numéricas de la calidad. Donde la primera tendrá una connotación subjetiva pues se basa en una recopilación estadística de las sensaciones de los usuarios durante una llamada, y la segunda se indica con estadísticas obtenidas mediante la monitorización del tráfico, los paquetes que se pierden, el tiempo que tardan en llegar, la fluctuación de ese tiempo, etc.

En la primera premisa se realiza una medida subjetiva. En función de la percepción de cada usuario se debe calificar la llamada con una nota. Este tipo de medida está estandarizada, en concreto, la ITU P.800 define un método de evaluación subjetiva de la calidad de la voz conocido como MOS (*Mean Opinion Score*).

El MOS es una medida subjetiva de la calidad de la voz que se obtiene a través de la evaluación, por parte de los usuarios, de la calidad de las muestras de voz durante una llamada telefónica. El MOS se define en una escala de 1 a 5, donde 1 indica una calidad de voz "muy pobre" y 5 indica una calidad de voz "excelente". La ITU establece los procedimientos para la selección y entrenamiento de los evaluadores de calidad de la voz, así como para la realización de pruebas de evaluación en diferentes escenarios y situaciones.

La QoE (*Quality of Experience*) analiza y cuantifica desde una perspectiva orientada a los usuarios sobre la comunicación, la experiencia que se tiene durante la llamada. El MOS es una métrica usada en QoE para conocer el grado de satisfacción del servicio en estos usuarios. La técnica usada para obtener el MOS se denomina ACR (*Absolute Category Rating*), donde se califica el audio de manera directa en función de la sensación de calidad. Otro método es el DCR (*Degradation Category Rating*), donde se realiza la calificación mediante comparación con un audio de referencia. También entre 1 y 5, siendo 5 que no

hay diferencias entre el audio de referencia y el medido. Los valores DCR son conocidos como DMOS (*Degradation MOS*). Un aspecto interesante, es que a pesar de ser el método utilizado por excelencia el valor obtenido como MOS puede estar sujeto al tipo de experimento realizado. Se ha demostrado que, si se utilizan varias muestras de buena calidad, una de ellas puede ser calificada peor que si esa misma muestra se presenta en un conjunto de muestras que tienen una calidad mala (o peor). Por esto se ha estandarizado también el "Q-Method", en la recomendación ITU-T P.810.

La segunda premisa, el valor de los parámetros medidos durante una llamada, es un valor objetivo. Fundamentalmente son 3 parámetros:

- *Delay* (latencia): Tiempo que tarda un paquete en llegar desde el punto final de envío al punto final de recepción. El exceso de retardo hace la conversación menos natural, llegando en casos extremos a ser incomprensible. La ITU-T establece en G.114 un tiempo de máximo de 150 ms de extremo a extremo en una transmisión unidireccional, hasta 400 ms lo considera aceptable, pero con posibles impactos en la calidad del servicio y mayor de 400 ms inaceptable.
  En la siguiente gráfica extraída de la recomendación se observa la relación entre el parámetro R y la latencia de boca a oído en milisegundos. Hay que destacar que tanto el *Rating R* como el MOS son medidas subjetivas de calidad de voz, utilizan escalas diferentes y tienen en cuenta distintos factores técnicos y enfoques de evaluación.

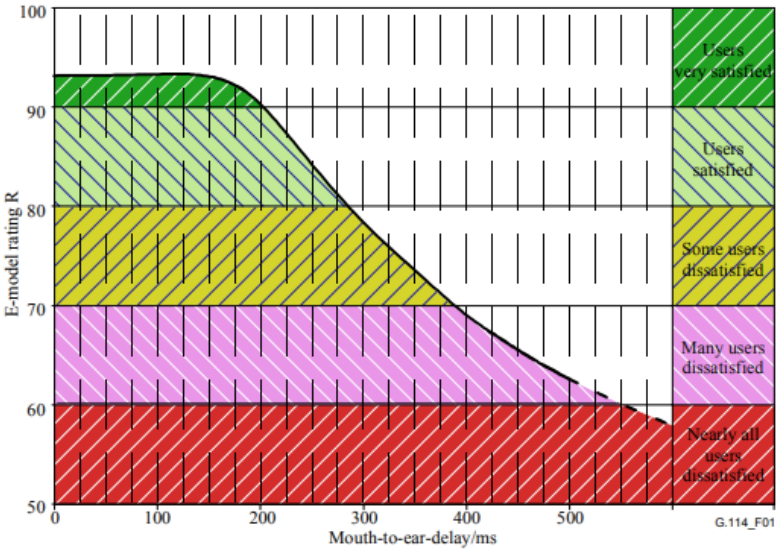


Ilustración 8. Calidad de voz y delay ITU-R G.114 [18]

- *Jitter* (variación de latencia): Variación, o diferencia, en el retardo de extremo a extremo en la recepción de paquetes secuenciales. Cuantifica los efectos de la latencia, en exceso produce una conversación entrecortada. Los valores deben aproximarse al promedio de llegada de paquetes al receptor con una desviación estándar lo más baja posible. Para contrarrestar los efectos se implementan buffers

para crear un flujo normal, estos son efectivos en variaciones menores a 100 ms. En la siguiente figura vemos como el paquete A se envía y no es recibido hasta que ha transcurrido D_1, acto seguido se envía el paquete B que tiene el mismo tiempo de emisión y recepción $D_2 = D_1$, sin embargo, cuando el paquete C se envía se encuentra con retardos en la red lo que supone un incremento del retardo entre la emisión y recepción del paquete respecto a D_1 y D_2.

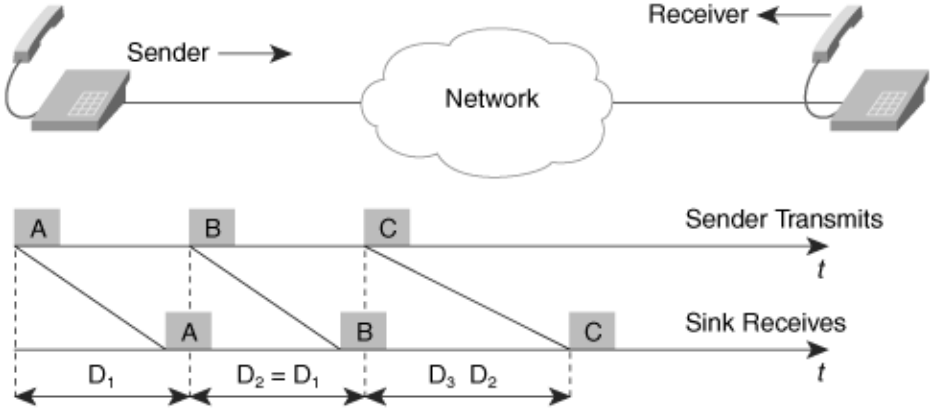


Ilustración 9. Variación del tiempo de recepción de paquetes [2]

- Pérdida de paquetes: Comparativa entre la cantidad de paquetes enviados y la cantidad recibida. Ocurre debido a la congestión de la red, pudiendo darse de manera periódica o abrupta. No debe superar el 10% pues afectaría de forma significativa en la comunicación. En la siguiente figura se observa la llegada de 3 paquetes dentro de los márgenes esperados, sin embargo, el cuarto paquete se ha perdido en alguna parte de la transmisión y se agota el tiempo máximo que el sistema puede esperar (en función del buffer).

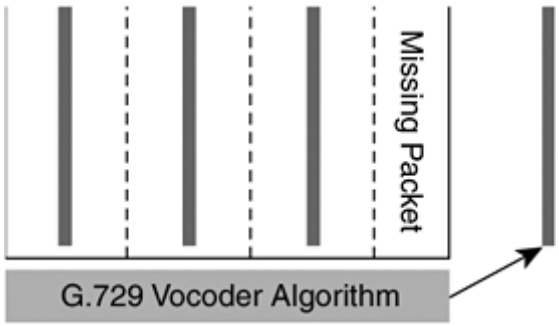


Ilustración 10. Recepción de paquetes y pérdida [2]

Una comunicación de voz IP es sensible a cualquiera de estas características, junto a ellas también existen otros aspectos a considerar como el eco, la congestión en los nodos y posibles errores en la secuencia de los paquetes.

Existe una relación entre el valor del MOS y los valores objetivos mencionados, diversos estudios han obtenido diferentes valores, pero a grandes rasgos un número mayor de descartes en paquetes, un aumento del *jitter*, un aumento del retardo o mayor pérdida de

paquetes significa una disminución del MOS, por tanto, peor calidad subjetiva. En las siguientes tablas se muestran los valores obtenidos en un estudio sobre la variación del MOS en diferentes condiciones de retardo, *jitter* y pérdida de paquetes.

Tabla 4. MOS en función del jitter y los descartes [19]

Impairment	MOS (ITU P.862)	Discards
No impairment	4.368	0
Delay 100 msec, standard deviation 5 msec	4.363	1
Delay 100 msec, standard deviation 10 msec	4.363	3
Delay 100 msec, standard deviation 15 msec	3.607	49
Delay 100 msec, Standard deviation 20 msec	2.961	114
Delay 100 msec, Standard deviation 30 msec	2.446	285
Delay 100 msec, Standard deviation 40 msec	1.928	434
Delay 100 msec, Standard deviation 50 msec	1.644	518
Delay 100 msec, Standard deviation 60 msec	1.501	626
Delay 100 msec, Standard deviation 70 msec	1.384	652
Delay 100 msec, Standard deviation 80 msec	1.287	704
Delay 100 msec, Standard deviation 90 msec	1.225	724
Delay 100 msec, Standard deviation 100 msec	1.212	724

Tabla 5. MOS en función de la pérdida de paquetes [19]

% Packet Lost	MOS-LQ Periodic Lost	MOS-LQ Random Lost
0	4.2	4.2
1	4.1	4.1
2	4.1	4
3	4.1	3.8
4	4	3.9
5	4	3.8
10	3.7	3.3
15	3.4	3.1
20	3.2	2.8
25	2.9	2.6
30	2.7	2.3
35	2.5	1.8

Tabla 6. Relación códecs más habituales y MOS [19]

Codec	Coding Method	Bit rate (kbps)	MOS-ITU
G.711A (no PLC)	PCMA	64	4.40
G.711A PLC	PCMA	64	4.40
G.711U (no PLC)	PCMU	64	4.40
G.711U PLC	PCMU	64	4.40
G.721	ADPCM	32	4.23
G.723.1	MP-MLQ	6.3	3.95
G.723.1	ACELP	5.3	3.78
G.726	ADPCM	16	2.95
G.726	ADPCM	24	3.51
G.726	ADPCM	32	4.23
G.726	ADPCM	40	4.36
G.727	ADPCM	16	2.84
G.727	ADPCM	24	3.83
G.729	LD-CELP	8	3.92
G.729A	CS-ACELP	8	3.7

El propósito fundamental de QoS es administrar los recursos de la red para maximizar la experiencia del usuario final de una sesión, cualquier tipo de sesión. Debido a que no todos los paquetes son iguales, no deben tratarse por igual. Por ejemplo, la VoIP requiere de un *jitter* bajo del orden de 100 ms y un ancho de banda garantizado entre 8Kbps y 64 Kbps (según el tipo de códec utilizado), sin embargo, una transmisión de ficheros basada en FTP no sufre tanto por el *jitter* pero sí por la pérdida de paquetes. En este proyecto nos centramos en la voz en las redes cableadas de ancho de banda fijo, pero es escalable a otros casos como el de acceso inalámbrico WiFi 802.11 donde el rendimiento y el ancho de banda es variable.

3.2 Mecanismos y arquitectura

En un primer intento de estandarizar la QoS la IETF publicó la arquitectura de servicios integrados (IntServ). Fue propuesta en las RFC 1633, 2211 y 2212 con el fin de soportar tráfico en tiempo real, así como tráfico *best effort*. Es relativamente compleja, requiere una reserva explícita de recursos, control de admisión, clasificación de paquetes y programación, y tiene dificultades para escalar a la red troncal. El procedimiento de la reserva de recursos es el siguiente:

1. Especificación del flujo: Se debe caracterizar la cantidad de tráfico en el flujo y las necesidades de QoS. Para ello se utilizan los parámetros TSpec (*Traffic Specification*) que describe el tráfico y RSpec (*Service Request specification*) que indica los requitiso de QoS y la reserva del ancho de banda que impone a la red.
2. Señalización: El protocolo encargado en Internet es el RSVP.
3. Admisión de la llamada: Al recibir la petición, en función de los parámetros de especificación se decide si admitir o denegar el nuevo flujo.

Se definen dos clases de servicios:

- Servicios garantizados: Están diseñados para aplicaciones en tiempo real que necesitan un retardo máximo garantizado en la transmisión entre los extremos y no aceptan la pérdida de paquetes. Estos servicios proporcionan una tasa de transmisión de datos, un límite de retardo en la transmisión y garantizan que los paquetes no se perderán en las colas de los encaminadores.
- Servicios de carga controlada: Ofrece a la sesión una calidad de servicio muy parecida a la QoS que recibiría el mismo flujo de datos con un servicio de mejor esfuerzo sin carga. Asegura que un porcentaje alto de paquetes no sufrirá prácticamente retardo ni será desestimado, y, por lo tanto, que llegará al destino correctamente. El servicio de carga controlada garantiza que la red reservará suficientes recursos para que cualquier aplicación que reciba este servicio no tenga que competir por los recursos con otras aplicaciones en tiempo real.

Esta arquitectura se basa en el Protocolo de Reserva de Recursos (RSVP), especificado en el RFC 2205, que reserva los recursos necesarios de la red IP antes de que comience

el intercambio de información de voz. El protocolo está orientado al receptor, es este el que hace la reserva para evitar problemas en caso de que el emisor haga multidifusión y cada receptor requiera de diferentes requisitos de QoS.

Los mensajes del protocolo son dos:

- Mensaje *Path*: Se envían desde el emisor hacia todas las destinaciones mediante árbol de distribución y contienen la información necesaria para que los receptores conozcan el camino.
- Mensaje *Resv*: Al recibir un mensaje *Path* en el receptor se contesta mediante el árbol de distribución y se hace la reserva de los recursos en los encaminadores.

En la siguiente figura se observa en la parte superior el camino de los mensajes *path* y la correspondiente respuesta de los receptores. Esta respuesta puede demandar diferentes necesidades en cada receptor.

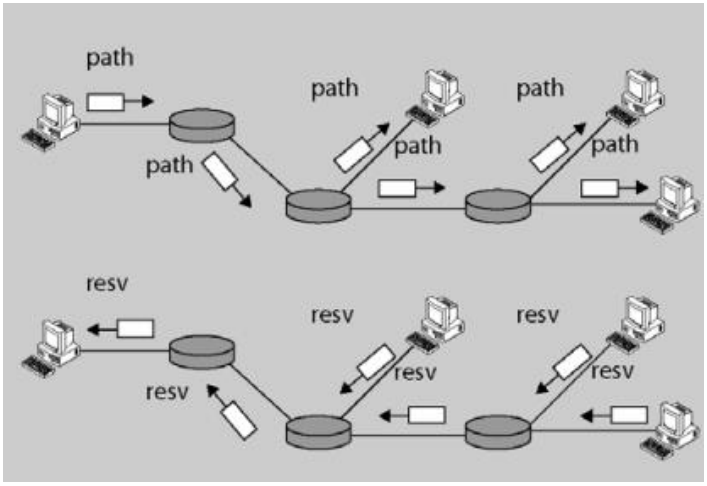


Ilustración 11. Establecimiento de camino mediante RSVP [20]

IntServ necesita saber qué recursos hay reservados y cuáles están utilizando los flujos en un momento determinado. En caso de recibir un nuevo flujo para poder utilizar este mecanismo, todos los nodos utilizados en la ruta, extremo a extremo, deben ser compatibles con RSVP. Esto hace que el protocolo sea menos flexible para su uso en telefonía fija sobre IP.

Para abordar los desafíos que suponían los servicios integrados surgió otro conjunto de estándares, el modelo de servicios diferenciados (DiffServ), detallados en las RFC 2474, 2597, 2598, 3246 y 4594. El objetivo principal de los servicios diferenciados es permitir que se proporcionen diferentes niveles de servicio para flujos de tráfico en una infraestructura de red común. Se pueden utilizar una variedad de técnicas de gestión de recursos para lograr esto, con el fin de que algunos paquetes reciban un servicio diferente (mejor o peor) que otros. Esto permitirá al administrador de la red mantener un servicio en tiempo real

dando prioridad al uso del ancho de banda y las colas del enrutador, hasta la capacidad configurada asignada al tráfico en tiempo real.

En la cabecera de IPv4 existía el campo ToS (*Type of Service*), descrito originalmente en la RFC 791, en las cabeceras IPv6 a este campo se le llamó *Traffic Class*. Este campo se utiliza para proporcionar información sobre cómo deben ser tratados los paquetes IP por los routers y otros dispositivos de red en el camino hacia su destino final. En ambos casos se reservan 8 bits, de los cuales los 3 primeros indican el *IP Precedence* posibilitando una combinación de 8 posibles clases de servicio. Mediante la publicación de la RFC 2474 se definió que los 6 primeros bits estarían destinados a DSCP (*Differentiated Services Code Point*) y sin uso los dos restantes (hoy en día se utilizan para indicar la congestión de la red extremo-a-extremo mediante *Explicit Congestion Notification)*, cambiando por tanto sus nombres de campo iniciales por el nombre del campo DS (*Differentiated Services*).

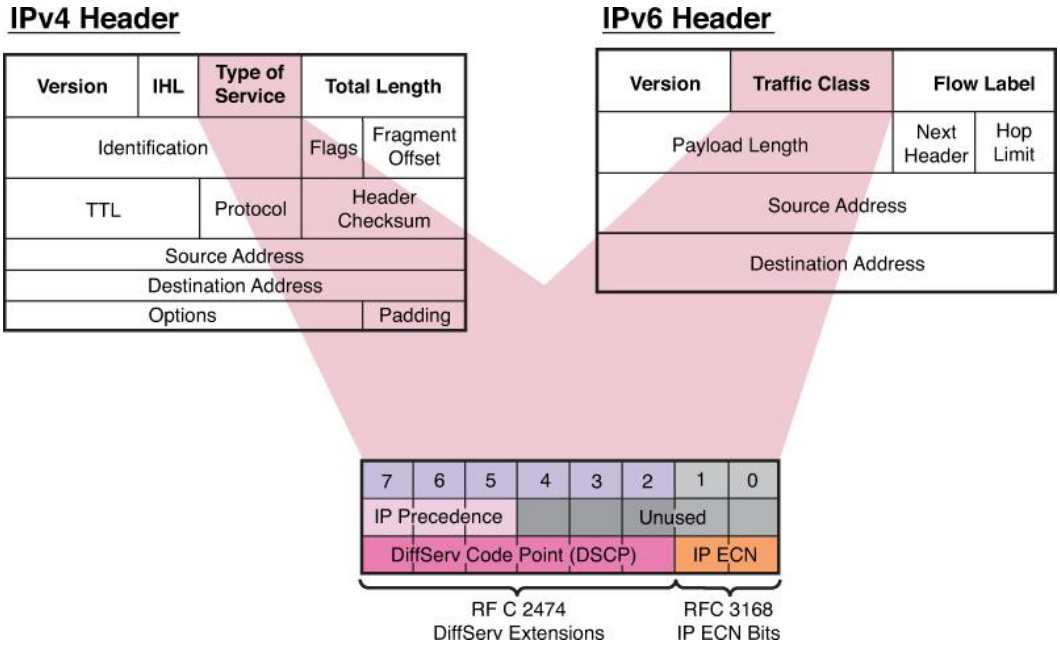


Ilustración 12. QoS en la cabecera de IPv4 e IPv6 [21]

El funcionamiento de los 6 bits del campo DSCP se definen en la RFC 2475, donde se indican una serie de políticas y grupos de comportamiento mediante el concepto de PHB (*Per-Hop Behaviours*) que aporta información sobre el comportamiento por salto. Los tres primeros bits indican la prioridad, se renombran las definiciones de los bits de *Precedence*.

Tabla 7. Selección clase DSCP

Prioridad	Descripción
0	Mejor esfuerzo *(Best Effort)*
1	Clase 1
2	Clase 2
3	Clase 3

4	Clase 4
5	*Expedited Forwarding* (EF)
6	Permanece igual (utilizado para protocolos de IP Routing)
7	Permanece igual (la capa de link y el protocolo de ruteo se mantienen activos)

La arquitectura Diffserv define dos tipos de comportamientos de reenvío, EF y AF, que utilizan diferentes puntos DSCP [22].

- Reenvío acelerado (EF): Se define en la RFC 2598, se puede utilizar para crear un servicio con un ancho de banda determinado, pérdida, latencia y fluctuación baja. Se le denomina servicio "Premium" y el ejemplo más habitual de su uso es en VoIP. El código DSCP corresponde con el 46 (101110 binario). Reciben el mejor tratamiento posible al enviarse a la red. El reenvío acelerado puede compararse con un canal dedicado.
- Reenvío asegurado (AF): Se define en la RFC 2597, proporciona cuatro clases diferentes de comportamientos de reenvío dentro de un dominio DiffServ. La siguiente tabla muestra las clases, las tres precedencias de descarte proporcionadas para cada clase y los puntos de código DSCP recomendados asociados con cada precedencia. Dentro de cada clase hay 3 probabilidades de descartes. A menor número, menor prioridad y menor probabilidad de descarte. Esta segmentación permite crear diferentes clases del tráfico que circula por la red, es habitual que se clasifiquen con nombres como "tráfico oro", "plata" o "bronce".

Tabla 8. Códigos de reenvío asegurado

	Clase 1	**Clase 2**	**Clase 3**	**Clase 4**
Baja probabilidad de descarte	001010 AF11	010010 AF21	011010 AF31	100010 AF41
Media probabilidad de descarte	001100 AF12	010100 AF22	011100 AF32	100100 AF42
Alta probabilidad de descarte	001110 AF13	010110 AF23	011110 AF33	100110 AF43

Al observar esto se puede concluir, una vez más, la importancia de asegurar una calidad del servicio en la transmisión de audio durante una llamada IP. La mayor prioridad, mediante el uso de EF se le da a este tipo de servicio con un código específico (46 decimal) para recibir el mejor tratamiento posible dentro de la red.

Para que un cliente reciba esta diferenciación de servicios debe llegar a un acuerdo con su proveedor de servicios de Internet (ISP), este acuerdo se conoce como SLA (*Service Level Agreement*). En él se especifican las clases de servicio soportadas y la cantidad de tráfico permitido en cada clase. Cada clase de servicio tiene asociado unos SLAs relativos a: Retardo máximo, variabilidad del retardo medio, pérdida de paquetes, seguridad,

monitorización, coste, etc. Los SLA concretos aplicables al servicio, a pesar de que su principal contenido es técnico, no dejan de ser un acuerdo contractual.

