FACULTAD DE CIENCIAS E INGENIERIAS FÍSICAS Y FORMALES

PROGRAMA PROFESIONAL DE INGENIERIA DE SISTEMAS

SIMULACION DE UN PROTOCOLO SINCRONO DE DETECCION LIMITADA POR MEDIO DE LA RESERVACION DE RECURSOS CON MPLS

Tesis presentada por las Bachilleres:

AYALA CARDENAS BRENDA LIZ

MAMANI IGLESIAS LINCCY VANESSA

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS

AREQUIPA-PERÚ

2016

PRESENTACIÓN

Sra. Directora del Programa Profesional de Ingeniería de Sistemas.

Sres. Miembros del Jurado.

De conformidad con las disposiciones del Reglamento de Grados y Títulos del Programa Profesional de Ingeniería de Sistemas, ponemos a vuestra consideración el presente trabajo de investigación titulado: "SIMULACION DE UN PROTOCOLO SINCRONO DE DETECCION LIMITADA POR MEDIO DE LA RESERVACION DE RECURSOS CON MPLS", el mismo que de ser aprobado me permitirá optar el Título Profesional de Ingeniería de Sistemas.

Ayala Cárdenas, Brenda Liz

Mamani Iglesias, Linccy Vanessa

AGRADECIMIENTOS

A Dios porque a pesar de los inconvenientes y problemas que tuvimos siempre estuvo presente en nosotras la fortaleza de seguir y continuar con nuestro trabajo.

A nuestros padres por estar presente en todos los momentos importantes de nuestra vida, por brindarnos su amor, su comprensión y su apoyo incondicional.

A nuestro Asesor por sus recomendaciones y guía a lo largo de nuestro proyecto.

DEDICATORIA

A Dios por ser nuestra guía, a nuestros amados padres por ser el pilar fundamental en todo lo que somos, por la motivación constante en toda nuestra educación, por ese incondicional apoyo perfectamente mantenido a través del tiempo, a cada uno de nuestros familiares , al pequeño Alessandro, a nuestros seres queridos que partieron a su encuentro con Dios y desde arriba nos protegen, a nuestros amigos por confiar en que lo lograríamos y para nuestra asesora por brindarnos su tiempo y sus consejos.

Todo este trabajo ha sido posible gracias a ellos.

TABLA DE CONTENIDO

Pág.

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE GRÁFICOS

Pág.

RESUMEN

En la actualidad con los cambios tecnológicos registrados y el uso de los servicios de internet ya no son los mismos, tenemos un crecimiento desmesurado, ya no estamos en la posibilidad de aceptar los estándares TCP/IP "como de mejor esfuerzo", donde asociábamos calidad de servicio con confiablidad.

Hoy en día la demanda de aplicaciones que utilizan la transmisión de video, Voz sobre IP son mayores y las empresas proveedoras de servicios de internet son las afectadas quienes atraviesan congestionamiento en las líneas de backbone. De este modo se hace inevitable la necesidad de desplegar una tecnología capaz de aliviar esta situación.

Utilizando el concepto de "Ingeniería de Tráfico " que consiste en adaptar los flujos de tráfico con los recursos disponibles de tal manera que no existan unos sobre utilizados generando cuellos de botella, mientras queden otros sub utilizados causando desperdicio de ancho de banda, todo esto empleado la señalización para garantizar la calidad de servicio al reservar ancho de banda para flujos de datos compatibles con RSVP con una correcta clasificación de paquetes y planificación para cumplir con las reservas especificadas. Es lo que nos promete el protocolo MPLS (siglas en inglés Multiprotocol Label Switching) y RSVP (siglas en inglés Resource Reservation Protocol) como una solución fiable, compatible con todos los protocolos, segura y fácil de administrar.

Habilitar túneles de ingeniería de tráfico para acelerar el encaminamiento de paquetes, podemos realizar esta función debido a que MPLS es capaz de integrar los niveles 2 (Enlace de datos) y 3 (Red), sacando máximo provecho de lo mejor de cada una de ellas (la inteligencia del routing con la rapidez del switching) MPLS implica una evolución tecnológica en el concepto de construir y gestionar las redes para contener los servicios de gran demanda en esta actualidad.

ABSTRACT

In our present with registered technological change, the use of internet services are no longer the same, we have an enormous growth and we are not able to accept the TCP / IP standards "as the best effort" where used to associate quality service with reliability.

Nowadays the demand for applications using streaming video, Voice over IP are higher and the companies providing Internet services affected are those experiencing congestion in backbone lines. In this mode the need to deploy a technology that can alleviate this situation is inevitable.

Using the concept of "Traffic Engineering", which is to adapt the traffic flows with the available resources so that there are few overused creating bottlenecks, while others remain sub used causing waste of bandwidth, all using signaling to ensure quality service reserve bandwidth for data streams compatible with RSVP with proper packet classification and planning to meet the specified reserves. This is what promises MPLS (acronym in English Multiprotocol Label Switching) and RSVP (acronym in English Resource Reservation Protocol) as a reliable solution, compatible with all protocols, secure and easy to manage.

Enable tunnel traffic engineering to accelerate packet routing, we can perform this function because MPLS is able to integrate the Level 2 (data link) and 3 (Red), taking full advantage of the best of each (the intelligence of routing with the speed of Switching) MPLS implies a technological evolution in the concept of building and managing networks to hold services in high demand today.

INTRODUCCIÓN

El internet en la actualidad goza de gran aceptación y el crecimiento de usuarios es cada vez mayor, los operadores de servicios de internet aprovechan esta situación para ofrecer nuevos servicios tales como telefonía, videoconferencia televisión y radio. Los mismos requieren volumen de tráfico y calidad de servicio. Se ha hablado mucho en los últimos tiempos de MPLS y RSVP pero su implantación no se ha llevado a cabo, por tal motivo surge la necesidad de simular un esquema donde se aplique esta tecnología y pueda ser comparada con el ruteo tradicional y nos permita evaluar sustancialmente las diferencias.

Cuando nace internet no fue diseñada por sus mentores para trabajar con este contexto de servicios, la cantidad de usuarios conectados ni los niveles de ancho de banda requeridos sus orígenes fueron con fines académicos para el intercambio de MAIL, FTP y HTTP entre las universidades. Esta situación nos lleva a enfocarnos en la problemática actual que llevan los ISP en la congestión de sus líneas de comunicación debido al consumo excesivo de voz y video por parte de los usuarios del servicio. Se hace necesario la implantación de nuevas tecnologías y/o protocolos que permitan un uso equilibrado de los recursos en los enlaces disponibles para satisfacer las necesidades actuales. Esto nos lleva a hablar de ingeniería de tráfico MPLS-TE.

En nuestro trabajo de investigación, en el Capítulo 1 presentaremos el Planteamiento del Problema, a continuación presentamos los objetivos propuestos como metas a alcanzar, en la tercera parte se muestra los Fundamentos Teóricos que nos servirán de sustento, en la cuarta parte se realiza la presentación de nuestro proyecto con la justificación respectiva, Pasamos a continuación con el plan de implantación donde se muestra el análisis, diseño y configuración de los equipos a desplegar. Luego haremos conocer la metodología empleada en nuestro trabajo de investigación. Finalmente exponemos el plan de trabajo, conclusiones y recomendaciones.

1. PLANTEAMIENTO DEL PROBLEMA

SIMULACIÓN DE UN PROTOCOLO SÍNCRONO DE DETECCIÓN LIMITADA POR MEDIO DE LA RESERVACIÓN DE RECURSOS CON MPLS.

1.1. Caracterización del Problema

Un administrador de redes toma en cuenta muchos aspectos al seleccionar un protocolo de enrutamiento. El tamaño de la red, el ancho de banda de los enlaces disponibles, la capacidad de procesamiento de los routers, las marcas, modelos y los protocolos que ya se encuentran en uso en la red son todos factores a considerar a la hora de elegir un protocolo de enrutamiento. Debe hallar las diferencias entre los protocolos de enrutamiento, los cuales serán útiles a la hora de hacer su elección.

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los enrutadores deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, la información de las rutas por donde deben enviar los paquetes, la obtienen de la tabla de enrutamiento de sus vecinos. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico.

Debido al crecimiento explosivo de internet en los últimos años se hace necesario contar con un monitoreo constante del consumo del ancho de banda, así como un

control de la información que deberá fluir por los enlaces de datos optimizar y priorizar la data agregando políticas de calidad de servicio, son decisiones que deben ser tomadas por un administrador de red a fin de garantizar el mejor rendimiento de los servicios de red.

El ruteo tradicional IP confía en las decisiones que toman los protocolos de enrutamiento para el envío de los paquetes es decir, que la decisión de reenvío está basada única y exclusivamente en la dirección IP destino. Todos los paquetes a un mismo destino siguen la misma ruta a través de la red, cualquier modificación en las tablas de ruteo es comunicado a todos los dispositivos que conforman el dominio de enrutamiento, este cambio trae consigo un período de convergencia para que la información sea actualizada a toda la red.

Ante esta situación está claramente expuesto la necesidad de un proceso que sea capaz de cambiar el trayecto sin afectar a los demás dispositivos que conformar el dominio de enrutamiento para llevar a cabo esta situación ya no podemos depender la información contenida en la cabecera IP necesitamos adjuntar etiquetas adicionales al paquete y las decisiones se tomarían en base a esta etiquetas cualquier cambio en el proceso de decisión puede ser llevado a cabo únicamente adjuntado nuevas etiquetas y así no se impactaría ninguno de los dispositivos de enrutamiento que conforman la red. MPLS es una tecnología que modifica el reenvío tradicional de paquetes.

