Universidad Nacional Autónoma de Nicaragua
UNAN-Managua.
Facultad de Ciencias e Ingenierías
Departamento de Tecnología
Ingeniería en Electrónica.

Seminario de Graduación

Tema: Redes de Nueva Generación.

Subtema:

Redes de Nueva Generación Utilizando Tecnología MPLS en Transporte de Servicios Convergentes.

Autores:

Br. José Daniel Poveda Pilarte.
Br. Fabio José baca Sevilla.

Tutor:
Msc. Edwin Quintero.

Fecha: 14 de Agosto 2014.

Tema:

Redes de Nueva Generación.

Subtema:

Redes de Nueva generación Utilizando Tecnología MPLS en Transporte de Servicios Convergentes.

DEDICATORIA

Dedico este trabajo de culminación de estudios superiores, en primera instancia a Dios, por brindarme la oportunidad de llegar al final y haberme dado salud para lograr mis objetivos de esta etapa, que significa un paso muy importante en mi vida.

A Dios, por brindarme fortaleza para superar los obstáculos que se me presentaron, sabiduría para tomar las decisiones adecuadas y siempre escoger el camino correcto para hacer las cosas.

A mi madre, Mirna Pilarte García, por estar siempre presente en los momentos difíciles y por su ayuda y sabiduría para dar los pasos necesarios y alcanzar mis metas. Por todo su amor y confianza en mi persona y brindarme le apoyo cuando lo necesitaba.

A mi padre (Q.E.P.D), José de Jesús Poveda Dávila, que aunque físicamente no se encuentre conmigo dejo en mi un ejemplo de perseverancia. Y me enseño a no rendirme ante las dificultades de la vida.

A mí esposa María Auxiliadora Espinoza Arcia y a mi Hijo Santiago Daniel Poveda Espinoza a quienes tanto quiero y fueron mi motivación para poder terminar mi formación profesional.

A mis hermanas, por el apoyo que me brindaron y por demostrarme siempre su cariño y apoyo incondicional, sin importar nuestras diferencias de opiniones para que lograra culminar mis estudios.

Br. José Daniel Poveda Pilarte.

DEDICATORIA

A:

DIOS por brindarme salud y darme la fuerza para cumplir las metas que me he propuesto en la vida.

Mi Madre, Amanda Sevilla, que ha sido el mejor ejemplo de superación que he tenido y por enseñarme que todo es posible si uno se lo propone.

Mi Padre, Gilberto Baca, de quien aprendí que no importa que cometa errores en el camino siempre existe otra oportunidad de salir adelante.

Mis Hermanos, Miguel, Patricia, Carlos Uriel, Johanna, Rodrigo, Ottoniel, Jasón, Jeimi por estar siempre a mi lado brindándome su apoyo.

Mi sobrino Carlos Saúl, espero que logre salir adelante.

Mis amigos, que me brindaron su apoyo durante esta etapa de mi vida y que me ayudaron a salir delante de las dificultades que surgieron en todos estos años Gustavo, José Antonio, Fernando, Oscar, Ezequiel, Freddy, Ramiro, Kenia. Walter, y todos los que no recuerdo en este momento.

Mis maestros, que nos brindaron el apoyo necesario en todo momento durante toda mi carrera y me permitieron el ahora ser un profesional.

Todos aquellos familiares y amigos que por motivos de espacio no pude mencionar al momento de escribir esta dedicatoria.

Br. Fabio José Baca Sevilla

AGRADECIMIENTOS

La realización del siguiente trabajo de seminario, no hubiera sido posible, sin la valiosa colaboración de los conocimientos científicos técnicos, que nos brindaron las siguientes personas:

El maestro Msc: Edwin Quintero, que con sus conocimientos, nos guio por las diferentes etapas de la investigación.

A nuestro querido maestro Msc. Jairo Gonzales, quien además de brindarnos sus conocimientos, tiempo y nos facilitó documentación.

Al ingeniero Francisco Morales, que nos facilitó mucha información y nos proporcionó algunas recomendaciones para la elaboración del trabajo.

Y por último a los docentes que nos impulsaron en el camino universitario, para alcanzar la meta de convertirnos en profesionales.

A todos gracias.

Br. José Daniel Poveda pilarte.
Br. Fabio José baca Sevilla.

Managua 4 de agosto de 2014

Ingeniero.
BISMARCK SANTANA TIJERINO.
Director.
Departamento de tecnología.
Facultad de ciencias e ingenierías.
UNAN-MANAGUA.

Estimado ingeniero santana.

Sirva la presente para comunicarle que he dirigido y examinado el trabajo de seminario de graduación realizado por los bachilleres: FABIO JOSE BACA SEVILLA Y JOSE DANIEL POVEDA PILARTE, Titulado:
"Redes de nueva generación utilizando tecnología MPLS en transporte de servicios convergentes".

Posterior a la pre defensa y en base a las recomendaciones del jurado calificador revisión del tema del documento, objetivos específicos, introducción y resumen, conclusiones, diseño de red, objetivo general, ventajas que ofrece la red.

ATT.

MSC. Edwin Quintero
Tutor.

Índice

Índice de figuras.

Índice de tablas.

RESUMEN.

En el presente trabajo de fin carrera universitaria nos hemos propuesto a realizar un análisis sobre redes de nueva generación para ver el desarrollo que han tenido las redes clásicas con el paso del tiempo y como se han visto en la necesidad de adaptarse a los nuevos requerimientos que exigen los usuarios en la actualidad.

Las NGN surgen ante la necesidad de brindar un mejor servicio al usuario que hoy en día demanda un servicio de mayor calidad con un alto nivel de QoS escogimos MPLS como red NGN por los distintos beneficios que brinda y no representa un problema a la aplicación sobre las ya establecidas redes basadas en IP.

Al realizar este análisis podremos evidenciar que MPLS es una propuesta muy tentadora para los operadores ya que brinda grandes ventajas como tener el control de la ruta, asignar distintos anchos de banda a los enlaces o crear prioridades para la utilización de un enlace, mejorara la escalabilidad de la red y el retardo de proceso en los routers y la necesidad de las operadoras de que sus redes tuviesen una cierta calidad de servicio ya que QoS se ha convertido en un criterio muy importante a la hora de definir una red.

Presentaremos la configuración de una red sencilla pero que nos permitirá ver el funcionamiento, características y beneficios que nos proporciona MPLS.
Nos valdremos de una herramienta de simulación para demostrar el correcto funcionamiento de la red MPLS así como brindaremos recomendaciones para los usuarios que se interesen en realizar una continuación de este análisis.

INTRODUCCION.

La trasmisión de datos y la comunicación en general a través de las redes clásicas, genero la necesidad de una evolución para satisfacer las necesidades de los usuarios. Entre estas demandas cabe mencionar la disponibilidad de ofrecer diferentes niveles de calidad de servicio, aplicaciones en tiempo real, la priorización de paquetes, los cambios tecnológicos en avalancha y la fusión de servicios prestados. Es así como surgen las redes de nueva generación (NGN), desarrolladas para solventar todas las deficiencias que presentaban las redes clásicas en la trasmisión y la gestión de un mayor ancho de banda.

MPLS brinda solución a este tipo de situaciones y aunque esta ya tiene algunos años de implementarse en las redes clásicas vemos necesario profundizar en el tema, dado que esta sirve de base para el futuro de las redes que funcionaran con GMPLS que es una extensión de esta aplicada sobre la capa óptica. Observaremos el funcionamiento de una red que trabaja con MPLS, así podremos determinar por qué este protocolo ha hecho posible la mejor conformación de las redes para los proveedores de servicios y a su vez un mejor y óptimo servicio para los usuarios finales. Brindaremos unas recomendaciones que deben tener en cuenta en el momento de implementar MPLS en una red.

La implementación de redes NGN se ha vuelto más frecuente y necesaria, el presente trabajo tiene el objetivo de brindar a cualquier persona con conocimientos básicos, comprender dicha arquitectura. En este documento trataremos temas como un análisis de redes NGN, su arquitectura, ventajas que ofrecen, una amplia explicación sobre MPLS, sus conceptos, componentes y funcionamiento, continuando veremos las ventajas que ofrece y la evolución actual que ha tenido el protocolo como lo representa GMPLS, veremos la configuración de una red MPLS y finalizaremos con recomendaciones básicas para su aplicación.

JUSTIFICACION.

El creciente incremento en tráfico de datos en las redes actuales así como la aparición de aplicaciones multimedia con altos requerimientos en las tasa de transferencia de datos y en la calidad de servicio prestada, dio paso a la aparición de las redes de nueva generación que vinieron a suplir las debilidades en las redes basadas en IP, con el principal propósito de que las redes se adaptaran a las necesidades que los usuarios demandan hoy en día.

En este trabajo, escogimos una red de nueva generación como MPLS que ofrece a los operadores de red una rápida provisión de servicios de cualquier tipo, en cualquier momento, con cualquier calidad de servicio, con cualquier grado de disponibilidad y a cualquier destino. Esta provisión tiene un costo operativo muy bajo por utilizar las ampliamente disponibles herramientas de control IP y utilizar un plano de control idéntico para gestionar la red óptica.

Podremos evidenciar como MPLS ofrece un panel de control único e integrado y extiende la disponibilidad de recursos y gestión del ancho de banda, a lo largo de todas las capas de red es decir los equipos de las redes dejan de estar separados en diferentes capas todos los elementos pueden tener información del resto ya que está diseñado para soportar diferentes tipos de tráfico.

OBJETIVO GENERAL

Analizar la tecnología MPLS como una red de nueva generación de servicios convergentes.

OBJETIVOS ESPECÍFICOS

- Analizar la tecnología de conmutación MPLS en el transporte de datos y servicios de redes de nueva generación.

- Presentar la configuración de una red de nueva generación para transporte de voz, video y datos así como los comandos necesarios para hacerlo.

- Demostrar el funcionamiento de MPLS mediante simulación o con una APP de redes así como las recomendaciones pertinentes para el correcto funcionamiento de la red.

Capítulo 1. Redes de Nueva Generación evolución y convergencia.

La evolución del sector hacia las redes convergentes o redes de nueva generación NGN está ligada a la evolución del estado hacia la sociedad de la información, en la medida que estas redes constituyen la principal infraestructura para el transporte de la información y para la conectividad de las personas. Esta evolución implica para los operadores la innovación continua de servicios y redes con el fin de satisfacer las necesidades de la sociedad.

La convergencia de servicios, aplicaciones y dispositivos impulsan esta tendencia, para beneficio del cliente, pues obtiene cada vez más y mejores servicios, a un costo competitivo. Las redes de nueva generación son una realidad que permite avanzar hacia la consecución de estos objetivos. En un marco de convergencia los servicios operan utilizando una misma plataforma tecnológica por lo cual se debe considerar que los distintos referentes y parámetros regulatorios deben también estar integrados, para que garanticen la competencia efectiva entre operadores de red.

Podemos definir una red de nueva generación como “una red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y proveedores de servicios o servicios de su elección. Se soporta la movilidad generalizada que permita la prestación coherente ubicua de servicios a todos los usuarios” mediante esta definición se sugiere que tanto las funciones referentes a los servicios como al transporte se pueden ofrecer separadamente.

1.1 - Características de la NGN

Según los lineamientos y estándares de la UIT, las principales características de las NGN son:

- La transferencia basada en paquetes.
- Las funciones de control están separadas de las capacidades del portador llamada/sesión, y aplicación/servicio.
- Desacoplamiento de la provisión de servicios del transporte, y se proveen interfaces abiertas.
- Soporte de una amplia gama de servicios, aplicaciones y mecanismos basados en construcción de servicios por bloques incluidos servicios en tiempo real/de flujo continuo en tiempo no real y multimedia.
- Tendrá capacidades de banda ancha con calidad de servicio extremo a extremo.
- Tendrá interconexión con redes tradicionales a través de interfaces abiertas.
- Movilidad generalizada.
- Acceso sin restricciones de los usuarios a diferentes proveedores de servicio.
- Diferentes esquemas de identificación.
- Características unificadas para el mismo servicio, como es percibida por el usuario.
- Convergencia entre servicios fijos y móviles.
- Independencia de las funciones relativas al servicio con respecto a las tecnologías subyacentes de transporte.
- Soporte de las múltiples tecnologías de última milla.
- Cumplimiento con todos los requisitos reglamentarios, por ejemplo en cuanto a comunicaciones de emergencia, seguridad, privacidad, interceptación legal, etc.

Estas características, se enfocan en la necesidad de ver al usuario como cliente potencial, cuya demanda debe ser atendida a través de nuevas herramientas tecnológicas, que le reporten beneficios en términos de costos, calidad de los servicios prestados y diversidad de servicios.

En cuanto a la tecnología aplicada a las redes de nueva generación, esta se basa en una nueva arquitectura, donde los servicios ya no están integrados verticalmente. Esta plataforma es conocida como IMS que significa protocolo internacional de sistemas multimedia por sus siglas en inglés, la cual permite la convergencia de servicios de texto, datos, video y multimedia. Entre los beneficios para el usuario se pueden destacar:

- Una red básica de servicios independientes.
- Una red para voz y datos que permite servicios multimedia integrados.

Lo anterior evidencia que la convergencia de red y servicios, es un aspecto central de las redes de nueva generación, que permite establecer redes de acceso al usuario final a gran escala, que exige la creación de una nueva gama de actividades en las cuales las empresas antes no tenían injerencia, y que crea una nueva cultura empresarial.

1.1.1. Migración hacia redes de nueva generación.

La migración hacia redes de nueva generación constituye un elemento fundamental para lograr la convergencia de redes y servicios, y específicamente para desarrollo de banda ancha. Esta migración consiste en pasar de redes PSTN o redes telefónicas públicas conmutadas, basadas en voz a NGN basadas en el protocolo IP.

En este sentido las redes PSTN no estaban diseñadas para la entrega unidireccional de radio o televisión, de modo distinto, el internet fue diseñado para

el transporte en tiempo no real de paquetes. Es así como se está dando un reemplazo progresivo entre las PSTN y las NGN, que se están extendiendo a gran velocidad en un número creciente de países.

Estas redes están estableciendo un cambio de redes PSTN separadas y redes IP hacia redes unificadas basadas en el protocolo de internet con plataformas multiservicios y basadas en paquetes de servicios. En este sentido habría que optar entre favorecer la construcción de nuevas redes o favorecer la explotación de las redes ya existentes.

Dentro de las principales razones para la migración hacia Redes de Nueva Generación, se pueden citar las siguientes:

- Eficiencia de costos: economía de alcance propio de una red troncal basada en IP y reducción de costos operativos al permitir la eliminación de centrales locales.
- Diversificación de fuentes de ingreso: erosión de ingresos por rubros tradicionales.
- Demanda de los consumidores de mayores velocidades de transmisión.
- Presión competitiva: prestadores de tv por cable, empresas eléctricas, proyectos municipales/públicos y proveedores alternativos.

La migración hacia NGN no significa la sustitución total de las redes ya existentes, si no por el contrario, la integración de las redes de telefonía convencionales. Esto significa que las redes tradicionales pueden evolucionar, adaptarse y hacer parte de las NGN, para mantener las inversiones. La modernización de acceso es la base para proveer los nuevos servicios y aplicaciones en la misma red. Las NGN irán reemplazando progresivamente elementos y áreas de las RTPC tradicionales, construyendo en base a xDSL, acceso de fibra y con la convergencia de servicios o aplicaciones fija – móvil e internet.

De ahí que el sector de las telecomunicaciones se modernice constantemente, incorporando nuevas tecnologías o adaptando las ya existentes, nuevos actores y nuevos escenarios de convergencia de redes y servicios para responder a las nuevos demandas de los usuarios finales.

Aquí es importante señalar que la migración a NGN trae consigo tanto ventajas como preocupaciones. Dentro de las ventajas se pueden citar:

- La disponibilidad de una gran variedad de servicios y fácil movilidad entre ellos.
- La posibilidad del usuario para elegir el tipo de acceso que más se adecue a sus necesidades ya sea atendiendo a criterios de precios o calidad de servicio.
- La mayor velocidad de transmisión.

Un aspecto importante a destacar, es que en las NGN permiten la convergencia de las comunicaciones fijas y móviles, permitiendo así que el usuario escoja el acceso fijo o móvil o una combinación de ambas con las capacidades de transporte utilizando una única identidad como suscriptor.

Lo anterior implica también un nuevo rol comercial que jugaran los proveedores de servicios de telecomunicaciones, para atender de manera oportuna y eficiente las diferentes demandas de los consumidores.

Sin embargo, a pesar de todas las ventajas mencionadas, surgen algunas preocupaciones como que la migración a NGN puede traer consigo un desarrollo desigual del despliegue de estas tecnologías tanto en países desarrollados como en aquellos en vías de desarrollo. Dado lo anterior, se espera que las áreas densamente pobladas sean atendidas primero y las áreas rurales más alejadas, escasamente pobladas y comercialmente menos factibles, sean atendidas después.

De esta manera, surge la necesidad de analizar un esquema de cobros con el mismo precio tanto para consumidores urbanos como rurales lo que constituiría una alternativa para atenuar las desigualdades entre grupos de consumidores o áreas geográficas.

Siguiendo este análisis, los consumidores con mayor capacidad de pago probablemente se moverán mucho más rápido a las NGN. Como el trafico migra hacia redes IP habrá menores consumidores generando ingresos por redes PSTN de servicios de voz. Es probable que los consumidores restantes de la red tradicional sean agrupados en locaciones más pobres y grupos demográficos.

Por otra parte la migración de redes PSTN podrían incrementar en promedio los costos por línea de las redes existentes y conducir al deterioro de la calidad de servicio. Todas estas posibles desventajas podrían atenuarse si los países en desarrollo adoptan una planeación optima de redes y aplicaciones innovadoras, ya que el acceso a NGN provee servicios en convergencia a costos más bajos, lo que constituiría una ventaja competitiva, aprovechable por parte de los operadores y los usuarios.

La disponibilidad de infraestructura basada en ip es una condición necesaria para la provisión de servicios NGN, lo cual puede traer consigue un ensanchamiento de la brecha tecnológica entre países en vías de desarrollo y países desarrollados. Debido a la existencia de segmentos de la población que tiene bajo o nulo acceso a los servicios de telecomunicaciones. De esta manera, el despliegue de infraestructura propia de las NGN en estas áreas, sería más costoso y menos rentable que si el despliegue se lleva a cabo en áreas urbanas densamente pobladas.

No obstante existe evidencia creciente que los mercados rurales alejados pueden responder significativamente a la provisión de nuevos servicios, especialmente si existen las condiciones regulatoria apropiadas. En este sentido, la gama de servicios convergentes provistos a través de las NGN pueden ofrecer acceso a estos servicios a un menor costo que los servicios de voz tradicionales, además, del ahorro en costos de operación que implica la adopción de plataformas tecnológicas basadas en IP.

1.1.2 Arquitectura NGN.

En una red clásica con tráfico de aplicaciones de datos y de valor agregado como la voz o el video, existe una frontera definida que separa sus dos dominios diferentes:

- Dominio de sistemas TDM.
- Dominio de sistemas IP.

Los sistemas TDM constituyen el grupo de centrales de conmutación que agregan tráfico desde los abonados hacia el resto de las etapas.

Los sistemas IP constituyen el grupo de centrales de conmutación que también agregan tráfico desde los abonados desde los abonados cuyo elemento básico es el paquete de datos hacia el resto de las etapas en lo que es conocido como capa de transporte.

Cuando ambos sistemas funcionan de forma simultánea y autónoma tendremos los sistemas independientes para los servicios digitales básicos de voz y otro para los servicios digitales de datos. Cuando ambos sistemas interactúan mutuamente mediante dispositivos denominados routers con interfaces PSTN tendremos los servicios de datos sobre redes conmutadas públicas.

En estas redes clásicas se tiene algunos servicios pero cada sistema que lo compone maneja una arquitectura propia e independiente, que impide el tratamiento y administración global de la información extremo a extremo. Así mismo los sistemas de facturación, asignación y gestión de los servicios, y los del manejo de la calidad de servicio por lo general son esencialmente independientes y autónomos dentro de cada dominio.

Por el contrario en la NGN existe un único elemento básico que es el paquete de la información y todo el sistema está diseñado para su administración, acceso, transporte y conmutación de extremo a extremo y basado en una única tecnología como se observa en la figura 1.

El sistema NGN está concebido para tratar tanto sea paquetes de voz, como de datos o video en forma totalmente transparente en una arquitectura única de extremo a extremo. Adicionalmente, la facturación, la asignación y gestión de

servicios, el manejo de la calidad de servicio y la planificación de la red se realiza sobre un sistema completo único para el dominio.

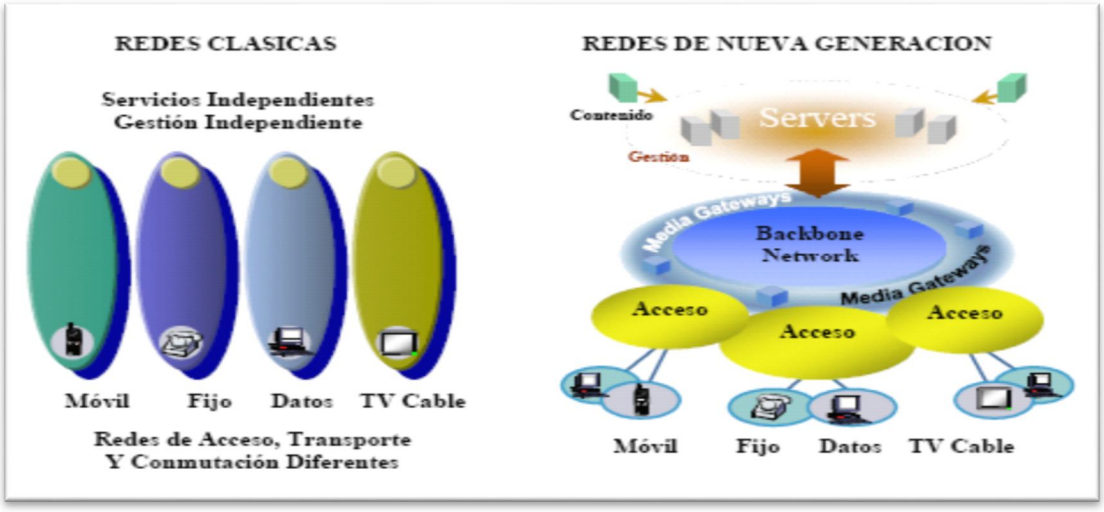


Figura 1: comparación redes clásicas vs redes de nueva generación.

En la figura 2 se muestra una arquitectura NGN de red convergente de voz y datos la arquitectura puede descomponerse en varias capas:

- Conectividad de núcleo.
- Acceso.
- Equipo de local del cliente (CPE).
- Gestión.

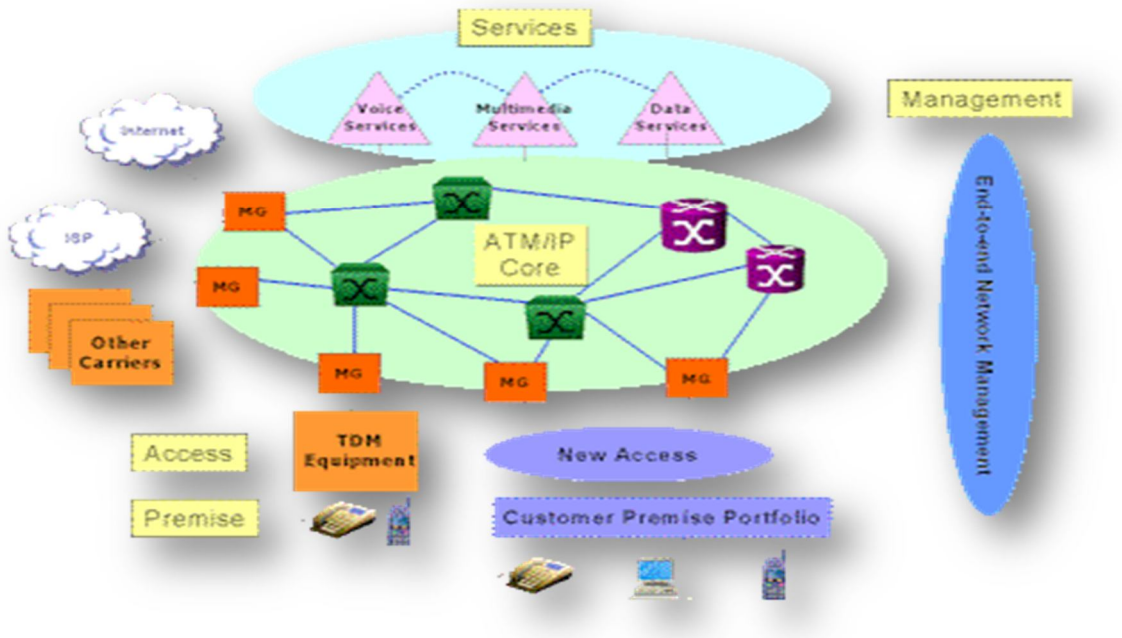


Figura 2 : Arquitectura convergente de voz, video y datos en redes de nueva generación.

- Capa de conectividad primaria.

La capa de conectividad de núcleo proporciona el encaminamiento y conmutación general del tráfico de la red de un extremo de esta al otro. Está basada en la tecnología de paquetes, ya sea ATM o IP. Y ofrece un máximo de flexibilidad. La tecnología que se elija dependerá de las consideraciones comerciales, pero la transparencia y la calidad del servicio deben garantizarse en cualquier caso, ya que el tráfico de los clientes no debe ser afectado por perturbaciones de la calidad, tales como las demoras, las fluctuaciones y los ecos.

Al borde de la ruta principal de paquetes están las denominadas pasarelas (Media GATEWAY), su función principal es adaptar el tráfico al cliente y de control a la tecnología de la NGN. Las pasarelas se interconectan con otras redes, en cuyo caso son llamadas pasarelas de red, o directamente con los equipos de usuarios finales, en cuyo caso se las denomina pasarela de acceso. Las pasarelas interfuncionan con los componentes de la capa de servicio, usando protocolos abiertos para suministrar servicios existentes y nuevos.

- Capa de acceso.