Gracias a la implementación de estas arquitecturas y métodos, la idea es que el procesado de los datos mediante el marcado del tipo de servicio se realice en los bordes del *core* de la red. En la periferia de la red se realiza el trabajo más costoso, dejando a los routers que componen la parte central de la red que los traten de manera diferente según el etiquetado que trae el paquete recibido.

Al haber definido los servicios integrados y los servicios diferenciados la siguiente pregunta puede ser ¿cuál es mejor? En la actualidad es generalmente más usado DiffServ, sin embargo, no se puede asegurar que uno sea mejor que el otro pues dependerá del caso de uso. El hecho de que se use más DiffServ se debe a su escalabilidad y la posibilidad tan avanzada de clasificar y tratar el tráfico. La reserva de recursos en los router en el modelo IntServ puede producir una sobrecarga importante en la red y los proveedores de servicio, además de que fue diseñado para ofrecer el mismo nivel de servicio a todos los usuarios, por lo que no se garantiza el mínimo de servicio a las aplicaciones en tiempo real. Cuando una aplicación requiere de un ancho de banda extra puede afectar al resto y producir congestión.

La implementación y configuración de estos métodos es labor del fabricante de los equipos. Además de estas arquitecturas los fabricantes han ido desarrollando diversos mecanismos para poder optimizar los recursos de la red, en general, las herramientas de QoS se clasifican en las siguientes categorías [21]:

- Herramientas de clasificación y marcado: Se analizan las sesiones, o flujos, para determinar a qué clase de tráfico pertenecen y, por tanto, qué tratamiento se debe dar a los paquetes. Una vez determinados, los paquetes se marcan para que el análisis ocurra solo un número limitado de veces, generalmente en el borde de entrada de una red. Un paquete puede atravesar varias redes diferentes hasta su punto final de destino, por lo que la reclasificación y el remarcado son bastantes comunes en los puntos de transferencia al ingresar a una nueva red.
- Herramientas de vigilancia, modelado y rebajas: Se asignan ciertas partes de los recursos de la red a cada sesión en función de la clase de tráfico (que pueden expresarse en términos de porcentaje absoluto o relativo). Cuando el tráfico supera los recursos de red disponibles, parte del tráfico se puede descartar, retrasar o volver a marcar de forma selectiva para evitar la congestión. Las sesiones se supervisan para garantizar que no utilicen más de lo que se les ha asignado y, si lo hacen, el tráfico se descarta (*policing*), se ralentiza (*shaped*) o se vuelve a marcar (*markdown*) para cambiar la prioridad.
- Herramientas gestión de la congestión: Cuando el tráfico supera los recursos de red disponibles se pone en cola para esperar a que se recupere la disponibilidad de los recursos.

- Herramientas específicas de enlaces: Algunos tipos de enlaces requieren un manejo y herramientas especiales, como técnicas de fragmentación e intercalado. Algunos enlaces también tienen acuerdos de ancho de banda contractuales (inferiores a la velocidad física) que no deben excederse, y si una ráfaga de tráfico excede estos límites, se configura (o se ralentiza) para cumplir con el acuerdo.

Por tanto, el flujo de datos y la gestión de este para tener el mayor control posible sobre la QoS podría esquematizarse como la Ilustración 13. Donde entra en la interfaz (router o switch) y se clasifica y marca para luego aplicar políticas de congestión mediante diferentes técnicas y finalmente dar salida a ese tráfico según la prioridad que le corresponda.

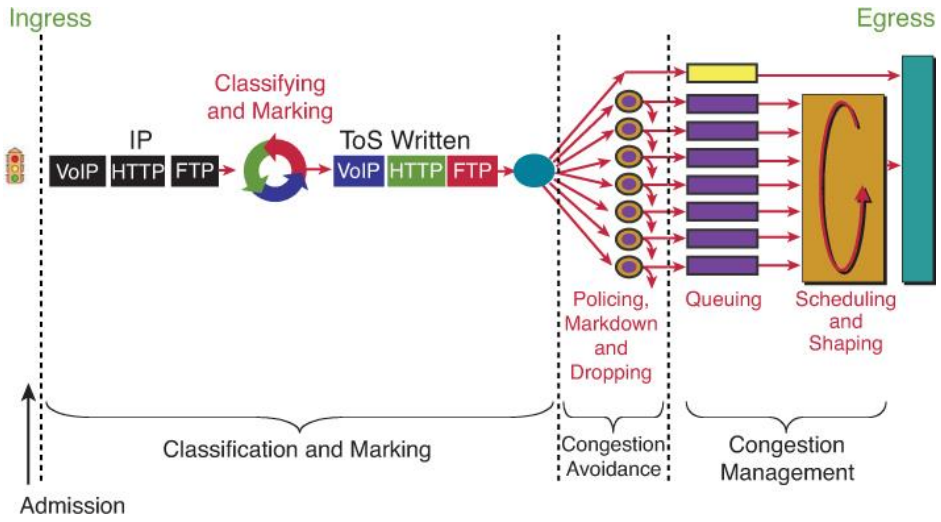


Ilustración 13. Conjunto de herramientas y secuencia en QoS [21]

3.3 QoS en una LAN

Antes de comenzar con el desarrollo de cómo garantizar QoS en una LAN es importante comentar que, tal y como ya se ha mencionado, existen diversas herramientas para resolver los desafíos entorno a la calidad de servicio. No existe una única solución que se adapte a cualquier escenario. Es posible llegar a resultados similares de diversas maneras, pero, si es conveniente tener en cuenta algunas buenas prácticas en el diseño de QoS. El fabricante Cisco recomienda las siguientes [21]:

- Habilitar siempre que sea posible las políticas de QoS en hardware antes que en software. Esto se debe a que la carga aumenta considerablemente en la CPU cuando se realiza en software, afectando a la velocidad de la interfaz, la velocidad y memoria del propio router, etc. En ciertos productos estas políticas se aplican al hardware dedicado exclusivamente a esto mediante circuitos integrados permitiendo realizar las configuraciones de QoS más complejas.
- Realizar una clasificación y marcado de las aplicaciones lo más próximo posible a la fuente. Ojo con permitir a los usuarios marcar ellos mismos su tráfico, podrían

realizar un uso indebido marcando paquetes como prioritarios cuando no es así. Es necesario que el administrador de la red tenga control sobre esto, o bien no permitiendo el marcado o desechando el marcado y asegurándose que este es correcto.

- Utilizar DSCP siempre que sea posible, utilizando los códigos PHB para asegurar el correcto funcionamiento y posibles futuras expansiones.
- Aplicar las políticas en el flujo de datos lo más próximo a su fuente. Aplicar el remarcado para poder cumplir con las reglas según el estándar.
- Habilitar las políticas de encolado especialmente en aquellos puntos que tengan potencial de sufrir congestión. Contar con al menos 4 tipos de colas basadas en el estándar.

Una LAN (*Local Area Network*) es una red de área local en la que se interconectan terminales que se encuentran en un área geográfica limitada. Al realizar el diseño se busca que esta red sea funcional, escalable, adaptable y lo más fácil posible de gestionar.

En un entorno LAN el principal problema a gestionar para garantizar QoS es la pérdida de paquetes, pues el *jitter* o la latencia están más relacionados con una WAN (*Wide Area Network*) o VPN (*Virtual Private Network*). Esta pérdida se ocasiona por el rebase del buffer ya que la velocidad de milisegundos en la transferencia de datos de Gigabit Ethernet puede generar congestión en la red si no hay capacidad suficiente y algoritmos para gestionar las tramas. En esta topología de red se desea priorizar el tráfico dentro de la propia red, el marcado de QoS suele realizarse en el switch. Los switches actuales pueden soportar diferentes mecanismos de QoS, como por ejemplo el etiquetado de prioridad IEEE 802.1p, que permite clasificar el tráfico en diferentes categorías de prioridad y asignar una etiqueta de prioridad a cada paquete. De esta manera, los switches pueden enviar los paquetes de alta prioridad antes que los de baja prioridad, mejorando el rendimiento y la latencia de la red.

Cabe mencionar que en la actualidad existen switches capaces de trabajar en capa 3, y que gracias al desarrollo de la tecnología que estos (switches tanto capa 2 como 3) implementan son capaces de realizar cada vez más funciones permitiendo un mayor y mejor control QoS en la red. Los switches de Capa 2 mejoraron significativamente el rendimiento de las redes al segmentar el tráfico de red en dominios de colisión separados, lo que redujo el ruido y la congestión de la red. Además, los switches de Capa 2 ofrecían una mayor seguridad y control de acceso que los HUBs. Posteriormente, los switches se desarrollaron para incluir funciones de Capa 3 (Capa de Red) en su arquitectura, lo que les permitió realizar enrutamiento de paquetes y funciones avanzadas de gestión de redes. Habitualmente el router tiene mayor capacidad de procesamiento y por tanto de aplicar diferentes algoritmos en la gestión del tráfico de datos. Los switches poseen una ventaja hardware en cuanto a la conmutación, mejorando en parte la lógica de software de un router mediante un hardware de circuito integrado que ofrece un mejor rendimiento en las LANs. Por otra parte, un Switch capa 3, diseñado específicamente para su uso en

intranets, normalmente no dispone de puertos WAN y cuenta con un router tradicional. Así que el Switch capa 3 suele ser el más utilizado para soportar enrutamiento entre VLANs.

Por tanto, en este apartado se verán métodos lo más genéricos posibles, en algunos casos aplicables en ciertos switches, o directamente en el router que hace de puerta de enlace con el exterior de la red. Las funcionalidades y métodos de control de la calidad dependerán de la selección del fabricante y el producto según la gama elegida. De hecho, cada fabricante tiene su sintaxis de comandos y métodos para desarrollar las políticas de QoS. Por ejemplo, Cisco (mediante IOS, *Internetwork Operating System*) utiliza MQC Syntax que consiste en un framework que mediante 3 comandos básicos permite:

- *Class-map*: Permite especificar los criterios que en caso de cumplirse desencadenan una sucesión de actos. Se pueden configurar varias condiciones y decidir si se deben cumplir o no de manera específica.
- *Policy-map*: Define las acciones que se aplicarán a cada class-map. Permite especificar diferentes políticas para cada clase de tráfico. Agrupa class-maps.
- *Service-policy*: Se usa para adjuntar un mapa de políticas (y, por lo tanto, las políticas asociadas para cada clase de tráfico que definió) a una interfaz lógica o física y para especificar la dirección (entrada o salida) en la que se aplicará la política.

Sin embargo, Juniper Networks utiliza un sistema basado en línea de comando estructurada, donde todo se engloba bajo el nombre de *Class-of-Service* (no hace referencia al CoS como tal, sino todo lo que engloba la gestión de QoS). Existen manuales de equivalencias entre los propios fabricantes para facilitar la labor a los ingenieros de redes encargados de configurar diferentes equipos [23].

Partiendo de un diseño de una LAN simple donde se encuentran como usuarios 2 PC y 2 dispositivos de telefonía fija sobre IP, junto a un switch que conecta estos cuatro equipos al router que ejerce como puerta de enlace al exterior. A este router se encuentra conectada la centralita telefónica la cual nos permite desplegar terminales para dotar a la LAN del sistema VoIP.

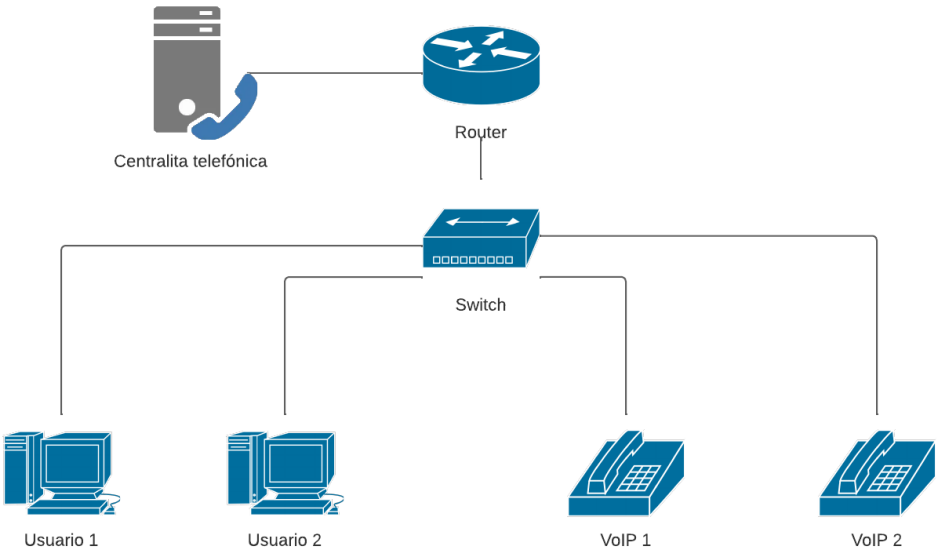


Ilustración 14. Sistema VoIP LAN simple

La LAN propuesta podría estar compuesta íntegramente por teléfonos fijos sobre voz IP, sin embargo, no sería una situación real. Lo habitual es tener un proveedor de internet y una LAN donde se integran todos los terminales, ordenadores y teléfonos fijos, entre otros. El hecho de compartir la misma red será un reto para garantizar QoS.

Si no aplicáramos QoS todos los paquetes de datos que circulan por la red serían tratados de la misma forma, no se podrían priorizar unos sobre otros, lo que implicaría no cumplir los requisitos de QoS de algunos servicios como sería la VoIP afectando directamente a la QoE de los usuarios.

Se comienza con el marcado del tipo de tráfico. Para ello mediante la gestión del switch al tener localizado cada terminal que se conecta en cada puerto podemos aplicar ciertas políticas. Utilizando el protocolo 802.1Q con la implementación de los 3 bits definidos en 802.1p indicamos el valor del campo PRI, tal y como se vio en la “Tabla 3. 802.1p Tipos de tráfico”. Este mismo protocolo permite hacer uso de un concepto interesante y muy habitual en el despliegue de LANs, el uso de LAN Virtual, o más conocida como VLAN.

Una VLAN consiste en la creación de redes LAN virtuales dentro de la propia LAN, proporciona conectividad de vínculo de datos para una subred. De esta manera se facilita la gestión mediante la partición de una única red conmutada para que coincida con los requisitos funcionales y de seguridad de sus sistemas sin tener necesidad de desplegar cables nuevos ni hacer cambios sustanciales en la infraestructura de red actual. Cada VLAN se puede identificar de forma exclusiva mediante el ID de VLAN, que se transmite y recibe como etiqueta IEEE 802.1Q en una trama Ethernet. Al implementar 802.1Q se añaden 4 bytes a la trama. Quedando de la siguiente manera:

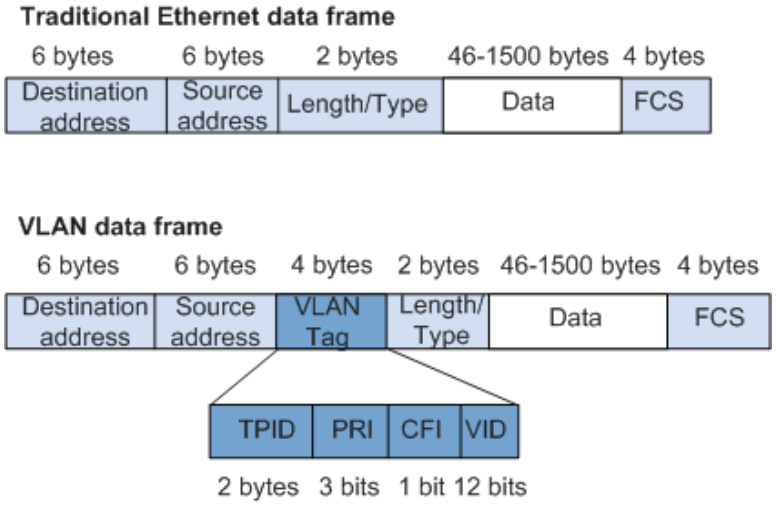


Ilustración 15. Formato trama 802.1Q [24]

El campo VID corresponde con la identificación de cada VLAN, siendo 4096 posibles opciones. El campo PRI, indica la prioridad y hace referencia a los códigos vistos previamente de 802.1p.

En el ejemplo dado anteriormente se podrían diferenciar dos VLANs, una para la parte de voz (Teléfonos IP) y la otra para los datos (PC). De esta manera es más sencillo agrupar el tipo de servicio y tener separadas las redes, a pesar de que estas pueden estar incluso en el mismo switch. La implementación de VLANs puede tener un impacto significativo en la calidad de servicio de una red al permitir la segmentación del tráfico de red en diferentes subredes lógicas.

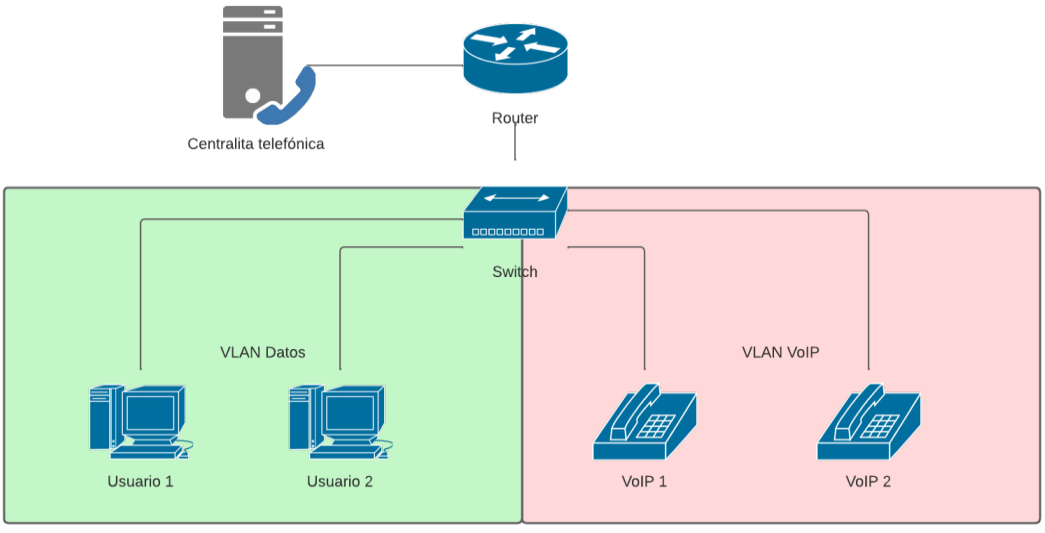


Ilustración 16. LAN simple implementando VLAN

El 802.1p fue desarrollado por el Grupo de Trabajo de Ingeniería de Redes de la IEEE en 1998, está integrado en los estándares IEEE 802.1D y 802.1Q, mientras que DiffServ fue

desarrollado por el Grupo de Trabajo de Ingeniería de Internet en 1999. Por lo tanto, el 802.1p fue desarrollado antes que DiffServ.

Ambos protocolos están diseñados para proporcionar calidad de servicio en las redes, pero utilizan enfoques diferentes. El 802.1p es un estándar de la capa 2 que utiliza etiquetas de prioridad de 3 bits en los encabezados de tramas Ethernet para diferenciar el tráfico. Por otro lado, DiffServ es un protocolo de la capa 3 que utiliza el campo DSCP en los encabezados de paquetes IP para clasificar el tráfico y aplicar diferentes niveles de QoS.

Por tanto, si la marca que se recibe de capa 2 contiene 3 bits y la que se utiliza en capa 3 tiene 6 bits, se debe realizar un mapeo de los valores para asociar, al menos en primera estancia, el valor CoS al valor DSCP.

El siguiente paso consiste en la clasificación del tráfico de la red. Las políticas definidas sólo podrán ser aplicadas si la clasificación del tráfico es correcta. Por tanto, se trata de un paso fundamental para poder cumplir con los requisitos de QoS en la red. Siguiendo las recomendaciones de buenas prácticas sería conveniente realizar el marcado del tráfico lo más próximo a la fuente. Este marcado puede venir determinado por el propio terminal, el cual previamente se debe dar de alta en un listado de terminales confiables, un ejemplo serían los teléfonos IP. Cuando el marcado es correcto no es necesario realizar un análisis del paquete para tener que identificarlo. Tal y como se ha visto unos párrafos atrás, el tráfico se puede clasificar mediante el análisis de la cabecera. Observando las marcas (CoS en capa 2 o DSCP en capa 3) o la dirección (puerto origen/destino, interfaz, etc.). Pero si un paquete no viene marcado, o peor aún, viene marcado incorrectamente, otra forma de clasificar sería profundizando más en el contenido del paquete mediante la examinación del contenido del *playload*. Existen diferentes tecnologías que buscan aportar información y facilitar el control de este tipo de tráfico sin identificación previa. En general realizan una inspección profunda de los paquetes basándose en firmas o heurísticas para reconocer el comportamiento de cierta información dentro del paquete. Permiten la monitorización y administración del rendimiento de las aplicaciones que se ejecutan en la red. Los administradores de red pueden aplicar políticas de firewall granulares que permiten o bloquean el tráfico basado en la aplicación, así como políticas de control de ancho de banda y calidad de servicio (QoS) basadas en la aplicación. Algunos productos concretos que realizan estas funciones son NBAR (Cisco), DPI (Juniper Networks), App-ID (Palo Alto Networks).