Los ISP con redes basadas en enrutamientos tradicionales TCP/IP no pueden ofrecer garantías de calidad servicio que hoy en día se demandan, las aplicaciones

en tiempo real son un verdadero problema para estas empresas que tienen que solucionar la congestión en sus enlaces en forma oportuna, para no causar impacto negativo a las líneas de comunicación de sus abonados MPLS ha sido una verdadera revolución ya que se presenta como la evolución del sistema tradicional, reduce significativamente el procesamiento de paquetes Su implementación más inmediata está en la gestión del tráfico de red de enlaces troncales, desviar por iniciativa propia el tráfico de rutas congestionadas por otros caminos más despejados, aunque estos no sean la trayectoria más corta, permitiendo poder dedicar a sus abonados determinados enlaces de forma exclusiva para sus servicios a los que se les puede garantizar la calidad de la conexión en cuanto a fluctuación, ancho de banda o retardo.

Para que MPLS pueda desempeñar mejor su función se hace necesario el apoyo del protocolo RSVP (Resource Reservation Protocol). El protocolo RSVP está orientado al control de la red, permitiendo que los programas que se han de ejecutar en Internet puedan obtener niveles óptimos de calidad de servicio que sus flujos de datos requieran. Los paquetes son tratados entre los enrutadores que soportan este protocolo con la información sobre la reserva de recursos que ha de realizarse durante toda la trayectoria que han de seguir, los dispositivos que ejecutan el proceso de RSVP utilizan un conjunto de mensajes con lo que logran su propósito.

1.2. Línea y Sub-línea de Investigación a la que corresponde el Problema

La línea de investigación: Redes de computadoras y telecomunicaciones.

Sub- línea: Protocolos de enrutamiento.

1.3. Palabras Clave

MPLS: Multi-Protocol Label Switching. Intercambio De Etiquetas Multiprotocolares.

RSVP: Resource Reservation Protocol. Protocolo de Reservación de Recursos.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protocolo para Control de Trasmisión/protocolo Inter red.

TE: Traffic Engineering. Ingeniería de tráfico.

2. OBJETIVOS DEL PROYECTO

2.1. Objetivo General

Simular un protocolo de comunicación síncrona bajo el esquema de la conmutación de etiquetas (MPLS) empleando reservación de recursos (RSVP), para mejorar la congestión en sus enlaces, que les permita ofrecer en forma óptima aplicaciones en tiempo real.

2.2. Objetivos Específicos

- Identificar los parámetros relevantes del protocolo simulado que permitan definir la situación ideal, utilizando inteligencia de enrutamiento de capa 3 y la eficiencia de la conmutación de capa 2.
- Identificar los valores óptimos del modelo de simulación para determinar el efecto del protocolo en el desempeño de la redes WAN de los proveedores de servicios de internet comparando los resultados obtenidos.
- Hallar la diferencia en el desempeño de la red con respecto a una topología donde no se usa la reservación de recursos.

- Determinar la información relevante de la cantidad de reservación de recursos y tiempo de transmisión de datos.
- Evaluar la simulación del protocolo síncrono de detección limitada en relación a la cantidad de accesos y retardos al medio de transmisión.

3. FUNDAMENTOS TEÓRICOS

3.1. Antecedentes del proyecto

MPLS es hoy día una solución clásica y estándar al transporte de información en las redes. Aceptado por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando Routing de paquetes con ciertas garantías de entrega.

A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de Conmutación, encabezadas por la tecnología ATM. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red.

De aquí derivan los siguientes problemas: el paradigma del Routing está muy extendido en todos los entornos, tanto empresariales como académicos, etc. El rediseño total del software existente hacia la conmutación supondría un enorme gasto de tiempo y dinero. Igualmente sucede con el hardware que está funcionando hoy día. (Hinojosa & Herrera, 2009).

El enorme crecimiento de la red Internet ha convertido al protocolo **IP (Internet Protocol)** en la base de las actuales redes de telecomunicaciones, contando con más del 80% del tráfico cursado. La versión actual de IP, conocida por IPv4 y recogida en la RFC 791, lleva operativa desde 1980. Este protocolo de capa de red (Nivel 3 OSI), define los mecanismos de la distribución o encaminamiento de paquetes, de una manera no fiable y sin conexión, en redes heterogéneas; es decir, únicamente

está orientado a servicios no orientados a conexión y a la transferencia de datos, por lo que se suele utilizar junto con TCP (Transmission Control Protocol) (Nivel 4 de OSI) para garantizar la entrega de los paquetes.

A mediados de la década de los 90, la demanda por parte de los clientes de los ISP (Internet Service Providers) de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS (Quality of Service) garantizada, propiciaron la introducción de ATM (Asyncronous Transfer Mode) en la capa de enlace (Nivel 2 de OSI) de sus redes. En esos momentos, el modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, utilizando el encaminamiento inteligente de nivel 3 de los "routers" IP en la red de acceso, e incrementando el ancho de banda y rendimiento basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los "switches" ATM en la red troncal. Esta arquitectura, no obstante, presenta ciertas limitaciones, debido a: la dificultad de operar e integrar una red basándose en dos tecnologías muy distintas, la aparición de switches ATM e IP de alto rendimiento en las redes troncales, y la mayor capacidad de transmisión ofrecida por SDH/SONET (Synchronous Digital Hierarchy/Syncronous Optical Network) y DWDM (Dense Wavelength Division Multiplexing) respecto a ATM.

Durante 1996, empezaron a aparecer soluciones de conmutación de nivel 2 propietarias diseñadas para el núcleo de Internet que integraban la conmutación ATM con el encaminamiento IP; como por ejemplo, "Tag Switching" de Cisco o "Aggregate Route-Based IP Switching" de IBM. La base común de todas estas tecnologías, era tomar el software de control de un "router" IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un "switch" ATM y crear un "router" extremadamente rápido y eficiente en cuanto a coste. La integración en esta

arquitectura era mayor, porque se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; pero los protocolos no eran compatibles entre sí y requerían aún de infraestructura ATM.

Finalmente en 1997, el IETF (Internet Engineering Task Force) establece el grupo de trabajo **MPLS (Multi Protocol Label Switching)** para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. El resultado fue la definición en 1998 del estándar conocido por MPLS, recogido en la RFC 3031. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad.

3.2. MPLS

3.1.1. Introducción

En una red IP convencional, los mecanismos de reenvió de los paquetes (forwarding) se basan en que cada nodo de la red examina la cabecera de los paquetes y se decide el siguiente salto (hop by hop) en el camino. Cuando el tamaño de la red incrementa. La primera solución posible es aumentar la capacidad de procesado de los encaminadores pero, como es fácilmente imaginable este aumento de potencia tienen un límite, por lo que es necesario encontrar otro tipo de soluciones que no tengan estas limitaciones. (García Tomas, Raya Cabrera, & Rodrigo Raya, 2002).

En la actualidad la acogida que poseen los dispositivos electrónicos en el ámbito de redes y conexiones personales ha logrado el desarrollo de nuevas tecnologías para el mejoramiento de la comunicación de las mismas. MPLS se ha convertido en una solución clara al trasporte de la información en la red,

ofreciendo nuevos servicios de telecomunicaciones que requieran nodos de conmutación a alta velocidad y que además garanticen la calidad de servicio CoS.

MPLS ha evolucionado desde sus orígenes y las razones para usarlo han cambiado sustancialmente. (Guevara & Cuevas Casado , Nivel de Desempeño en Redes IPv4 con respecto a redes IPv6 con MPLS y RSVP, 2010).

3.1.2. Concepto de MPLS

MPLS o Protocolo Múltiple de Conmutación de Etiquetas es un estándar IP de conmutación de paquetes del IETF y definido en RFC. 3031. Es un mecanismo de conmutación de etiquetas utilizado por switches y routers para el intercambio de tráfico de las mismas.

MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y calidad, realiza una conmutación de paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la calidad de servicio, es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.

En la capa 2 del OSI permite ofrecer servicios multiprotocolos y a su vez ser portable sobre varias tecnologías de capa de enlace como ATM, Frame Relay, líneas dedicadas, LANs.

3.1.3. Arquitectura MPLS

Los elementos MPLS permiten que dicha red funcione más efectivamente que otras tecnologías.

3.2.3.1. LER (Router de Etiqueta de Borde)

Router de Etiqueta de Borde están situados en la periferia las cuales clasifican el tráfico que ingresa al dominio MPLS, conectando un dominio MPLS con los nodos externos de dominio, tienen la función de asignar y retirar las etiquetas (entradas y salidas) y su conmutación se basa en FECs (Forwarding Equivalence Classes). Son conocidos también como nodos PE se comunican o hablan BGP externo y poseen un sistema autónomo.

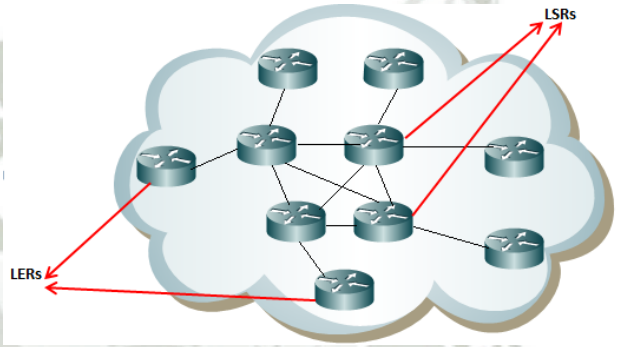

Gráfico N° 1. **LER y LSR**

Fuente: (Barberá, 2000)

3.2.3.2. LSR (Router de Conmutación de Etiquetas)

Router de Conmutación de Etiquetas son los nodos internos de un dominio MPLS los cuales conmutan los paquetes en función a sus etiquetas.

3.2.3.3. FEC (Clase Equivalente de Envío)

Clase de Equivalente de Envío, está constituida por todos los paquetes a los que se puede aplicar una etiqueta específica y gracias a esta la escalabilidad de MPLS está garantizada.

3.2.3.4. LSP (Intercambio de Rutas por Etiquetas)

Intercambio de Rutas por Etiquetas es el camino específico del tráfico a través de la red, sirven como túneles de transporte a lo largo de la red MPLS.