La capa de acceso incluye las diversas tecnologías usadas para llegar a los clientes. En el pasado, el acceso estaba generalmente limitado a líneas de cobre a través de canales DS1/E1.

En las NGN se observa una multiplicidad de tecnologías que han surgido para resolver la necesidad de un ancho de banda más alto, y para brindar a las empresas competidoras de comunicaciones un medio para llegar directamente a los clientes. Los sistemas de cable, xDSL, fibra e inalámbricos se cuentan entre las soluciones más prometedoras que están creciendo e introduciendo innovaciones rápidamente.

El equipo del local del cliente, ya sea de su propiedad o arrendado, proporciona la adaptación entre la red de la empresa explotadora y la red o equipo del cliente. Puede tratarse de un simple teléfono, pero podemos pero podemos apreciar una migración progresiva hacia dispositivos inteligentes que pueden trabajar con servicios de voz como de datos.

- Capa de servicio.

Esta capa contiene el sistema que proporciona los servicios y aplicaciones disponibles a la red. Los servicios se ofrecerán a toda la red, sin importar la ubicación del usuario. Dichos servicios serán tan independientes como sea posible de la tecnología de acceso que se use. El carácter distribuido de la NGN hará posible consolidar gran parte del equipo que suministra servicios en puntos situados centralmente, en los que pueda lograrse una mayor eficiencia. Además, hace posible distribuir los servicios en los equipos de los usuarios finales, en vez de distribuirlos en la red. Los tipos de servicio que se ofrecerán abarcaran todos los de voz existentes, y también una gama de servicios de datos y otros servicios nuevos de medios múltiples.

- Capa de gestión.

Esta capa, esencial para minimizar los costos de explotar una NGN, proporciona las funciones de dirección empresarial, de los servicios y de la red. Permite la

provisión, supervisión, recuperación y análisis del desempeño de extremo a extremo necesarios para dirigir la red.

1.2. MPLS el presente de las redes IP.

MPLS es un protocolo que se ubica entre la capa de red y la capa de enlace de datos del modelo OSI (como se muestra en la figura 3). Este es implementado en WAN y Backbones de proveedores de servicio. El protocolo MPLS describe los mecanismos para realizar la conmutación de etiquetas sobre la WAN. Funcionalmente el protocolo MPLS añade un cabecera MPLS a cada paquete IP que ingresa a la WAN, esta acción cambia la forma en como los enrutadores de la WAN envían y procesan los paquetes IP.

Lo que viaja por la WAN ahora son paquetes IP más una cabecera MPLS de 3 bytes. La cabecera MPLS es insertada sobre la capa de enlace de datos y bajo la capa de red. La cabecera MPLS consta de 4 campos un campo de etiquetas, campo de pila, campo experimental y campo TTL.

MPLS fue estandarizado en 1998 por la IETF en RFC 3031. Su objetivo inicial era proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión, permitiendo así sobre una misma red IP ofrecer todo tipo de servicios.

En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que atraviesa un router, lo cual supone que cada router pierda cierto tiempo dependiendo del tamaño de su tabla de enrutamiento, y además, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la calidad de servicio.

MPLS combina las ventajas del encaminamiento inteligente de nivel 3 con la rápida conmutación de nivel 2, utilizando para ello la conmutación de paquetes por una pequeña etiqueta antes mencionada de longitud fija consiguiendo de este modo un mayor rendimiento en el transporte de paquetes IP.

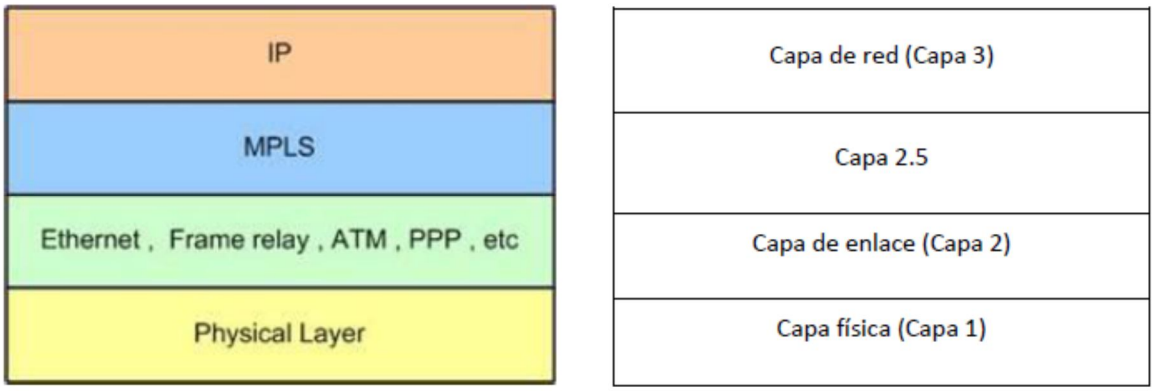


Figura 3 : posición de MPLS en el modelo OSI.

Como ya hemos comentado anteriormente, la necesidad de las operadoras de que sus redes tuviesen una cierta calidad de servicio, ha llevado a la búsqueda de una tecnología que ofreciese ese QoS por sí misma. Las tecnologías como ATM o SDH se han quedado obsoletas y aplicar calidad de servicio es una tarea muy complicada.

Por estas razones surgió MPLS. Es una tecnología orientada a paquetes muy flexible. En la figura 1 vemos si la situásemos en el modelo ISO/OSI (International Standard Organization / Open System Interconnection) se encontraría en la capa 2.5, entre la capa de enlace y de red, o sea, entre la capa 2 y 3. El hecho de que se encuentre entre dos capas, le proporciona el nombre de “Multi Protocol”. Este hecho le da la ventaja de poder usar las características de los protocolos de las capas adyacentes sin ninguna restricción.

Además de esto, MPLS ofrece adaptación total a IP. Esto es de gran importancia porque actualmente el mundo se mueve con este protocolo.

El estándar MPLS abarca la utilización de IPv4 e IPv6 sobre las principales tecnologías de nivel 2 orientadas a la conmutación de paquetes. Por ello mediante MPLS se consigue también una mayor integración y una menor complejidad en la parte de control de los distintos dispositivos de la red IP. Pues

los caminos de tráfico o LSP, son creados utilizando los mismos protocolos de señalización y de distribución de etiquetas como se muestra en la siguiente figura.

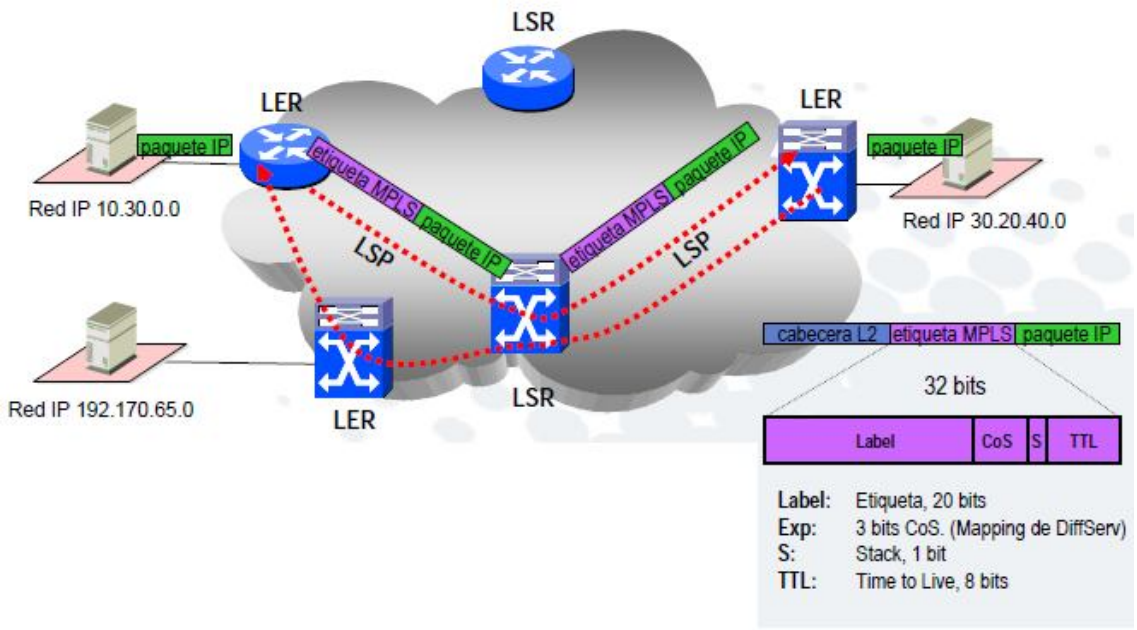


Figura 4 : Esquema de conmutación de etiquetas.

Los elementos de una red MPLS son los siguientes:

- **LER** (*Label Edge Router*): Elemento que inicia o termina el túnel (pone y quita cabeceras), es decir, es el elemento de entrada/salida a la red MPLS (hace de interfaz con otras redes). Un *router* de entrada se conoce como *Ingress Router* (*router* de ingreso) y uno de salida como *Egress Router* (*router* de egreso). Ambos se suelen denominar *Edge Label Switch Router* ya que se encuentran en los extremos de la red MPLS.

- **LSR** (*Label Switching Router*): Elemento que conmuta etiquetas. Funcionan a gran velocidad y participan en el establecimiento de LSPs

- **LSP** (*Label Switched Path*): Son circuitos que van de extremo a extremo de la red, es decir, una LSP es un túnel MPLS establecido entre los extremos. Esta ruta es creada por la concatenación de uno o más saltos conmutados de etiqueta, permitiendo a un paquete ser enviado mediante canjeo de

etiqueta desde un nodo MPLS a otro nodo MPLS. Una LSP en MPLS es unidireccional.

- **Túnel LSP** (*Label Switched Path Tunnel*): Una LSP la cual es usada para tunelar bajo el encaminamiento normal IP y/o mecanismos de filtrado.

- **LDP** (*Label Distribution Protocol*): Es un protocolo de MPLS para la distribución de etiquetas MPLS.

- **FEC** (*Forwarding Equivalence Class*): Nombre que se le da al tráfico que se encamina bajo una etiqueta. De hecho, un FEC es un conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino.

1.2.1 Cabecera MPLS

Figura 5 : Cabecera MPLS que se agrega al paquete IP.

Dónde:

- **Label** (20 bits): Es la identificación de la etiqueta.

- **Exp** (3 bits): También se puede llamar CoS o QoS. Afecta al encolado y al descarte de paquetes.

- **S** (1 bit): Del inglés *stack*, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay más etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.

- **TTL** (8 bits): *Time-to-Live*, misma funcionalidad que en IP, se decremento en cada enrutador y, al llegar al valor de 0, el paquete es descartado.

1.3 Funcionamiento del MPLS

En el ingreso de una red MPLS, los paquetes IP entrantes se examinan y se les asigna una "etiqueta" (figura 5) a través de un *router* (LER). Los paquetes etiquetados entonces se remiten a lo largo de una LSP, donde cada router LSR toma una decisión para la conmutación basándose en el campo de la etiqueta (*label*) del paquete.

Un LSR no necesita examinar las cabeceras IP de los paquetes para encontrar un puerto de salida (salto siguiente), lo que hace es quitar simplemente la etiqueta existente y aplicar una nueva etiqueta para el salto siguiente. La base de la información de la etiqueta (LIB) proporciona una etiqueta saliente (que será insertada en el paquete) y un interfaz saliente (basado en una etiqueta entrante y en un interfaz entrante). Para cada servicio específico, se crea una tabla para una clase de equivalencia de la expedición (FEC) y para representar un grupo de flujos con los mismos requisitos de ingeniería de tráfico. De esta manera, una etiqueta específica está limitada a un FEC. Cada FEC puede representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija, además la clase FEC a la cual se asigna el paquete, se codifica como un valor corto de longitud fija conocido como *etiqueta*.

La señalización para establecer un tráfico-dirigido LSP se hace usando un protocolo de distribución de etiqueta que funcione para cada nodo de MPLS. Hay

bastantes protocolos de distribución de etiqueta, los dos más populares son el RSVP y el CR-LDP.

El marco de MPLS incluye extensiones a los protocolos existentes en el encaminamiento y en el estado de acoplamiento del protocolo IP. Estos protocolos proporcionan la coordinación en tiempo real de la topología actual de la red, incluyendo cualidades de cada acoplamiento. Las extensiones de MPLS al OSPF y al IS-IS permiten que los nodos no sólo intercambien información sobre la topología de la red, sino también la información del recurso, las direcciones IP, la anchura de banda disponible, y las políticas de carga que balancean.

1.4 ventajas que ofrece MPLS.

Entre las principales ventajas que MPLS puede aportar cabe destacar los siguientes:

- Ahorro de costos: dependiendo de la combinación especifica de aplicaciones y de la configuración de red de una empresa, los servicios basados en MPLS pueden reducir los costos entre un 10 y un 25% frente a otros servicios de datos compatibles y a medida que se vayan añadiendo a las infraestructuras de networking el tráfico de video y voz, los ahorros de costos empiezan a dispararse alcanzando niveles de hasta un 40%.

- Soporte de QoS: uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y video en las redes de datos.

- Rendimiento mejorado: debido a la naturaleza de “muchos a muchos” de los servicios MPLS, los diseñadores de red pueden reducir el número de saltos entre puntos, lo que se traduce directamente en una mejora de los tiempos de respuesta y el rendimiento de las aplicaciones.

- Simplifica el paradigma de envíos aumentando las prestaciones precio/rendimiento y el tiempo de vida en el mercado.

- Permite a los switch ATM ser utilizados como routers (LSR).

- Él envió es independiente de la capa de red, capas inferiores y los criterios empleados para asociar paquete en clases de equivalencia. Además los cambios en estos criterios son transparentes, aportando robustez en los posibles cambios de decisiones futuras.

- El criterio de envió no está basado exclusivamente en la cabecera del paquete. Estos criterios pueden llegar a ser tan complejos como se desee, sin que tengan ningún efecto negativo sobre los LSR internos de la red.

- El etiquetado es un mecanismo más eficiente que el encapsulado para emplear túneles.

- El envío MPLS puede utilizar switches que no puedan analizar las cabeceras de la capa de red. Basta con que puedan sustituir las etiquetas de los paquetes.

- Un paquete que entre en la red por un router concreto puede ser etiquetado de manera distinta que en el caso de haber entrado por otro router, como resultado, las decisiones de envío que dependen del router de entrada pueden realizarse fácilmente

- Recuperación entre desastres: los servicios basados en MPLS mejoran la recuperación ante desastres de diversas maneras. En primer lugar, permiten conectar los centros de datos y otros emplazamientos clave mediante múltiples conexiones redundantes a la nube MPLS y a través de ella, a otros sitios de la red. Además, los sitios remotos pueden ser reconectados fácil y rápidamente a las localizaciones, de respaldo en caso de necesidad; a diferencia de lo que ocurre con las redes ATM y Frame Relay, en las cuales se requieren circuitos virtuales de respaldos permanentes o conmutados.

1.5. Diferencias entre GMPLS y MPLS

El MPLS generalizado (GMPLS) difiere del tradicional MPLS en que soporta múltiples tipos de conmutación, por ejemplo la adición de soporte para TDM (*time division Multiplexing*), lambda, y conmutación de fibra (puerto). El soporte para los tipos adicionales de conmutación ha conducido a GMPLS a extender
ciertas funciones base del MPLS tradicional y, en algunos casos, añadir funcionalidad. Estos cambios y adiciones impactan básicamente en las propiedades de las LSPs (*label SwitchedPath*) en cuanto a cómo las etiquetas son solicitadas y comunicadas, a la naturaleza unidireccional de las LSPs (*label SwitchedPath*), a cómo los errores son propagados, y a cómo la información es producida para sincronizar el LSR de ingreso y de egreso.

1.6. Ampliaciones de MPLS para soporte de GMPLS

El destacamento de fuerzas de la ingeniería internacional (IETF) ha extendido el conjunto de los protocolos MPLS para incluir los dispositivos que conmutan en tiempo, en longitud de onda, (p.ej. DWDM) y en los dominios del espacio (p.ej. OXC (*opticalcross-connect*)) vía GMPLS. Esto permite que las redes basadas en GMPLS encuentren a su disposición una trayectoria óptima basada en los requisitos de tráfico del usuario, para un flujo que potencialmente comience en una red IP, sea transportado por SONET, y después se cambie con una longitud de onda específica en una fibra física específica.

Dominio de la conmutación	***Tipo de trafico***	***Esquema de la expedición***	***Ejemplo del dispositivo***	***Nomenclatura***
Paquete célula	***IP, AsynchronousTransferMode (ATM)***	***conexión virtual del canal (VCC)***	***router IP, Switch ATM***	***PSC (packetSwitchcapable)***
Tiempo	***TDM/SONET***	***Ranura de tiempo en la repetición del ciclo***	***Sistema con conexión digital a través de***	***TDM (time divisiónMultiplexing)***

			él (DCS), ADM	
Longitud de onda	***Transparente***	***Lambda***	***DWDM***	***LSC (layerSwitchcapable)***
Espacio físico	***Transparente***	***Fibra, línea***	***OXC (Optical cross-connect)***	***FSC (FiberSwitchcapable***

La Tabla 1 ofrece un resumen del marco de GMPLS.

1.6.1. DWDM

La DWDM (*Dense Wavelength Division Multiplexing*) es una técnica de multiplexación eficiente en cuanto a coste que ofrece unas ventajas técnicas considerables. La DWDM incrementa la capacidad del ancho de banda de transporte de una sola fibra óptica debido a la creación efectiva de múltiples fibras virtuales, cada una transportando multigigabit de tráfico por segundo, en una sola fibra. Esto provoca un incremento en el ancho de banda mientras se mejora la infraestructura de fibra existente. Asimismo, las conexiones a través de conmutadores ópticos (OXCs), son adecuadas para emerger como la opción favorita para la conmutación multigigabit o incluso para flujos de datos de Tera bits, desde que es evitado el procesado electrónico del paquete.

Se espera que el tráfico predominante que se transporte por las redes de datos futuras esté basado en IP, ya que la multiplexación estadística basada en IP es adecuada para ser la tecnología de multiplexación predominante para flujos de datos más pequeños que aquellos que son apropiados para DWDM.

1.7. Tecnologías GMPLS un sistema de convergencia para redes IP.

El enrutamiento IP ha evolucionado para incluir nuevas funcionalidades desarrolladas en la arquitectura MPLS (multiprotocol label switching). Recientemente se ha extendido MPLS como un plano de control que puede utilizarse con nuevos dispositivos como los OXCs. Esta generalización proporciona el plano de control común estandarizado necesario en la evolución de

redes ópticas abiertas e interoperables. En primer lugar, un plano de control común simplifica las operaciones y la gestión, lo que reduce el costo de las operaciones. En segundo lugar, un plano de control común proporciona un amplio rango de escenarios de desarrollo.

GMPLS (RFC-3945) nace con la idea de poder aplicar un único plano de control universal para cualquier topología de transporte (redes WDM, redes TDM, etc.). Esta arquitectura tiene por objetivo generalizar el protocolo MPLS de forma que se pueda realizar conmutación de cualquier tipo de recursos. Los protocolos en los que se basa fueron diseñados e implementados para aplicar mecanismos Ingeniería de Tráfico a redes MPLS. Estos mecanismos se utilizan para dar la posibilidad de establecer tráfico de datos en un camino pre computado en la red, de forma que podamos maximizar la utilización de los recursos de red disponibles. Así podemos encaminar tráfico evitando puntos saturados de la red o elegir enlaces que cumplan los requisitos de calidad de servicio.

Una red óptica se compone de un conjunto de OXC (*Optical Cross Connects*) unidos formando una topología arbitraria, cuya función es la de proveer conectividad a diferentes subredes IP/MPLS. El mecanismo de transporte en estas redes, es una longitud de onda, es decir, una señal óptica. Con GMPLS, el *backbone* formado por los OXC y las subredes IP/MPLS comparte funciones comunes en el plano de control, permitiendo la integración de las redes ópticas en la estructura global de Internet como se observa en la figura 6.

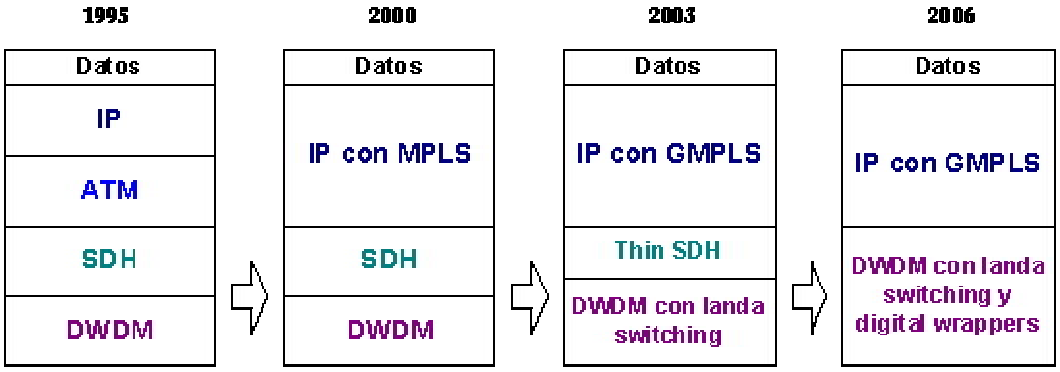


Figura 6 : Evolución hacia GMPLS en redes fotonicas.

1.8. Arquitectura de red de próxima generación.

El modelo de red ASON (Automatically Switched Optical Network) mostrado en la figura 7 es el resultado de este auge de las tecnologías de redes ópticas, y lo que se busca con esta arquitectura es el desarrollo de una red óptica conmutada en todos sus ámbitos: plano de control, datos y gestión. Esta arquitectura nos define los componentes de la capa óptica de control y sus interacciones, de tal forma que se permita el establecimiento y finalización de conexiones a partir de peticiones directas desde el usuario (cliente). Para soportar las posibles peticiones de diferentes clientes, la arquitectura define los componentes, puntos de referencia y reglas que hay que aplicar en las distintas interfaces entre los clientes y las redes (dominios) y entre distintas redes entre sí.

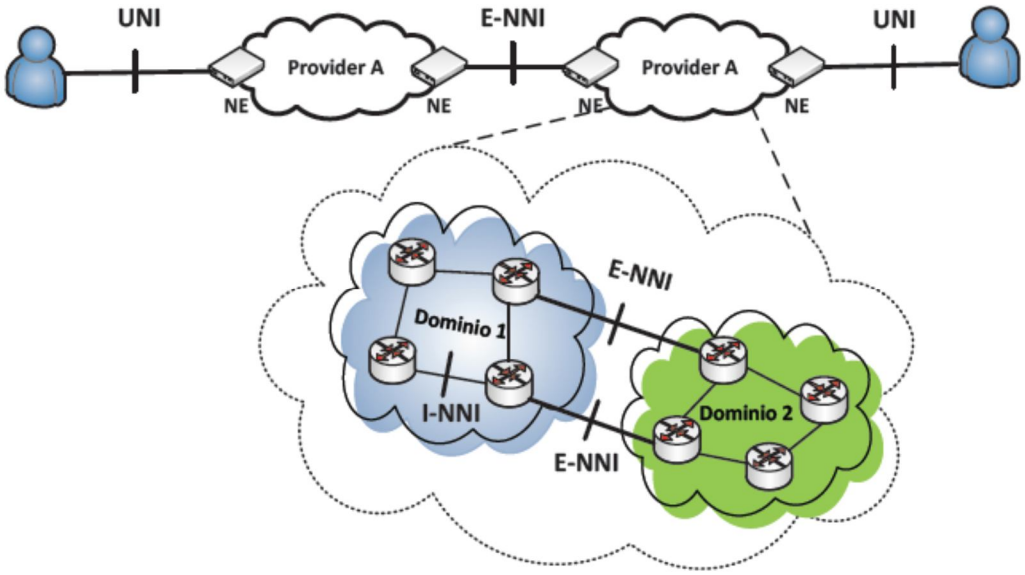


Figura 7 : Esquema del modelo de red ASON.

A continuación se explica la utilidad de los distintos puntos de referencia de la arquitectura:

- *User-to-Network Interface* (UNI): se encuentra en el borde la las redes (dominios) y se utiliza para pedir un servicio punto a punto de esa red.

- *External Network-to-Network Interface* (E-NNI): se encuentra situado entre subredes o dominios de red y se encarga de transmitir la petición de servicio entre esas regiones.

- *Internal Network-to-Network Interface* (I-NNI): se encuentra situado entre los elementos de red de una subred y se encarga de que se realice el servicio a través de dicha subred.

GMPLS nos aporta el conjunto de protocolos (mostrados en la figura 10)que se encargan de organizar el funcionamiento y distribución de conexiones entre las distintas subredes que forman Internet. Cada red puede tener distintas capacidades de conmutación, por lo que GMPLS se encarga de gestionar todas ellas.

Mientras que ASON define una arquitectura, el plano de control GMPLS implementa unas funcionalidades. Mezclando las funcionalidades de GMPLS junto con la arquitectura de ASON se puede conseguir una solución de plano de control para las redes de transporte. Con ello podemos realizar un establecimiento y gestión automatizado de conexiones en toda la red.

1.9. GMPLS: El siguiente paso.

La conmutación de etiquetas multiprotocolo generalizada corresponde al siguiente desarrollo evolutivo desde MPLS con ingeniería de Tráfico (MPLS-TE) encaminado a proporcionar características de redes orientadas a entornos no orientadas a conexión. Debido a la necesidad de asignar el tráfico IP directamente sobre la capa óptica (ver modelo en la figura 7) para reducir la complejidad de las conexiones y permitir la rápida asignación del ancho de banda y flexibilidad IP. GMPLS extiende MPLS para abarcar división de tiempo (por ejemplo, SONET / SDH, PDH), longitud de onda (lambda) y la conmutación en el espacio.

GMPLS abarca, además de los routers IP y los switches ATM, dispositivos como conmutadores digitales de señales multiplexadas en el tiempo (DXC), conmutadores de longitudes de onda con conversión electroóptica (OXC) y los Photonic Cross Connect (PXC) . Para ello, GMPLS extiende ciertas funciones base del tradicional MPLS y, en algunos casos, añade nueva funcionalidad. Estas adaptaciones han supuesto la extensión de los mecanismos de etiqueta y de LSP para crear labels generalizados y G-LSP (Generalized LSP); afectando también los protocolos de encaminamiento y señalización para actividades tales como la distribución de etiquetas, la ingeniería del tráfico, y la protección y restauración de enlaces.