Por tanto, se genera una situación en la red que a partir de un punto los datos del etiquetado deben considerarse correctos y fiables para poder trabajar con ellos. A este concepto se le conoce como límite de confianza, del inglés *trust boundary*. Siguiendo los consejos de buenas prácticas este elemento debería estar lo más próximo a la fuente, pero podría estar en los siguientes tres casos:

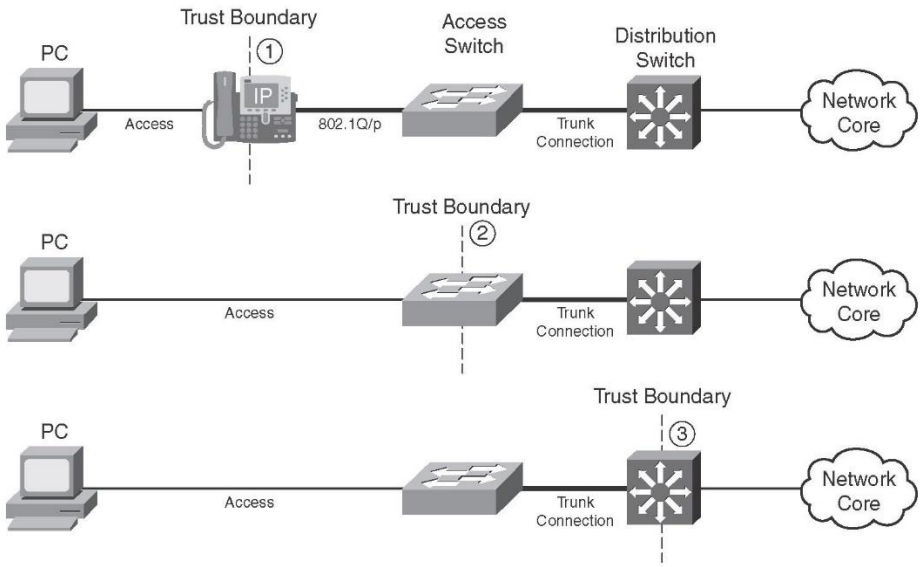


Ilustración 17. Límites de confianza en la red [25]

Tal y como se ha comentado previamente, cada fabricante tiene su forma de configurar la gestión de la QoS. Pero en general se sigue el mismo criterio. Primero se definen las reglas con las que si un paquete de datos coincide se tendrá en cuenta para aplicar ciertas acciones. Por ejemplo, los paquetes que contengan en el campo DSCP el valor EF (46) o que contengan en el campo CoS el valor 5. De esta manera cada paquete de VoIP, o que venga etiquetado como tal, pertenece a un grupo formado por estas dos condiciones.

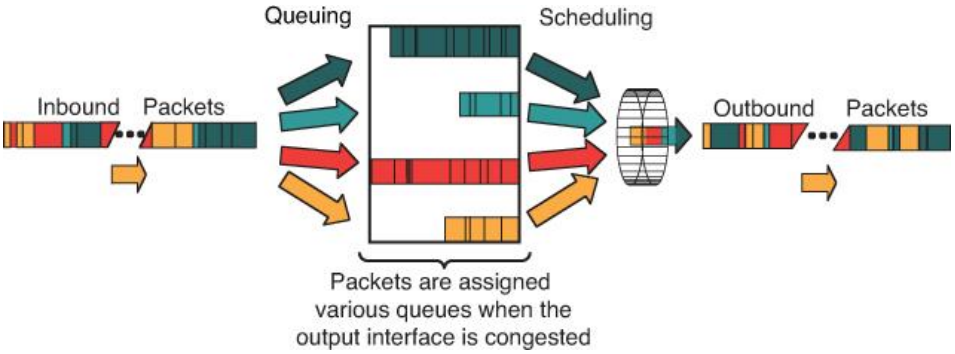


Ilustración 18. Ejemplo genérico de cola y programación de paquetes [21]

El siguiente paso consiste en encolar los paquetes y tomar una decisión sobre cómo hacerlo y qué hacer en caso de que las colas comiencen a llenarse. Existen diferentes tipos de encolamiento, todos son herramientas que permiten un control sobre la congestión mediante la administración del buffer, priorizando a su entrada o reordenando a su salida antes de ser transmitidos. Los más destacables son:

- FIFO: Del inglés *First In First Out*, primero en entrar primero en salir. Es el modelo de cola que se ha usado tradicionalmente. En cada puerto de salida existe una cola simple, donde los paquetes se van ordenando según el orden de llegada y a su salida el primero será el que mayor tiempo lleve almacenado en la cola. Todos los

paquetes tienen el mismo tratamiento por lo que es poco eficiente su uso en un sistema donde se está intentando optimizar los recursos y dar prioridad al tráfico que se ha marcado como tal.

- PQ: Del inglés *Priority Queuing*, colas con prioridad. En ellas se establecen colas con diferentes clases de prioridad, donde los paquetes se van almacenando según el tipo de prioridad indicado en la cabecera del paquete, dirección IP origen o destino o el criterio seleccionado. Una vez los paquetes deben transmitirse se sigue el mismo concepto que FIFO, siendo siempre la prioridad los paquetes de clase más alta de una cola no vacía. Este sistema aporta una planificación más orientada a la priorización de paquetes, sin embargo el concepto final dentro de cada cola sigue siendo muy básico.
- FQ o WFQ: Del inglés *Fair Queuing* o *Weighted Fair Queuing*, colas equitativas o equitativas ponderadas. La primera consiste en clasificar los paquetes en clases, en este caso pudiendo haber una clase para cada flujo. Las cosas siguen el algoritmo *Round Robin* con el que se toma un paquete en cada cola no vacía por turno, se sirven los datos de forma secuencial, de esta manera cada cola consigue enviar un paquete por turno. La WFQ sigue la misma idea inicial, sin embargo, las colas tienen pesos para poder dar más capacidad a las colas que tienden a estar más ocupadas.
- CBWFQ: Del inglés *Class Based weighted Fair Queuing*, colas equitativas ponderadas basadas en clases. Son un híbrido de los sistemas anteriores, donde se combina WFQ con el uso de FQ simple, de esta forma se asegura la equidad entre diferentes colas y el ancho de banda. Por defecto se ejecuta *Tail drop*, que consiste en descartar paquetes del final de la cola cuando está en congestión.

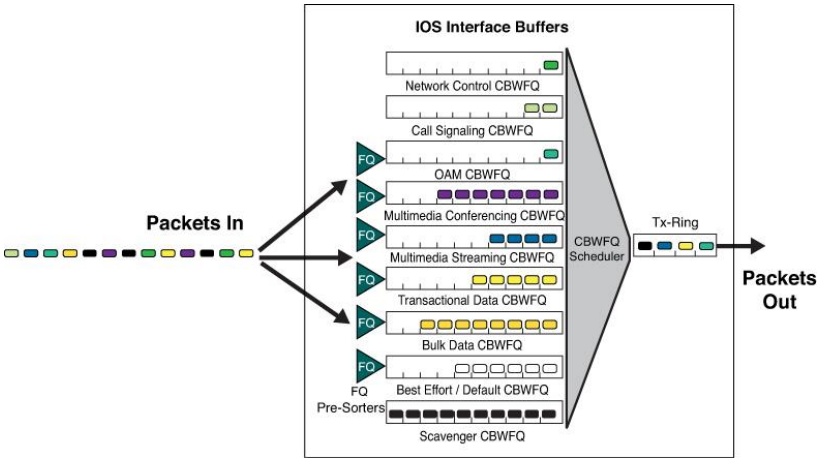


Ilustración 19. Funcionamiento cola CBWFQ [21]

- LLQ: Del inglés *Low-Latency Queuing*, cola de baja latencia. Añade a WFQ una capacidad de clasificar con prioridad estricta, es un complemento a este tipo de colas pues no ofrecen (ni WFQ ni CBWFQ) una clase predeterminada para el

tráfico en tiempo real. Es un concepto muy interesante para tráfico tanto en tiempo real como el resto ya que garantiza baja latencia y el ancho de banda.

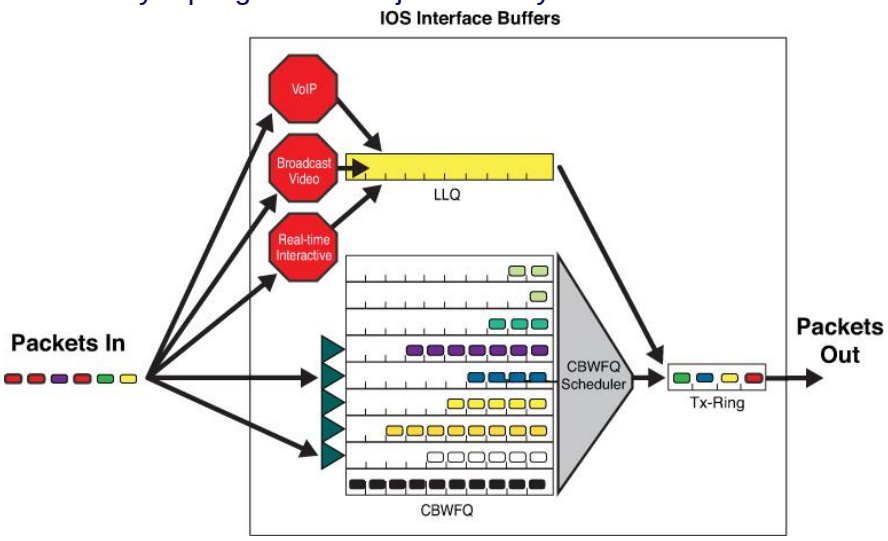


Ilustración 20. Funcionamiento CBWFQ junto a LLQ [21]

De esta manera, aplicando los mecanismos vistos en este capítulo podemos afirmar que en un entorno de área local, pudiendo ser esta incluso de grandes dimensiones, la calidad de servicio en el sistema de telefonía fija de voz sobre IP está gestionada y controlada. Una vez los paquetes pasan a ser enrutados en capa 3, bien por el router o el switch con estas capacidades, la trama de Ethernet deja de tener valor pues se descarta y con ella se pierde la etiqueta 802.1p. Es por esto que siempre se realiza un mapeo con DSCP, para cuando este paquete a nivel IP continúe su camino tenga esta marca que lo diferencia del resto y en los nodos que componen la red se gestione como es debido. El éxito de aplicar QoS de inicio a fin dependerá de la configuración y la arquitectura de red planteada.

3.4 QoS en MPLS

Multi-Protocol Label Switching se definió en la RFC 3031 para ser utilizado en las redes basadas en capa 3 con el objetivo de aumentar la eficiencia en la red. MPLS se desarrolló para superar las limitaciones de Frame Relay y ATM en términos de escalabilidad, flexibilidad y calidad de servicio (QoS), y para proporcionar mayor eficiencia y flexibilidad en el enrutamiento t conmutación de paquetes en redes IP.

Mediante el uso de etiquetas adjuntas al paquete IP, entre los routers se crea un mapeo de etiquetas que permite que estos reenvíen el tráfico mirando la etiqueta y no la dirección IP de destino. Los paquetes se reenvían mediante conmutación de etiquetas en lugar de conmutación de IP. Por ello se dice que el protocolo trabaja en capa 2.5, ya que se encuentra entre la cabecera de capa 2 y el paquete IP.

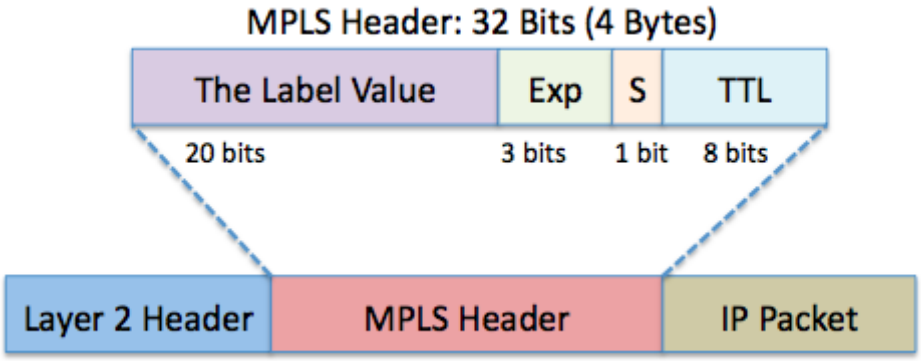


Ilustración 21. Cabecera MPLS [26]

Las redes pueden implementar MPLS para mejorar la eficiencia y la calidad de servicio en sus redes WAN (redes de área amplia). Esto les permite establecer circuitos virtuales privados y gestionar el enrutamiento y la priorización del tráfico según sus necesidades. MPLS permite a las organizaciones tener mayor control sobre su conectividad, optimizar la transmisión de datos y garantizar niveles adecuados de rendimiento para aplicaciones críticas, es una herramienta muy potente con un gran abanico de posibilidades de configuración. Esta sección se centra en cómo se detalla el uso de QoS dentro de una red implementada con MPLS.

El sistema busca resolver un problema directamente relacionado con la calidad de servicio, la congestión, ya que tradicionalmente el algoritmo de enrutamiento ha sido el de Dijkstra, que se basa en encontrar la ruta más corta. Esto puede ocasionar congestiones pues algunos enlaces pueden estar excesivamente ocupados cuando otros están sin utilizar. Por ello MPLS, mediante el uso de etiquetas, busca separar el plano de control (*routing*) del plano de datos. Los protocolos de enrutamiento se utilizan para funciones de control y las decisiones de enrutamiento se toman en función de la etiqueta.

Una red MPLS está compuesta por los siguientes elementos:

- *Label Switching Router* (LSR): Son los routers que componen el núcleo de la red, no conectan clientes, solo transportan los datos de las redes de estos pero no participan en ella. Se encargan de reenviar paquetes y conmutar etiquetas, además comparten información con otros LSR para actualizar sus tablas. Se identifica con una P de *Provider*, haciendo referencia en una red ISP a los routers internos de la propia red MPLS.
- *Label Edge Router* (LER): Son los routers que se encuentran en los extremos de la red MPLS, a él se conectan los clientes mediante interfaces IP. Se encargan de preparar los paquetes entrantes y salientes, mediante agrupación y etiquetación de estos en el caso de entrada a la red MPLS, o bien de quitar esta etiqueta para encaminarlos mediante IP en caso de salida de la red. Se indica con las siglas PE de *Provider Edge*, pues en una red ISP es el router que se encuentra el borde del núcleo MPLS.

- *Customer Edge* (CE): Primera conexión fuera de la red MPLS, utiliza una conexión IP pura e intercambia con el LER las rutas de cada destino.
- *Label Switched Path* (LSP): Es el camino establecido dentro de la red para un determinado grupo de paquetes, este grupo se denomina *Forwarding Equivalent Class* (FEC), independientemente su destino final, cada LSP es independiente por lo que los caminos de ida no tienen por qué coincidir con los de vuelta.
- *Label Forwarding Information Base* (LFIB): Base de datos que almacena la información relacionada con las etiquetas a utilizar en los paquetes que pasan por los LSR y LER.

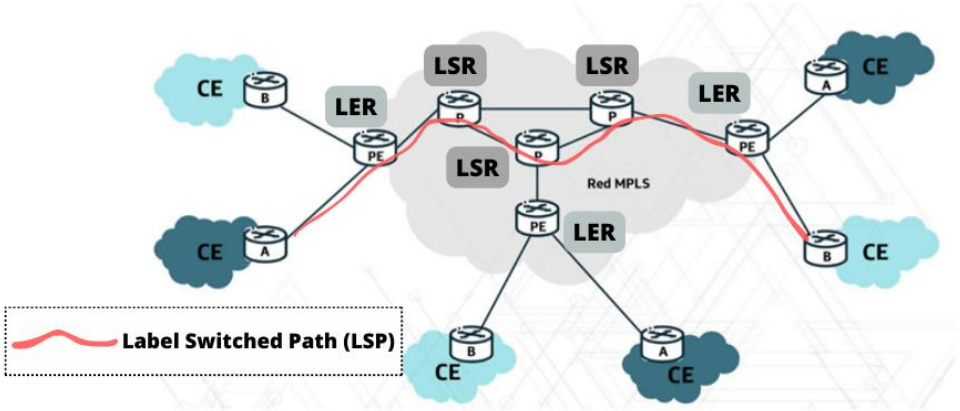


Ilustración 22. Esquema básico de una red MPLS

Los paquetes se etiquetan y se conmutan a través de los LSP, los LSR realizan la operación de intercambio para conmutar los paquetes. Se necesita una etiqueta que se distribuya en todos los routers adyacentes, para ello se debe utilizar un protocolo de distribución de etiquetas. El protocolo LDP, *Label Distribution Protocol*, se definió en la RFC 3036 y actualizó en la RFC 5036 con el propósito de establecer las sesiones entre los nodos adyacentes para poder hacer este intercambio. LDP es uno de los protocolos más comunes utilizados para la distribución de etiquetas en una red MPLS, aunque con el tiempo se han ido desarrollando alternativas como RSVP-TE. Una extensión de LDP es CR-LDP, *Constrained-based Routing LDP*, que permite encontrar la ingeniería de tráfico requerida para hallar rutas más eficientes. CR-LDP se utiliza para establecer rutas basadas en restricciones de QoS y recursos, y para distribuir etiquetas correspondientes a los paquetes en la red MPLS.

Una de las grandes ventajas de MPLS es la Ingeniería de Tráfico, su acrónimo TE del inglés *Traffic Engineer*. Es una disciplina centrada en la optimización del rendimiento de la red, utiliza diferentes técnicas de medición, caracterización, modelado y control de tráfico para realizar un manejo más eficiente de sus recursos [27]. Se puede identificar dos tipos según el objetivo de las decisiones que se tomen:

- Orientada al tráfico: Cuando se busca mejorar el transporte de datos mediante la reducción de pérdida de paquetes, del retardo y *jitter*, aumentar en general el rendimiento del transporte.

- Orientada a los recursos: Cuando se busca optimizar las colas, el búfer disponible, mediante la toma de decisiones de las rutas en función del ancho de banda.

En líneas generales el objetivo es adaptar los flujos de tráfico a los recursos de los que dispone la red MPLS, hacer un reparto de estos de la manera más optima posible procurando dar equilibrio en el uso de estos y así evitando cuellos de botella. Por ello se considera que se hace una adaptación de un proceso dinámico (tráfico de datos) a uno estático (la red física), se utiliza para redistribuir de forma eficiente los aumentos de tráfico en la red.

Una de las capacidades funcionales más importantes para MPLS-TE es el encaminamiento basado en restricciones, CBR del inglés *Constraint Based Routing*. El concepto consiste en definir ciertas restricciones o criterios específicos para establecer diferentes rutas. De esta manera se influye en el camino que debe seguir el tráfico, algunos parámetros sobre los que se aplican las restricciones son el ancho de banda disponible, la latencia, el costo, o el tipo de tráfico, entre otros. La alternativa mencionada unos párrafos más atrás, RSVP-TE, consiste en utilizar el protocolo de control visto en capítulos anteriores, donde un host solicita servicios específicos de calidad de la red para flujos o corrientes de datos de aplicaciones particulares. En este caso utiliza extensiones de ingeniería de tráfico para admitir la señalización automática de los LSPs. Hace uso de los mismos mensajes del protocolo RSVP, el LER de ingreso envía un mensaje *Path* al LER de salida indicando el FEC al que se deben vincular las etiquetas. Estos mensajes permiten que los routers del camino reserven el ancho de banda y distribuyan la etiqueta al router siguiente. Solo se considera el LSP operacional cuando el LER de ingreso recibe el mensaje de respuesta enviado por LER de egreso, el mensaje *Resv*.

La combinación de MPLS con DiffServ y el encaminamiento basado en restricciones ofrece una potente herramienta para aplicar QoS en redes IP. El *DiffServ-aware* MPLS (DS-MPLS) es una tecnología que permite la implementación de esquemas de calidad de servicio transparentes dentro de un dominio MPLS. Esto significa que el dominio MPLS puede utilizar un esquema de QoS diferente al del paquete IP encapsulado, pero aun así preservar los bits DSCP del paquete IP. Además, DS-MPLS permite la selección diferenciada de caminos para el tráfico basado en sus requisitos de QoS, lo que garantiza el ancho de banda por separado para cada clase de tráfico.

Cuando los LER tienen la responsabilidad del marcado de los paquetes entrantes y los mecanismos de descartes permite que cuando muchos conmutadores de borde envíen datos a los conmutadores del *core* estos no tengan la necesidad de descartar paquetes, al menos no grandes cantidades debido al rebose de su *buffer* [28]. Surgen dos problemas en la asociación de DSCP y MPLS, tal y como se ha comentado en el desarrollo de la memoria, el DSCP es transportado en la cabecera IP, pero los LSR solo examinan el encabezado de etiqueta, no pueden analizar el valor DSCP. Además de que el campo EXP de MPLS tiene 3 bits y no los 6 bits con los que se definen los valores DSCP. Para ello la IETF describe dos soluciones:

- E-LSP: *EXP-Inferred-PSC LSP*, mapea DSCP al campo EXP asignando un PHB. La etiqueta contiene la información de reenvío y el campo EXP el comportamiento que tiene que recibir ese flujo. En caso de recibir un paquete con *IP Precedence* al contener 3 bits el mapeo es directo al campo EXP, pero si se recibe DSCP el IEEE define que se usarán los 3 bits de la izquierda (los que indican la clase de servicio en DSCP).

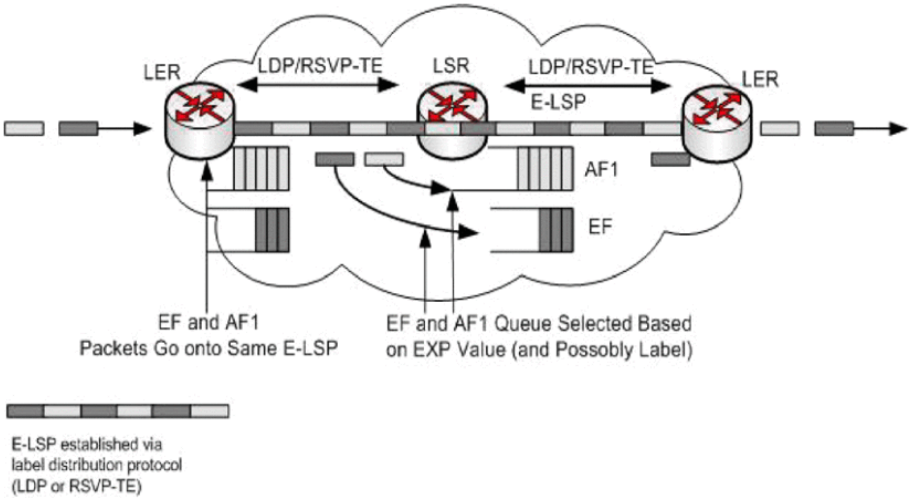


Ilustración 23. Ejemplo de E-LSP para DSCP EF y AF1 [29]

- L-LSP: *Label-Only-Inferred-PSC LSP*, solventa el problema de más de 8 PHB. La "L" indica que deriva de la etiqueta esto es porque el campo EXP indica la prioridad de descarte asignada al paquete y en la propia etiqueta se indica el PHB. Hay una relación implícita entre la etiqueta y el PHB, por ello se debe informar al establecer la señalización LSP.