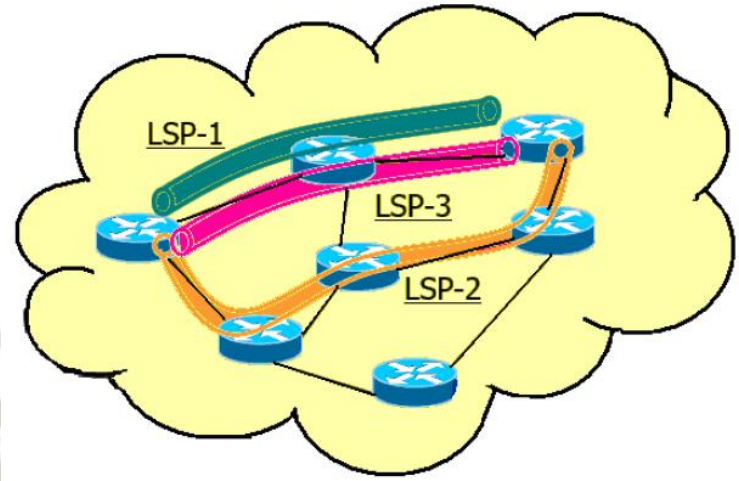

Gráfico Nº 2. **LSP**

Fuente: **(Barberá, 2000)**

3.2.3.5. Etiqueta

Una etiqueta es un identificador pequeño de longitud fija que es usado para identificar un FEC, las mismas solo tienen significado local en cada interfaz tiene dos operaciones:

Label swap: es el cambio de valor de la etiqueta que se realiza en cada nodo.

Label merging: es el cambio de varias etiquetas a una única, que identifica al mismo FEC.

La etiqueta MPLS genérica está conformada por 32 bits dividida en cuatro campos:

- **EXP:** campo reservado para uso experimental, consta de 3 bits.

- **S:** campo de posición de pila de 1 bit, si tiene el valor de 1 indica que es la última etiqueta añadida al paquete IP, si es 0 indica que hay más etiquetas añadidas al paquete.
- **ETIQUETA:** contiene el valor de la etiqueta conformada por 20 bits, esta proporciona la información sobre el protocolo de nivel de red así como información adicional necesaria para reenviar el paquete.

Tabla Nº 1. **Valores Reservados de Etiquetas.**

Etiqueta	Descripción
0	El paquete proviene de una red IPv4
1	Etiqueta alerta de router
2	El paquete proviene de una red IPv6
3	Etiqueta nula implícita
4 – 15	Reservados para uso futuro por la agencia de asignación de números de internet

Fuente: **(Barberá, 2000)**

- **TTL:** time to live, es un campo de 8 bits que se utilizan para codificar el valor de conteo de saltos (IPv6) o de tiempo de vida (IPv4). Para procesar un paquete TTL es necesario considerar que el paquete IP llega al router de entrada al dominio MPLS, se añade una etiqueta de entrada a la pila. Cuando el paquete MPLS llega a los LSR's del núcleo de red el valor TTL es disminuido.

El paquete excluido si llego a cero para evitar lazos o que el paquete permanezca demasiado tiempo en la red. Si el valor es positivo se añade una nueva etiqueta y es reenviado al próximo salto.

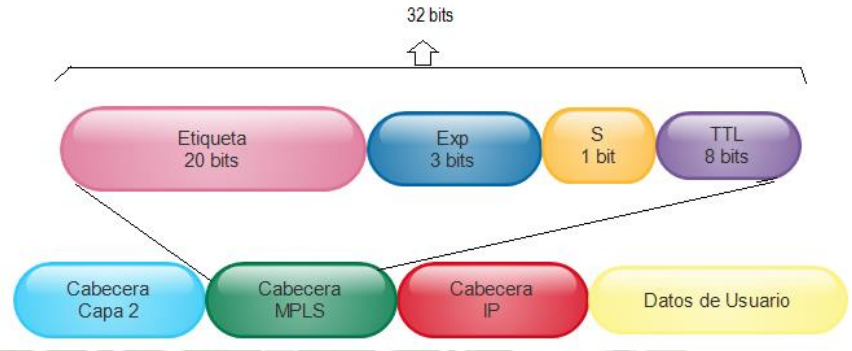

Gráfico Nº 3. **Formato de Etiqueta MPLS – 32bits**

Fuente: (Barberá, 2000)

3.2.3.6. Pila de etiquetas (label Stack)

Un paquete puede etiquetar varias etiquetas según la filosofía LIFO (ultimo en entrar, primero en salir) su proceso no sigue ningún nivel jerárquico, en cualquier LSR se pueden realizar dos operaciones en la pila de etiquetas la push para añadirse y la pop para quitarse. Dicho apilamiento permite crear un túnel, es decir agrupar varios LSP's en uno solo.

3.2.3.7. Encapsulación de Etiquetas

La cabecera de MPLS se encapsula entre la capa "y la capa 3, MPLS función sobre cualquier tipo de protocolo de transporte tales como: PPP (Point to Point Protocol), LAN, ATM; Frame Relay etc.

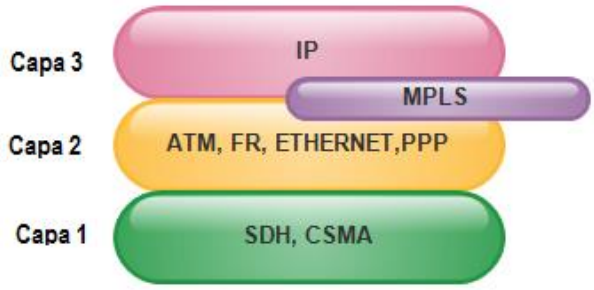

Gráfico Nº 4. **Encapsulación de MPLS**

Fuente**: (Barberá, 2000)**

Si dicho protocolo de transporte contiene un campo para etiquetas entonces se utilizan esos campos para las etiquetas MPLS, si no tiene un campo para etiquetas como PPP se emplea una cabecera genérica MPLS de 32 bits.

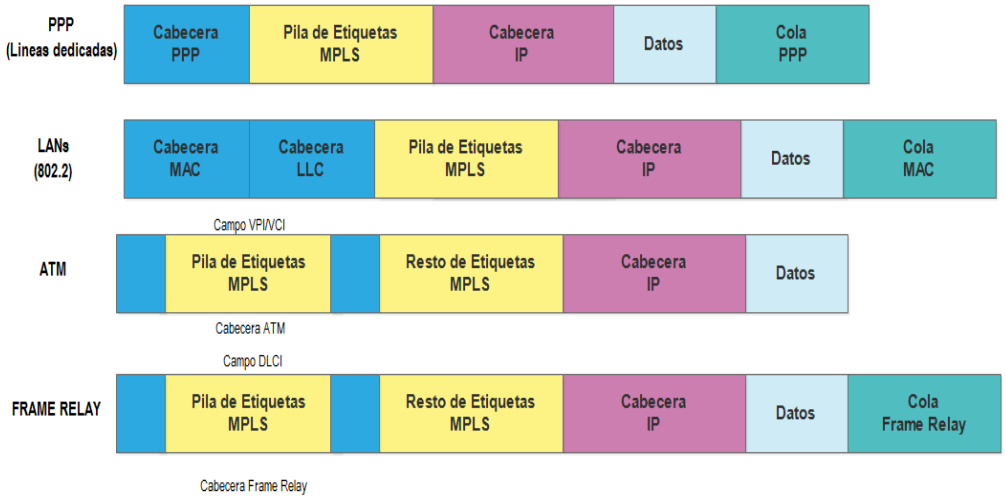

Gráfico Nº 5. **Encapsulación ATM, PPP, IEE 802 y Frame Relay**

Fuente**: (Barberá, 2000)**

3.2.3.8. Tunelización en MPLS

Se crean túneles a través de los routers intermedios para controlar la ruta de un paquete sin especificar los routers intermedios.

MPLS crea túneles a través de los routers intermedios para controlar la ruta de un paquete sin especificar los routers intermedios. Un LSP puede ser un túnel, se utiliza una conmutación de etiquetas.

Un túnel LSP se define como LSP <R1,R2,…Rn>, donde R1 es el punto de transmisión del túnel y añade una etiqueta para el túnel en la pila, el punto de recepción extrae la etiqueta de la pila. (Ojeda & Carrión, Noviembre 2011).

3.1.1. FUNCIONAMIENTO MPLS

El dominio MPLS está conformado por un conjunto de nodos LERs (nodos de acceso) y LSRs (nodos de tránsito), estos son capaces de conmutar y enviar paquetes en base a la etiqueta añadida a cada paquete.

Dichas etiquetas determinan un flujo de paquetes entre dos puntos terminales; este flujo se denomina FE, el mismo que crea un camino particular llamado LSP y contiene los requisitos de calidad de servicio.

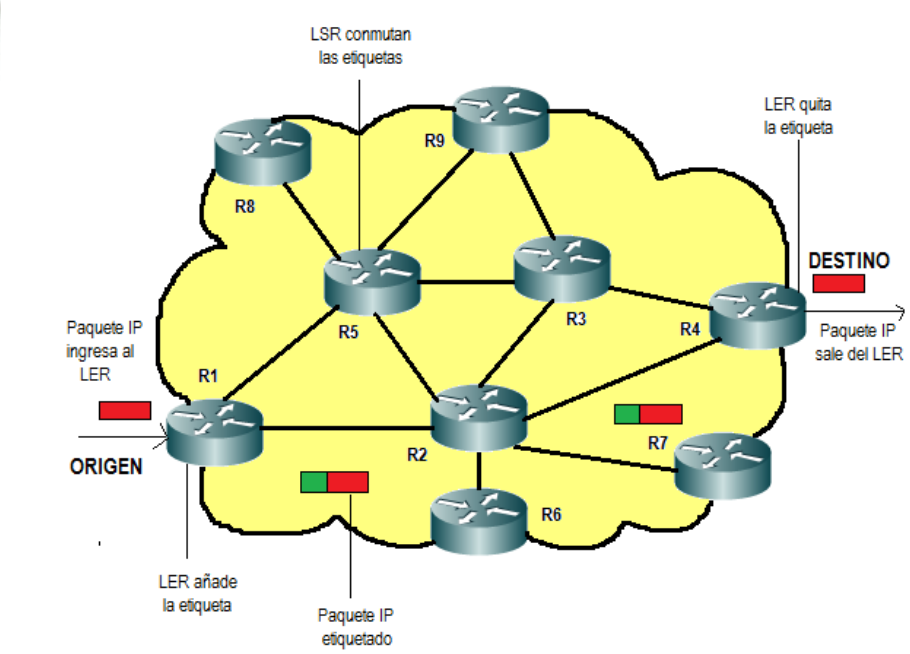

Gráfico Nº 6. **Descripción del Funcionamiento MPLS**

Fuente**: (Barberá, 2000)**

Antes de enviar la información se debe determinar un LSP y establecer los parámetros de calidad de servicio para dicho camino. Los parámetros de QoS sirven para comprobar:

- La cantidad de recursos a reservar al LSP.
- Las políticas de descarte de paquetes y prioridades en colas en cada LSR.