Entre sus funciones principales se encuentran:

- Descubrimiento de vecinos: Con el fin de gestionar el backbone, cada componente conectado debe ser conocido de antemano. Entre otros dispositivos se incluye switches, routers, multiplexores y conmutadores.

- Difusión de estado del enlace: En GMPLS, los protocolo de enrutamiento de primero el camino más corto (OSPF) y de sistema intermedio a sistema intermedio (IS-IS) son modificados para tal fin, añadiéndose vínculos de tipo TE.

- Gestión de rutas: El protocolo de distribución de etiquetas (CR-LDP) y el de reservación de recursos con Ingeniería de tráfico (RSVP-TE) se encargan del proceso de señalización.

- Gestión de enlaces: Necesaria para desarrollar y lanzar un total de canales ópticos con el fin de aumentar la escalabilidad.

- Protección y recuperación: Se pueden crear una estructura malla que permita la aparición de un número de caminos diferentes.

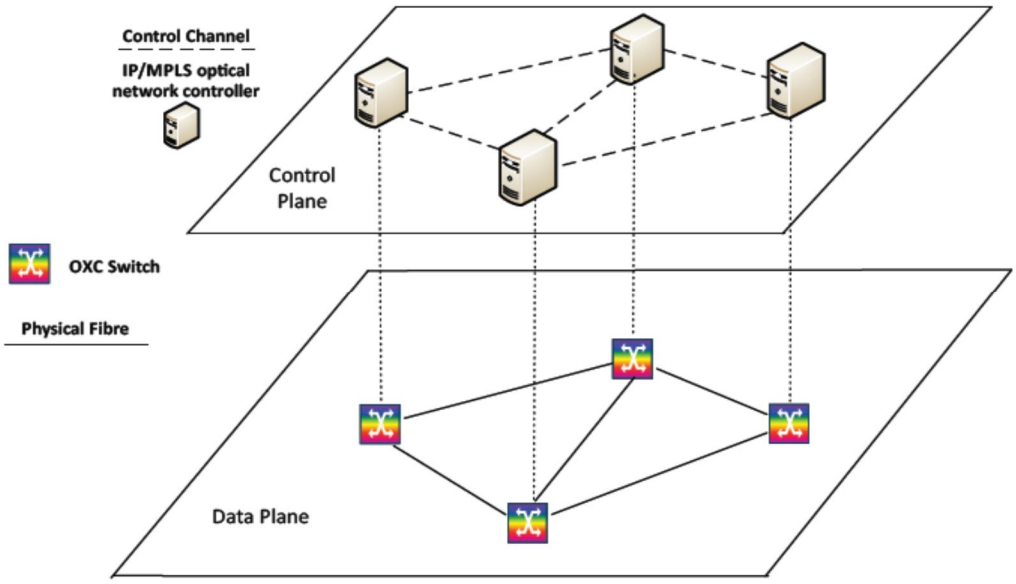


Figura 8 : Modelo GMPLS basado en una red óptica.

GMPLS extiende las funciones de MPLS para que se puedan soportar múltiples tipos de jerarquías de conmutación y distintos niveles de conmutación en GMPLS. Conmutación TDM, lambda y por fibra (puerto). Para incluir estos tipos adicionales de conmutación se han extendido ciertas funciones base de MPLS. Estos cambios y añadidos afectan las propiedades básicas de los LSP, cómo se solicitan y comunican las etiquetas, la naturaleza unidireccional de los LSP, cómo se propagan los errores y la información proporcionada para sincronizar los LSR de entrada y salida (frontera).

La arquitectura original de MPLS se ha extendido para incluir un nuevo conjunto de interfaces en los LSR. Estas interfaces se clasifican en:

- Interfaces PSC: Packet Switch Capable. Estas interfaces reconocen los límites de paquetes y pueden enviar datos basándose en el contenido de la cabecera de paquete.

- Interfaces L2SC: Layer-2 Switch Capable. Estas interfaces reconocen los límites de tramas/celdas y pueden enviar datos basándose en el contenido de la cabecera de las tramas/celdas.

- Interfaces TDM: Time-Division Multiplex Capable. Estas interfaces enrutan los datos basándose en la ranura temporal de los datos dentro de un ciclo de repetición.

- Interfaces LSC: Lambda Switch Capable. Estas interfaces enrutan los datos basándose en la longitud de onda sobre la que se reciben los datos.

- Interfaces FSC: Fiber-Switch Capable. Estas interfaces enrutan los datos basándose en la posición en que se reciben éstos en el espacio físico (puerto).

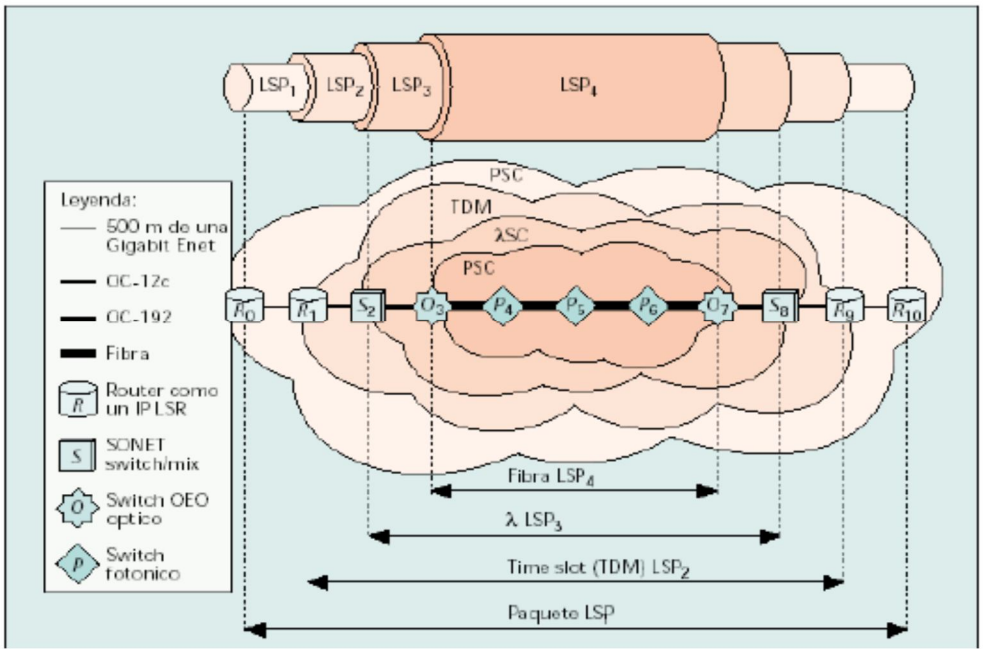


Figura 9 : Jerarquía de los LSP.

GMPLS soporta cinco interfaces: interfaz de conmutado de paquetes, interfaz de conmutado a nivel 2, interfaz de multiplexado por división de tiempo, interfaz de conmutado por longitud de onda y interfaz de conmutado de fibra.

Un interfaz de conmutado de paquetes reconoce los límites del paquete y puede encaminar paquetes basándose en la cabecera IP. Un interfaz de conmutado de nivel 2 reconoce los límites de una célula o “frame” y puede encaminar los datos basándose en el contenido de la cabecera de la célula o “frame”. El ejemplo de ATM que encaminan células basándose en su valor VPI/VCI o switches Ethernet que encaminan el tráfico basándose en la información de MAC.

Un interfaz de multiplexado por división de tiempo encamina datos basándose en las ranuras temporales que forman tramas, “frames” en el caso SONET/SDH. Un interfaz de conmutado por longitud de onda encamina señales ópticas de una longitud de onda entrante a otra saliente. Como ejemplo los OXCs que operan a nivel de longitud de onda individual. Interfaz de conmutado por fibra encamina señales de una o más fibras de entrada a una o más fibras de salida. Como ejemplo los OXCs que operan a nivel de fibra.

La jerarquía de GMPLS permite a la red operar con distintos tipos de conmutación, los cuales nos definen las unidades de datos que cada dispositivo puede manejar y conmutar. Es decir, nos definen el nivel al que se puede demultiplexar las señales de datos entrante sale al nodo por una interfaz, conmutarlas y enviarlas por otra interfaz. Para crear dicha jerarquía se definen los siguientes procedimientos:

- Un LSR crea un Label Switched Path (LSP) usando *Traffic Engineering LabelSwitched Path (TE LSP).* Un Label Switch Router (LSR) es la manera de denominar a los routers que soportan GMPLS.

- El LSR se encarga de formar una Forwarding Adjacency (FA) a partir de un LSP. Mencionar que esto solamente es posible en caso de que los LSPs que forman el FA están controlados por la misma instancia del plano de control, es decir, si el plano de control es integrado.

- Se permite a otros LSRs usar FAs para la computación de los caminos.

- Usando otros LSPs creados por otros LSRs para crear el suyo propio.

Para hacernos idea práctica, cada conexión que establecemos esta caracterizada por una tecnología de conmutación. En una red multicapa estas conexiones se pueden combinar para dar lugar a nuevas conexiones de diferentes tecnologías. No todas las combinaciones son posibles, por ello GMPLS define una jerarquía a partir de las tecnologías de plano de datos disponibles, y a partir de las interfaces de adaptación que hay definidos.

GMPLS tiene la función de cubrir las siguientes tareas:

- Autodescubrimiento de la topología de la red. Cada vez que se conecta un nuevo elemento de red, se le notifica automáticamente información sobre sus vecinos.

- Anuncio de recursos disponibles. Además de tener información sobre la topología de la red, puede conocer el estado de los recursos disponibles en ésta.

- Gestión de los enlaces disponibles. Se encarga de la gestión de cada uno de los enlaces que forman parte de una ruta o LSP, de forma que tienen que ser establecidos, reservados o liberados según los requerimientos de la red.

- Encaminamiento de paquetes. Con la información que se posee del estado de la red, se realiza una computación de caminos mediantes algoritmos para selección la ruta óptima, aplicando restricciones de ingeniería de tráfico.

- Gestión del camino. Incluye distribución de etiquetas, así como establecimiento, gestión y terminación de la ruta. Estas funcionalidades están cubiertas por el plano de control, el cual se organiza con una serie de módulos que se muestran en el diagrama de la Figura 10.

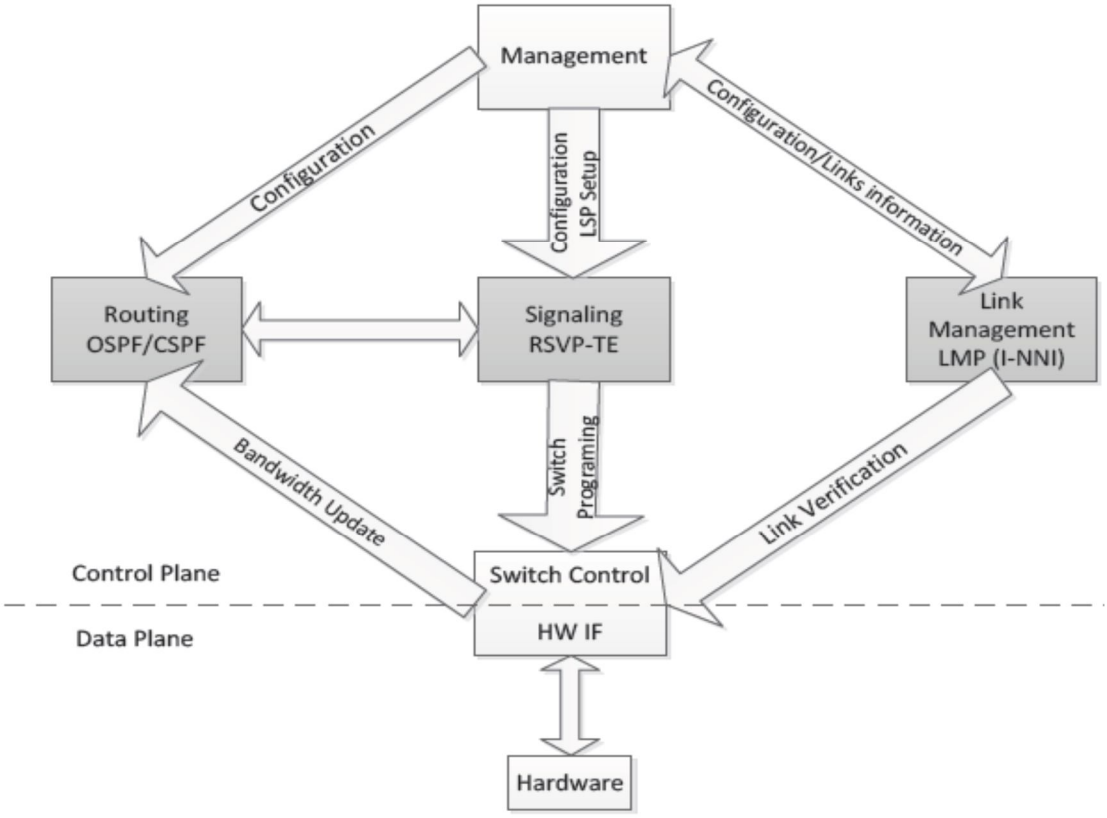


Figura 10 : Diagrama de funcionalidad del plano de control.

Capitulo2. Los protocolos que componen las funciones de la arquitectura MPLS.

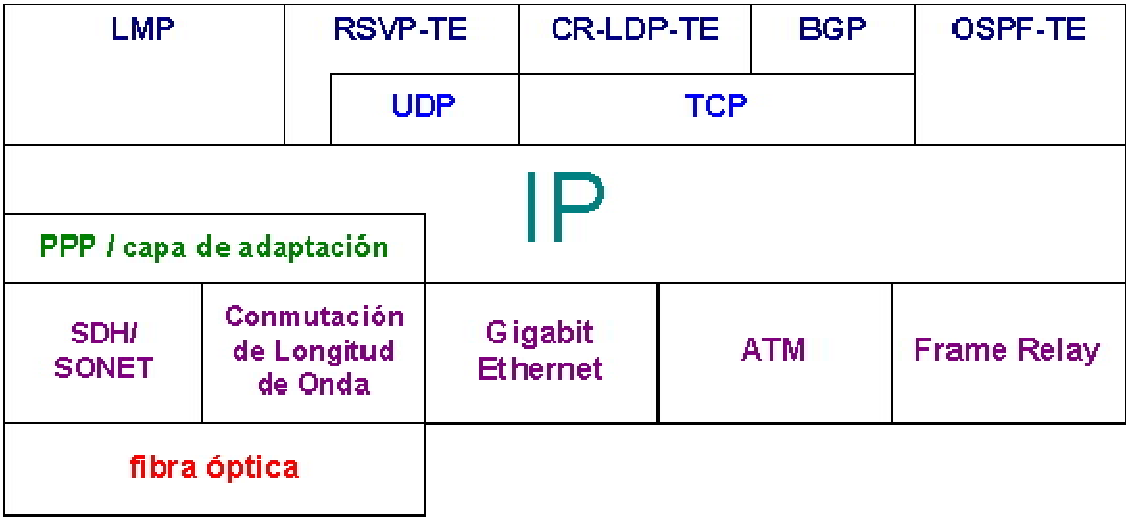


Figura 11 : pila de protocolos MPLS y GMPLS.

En GMPLS se utiliza la distribución de etiquetas ya comentamos que es una evolución de MPLS, Algunas formas nuevas de etiquetas son necesarias para soportar la amplia visión de GMPLS en el dominio óptico y en el multiplexado por división temporal. La nueva etiqueta no sólo permite que las etiquetas tradicionales viajen junto con el paquete asociado también permite que las etiquetas identifiquen ranuras temporales, longitudes de onda o fibras. Los protocolos de distribución de etiquetas LDP y RSVP. Los protocolos interiores ISIS y OSPF también han sido extendidos para poder utilizarse con las tecnologías ópticas. También se ha desarrollado un protocolo administrar el nivel de enlace en redes ópticas, el protocolo LMP (Link Management Protocol) todos estos mostrados en la figura 11.

2.1 OSPF-TE

El protocolo OSPF se utiliza para diseminar la información de topología e ingeniería de tráfico y construir una base de datos de ingeniería de tráfico(ver figura 12). OSPF es capaz de diseminar la información de la topología de red y de la ingeniería de tráfico por ejemplo el ancho de banda disponible en los enlaces, grupos de riesgo compartido a los que pertenece.

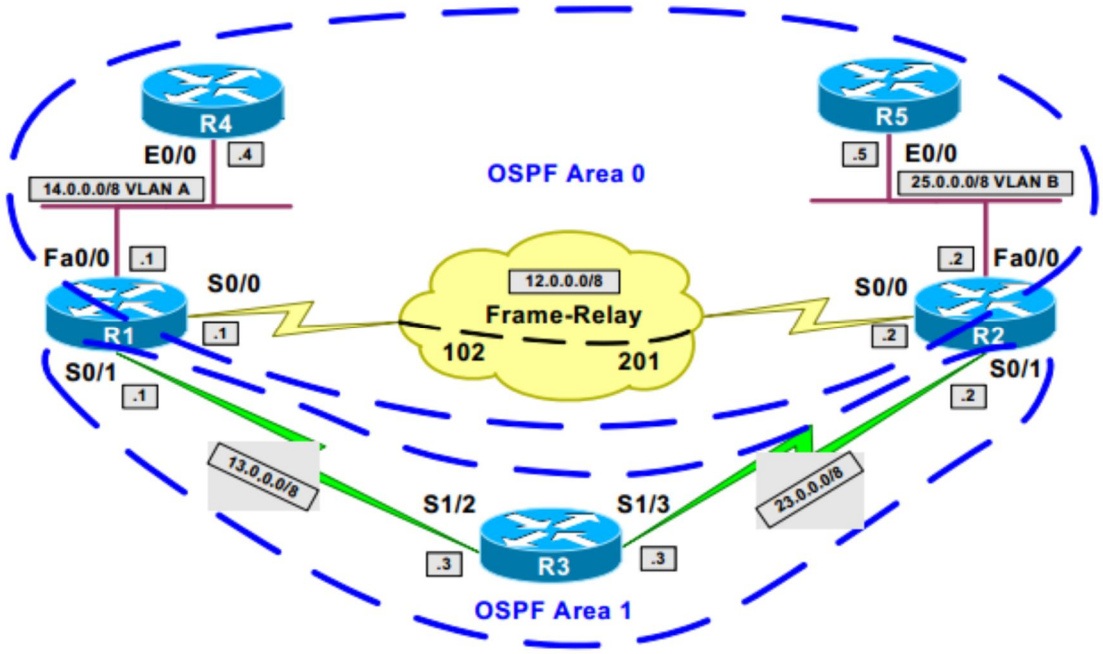


Figura 12 : Protocolo open shortest path first.

Mediante la información que se obtiene a partir de OSPF-TE se puede construir una base de datos de ingeniería de tráfico. Para que OSPF pueda soportar GMPLS se definen una serie de mejoras en las propiedades de la ingeniería de tráfico de los GMPLS-TE links para que puedan ser notificados en OSPF-TE como maquinas en los campos binarios de los paquetes.

Cada “host” debe convertir los datos de su propia representación interna al orden de byte de la red antes de enviar un paquete, lo mismo tiene que hacer el destinatario cuando reciba un paquete. Naturalmente, el campo de datos en el paquete está exento de este estándar, cada usuario es libre de elegir el formato de datos

2.2 RSVP-TE

El protocolo RSVP se encarga de la señalización de rutas para la reserva de recursos de flujos de datos tanto multicast como unicast. A este protocolo se le han hecho extensiones de ingeniería de tráfico para que pueda soportar el establecimiento de túneles en MPLS. Mediante esta extensión, RSVP-TE consigue la señalización de túneles LSP para que sean automática y fácilmente

reconfigurables ante posibles incidentes de la red como fallos, congestión de red o cuellos de botella.

También se han definido las extensiones necesarias de RSVP-TE para GMPLS. Con estas extensiones, en GMPLS conseguimos definir los LSP como TE-Links que son los enlaces entre dos nodos con propiedades de ingeniería de tráfico. Definiendo los LSP de esta manera estos pueden ser usados para formar otros LSP, a los que se les denomina en terminología MPLS/GMPLS como “Forwarding Adjacency links”. Cabe mencionar que esto solamente es posible si el plano de control es el mismo para los LSP que forma el FA Link.

Una ventaja de usar el RSVP para establecer túneles LSP, es que permite la asignación de los recursos a lo largo de la ruta. Por ejemplo, el ancho de banda puede ser asignado a un túnel LSP usando reservas RSVP estándar y clases de servicio de Servicios Integrados.

Cabe decir que las reservas de recursos son útiles, pero no son obligatorias. En realidad, una LSP puede ser instanciada independientemente de la reserva de los recursos. Tales LSPs sin reservas de recursos pueden ser usadas, por ejemplo, para llevar tráfico *best effort*. Estos pueden también ser usados en muchos otros contextos, incluyendo la implementación de retardos (*fall-back*) y las políticas de recuperación bajo condiciones de errores, etc.

2.3. Protocolo CR-LDP (Constraint-Based Routing Label Distribution Protocol)

Este protocolo, es una variante del protocolo de encaminamiento LDP que incluye restricciones (CR, *Constraint-based routing*). Su uso está sujeto a restricciones en la elección de la ruta a seguir, como pueden ser el ancho de banda máximo a utilizar, el retardo máximo, la QoS mínima, etc.

El CR-LDP también proporciona mecanismos para establecer y mantener LSPs encaminadas explícitamente, de hecho, estos mecanismos son definidos como extensiones del protocolo LDP. Las capacidades opcionales adicionales incluidas tienen un impacto mínimo en la ejecución del sistema y en sus requerimientos, cuando no están en uso para una LSP encaminada explícitamente. Las capacidades proporcionan capacidad de negociación de servicios LSP y parámetros de administración del tráfico sobre y bajo deliberación de paquete *best-effort*, incluyendo asignación de ancho de banda, configuración y prioridades de mantenimiento. El CR-LDP, opcionalmente, permite que estos parámetros sean modificados dinámicamente sin interrupción de la LSP operacional.

Debido a que el LDP es un protocolo punto a punto (*peer-to-peer*) basado en el establecimiento y el mantenimiento de sesiones TCP, existen los siguientes beneficios naturales:

- Los mensajes CR-LDP son deliberados de fuentes fidedignas por el subyacente TCP, y la información de estado asociada con las LSPs encaminadas explícitamente no requiere un refresco periódico.

- Los mensajes CR-LDP son controlados en cuanto a flujo (filtrados) a través del TCP.

También está designado para soportar adecuadamente los variantes tipos de medios de comunicación para los que MPLS fue designado para soportar (ATM, FR, Ethernet, PPP, etc.).

El CR-LDP es aplicable en aquellas partes de Internet donde números muy grandes de LSPs pueden necesitar ser conmutados en cada LSR. Un ejemplo de esto serían las redes de *backbone* grandes, que usan el GMPLS exclusivamente para transportar números muy grandes de flujos de tráfico entre un número moderadamente grande de nodos extremos MPLS.

El CR-LDP puede también ser aplicable como un servicio mediador entre redes que proporcionan extensiones de servicio similares usando modelos de señalización que varían significativamente.

La implementación del CR-LDP y su desarrollo no requiere todas las funcionalidades definidas en la especificación del LDP, sin embargo, el CR-LDP requiere una combinación específica de los modos de distribución de etiqueta: distribución de etiqueta ordenada *downstream on demand* y modo de retención de etiqueta conservativo.

Aunque el CR-LDP es definido como una extensión para el LDP, el soporte para el anuncio de la etiqueta no solicitada *downstream* y los modos de control independientes no son requeridos para el soporte de rutas explícitas estrictas. Además, las implementaciones del CR-LDP pueden ser capaces de soportar rutas explícitas suaves a través del uso de nodos abstractos y/o rutas explícitas jerárquicas, sin usar el LDP para la configuración LSP salto-a-salto.

El CR-LDP también incluye soporte para rutas explícitas. El uso de esta capacidad permite al operador de red definir una ruta explícita a través de partes de su red con un conocimiento imperfecto de la entera topología de la red.

Limitaciones:

- La especificación CR-LDP solo soporta LSPs punto-a-punto. Las LSPs Multi-punto-a-punto y punto-a-multi-punto son para un estudio posterior.

- La especificación CR-LDP solo soporta una configuración LSP unidireccional. La configuración LSP bidireccional es FFS.

- La especificación CR-LDP solo soporta una única asignación de etiqueta por configuración de cada LSP. Las asignaciones de etiqueta múltiple por configuración LSP son FFS.

Finalmente, habría que aclarar que tanto el CR-LDP como el RSVP-TE son dos protocolos de señalización que ejecutan funciones similares en las redes GMPLS. No hay consenso actualmente sobre que protocolo es técnicamente superior. Por lo tanto, los administradores de red harán una elección entre los dos teniendo en cuenta sus necesidades y la situación particular.

2.4. LMP

El protocolo LMP es el protocolo de gestión de enlaces, se encarga de gestionar el correcto funcionamiento de los enlaces, verificación de los enlaces y comprueba conectividad entre nodos adyacentes. Para el establecimiento de una sesión LMP tenemos que tener siempre disponible un canal físico para utilizarlo como canal de control.

A continuación mostramos la secuencia de mensajes que se intercambian entre los dos nodos en la Figura 13. Lo primero que tienen que conocer son las interfaces usadas por los *data links* a ambos extremos del enlace para poder enviarse los *Test Messages*, por lo que se intercambian una serie de mensajes por un canal de control bidireccional para poder realizar el mapeo de interfaces o puertos en cada extremo de los data links (tendremos 2 Interface IDs por cada data link que contenga el TE Link).