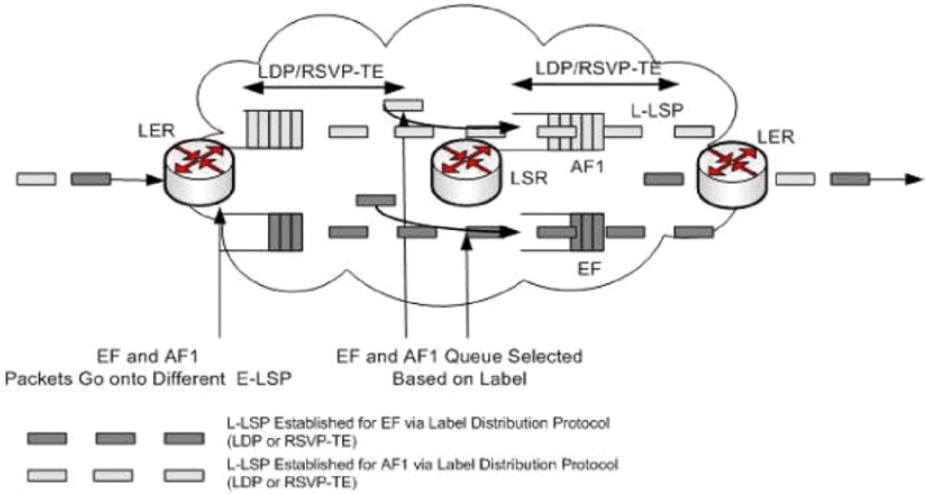


Ilustración 24. Ejemplo de L-LSP para DSCP EF y AF1 [29]

El marcado DSCP define el comportamiento de los routers (PHB), crear túneles dentro de DS-MPLS permite ser transparente desde un extremo de la red a otro. El comienzo del túnel coincide con la colocación de la etiqueta MPLS, y el final con su retirada. Existen 3 modelos en función de esta gestión:

- *Pipe mode*: Se analiza la marca DSCP y se impone un valor que se enviará dentro de la red MPLS en la etiqueta. Dentro de la red los paquetes se etiquetan con el mismo valor de la etiqueta recibida. En el último salto los PE eliminan la etiqueta MPLS y aplican QoS en su interfaz de salida según el valor MPLS EXP. De esta forma se pueden interconectar diferentes dominios DiffServ garantizando la transparencia en el campo DSCP.
- *Short pipe mode*: Idéntico al *pipe mode* a excepción del comportamiento del PE. El PHB no se obtiene del marcado del LSP si no del propio encabezado DSCP. Por tanto en el router de salida se basa en la información de DiffServ y no de las etiquetas que viajaban dentro de la red MPLS.
- *Uniform mode*: Los paquetes se tratan de manera uniforme en la red IP y MPLS. Esto es que el valor PRI y el valor MPLS EXP es idéntico, la red MPLS comparte el dominio DiffServ que se indica en el router de ingreso. Cada cambio de comportamiento se refleja dentro de MPLS y por tanto a la salida hacia el CE.

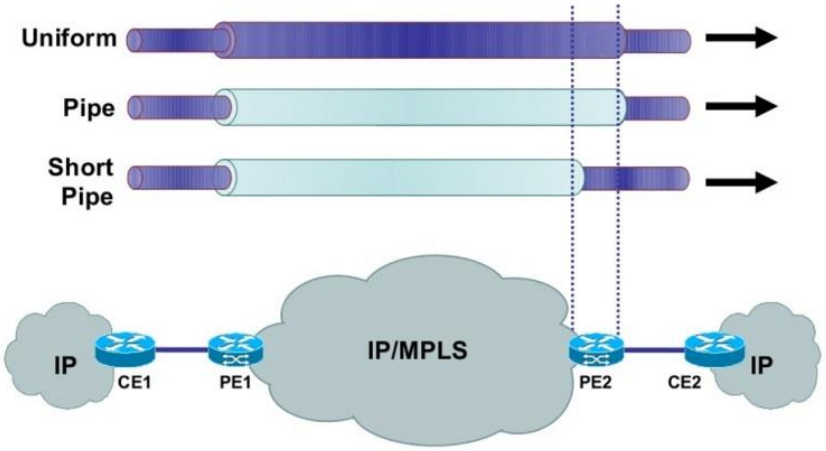


Ilustración 25. Túneles Diff Serv MPLS [30]

En [31] se lleva a cabo una simulación para comparar el impacto que tiene el uso de las prioridades en la red IP y la ingeniería de tráfico en MPLS. Los resultados obtenidos se centran en describir el retardo medio, el *jitter* medio y el porcentaje de paquetes perdidos. El tráfico que se añade a la red es de voz, vídeo, transferencia de ficheros (FTP, *File Transfer Protocol*) y datos simples para modelar el fondo del flujo. Los dos primeros tienen un *bit rate* constante, 400 kbps para la voz y 300 kbps para el vídeo, la transferencia genera un flujo aleatorio y el tráfico de datos normales tiene una distribución exponencial con un *bit rate* de 250 kbps. El primer escenario no tiene ningún tipo de restricción en el ancho de banda, se trata de un caso de *Best Effort*. El segundo escenario se prioriza el tráfico de voz. En el tercero se prioriza la voz y el vídeo. En el cuarto escenario se añade a la voz y el vídeo la priorización de FTP. En el quinto y último escenario se implementa CR-LDP, permitiendo aplicar ingeniería de tráfico para seleccionar diferentes rutas de las que se establecen en el enrutamiento IP. En este caso, la restricción se aplica para que el camino más corto sea usado exclusivamente por el tráfico RTP, quedando el camino más largo para el resto de tráfico.

En las siguientes tablas se citan los valores que obtuvieron en las simulaciones. Se observa como la gestión del tráfico tiende a mejorar con cada medida implementada, pero sobre todo la mejora llega de la mano de la aplicación de CR-LDP con la ingeniería de tráfico. Donde hay pérdidas nulas de paquetes, un retardo y un jitter más que aceptable para garantizar una comunicación con una QoE alta.

Tabla 9. Pérdida de paquetes [%] en las simulaciones [31]

Tipo de tráfico	Best Effort	Prioridad voz	Prioridad RTP	Prioridad RTP + FTP	CR-LDP
Voz	16.42	0.00	0.00	0.77	0.00
Vídeo	9.93	8.83	0.03	0.22	0.00
FTP	14.67	13.24	11.81	8.09	7.15

Tabla 10. Retardo promedio [ms] en las simulaciones [31]

Tipo de tráfico	Best Effort	Prioridad voz	Prioridad RTP	Prioridad RTP + FTP	CR-LDP
Voz	7.84	4.63	4.41	6.54	1.05
Vídeo	3.90	14.99	4.16	3.89	0.21
FTP	6.93	18.08	25.76	87.49	3.31

Tabla 11. Jitter promedio [ms] en las simulaciones [31]

Tipo de tráfico	Best Effort	Prioridad voz	Prioridad RTP	Prioridad RTP + FTP	CR-LDP
Voz	58.41	47.39	47.49	55.59	42.48
Vídeo	56.95	67.09	52.10	56.96	44.14
FTP	69.62	102.73	114.19	216.48	74.52

El hecho de implementar prioridad a la voz aporta una mejora considerable, sobre todo en la pérdida de paquetes debido a la congestión que no puede gestionar de manera correcta la red. Sin embargo, no es un caso práctico real, por ello a medida que se implementan mejoras para el resto del tráfico se debe conseguir no perjudicar otras aplicaciones. Otro aspecto a destacar es el gran descenso en el valor del retardo medio medido, en concreto para la voz. Al implementar ingeniería de tráfico se disminuye 7 veces menos, lo cual es interesante pues en grandes arquitecturas este valor es más elevado y conseguir reducirle puede impactar directamente en la calidad de servicio.

Por tanto, MPLS es una tecnología prometedora que ofrece numerosas ventajas en términos de gestión de QoS y optimización de recursos de red. En la actualidad está consolidada en redes IP de gran escala en los ISP. Su integración en las redes de banda ancha permite a los proveedores de servicios ofrecer un rendimiento confiable y capacidades personalizadas para satisfacer las necesidades de los usuarios en un entorno en constante cambio. Como se ha expuesto en la simulación seleccionada del documento la práctica corrobora todas las ventajas teóricas. Donde las ventajas pueden ser muy significantes desde el punto de vista del ancho de banda consumido, reducción del retardo

y el *jitter*. Especialmente en los servicios de tiempo real, como lo es la telefonía fija por voz IP.

3.5 QoS en Internet

La garantía de calidad de servicio en Internet para llamadas de voz sobre IP puede ser un desafío debido a la naturaleza misma de la red y a diversos factores. El Internet que se conoce hoy en día ha sido fruto de diversos avances que se fueron incorporando a la idea inicial de desplegar una red global de redes interconectadas. En este desarrollo han sido partícipes diversas entidades, tales como el propio ARPA, IETF, ICANN, W3C, ISOC o ITU. Han contribuido al desarrollo de Internet y han establecido normas y estándares para su funcionamiento.

La naturaleza de la red es una red pública y global compuesta por múltiples proveedores de servicios de Internet (ISP) y enlaces interconectados. Los paquetes de datos viajan a través de múltiples redes y routers gestionados por diferentes entidades. En ese sentido, se puede considerar que Internet es un recurso público, ya que está compuesto por cables submarinos, enlaces satelitales, servidores y otros componentes de red que son mantenidos y administrados por diferentes organizaciones y proveedores de servicios de Internet en todo el mundo. Aunque la infraestructura de Internet es pública, es importante destacar que el acceso a Internet puede ser tanto público como privado. Los usuarios pueden acceder a Internet a través de proveedores de servicios de Internet (ISP) que brindan conexiones de Internet a nivel individual o empresarial. Estos ISP pueden ser entidades comerciales, gubernamentales o sin fines de lucro. Además, el contenido y los servicios disponibles en Internet también pueden ser públicos o privados.

La estructura actual de internet está basada en redes de forma jerárquica, 3 niveles conocidos como *Tiers*. Donde las número 1 son las redes de las grandes operadoras, forman el troncal de Internet. De aquí se van “descolgando” redes conectadas a estas, reduciendo el foco hasta llegar a las redes nacionales, regionales o locales, las que proporcionan los ISP. Los proveedores tienen conectividad entre ellos directamente o a través de puntos de intercambio (IXP), por lo que en relación a la calidad del servicio esto afecta de manera directa, ya que como se ha visto es factible gestionarla de manera local e incluso en la gran red que el proveedor puede tener, sin embargo, cuando hablamos de Internet como tal esta interconexión podría generar eslabones débiles en la cadena desde el inicio al final de la comunicación, originando los síntomas de una conexión sin calidad de servicio garantizada.

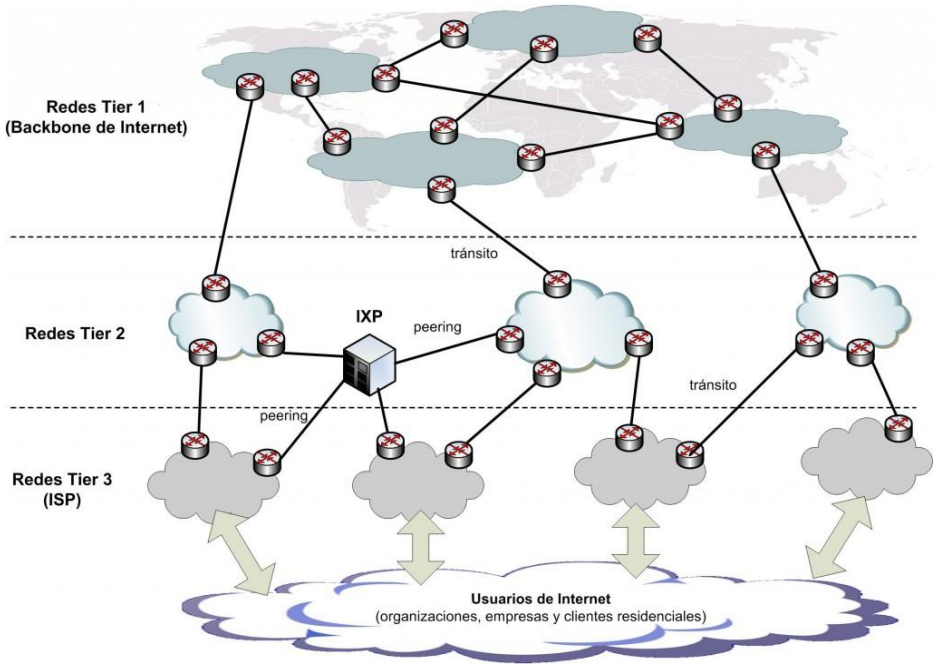


Ilustración 26. Estructura resumida de red Internet [32]

El enrutamiento no determinista puede generar diversos problemas de retardo y pérdidas de paquetes. Ya que una vez la llamada sale de la red del ISP (con el cual se pacta un SLA donde garantiza QoS en su red), puede sufrir este tipo de errores. Otro problema puede ser la congestión de la red en ciertos puntos debido a la amplia variedad (y en aumento) de aplicaciones y servicios que demandan ancho de banda. Junto a ellos, también se debe tener en cuenta la calidad del enlace con el que se realiza el acceso a la propia red de Internet, no siempre es posible realizarlo mediante enlaces guiados y se recurre a tecnología inalámbrica como primer punto de acceso, esto también podría suponer un problema en caso de que no sea estable o no ofrezca un ancho de banda mínimo para establecer correctamente una comunicación VoIP.

Existen mecanismos que podrían limitar el número de errores, como que no se consuma más ancho de banda del contratado al ISP permitiendo solo un número de llamadas simultáneas, o bien creando túneles VPN mediante L2TP sobre IPSec. Sin embargo, ninguno de ellos asegura la calidad de servicio *end-to-end*. La variedad de mecanismos es amplia, pero consiste en un esfuerzo que va más allá de ello, entran en juego otros intereses como los económicos y estratégicos por parte de los proveedores de servicio.

El objetivo de proveer una calidad de servicio de inicio a fin garantizada a cualquier cliente es muy desafiante porque múltiples redes independientes están involucradas en el proceso, por lo que actualmente se podría afirmar que no está asegurada la calidad de servicio en una comunicación de telefonía IP sobre Internet.

3.6 Diseño entorno de simulación

Para realizar el desarrollo de un entorno de pruebas se podría adaptar cualquiera de los diversos sistemas de comunicaciones ToIP existentes. De software libre, como 3CX, Asterisk o MicroSIP, o propietario, de fabricantes como Cisco, Avaya, Mitel o Alcatel. Incluso opciones de solo simulación como GNS3 (Cisco). Ya que el objetivo del proyecto es no solo implementar este sistema sino analizar las medidas de QoS, se ha optado por el sistema propietario de Alcatel dada la experiencia en campo con este producto. Configurando la centralita OXE en un entorno donde se pueden modificar parámetros QoS para marcar la prioridad de las tramas/paquetes, junto a la selección de otros parámetros como los códecs utilizados, el uso de VLAN o la consulta del registro de las llamadas que ofrece la centralita en *Tickets IP* con datos de la duración de la llamada, el *jitter*, los paquetes perdidos, el *delay*, etc., gracias a ello se podrá elaborar una serie de conclusiones en base a las pruebas que se realicen.

Para implementar el entorno se ha utilizado un switch Cisco Catalyst WS-C3560-24PS de 24 puertos 10/100 (FastEthernet) con posibilidad de PoE (*Power over Ethernet*). Entre los estándares con los que puede trabajar se encuentra el 802.1p/Q.

Ilustración 27. Switch Cisco Catalyst 3560

Para su configuración es necesario acceder mediante el cable de consola del fabricante, el cual se conecta en la parte trasera mediante RJ45 y por el otro extremo tiene una terminación de 9 pines RS232.

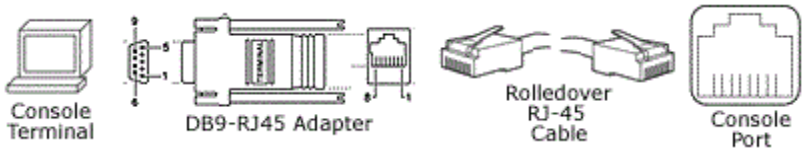


Ilustración 28. Esquema gráfico conexión switch

En la actualidad para poder leer estos datos desde un PC se debe conectar al extremo sobrante otro cable con capacidad de transferencia del puerto serie a USB.

Ilustración 29. Cable RS232 a USB

Se identifica el puerto COM asignado donde se ha conectado el dispositivo serie al ordenador y mediante un software emulador de terminal realizamos la configuración para poder acceder por consola al switch:

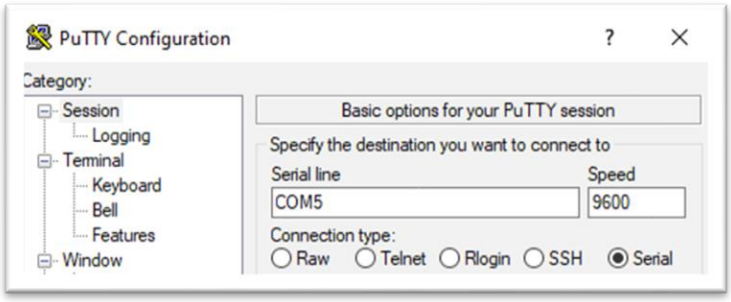


Ilustración 30. Configuración Putty puerto serie

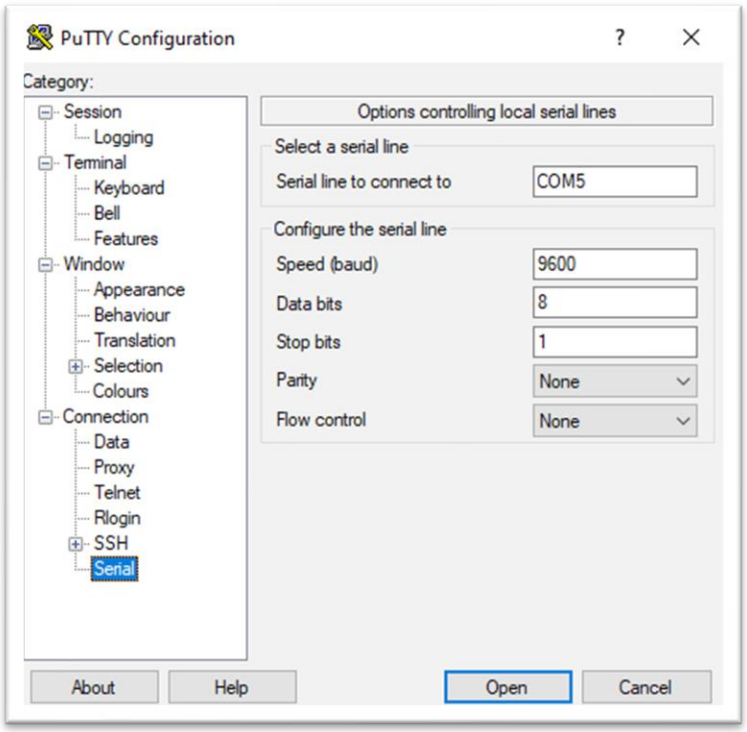


Ilustración 31. Características puerto serie para conexión

La arquitectura para este entorno de pruebas mantiene la idea del apartado 3.3, representar una LAN de una manera sencilla. En este caso se encuentra dentro de un entorno de maquetas, donde hay un switch que hace de puerta de enlace de la red local física hacia el router. A este switch se ha conectado el switch Cisco descrito anteriormente mediante un enlace *trunk* y se tiene comunicación con la centralita. Esto nos permite desplegar al menos dos teléfonos para hacer pruebas.

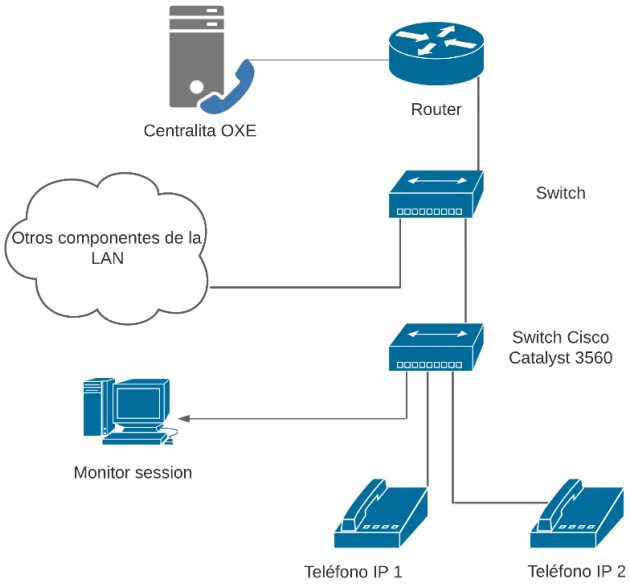


Ilustración 32. Arquitectura entorno de pruebas inicial

En este caso siguiendo la arquitectura propuesta se configuran las interfaces 20 y 22 del switch Cisco para conectar los terminales de VoIP:

```
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mls qos trust dscp

interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mls qos trust dscp
```

En ambas se realiza lo mismo, permiten el encapsulado del puerto con 802.1Q para poder marcar la VLAN y la prioridad. Están en modo *trunk* pues por ellos podrían tratarse VLANes distintas. En este entorno no se tomarán decisiones en función de la VLAN, aunque es necesario identificarlas porque el resto de componentes de red y la centralita están configuradas para utilizar la VLAN 21 en la parte de voz. Y por último se les indica

que confíen en el valor DSCP del paquete que reciben (frontera de confianza), de esta forma si se recibe una trama con *dot1q* mediante el mapeo de valores (se describe en detalle unos párrafos más adelante) se asigna la traducción a DSCP. Existen diversas formas de realizar la clasificación y marcado, en este ejemplo se ha optado por la configuración basada en el puerto con los comandos `mls qos` asociados a la interfaz. No permite tanta flexibilidad como con MQC (class-map y policy-map) pero tiene suficientes funciones como para demostrar la importancia del proceso de la clasificación y marcado.

Para poder capturar el tráfico que viaja por los puertos del switch se debe crear una sesión de monitorización en otro puerto para replicar este tráfico y poder mostrarlo en un software analizador de paquetes de red, conocido como *sniffer*, en este caso se usará Wireshark.

Mediante los siguientes comandos definimos la fuente y el destino de esta monitorización. Es importante indicar que en la interfaz de destino, por donde capturaremos el tráfico, se permita el encapsulado 802.1Q, de otra forma no podremos ver las tramas Ethernet con el etiquetado 802.1p/Q:

```
monitor session 1 source interface Fa0/20
monitor session 1 destination interface Fa0/2 encapsulation dot1q
```

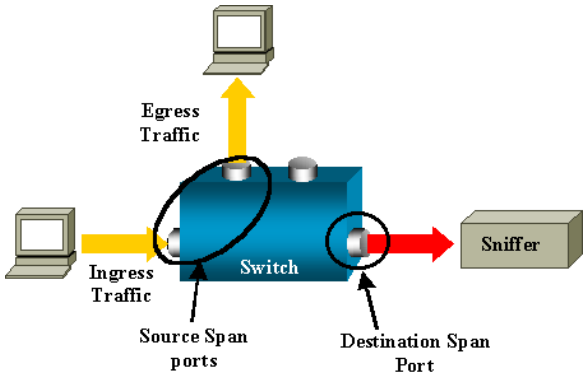


Ilustración 33. Estructura y funcionamiento sniffer de tráfico

Una vez hecha esta configuración, y dando por realizada toda la configuración y puesta en marcha de la centralita telefónica junto a la resolución de direccionamientos, y otros posibles aspectos básicos necesarios para establecer la comunicación pero que no son el objetivo de este documento, los teléfonos IP contactarán con la OXE y se registrarán en la extensión que se les indique.