Para lograr lo mencionado anteriormente se utilizan dos protocolos para el intercambio de información entre los routers:

- El protocolo OSPF es utilizado para intercambiar información sobre la topología, y el enrutamiento en sí.
- Para determinar los LSPs y establecer las etiquetas entre los siguientes LSRs se puede utilizar el protocolo LDP (*Label Distribution Protocol*) o el protocolo RSVP-TE (*Resource Reservation Protocol Traffic Engineering*), también se lo puede realizar manualmente.

Un paquete ingresa al dominio MPLS a través de un router de acceso (LER), este router determina los parámetros de QoS, le asigna un FEC específico al paquete el cual determina un LSP, se etiqueta y se envía el paquete.

Si no existe un LSP para este FEC, el LER junto con los otros routers definen un nuevo LSP. El administrador de red para determinar un FEC debe considerar uno o varios de los siguientes parámetros:

- Direcciones IP de origen o destino y/o direcciones IP de la red.
- Número de puerto de origen o destino.

- Punto de código de servicios diferenciados.
- ID del protocolo IP.
- Flujo de etiquetas IPv6.

El paquete enviado por el LER es recibido por un router de tránsito (LSR), en este momento el paquete se encuentra dentro del dominio MPLS.

El LSR realiza las siguientes funciones:

- Desecha la etiqueta del paquete entrante y añade una nueva etiqueta al paquete saliente.
- Envía el paquete al próximo LSR dentro del LSP.
- El LER de salida desecha la etiqueta, lee la cabecera del paquete IP y envía el paquete a su destino final.

3.1.2. APLICACIONES

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico.
- Diferenciación de niveles de servicio mediante clases (CoS).
- Servicio de redes privadas virtuales (VPN).

3.1.2.1. Ingeniería de Tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera de evitar que un subconjunto (enlaces, equipos...) de la red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, mejorando el rendimiento de la red global. (Braden, R;1994).

Los flujos de tráfico siguen el camino más corto calculado por el algoritmo **IGP** correspondiente. En casos de congestión de algunos enlaces, el problema se resolverá teniendo más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo **IGP** sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

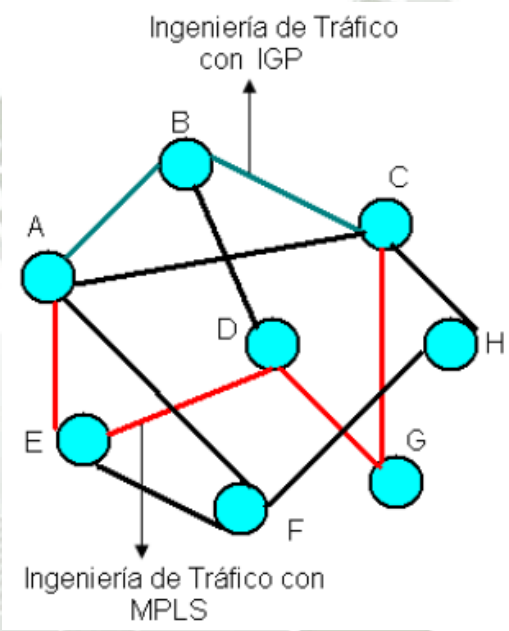

Gráfico Nº 7. **Ingeniería de Tráfico MPLS vs IGP**

Fuente**: (Braden , 1994)**

Se observa que la ruta más corta AC utilizando IGP (métricas) necesita de dos saltos, pero si hay exceso de tráfico por esta ruta, MPLS da otra.

La alternativa de ruta con cuatro saltos. Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un **LSP**. (Braden , 1994).

Permite obtener estadísticas de uso **LSP**, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos

de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

Permite hacer "enrutamiento restringido" (Constraint-based Routing, **CBR**), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad).

La ventaja de la ingeniería de tráfico **MPLS** es que se puede hacer directamente sobre una red **IP**, al margen de que haya o no una infraestructura **ATM** por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

3.1.2.2. Calidad de Servicio

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del **IETF**. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. (Braden , 1994).

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas **MPLS** tienen el campo **EXP** para poder propagar la clase de servicio **CoS** en el correspondiente **LSP**.

De este modo, una red **MPLS** puede transportar distintas clases de tráfico, ya que:

El tráfico que fluye a través de un determinado **LSP** se puede asignar a diferentes colas de salida en los diferentes saltos **LSR**, de acuerdo con la información contenida en los bits del campo **EXP**.

Entre cada par de **LSR** exteriores se pueden provisionar múltiples **LSPs**, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda (i.e. un **LSP** puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort).

3.1.2.3. Redes Virtuales Privadas

Una red privada virtual (**VPN**) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las **VPNs** es el soporte de aplicaciones intranet/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces.

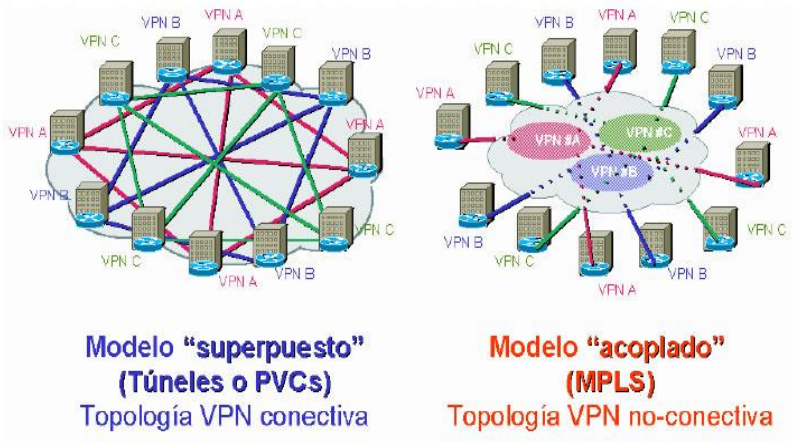

Gráfico Nº 8. **Ingeniería de Trafico MPLS vs IGP**

Fuente**: (Braden , 1994)**

En el gráfico N° 8 se presenta una comparación entre el modelo de túneles de **IPSec** (**PVCs**) y el modelo de **LSPs** de **MPLS**. La diferencia entre los túneles **IP** convencionales (o los circuitos virtuales) y los "túneles **MPLS**" (**LSPs**) está en que éstos se crean dentro de la red, basados en **LSPs**, y no de extremo a extremo a través de la red.

Resumiendo, las ventajas que **MPLS** ofrece para **IP VPNs** son:

- Proporcionar un modelo "acoplado" o "inteligente", ya que la red **MPLS** conoce de la existencia de **VPNs** (lo que no ocurre con túneles ni **PVCs**).
- Evita la complejidad de los túneles y **PVCs**.
- Provee de un servicio sencillo: una nueva conexión afecta a un solo enrutador y tiene mayores opciones de crecimiento modular.
- Permite mantener garantías **QoS** extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el

campo **EXP** de las etiquetas **MPLS** con las clases definidas a la entrada.

- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación, etc.), lo que es necesario para un servicio completo **VPN**.

3.1.3. IMPLEMENTACIONES DE MPLS

Una vez visto el concepto de MPLS, veamos los distintos tipos de implementaciones actuales, en concreto: MPLS como una solución IP sobre Ethernet, IP sobre ATM, e IP sobre Frame Relay. No se contempla la aplicación de MPLS a las redes ópticas de próxima generación, conocida como GMPLS (Generalized MPLS), por encontrarse aún en proceso de estudio y estandarización por parte del IETF. GMPLS es una extensión natural de MPLS para ampliar el uso de MPLS como un mecanismo de control y provisión, no únicamente de caminos en dispositivos basados en paquetes, sino también de caminos en dispositivos no basados en paquetes; como los conmutadores ópticos de señales multiplexadas por división en longitud de onda, los conmutadores de fibras ópticas, y los conmutadores de señales digitales multiplexadas por división en el tiempo.3333 (Blake , diciembre de 1998).

La implementación de MPLS como una **solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet**, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, en este caso, la etiqueta MPLS está ubicada después de la cabecera de nivel 2 y antes de la cabecera

IP. Los LSR saben cómo conmutar utilizando la etiqueta MPLS en vez de utilizar la cabecera IP. El funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad. Estas limitaciones propiciaron el desarrollo de la siguiente generación del protocolo Internet o IPv6, definido en la RFC 1883. La versión IPv6 puede ser instalada como una actualización del software en los dispositivos de red de Internet e interoperar con la versión actual IPv4, produciéndose esta migración progresivamente durante los próximos años. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6, estando su uso descrito en la RFC 1809. (Blake , diciembre de 1998).

La implementación de MPLS como una **solución IP sobre ATM** también está muy extendida. Primeramente indicar, que MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de "switches" ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (Private Network to Network Interface). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM, puesto que LDP entiende y utiliza direcciones IP y los protocolos de encaminamiento utilizados en las redes

MPLS son los mismos que los utilizados en las redes IP. En este caso, descrito en la RFC 3035, la etiqueta es el valor del VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) de la cabecera de la celda ATM.

Finalmente, MPLS también se ha desarrollado como una **solución IP sobre Frame Relay**. En este caso, descrito en la RFC 3034, la etiqueta es el DLCI (Data Link Control Identifier) de la cabecera Frame Relay. (Blake , diciembre de 1998).