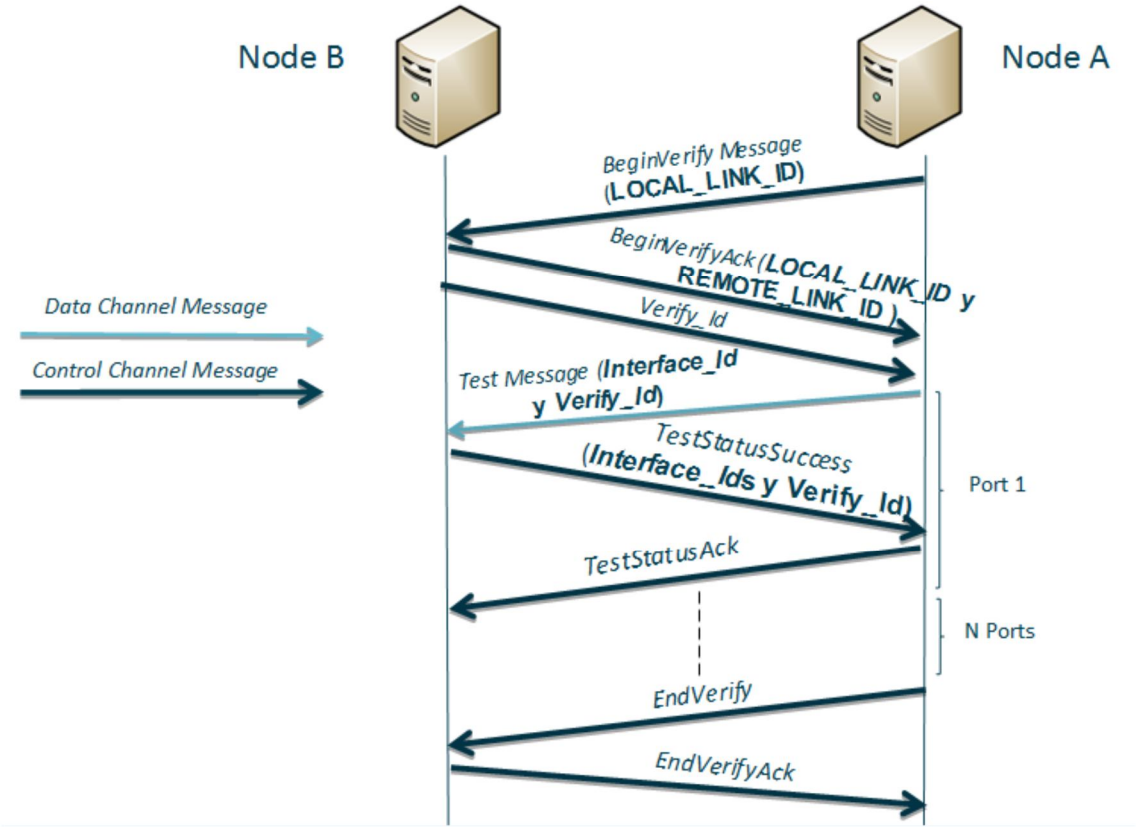


Figura 13 : intercambio de mensajes entre nodos para comprobar la conectividad de link.

La figura 13 hace ilustración del siguiente proceso para realizar el establecimiento y verificación del nuevo link:

1. El nodo A envía un mensaje *BeginVerify* al nodo B a través del canal de control. En este mensaje se incluye el identificador local (dirección IP o interfaz) que A asigna al *Link.*

2. Cuando B recibe el mensaje crea un objeto *Verify_Id* y lo asocia al TE_Link de A. Esta asignación nos sirve luego cuando B recibe los Test Messages de A, los cuales incluyen el objeto anteriormente mencionado. De esta manera B descubre también el identificador que A ha asignado al TE_Link. Posteriormente B contesta con un *BeginVerifyAck* que lleva el identificador que B asigna al TE_Link. También se incluye un objeto REMOTE_LINK_ID con la asociación de Link_Ids asignada por ambos. El objeto *Verify_Id*

también es incluido en este mensaje, el cual se envía a través del canal de control.

3. Cuando A recibe el mensaje previamente enviado, empieza a enviar *Test messages* periódicos que incluyen el objeto *Interface_Id* para el puerto usado y el objeto *Verify_Id* que fue creado por B.

4. Cuando B recibe el *Test message* mapea el *Interface_Id* enviado (*Interface_Id* = 1) con el suyo propio (*Interface_Id* = 10) y envía de vuelta un mensaje *TestStatusSuccess*, el cuál incluye ambas *Interface_Ids* para los puertos utilizados junto con el objeto *Verify_Id.* Con este objeto el nodo A puede determinar los identificadores del TE_Link a los que pertenece el data link.

5. El nodo A devolverá un mensaje *TestStatusAck* por el canal de control indicando que ha recibido el *TestStatusSuccess.*

.

6. Este proceso se repite hasta que todos los puertos de los data Links han sido comprobados.

7. Una vez comprobados el nodo A envía un mensaje *EndVerify* por el canal de control indicando que la comprobación ha terminado.

8. nodo B responderá con un mensaje *EndVerifyAck*.

2.4.1 - El protocolo LMP como solución a los errores de administración del enlace

El error de administración o de manejo, es un requerimiento importante desde el punto de vista operacional. El error de administración incluye normalmente: detección del error, localización del error y notificación del error. Cuando un error

ocurre y es detectado (detección de error), un operador necesita conocer exactamente donde ocurrió (localización de error) y se debe notificar al nodo origen para tomar algunas medidas (notificación del error).

Hay que tener en cuenta que, aprovechando la localización de un error, se pueden utilizar también una serie de mecanismos específicos de restauración de la red.

En las nuevas tecnologías tales como la conmutación fotónica transparente, ningún método es definido para localizar un error y, por lo tanto, la información de error que es propagada debe ser enviada “fuera de banda” (a través del plano de control).

El LMP (*link management protocol*) proporciona un procedimiento de localización de errores que puede ser usado para localizar rápidamente errores en el enlace, notificando un error al nodo siguiente (*upstream*) (a través de un procedimiento de notificación de error). Un nodo vecino que detecta errores en el enlace de datos, enviará un mensaje LMP (*link management protocol*) a su vecino notificándole el error. Cuando un nodo recibe un fallo de notificación, puede detectar el fallo con los correspondientes puertos entrantes para determinar si el fallo está entre los dos nodos y, una vez el fallo ha sido localizado, pueden ser usados los protocolos de señalización para iniciar los procedimientos de restauración de enlace o de ruta.

Protocolo		Descripción
Encaminamiento	OSPF-TE, IS-IS TE	Las características principales son: 1. tipo de acoplamiento-protección 2. acoplamientos en ejecución derivados (adyacencia de la expedición) para la escalabilidad (scalability) mejorada

		3. Aceptar y anunciar acoplamientos sin la identificación del acoplamiento del IP 4. Identificación entrante y saliente de interfaz 5. Descubrimiento de la ruta para el apoyo que es diferente de la ruta primaria (grupo de acoplamiento de riesgo)
Señalización	RSVP-TE	Protocolos de señalización para el establecimiento de LSPs (labelswitchedpath) y el tráfico dirigido. Los pasos de funcionamiento principales son como sigue: 1. Intercambio de etiqueta para incluir las redes non-packet (etiquetas generalizadas). 2. Establecimiento de LSPs (labelswitchedpath) bidireccionales. 3. Señalización para el establecimiento de una ruta de reserva (información de la protección). 4. Apresurar la asignación de la etiqueta vía etiqueta sugerida. 5. La conmutación de una banda de longitudes de onda fija las longitudes de onda siguientes a conmutar.
Gestión del acoplamiento	LMP (link management protocol)	1. Gestión del Canal de Control: Establecer los

		parámetros de acoplamiento (p.ej., frecuencia en enviar mensajes) y asegurar la seguridad de un acoplamiento (protocolo Hello). 2. Verificación del Acoplamiento-Conectividad: Asegura la conectividad física del acoplamiento entre los nodos vecinos. 3. Correlación de la Característica de Acoplamiento: Identificación de las características del acoplamiento de los nodos adyacentes (por ej., mecanismo de protección). 4. Aislamiento de fallos: Aísla averías solas o múltiples en el dominio óptico.

Tabla 2. Protocolos de MPLS

Capítulo 3. Presentar la Configuración de una red MPLS.

En este capítulo 3 se va a explicar cómo configurar una pequeña red MPLS, los distintos routers y aplicaciones para poder realizar las distintas pruebas.

Materiales necesarios

Para la realización de esta práctica es necesario disponer de:

- cables Ethernet normales.
- cuatro routers Cisco Systems de la serie 2600 equipados mínimo con 16 MB de Flash y 48 MB de RAM, con una interfaz serie y otra Ethernet, con la IOS Versión 12.3 (26) Telco Feature Set- General Deployment1. (ver anexos).
- Un hub.
- Ordenadores, uno de ellos equipado con un analizador de protocolos.

3.1 - Escenario básico:

El escenario (figura 14) está compuesto por tres routers que configuran dos tramos MPLS, un Hub entre cada uno de los routers y un host de origen y destino en los extremos de la red. También se ha incluido un "marcador" entre el host de origen y el primer router MPLS de la red para poder diferenciar distintos tipos de tráfico. Finalmente se ha conectado un Analizador a los Hubs para poder observar los paquetes cuando viajan dentro de la red.

La siguiente figura ilustra el escenario implementado.

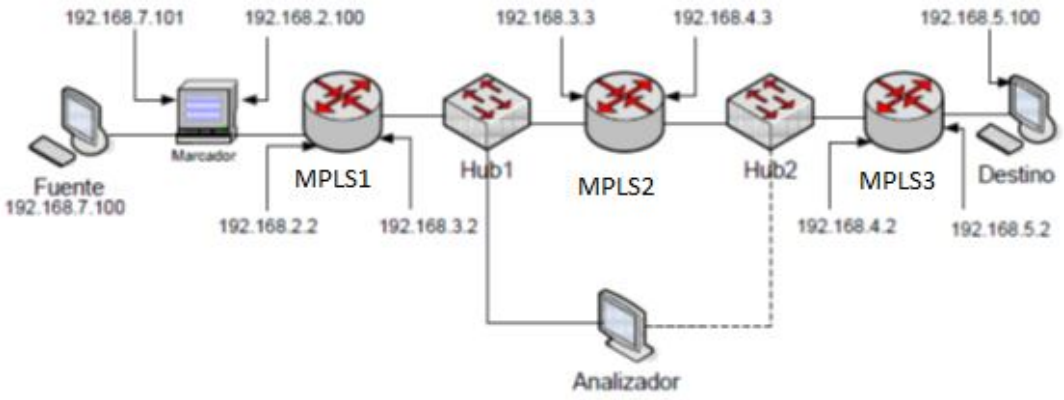


Figura 14 : Escenario básico.

La razón por la que se ha elegido este escenario es porque es el mínimo para poder observar correctamente la conectividad extremo-extremo de la red MPLS.
El penúltimo router de la red el que quita la etiqueta MPLS (**Penultimate Hop Popping**). Si solo tuviéramos 2 routers MPLS en la red, el router de entrada sería a su vez el penúltimo de salida. Al ser este el que añadiría (push) y quitaría (pop) la etiqueta, no podríamos observar su comportamiento. Por lo tanto el número mínimo de routers necesarios es el de 3.

También se han escogido Hubs, en lugar de Switches, para que actúen de repetidores y envíen una copia de cada paquete al Analizador. Para ganar esta funcionalidad, tenemos que sacrificar un poco la eficiencia de la red, ya que con un Hub se producen más colisiones de paquetes (más pérdidas) que con un Switch.

Finalmente, se ha incluido el “marcador”, como ya hemos dicho, para diferenciar distintos tipos de tráfico. El ordenador “marcador” dispone del software Xmarker, que nos permite modificar el campo DSCP de los paquetes IP siguiendo un conjunto de reglas que definiremos.

3.2. Configuración del escenario:

Nuestro objetivo es establecer un enlace MPLS que esté capacitado para ofrecer Traffic Engineering, por eso vamos a orientar la configuración para que soporte la implementación de DiffServ. Todas las configuraciones presentadas se aplican sobre routers cisco de la serie 2600(para características ver anexos).
Para trabajar con una red MPLS con Traffic Engineering debemos comprobar que la red tiene habilitada una serie de protocolos:

- La red tiene que tener habilitado el protocolo CEF (Cisco Express Forwarding)
- Un protocolo de routing, en nuestro caso OSPF
- Una interfaz de Loopback para poder ser usada como router ID (RID).

3.2.1. Reseteo de la configuración de los routers:

El primer paso que realizamos fue el de resetear los routers para eliminar cualquier configuración de usos anteriores. Además, los tres routers usados disponían de contraseñas tanto para conectarse a ellos como para editar sus configuraciones, y estas contraseñas eran desconocidas para nosotros. Para ellos realizamos los siguientes pasos:

Primero reiniciamos el router manualmente.

Antes de que pasen 60 segundos pulsamos **Ctrl+Break** para parar la carga de la configuración.

*RouterMPLS # **confreg 0x2142***
*RouterMPLS # **reset***

Al volver a reiniciar el router nos pregunta si queremos realizar una configuración básica siguiendo un plantilla. Le decimos que no.

3.2.2 Configuración básica del router:

Para empezar la configuración le asignaremos un nombre al router, así como contraseñas para la consola y para editar la configuración.

Router > ***enable***

Router # ***configure terminal***

Router (config) # ***hostname MPLS1*** //Introducimos el nombre de MPLS1 para el router

MPLS1 (config) # ***line con 0***

MPLS1 (config - con) # ***password***

MPLS1 (config - con) # ***<contraseña de la consola>*** //Definimos el password de la consola

MPLS1 (config - con) # ***login***

MPLS1 (config - con) # ***exit***

MPLS1 (config) # ***enable secret <contraseña enable>*** //Habilitamos el password del enable

Finalmente guardamos todos los cambios en la memoria.

MPLS1 (config) # ***config-register 0x2102***

Pulsamos **Ctrl+z** para salir del modo configuración

MPLS1 # ***write memory*** // Guardamos los cambios

3.2.3. Configuración básica para IP y MPLS.

Ahora que ya tenemos configurado el router de forma básica, procederemos a configurar sus interfaces y a habilitar MPLS. Para empezar ejecutaremos unos comandos para habilitar el enrutamiento MPLS en el router de manera global.

MPLS1 # ***config terminal***

MPLS1 (config) # ***ip cef*** //Habilitamos el protocolo CEF en el router

MPLS1 (config) # ***mpls label protocol ldp*** //Definimos el protocolo LDP como protocolo para la distribución de las etiquetas

MPLS1 (config) # ***mpls ip*** //Habilitamos MPLS a nivel global

Una vez configurado el protocolo que usará el router para realizar la conmutación de etiquetas (CEF) y su distribución (LDP), procedemos a realizar la configuración de OSPF para poder hacer el routing interno.

MPLS1 (config) # ***router ospf 1*** // Configuramos el enrutamiento interno con OSPF con el identificador 1

MPLS1 (config-router) # ***mpls traffic-eng router-id loopback0*** // Usaremos la interfaz de Loopback como identificador del router para Traffic Engineering

MPLS1 (config-router) # ***mpls traffic-eng area 0*** // Configuramos el área 0 como la área en la que habilitamos el traffic engineering

MPLS1 (config-router) # ***network 192.168.1.1 0.0.0.0 area 0*** // Habilitamos el interfaz de Loopback para usar OSPF y lo asignamos al área 0

MPLS1 (config-router) # ***network 192.168.3.0 0.0.0.255 area 0*** // Habilitamos la subred 192.168.3.0/24 para usar OSPF y lo asignamos al área 0
MPLS1 (config-router) # ***exit***

La configuración de los otros dos routers es prácticamente la misma. Simplemente tenemos que realizar los siguientes cambios:

MPLS2

Sustituimos *network 192.168.1.1 0.0.0.0 área 0* por *192.168.1.2 0.0.0.0 área 0* ya que su interfaz de Loopback es la 192.168.1.2 y no la 192.168.1.1

Añadimos el comando network *192.168.4.0 0.0.0.255 área 0* ya que el router MPLS2 tiene dos interfaces vecinas que realizan MPLS.

MPLS3

Sustituimos network *192.168.1.1 0.0.0.0 área 0* por *192.168.1.3 0.0.0.0 área 0* ya que su interfaz de Loopback es la 192.168.1.3 y no la 192.168.1.1

También tenemos que sustituir el comando *network 192.168.3.0 0.0.0.255 área 0* por el *network 192.168.4.0 0.0.0.255 área 0* ya que la red 192.168.4.0 es la adyacente a este router y no la 192.168.3.0

Finalmente solo nos queda configurar las interfaces de los routers.

MPLS1 (config) # ***interface loopback0*** // Accedemos al interfaz de Loopback
MPLS1 (config-if) # ***ip address 192.168.1.1 255.255.255.255*** //Le asignamos una IP y mascara de subred
MPLS1 (config-if) # ***exit***
MPLS1 (config) # ***interface f0/0*** // Accedemos al interfaz f0/0
MPLS1 (config-if) # ***ip address 192.168.2.2 255.255.255.0*** //Le asignamos una IP y mascara de subred
MPLS1 (config-if) # ***no shutdown*** // Habilitamos el interfaz
MPLS1 (config-if) # ***exit***

MPLS1 (config) # ***interface f0/1*** // Accedemos al interfaz f0/1
MPLS1 (config-if) # ***mpls ip*** //Habilitamos MPLS en el interfaz
MPLS1 (config-if) # ***ip address 192.168.3.2 255.255.255.0*** //Le asignamos una IP y mascara de subred
MPLS1 (config-if) # ***no shutdown*** // Habilitamos el interfaz
MPLS1 (config-if) # ***exit***
MPLS1 (config) # ***ip route 192.168.5.0 255.255.255.0 192.168.3.0***
MPLS1 (config-if) # ***ip route 192.168.7.0 255.255.255.0 192.168.2.0***

En este último comando hemos añadido la ruta estática para que el router sepa por donde enviar los paquetes con destino a la subred 192.168.5.0/24 y a la 192.168.7.0/24. También podemos ver como se ha habilitado el protocolo MPLS en la subred 192.168.3.0/24 ya que es la única que es adyacente a la red MPLS.

La configuración de los otros dos routers son parecidas.

MPLS2 (config) # ***interface loopback0***
MPLS2 (config-if) # ***ip address 192.168.1.2 255.255.255.255***
MPLS2 (config-if) # ***exit***

MPLS2 (config) # ***interface GigabitEthernet0/0***
MPLS2 (config-if) # ***mpls ip***
MPLS2 (config-if) # ***ip address 192.168.3.3 255.255.255.0***
MPLS2 (config-if) # ***no shutdown***

MPLS2 (config-if) # ***exit***
MPLS2 (config) # ***interface GigabitEthernet0/1***
MPLS2 (config-if) # ***mpls ip***
MPLS2 (config-if) # ***ip address 192.168.4.3 255.255.255.0***
MPLS2 (config-if) # ***no shutdown***
MPLS2 (config-if) # ***exit***

MPLS2 (config) # ***ip route 192.168.5.0 255.255.255.0 192.168.4.0***
MPLS2 (config) # ***ip route 192.168.2.0 255.255.255.0 192.168.3.0***
MPLS2 (config) # ***ip route 192.168.7.0 255.255.255.0 192.168.3.0***

MPLS3 (config) # ***interface loopback0***
MPLS3 (config-if) # ***ip address 192.168.1.3 255.255.255.255***

MPLS3 (config-if) # ***exit***

MPLS3 (config) # ***interface f0/0***
MPLS3 (config-if) # ***mpls ip***
MPLS3 (config-if) # ***ip address 192.168.4.2 255.255.255.0***
MPLS3 (config-if) # ***no shutdown***
MPLS3 (config-if) # ***exit***

MPLS3 (config) # ***interface f0/1***
MPLS3 (config-if) # ***ip address 192.168.5.2 255.255.255.0***
MPLS3 (config-if) # ***no shutdown***
MPLS3 (config-if) # ***exit***

MPLS3 (config) # ***ip route 192.168.2.0 255.255.255.0 192.168.3.0***
MPLS3 (config) # ***ip route 192.168.7.0 255.255.255.0 192.168.3.0***

Una vez tenemos los tres routers configurados, vamos a ver cómo han quedado sus configuraciones usando los siguientes comandos.

MPLS1# ***show ip route*** // Nos muestra la tabla de rutas IP.

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.4.0/24 [110/11] via 192.168.3.3, 00:02:19, FastEthernet0/1
S 192.168.5.0/24 [1/0] via 192.168.3.3
S 192.168.7.0/24 [1/0] via 192.168.2.101
192.168.0.0/32 is subnetted, 3 subnets
C 192.168.0.1 is directly connected, Loopback0
O 192.168.0.2 [110/11] via 192.168.3.3, 00:02:19, FastEthernet0/1
O 192.168.0.3 [110/12] via 192.168.3.3, 00:02:19, FastEthernet0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/1

Las rutas marcadas con una C son las que están conectadas directamente al router, las marcadas con una S son las rutas estáticas que hemos definido, y finalmente, las rutas marcadas con una O son las rutas que se han obtenido del protocolo OSPF.

Para ver el comportamiento del protocolo MPLS que hemos configurado, ejecutamos:

MPLS1# ***show mpls forwarding-table***

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing Interface	Next Hop
16	17	192.168.5.0/24	0	Fa0/1	192.168.3.3
17	Untagged	192.168.7.0/24	296	Fa0/0	192.168.2.101
18	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.3
19	Pop tag	192.168.0.2/32	0	Fa0/1	192.168.3.3
20	20	192.168.0.3/32	0	Fa0/1	192.168.3.3

Tabla 3: LIB de MPLS1 en el escenario básico.

Observamos como los paquetes con destino a la subred 192.168.5.0/24 cambiaran su etiqueta del 16 al 17 al pasar por este router. Por otro lado, los paquetes con destino la subred 192.168.7.0/24 no serán etiquetados ya que esa red está fuera de la red MPLS.

Análogamente, si ejecutamos estos comandos en los otros dos routers, obtendremos su configuración.

MPLS2# ***show ip route***

Gateway of last resort is not set

C 192.168.4.0/24 is directly connected, GigabitEthernet0/1
S 192.168.5.0/24 [1/0] via 192.168.4.2
S 192.168.7.0/24 [1/0] via 192.168.3.2
192.168.0.0/32 is subnetted, 3 subnets
O 192.168.0.1 [110/11] via 192.168.3.2, 00:07:08, GigabitEthernet0/0
C 192.168.0.2 is directly connected, Loopback0
O 192.168.0.3 [110/2] via 192.168.4.2, 00:07:08, GigabitEthernet0/1
S 192.168.2.0/24 [1/0] via 192.168.3.2
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0

MPLS2# ***show mpls forwarding-table***

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	17	192.168.7.0/24	1227842	Gi0/0	192.168.3.2
17	Pop tag	192.168.5.0/24	56196236	Gi0/1	192.168.4.2
18	Pop tag	192.168.2.0/24	0	Gi0/0	192.168.3.2
19	Pop tag	192.168.0.1/32	0	Gi0/0	192.168.3.2
20	Pop tag	192.168.0.3/32	0	Gi0/1	192.168.4.2

Tabla 4: LIB de MPLS2 en el escenario básico.

Cabe destacar que como es el penúltimo router el que elimina la etiqueta, será el router central el que haga esta acción en nuestro escenario, tal como muestra la tabla anterior.

MPLS3# ***show ip route***

C 192.168.4.0/24 is directly connected, FastEthernet0/0

C 192.168.5.0/24 is directly connected, FastEthernet0/1

S 192.168.7.0/24 [1/0] via 192.168.4.3

192.168.0.0/32 is subnetted, 3 subnets

O 192.168.0.1 [110/12] via 192.168.4.3, 00:08:51, FastEthernet0/0

O 192.168.0.2 [110/2] via 192.168.4.3, 00:08:51, FastEthernet0/0

C 192.168.0.3 is directly connected, Loopback0

S 192.168.2.0/24 [1/0] via 192.168.4.3

O 192.168.3.0/24 [110/11] via 192.168.4.3, 00:08:51, FastEthernet0/0

MPLS3# ***show mpls forwarding-table***

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	192.168.7.0/24	0	Fa0/0	192.168.4.3
17	18	192.168.2.0/24	0	Fa0/0	192.168.4.3
18	Pop tag	192.168.3.0/24	0	Fa0/0	192.168.4.3
19	19	192.168.0.1/32	0	Fa0/0	192.168.4.3
20	Pop tag	192.168.0.2/32	0	Fa0/0	192.168.4.3

Tabla 5: LIB de MPLS3 en el escenario básico.

3.2.4. Configuración del “marcador”

Al realizar el envío del vídeo también marcaremos los paquetes en su campo DSCP. Esto nos permitirá diferenciar distintos flujos de tráfico en el futuro.

Primero de todo, y como el ordenador usa una distribución del Sistema Operativa Linux, vamos a habilitar la opción de enrutar los paquetes que lleguen a sus interfaces. Para ello ejecutamos el siguiente comando:

root@marcador: *home/Poveda#* ***echo 1 > /proc/sys/net/ipv4/ip_forward***

Ahora que el ordenador ya se comporta como un router, configuramos sus interfaces utilizando el asistente que nos ofrece el Sistema Operativo.