El entorno de pruebas queda configurado, la conexión de los terminales descritos en los párrafos anteriores y los equipos utilizados corresponde con las imágenes tomadas que se muestran en la Ilustración 34.

Ilustración 34. Equipos implicados en el entorno de pruebas

Antes de comenzar a cambiar ciertos parámetros y ajustar el sistema para que aplique QoS en la LAN se observa que al establecer una llamada entre los terminales se muestra el encapsulamiento, la VLAN, y el DSCP:

No.	Time	Source	Destination	Protocol	Length	Info
1753	54.585884	10.10.1.14	10.10.1.19	UDP	218	32514 → 32514 Len=172
1754	54.596782	10.10.1.19	10.10.1.14	UDP	218	32514 → 32514 Len=172
1755	54.601615	10.10.1.14	10.10.1.19	UDP	218	32514 → 32514 Len=172
1756	54.617787	10.10.1.19	10.10.1.14	UDP	218	32514 → 32514 Len=172
1757	54.626139	10.10.1.14	10.10.1.19	UDP	218	32514 → 32514 Len=172
1758	54.637706	10.10.1.19	10.10.1.14	UDP	218	32514 → 32514 Len=172
1759	54.646678	10.10.1.14	10.10.1.19	UDP	218	32514 → 32514 Len=172

```
> Frame 1757: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface \Device\NPF_{E9E57F56-D135-4C4C-8F4D-5CB
> Ethernet II, Src: Sercomm_9e:a8:82 (78:81:02:9e:a8:82), Dst: AlcatelB_d5:8d:02 (00:80:9f:d5:8d:02)
v 802.1Q Virtual LAN, PRI: 5, DEI: 0, ID: 21
    101. .... .... .... = Priority: Voice, < 10ms latency and jitter (5)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0001 0101 = ID: 21
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.10.1.14, Dst: 10.10.1.19
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
      1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 200
    Identification: 0x6504 (25860)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xbe34 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.10.1.14
    Destination Address: 10.10.1.19
> User Datagram Protocol, Src Port: 32514, Dst Port: 32514
> Data (172 bytes)
```

Ilustración 35. Captura de Wireshark tráfico UDP con etiquetado

Estos parámetros son modificables en la centralita de manera global. Mediante el uso de diferentes clases de servicio es posible desplegar hasta 16 configuraciones distintas. Cada una aplica a un dominio IP. Más adelante se realizará una prueba con un terminal utilizando diferentes parámetros QoS.

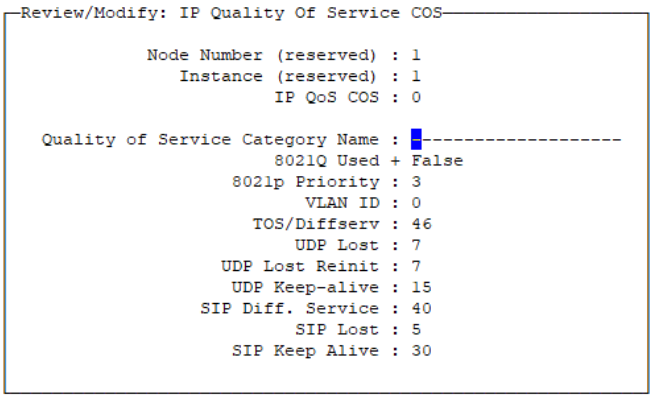


Ilustración 36. Configuración parámetros QoS en la OXE

Aunque se observa que el *802.1Q Used* no está activo, la trama sí llega con el etiquetado, esto se debe a que la OXE por defecto coloca el valor de VoIP. Sin embargo, para poder modificar el parámetro *8021p Priority* se debe colocar en *true*. En las siguientes trazas se observa una modificación de los parámetros. El valor del campo PRI pasa a ser 2, y el valor de DSCP a ser 45:

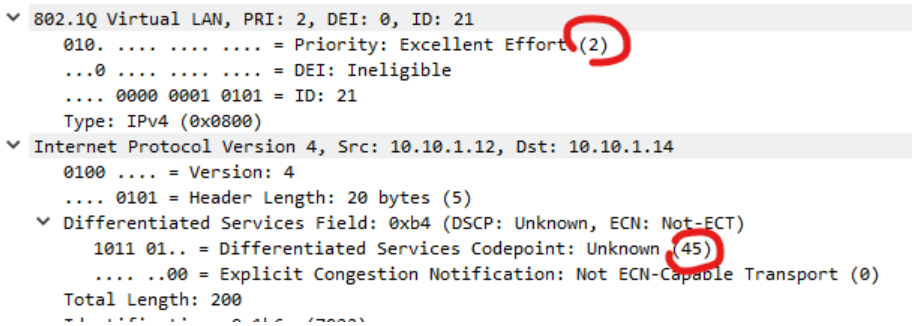


Ilustración 37. Valores de prioridad modificados por la OXE

Para implementar la VLAN se puede abordar de diferentes maneras, en este ejemplo se ha optado por una de las más sencillas. Consiste en indicar de manera manual en el propio terminal qué VLAN usará. Es por este motivo que en las trazas mostradas anteriormente

ya figuraba el valor ID: 21. De esta manera el mismo terminal realiza el *tagging* 802.1Q, añadiendo el VLAN ID que se indica manualmente:

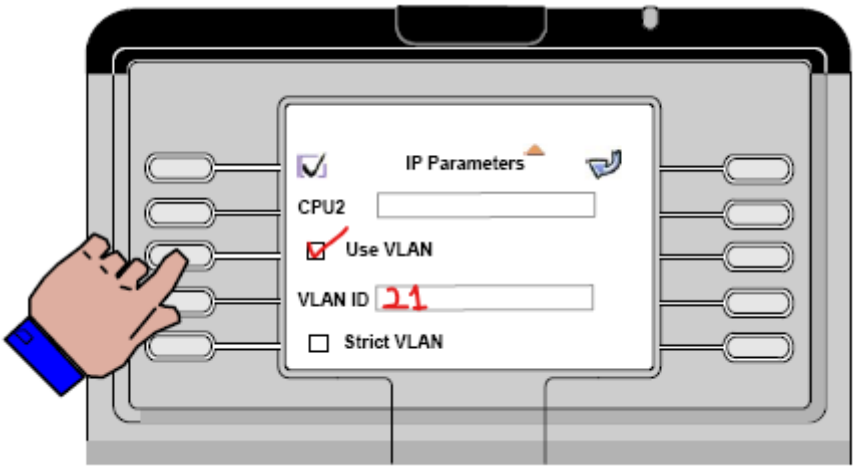


Ilustración 38. Configuración VLAN terminal

En el switch se dan de alta las dos VLANes, la VLAN 20 destinada a los datos y la VLAN 21 para la voz:

```
vlan 20
 name DATOS
!
vlan 21
 name VOZ
```

En este caso la clasificación no se hará por el ID de VLAN, pero podría ser una manera de identificar el tráfico y clasificarlo en función de ello. Sin embargo, se crean porque es importante tener al menos la VLAN de voz, ya que recordemos que este switch conecta con una red ya configurada en la que la voz viaja mediante la VLAN 21. Para un correcto funcionamiento y que el tagging de 802.1Q viaje en las tramas se identifica de esta manera.

Por defecto la calidad de servicio está desactivada en el switch, para poder activarla se debe lanzar el comando `mls qos` que activa la QoS de manera global. Tal y como se comentó al final del apartado 3.3 debe existir una relación entre los valores del marcado en el campo PRI (también llamado CoS) y el campo DSCP. El switch trae por defecto ciertos valores que mapean el DSCP con CoS y viceversa. Sin embargo, en este caso práctico se reescribirá ese mapeo para realizarlo de una forma más drástica, centrándose en VoIP, el resto no será importante y por ello le colocaremos la etiqueta de *Best Effort* (valor 0). Los comandos para aplicar estos cambios son:

```
mls qos map dscp-cos  8 9 10 11 12 13 14 15 to 0
mls qos map dscp-cos  16 17 18 19 20 21 22 23 to 0
mls qos map dscp-cos  24 25 26 27 28 29 30 31 to 0
mls qos map dscp-cos  32 33 34 35 36 37 38 39 to 0
mls qos map dscp-cos  41 42 43 44 45 47 49 50 to 0
mls qos map dscp-cos  51 52 53 54 55 57 58 59 to 0
mls qos map dscp-cos  60 61 62 63 to 0
mls qos map cos-dscp 0 0 0 0 0 46 48 56
mls qos
```

La tabla de mapeo queda de la siguiente manera, donde d1 corresponde al primer dígito y d2 al segundo dígito de DSCP. Por ejemplo, el valor 46 será el 5 en el primer caso y en el segundo el 5 será el 46:

```
Dscp-cos map:
     d1:d2    0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 00
      1 :    00 00 00 00 00 00 00 00 00 00
      2 :    00 00 00 00 00 00 00 00 00 00
      3 :    00 00 00 00 00 00 00 00 00 00
      4 :    05 00 00 00 00 00 05 00 06 00
      5 :    00 00 00 00 00 00 07 00 00 00
      6 :    00 00 00 00
 Cos-dscp map:
       cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  0  0  0  0 46 48 56
```

Es interesante destacar que al confiar en las tramas con marca DSCP y no alterar la configuración del mapeo de mutación, el valor DSCP no se modifica, pero el del CoS sí. Este se sobrescribe en función del mapeo DSCP-to-CoS.

Por tanto, cuando un paquete llega al switch, según la configuración actual, lo primero que se hará será evaluar la etiqueta que este lleve, en este caso como se le indica que confíe en DSCP será esta la que aplique. Una vez reconozca el valor, tras mapear si es necesario, se envía a una cola de ingreso donde según el estado de esta cola y la prioridad del paquete se evaluará qué se hace con él. Si las colas están congestionadas se aplican diferentes algoritmos, según la prioridad o se descarta o se envía a la cola de egreso. Una vez el paquete llega al switch el diagrama de flujo para aplicar QoS es el siguiente:

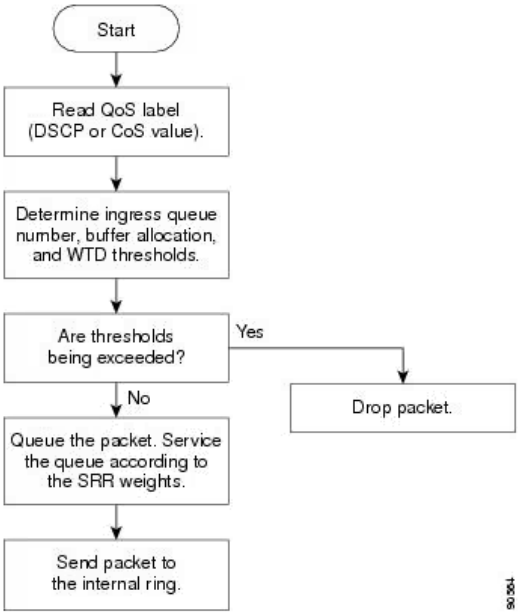


Ilustración 39. Diagrama de colas y procesado en los puertos de entrada [33]

Existen 2 colas de ingreso, las cuales se pueden configurar por pesos para dar diferentes características en cuanto a priorización del tráfico. Además, una de ellas puede identificarse como cola prioritaria para que en ella se garantice el ancho de banda. Al recibir el paquete/trama se coloca según su etiqueta de QoS en una cola de ingreso. Por defecto estos son los valores del mapeo del CoS/DSCP a las colas:

Tabla 12. Mapeo valores CoS-DSCP-Cola de ingreso

CoS	DSCP	Cola de ingreso
0	0 a 7	1
1	8 a 15	1
2	16 a 23	1
3	24 a 31	1
4	32 a 39	1
5	40 a 47	2
6	48 a 55	1
7	56 a 63	1

Cuando a una cola se le da prioridad se asigna un ancho de banda garantizado del total disponible. Por tanto, a efectos prácticos existen 2 colas, una de ellas con prioridad en la que se reserva un porcentaje del ancho de banda y lo que sobra de este ancho de banda se reparte entre las dos colas (nuevamente la prioritaria). Se podría decir que recibe su turno de transferencia de flujo por dos ocasiones.

En la cola es posible configurar el buffer, el ancho de banda, la prioridad y los dos umbrales que hay dentro de cada cola. Estos umbrales, llamados en inglés *threshold*, se basan en el mecanismo WTD (*Weighted tail drop*) ya que hasta ese umbral se permite el

almacenamiento de paquetes dependiendo del CoS/DSCP, una vez superado se descartan. Se observa en la siguiente figura a modo gráfico el llenado y descarte con un ejemplo de cola y los diferentes valores CoS que pueden ir llenando cada umbral. Los valores 6 y 7 son los considerados como más importantes ya que hasta que no esté llena la cola no se descartarán:

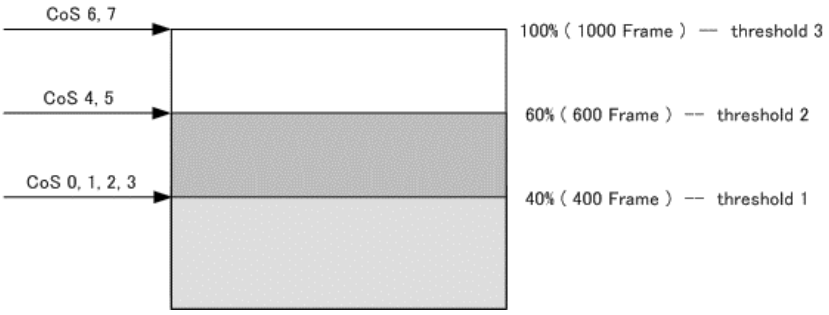


Ilustración 40. Llenado de colas hasta el límite según su CoS

El proceso global para las colas de entrada quedaría esquematizado de la siguiente manera. Donde mediante el algoritmo de *Shared Round Robin* se envía a una de las dos colas, según el marcado se va dando entrada a los paquetes/tramas en el anillo interno del switch, del cual saldrán hacia su destino en función de la gestión que se realice en las colas de salida (se detalla más adelante).

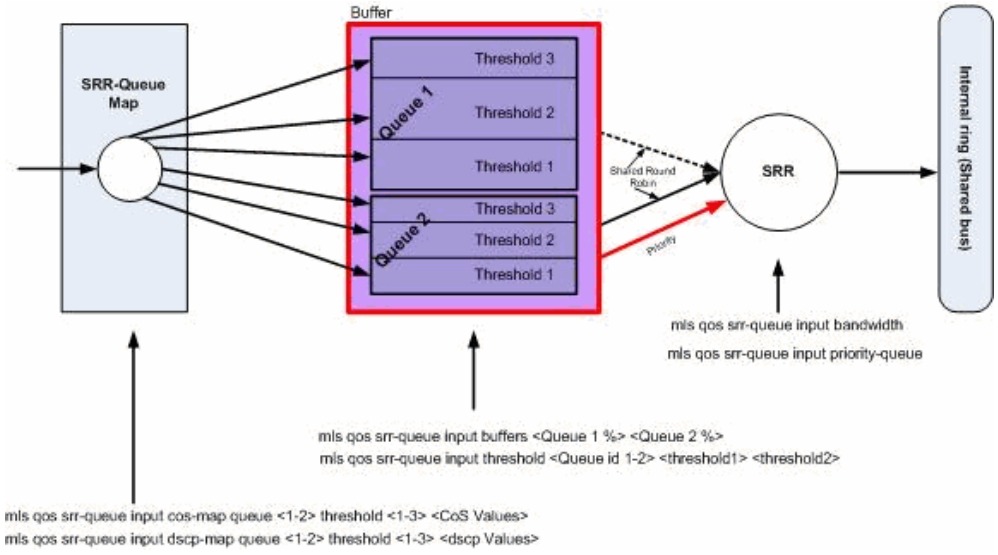


Ilustración 41. Enrutamiento y programación con garantía de calidad de servicio [34]

En *Shared Round Robin*, se utilizan múltiples colas de prioridades. Cada cola está asociada con un nivel de prioridad distinto, y se asigna un quantum específico a cada una de ellas. Cada proceso recibe un intervalo de tiempo predeterminado llamado *quantum* o *slice*, durante el cual se le permite ejecutarse. Después de que cada proceso haya utilizado su *quantum*, el planificador pasa al siguiente proceso en la cola. Esto se repite en un ciclo continuo. Los procesos con mayor prioridad se colocan en las colas de prioridad más altas, mientras que los de menor prioridad se colocan en las colas de prioridad más bajas. En

este caso, se asemejan a las colas *Weighted Fair Queuing* vistas al final del capítulo QoS en una LAN, ya que se clasifican según sus clases con diferentes pesos.

Tras dirigir los datos al bus compartido por todos los puertos del switch, comienza el proceso de QoS de salida. En este caso es posible asignar 2 grupos de colas, llamados *queue-set*, los cuales tienen 4 colas cada uno. En cada cola existe la posibilidad de configurar los umbrales para realizar descarte ponderado al igual que en las colas de entrada. Se debe tener en cuenta que los parámetros de cola de ingreso son globales, no se basan por puertos, sin embargo, los de salida sí se configuran por puertos. Otra diferencia reside en la forma que puede actuar el algoritmo *Round* Robin, en entrada solo existe la forma compartida, *Share Round Robin*, en salida es posible configurarlo en el modo "formato", *Shaped Round Robin*. En el modo *share*, las colas comparten el ancho de banda según los pesos configurados, en este caso se garantiza según el peso dado. En el modo *shaped*, las colas de salida se aseguran un porcentaje de ancho de banda, y a su vez este porcentaje limita el uso del ancho de banda impidiendo usar más que la cantidad designada. En la siguiente figura se observa el diagrama de las colas de salida y los valores por defecto que aplica el Catalyst 3560.

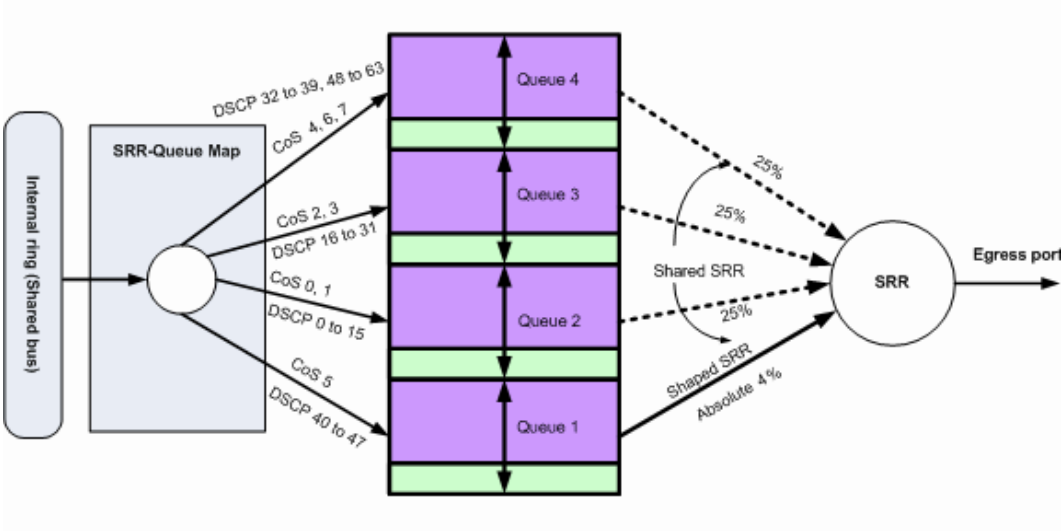


Ilustración 42. Diagrama y valores por defecto en las colas de salida del puerto del switch [34]

Los dos colores de las colas indican el buffer de cada una, en morado el *common pool* que sería el grupo común, y en verde el *reserved pool* que sería el reservado para dicha cola. Se configura en porcentajes y la suma delos 4 debe dar el 100%.

En las pruebas que se exponen a continuación para comenzar se dirige todo el tráfico a la primera cola, como no hay configurado ningún umbral es indiferente a cuál de ellos vaya, aunque por defecto será el *threshold* 1. Los comandos para alterar los valores por defecto del switch dirigiendo todos los paquetes a la cola 1 son los siguientes:

```
mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3 4 6 7
mls qos srr-queue output cos-map queue 1 threshold 1 5
mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 1 threshold 1 8 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 1 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 1 threshold 1 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 1 threshold 1 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 1 threshold 1 40 41 42 43 45 47
mls qos srr-queue output dscp-map queue 1 threshold 1 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 1 threshold 1 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 1 threshold 1 46
```

Se debe tener en cuenta el objetivo de esta demostración, entendiendo los conceptos y las posibilidades, pero siendo conscientes de que el caso expuesto busca generar conflictos en la red para intentar resolverlos aplicando QoS. Por ello se opta por utilizar la gestión de colas de salida exclusivamente, ya que permiten el uso de la función *shaped* y por tanto limitar el ancho de banda de la interfaz utilizada en función de la prioridad.

Con la intención de abarcar y demostrar la mayoría de la teoría expuesta en los apartados previos de esta memoria, se busca tener un entorno controlado donde el ancho de banda, al establecer una llamada esté muy próximo a rebasarse de esta forma si se introduce más tráfico por el canal se producirá congestión y comenzarán a experimentarse los problemas relacionados con esta condición. Para reducir estos efectos se aplicará QoS dando prioridad a los paquetes identificados con la etiqueta DSCP 46 o bien las tramas con CoS 5.

Antes de comenzar con la calidad de servicio se debe necesitar aplicarla, para intentar ocupar el máximo ancho de banda se establece el códec G.722 en la OXE en los dominios donde se encuentran los terminales instalados, ya que además de utilizar una velocidad de 64 Kbit/s suele considerarse uno de los códecs con mejor MOS. El valor del ancho de banda consumido en Ethernet, debido a las cabeceras, será de 87’2 kbps [35]. Como en esta prueba se busca limitar el ancho de banda de manera que se genere congestión, este será el valor de referencia para aplicar dicha limitación.