3.1.4. BENEFICIOS DE MPLS

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3 a través de la conmutación por etiqueta, pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering), cursar tráfico con diferentes calidades de clases de servicio o CoS (Class of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir,

se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, descrita en la RFC 2702, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red. (Blake , diciembre de 1998).

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá

conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPNs mediante MPLS, pero la mayoría se basan en la RFC 2547. (Blake , diciembre de 1998).

3.4. Reservación de recursos

El Protocolo de Reserva de Recursos (Resource Reservation Protocol, RSVP) es el protocolo diseñado por ISA para trabajar con cualquier servicio IS.

RSVP se utiliza por el nodo extremo para solicitar a la red QoS para un flujo o conjunto de flujos, y por los nodos intermedios para entregar las solicitudes de QoS al resto de los nodos de la ruta de datos, y para establecer y mantener el estado del servicio solicitado.

RSVP opera sobre el protocolo IP (IPv4 o IPv6), el cual no permite realizar reserva de recursos y establecer un circuito virtual simultáneamente. De modo que, los mensajes RSVP se envían en paralelo con los paquetes IP. Pero RSVP no es un protocolo de transporte ni un protocolo de encaminamiento, más bien está diseñado para funcionar sobre cualquier protocolo de encaminamiento ya sea la unidifusión (unicasting) o multidifusión (multicasting). El protocolo de encaminamiento mandará sus mensajes a cada destino y a continuación mandará los mensajes RSVP para reservar los recursos a lo largo de la(s) ruta(s). Así, pues el protocolo de encaminamiento es el que determina dónde se envían los paquetes y RSVP determina la QoS de estos paquetes según las rutas.

RSVP requiere reservar recursos en cada nodo a lo largo de la ruta de datos. Las solicitudes de reserva RSVP son simplex, es decir, las reservas se hacen en una dirección. Además, RSVP distingue entre emisor y receptor, de modo que una misma aplicación puede actuar tanto como emisor o receptor.

RSVP asume que necesitará reservar recursos para diversas aplicaciones, ya que los receptores de estas transmisiones son muchos, diferentes y heterogéneos, por lo que no tiene sentido reservar recursos al establecer la conexión y así hace responsable a los receptores de realizar la solicitud de QoS. La solicitud RSVP del receptor pasa al proceso RSVP local. El proceso RSVP pasa la solicitud a todos los nodos a lo largo de la(s) ruta(s) de datos en orden inverso hasta alcanzar el origen.

Durante la ejecución de la reserva, la solicitud pasa por los componentes ISA Control de Admisión y Control del Sistema. Si ambos controles se pasan con éxito, es el componente ISA Clasificador de Paquetes quien establece la QoS deseada. En caso contrario, se envía un mensaje de error a la aplicación que solicito la reserva. (García Tomas, Raya Cabrera, & Rodrigo Raya, 2002).

Las carencias de Internet son una realidad patente a medida que su uso se incrementa y se trata de exprimir todas sus posibilidades. Una evidencia que sufren en mayor medida los responsables de red y proveedores de servicio que se las ven y se las desean para que sus sistemas puedan asumir un tráfico cada vez más intenso y complejo que generan unos usuarios insaciables de recursos (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

En los comienzos de Internet, se primó en su diseño la funcionalidad y conectividad frente a cualquier otra consideración. Importaba y se buscaba lograr conectar. Nadie, a principio de los años setenta, podía imaginar el escenario actual de La Red sin que le tomaran por un visionario desquiciado. Si esta premisa de conexión a toda costa provocó que Internet haya crecido y siga creciendo, a ritmo vertiginoso, también ha traído consigo otros problemas y limitaciones que lastran profundamente su actual e inevitable evolución y frente a ellos, la industria trata de dar la respuesta oportuna para poder implementar una verdadera red global sin

cortapisas en seguridad, direccionamiento, rendimiento y capacidad (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

En cuanto a rendimiento y capacidad, las empresas que mantienen líneas de negocio en Internet necesitan disponer de un soporte de red que responda con un servicio siempre en condiciones fiables que garantice a sus clientes disponibilidad, comodidad y variedad de servicios. Otro tanto les ocurrirá a aquellas otras organizaciones, en las que las facilidades de conexión de Internet pueden hacer muy atractivos el teletrabajo o el trabajo en equipo con miembros muy dispersos geográficamente, pero siempre y cuando tengan resuelta la necesaria operatividad de los recursos necesarios (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Estos escenarios y servicios, tomados a modo de ejemplo, no resultan ya de ciencia ficción y la presión de su demanda choca frontalmente con la tecnología actualmente desplegada en La Red que no es capaz de asumirla en óptimas condiciones. El tráfico de paquetes que hoy viaja por Internet se basa en ser procesado en cuanto sea posible, según las circunstancias de la red, sin ninguna garantía sobre el propio proceso, ni cuándo tendrán lugar ese tratamiento. La tecnología que gira en torno a Ipv4, por diseño, no es capaz de asimilar ni responder a las expectativas que hoy por hoy se han generado en la red de redes (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Así surge RSVP (Reservation Protocol), protocolo de reservación de recursos, un protocolo de control de la red que permite que los programas que van a trabajar en Internet puedan obtener la calidad de servicio que sus flujos de datos puedan requerir. Se trata de un protocolo totalmente emergente que se encuentra aún en fase de normalización por parte del IETF, que está desarrollando su estandarización partiendo de los trabajos iniciales que se realizaron en la Universidad del Sur de

California con la participación de Xerox, en donde fue concebido (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Este protocolo no es, en contra de lo que pudiera parecer, un protocolo de enrutamiento. Es un protocolo que se inscribe dentro de la capa de Transporte del modelo de conectividad OSI y se apoya en las tablas de rutas dinámicas que manejan los protocolos de enrutado clásicos para establecer una conexión a modo de circuito virtual entre emisor y receptor o receptores implicados. Para RSVP el flujo de datos es simplemente una secuencia de paquetes que tienen un mismo origen, uno o varios destinos, según sea la difusión, unicast o multicast, y una calidad de servicio, todo ello caracterizado mediante sesiones. Una sesión RSVP es cada torrente de datos que el protocolo maneja de forma independiente (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Las especificaciones de operación de este protocolo se materializan en un programa, en un dominio, RSVP estructurado en módulos, cada uno de ellos con unas funciones específicas. Por una parte están el módulo de Control de Admisión y el módulo de Control de Política. El primero se encarga de determinar si el nodo tiene los recursos solicitados disponibles para soportar la calidad de Servicio pedida. El Control de Política determina si el solicitante tiene los permisos necesarios para poder disponer de los recursos que solicita. En otro lado se encuentra el motor de la reserva, el módulo de Clasificación, encargado de recepcionar los paquetes para determinar su ruta y QoS necesaria y el módulo Esquemático, al que se le encomienda la transmisión de los paquetes (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

El host, en donde se ejecuta la aplicación que genera el tráfico en la red, inicia una sesión con el router con capacidad RSVP, especificando la dirección de destino,

el identificador de protocolo y puerto a utilizar. Si recibe respuesta, obtiene un identificador de sesión que marcará el camino que seguirán los paquetes que genere el programa. Cuando se activa la sesión, cuando los paquetes son enviados, el router recibirá, junto a ellos, mensajes RSVP en donde se especifican la reserva de recursos que ha de realizar a lo largo de toda la trayectoria. (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

El dominio RSVP recepciona los paquetes y los clasifica, encolándolos según criterios temporales. Se les asigna ruta, Calidad de Servicio y en función del temporizador se colocan en el interface del router adecuado. Si la capa de enlace del puerto seleccionado tiene su propia gestión de QoS, el programa del protocolo de reservación, negociará con él la obtención de la Calidad de Servicio requerida. Si no dispone de esta capacidad, es el propio programa quien puede encargarse de reservar la capacidad necesaria para la transmisión, pudiéndose ocupar no sólo de los parámetros que afecten a la línea de comunicación, si no que puede abarcar CPU y almacenamiento (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

El inicio del proceso de reservación de este protocolo comienza realmente cuando el programa consulta a los protocolos de enrutado local las rutas que ha de utilizar. En cada salto, en cada nodo del camino, el programa RSVP local tiene que aplicar el mismo procedimiento, es decir, calcular si puede ofrecer la Calidad de Servicio que le han solicitado. Si este Control de Admisión y Control de Política es satisfactorio, el nodo local clasifica y encola los paquetes para darles la QoS que requieren. Si no le es posible proporcionar los recursos que le han sido pedidos, la aplicación que originó el flujo de datos recibirá una indicación de error (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

En el contexto de operación de RSVP, la distribución de datos puede hacerse por difusión en unicast en donde sólo hay un emisor y un receptor o por multicast, en cuyo caso hay un emisor y varios receptores. El flujo de datos que se maneja en una sesión de este protocolo siempre tiene un solo emisor y los paquetes de cada sesión en particular irán dirigidos a la misma dirección IP y a un puerto. Si hay difusión multicast, la dirección IP será la dirección del grupo. Si para este protocolo cada emisor y receptor debe corresponderse con un host único, no hay inconveniente para que un mismo host pueda contener varios emisores o receptores lógicos que se identifiquen por los puertos (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

En lo que respecta a QoS, los requerimientos que pueda necesitar la aplicación se definen mediante la especificación del flujo de datos, que es la estructura de datos utilizada por los hosts para solicitar servicios especiales a la red. Mediante un atributo que va incorporado en los mensajes con los que se relacionan RSVP y los programas, se determina de qué forma han de intercambiar datos los actores de la transmisión. Así, el host utiliza su parte RSVP para solicitar el nivel de Calidad de Servicio que necesita para cada ráfaga de datos. El router utiliza su parte de protocolo para propagar esas necesidades a los otros encaminadores de la ruta a seguir (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Para que los programas puedan interactuar con este protocolo están definidas las RAPI, RSVP Aplication Programming Interface, que proporciona a las aplicaciones los mecanismos que pueden necesitar para comunicar con el dominio RSVP y obtener la reserva de recursos que vayan a necesitar a lo largo de toda la trayectoria de la conexión. Esta herramienta permite que las aplicaciones no tengan que ser

nuevamente diseñadas ni reescritas para integrarse en este modo de trabajo (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

Aunque el diseño del protocolo está orientado a la multidifusión, no desmerece las reservas que puede realizar para aplicaciones de unidifusión, pero es en el primer tipo de transmisión en donde se saca mejor partido al protocolo. El mayor potencial que ofrece es la forma con la puede asumir los grupos de difusión ya que al estar determinada la reserva de los recursos por el receptor, no es necesario que éste tenga que acudir al origen para obtenerla, basta con que acuda a la rama que le corresponda. Esto se debe a que el flujo del tráfico de red depende inicialmente de que el emisor pueda conectar con el receptor para que pueda establecerse el circuito virtual y a partir de ahí, el tráfico se va ramificando en cada nodo para que los paquetes puedan llegar a sus destinatarios. A modo de árbol invertido, el emisor se corresponde con la raíz, los nodos en las ramas y los host destinatarios en las hojas. El tráfico fluye de arriba hacia abajo (Cuevas Casado , 2006) (Leon-Garcia & Widjaja, 2001).