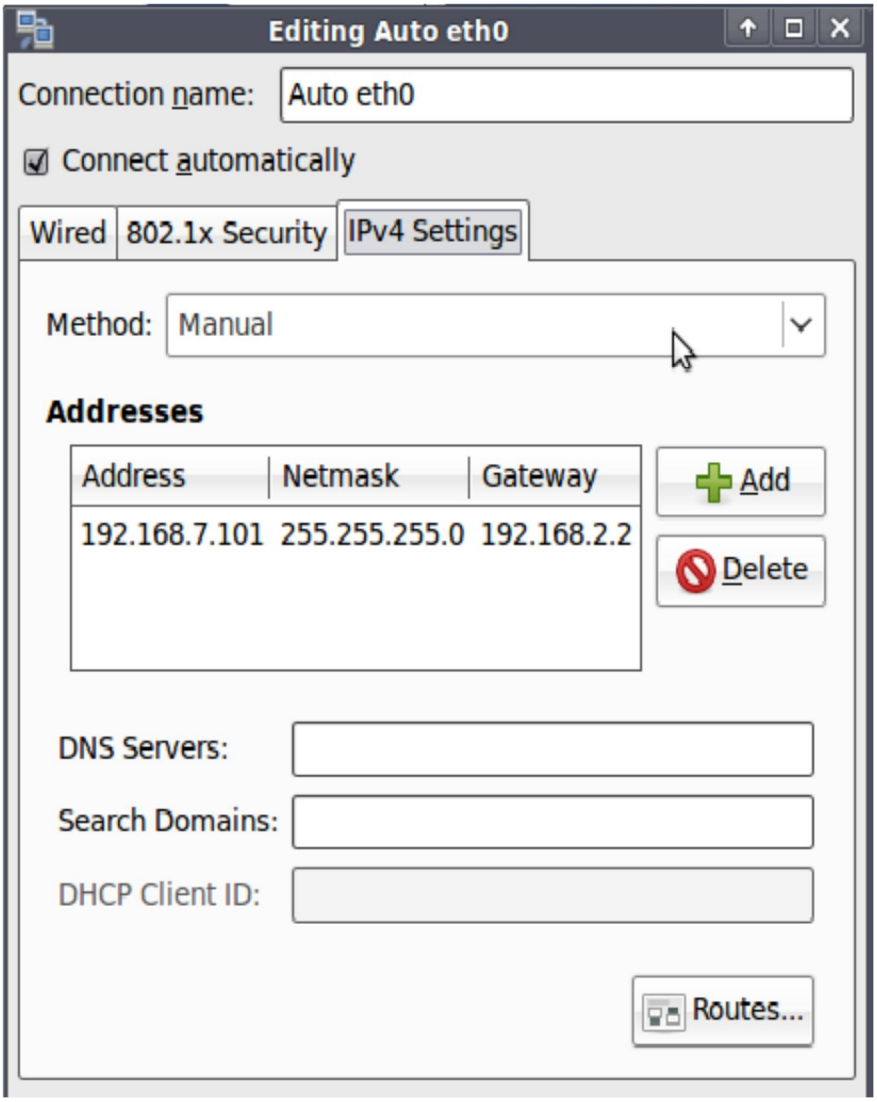


Figura 15 : configuración de la interfaz.

De igual forma configuramos el interface eth1, con la dirección 192.168.2.100.

Como último paso, en el ordenador “marcador” disponemos del software Xmarker (figura 16), el cual nos permite asignar “reglas” a los distintos interfaces de la máquina. En nuestro caso crearemos una regla que nos marque el campo DSCP de los paquetes que entren por el interfaz eth0 (red 192.168.7.0/24) con destino al Host “Destino” (192.168.5.100), con el valor CS4 (0x20).

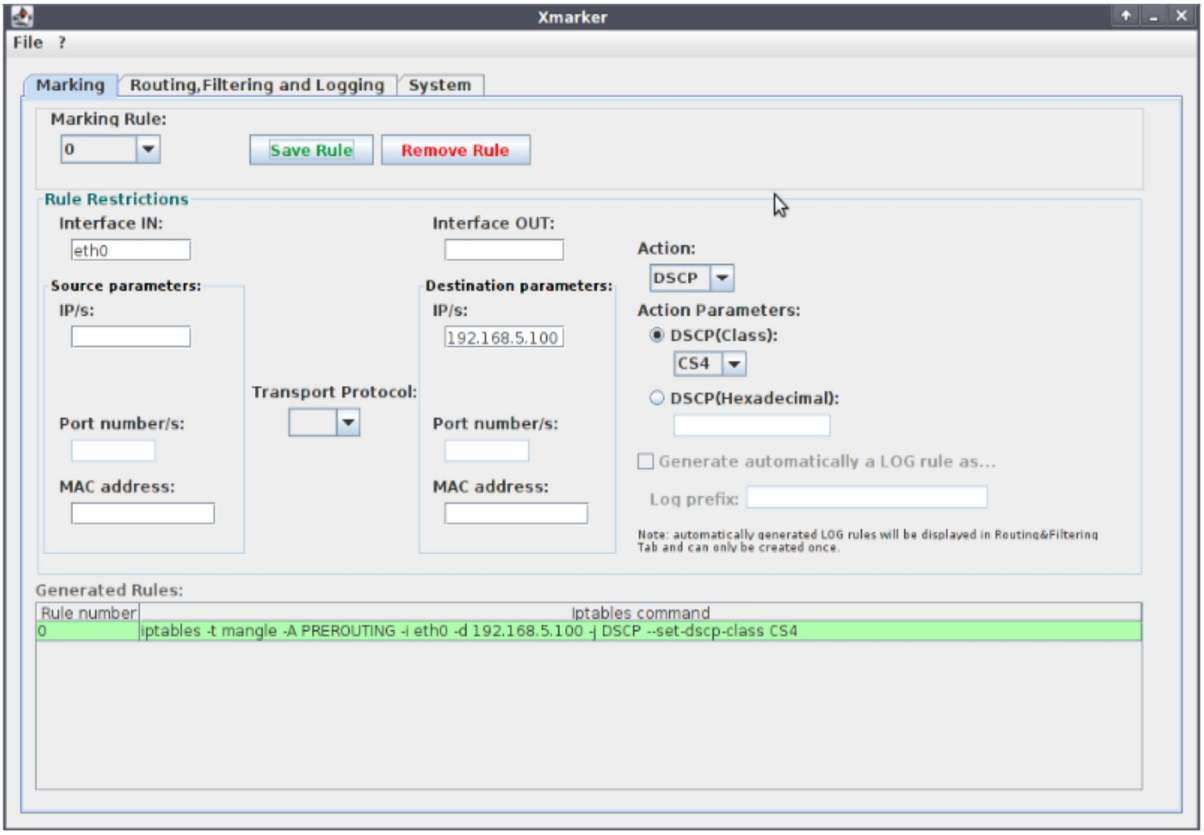


Figura 16 : configuración de reglas en el marcador.

3.3 Pruebas de conexión extremo-extremo

Una vez tenemos configurado todo el escenario, debemos comprobar que funciona la conexión extremo-extremo en ambos sentidos.

Se entiende como conexión extremo-extremo aquella que va desde el Host "Fuente" al Host "Destino" pasando a través de los 3 routers MPLS y del "marcador".
Para ello enviaremos una serie de paquetes ICMP (Internet Control Message Protocol), o sea, pings a través de la red.

Nos conectamos al Host "Fuente" (192.168.7.100) y enviamos 4 paquetes al Host "Destino" (192.168.5.100)

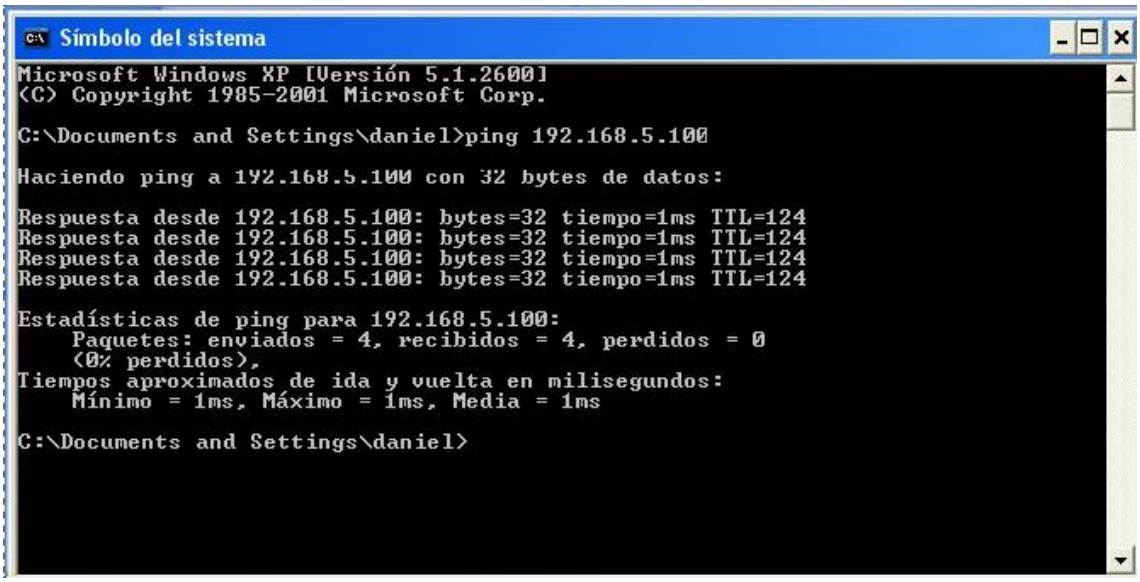


Figura 17 : Ping desde la fuente hacia el destino.

Podemos observar cómo se han recibido los 4 paquetes y ninguno se ha perdido, por lo tanto podemos confirmar que hay conectividad extremo-extremo.

Finalmente vamos a realizar la misma prueba pero en sentido contrario, del Host "Destino" al Host "Fuente"

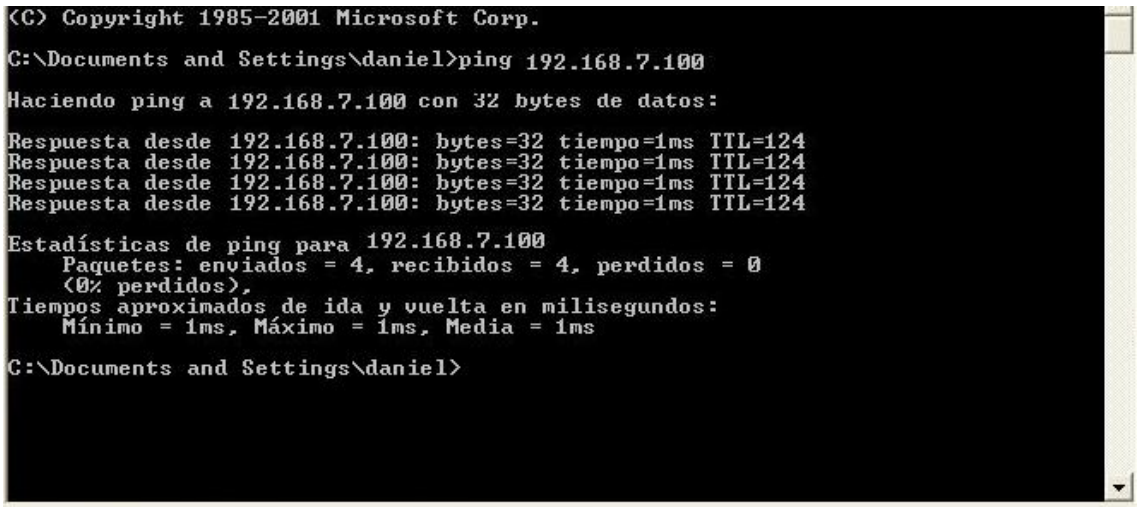


Figura 18 : ping desde el destino hacia la fuente.

Igual que en el caso anterior la prueba de conexión ha sido un éxito.

3.4. Pruebas de envío de vídeo extremo-extremo

3.4.1. Configuración del VLC

Ahora que ya tenemos la red configurada y con conexión, vamos a enviar un archivo de vídeo por streaming con el programa VLC.

En el Host “Fuente” seleccionamos el vídeo a transmitir, protocolo (HTTP), por qué interfaz y puerto enviarlo (192.168.7.100:8080) y que no haga Transcoding(figura 19).

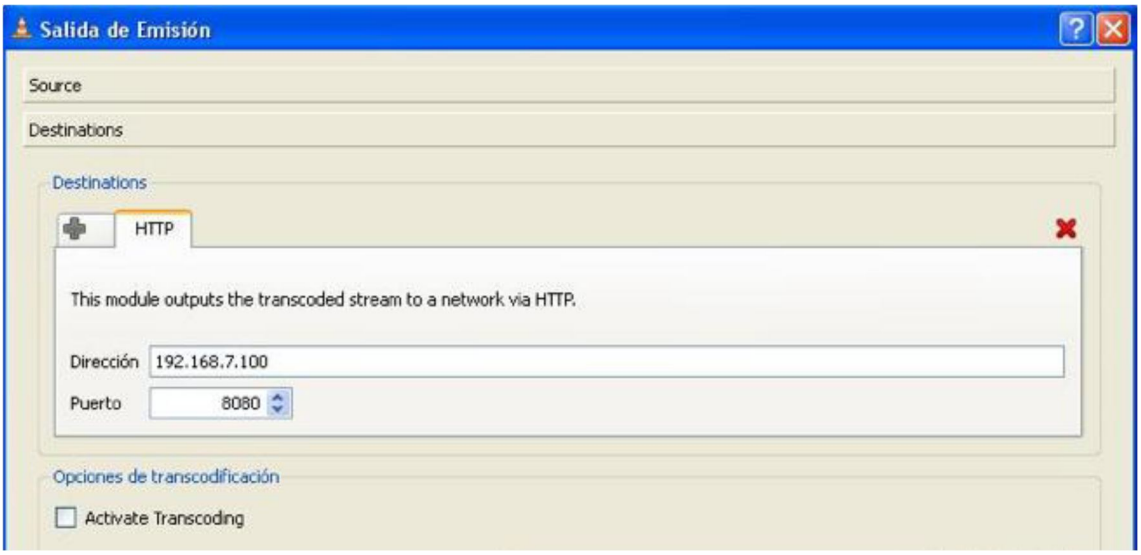


Figura 19 : configuración del VLC en l a fuente.

En el Host “Destino” simplemente seleccionamos el protocolo y origen de los datos, los cuales deben ser igual a los de la fuente (figura 20).

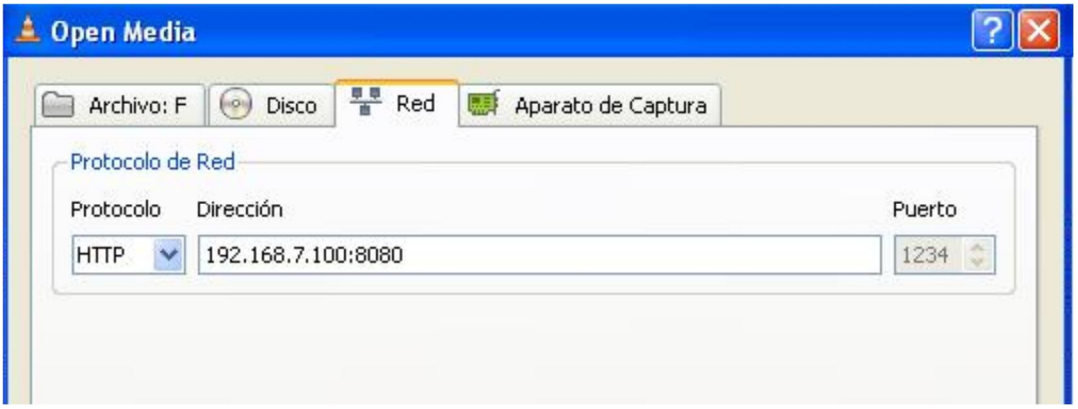


Figura 20 : configuración del VLC en el destino.

3.4.2. Resultados

Con esta configuración el vídeo se recibe correctamente en el Host “Destino” aunque con un pequeño retraso con respecto al vídeo original, inferior al segundo. Este hecho es lógico ya que los datos tienen que ser reenrutados por 2 routers y por el marcador y representarse de nuevo en el Host “Destino”.

Para poder observar los paquetes usaremos el Analizador conectado al Hub 1, ya que si los mirásemos en el Host “Destino” no podríamos ver los paquetes MPLS ya que estaríamos fuera de la red MPLS, pues el penúltimo router (MPLSCore) hace un Pop de las etiquetas.

Con el Analizador podemos ver el siguiente paquete:

```
No.     Time        Source                Destination           Protocol Info
    537 4.462910    192.168.7.100         192.168.5.100         HTTP     Continuation or non-HTTP t

Frame 537 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: Cisco_f7:d3:e1 (00:d0:bb:f7:d3:e1), Dst: Cisco_a4:9a:78 (00:13:80:a4:9a:78)
MultiProtocol Label Switching Header, Label: 17, Exp: 4, S: 1, TTL: 126
    MPLS Label: 17
    MPLS Experimental Bits: 4
    MPLS Bottom Of Label Stack: 1
    MPLS TTL: 126
Internet Protocol, Src: 192.168.7.100 (192.168.7.100), Dst: 192.168.5.100 (192.168.5.100)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x80 (DSCP 0x20: Class Selector 4; ECN: 0x00)
    Total Length: 1496
    Identification: 0x1ed5 (7893)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 126
    Protocol: TCP (0x06)
    Header checksum: 0x49b2 [correct]
    Source: 192.168.7.100 (192.168.7.100)
    Destination: 192.168.5.100 (192.168.5.100)
Transmission Control Protocol, Src Port: http-alt (8080), Dst Port: bnetgame (1119), Seq: 516637, A
Hypertext Transfer Protocol
```

Figura 21 : detalle de un paquete MPLS.

En la imagen 21 se puede observar que es un paquete MPLS con la etiqueta 17 y que es la única etiqueta del paquete, que su origen es el HOST “Fuente” y su destino el Host “Destino”. Que el paquete tenga la etiqueta 17 concuerda con la configuración que habíamos obtenido al ejecutar el comando show mpls forwarding-table en el router MPLS1. También se puede ver muy claramente en la cabecera IP como el campo DSCP está marcado con el valor 0x20 que se corresponde con el Class Selector 4, tal y como lo habíamos configurado.

3.5 Configuración del camino Backup

Una vez tenemos nuestra red funcionando, vamos a añadirle un nodo de Backup para dotar de redundancia al router MPLS2. El nuevo escenario es el siguiente:

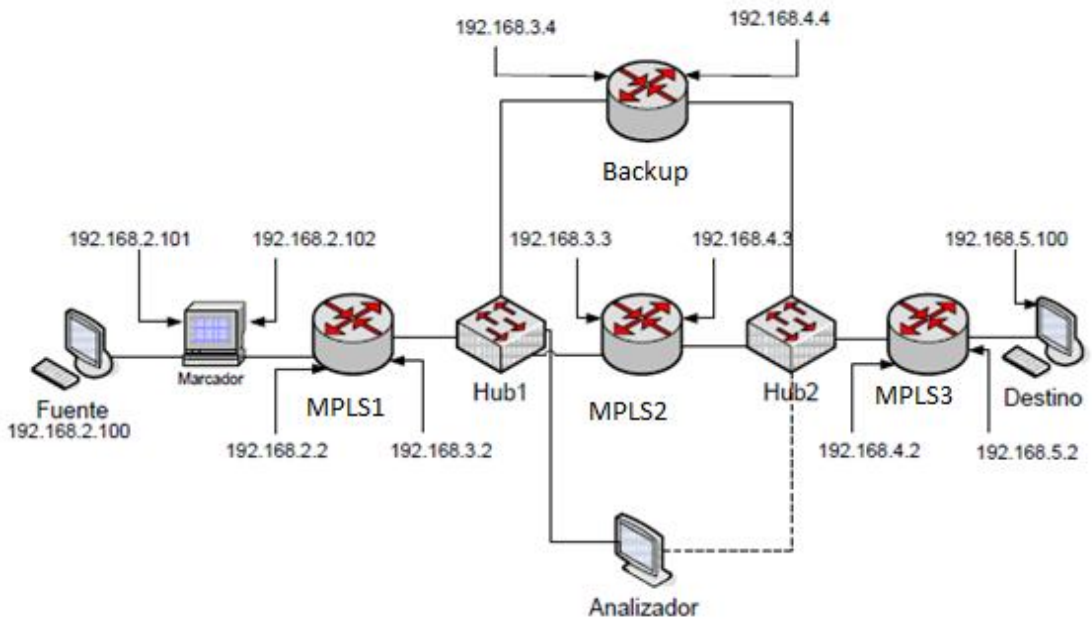


Figura 22 : escenario con backup.

Como se puede observar (figura 22) se ha añadido el router Backup entre los dos extremos, de modo que está en paralelo con el MPLS2. También se han modificado las IP de la Fuente y del Marcador para que este último actúe de una forma más "transparente" en la red.

El objetivo del router de Backup es que solo funcione cuando el router central (MPLS2) no pueda hacerlo, ya sea por un problema en el propio router o en alguno de sus enlaces.

Como hemos visto anteriormente, la forma más sencilla de hacerlo sería aplicando el mecanismo de Fast Rerouteing (FRR), pero los modelos de los 3 primeros routers no los soportan. Para solucionarlo usaremos el protocolo OSPF, modificando el coste de los enlaces para que los routers solo vean el camino con menos coste.

El primer paso a realizar es configurar el router de Backup de la misma forma como hemos hecho con el MPLS2, pero modificando las IP de las interfaces. Así pues la única diferencia será:

Sustituir el comando *ip address 192.168.1.2 255.255.255.255* de la interfaz de loopback por el *ip address 192.168.1.4 255.255.255.255* y los comandos *ip address 192.168.3.3 255.255.255.0* y *ip address 192.168.4.3 255.255.255.0* de sus otros interfaces por los *ip address 192.168.3.4 255.255.255.0* y *ip address 192.168.3.4 255.255.255.0* respectivamente.

Como ahora vamos a utilizar el protocolo OSPF para la realización del Backup, este protocolo será el encargado de construir toda la tabla de rutas, y por lo tanto no necesitaremos las rutas estáticas. En su lugar añadiremos las siguientes redes en las distintas configuraciones del OSPF de cada router:

MPLS1

MPLS1 (config-router) # ***network 192.168.2.0 0.0.0.255 área 0*** // Habilitamos la subred 192.168.2.0/24 para usar OSPF y lo asignamos al área 0

MPLS1 (config-if) # ***ip route 192.168.2.100 255.255.255.0 192.168.2.101*** // Solo tenemos que añadir esta ruta estática porque el marcador no usa el protocolo OSPF y no puede notificarlo al router MPLS1

MPLS3

MPLS3 (config-router) # ***network 192.168.5.0 0.0.0.255 área 0*** // Habilitamos la subred 192.168.5.0/24 para usar OSPF y lo asignamos al área 0

Con esta configuración la red ya es capaz de transmitir un paquete desde el Host "Origen" hasta el Host "Destino" por el camino con menos coste, que ahora mismo es idéntico, ya sea a través del router MPLS2 como por el Backup. Podemos ver cómo queda la tabla de rutas y de etiquetas MPLS en el router MPLS1:

MPLS1# ***show ip route***

O 192.168.4.0/24 [110/2] via 192.168.3.4, 00:00:03, FastEthernet0/1

[110/2] via 192.168.3.3, 00:00:03, FastEthernet0/1

O 192.168.5.0/24 [110/3] via 192.168.3.4, 00:00:03, FastEthernet0/1

[110/3] via 192.168.3.3, 00:00:03, FastEthernet0/1

192.168.0.0/32 is subnetted, 4 subnets

C 192.168.0.1 is directly connected, Loopback0

O 192.168.0.2 [110/2] via 192.168.3.3, 00:00:03, FastEthernet0/1

O 192.168.0.3 [110/3] via 192.168.3.4, 00:00:03, FastEthernet0/1

[110/3] via 192.168.3.3, 00:00:04, FastEthernet0/1

O 192.168.0.4 [110/2] via 192.168.3.4, 00:00:04, FastEthernet0/1

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

S 192.168.2.100/32 [1/0] via 192.168.2.101

C 192.168.2.0/24 is directly connected, FastEthernet0/0

C 192.168.3.0/24 is directly connected, FastEthernet0/1

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.4
	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.3
18	Pop tag	192.168.0.2/32	0	Fa0/1	192.168.3.3
19	16	192.168.0.3/32	0	Fa0/1	192.168.3.4
	18	192.168.0.3/32	0	Fa0/1	192.168.3.3
20	19	192.168.5.0/24	0	Fa0/1	192.168.3.4
	19	192.168.5.0/24	0	Fa0/1	192.168.3.3
21	Pop tag	192.168.0.4/32	0	Fa0/1	192.168.3.4
22	Untagged	192.168.2.100/32	0	Fa0/0	192.168.2.101

Tabla 6: LIB en MPLS1 con dos caminos.

En este caso todo el tránsito con destino a la red 192.168.5.0/24 iría con la etiqueta 20 a través del router Backup (192.168.3.4), porque es la primera que se

ha añadido a la red, y no podríamos decir que router priorizamos. Si hubiera un problema con el router Backup el tránsito se redirigiría automáticamente hacia el otro router (MPLS2 192.168.3.3), pero no volvería al router Backup cuando volviera a estar online porque su etiqueta se añadiría debajo de la del salto 192.168.3.3. Para solucionar este comportamiento, que no es el deseado, tenemos que modificar el coste de los interfaces.

Lo que haremos es aumentar el coste de los interfaces entre el router MPLS1 y Backup, y entre el Backup y el MPLS3. De este modo, el protocolo OSPF encontrará dos caminos del Host "Origen" al Host "Destino", pero uno de ellos con un coste superior al otro, y por tanto lo desestimará. Cuando el router MPLS2 falle, solo habrá un camino disponible (aunque tenga un coste alto) y todo el tráfico irá a través de él. En el momento en que se recupere el router MPLS2, volveremos a estar en la primera situación y por lo tanto desestimaremos el camino con más coste.

Para modificar el coste, simplemente tenemos que entrar en la configuración del interfaz e introducir el siguiente comando:

Backup *(config-if)* # ***ip ospf cost 10*** //Asignamos el coste del interfaz a 10
Backup *(config-if)* # ***ip ospf hello-interval 2*** //Modificamos el intervalo entre los mensajes "hello"
Backup *(config-if)* # ***ip ospf dead-interval 5*** //Modificamos el intervalo entre los mensajes "dead"

El intervalo de los mensajes "dead" es el tiempo que tarda el router para decidir que un router ya no está disponible, y por lo tanto eliminarlo de las tablas de enrutamiento. Por otro lado, el intervalo de mensajes "Hello" es el tiempo entre que el router envía mensajes a los otros routers para notificar que está activo. Estos dos tiempos tienen que ser los mismos en todos los interfaces de una misma subred, y por lo tanto se tendrán que modificar en los routers MPLS1 y MPLS3.