La interfaz tiene capacidad de hasta 100 Mbps, por lo que con una sola llamada no es posible ocupar todo el ancho de banda y generar congestión. Para forzar el límite del ancho de banda se utiliza el comando `srr-queue bandwidth shape 2000 2000 2000 2000` el cual permite limitar el ancho de banda de las 4 colas de salida que existen en la estructura, cada valor dado es el inverso del porcentaje total permitido. De esta forma se limita todo el conjunto de colas sin importar quién se dirige a estas (no hay prioridad). El cálculo de la velocidad permitida en la salida de las tramas/paquetes de la interfaz es el siguiente:

$$2.000 \rightarrow \frac{100}{2.000} Mbps = 0'05\ Mbps = 51'2\ Kbps$$

Con esta situación forzamos la congestión en la interfaz de tal manera que se comienzan a producir fallos y la calidad de la comunicación disminuye. El valor de ejemplo es un caso extremo para demostrar que si solo queda disponible un pequeño porcentaje del total del ancho de banda realmente existen errores.

Al realizar una llamada de prueba podemos observar en el analizador las estadísticas que este recopila. Donde se observa la gran pérdida de paquetes, entorno al 50% en ambos sentidos, RTP debido a la congestión:

Source Address	Sourc	Destination	Destir	SSRC	Start T	Duración	Payload	Paquet	Lost
10.10.1.12	32514	10.10.1.14	32514	0...6	2....20	18.05	g722	408	452 (52.6%)
10.10.1.14	32514	10.10.1.12	32514	0...d	2....37	17.76	g722	508	354 (41.1%)

Ilustración 43. Información RTP

El mayor porcentaje de los paquetes del flujo de comunicación se deben al tráfico directo de la voz, el cual se encapsula en RTP. El bit rate calculado por el *sniffer* es el siguiente:

Protocolo	Porcentaje de paquetes	Paquetes	Porcentaje de bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1033	100.0	211657	75 k	0	0	0	1033
Ethernet	100.0	1033	6.8	14462	5185	0	0	0	1033
Internet Protocol Version 4	0.4	4	0.0	80	28	0	0	0	4
User Datagram Protocol	0.4	4	0.0	32	11	0	0	0	4
802.1Q Virtual LAN	99.6	1029	2.3	4826	1730	0	0	0	1029
Logical-Link Control	4.6	48	1.1	2256	808	0	0	0	48
Internet Protocol Version 4	92.9	960	9.1	19200	6883	0	0	0	960
User Datagram Protocol	91.8	948	3.6	7584	2719	0	0	0	948
UA/UDP Encapsulation Protocol	2.9	30	0.7	1469	526	17	69	24	30
Real-Time Transport Protocol	88.7	916	74.4	157552	56 k	916	157552	56 k	916
Data	0.2	2	0.2	376	134	2	376	134	2
Internet Control Message Protocol	1.2	12	1.2	2496	894	0	0	0	12
Configuration Test Protocol (loopback)	0.2	2	0.0	92	32	0	0	0	2
Address Resolution Protocol	1.8	19	0.4	874	313	19	874	313	19

Ilustración 44. Estadísticas según jerarquí de protocolos

Comparando con el bit rate de las estadísticas que nos ofrece Wireshark concretamente para los paquetes del protocolo RTP vemos que hay una ligera diferencia entre el cálculo teórico del límite y el real. Esto se debe a que la monitorización se realiza con la interfaz Fa0/20 como fuente, tanto los paquetes entrantes como salientes, pero la otra interfaz con la que se establece la comunicación no está limitada y su *bit rate* es mucho mayor, al mostrarse las estadísticas clasificadas por protocolos incluyen ambos sentidos. Existen otros valores dentro de Wireshark para obtener una estimación del *bit rate*, por ejemplo en la pestaña “Telefonía” la sección “RTP Stream Analysis” se detalla el ancho de banda de cada paquete RTP. El valor medio es de 46.40 kbps. Muchos paquetes se muestran con un código de secuencia erróneo ya que no llegan correctamente.

Wireshark · RTP Stream Analysis · Llamada_001.pcapng

Stream 0 | Gráfica

Stream

10.10.1.14:32514 →
10.10.1.12:32514

SSRC	0x01518e2d
Max Delta	71.833000 ms @ 924
Max Jitter	13.538405 ms
Mean Jitter	8.282252 ms
Max Skew	-558.999000 ms
RTP Packets	508
Expected	862
Lost	354 (41.07 %)
Seq Errs	344
Start at	2.363037 s @ 25
Duration	17.76 s
Clock Drift	-108 ms
Freq Drift	7903 Hz (-0.61 %)

Paquete	Sequence	Delta (ms)	Jitter (ms)	Skew	Ancho de banda	Marker	Estado
123	11798	34.750000	13.342643	-516.867000	46.40		✓
125	11799	34.663000	13.425166	-531.530000	46.40		✓
128	11800	35.237000	13.538405	-546.767000	46.40		✓
131	11802	35.129000	12.996693	-541.896000	46.40		Wrong sequence numbe
134	11804	34.527000	12.526462	-536.423000	46.40		Wrong sequence numbe
136	11805	34.746000	12.665183	-551.169000	46.40		✓
140	11807	35.450000	12.157984	-546.619000	46.40		Wrong sequence numbe
143	11809	34.511000	11.741172	-541.130000	46.40		Wrong sequence numbe
146	11811	34.914000	11.325224	-536.044000	46.40		Wrong sequence numbe
148	11812	34.805000	11.542710	-550.849000	46.40		✓
151	11814	34.689000	11.153228	-545.538000	46.40		Wrong sequence numbe
154	11816	35.356000	10.746402	-540.894000	46.40		Wrong sequence numbe
157	11818	34.662000	10.408376	-535.556000	46.40		Wrong sequence numbe
161	11819	34.648000	10.673353	-550.204000	46.40		✓

Ilustración 45. RTP Stream Analysis

Un análisis interesante que nos permite la herramienta es el de las secuencias RTP, además del anterior dato del ancho de banda se puede ver la forma de onda del audio transferido en la comunicación. En negro podemos ver la onda correspondiente a la generada en el terminal con IP 10.10.1.12, el cual envía sin problemas esta información vía RTP al otro terminal. En azul se observa la señal que genera el terminal cuya IP es la 10.10.1.14, esta sin embargo si presenta problemas, aunque se genera correctamente luego es enviada a la interfaz 20, en la cual está aplicado el límite de ancho de banda a la salida. Por esto los paquetes de salida de la interfaz (visto desde el punto de vista de la interfaz FastEthernet0/20) sufren congestión y se pierden, ocasionando problemas en la comunicación y viéndose reflejado en la figura. Al inicio la señal de ambos micrófonos es la misma (se habla a la vez a ambos micrófonos), pero se observa mediante las flechas rojas situadas a la izquierda como la señal azul tiene un retardo mucho mayor, la señal se retarda y por eso aparece desplazada a la derecha. Además de una gran pérdida de información la cual el sistema intenta interpolar en medida de lo posible, aumentando el detalle de la onda se observa en la Ilustración 47.

Ilustración 46. Forma de onda señal transferida por RTP

Si se detalla en el eje de abscisas, siguiendo la leyenda, se observa las pérdidas de señal debidas a la congestión y el descarte de paquetes. La línea no es continua, las marcas de la leyenda están solapadas, pero indican el error de los paquetes. Estos errores se traducen en la percepción del usuario que está al otro lado del terminal que recibe estas secuencias erróneas como retardos, sonido metálico, clicks debido a interrupciones. En general es imposible entablar una comunicación. Por tanto se podría afirmar que si hubiera que darle un MOS a esta prueba sería lo más bajo posible.

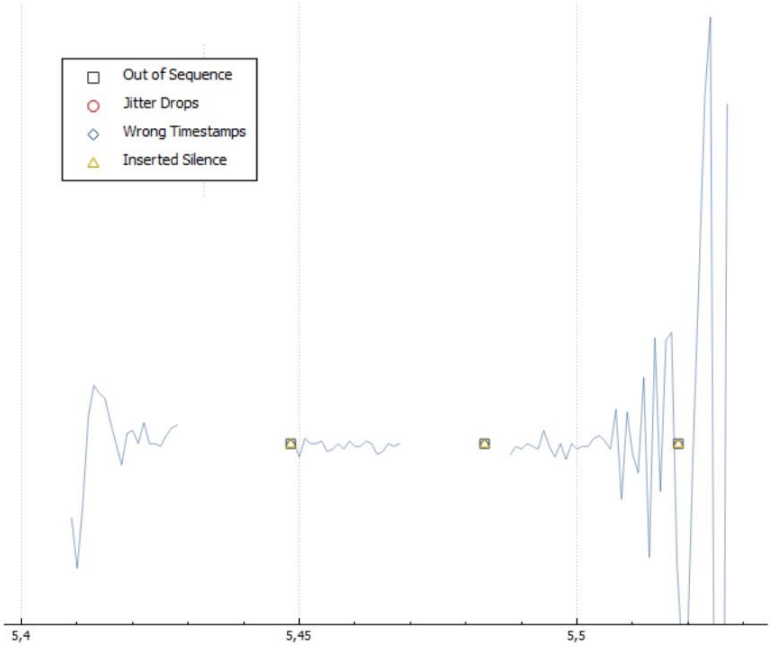


Ilustración 47. Detalle de forma de onda con grandes pérdidas

Otra forma de monitorización para añadir información y comprender con mayor exactitud qué ocurre en la llamada consiste en consultar las estadísticas de la propia interfaz del

switch. En ella vemos los paquetes marcados con etiqueta DSCP que entran y salen de la interfaz agrupados en filas con 5 valores por fila desde el DSCP 0 hasta el 64, las tramas con la etiqueta CoS que llegan y salen de la interfaz también agrupadas en filas, además de la información de las 4 colas de salida del *queue-set* 1, con los umbrales de cada cola (en este caso sin alterar el valor de cada umbral). Los que se han encolado, indicando qué cola, y los que se han descartado de cada cola.

```
   dscp: incoming
-------------------------------
  0 -  4 :     1              0              0              0              0
  5 -  9 :     0              0              0              0              0
 10 - 14 :     0              0              0              0              0
 15 - 19 :     0              0              0              0              0
 20 - 24 :     0              0              0              0              0
 25 - 29 :     0              0              0              0              0
 30 - 34 :     3              0              0              0              0
 35 - 39 :     0              0              0              0              0
 40 - 44 :     0              0              0              0              0
 45 - 49 :     0            422              0              0              0
 50 - 54 :     0              0              0              0              6
 55 - 59 :     0              0              0              0              0
 60 - 64 :     0              0              0              0
   dscp: outgoing
-------------------------------
  0 -  4 :    18              0              0              0              0
  5 -  9 :     0              0              0              0              0
 10 - 14 :     0              0              0              0              0
 15 - 19 :     0              0              0              0              0
 20 - 24 :     0              0              0              0              0
 25 - 29 :     0              0              0              0              0
 30 - 34 :     0              0              0              0              0
 35 - 39 :     0              0              0              0              0
 40 - 44 :     0              0              0              0              0
 45 - 49 :     0            508              0              0              0
 50 - 54 :     0              0              0              0              6
 55 - 59 :     0              0              0              0              0
 60 - 64 :     0              0              0              0
```

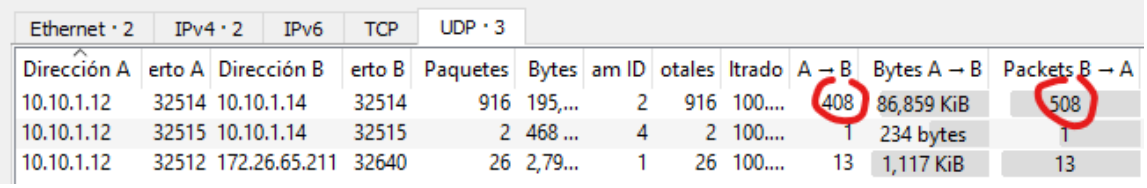
```
  cos: incoming
-------------------------------
  0 -  4 :   24            0            0            3            0
  5 -  7 :  422            0            0
  cos: outgoing
-------------------------------
  0 -  4 :   29            0            0            0            0
  5 -  7 :  508            0            0

output queues enqueued:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:    523           0            0
 queue 1:     22           0          129
 queue 2:      0           0            0
 queue 3:      0           0            0

 output queues dropped:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:    374           0            0
 queue 1:      0           0            0
 queue 2:      0           0            0
 queue 3:      0           0            0
```

En negrita se subrayan los valores a considerar, el resto que se observan se debe a otro tipo de tráfico que la sesión de monitorización implementada en la interfaz captura, paquetes broadcast o de información del propio switch.

Estas estadísticas hacen referencia a los paquetes/tramas que llegan a la interfaz, en este caso la utilizada es la FastEthernet0/20 (donde está conectado el terminal con IP 10.10.1.12) del switch de pruebas. Por ello las estadísticas identificadas como *incoming* (entrantes) deben tenerse en cuenta desde el punto de vista de la interfaz. Lo mismo aplica al tráfico saliente, todo el que pasa por la interfaz en sentido contrario se enumera como *outgoing*. En el caso de las colas de salida, la información interesante para esta prueba es saber que el tráfico está dirigido hacia la primera cola, la 0 (esta es la cola 1 en la configuración, hay un cambio de nomenclatura, no se debe confundir), y los umbrales (*threshold*) no están configurados, por ello figura la mayoría del tráfico en el primero. Los paquetes residuales de la segunda cola se deben a paquetes de control o broadcast del propio switch y el terminal. Además se observa que existe congestión en el flujo de salida de la interfaz, pues se descartan un número elevado de paquetes, comparado con el total que circulan en este ejemplo. En los siguientes ejemplos será más útil esta información.

Los resultados esperados son los obtenidos pues actualmente los terminales etiquetan con DSCP 46 y COS 5 sus comunicaciones, a pesar de que se cuelan algunos paquetes de control que pueden hacer variar el resultado mostrado en la estadística del switch con el de

los datos capturados por el *sniffer*, el número total es próximo en cada caso. A la interfaz llegan del orden de 422 paquetes con DSCP 46 y de ella salen del orden de 508 paquetes con la misma etiqueta. Tal y como se muestra en la siguiente imagen con las estadísticas del tráfico RTP:



Ethernet · 2 | IPv4 · 2 | IPv6 | TCP | UDP · 3

Dirección A	erto A	Dirección B	erto B	Paquetes	Bytes	am ID	otales	ltrado	A → B	Bytes A → B	Packets B → A
10.10.1.12	32514	10.10.1.14	32514	916	195,...	2	916	100....	408	86,859 KiB	508
10.10.1.12	32515	10.10.1.14	32515	2	468 ...	4	2	100....	1	234 bytes	1
10.10.1.12	32512	172.26.65.211	32640	26	2,79...	1	26	100....	13	1,117 KiB	13

Ilustración 48. Estadísticas Wireshark paquetes entrantes y salientes

Gracias a la recopilación de la información que se transfieren los terminales mediante el protocolo RTCP existe un método más para obtener información acerca la comunicación establecida entre los dos terminales. Esta información se recopila gracias al sistema de Alcatel, donde mediante el uso de *Tickets IP* se pueden conocer una estimación de los paquetes RTP recibidos y enviados, el *jitter* y múltiples valores relacionados con la QoS. Para esta llamada los tickets se pueden consultar más adelante en el anexo. A destacar de esta información los campos 22, 23 y 24, donde se indica el número de paquetes RTP enviados, recibidos y perdidos.

Analizando todos estos datos podemos confirmar lo descrito al inicio sobre la percepción del audio. La calificación del MOS en esta llamada sería muy baja debido a los altos valores de pérdidas, *jitter* y en general errores. Cuando se establece esta llamada, en uno de los sentidos hay pérdidas de paquetes. La interfaz está congestionada (en este caso debido al límite impuesto y no por gran cantidad de tráfico como tal), y el switch comienza a descartar paquetes cuando se rebosa su *buffer*. Por ello se producen retardos apreciables y micro cortes que hacen la comunicación prácticamente imposible en uno de los sentidos.

Ahora se sabe que el flujo de datos que llegue por la interfaz FastEthernet0/20 tendrá problemas de congestión. Una vez limitado el ancho de banda en la interfaz del switch, se debe analizar qué ocurre cuando a esta interfaz llega tanto tráfico que se rebosa ese límite impuesto. Para ello se procede con la conexión en cascada de un segundo terminal tal y como se muestra en el diagrama siguiente.

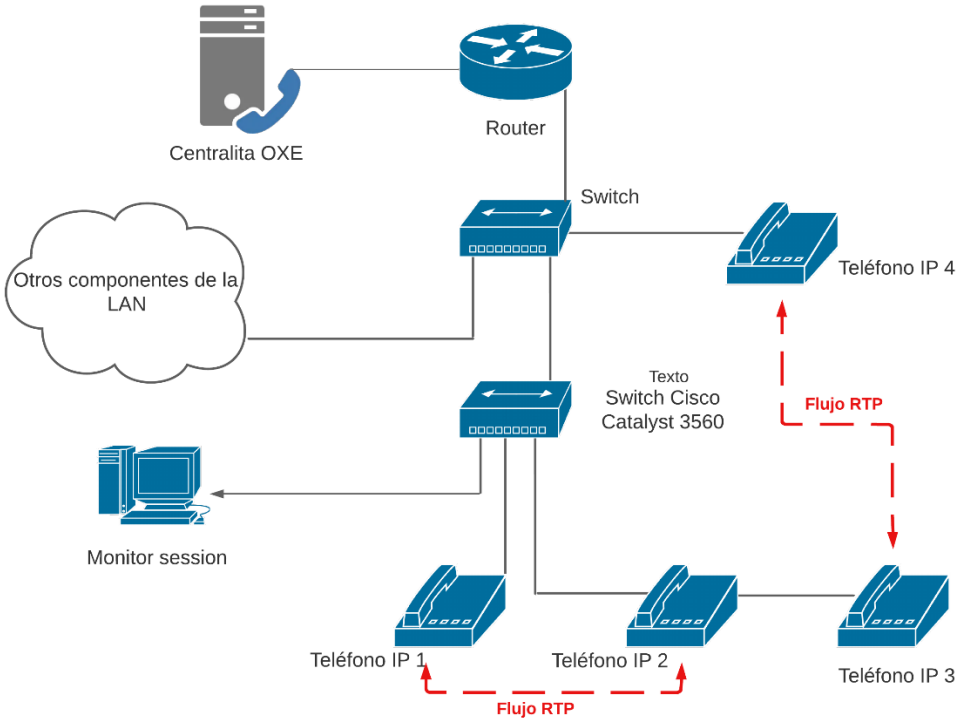


Ilustración 49. Arquitectura con 2 terminales generando tráfico en misma interfaz

Los terminales IP Touch poseen un switch interno que permite la conexión de uno o más dispositivos detrás del propio terminal. El uso habitual es colocar un PC en este puerto para evitar la necesidad de realizar el despliegue de dos cables de red al puesto donde se encuentran el teléfono fijo IP y el PC del usuario. La OXE permite modificar el puerto destinado a conectar un PC en modo puente, se le indica que filtre la trama recibida en dicho puerto o no. En este caso para diferenciar del flujo de datos con prioridad (la llamada VoIP) se indica que no filtre ese puerto para que se pueda tratar como tráfico no prioritario en el switch según las etiquetas que le asignemos al terminal en cuestión.

Los terminales se registran contra la centralita en un dominio IP. Este dominio define diversos parámetros, desde el rango de IPs hasta las características en red de los terminales que se encuentran en él. Para poder tener dos terminales con diferente etiquetado de prioridad se debe crear un domino que se llamará “No prioritario” y a él se asociarán valores DSCP y CoS distintos de los que se estaban usando. Mediante otro dominio IP con otra categoría de servicio indicamos que este terminal tenga un DSCP y CoS diferente al de la voz IP, para que tenga menor prioridad. En conreto los valores son CoS 3 y DSCP 30:

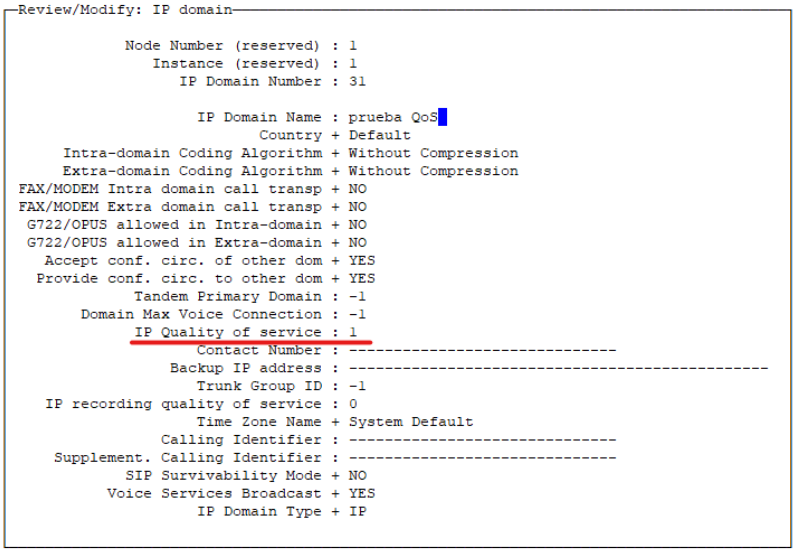


Ilustración 50. Dominio IP diferente con distinta QoS

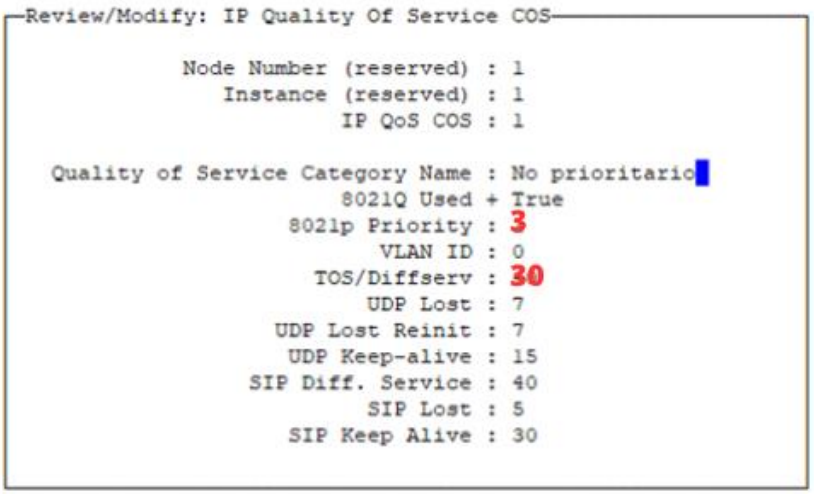


Ilustración 51. Definición de parámetros QoS para el dominio no prioritario

Con tal de evitar el exceso de pérdidas de paquetes, lo cual podría ocasionar la pérdida momentánea de conexión y con ello el reinicio de los terminales, se ajusta el límite del ancho de banda en esta interfaz donde se generará tráfico de dos teléfonos distintos. Comando utilizado `srr-queue bandwidth shape 1200 1200 1200 1200.`

$$1.200 \rightarrow \frac{100}{1200}\ Mbps = 0'083\ Mbps = 85'33\ Kbps$$

Al analizar la traza que se captura mediante el *sniffer*, vemos como la onda de la señal nos da bastante información acerca de lo ocurrido en la llamada.