4. PRESENTACIÓN DEL PROYECTO

4.1. Justificación

Se ha hablado mucho de MPLS en los últimos tiempos pero hasta ahora son muy pocas las empresas que han decidido adoptar esta nueva tecnología como un proyecto a mediano o largo plazo, la justificación de este proyecto de investigación está centrado en ofrecer un panorama amplio de las ventajas que nos ofrece la conmutación por etiquetas frente al ruteo por direcciones IP, despejar dudas y mitos sobre la eficiencia cuando hablamos de Ingeniería de tráfico y reservación de recursos en los enlaces de datos.

Los proveedores de servicios de internet se enfrentan día a día a congestionamiento en sus líneas de comunicaciones, la internet ya no es la misma, viene evolucionando y son más los servicios que se pueden brindar hoy en día, sus abonados acogen estas nuevas aplicaciones y las incorporan dentro del sus planes de mejora continua, en este mundo globalizado las videoconferencias, entre sucursales o con proveedores (Nacionales o internacionales) son cada vez mayor y demandan un alto consumo de acho de banda, del mismo modo presentan las comunicaciones de voz sobre IP que un pueden esperar al acuse de recibo o peor aún al reenvió del paquete perdido, se necesitan una transferencia fluida de datos sin interrupciones.

Ante lo expuesto se hace necesario profundizar los estudios en la aplicación de esta nueva tecnología de computación de etiquetas y reservación de recursos, para obtener los parámetros más relevantes y comparar los resultados recopilados frente al esquema actual de enrutamiento, dentro de un ambiente de laboratorio donde podamos efectuar las respectivas pruebas de stress a las que serán sometidas las líneas de comunicaciones en un ambiente real.

Así es cómo surge nuestra idea de dar solución al problema de congestionamiento actual que se tiene en las horas pico de tráfico en las líneas de internet, la tecnología está a nuestro alcance, solo nos resta hacer uso de ella para satisfacer nuestras necesidades crecientes de ancho de banda y calidad de servicio.

4.2. Resumen del Proyecto

SIMULACION DE UN PROTOCOLO SINCRONO DE DETECCION LIMITADA POR MEDIO DE LA RESERVACION DE RECURSOS CON MPLS.

4.2.1. Descripción del proyecto a medio y largo plazo

Con la simulación de este proyecto de investigación pretendemos despejar dudas, tomar medición de la mejora de la introducción de MPLS-TE y RSVP dentro de un direccionamiento IPV6, y contrastarlo con el enrutamiento tradicional para poder analizar los tiempos de mejora de esta tecnología.

Simular un protocolo de comunicación síncrona bajo el esquema de la conmutación de etiquetas (MPLS) empleando reservación de recursos (RSVP), para mejorar sustancialmente las líneas de comunicación de los proveedores de servicios de internet (ISP), permitiendo ofrecer mejores servicios a sus abonados.

Aplicado el protocolo de comunicación síncrona se espera obtener elementos que permitan reducir la latencia del de enrutamiento entre los dispositivos de capa 3 del modelo de referencia OSI.

El presente trabajo de investigación permite profundidad en el tema de la definición de un protocolo síncrono empleando MPLS. El hecho de emplear la reservación de recursos permite reducir los tiempos de transmisión de información.

Los inconvenientes que se pueden encontrar es que no se aplica el mismo algoritmo para un protocolo de comunicación síncrona sin reservación de recursos, ante este inconveniente, es necesario elaborar un proceso de simulación que permita una comparación adecuada y obtener las diferencias sustanciales en tiempo de comunicación.

4.2.2. Usuarios del Proyecto

Nuestro estudio está enfocado a las empresas de comunicaciones ISP, quienes sufren la congestión en sus líneas de comunicaciones ante las deficiencias del

enrutamiento tradicional, con la aplicación de los avances de MPLS-TE lograran obtener una mejora sustancial en la transmisión de datos.

4.2.3. Beneficios

Esta tecnología permite mejora notalmente las líneas de backbone de los ISP para soportar y ofrecer servicios de gran demanda y garantizar un control de calidad así mismo pretende ilustrar las mejoras del IPV6.Dentro de los beneficios sustanciales que ofrece nuestro proyecto son:

- Ingeniería de tráfico
- Fast reroute
- Balanceo de cargas

4.2.4. Localización

La localización de este caso de estudio está localizado en la red corporativa de los ISP, donde se encuentran operando sus enrutadores, en estos dispositivos el equipo humano deberá realizar las configuraciones necesarias para la migración a la tecnología MPLS-TE y RSPV.

4.2.5. Impacto y sostenibilidad del Proyecto:

Como hemos venido explicando esta tecnología aporta beneficios en la trasferencia de datos especialmente enfocado a la trasmisión de video, voz sobre IP, video conferencia, al aprovechar los beneficios de la conmutación de paquetes con la inteligencia del enrutamiento.

Como aporte tenemos la simulación realizada en paralelo para el ruteo tradicional y el ruteo con la conmutación de etiquetas, donde se pudo efectuar las pruebas de stress respectivas.

La repercusión luego de esta implantación es favorable para las empresas proveedoras de servicios de internet quienes tendrán descongestión en sus enlaces saturados, un mejor rendimiento en sus líneas sub utilizadas y podrán ofrecer mejores servicios a sus abonados.

4.2.6. Riesgos que debemos afrontar

• Económicos: Los dispositivos tales como enrutadores ya cuentan en la actualidad con el soporte para IPV6, Rsvp y MPLS-Ten por tal motivo la introducción de esta tecnología no representa un costo directo en adquisición de nuevos equipos, pero si podríamos suponer de un gasto indirecto en la capacitación y/o contratación de mano de obra califica para implantar esta tecnología y brindar el mantenimiento debido.

• Competencia: MPLS no es una tecnología nueva ya tiene varios años desde su publicación en el RFC-3031 en 2001, es una arquitectura segura, confiable, escalabre y fácil de administrar los dispositivos tales como enrutadores ya cuentan en su IOS soporte para MPLS.

• Tecnológicos: Cuando hablamos de esta nueva tecnología estamos garantizando completamente su compatibilidad con los protocolos de enrutamiento, direccionamiento IPV4 total aceptación con IPV6 y está diseñado para soportar nuevos servicios.

• No tecnológicos: El trabajo de investigación no contempla a aquellos esquemas como la falta de reservación de recursos ni a los protocolos de comunicación no síncronos y solo se encuentra diseñada a una red síncrona con RSVP y MPLS.

5. PLAN DE IMPLANTACIÓN DEL PROYECTO.

5.1. Definición del Proyecto

Realizar la simulación para la puesta en marcha de los protocolos MPLS y RSVP que nos permita aplicar ingeniería de tráfico MPLS-TE, pruebas que se llevaran paralelo con un modelo de enrutamiento tradicional, comparar e interpretar los resultados obtenidos durante las pruebas de recopilación de información.

5.1.1. Aspectos Técnicos:

La tecnología a aplicar en este proyecto de investigación es MPLS(*Multiprotocol Label Switching*) quien no sólo suministra una mayor fiabilidad y superior rendimiento en la red sino también nos brinda Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz que nos permite proporcionar la solución idónea para efectuar las llamadas voz sobre IP y transmisión de video esto de la mano con el protocolo RSVP (siglas de Resource Reservation Protocol) para brindar las reservas necesarias que nos permita brindar calidad de servicio.

5.1.2. Aspectos Económicos:

En nuestro trabajo de investigación se ha considerado un análisis económico para cada uno de los beneficios que se obtendrá del mismo, como son los equipos que soportan dichas tecnologías así como también la inversión que la empresa hará en capacitaciones al personal para el manejo de equipos usando el protocolo síncrono con los beneficios de la tecnología MPLS.

Viendo la relación beneficio-costo de nuestro proyecto la inversión asciende a la suma S/. 3000.00 nuevos soles, para la capacitación personalizada a cada uno de los ingenieros de soporte en las instalaciones de la organización.

5.1.3. Aspectos Comerciales:

Dentro de los aspectos comerciales es su grato interés, para aquellas empresas comercializadoras de servicios de internet quienes se beneficiarán de las mejoras de este protocolo tales como el descongestionamiento de sus líneas de Backbone la capacidad de poder atender con mayor eficiencia las demanda de transmisión de voz y video por parte de sus abonados.

5.1.4. Recursos del Proyecto:

La implantación de este proyecto con incurre en gastos directos para la organización, puesto que los equipos que se dispone en el mercado y sus antecesores ya cuentan con el soporte para este tecnología, MPLS y RSVP nos es nuevo en el mercado pero su puesta en marcha aún está rezagada por algunas compañías, debemos contemplar la posibilidad de capacitar al personal existente para configuración de los dispositivos o contratar mano de obra especializada para este fin.