Con esta modificación, las rutas y etiquetas quedan del siguiente modo:

O 192.168.4.0/24 [110/2] via 192.168.3.3, 00:10:44, FastEthernet0/1
O 192.168.5.0/24 [110/3] via 192.168.3.3, 00:10:44, FastEthernet0/1
192.168.0.0/32 is subnetted, 4 subnets
C 192.168.0.1 is directly connected, Loopback0
O 192.168.0.2 [110/2] via 192.168.3.3, 00:10:44, FastEthernet0/1
O 192.168.0.3 [110/3] via 192.168.3.3, 00:10:44, FastEthernet0/1
O 192.168.0.4 [110/2] via 192.168.3.4, 00:10:44, FastEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
S 192.168.2.100/32 [1/0] via 192.168.2.101
C 192.168.2.0/24 is directly connected, FastEthernet0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/1

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.3
18	Pop tag	192.168.0.2/32	0	Fa0/1	192.168.3.3
19	18	192.168.0.3/32	0	Fa0/1	192.168.3.3
20	19	192.168.5.0/24	0	Fa0/1	192.168.3.3
21	Pop tag	192.168.0.4/32	0	Fa0/1	192.168.3.4
22	Untagged	192.168.2.100/32	0	Fa0/0	192.168.2.101

Tabla 7: LIB en MPLS1 con el Backup configurado.

Se puede observar como el protocolo OSPF ha eliminado las rutas perteneciente al router Backup (Solo queda la ruta de su interfaz de Looback, ya que es el único router que tiene acceso a esa interfaz).

Con esta configuración todo el tránsito irá a través del router MPLS2. Ahora, si desconectamos el interfaz 192.168.3.3 del router MPLS2, el protocolo OSPF encontrará el único camino disponible:

O 192.168.4.0/24 [110/11] via 192.168.3.4, 00:01:41, FastEthernet0/1
O 192.168.5.0/24 [110/12] via 192.168.3.4, 00:01:41, FastEthernet0/1
192.168.0.0/32 is subnetted, 4 subnets
C 192.168.0.1 is directly connected, Loopback0
O 192.168.0.2 [110/12] via 192.168.3.4, 00:01:41, FastEthernet0/1
O 192.168.0.3 [110/12] via 192.168.3.4, 00:01:41, FastEthernet0/1
O 192.168.0.4 [110/2] via 192.168.3.4, 00:01:41, FastEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
S 192.168.2.100/32 [1/0] via 192.168.2.101
C 192.168.2.0/24 is directly connected, FastEthernet0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/1

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.4
18	17	192.168.0.2/32	0	Fa0/1	192.168.3.4
19	16	192.168.0.3/32	0	Fa0/1	192.168.3.4
20	19	192.168.5.0/24	0	Fa0/1	192.168.3.4
21	Pop tag	192.168.0.4/32	0	Fa0/1	192.168.3.4
22	Untagged	192.168.2.100/32	0	Fa0/0	192.168.2.101

Tabla 8: LIB en MPLS1 con Backup active.

Si ahora el interfaz original se vuelve a recuperar, todo el tránsito vuelve a él:

O 192.168.4.0/24 [110/2] via 192.168.3.3, 00:10:44, FastEthernet0/1
O 192.168.5.0/24 [110/3] via 192.168.3.3, 00:10:44, FastEthernet0/1
192.168.0.0/32 is subnetted, 4 subnets

C 192.168.0.1 is directly connected, Loopback0

O 192.168.0.2 [110/2] via 192.168.3.3, 00:10:44, FastEthernet0/1

O 192.168.0.3 [110/3] via 192.168.3.3, 00:10:44, FastEthernet0/1

O 192.168.0.4 [110/2] via 192.168.3.4, 00:10:44, FastEthernet0/1

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

S 192.168.2.100/32 [1/0] via 192.168.2.101

C 192.168.2.0/24 is directly connected, FastEthernet0/0

C 192.168.3.0/24 is directly connected, FastEthernet0/1

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	192.168.4.0/24	0	Fa0/1	192.168.3.3
18	Pop tag	192.168.0.2/32	0	Fa0/1	192.168.3.3
19	18	192.168.0.3/32	0	Fa0/1	192.168.3.3
20	19	192.168.5.0/24	0	Fa0/1	192.168.3.3
21	Pop tag	192.168.0.4/32	0	Fa0/1	192.168.3.4
22	Untagged	192.168.2.100/32	0	Fa0/0	192.168.2.101

Tabla 9: LIB en MPLS1 con el enlace principal recuperado.

Como se ha podido observar, el tránsito siempre, y únicamente, viaja a través del router MPLS2 que hemos definido como el router “principal”. Sólo en el caso de que el tráfico a través de este camino sea imposible, se usará el router de backup .

3.6. Configuración de un punto de acceso Wifi

Con la red ya configurada y con un camino de Backup para darle redundancia, el siguiente paso a seguir es añadirle un punto de acceso Wifi (figura 23) al final de los routers. De esta manera, el escenario es el siguiente:

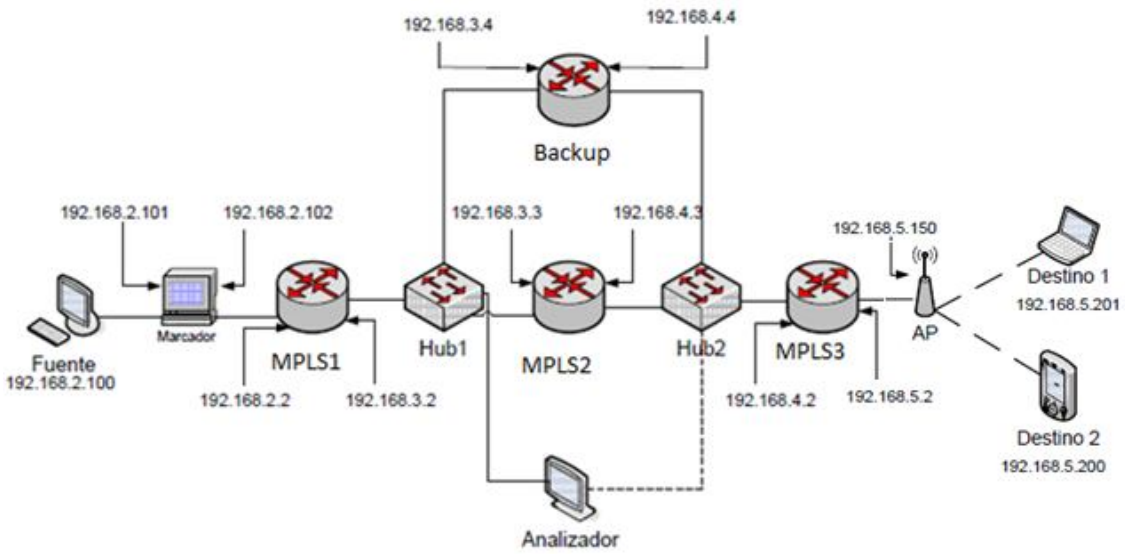


Figura 23 : escenario con backup y wifi.

Como lo que queremos es ver cómo se comporta el tráfico MPLS a través de un punto de acceso inalámbrico, vamos a configurar este de la manera más sencilla posible: Sin autenticación ni protocolo DCHP. Por lo tanto el cliente que se conecte al puto Wifi, tendrá que introducir manualmente su IP, máscara de subred y Gateway.

De la misma forma como hemos configurado los routers, vamos a realizar la configuración básica del punto de acceso.

AccessPoint > ***enable***

AccessPoint # ***configure terminal***

AccessPoint (config) # ***hostname ap*** //Introducimos el nombre de ap al Access Point

ap (config)# ***ip default-gateway 192.168.5.2*** //Como el Access Pont no es un router, necesitamos indicarle en que ip se encuentra el router.

ap (config)# ***interface FastEthernet0*** //Entramos en el modo conf-if del interfaz conectado al router

ap (config-if)# ***ip address 192.168.5.150 255.255.255.0***

ap (config-if)# ***exit***

ap (config)# ***interface Dot11Radio0*** // Entramos en el interfaz radio

ap (config-if)# ***ssid electronica*** //Le asignamos un nombre a la red inalámbrica

ap (config-if)# ***authentication open*** //Quitamos la seguridad de la red

ap (config-if)# ***exit***

Una vez tenemos configurado el punto de acceso, pasamos a configurar los terminales clientes. Para probar el correcto funcionamiento de la interfaz.

Dirección IP estática

Dirección IP: 192.168.5.200

Mascara de subred: 255.255.255.0

Router: 192.168.5.2

La dirección del Gateway (o router) debe ser la del router y no la IP del punto de acceso, ya que este solo interviene para realizar la conversión de medios de los paquetes, y no para enrutarlos.

3.7. QoS en redes MPLS

Conceptos básicos

El término de QoS apareció en 1987 para englobar las características del rendimiento de la red. Con la extensión de IP, el termino QoS pasó a ser usado para describir las técnicas encargadas de controlar la pérdida de paquetes, el retraso (delay) y el jitter. Con el aumento del ancho de banda que consumen las aplicaciones y su demanda de menor retardo y pérdida de paquetes, el QoS se ha convertido en un criterio muy importante a la hora de definir una red.
La pérdida de paquetes, como su nombre indica, se encarga de controlar el número de paquetes que alcanzan su destino correctamente.

El retraso, o delay, controla el tiempo que tardan los paquetes en llegar a su destino. Y finalmente el jitter, controla las fluctuaciones del tráfico, es decir, que los paquetes lleguen "uniformemente" a su destino.

Así pues, dependiendo del tipo de aplicación que queramos, serán necesarios unos criterios u otros de QoS. Una videoconferencia, por ejemplo, necesita un retraso y un jitter muy bajo, pero no es crítico si se pierden algunos paquetes. Por otro lado, el envío de un email requiere que no se pierdan paquetes, ya que algún error en estos podría provocar que se recibiera un mensaje totalmente distinto al original. El delay en este caso es muy poco importante.
A día de hoy, hay dos grandes arquitecturas para QoS:

- Integrated Services (**IntServ**): Se usa para redes pequeñas y medianas, pero no es escalable ya que usa mucha señalización entre los hosts de la red.

- Differenciated Services (**DiffServ**): Si que es escalable, ya que se basa en una clasificación previa de los paquetes, de forma que se reduce mucho la señalización.

Como MPLS está pensado para ser usado como una red troncal o “backbone”, nos centraremos por usar la arquitectura de DiffServ.

3.7.1 Servicios Diferenciados (DiffServ)

El modelo de arquitectura DiffServ está especificado en el RFC 2475, y permite distinguir diferentes clases de servicio marcando los paquetes.

El tráfico entra en la red, se clasifica y se asigna a un conjunto de comportamiento. Cada uno de estos conjuntos se identifica con un *codepoint* DS que se añade a la cabecera del paquete. Luego, estos paquetes son enviados por la red en función de lo que decida cada nodo en referencia a dicho *codepoint.*

En la cabecera de los paquetes MPLS, tenemos el campo EXP para controlar el QoS. Como hemos podido observar, la cabecera IP tiene 6 bits destinados al DSCP para clasificar los distintos paquetes, pero la cabecera MPLS solo dispone de 3 bits de EXP. Por lo tanto se tendrán que mapear las distintas 64 clases en las 8 que permite MPLS. Esto no es un gran problema, ya que 8 clases de servicio suelen ser más que suficiente.

Según los requisitos de cada usuario, DiffServ permite diferenciar distintos servicios como tráfico web, correo electrónico o transferencia de ficheros, donde el retardo no es muy importante, o servicios como video llamada y VoIP donde sí lo es.

DiffServ tiene un campo en los encabezados de los paquetes IP conocido como DiffServ Codepoint (DSCP). Los hosts o routers que envían el tráfico a una red DiffServ, marcan los paquetes IP con un valor DSCP, y los routers de la red, clasifican estos paquetes en función de dicho valor. Los tráficos con requisitos de QoS parecidos son marcados de igual forma.

Este proceso de envío de paquetes con el campo DSCP modificado desde los routers, se conoce como “Per Hop Behavior” PHB, o comportamiento por salto. Estos PHB nos indican las políticas aplicadas en los routers, la gestión del tráfico o los encolamientos.

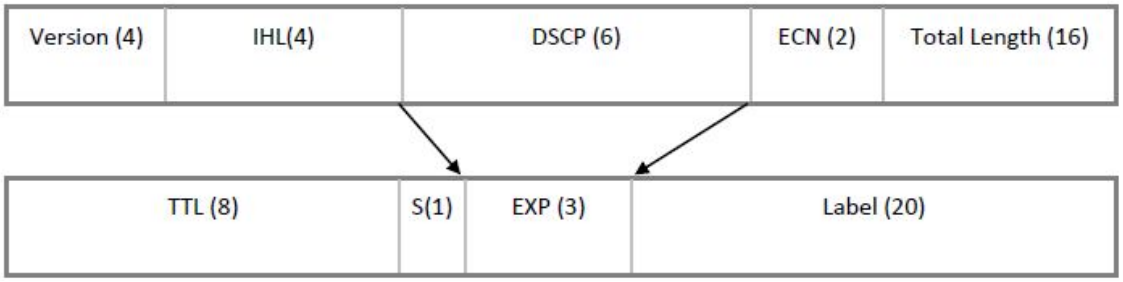


Figura 24 : detalle y relación de las cabeceras IP y MPLS.

3.8. Configuración de QoS

Como se ha explicado anteriormente en la configuración básica del escenario, los paquetes se marcan en el campo DSCP antes de entrar en la red MPLS con el ordenador "Marcador". Esto nos permitirá definir distintos comportamientos y calidades para el tráfico que pasa a través de la red.

Para asignar QoS en MPLS se tienen que seguir 3 pasos:

- Definir las clases de tráfico
- Definir las políticas de QoS
- Asignar a qué interfaces se aplican las políticas

3.8.1. Definir las clases de tráfico

Para definir las clases de tráfico se utiliza en comando **class-map** seguido de **match-any** o **mach-all**, dependiendo de si queremos que cumpla todas las condiciones o solo una de ellas, y del nombre de la clase.

En nuestro caso podríamos diferencias dos tipos de clase: los paquetes con destino una red Ethernet, y los paquetes con destino una red Wifi.

MPLS1 (config) # ***class-map match-all Ethernet*** // creamos la clase "Ethernet" que debe cumplir todas las condiciones
MPLS1 (config-cmap) # ***match dscp CS1*** // creamos la condición que el paquete tenga el campo DSCP igual a CS1
Ahora aplicamos los mismos comandos, pero para crear la clase adecuada para la Wifi
MPLS1 (config) # ***class-map match-all Wifi*** // creamos la clase "Wifi" que debe cumplir todas las condiciones
MPLS1 (config-cmap) # ***match dscp CS2*** // creamos la condición que el paquete tenga el campo DSCP igual a CS2
MPLS1 (config-cmap) # ***end*** // salimos de la configuración de la clase
MPLS1 (config) # ***class-map match-all videoEthernet*** // creamos la clase "videoEthernet" que debe cumplir todas las condiciones
MPLS1 (config-cmap) # ***match mpls experimental 1*** // creamos la condición que el paquete tenga el campo EXP igual a 1
MPLS1 (config-cmap) # ***end*** // salimos de la configuración de la clase
MPLS1 (config) # ***class-map match-all videoWifi*** // creamos la clase "videoWifi" que debe cumplir todas las condiciones.
MPLS1 (config-cmap) # ***match mpls experimental 2*** // creamos la condición que el paquete tenga el campo EXP igual a 2
MPLS1 (config-cmap) # ***end*** // salimos de la configuración de la clase.

Ahora mismo puede que no quede muy clara la función de estas dos últimas clases, pero se entenderá mejor después de asignar las políticas a los interfaces.

3.8.2. Definir políticas de QoS

Para definir las políticas de QoS tenemos que usar el comando **policy-map** seguido del nombre de la política.
MPLS1 (config) # ***policy-map marcarEXP1*** // creamos la política "marcarEXP1"

MPLS1 (config-pmap) # ***class Ethernet*** // asignamos la clase "Ethernet" a esta política

MPLS1 (config-pmap) # ***set mpls experimental 1*** // la política marcará los paquetes de la clase con el campo EXP igual a 1

MPLS1 (config-pmap) # ***end*** // salimos de la configuración de la política

MPLS1 (config) # ***policy-map marcarEXP2*** // creamos la política "marcarEXP2"

MPLS1 (config-pmap) # ***class Wifi*** // asignamos la clase "Wifi" a esta política

MPLS1 (config-pmap) # ***set mpls experimental 2*** // la política marcará los paquetes de la clase con el campo EXP igual a 2

MPLS1 (config-pmap) # ***end*** // salimos de la configuración de la política

Ahora vamos a crear las políticas que realmente modificarán el comportamiento del tráfico:

Por ejemplo podemos definir que todo el tráfico que supere los 5Mbps con destino una red Ethernet sea descartado. Así mismo, todo el que supere 3Mbps con destino una red Wifi también será descartado.

MPLS1 (config) # ***policy-map shapeEthernet*** // creamos la política "shapeEthernet"

MPLS1 (config-pmap) # ***class videoEthernet*** // asignamos la clase "videoEthernet" a esta política

MPLS1 (config-pmap) # ***shape peak 500000*** // la política descartará los paquetes que superen los 5Mbps

MPLS1 (config-pmap) # ***end*** // salimos de la configuración de la política

MPLS1 (config) # ***policy-map shapeWifi*** // creamos la política "shapeWifi"

MPLS1 (config-pmap) # ***class videoWifi*** // asignamos la clase "videoWifi" a esta política

MPLS1 (config-pmap) # ***shape peak 300000*** // la política descartará los paquetes que superen los 3Mbps

MPLS1 (config-pmap) # ***end*** // salimos de la configuración de la política

3.8.3. Asignar las políticas a los interfaces

Ahora que ya tenemos definidas las clases de servicios y las políticas, solo nos queda asignar dichas políticas a los interfaces. Para hacerlo debemos usar el comando **service-policy**.

MPLS1 (config)# ***interface f0/0*** //Entramos en la configuración del interfaz f0/0
MPLS1 (config-if)# ***service-policy input marcarEXP1*** // Asignamos la política "marcarEXP1" a la entrada de la interfaz
MPLS1 (config-if)# ***exit***// Salimos de la configuración del interfaz
MPLS1 (config)# ***interface f0/1*** //Entramos en la configuración del interfaz f0/1
MPLS1 (config-if)# ***service-policy output shapeEthernet*** // Asignamos la política "shapeEthernet" al interfaz de salida f0/1

El total de pasos que hemos seguido se pueden resumir en el siguiente diagrama:

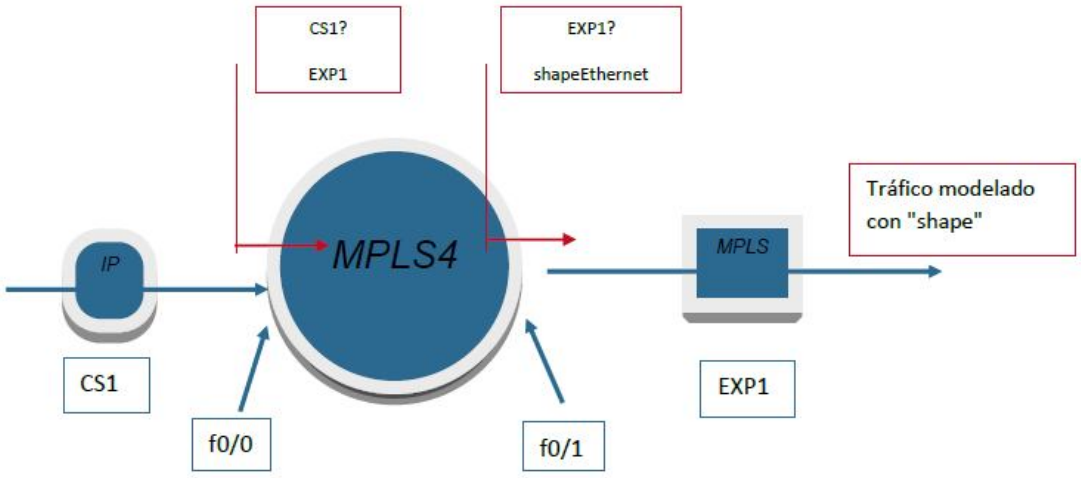


Figura 25 : diagrama de la aplicación de QoS.

En este diagrama se recoge de forma esquemática el proceso que sigue un paquete que entra en la red MPLS cuando está configurada una política de QoS para modelar el tráfico de Ethernet. El caso de Wifi sería equivalente:

1. Llega un paquete IP

2. La interfaz de entrada (f0/0) comprueba si el campo DSCP del paquete es CS1 (Si su destino es una red Ethernet, tendrá marcado su campo DSCP con el valor "CS1"). En caso afirmativo, marca el paquete con el campo EXP igual a 1

3. La interfaz de salida (f0/1) comprueba si el campo EXP del paquete es igual a 1, si lo es, aplica la política "shapeEthernet"

Esta solución parece un poco rebuscada, ya que parece más sencillo que el interfaz de salida comprobara si el campo DSCP del paquete tiene el valor "CS1" y entonces aplique la política. El problema es que el paquete que sale de la interfaz de salida ya no es un paquete IP, sino que es un paquete MPLS, y por lo tanto el interfaz no encuentra el campo DSCP.

3.9. Pruebas a través de los routers IP-MPLS - Ethernet

Medidas: Caudal, retardo extremo-extremo, jitter extremo-extremo, pérdidas
Estas medidas se tomarán mediante ping e Jperf (duración 2 minutos), capturando mediante WireShark las trazas de todo el tráfico emitido y recibido, para los siguientes casos de uso:

Caso 1: Medidas sin afectación de ningún tipo (medidas libres)
Caso 2: Medidas con rotura de enlace y activación de Backup. La rotura se emulará mediante la simple desconexión de uno de los enlaces.
Caso 3: Transmisión de tráfico real enviando video con el programa VLC, repitiendo los casos 1, 2.
Escenario: Como usaremos el camino de Backup, el escenario será el siguiente:

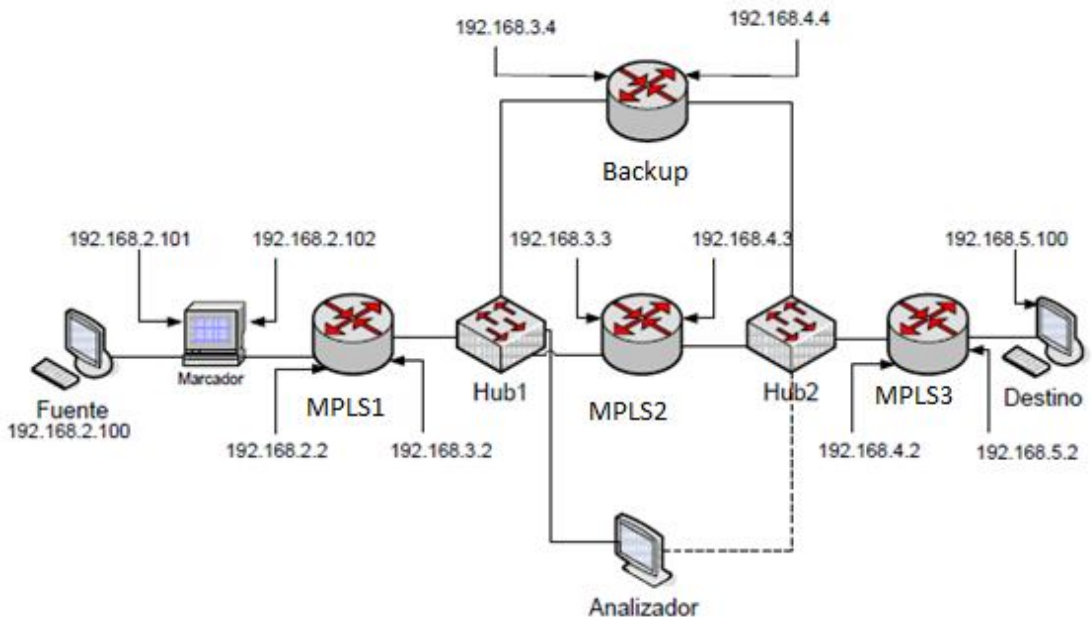


Figura 26 : escenario con backup pruebas Ethernet.

Caso 1:

Con el comando ping obtenemos los siguientes paquetes:

```
No.          Time                Source       Destination  Protocol Info

37           15.996779           192.168.2.100      192.168.5.100      ICMP   Echo
(ping) request

Internet   Protocol,   Src:   192.168.2.100   (192.168.2.100),   Dst:   192.168.5.100
(192.168.5.100)
```

```
No.          Time                Source       Destination        Protocol Info

38           15.996824           192.168.5.100      192.168.2.100            ICMP
      Echo (ping) reply
```

Figura 27 : caso 1 comando ping.

Esto nos indica que el retraso es (15.996824-15.996779)/2 = **22.5 µs**

En media, el retardo del comando ping es: **22.33 µs.**

Ahora medimos el caudal, con la herramienta Jperff, configurada con el protocolo UDP para que no introduzca retardo.

El caudal capturado en cada uno de los puntos de observación es el siguiente:

Origen.

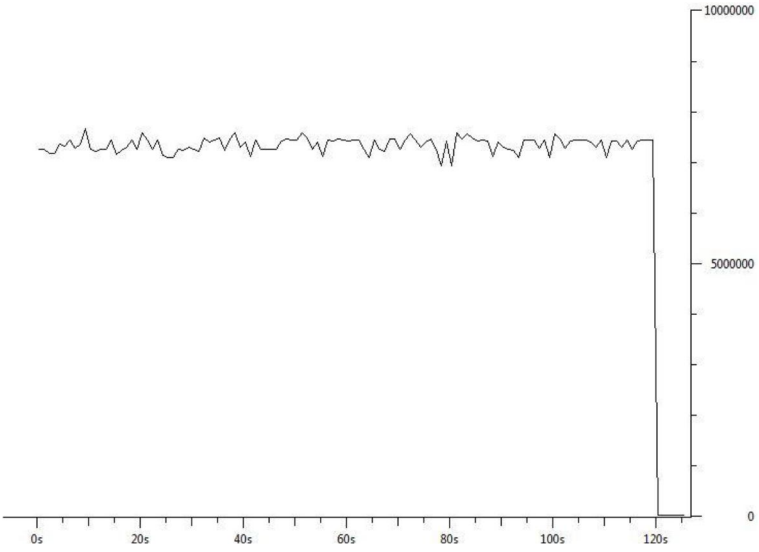


Figura 28 : caudal en el origen en bits por segundo A.