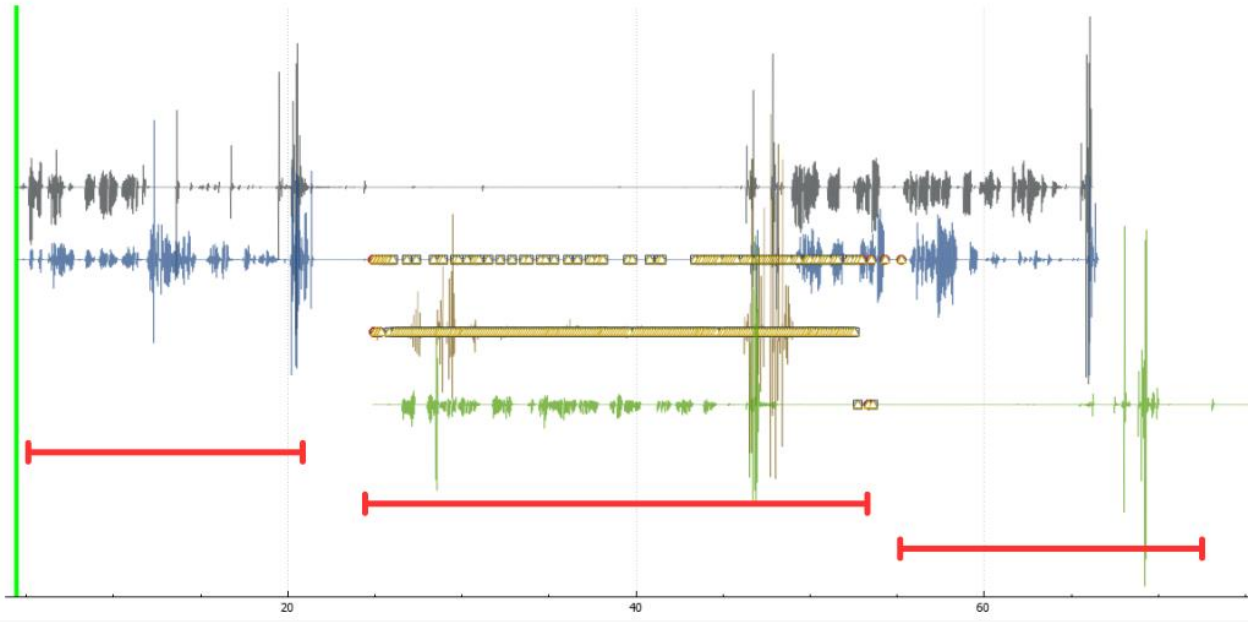


Ilustración 52. Segunda llamada establecida genera congestión en interfaz

En la figura se observan 3 zonas bien definidas, marcadas mediante las franjas rojas de la Ilustración 52. En la primera se establece la llamada y se comunican los terminales con IP 10.10.1.12 y 10.10.1.14, sin ningún problema con bastante fluidez, algún pequeño retardo casi inapreciable. Sin embargo, conforme la segunda llamada es establecida comienzan los problemas. A pesar de estar el tráfico etiqueta de manera distinta, actualmente este no tiene diferente trato y, por tanto, no hay prioridad. Conforme la segunda llamada comienza se produce congestión. Esta congestión afecta a ambas llamadas, sobre todo más a la segunda, llegando incluso en la tercera zona identificada a causar tales problemas que el terminal se reinicia ya que considera que ha sufrido una pérdida de conectividad con la centralita. El ancho de banda disponible está ocupado, no es posible añadir más información por él y todos los paquetes se comienzan a descartar, este aspecto se detalle con valores en la conclusión final de este capítulo, en la Tabla 13. Comparativa límites y bit rate en pruebas. Es por esto que en el eje de abscisas la señal amarilla, la causante de los problemas, se corta al final de la segunda zona identificada. Esto también afecta a las estadísticas donde el envío de paquetes RTP se ve cortado en una dirección. De hecho, la OXE no es capaz de generar el *Ticket IP* correspondiente a este terminal pues no ha recibido la información de cierre y estos datos se pierden.

En las estadísticas recopiladas en la interfaz del switch ocurre un cambio sustancial, ahora se identifican paquetes con diferente DSCP y CoS debido al nuevo terminal introduciendo tráfico en la interfaz. Estos paquetes en entrada se identifican con su etiqueta de origen, pero en salida según el mapeo todo lo que no sea DSCP 46 se convierte en 0, lo mismo para la etiqueta CoS. En este caso en salida no hay la misma cantidad de paquetes que han entrado con DSCP 30, ya que las pérdidas son extremadamente grandes. Así se refleja en la Ilustración 53.

Source Address	Sourc	Destina	Destir	SSRC	Start Time	Duración	Payload	Paquetes	Lost
10.10.1.12	32514	10.....14	32514	0...7	4.424054	61.81	g722	3092	0 (0.0%)
10.10.1.14	32514	10.....12	32514	0...8	4.518050	61.62	g722	2946	136 (4.4%)
10.10.1.19	32514	10.....24	32514	0...a	24.824886	27.73	g722	339	1036 (75.3%)
10.10.1.24	32514	10.....19	32514	0...6	24.911024	59.65	g722	2982	2 (0.1%)

Ilustración 53. Información RTP 2 llamadas con congestión

dscp: incoming

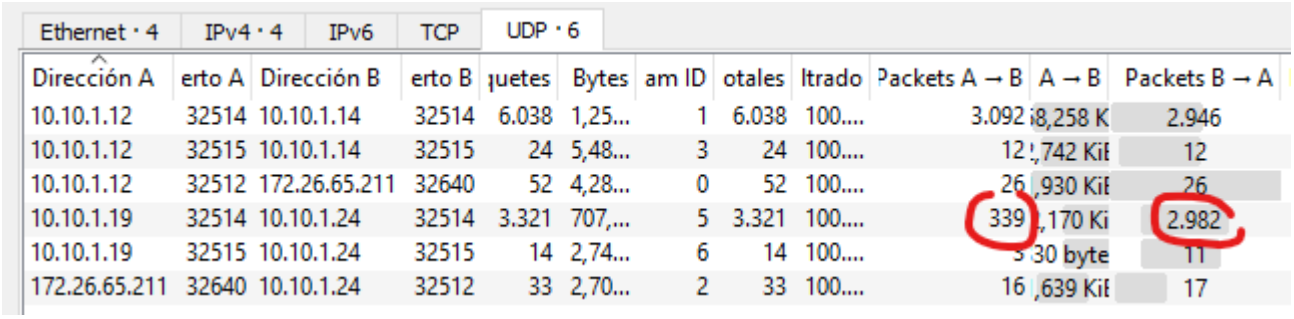
0 - 4 :	23	0	0	0	0
5 - 9 :	0	0	0	0	0
10 - 14 :	0	0	0	0	0
15 - 19 :	0	0	0	0	0
20 - 24 :	0	0	0	0	0
25 - 29 :	0	0	0	0	0
30 - 34 :	**2999**	0	0	0	0
35 - 39 :	0	0	0	0	0
40 - 44 :	0	0	0	0	0
45 - 49 :	0	**3117**	0	2	0
50 - 54 :	0	0	0	0	0
55 - 59 :	0	0	0	0	0
60 - 64 :	0	0	0	0	

dscp: outgoing

0 - 4 :	**554**	0	0	0	0
5 - 9 :	0	0	0	0	0
10 - 14 :	0	0	0	0	0
15 - 19 :	0	0	0	0	0
20 - 24 :	0	0	0	0	0
25 - 29 :	0	0	0	0	0
30 - 34 :	0	0	0	0	0
35 - 39 :	0	0	0	0	0
40 - 44 :	0	0	0	0	0
45 - 49 :	0	**2946**	0	0	0
50 - 54 :	0	0	0	0	9
55 - 59 :	0	0	0	0	0
60 - 64 :	0	0	0	0	

```
cos: incoming
-------------------------------
  0 -  4 :   49            0            0         2999            0
  5 -  7 : 3117            0            0
  cos: outgoing
-------------------------------
  0 -  4 :  582            0            0            0            0
  5 -  7 : 2946            0            0
  output queues enqueued:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:        3532           0            0
 queue 1:           0           0          343
 queue 2:           0           0            0
 queue 3:           0           0            0

  output queues dropped:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:        1199           0            0
 queue 1:           0           0            0
 queue 2:           0           0            0
 queue 3:           0           0            0
```

Analizando ahora los resultados se observa que se identifican paquetes entrantes a la interfaz con la etiqueta DSCP 30, tal y como se había configurado en el marcado del propio terminal. La mejor manera de comprobarlo es contrastar con las estadísticas del *sniffer*. Donde vemos que en la comunicación entre los terminales con IPs 10.10.1.19 y 10.10.1.24 los paquetes identificados en RTP son los siguientes:



Ethernet · 4 | IPv4 · 4 | IPv6 | TCP | UDP · 6

Dirección A	erto A	Dirección B	erto B	uetes	Bytes	am ID	otales	ltrado	Packets A → B	A → B	Packets B → A
10.10.1.12	32514	10.10.1.14	32514	6.038	1,25...	1	6.038	100....	3.092	8,258 K	2.946
10.10.1.12	32515	10.10.1.14	32515	24	5,48...	3	24	100....	12	,742 Kil	12
10.10.1.12	32512	172.26.65.211	32640	52	4,28...	0	52	100....	26	,930 Kil	26
10.10.1.19	32514	10.10.1.24	32514	3.321	707,...	5	3.321	100....	339	,170 Ki	2.982
10.10.1.19	32515	10.10.1.24	32515	14	2,74...	6	14	100....	3	30 byte	11
172.26.65.211	32640	10.10.1.24	32512	33	2,70...	2	33	100....	16	,639 Kil	17

De la IP 10.10.1.24 salen, por tanto llegan a la interfaz, del orden de casi 3000 paquetes, coincidiendo este valor con los casi 3000 paquetes con DSCP 30 identificados en *incoming* por las estadísticas del switch. De la IP 10.10.1.19 salen del orden de casi 600 paquetes solamente, debido a la gran pérdida que ocurre por culpa de la congestión.

En los tickets registrados por los terminales se aprecia en el campo 22, 23 y 24 los valores relacionados con RTP, sin embargo, al reiniciarse el terminal debido la alta congestión el ticket más interesante se ha perdido, por ello no se incluye esta inform. El del terminal

conectado en cascada al otro terminal y a la interfaz limitada, en él se verían una cantidad similar de pérdidas como se ven en Wireshark o las estadísticas de la propia interfaz.

Ahora se aplicarán medidas de QoS para dar prioridad al tráfico identificado como VoIP, dejando el resto del tráfico a merced de la disponibilidad del ancho de banda y los recursos disponibles. Para ello se indica una cola sin restricción a los paquetes que lleven DSCP=46 y CoS 5:

```
mls qos srr-queue output cos-map queue 2 5
mls qos srr-queue output dscp-map queue 2 46
```

La cola de salida ahora es la 2, en lugar de la 1. El tráfico que no cumple con esta condición sigue dirigiéndose a la 1. De esta manera se corrige la posible congestión que existía en la interfaz, al asignar cada tráfico según su marcado a una cola diferente se da comienzo al principio fundamental de la calidad de servicio, a la clasificación mediante la diferenciación de etiquetas.

La llamada tiene la mejor calidad conseguida hasta ahora en los ejemplos dados, a pesar de la posibilidad de congestión, se consigue entablar una conversación con éxito donde se puede intercambiar información de forma clara. Si del MOS se tratara, para este caso podría darse, comparando con el resto de pruebas el valor más alto de todos. A pesar de existir *jitter* este es bajo, no hay pérdidas de paquetes, coincidiendo estas premisas con las mismas que relacionaban un valor alto de MOS como se vio en el desarrollo teórico. La forma de onda se muestra correctamente en los 4 sentidos posibles, los niveles más altos no coinciden en las dos llamadas pues físicamente están separados (por parejas), cuando se prueban dos de ellos los otros dos quedan alejados y no perciben el audio:

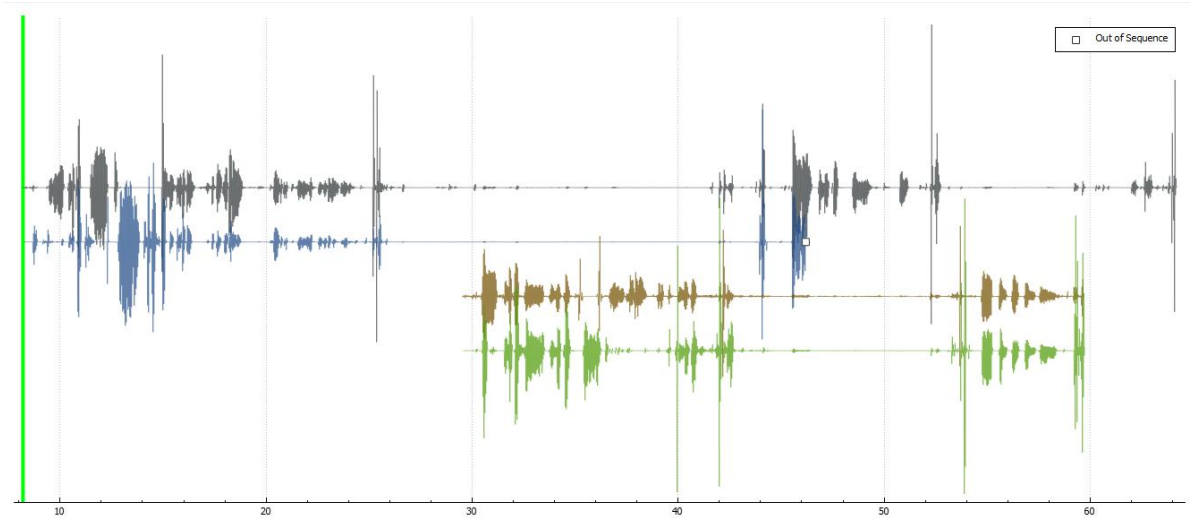


Ilustración 54. Forma de onda sin errores con gestión de QoS

Tal y como se mencionaba, los micrófonos están separados por lo que en parejas perciben la misma señal, por ello se aprecian los silencios en la forma de onda. Sin embargo, estos

silencios también están codificados y enviados por RTP. No se aplica una codificación o envío dinámico en función de los silencios pues no está configurada esta opción en la centralita. Esta función se llama *Voice Activity Detect*. En caso de activarla afectaría al ancho de banda consumido.

Las estadísticas de Wireshark de los paquetes RTP muestra que no ha habido pérdidas en ninguna de las llamadas:

Source Addr	Sourc	Destinat	Destir	SSRC	Start Time	Duración	Payload	Paquetes	Lost
10.10.1.12	32514	10.....14	32514	0...2	8.199064	55.95	g722	2799	0 (0.0%)
10.10.1.14	32514	10.....12	32514	0...b	8.256576	55.93	g722	2798	0 (0.0%)
10.10.1.19	32514	10.....24	32514	0...d	29.535155	30.12	g722	1507	0 (0.0%)
10.10.1.24	32514	10.....19	32514	0x...3f	29.594392	30.12	g722	1507	0 (0.0%)

Ilustración 55. Información RTP 2 llamadas QoS activo

Ahora las estadísticas de la interfaz del switch muestran lo esperado, al haber un correcto funcionamiento de QoS los paquetes entran y salen de manera correcta y según el mapeo indicado, no como ocurría en el ejemplo anterior:

```
dscp: incoming
--------------------------------
  0 -  4 :   17            0            0            0            0
  5 -  9 :    0            0            0            0            0
 10 - 14 :    0            0            0            0            0
 15 - 19 :    0            0            0            0            0
 20 - 24 :    0            0            0            0            0
 25 - 29 :    0            0            0            0            0
 30 - 34 : 1527            0            0            0            0
 35 - 39 :    0            0            0            0            0
 40 - 44 :    0            0            0            0            0
 45 - 49 :    0         2821            0            2            0
 50 - 54 :    0            0            0            0            2
 55 - 59 :    0            0            0            0            0
 60 - 64 :    0            0            0            0
  dscp: outgoing
--------------------------------
  0 -  4 : 1568            0            0            0            0
  5 -  9 :    0            0            0            0            0
 10 - 14 :    0            0            0            0            0
 15 - 19 :    0            0            0            0            0
 20 - 24 :    0            0            0            0            0
 25 - 29 :    0            0            0            0            0
 30 - 34 :    0            0            0            0            0
 35 - 39 :    0            0            0            0            0
 40 - 44 :    0            0            0            0            0
 45 - 49 :    0         2798            0            0            0
 50 - 54 :    0            0            0            0            2
 55 - 59 :    0            0            0            0            0
 60 - 64 :    0            0            0            0
```

```
cos: incoming
-------------------------------
  0 -  4 :   29            0            0         1528            0
  5 -  7 : 2821            0            0
  cos: outgoing
-------------------------------
  0 -  4 : 1582            0            0            0            0
  5 -  7 : 2798            0            0

output queues enqueued:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:        1584            0            0
 queue 1:        2798            0          172
 queue 2:           0            0            0
 queue 3:           0            0            0
  output queues dropped:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:           0            0            0
 queue 1:           0            0            0
 queue 2:           0            0            0
 queue 3:           0            0            0
```

No se descarta ningún paquete, de ninguna de las dos colas. Los que llegan salen correctamente compartiendo la misma interfaz. Al igual que vemos en la información recopilada por los terminales es similar a la de una llamada sin incidencias, con cero perdidas de paquetes y unos valores de *jitter* bajos.

Los problemas de congestión se resuelven ya que ahora los paquetes salen de la interfaz por diferentes colas en función de la prioridad que estos tienen. Estas colas tienen suficiente ancho de banda para soportar al menos el flujo de una llamada, ya que aunque G.722 tiene un *Bit Rate* de 64kbps al estar encapsulado en el protocolo RTP se deben tener en cuenta las cabeceras de los paquetes. El valor del ancho de banda consumido en Ethernet será de 87’2 kbps [35]. Lo cual se aproxima mucho a los límites impuestos en los ejemplos, cualquier valor superior a los 1200 en el comando *shape* de las colas de salida implicará congestión en dicha cola.

Con la siguiente tabla se resume lo sucedido con las colas, la congestión en estas y los límites impuestos. En la primera llamada entre dos extensiones existe un límite en las colas de salida muy estricto, el cual se encuentra por debajo del ancho de banda total que necesita el códec utilizado. El *Bit Rate* medido en el analizador de tráfico es prácticamente el valor del límite. Por esto ocurre congestión, porque realmente es necesario casi el doble de este ancho de banda para poder ejercer correctamente la comunicación utilizando el códec. El sistema intenta mandar los paquetes de audio al ritmo que el códec le exige pero se encuentra con la limitación de la cola y comienzan a acumularse los paquetes en el búfer, cuando se supera el nivel del búfer permitido se producen los descartes.

En la segunda llamada se aumenta el límite impuesto a la cola, pero no es suficiente ya que el valor es prácticamente todo el ancho de banda requerido por el códec. Por tanto, cuando una llamada se establece no hay problema y se ocupa todo el ancho de banda permitido, sin embargo, al establecerse la segunda llamada no hay capacidad suficiente y esta segunda llamada se ve afectada drásticamente, hasta el punto de abortarse la comunicación por falta de conectividad. Según las estadísticas medidas del analizador la primera llamada tiene velocidad de unos 83 kbps y la segunda llamada no llega a 1 kbps.

Por último, al diferenciar el tráfico con distintas marcas es posible gestionar hacia que cola se dirige. Manteniendo el límite de la cola 1, donde ahora se dirige todo el tráfico que no sea DSCP 46 o CoS 5, no hay problemas de congestión pues cómo ya se ha visto en la prueba anterior, el límite es justo el ancho de banda de 1 llamada con G.722. Hacia la cola 2 se dirigen exclusivamente los paquetes considerados más importantes, por ello no se aplica restricción alguna a la cola y por tanto no hay congestión de ningún tipo, permitiendo al flujo de datos transcurrir consumiendo el ancho de banda esperado.

Tabla 13. Comparativa límites y bit rate en pruebas

	Límite cola 1	***Bit Rate* medido cola 1**	**Límite cola 2**	***Bit Rate* medido cola 2**
Llamada 1	51.2 kbps	49 kbps	N.A.	N.A
Llamada 2	85.3 kbps	83 kbps + 1 kbps	N.A	N.A
Llamada 3	85.3 kbps	87 kbps	Sin límite	87 kbps

Como se ha podido comprobar la gestión de las etiquetas según la prioridad es de máxima importancia en sistemas donde el tráfico es en tiempo real, como lo son las llamadas en telefonía fija de voz sobre IP. Sobre esta base se podrían aplicar cientos de combinaciones, aplicar no solo gestión en las colas de salida sino en las de entradas, modificar los umbrales, la asignación de cada cola, y un larguísimo etc.

Para enseñar otro ejemplo de este tratamiento, se supone ahora que el tráfico identificado con DSCP 30 o CoS 3 no debe exceder cierto ancho de banda ya que esto podría implicar pérdidas importantes en el tráfico de voz IP. Para ello bastaría con dirigir este tráfico a una de las colas y a esta cola indicarle mediante el comando *shape* cuál es su límite. Por ejemplo, garantizamos y limitamos de la siguiente manera `srr-queue bandwidth shape 1200 2000 0 0`, para obtener los siguientes resultados.

Source Addr	Sourc	Destinat	Destir	SSRC	Start Time	Duración	Payload	Paquetes	Lost
10.10.1.12	32514	10.....14	32514	0...c	10.873428	45.99	g722	2301	0 (0.0%)
10.10.1.14	32514	10.....12	32514	0...8	11.075895	37.98	g722	1900	0 (0.0%)
10.10.1.19	32514	10.....24	32514	0x...f0	25.404336	43.27	g722	1232	905 (42.3%)
10.10.1.24	32514	10.....19	32514	0...7	25.322998	44.06	g722	2204	0 (0.0%)

Ilustración 56. Información RTP 2 llamadas con diferente tratamiento

Pérdidas intencionadas en el terminal que envía tráfico con las etiquetas DSCP 30 o CoS 3. En este ejemplo al tratarse de otro terminal VoIP carece de sentido, pero suponiendo que sea un PC o cualquier otro tipo de dispositivo que maneja un tipo de tráfico distinto a RTP donde las pérdidas se pueden gestionar para no generar errores en la comunicación, se observa otra (de las muchas) forma de limitar el tráfico según la prioridad.