6. METODOLOGIA A EMPLEAR

Para la implantación de este proyecto de investigación utilizaremos una metodología estructural para garantizar el desarrollo y puesta en marcha del enrutamiento basado en

la conmutación de etiquetas proporcionando puntos de control y revisión. Teniendo en cuenta los siguientes puntos:

- **Adecuación**: El sistema debe permitir la completa satisfacción de las expectativas de los ISP.
- **Mantenibilidad:** Facilidad para realizar cambios, mejora continua del servicio esto una vez que se encuentre en producción en la empresa del cliente.
- **Usabilidad:** Es el grado de dificultad en adquirir las habilidades y destrezas por parte del personal responsable de la gestión de los equipos.
- **Fiabilidad:** Es la capacidad de la introducción de estas nuevas configuración en los equipos pueda funcionar correctamente durante un intervalo de tiempo. Prestando suma importancia sobre todo:

  MTBF: Mean Time Between Failures (Tiempo medio entre fallos).

  Disponibilidad: Probabilidad de que el sistema esté funcionando en un instante dado.
- **Eficiencia:** los protocolos MPLS-TE y RSVP El están en la capacidad de realizar su prometido con el mínimo consumo de recursos de hardware sin decaer el performance de las líneas de backbone.

a) Análisis: Estudio de viabilidad; Definición de requisitos; Modelado funcional; Modelado estructural; Modelado dinámico; Procesos de análisis.

Nuestro estudio está enfocado a satisfacer las demandas crecientes de ancho de banda, calidad de servicio de los ISP para que puedan pueda brindar un mejor servicio a sus abonados en enrutamiento tradicional basado en la filosofía de mejor esfuerzo ya no se adecua a los cambios actuales de la internet, con la introducción de ingeniería de tráfico y reserva de recursos estarán en la capacidad de sacar el máximo provecho de sus enlaces

de datos, mejor uso de sus líneas sub utilizadas, permitir un enrutamiento rápido en caso de fallas y la factibilidad de contar la posibilidad de manejar balanceo de cargas en sus enlaces de datos.

En la actualidad los equipos, no solo los de última generación ya cuentan con soporte para MPLS-TE y RSVP, del mismo se dispone amplia información sobre los alcances de estos protocolos tratados en el presente caso de estudio, que permite despejar dudas al personal involucrado en la implantación y/o mantenimiento de los equipos de comunicaciones.

b) Diseño: Para efectos de recreación de nuestro escenario se hará uso de la herramienta de simulación GNS3, quien nos permitirá recrear con exactitud y precesión el estado actual del enrutamiento y estado de las enlaces (LAN Y WAN), realizaremos las pruebas simulando la red corporativa del proveedor utilizando el enrutamiento tradicional para brindar conectividad a tres abonados, aplicaremos los protocolos MPLS y RSVP junto con Ingerirá de Trafico para brindar un servicio de Premium a uno de los abonados.

Se tomaran las muestras para su análisis respectivo a fin de detectar cuellos de botellas, mejora en el servicio y valores que se pueden ajustar para obtener el máximo rendimiento de la red.

- **Condiciones del protocolo síncrono**

  En primer lugar se definen las condiciones para que el protocolo propuesto logre su cometido. Estas condiciones son las siguientes:

  - Se asume que se trabaja con ranura de tiempo.

  Se condiciona que las estaciones de trabajo envían requerimientos de transmisión.

- Cada estación de trabajo envía un paquete de datos por cada ranura de tiempo.
- Existe una realimentación de la estación base al final de cada ranura.
- El retardo de propagación es cero.
- El canal se encuentra libre de errores.
- Para transmitir la información, las estaciones compiten por turnos.
- Cada estación transmite sus datos en la fase DTP.
- Durante la reservación de recursos, cuando las estaciones de trabajo deseen transmitir información, estas la hacen por cada ranura asignada.
- Si una estación de trabajo deja de transmitir, entonces pierde la respectiva ranura asignada.
- Las tramas, donde se encuentra la información a transmitir, no presentan la misma longitud.
- Cada estación de trabajo reconoce el número de la ranura asignada y asigna una variable donde mantiene información de la trama, y su contenido, que va a transmitir.

6.1. Diseño de Red

Para que una LAN sea segura confiable escalable y fácil de administrar se debe diseñar e implementar de acuerdo con una serie de pasos sistemáticos que satisfaga las necesidades de los usuarios.

El paso final en la metodología de diseño LAN es plasmar toda la documentación física y lógica de la red. La topología física de la red se refiere a la forma en que distintos componentes de LAN se conectan entre sí. El bosquejo lógico de la red se refiere al flujo de datos que hay dentro de una red. También se refiere a los croquis de nombre y dirección que se utilizan en la implementación de la solución de diseño

LAN. Para un buen entendimiento de la estructura con la cual estamos trabajando necesitamos confeccionar el mapa lógico, mapa de direcciones y el cuadro de direccionamiento, como según se detalla:

A continuación mostramos el diseño lógico de la red.

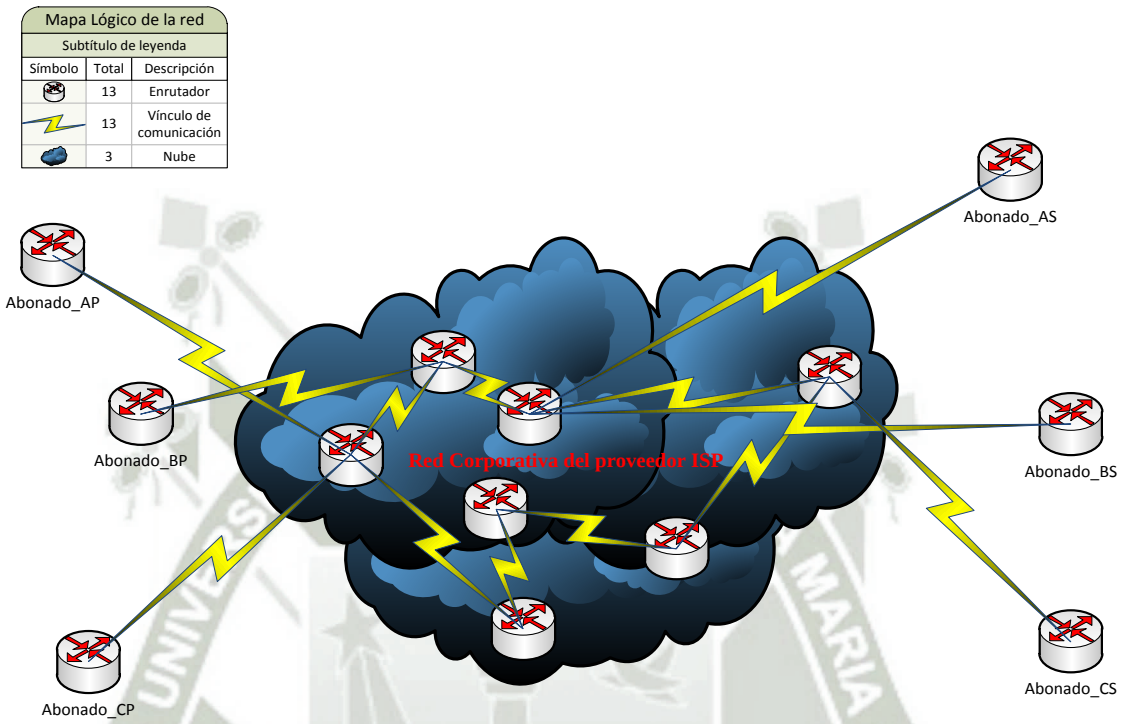

Gráfico Nº 9. **Diseño Lógico de la Red Simulada**

Fuente**: Elaboración propia**

Detallamos a continuación plan de direccionamiento utilizado en nuestro trabajo de simulación.

Tabla Nº 2. **Cuadro de direcciones IPv6 desplegable en los túneles VPN**

Cuadro de direcciones IPV6 desplegadas en los túneles VPN								
Dirección Inicio		Dirección Final	Numero de Bits	Host Disponibles	Interface	Principal	Sede	Nombre y número de agencia
2001:CCCC:AAAA::0	-	2001:CCCC:AAAA::3	126	2	tunel 0	2001:CCCC:AAAA::1/126	2001:CCCC:AAAA::2/126	Abonado_AP-Abonado_AS
2001:CCCC:AAAA::4	-	2001:CCCC:AAAA::7	126	2	tunel 1	2001:CCCC:AAAA::5/126	2001:CCCC:AAAA::6/126	Abonado_BP-Abonado_BS
2001:CCCC:AAAA::8	-	2001:CCCC:AAAA::B	126	2	tunel 2	2001:CCCC:AAAA::9/126	2001:CCCC:AAAA::A/126	Abonado_CP-Abonado_CS
2001:CCCC:AAAA::C	-	2001:CCCC:AAAA::F	126	2	tunel 3			Disponible
2001:CCCC:AAAA::10	-	2001:CCCC:AAAA::13	126	2	tunel 4			Disponible
2001:CCCC:AAAA::14	-	2001:CCCC:AAAA::17	126	2	tunel 5			Disponible
2001:CCCC:AAAA::18	-	2001:CCCC:AAAA::1B	126	2	tunel 6			Disponible
2001:CCCC:AAAA::1C	-	2001:CCCC:AAAA::1F	126	2	tunel 7			Disponible
2001:CCCC:AAAA::20	-	2001:CCCC:AAAA::23	126	2	tunel 8			Disponible
2001:CCCC:AAAA::24	-	2001:CCCC:AAAA::27	126	2	tunel 9			Disponible
2001:CCCC:AAAA::28	-	2001:CCCC:AAAA::2B	126	2	tunel 10			Disponible