Analizador:

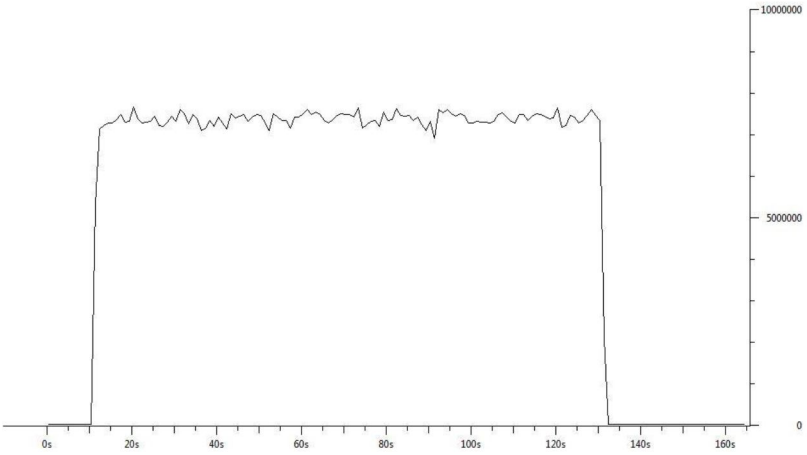


Figura 29 : caudal en el analizador en bits por segundo A.

Destino:

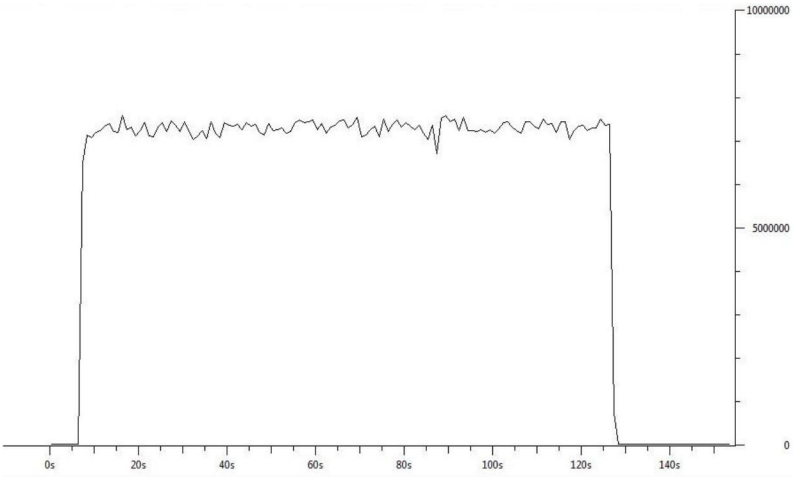


Figura 30 : caudal en el destino en bits por segundo A.

Donde podemos observar como el tráfico está limitado a unos 7,5 Mbps y es prácticamente idéntico en los 3 puntos. Aunque esta red MPLS puede llegar a una velocidad de 100Mbps, la tarjeta de red entre el "Origen" y el "Marcador" limita la red a 10Mbps como máximo.

También obtenemos el siguiente jitter extremo a extremo:

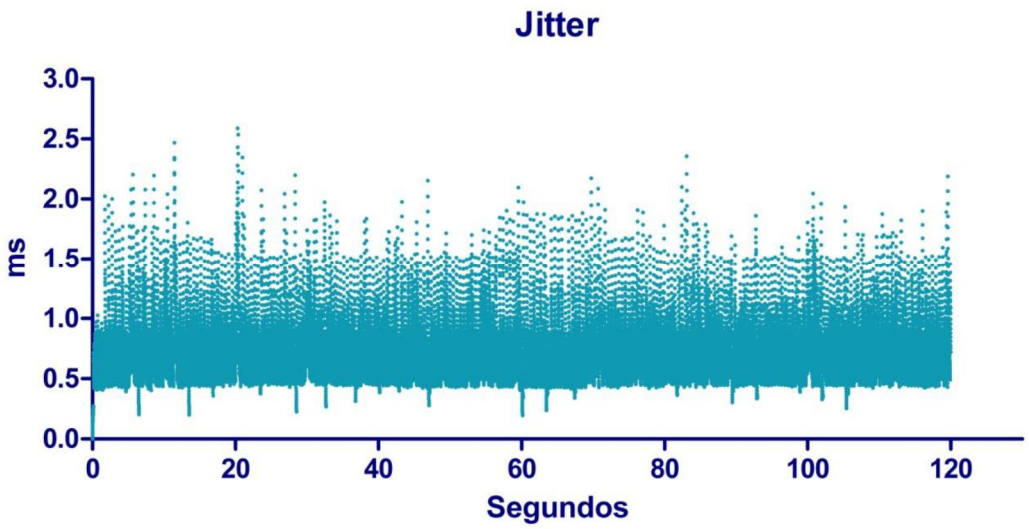


Figura 31 : jitter del caso 1.

Con **valor medio**: **0.7818 ms**

Cabe destacar que cada uno de los puntos de la gráfica corresponde a un paquete enviado a través de la red. Se puede observar que el jitter de una muestra depende de la anterior, ya que se ha calculado siguiendo la siguiente fórmula:

D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)

Donde Rn es el tiempo en que se recibe el paquete “n” y Sn el momento en que se envía ese paquete.

J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16

J(x) es la función del jitter, y por lo tanto J(i) es el jitter del paquete “i”.

Finalmente, si observamos en número de paquetes emitidos y los recibidos, podemos calcular que el tanto por ciento de pérdidas es: (278779/280528)=99.37%, **pérdidas** = 100-99,37= **0.63%**

Caso 2:

En este segundo caso desconectaremos el cable entre el Hub1 y el router MPLS2 sobre el segundo 30 de la transmisión. Luego, a los 60 segundos lo volveremos a conectar.

El caudal capturado en cada uno de los puntos de observación es el siguiente:

Origen:

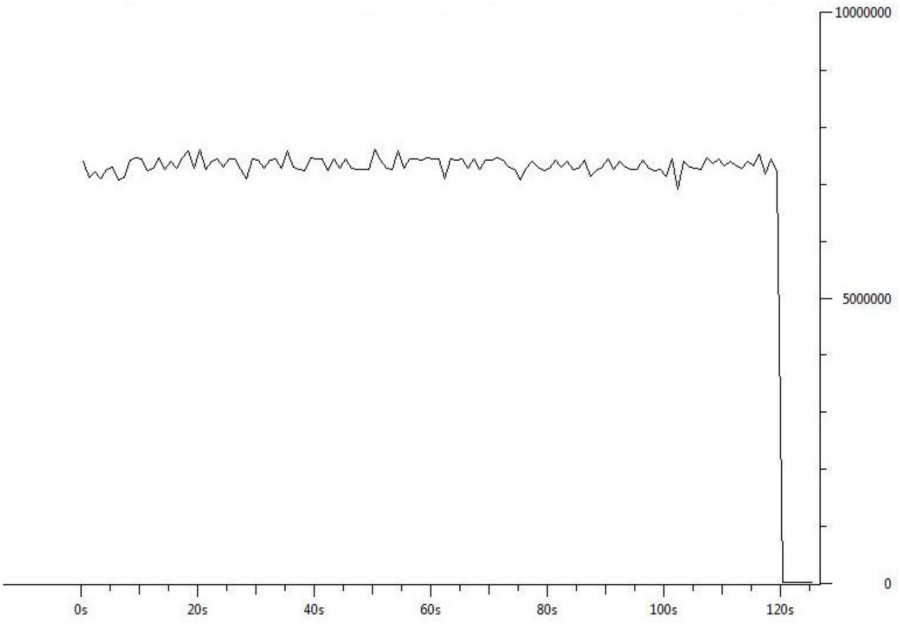


Figura 32 : caudal en el origen en bits por segundo B.

Analizador:

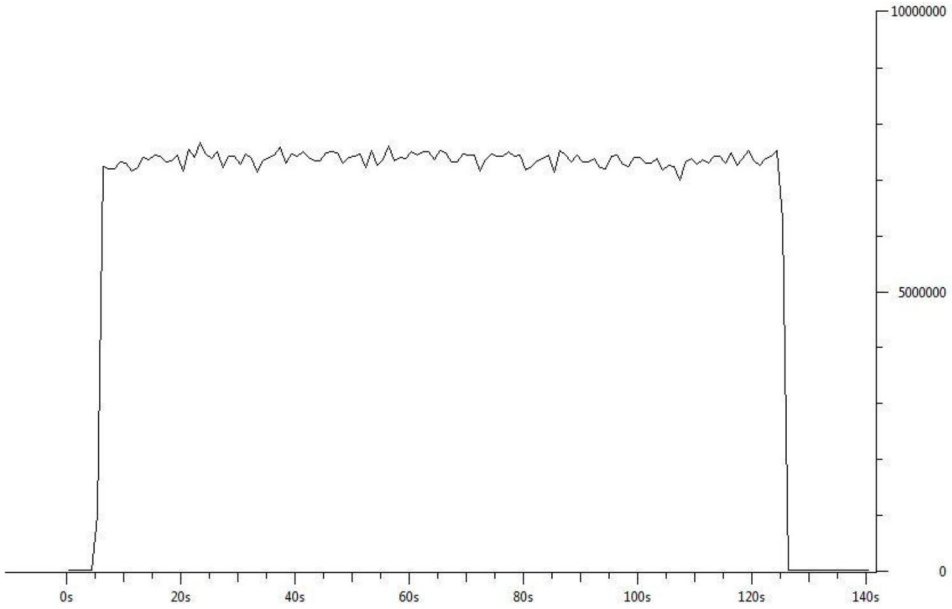


Figura 33 : caudal en el analizador en bits por segundo B.

Destino:

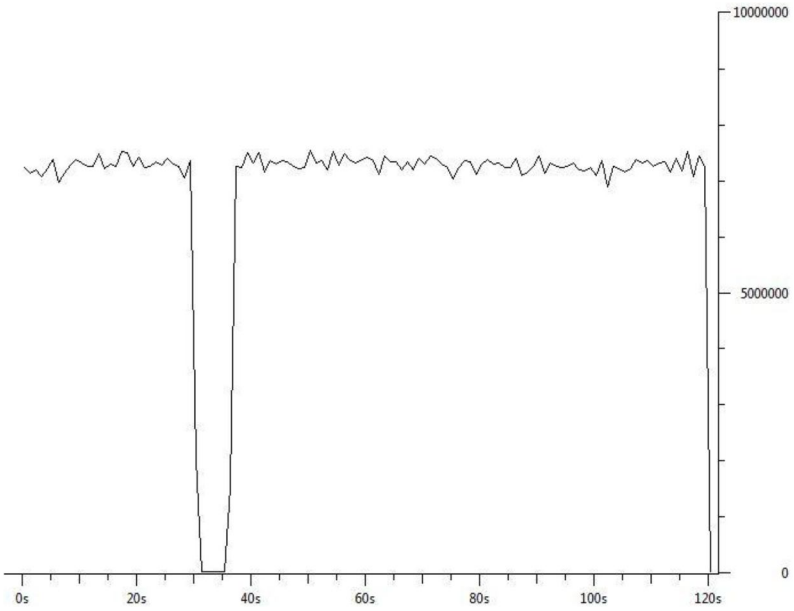


Figura 34 : caudal en el destino en bits por segundo B.

Si separamos el ancho de banda capturado por el “Analizador” en función del destino del paquete, podemos ver claramente cómo actúa el mecanismo de Backup que hemos implementado:

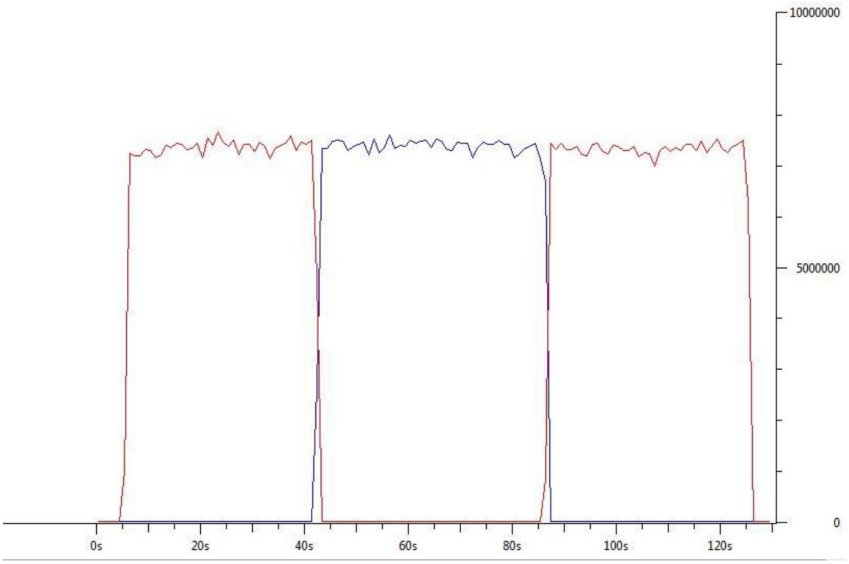


Figura 35 : detalle del destino de los paquetes en el analizador en bits por segundo.

El jitter extremo-extremo en este caso es el siguiente:

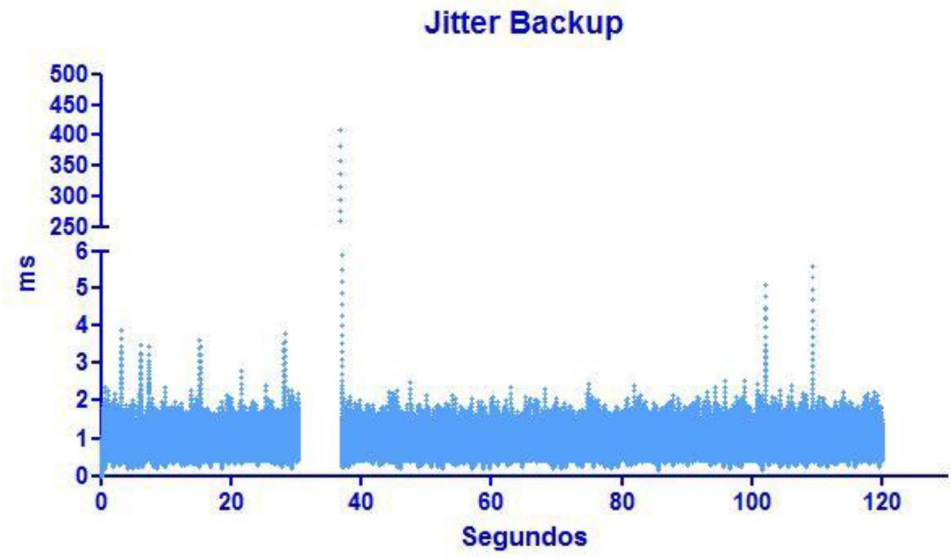


Figura 36 : jitter caso 2.

Y con valor medio: 0.8046 ms

En este caso el porcentaje de pérdidas será muy superior debido al corte: (263119/280045)=93.95% recibidos, por lo tanto las pérdidas = 100-93.95= **6.05%** Cabe destacar que el enlace ha estado caído 6.6seg, que representa un **5.5%** del tiempo total.

Caso 3:

Caso 3.1:

Transmitimos 2 minutos de vídeo sin afectación. Para este caso, usaremos para el envío el mismo protocolo de trasporte UDP con el Jperff, ya que es el más adecuado para la transmisión de vídeo, porque no introduce retardo.

Origen:

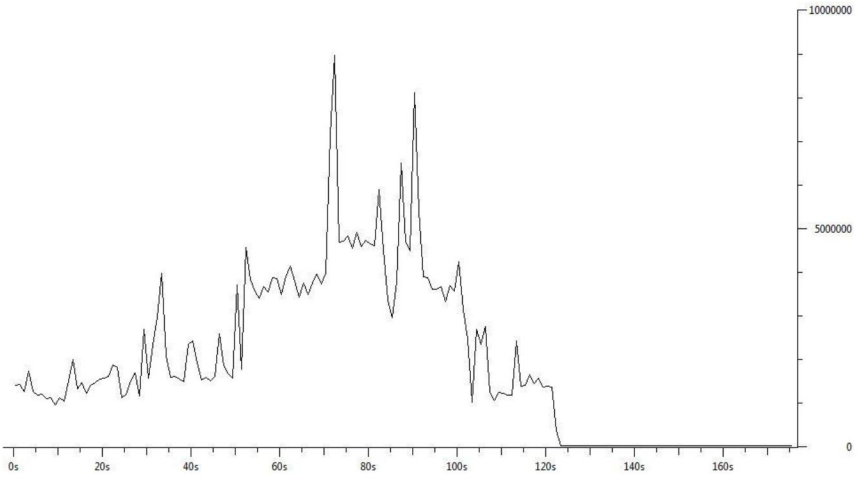


Figura 37 : caudal en el origen en bits por segundo C.

Analizador:

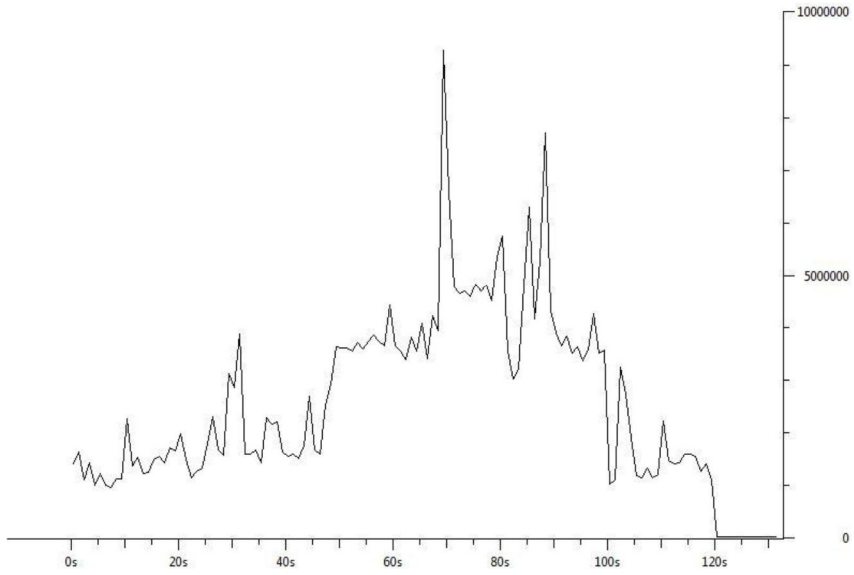


Figura 38 : caudal en el analizador en bits por segundo C.

Destino:

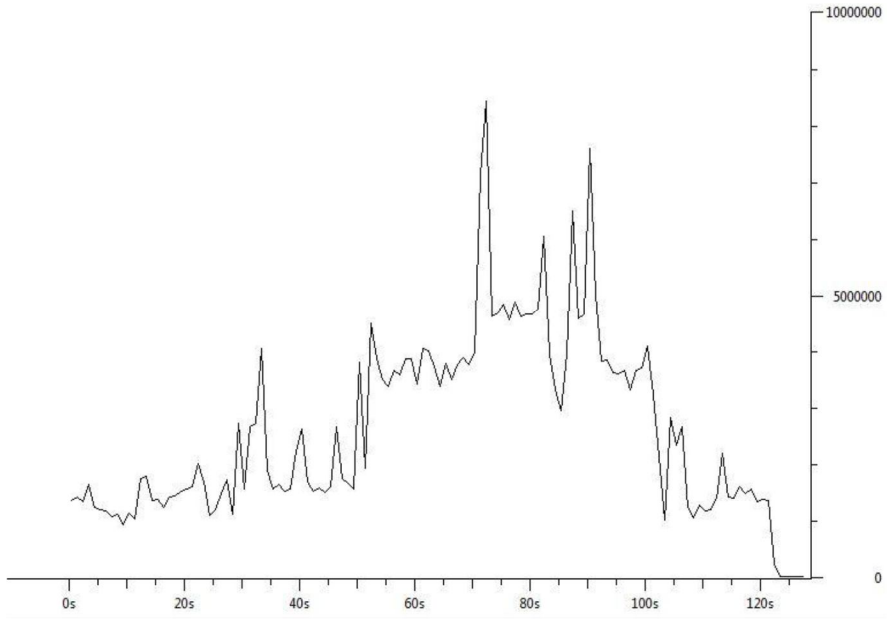


Figura 39 : caudal en el destino en bits por segundo C.

Y el jitter en este caso es:

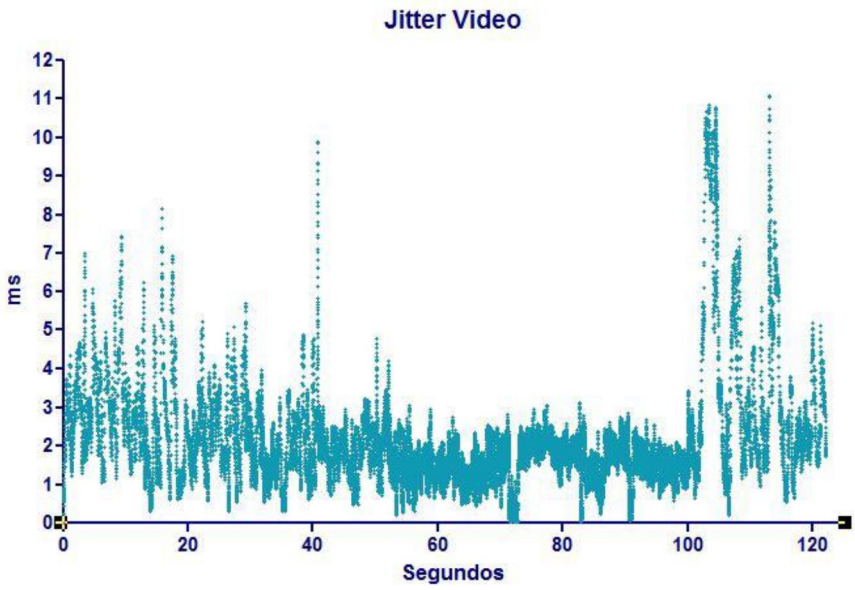


Figura 40 : jitter caso 3.1.

Con valor medio: **2.81 ms**

Las pérdidas sin corte son: 1- (30745/30917)= **0.56%**

Caso 3.2:

Ahora repetimos la misma transmisión pero desconectando el mismo enlace que en el **Caso 2**, en los mismos instantes.

Origen:

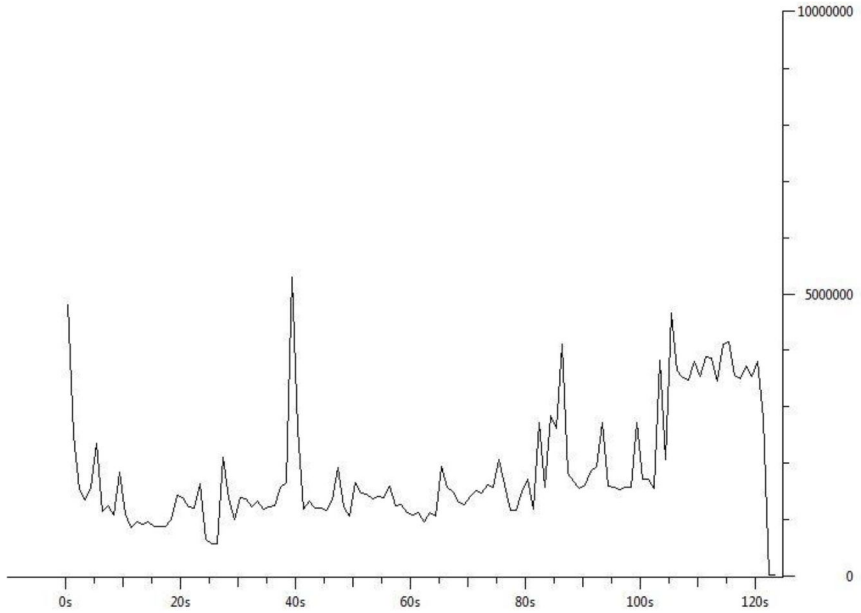


Figura 41 : caudal en el origen en bits por segundo D.

Analizador:

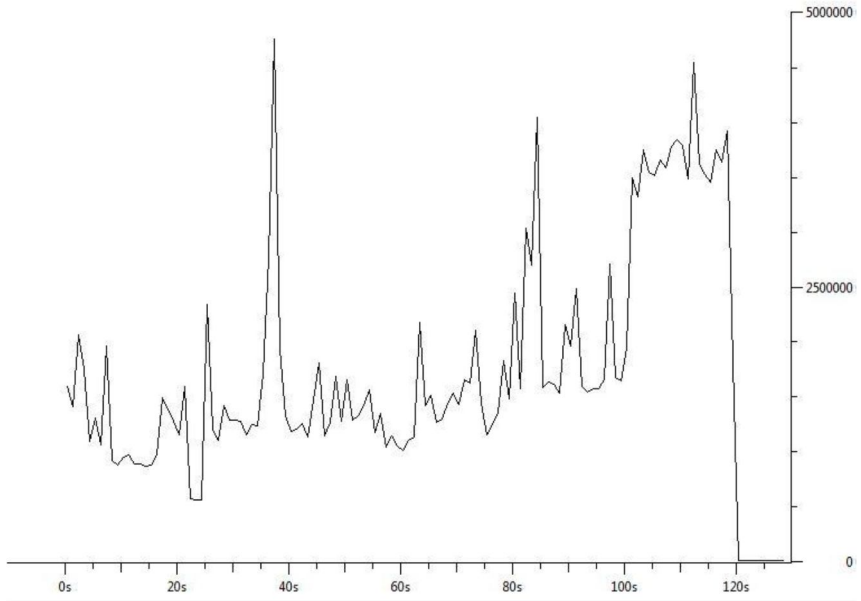


Figura 42 : caudal en el analizador en bits por segundo D.