Si se analizan el límite de las colas actual y el bit rate medido se puede entender nuevamente el motivo de la congestión producido en la cola 1, donde el límite del ancho de banda impuesto genera la congestión y con ella el llenado del búfer de dicha cola, hasta el punto del rebose de este y la pérdida de paquetes. En la cola 2 no se sufren pérdidas pues no hay problemas de congestión.

Tabla 14. Comparativa límites y bit rate en pruebas

	Límite cola 1	***Bit Rate* medido cola 1**	**Límite cola 2**	***Bit Rate* medido cola 2**
Llamada 4	51.2 kbps	48 kbps	85.3 kbps	85 kbps

Junto a estas configuraciones existen cientos de posibilidades y medidas para gestionar la posible congestión. En estas pruebas mostradas se cuenta con que el ancho de banda de la interfaz es mucho más amplio que lo que se puede usar con solo dos terminales mandando tráfico por esta vía. Sin embargo, en implementaciones reales no tiene por qué ser suficiente y cualquier estrategia orientada a mejorar la calidad de servicio aportará una mejora en la experiencia de usuario. En los casos vistos se analizan los paquetes RTP porque son los que interesan en cuanto a transmisión de voz, sin embargo los paquetes de control que viajan por la red también tienen sus prioridades. Por ejemplo, se ha comprobado que en ocasiones los terminales sufren un reinicio repentino mientras hay una llamada establecida. Esto se debe a que hay congestión, el búfer se llena y comienza a retrasar la entrega de paquetes o incluso descartarlos. La OXE tiene constancia de si el terminal está conectado gracias a un mensaje *KEEP_ALIVE* que envía al terminal y espera una respuesta en un determinado tiempo. Cuando se excede ese tiempo considera una pérdida de conectividad y fuerza el reinicio del terminal. Por tanto, una vez más vemos la importancia de asegurar la calidad del servicio, de tener controla sobre el etiquetado de paquetes y la gestión en función de la importancia que estos tengan, todo ello teniendo en cuenta las capacidades del sistema de telefonía sobre IP, desde los terminales y centralita, la red y sus equipos, el uso que se le da, la convivencia con otros terminales y un amplio abanico de premisas que reivindican la importancia de aplicar QoS.

4. Conclusiones y trabajos futuros

La VoIP es una tecnología que durante la última década ha crecido hasta un punto de madurez que se establece como el método más habitual de comunicación a distancia. Ha recibido un incremento de atención tanto por los investigadores como por los usuarios finales. Se ha evaluado exhaustivamente y analizado en función de la QoS. Sin embargo, son pocos los estudios que relacionen el uso de VoIP con la QoS en un entorno real, con software y hardware en un entorno de simulación y comprueben cómo afectan los parámetros teóricos en la calidad de la experiencia de una llamada. El proyecto aquí planteado analiza en detalle cómo se puede ver afectada la QoS en un entorno LAN mediante un ejemplo real y las principales características que debe tener en cuenta el usuario al implementarlo. Se ha hecho uso de material real, un switch de un fabricante de prestigio como es Cisco, al igual que terminales especialmente diseñados para el uso de VoIP de un fabricante líder en el sector como es Alcatel, ambos son perfectamente válidos para su uso a pesar de no ser un modelo de última generación. Además, se introduce el concepto de la priorización mediante el uso de una red MPLS, una competencia que recae sobre el proveedor de servicios pero que el usuario debería conocer para entender el proceso y los efectos que puede tener en la QoS sobre el flujo de voz. Por último, se ha señalado el uso de Internet en las comunicaciones de telefonía fija por voz IP, donde se hace una breve introducción y se citan los motivos por los que no es posible garantizar una calidad en este tipo de red. Las tres opciones son de gran valor para cualquier entidad que esté interesada en implementar un sistema VoIP o bien tenga uno y desconozca ciertos aspectos interesantes que pueden afectar a la calidad de este.

Entre los retos encontrados destacaría la necesidad de filtrar la gran cantidad de documentación e investigación respecto a la materia. Existen diversas estandarizaciones y en general documentación que desarrolle conceptos relacionado con la calidad de servicio, de los cuales muchos se centran en los servicios de tráfico de tiempo real. Los fabircantes también aportan numerosa documentación, cada fabricante acaba haciendo con sus herramientas y métodos trabajos muy similares, pero con diferentes algoritmos e ideas de cómo afrontar el problema a resolver. Esto provoca una gran cantidad de nombres, nomenclaturas, definiciones, etc., para una misma solución (o muy similar). La gran mayoría de documentación se ha sacado del fabricante Cisco, pero siempre intentando obtener el concepto genérico, por ello se ha procurado comparar con otros fabricantes como Huawei, Fortinet, Juniper.

Configurar desde cero un switch sin experiencia de campo no es una tarea sencilla, si bien ponerlo en marcha puede ser cuestión de tiempo y esfuerzo, hacerlo funcionar de la manera deseada implementando calidad de servicio es un reto en mayúsculas. Tal y como se desarrolla en la memoria, las posibilidades son muy variadas, no existe una única solución a un problema y en muchas ocasiones un pequeño cambio alterna la lógica del funcionamiento arrojando resultados no deseados. Entre los retos también se podría mencionar la necesidad de resumir un estado del arte tan amplío, hacer foco en los puntos

que más importancia tienen en la telefonía fija sobre IP, seleccionar las recomendaciones y estándares relacionados con cada tema descrito.

Como en cualquier proyecto, ha habido imprevistos y cambios, pero el resultado final de la memoria refleja con mucho acierto la idea inicial. Se ha buscado resolver ciertas dudas que pueden surgir a la hora de implementar un servicio de telefonía sobre IP, por dónde empezar, qué tener en cuenta y qué aspectos pueden afectar a la experiencia que van a tener los usuarios que utilizan el sistema. En detalle el aspecto de la configuración LAN, que hila el contenido con lo que será un análisis en las siguientes fases por las que pasa el flujo de voz, junto a lo qué ocurrirá en la red del ISP que implemente MPLS.

Se ha procurado seguir los objetivos establecidos y cumplirlos, se ha seguido el plan previsto de manera consistente, cumpliendo con los puntos de referencia esenciales y adaptando en tiempo y forma a las entregas en cada etapa. Gracias al trabajo previo y a la sólida base establecida en las etapas iniciales del proyecto, así como a la metodología definida que se centra en un análisis tecnológico exhaustivo de las necesidades, se ha logrado dirigir este proyecto de manera práctica y mantener un ritmo de trabajo adecuado. Además, se han evaluado varias soluciones disponibles, lo que nos ha permitido tomar decisiones fundamentadas.

El cambio principal que se ha realizado ha sido en relación a la parte práctica. En la implementación del entorno de pruebas se planteó una idea inicial con máquinas virtuales la cual podría haberse llevado a cabo, pero tenía muchas limitaciones de procesamiento y funcionalidades. Gracias a que se pudo optar por material físico se comenzó a trabajar en este sentido, teniendo que hacer otros cambios más dado que no todo el material era válido (el primer switch tenía problemas de hardware). Finalmente, los cambios surgieron efecto y se pudo cumplir con los objetivos previstos.

Se cumplen los impactos previstos, se observa como la capacidad de la red se aprovecha de una manera más eficiente con la gestión de la calidad de servicio y con ello se reduce el impacto en el gasto energético. Aplicar de manera correcta esta gestión del tráfico fomenta el uso de esta tecnología. La VoIP cumple con el Objetivo de Desarrollo Sostenible 7 al permitir una comunicación eficiente y accesible a través de la tecnología, reduciendo así la brecha digital y facilitando el acceso a servicios de comunicación a comunidades remotas. Además, también cumple con el ODS 9 al fomentar la innovación tecnológica y la infraestructura resiliente al utilizar redes de datos existentes para transmitir voz, optimizando el uso de recursos y promoviendo la conectividad global.

En cuanto a las líneas de trabajo futuro cabe decir que hay mucho campo posible donde desarrollar diferentes propuestas, desplegar e investigar el impacto con pruebas como las aquí presentes. Aumentar la cantidad de terminales para poder simular un entorno que sufra congestión real y así implementar todo tipo de algoritmos relacionados con la gestión de prioridades. Pero dando un salto más allá, otras tecnologías relacionadas y cada vez más habituales donde la voz se ve implicada serían el uso de WebRTC o de *Segment*

Routing. La primera es una tecnología que permite realizar comunicaciones de audio y video en tiempo real a través de navegadores web sin necesidad de plugins adicionales, lo cual podría afectar al MOS relacionado con la comunicación debido a la compresión que pueda sufrir el audio, los retardos en el envío de tramas, etc. La segunda utiliza MPLS como una herramienta para implementar su enrutamiento basado en segmentos, simplifica y optimiza las redes al agregar información en el encabezado de los paquetes, lo que permite dirigir el tráfico de manera eficiente y flexible.

5. Glosario

Definición de los términos y acrónimos más relevantes utilizados en la memoria:

- VoIP: Voice over Internet Protocol
- ToIP: Telephony over Iternet Protocol
- QoS: Quality of Service
- Vishing: Voice y Phising, amenaza mediante llamada telefónica fraudulenta.
- SIP: Session Initiation Protocol
- RTP: Real Time Protocol
- RTCP: Real Time Control Protocol
- SDP: Session Description Protocol
- MOS: Mean Opinion Score
- IETF: Internet Engineering Task Force
- DSCP: Differenciated Services Code Point
- QoE: Quality of Experience
- FTP: File Transfer Protocol
- ACR: Absolute Category Rating
- ISP: Internet Service Provider
- RSVP: Resource Reservation Protocol
- MQC: Modular QoS Command-Line Interface
- MPLS: Multi-Protocol Label Switching
- TE: Traffic Engineer
- CBR: Constraint Based Routing
- LSR: Label Switching Router
- LER: Label Edge Router
- PE: Provider Edge
- CE: Customer Edge
- LSP: Label Switched Path
- FEC: Forwarding Equivalent Class
- LFIB: Label Forwarding Information Base
- L2TP: Layer 2 Tunneling Protocol
- IPSec: Internet Protocol Security

6. Bibliografía

[1] D. Barril Mares, «Historias de Telefonía en España,» abril 2017. [En línea]. Available: https://historiatelefonia.com/2017/04/29/el-principio-del-fin-de-las-redes-de-cobre/. [Último acceso: marzo 2023].

[2] D. Jonathan, P. James, B. Manoj, K. Satish y M. Sudipto, Voice over IP Fundamentals 2nd Edition, Indianapolis: Cisco Press, 2007.

[3] J. M. Huidobro y D. Roldán, Tecnología VoIP y Telefonía IP, México: Alfaomega, 2006.

[4] J. R. Machado Fernández, Principios Básicos de la Red Telefónica, la Conmutación y el Teletráfico., 2016.

[5] F. R. Miquel, L. O. Eduard, S. i. G. René y V. G. Xavier, «Los contextos del nivel de enelace y la capa física,» septiembre 2010. [En línea]. Available: https://openaccess.uoc.edu/bitstream/10609/9842/11/Estructura%20de%20redes%20de%20computadores_M%C3%B3dulo5_Los%20contextos%20del%20nivel%20de%20enlace%20y%20la%20capa%20f%C3%ADsica.pdf. [Último acceso: junio 2023].

[6] H. Rifà Pous, R. Gallego Terris y V. Huertas García, Contexto actual y evolución hacia las redes de nueva generación, UOC, PID_00265733, 2019.

[7] S. W. Richard y G. R. Wright, TCP/IP Illustrated: Vol. 1: The Protocols. 1st edition., Place of publication not identified: Addison Wesley Professional, 1996.

[8] Dirección de Comunicación Corporativa. Telefónica S.A., «Nota de Prensa. Transformación de red telefónica,» de *TELEFÓNICA APAGARÁ UNA CENTRAL DE COBRE AL DÍA HASTA 2020* , Madrid, 2018.

[9] B. Goode, Voice over Internet protocol (VoIP), Proceedings of the IEEE, vol. 90, no. 9, pp. 1495-1517, 2002.

[10] 3CX, «3cx.es,» [En línea]. Available: https://www.3cx.es/voip-sip/ip-pbx-overview/. [Último acceso: marzo 2023].

[11] Y. D. C. Toll Palma, O. A. Guzmán Obregón, Y. Ril Gil y L. Vigoa Machin, «Voz sobre IP. Técnicas de paquetización,» de *Tecnología y pensamiento. Vol 5.*, 2011, pp. 109-120.

[12] C. Mittal y Ranjan Roy, «SIP Call Flow,» SoftSwitchNGN, 2007. [En línea]. Available: https://sites.google.com/site/softswitchngn/sipcallflow. [Último acceso: 2023].

[13] B. R.M y B. M.A, «{Quality of service provisioning for VoIP applications with policy-enabled differentiated services,» de *IEEE/IFIP Network Operations and Management Symposium (IEEE Cat. No.04CH37507)*, 2004, pp. 335-348 Vol.1.

[14] I. Cisco Systems, «End of Support for the H.323 call control features in Cisco IOS XE Software,» 27 mayo 2021. [En línea]. Available:

https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-border-element/bulletin-c25-2479306.html. [Último acceso: 2023].

[15] 3CX, «¿Qué es H323?,» [En línea]. Available: https://www.3cx.es/voip-sip/h323/. [Último acceso: 2023].

[16] IETF, «RFC 2210,» de *The Use of RSVP with IETF Integrated Services*, 1997.

[17] IETF, «RFC 2474,» de *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, 1998.

[18] I. T. UNION, «ITU-R G.114, SERIES G: TRANSMISSION SYSTEMS AND MEDIA,,» 05/2023.

[19] A. F. Ribadeneira, «An Analysis of the MOS under Conditions of Delay, Jitter andPacket Loss and an Analysis of the Impact of Introducing Piggybacking and Reed Solomon FEC for VOIP,» Thesis, Georgia State University, 2007.

[20] E. L. Rocafiguera, Calidad de servicio en redes interconectadas, Barcelona: UOC, 2018.

[21] Tim Szigeti, Christina Hattingh, Robert Barton y Kenneth Briley Jr., End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, Second Edition, Cisco Press, 2013.

[22] J. Jimenez, «Implementación de políticas de calidad de servicio con punto de código de servicios diferenciados,» agosto 2022. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html.

[23] V. Krishnan, «Juniper Networks,» diciembre 2012. [En línea]. Available: https://www.juniper.net/documentation/en_US/day-one-books/JunosQosforIOSEngineers.pdf. [Último acceso: mayo 2023].

[24] Huawei, «IEEE 802.1Q Frame format,» julio 2019. [En línea]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100088104. [Último acceso: mayo 2023].

[25] T.-C. Publishing's, «Trust Boundaries (Classification, Marking, and NBAR),» [En línea]. Available: http://what-when-how.com/ccnp-ont-exam-certification-guide/trust-boundaries-classification-marking-and-nbar/.

[26] M. Tripathi, «Multiprotocol Label Switching(MPLS) Explained,» Towards Data Science, agosto 2019. [En línea]. Available: https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94. [Último acceso: mayo 2023].

[27] J. Sáez Cano, Configuración de servicios VPN en entorno MPLS, Valencia: Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, 2018.

[28] M. Pengxuan, Z. Nan, X. Yang y K. Kim, «The QOS of the Edge Router Based on Diffserv/MPLS,» IEEE, Beijing, China, 2009.

[29] S. Baraković y J. Baraković, «Traffic Performances Improvement using DiffServ and MPLS Networks,» IEEE, Sarajevo, Bosnia and Herzegovina, 2009.

[30] T. Abraham, «MPLS QOS – RFC 3270,» abril 2015. [En línea]. Available: https://ipfiles.wordpress.com/2015/04/01/mpls-qos-rfc-3270/. [Último acceso: junio 2023].

[31] K. Molnar y M. Vlcek, «Evaluation of Quality of Service support in MultiProtocol Label Switching,» IEEE, Fifth International Conference on Systems and Networks Communications, Brno, 2010.

[32] N. d. Río, «Diseño e implementación de una solución de administración de tráfico de red basada en DNS y chequeos de disponibilidad.,» noviembre 2015. [En línea]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/51098/Tesis_completa__134_p._.pdf-PDFA.pdf?sequence=4&isAllowed=y. [Último acceso: junio 2023].

[33] C. Systems, Catalyst 3560 Switch Software Configuration Guide, California: Cisco IOS Release 15.0(2)SE and Later, 2013.

[34] C. System, «Ejemplos de configuración de QoS en Cisco Catalyst 3750,» mayo 2007. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-3750-series-switches/91862-cat3750-qos-config.html. [Último acceso: mayo 2023].

[35] J. P. V. Urena, «Modify Bandwidth Consumption Calculation for Voice Calls,» septiembre 2022. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html. [Último acceso: mayo 2023].

[36] S. Soulhi, «Telephony over packet networks,» IEEE Canadian Review, 1999.

[37] L. D. Ghein, MPLS Fundamentals, Cisco Press, 2007.

[38] Huawei, «MPLS DiffServ Mode Configuration,» noviembre 2022. [En línea]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100279274/f46b5cc0/mpls-diffserv-mode-configuration. [Último acceso: mayo 2023].

[39] S. M. Eugene y E. H. Bjarne, «Analysis of Evolution Scenarios for End-to-end Quality of Services Provisioning in the Internet,» *Centre for Quantifiable Quality of Service in Communication Systems (Q2S); IEEE,* vol. 2009 International Conference on Ultra Modern Telecommunications & Workshops, 2009.

7. Anexos

7.1. Ticket IP generado en la OXE en la llamada 1

```
[ 1] End of communication           : Tue May 30 12:25:43 2023
[ 2] Node Number                    : 1
[ 3] Protocol Version               : 2
[ 6] Equipement Type                []=     2 values
        [Type:1=IPP|2=APC|3=CplOmEnt|4=CplOmOFF|6=xBS] : 1                 |
        [Type:1=IPPv2|2=NOEIPP|0=4980|1=WSftIP|0=IntIP|1=GD|2=eVA|3=I] : 2 |
[ 8] Local IP                       : 10.10.1.12
[ 9] Distant IP                     : 10.10.1.14
[10] Local ID                       : 3117
[11] Distant ID                     : 2082
[12] Call Duration                  : 17 sec
[13] Local SSRC                     : 0x2ef80b16
[14] Distant SSRC                   : 0x1518e2d
[15] Compression Type     5-7=G722| 0=G711A|1=G711U|2=G723|3=G729|8=OPUS: 5
[16] VAD                            : false
[17] Echo Canceler                  : true
[18] Voice Mod                      : Handset (for filter use val 81)
[19] Requested Framing Duration     : 20 ms
[20] Received Framing               : 20 ms
[21] Framing Change NB              : 0
[22] RTP Received Paquets NB        : 489
[23] Total RTP Paquets Sent         : 859
[24] RTP Lost Paquets NB            : 341
[25] Total Silence                  : 0 sec
[26] NB SID Received Paquets        : 0
[27] Delay                          []=     5 values: Bound expressed in ms
        [0-40] : 0    | [40-80] : 0   | [80-150] : 0  | [150-250] : 0 |
        [+250] : 0    |
[28] Max Delay                      : 0 ms
[29] NB DTMF Detected               : 0
[31] Distribution BFI               []=     5 values
        0 | 0 | 0 | 0 | 0 |
[32] Jitter Depth                   []=    10 values
        [0] : 4390912 | [1] : 0      | [2] : 8224    | [3] : 8224    |
        [4] : 8224    | [5] : 8224   | [6] : 522     | [7] : 0       |
        [8] : 0       | [9] : 0      |
[38] Software Version               []=     2 values
        5  | 45 |
[39] TERMINAL MCDU(IPP,eVA,xBS)     : 3117
[41] DSP Framing Duration           : 5 ms
[42] NB SID Transmitted             : 0
[45] Min Delay                      : 0 ms
[46] Qos 8021Q Used                 : 1
[47] Qos 8021Q Priority             : 5
[48] Qos Vlan Id                    : 21
[49] Qos Diffserv (DSCP)            : 46
[55] Ticket Encryption              : true
[60] Local Jetlag                   : 2
```

```
================================================================================
[ 1] End of communication           : Tue May 30 12:25:43 2023
[ 2] Node Number                    : 1
[ 3] Protocol Version               : 2
[ 6] Equipement Type                []=     2 values
        [Type:1=IPP|2=APC|3=CplOmEnt|4=CplOmOFF|6=xBS] : 1                 |
        [Type:1=IPPv2|2=NOEIPP|0=4980|1=WSftIP|0=IntIP|1=GD|2=eVA|3=I] : 2 |
[ 8] Local IP                       : 10.10.1.14
[ 9] Distant IP                     : 10.10.1.12
[10] Local ID                       : 2082
[11] Distant ID                     : 3117
[12] Call Duration                  : 17 sec
[13] Local SSRC                     : 0x1518e2d
[14] Distant SSRC                   : 0x2ef80b16
[15] Compression Type     5-7=G722| 0=G711A|1=G711U|2=G723|3=G729|8=OPUS: 5
[16] VAD                            : false
[17] Echo Canceler                  : true
[18] Voice Mod                      : Handset (for filter use val 81)
[19] Requested Framing Duration     : 20 ms
[20] Received Framing               : 20 ms
[21] Framing Change NB              : 0
[22] RTP Received Paquets NB        : 401
[23] Total RTP Paquets Sent         : 861
[24] RTP Lost Paquets NB            : 0
[25] Total Silence                  : 0 sec
[26] NB SID Received Paquets        : 0
[27] Delay                          []=     5 values: Bound expressed in ms
        [0-40] : 0    | [40-80] : 0   | [80-150] : 0  | [150-250] : 0 |
        [+250] : 0    |
[28] Max Delay                      : 0 ms
[29] NB DTMF Detected               : 0
[31] Distribution BFI               []=     5 values
       0 | 0 | 0 | 0 | 0 |
[32] Jitter Depth                   []=    10 values
        [0] : 786432 | [1] : 0      | [2] : 8224   | [3] : 8224   |
        [4] : 8224   | [5] : 8224   | [6] : 769    | [7] : 0      |
        [8] : 0      | [9] : 0      |
[38] Software Version               []=     2 values
        5  | 45 |
[39] TERMINAL MCDU(IPP,eVA,xBS)     : 2082
[41] DSP Framing Duration           : 5 ms
[42] NB SID Transmitted             : 0
[45] Min Delay                      : 0 ms
[46] Qos 8021Q Used                 : 1
[47] Qos 8021Q Priority             : 5
[48] Qos Vlan Id                    : 21
[49] Qos Diffserv (DSCP)            : 46
[55] Ticket Encryption              : true
[60] Local Jetlag                   : 2
```