Destino:

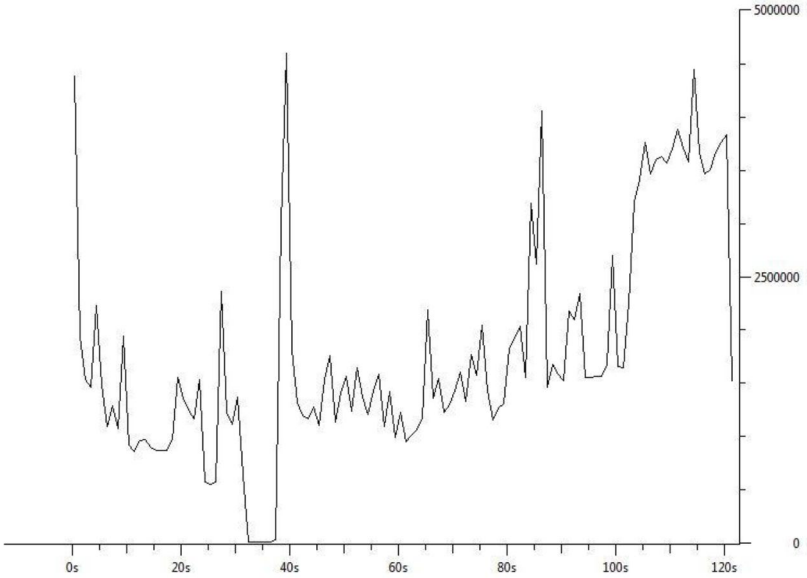


Figura 43 : caudal en el destino en bits por segundo D.

Como en el caso anterior, si separamos el ancho de banda capturado por el "Analizador" en función del destino del paquete, podemos ver claramente cómo actúa el mecanismo de Backup que hemos implementado:

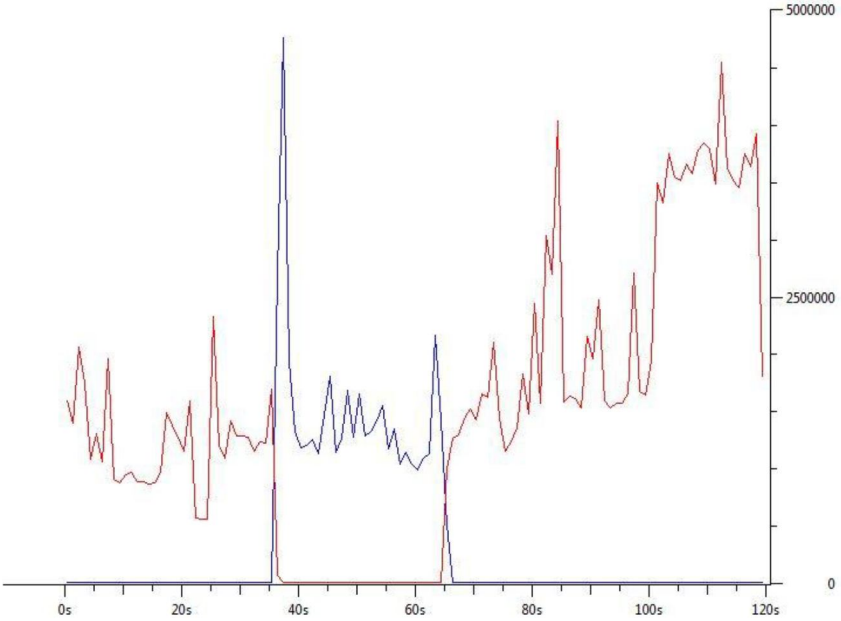


Figura 44 : detalle del destino de los paquetes en el Analizador en bits por segundo.

Y con Jitter:

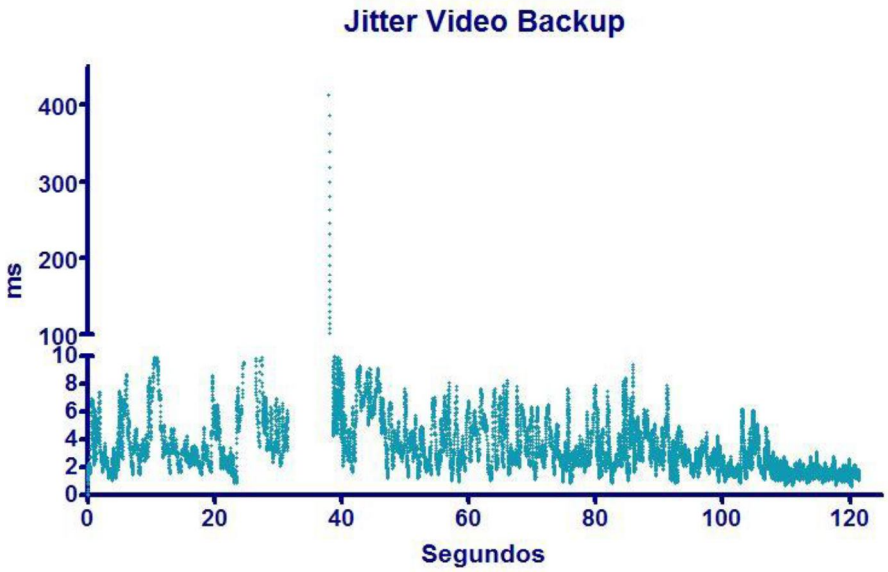


Figura 45 : jitter caso 3.2.

Con **valor medio: 3.733 ms**

Las pérdidas con el corte son: 1 - (19986/20900) = **4.38%.** Aunque el enlace está interrumpido durante **6.5 seg.** que es equivalente al **5.3%** del tiempo, la interrupción se ha producido durante un periodo con tasa de envió baja, lo que explica las bajas pérdidas.

3.9.1. Resultados.

Si recogemos los resultados obtenidos en los anteriores casos, obtenemos la siguiente tabla:

Caso	Porcentaje de tiempo sin conexión	Porcentaje de pérdidas	Valor medio del Jitter
Caso 1	0%	0.63%	0.7818 ms
Caso 2	5.5%	6.05%	0.8046 ms
Caso 3.1	0%	0.56%	2.1 ms
Caso 3.2	5.3%	4.38%	3.733 ms

Tabla 10: Resultados de las pruebas MPLS – Ethernet.

En el caso 1 hemos sometido a la red a su máxima capacidad. Los resultados de este caso nos sirven como control para las medidas del resto de casos. Vemos que la red se comporta de forma bastante transparente (la forma de las gráficas del caudal del origen y destino son prácticamente iguales), y solo se pierden el 0.63% de los paquetes, con un jitter que oscila entre 0.5 y 2 ms, pero con valor medio bastante inferior a 1ms.

Cuando en el caso 2 se pierde la conectividad en un nodo durante 30 segundos, debido a que se ha configurado el “dead time” del OSPF a 5 segundos, la red tarda esos 5 segundos en darse cuenta que el nodo ha sido desconectado. Luego realiza el cambio hacia el router de Backup, tardando en total 6.6 segundos en recuperarse. En total se pierden un 6.05% de los paquetes, aunque el 5.5% se pierden debido a la rotura del enlace. Por lo que respecta al jitter, aumenta ligeramente si lo comparamos con el caso 1, debido obviamente a la desconexión que ha sufrido la red, pero sigue siendo inferior a 1 ms.

Finalmente, cuando repetimos las medidas pero con tráfico real (caso 3.1), vemos que el porcentaje de paquetes perdidos disminuye. Este hecho es lógico, ya que el vídeo transmitido no usa el máximo caudal disponible por el enlace, y por lo tanto se producen menos errores. Por otro lado, al no tener el vídeo un caudal constante, el jitter aumenta considerablemente (2.1 ms de media) y fluctúa entre 0 y 11 ms. A pesar de este aumento, cómo el programa VLC usa un buffer donde

guardar momentáneamente los paquetes recibidos, el vídeo se reproduce correctamente y sin saltos en el destino.

Cuando se desconecta el enlace en el caso 3.2, la red se recupera como en el caso 2, pero un observador en el destino, que esté viendo el vídeo, no se percata de la desconexión. Esto se debe a que en el instante de la desconexión se estaban transmitiendo pocos datos (vemos que el porcentaje de paquetes perdidos es inferior al porcentaje de tiempo desconectado) y por lo tanto si el buffer tarda más en vaciarse que el tiempo que el enlace está desconectado, el vídeo no se interrumpe.

El jitter para este caso aumenta más que en la relación del caso 1 y 2, pero los instantes de vídeo transmitidos en los casos 3 .1 y 3.2 no son exactamente los mismos, y por lo tanto no es comparable.

Con esta prueba se puede concluir que la red troncal MPLS funciona tal como se esperaba al conectar a su destino una red Ethernet.

Recomendaciones.

Según los requisitos específicos que tienen algunas redes se deben adoptar ciertos parámetros para poder migrar a una implementación MPLS, sin embargo existen algunos aspectos a tomar en cuenta para la migración hacia una arquitectura MPLS.

- Actualizar el Software de los dispositivos de la Red a una versión compatible con los requerimientos necesarios de MPLS, así mismo se debe tener en cuenta los requisitos mínimos de memoria en los dispositivos.

- Diseñar e implementar la nueva configuración de los protocolos de enrutamiento (BGP, Intercambio de Información con otros Routers) que funcionará en paralelo al Control de Enrutamiento MPLS (Intercambio de Asignación con otros Routers). Sobre una Red LAN se debe tener en cuenta los valores Ethertype 8847 HEX y 8848 HEX. Sobre enlaces PPP se debe introducir un nuevo protocolo de Control de Red (NCP) que dentro del ambiente MPLS se conocerá como MPLSCP donde los paquetes estarán marcados con el valor 8281 HEX dentro del protocolo PPP. Sobre una infraestructura Frame Relay en el campo DLCI se tendrá un valor Ethertype 8847 HEX y por último los paquetes que serán transmitidos sobre una Red ATM tendrán el mismo tratamiento que una Red LAN incluyendo los valores Ethertype.
- Teniendo en cuenta los requisitos mínimos de actualización se puede realizar una Migración Parcial o Total de la Red.

- Migrar la parte de Routers de la Red, para redes que utilizan como infraestructura principal ATM se debe ejecutar MPLS como paso provisional.
- Verificar que la Red se encuentre estable y que se realice la Conmutación. Se debe verificar que los Routers principales sólo envíen paquetes etiquetados.

Conclusiones.

Con este trabajo de redes de nueva generación con énfasis en la tecnología de transporte MPLS expusimos las ventajas y debilidades que esta proporciona.

Al estudiar la arquitectura y el funcionamiento del protocolo MPLS vemos que estas redes son adecuadas para la trasmisión de tráfico con altas demandas de QoS como la video conferencia o la transmisión de video con streaming.

Presentamos la propuesta de un diseño de una red MPLS así como las configuraciones básicas para establecer una conexión extremo-extremo también la de un camino Backup para dotar a la red de estabilidad. Y una técnica de marcado de trafico con Diffserv para que la red posea cierto QoS.

En nuestra opinión no cabe duda que MPLS representa una de las soluciones más eficaces para las redes de transporte su condición de multiprotocolo y su capacidad de ofrecer mecanismo de QoS la convierten en uno de los mejores sistemas.

Bibliografía.

(Rosen)
Rosen, (s.f) et al. Standards. *RFC 3031* MPLS Architecture January 2001 recuperado el 1 de mayo del 2014,
www.ietf.org/rfc/rfc3031.txt

(E Mannie)
E Mannie (s.f) RFC 3945 GMPLS Architecture, 2004 recuperado el 1 de mayo del 2014,
tools.ietf.org/html/rfc3945

(CISCO)
Recuperado el 5 de mayo del 2014,
http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

(Canalis)
Canalis, MS (s.f) conceptos MPLS, recuperado el 10 de mayo del 2014,
exa.unne.edu.ar/depar/areas/informatica/.../libmpls.PDF

(Flores)
Flores Moyano - 2006 (s.f) arquitectura MPLS, recuperado el 11 de Mayo del 2014.
dspace.ups.edu.ec/bitstream/123456789/209/2/Capitulo%201.pdf

(Rivera)
Rivera Fuertes – 2005 (s.f) GMPLS, recuperada el 11 de mayo del 2014
bibdigital.epn.edu.ec/bitstream/15000/5021/1/T10102.pdf

(Pitágoras)

Pitágoras -2010 (s.f) arquitectura GMPLS, recuperado el 13 de mayo del 2014

http://pitagoras.usach.cl/~eflores/lcc/cd_redes/arquitectura-gmpls.pdf

(Ramón)

Ramón Jesús Millan -2008 (s.f) tutorial MPLS, recuperado el 15 de mayo del 2014,

www.abcdatos.com/tutoriales/tutorial/z9527.html

(IETF)

IETF (s.f) diciembre 1998 *RFC 2475* Architecture for Differentiated Services recuperado el 17 de mayo del 2014.

www.ietf.org/rfc/rfc2475.txt

(Adrian)

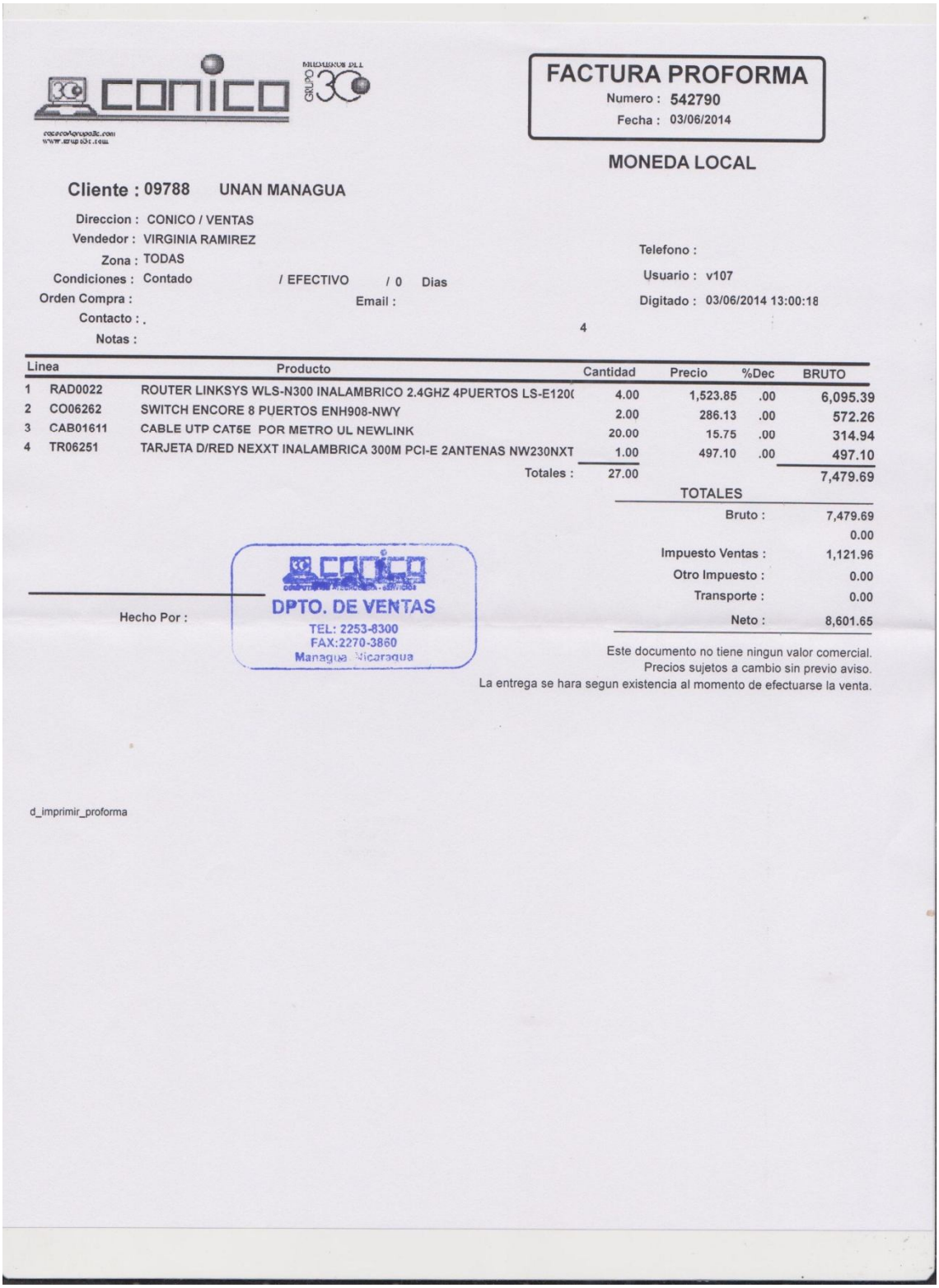
Adrian Delfino (s.f) -2010 Ingeniería de tráfico, recuperado el 17 de mayo del 2014,

http://iie.fing.edu.uy/investigacion/grupos/artes/fce/nette/Ingenieria_de_Trafico_en_Redes_MPLS.pdf

(Sebastián)

Sebastián Rivero (s.f) - 2010 RFC 5777, recuperado el 18 de mayo del 2014 tools.ietf.org/html/rfc5777

Anexos



CONICO

FACTURA PROFORMA
Numero : 542790
Fecha : 03/06/2014

MONEDA LOCAL

Cliente : 09788 UNAN MANAGUA

Direccion : CONICO / VENTAS
Vendedor : VIRGINIA RAMIREZ
Zona : TODAS
Condiciones : Contado / EFECTIVO / 0 Dias
Orden Compra :
Contacto : .
Notas :

Telefono :
Usuario : v107
Digitado : 03/06/2014 13:00:18
Email :
4

Linea		Producto	Cantidad	Precio	%Dec	BRUTO
1	RAD0022	ROUTER LINKSYS WLS-N300 INALAMBRICO 2.4GHZ 4PUERTOS LS-E120(	4.00	1,523.85	.00	6,095.39
2	CO06262	SWITCH ENCORE 8 PUERTOS ENH908-NWY	2.00	286.13	.00	572.26
3	CAB01611	CABLE UTP CAT5E POR METRO UL NEWLINK	20.00	15.75	.00	314.94
4	TR06251	TARJETA D/RED NEXXT INALAMBRICA 300M PCI-E 2ANTENAS NW230NXT	1.00	497.10	.00	497.10
		Totales :	27.00			7,479.69

TOTALES

Bruto :	7,479.69
	0.00
Impuesto Ventas :	1,121.96
Otro Impuesto :	0.00
Transporte :	0.00
Neto :	8,601.65

Hecho Por :

CONICO
DPTO. DE VENTAS
TEL: 2253-8300
FAX:2270-3860
Managua Nicaragua

Este documento no tiene ningun valor comercial.
Precios sujetos a cambio sin previo aviso.
La entrega se hara segun existencia al momento de efectuarse la venta.

d_imprimir_proforma

Anexo I. a proforma CONICO.

Anexo I. b proforma SEVASA.

Descripción de los componentes que se utilizan en la propuesta de esta red.

Anexo I.c Cisco 2600 Series Routers de acceso modular

Enrutador Con un amplio apoyo para el enrutamiento de datos multiprotocolo, la voz y la integración de datos, acceso ADSL, ATM, marque los servicios de acceso y conmutación integrada, la serie Cisco 2600 ofrece una solución flexible, escalable e integrada que simplifica el proceso de implementación y administración de la rama-oficina soluciones de red.

La serie Cisco 2600 ofrece un completo conjunto de características ideales para soluciones que requieren los siguientes apoyos:

• Integración multiservicio de voz y datos

• Acceso VPN con opciones de firewall y encriptación

• Servicios de acceso de línea analógica

• Enrutamiento con gestión de ancho de banda

• Enrutamiento entre VLAN

• Entrega de acceso DSL de clase empresarial de alta velocidad

• Acceso ATM Rentable

• Integración de enrutamiento flexible y conmutación de baja densidad

• Integración de redes de contenido

• Integración de los sistemas de detección de intrusiones (IDS)

• Integración de los sistemas de análisis de red

Los fundamentos de estas soluciones son el Cisco IOS ® Software con elementos de seguridad, disponibilidad, calidad de servicio (QoS), capacidad de gestión, y la integración combinadas,.

La arquitectura modular de la serie Cisco 2600 permite a las interfaces actualizarse para adaptarse a la expansión de la red o los cambios en la tecnología, se implementan nuevos servicios y aplicaciones. Sus Interfaces modulares son compartidos con el Cisco 1700 y Cisco 3700. Módulos de red disponibles para el Cisco 2600 y Cisco 3700 series soportan una amplia gama de aplicaciones, incluyendo multiservicio de voz y la integración de datos, conmutación integrada, analógica y de acceso telefónico RDSI, y la concentración de dispositivo serie.

Anexo I. d Tabla. Características de los router cisco 2600.

Plataforma	Módulos de Red	AIM	WIC	Fijos puertos LAN	Rendimiento (hasta kpps)	DRAM (MB por defecto y / o máxima MB)	Memoria Flash (por defecto MB / máxima MB)	Incluye software de funciones de Cisco IOS Set
Cisco 2610XM y Cisco 2611XM	1	1	2	1 Fast Ethernet / Fast Ethernet 2	20	128/256	32/48	Cisco IOS Software Base IP
Cisco 2612	1	1	2	1 Token Ring / Ethernet 1	15	32/64	8/16	Cisco IOS Software Base IP
Cisco 2620XM y Cisco 2621XM	1	1	2	1 Fast Ethernet / Fast Ethernet 2	30	128/256	32/48	Cisco IOS Software Base IP
Cisco 2650XM y Cisco 2651XM	1	1	2	1 Fast Ethernet / Fast Ethernet 2	40	256/256	32/48	Cisco IOS Software Base IP

Anexo I. e Linksys E900

Modelo:	Linksys E900
Tecnología:	Inalámbrica N
Bandas:	2,4 GHz
Transmisión/recepción:	2 x 2
Antenas:	2 (internas)
Puerto USB:	No
Puertos x velocidad:	4 x Ethernet
Software Cisco Connect:	Sí, pero no incluye control parental ni acceso a invitados
Configuración:	CD de instalación Cisco Connect
Garantía:	Garantía limitada de 2 años para hardware
Compatibilidad con sistemas operativos:	Windows, Mac
Requisitos mínimos del sistema:	PC: equipo con Wi-Fi y unidad de CD o DVD, con Windows XP SP3, Windows Vista SP1 o versión posterior, Windows 7, o Windows 8 Mac: equipo con Wi-Fi y unidad de CD o DVD, con OS X Leopard 10.5 o Snow Leopard 10.6
Requisitos del navegador de Internet:	Internet Explorer 7, Safari 4, Firefox 3 o versión posterior para la configuración opcional en navegador

Anexo I. f tabla de descripción de router Linksys E900.

Anexo I. g Hub EN 104.

HUB o concentrador.

Un concentrador o HUB es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos. Trabaja en la capa física del modelo OSI o capa de Acceso en modelo TCP/IP.

Wireshark: es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

Jperf: permite al usuario ajustar varios parámetros que pueden ser usados para hacer pruebas en una red, o para optimizar y ajustar la red. Jperf puede funcionar como cliente o como servidor y puede medir el rendimiento entre los dos extremos de la comunicación, unidireccional o bidireccionalmente. Es software de código abierto y puede ejecutarse en varias plataformas incluyendo Linux, Unix y Windows.

- UDP: Cuando se utiliza el protocolo UDP, Jperf permite al usuario especificar el tamaño de los datagramas y proporciona resultados del rendimiento y de los paquetes perdidos.
- TCP: Cuando se utiliza TCP, Jperf mide el rendimiento de la carga útil.

Comparación de MPLS vs ETHERNET.

Costo	El coste de MPLS es mayor que el de Ethernet, pero menor que las líneas T1.	Ethernet es normalmente más asequible que MPLS.
Escalabilidad	MPLS puede escalarse a miles de sitios.	Ethernet puede escalarse a cientos de sitios.
Aplicaciones comunes	MPLS es la mejor opción para conectar centros de datos con sucursales, y conectar las sucursales entre sí.	Ethernet es la mejor opción para conectar centros de datos.
Enrutamiento WAN	MPLS permite que sean los proveedores los que controlen la WAN y requiere de menos personal para su gestión.	Ethernet requiere que los ingenieros controlen la WAN y el enrutamiento.
Conducta del protocolo WAN	MPLS puede gestionar casi cualquier aplicación, incluyendo voz y video.	Ethernet ofrece baja latencia y alta disponibilidad, perfecta para recuperación de desastres.
Calidad de servicio	MPLS ofrece opciones de calidad de servicio (QoS) para tratar especialmente ciertos tráficos, como el VOIP.	Los ingenieros de red pueden esquivar la complejidad de QoS mediante conmutadores conectados a la Ethernet.
Niveles de servicio	Los servicios MPLS incluyen acuerdos de nivel de servicio (SLAs) que incorporan garantías de rendimiento, igual que la banda ancha de consumo.	Los profesionales de IT tienen que pedir el SLA de su servicio Ethernet o de la aplicación WAN que estén usando.
Gestión WAN	Si usamos conectividad MPLS para WAN es necesario que todos los dispositivos y herramientas sean compatibles con MPLS y Ethernet.	Puesto que la LAN usa Ethernet, el uso de Ethernet sobre WAN ofrece a las empresas una infraestructura integral que simplifica la gestión de la red.
Disponibilidad	Muchos proveedores de servicio ofrecen MPLS en zonas metropolitanas, pero no en todas.	Los cambios en las WAN sobre Ethernet hacen que estén disponibles en muchas ubicaciones.

Anexo I. h tabla .comparativa MPLS y Ethernet para WAN.

Abreviaturas.

AS	Autonomous System.
ATM	Asynchronous Transfer Mode.
ASON	Automatically Switched Optical Network.
BGP	Border Gateway Protocol.
CR-LDP	Constraint-based Routing LDP.
CSPF	Constraint-based Shortest Path First.
CEF	Cisco Express Forwarding.
DWDM	Dense Wavelength Division Multiplexing.
FA	Forwarding Adjacency.
FRR	Fast Rerouting.
FSC	Fiber Switched Channel.
GMPLS	Generalized Multi-Protocol Label Switching.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
IGP	Interior Gateway Protocol.
IS-IS	Intermediate System to Intermediate System.
LDP	Label Distribution Protocol.
LMP	Link Management Protocol.
LSA	Link State Advertisement.
LSC	Lambda Switched Channel.
LSR	Label Switched Router.
LSP	Label Switched Path.
LOL	Loss Of Light.
MPLS	Multi-Protocol Label Switching
NGN	Next Generation Networks.
OSI	International Standard Organization.
OSPF	Open Shortest Path First.
OXC	Optical Cross-Connect.
PXC	Photonic Cross-Connect.
PSC	Packet Switch Capable.
QoS	Quality of service.
RSVP	Resource Reservation Protocol.
SDH	Synchronous Digital Hierarchy.
OSPF	Open Shortest Path First.
TCP	Transmission Control Protocol.
TDM	Time-Division Multiplexing.
TE	Traffic Engineering.