***Fuente*: Elaboración propia**

Tabla Nº 3. **Cuadro de direcciones IPV4 desplegable en los túneles VPN**

Cuadro de direcciones IPV4 desplegadas en los túneles VPN													
Pool de red									Mascara	Mascara wilcard	Interface	Principal	Sede	Nombre y número de agencia
10	10	0	0	-	10	10	0	3	255.255.255.252	0.0.0.3	tunel 3	10.10.0.1	10.10.0.2	Disponible
10	10	0	4	-	10	10	0	7	255.255.255.252	0.0.0.3	tunel 4	10.10.0.5	10.10.0.6	Disponible
10	10	0	8	-	10	10	0	11	255.255.255.252	0.0.0.3	tunel 5	10.10.0.9	10.10.0.10	Abonado_CP-Abonado_CS
10	10	0	12	-	10	10	0	15	255.255.255.252	0.0.0.3	tunel 3	10.10.0.13	10.10.0.14	
10	0	0	16	-	10	10	0	19	255.255.255.252	0.0.0.3	tunel 4	10.10.0.17	10.10.0.18	
10	0	0	20	-	10	10	0	23	255.255.255.252	0.0.0.3	tunel 5	10.10.0.21	10.10.0.22	
10	0	0	24	-	10	10	0	27	255.255.255.252	0.0.0.3	tunel 6	10.10.0.25	10.10.0.26	
10	10	0	28	-	10	10	0	31	255.255.255.252	0.0.0.3	tunel 7	10.10.0.29	10.10.0.30	
10	10	0	32	-	10	10	0	35	255.255.255.252	0.0.0.3	tunel 8	10.10.0.33	10.10.0.34	
10	10	0	36	-	10	10	0	39	255.255.255.252	0.0.0.3	tunel 9	10.10.0.37	10.10.0.38	
10	10	0	40	-	10	10	0	43	255.255.255.252	0.0.0.3	tunel 10	10.10.0.41	10.10.0.42	

Fuente: **Elaboración propia**

Tabla Nº 4. **Cuadro de direcciones IPV6 utilizadas en la red LAN de cada agencia**

Cuadro de direcciones IPV6 utilizadas en la red lan de cada agencia					
Dirección Inicio		Dirección Final	Numero de Bits	Host Disponibles	Nombre y numero de agencia
2001:BBBB:AAAA::0	-	2001:BBBB:AAAA::FF	120	254	Abonado_AP
2001:BBBB:AAAA::100	-	2001:BBBB:AAAA::1FF	120	254	Abonado_AS
2001:BBBB:AAAA::200	-	2001:BBBB:AAAA::2FF	120	254	Abonado_BP
2001:BBBB:AAAA::300	-	2001:BBBB:AAAA::3FF	120	254	Abonado_BS
2001:BBBB:AAAA::400	-	2001:BBBB:AAAA::4FF	120	254	Abonado_CP
2001:BBBB:AAAA::500	-	2001:BBBB:AAAA::5FF	120	254	Abonado_CS
2001:BBBB:AAAA::600	-	2001:BBBB:AAAA::6FF	120	254	Disponible
2001:BBBB:AAAA::700	-	2001:BBBB:AAAA::7FF	120	254	Disponible
2001:BBBB:AAAA::800	-	2001:BBBB:AAAA::8FF	120	254	Disponible
2001:BBBB:AAAA::900	-	2001:BBBB:AAAA::9FF	120	254	Disponible

Fuente: **Elaboración propia**

Tabla Nº 5. **Cuadro de direcciones IPV4 utilizadas en la red LAN de cada agencia**

Cuadro de direcciones IPV4 utilizadas en la red lan de cada agencia											
Pool de red									Mascara red	mascara wilcard	Nombre y numero de agencia
192	168	0	0	-	192	168	0	255	255.255.255.0	0.0.0.255	Disponible
192	168	1	0	-	192	168	1	255	255.255.255.0	0.0.0.255	Disponible
192	168	2	0	-	192	168	2	255	255.255.255.0	0.0.0.255	Disponible
192	168	3	0	-	192	168	3	255	255.255.255.0	0.0.0.255	Disponible
192	168	4	0	-	192	168	4	255	255.255.255.0	0.0.0.255	Abonado_CP
192	168	5	0	-	192	168	5	255	255.255.255.0	0.0.0.255	Abonado_CS
192	168	6	0	-	192	168	6	255	255.255.255.0	0.0.0.255	Disponible
192	168	7	0	-	192	168	7	255	255.255.255.0	0.0.0.255	Disponible
192	168	8	0	-	192	168	8	255	255.255.255.0	0.0.0.255	Disponible

Fuente**: Elaboración propia**

Tabla Nº 6. **Cuadro de direcciones IPv6 utilizadas en os enlaces WAN**

Cuadro de direcciones IPV6 utilizadas en los enlaces WAN								
Dirección Inicio		Dirección Final	Número de Bits	Interface				
2001:AAAA:AAAA::0		2001:AAAA:AAAA::3	126	Fast 0/0	R1	2001:AAAA:AAAA::1/126	R2	2001:AAAA:AAAA::2/126
2001:AAAA:AAAA::4		2001:AAAA:AAAA::7	126	Fast 0/1	R2	2001:AAAA:AAAA::5/126	R3	2001:AAAA:AAAA::6/126
2001:AAAA:AAAA::8		2001:AAAA:AAAA::B	126	Fast 0/0	R3	2001:AAAA:AAAA::9/126	R4	2001:AAAA:AAAA::A/126
2001:AAAA:AAAA::C		2001:AAAA:AAAA::F	126	Fast 0/1	R1	2001:AAAA:AAAA::D/126	R5	2001:AAAA:AAAA::E/126
2001:AAAA:AAAA::10		2001:AAAA:AAAA::13	126	Fast 0/0	R5	2001:AAAA:AAAA::11/126	R6	2001:AAAA:AAAA::12/126
2001:AAAA:AAAA::14		2001:AAAA:AAAA::17	126	Fasf 0/1	R6	2001:AAAA:AAAA::15/126	R7	2001:AAAA:AAAA::16/126
2001:AAAA:AAAA::18		2001:AAAA:AAAA::1B	126	Fast 1/0	R7	2001:AAAA:AAAA::19/126	R4	2001:AAAA:AAAA::1A/126
2001:AAAA:AAAA::1C		2001:AAAA:AAAA::1F	126	Fast 1/0	Abonado_AP	2001:AAAA:AAAA::1D/126	R1	2001:AAAA:AAAA::1E/126
2001:AAAA:AAAA::20		2001:AAAA:AAAA::23	126	Fast 1/0	Abonado_AS	2001:AAAA:AAAA::21/126	R3	2001:AAAA:AAAA::22/126
2001:AAAA:AAAA::24		2001:AAAA:AAAA::27	126	Fast 1/0	Abonado_BP	2001:AAAA:AAAA::25/126	R2	2001:AAAA:AAAA::26/126
2001:AAAA:AAAA::28		2001:AAAA:AAAA::2B	126	Fast 1/1	Abonado_BS	2001:AAAA:AAAA::29/126	R3	2001:AAAA:AAAA::2A/126
2001:AAAA:AAAA::2C		2001:AAAA:AAAA::2F	126	Fast 1/1	Abonado_CP	2001:AAAA:AAAA::2D/126	R1	2001:AAAA:AAAA::2E/126
2001:AAAA:AAAA::30		2001:AAAA:AAAA::33	126	Fast 1/1	Abonado_CS	2001:AAAA:AAAA::31/126	R4	2001:AAAA:AAAA::32/126
2001:AAAA:AAAA::34		2001:AAAA:AAAA::37	126	Disponible				
2001:AAAA:AAAA::38		2001:AAAA:AAAA::3B	126	Disponible				
2001:AAAA:AAAA::60		2001:AAAA:AAAA::63	126	Disponible				
2001:AAAA:AAAA::64		2001:AAAA:AAAA::67	126	Disponible				
2001:AAAA:AAAA::68		2001:AAAA:AAAA::71	126	Disponible				

Fuente**: Elaboración propia**

Tabla Nº 7. **Cuadro de direcciones IPv4 utilizadas en los enlaces WAN**

Cuadro de direcciones IPV4 utilizadas en los enlaces WAN														
Pool de red									Mascara red	Mascara wilcard	Interface			
172	16	0	0	-	172	16	0	3	255.255.255.252	0.0.0.3	Fast 0/0	R1	172.16.0.1	R2	172.16.0.2
172	16	0	4	-	172	16	0	7	255.255.255.252	0.0.0.3	Fast 0/1	R2	172.16.0.5	R3	172.16.0.6
172	16	0	8	-	172	16	0	11	255.255.255.252	0.0.0.3	Fast 0/0	R3	172.16.0.9	R4	172.16.0.10
172	16	0	12	-	172	16	0	15	255.255.255.252	0.0.0.3	Fast 0/1	R1	172.16.0.13	R5	172.16.0.14
172	16	0	16	-	172	16	0	19	255.255.255.252	0.0.0.3	Fast 0/0	R5	172.16.0.17	R6	172.16.0.18
172	16	0	20	-	172	16	0	23	255.255.255.252	0.0.0.3	Fasf 0/1	R6	172.16.0.21	R7	172.16.0.22
172	16	0	24	-	172	16	0	27	255.255.255.252	0.0.0.3	Fast 1/0	R7	172.16.0.25	R4	172.16.0.26
172	16	0	28	-	172	16	0	31	255.255.255.252	0.0.0.3	Fast 1/0	Abonado_AP	172.16.0.29	R1	172.16.0.30
172	16	0	32	-	172	16	0	35	255.255.255.252	0.0.0.3	Fast 1/0	Abonado_BP	172.16.0.33	R2	172.16.0.34
172	16	0	36	-	172	16	0	39	255.255.255.252	0.0.0.3	Fast 1/1	Abonado_CP	172.16.0.37	R1	172.16.0.38
172	16	0	40	-	172	16	0	43	255.255.255.252	0.0.0.3	Fasf 0/1	Abonado_AS	172.16.0.41	R3	172.16.0.42
172	16	0	44	-	172	16	0	47	255.255.255.252	0.0.0.3	Fast 1/1	Abonado_BS	172.16.0.45	R3	172.16.0.46
172	16	0	48	-	172	16	0	51	255.255.255.252	0.0.0.3	Fast 1/1	Abonado_CS	172.16.0.49	R4	172.16.0.50
172	16	0	52	-	172	16	0	55	255.255.255.252	0.0.0.3	Disponible		172.16.0.53		172.16.0.54
172	16	0	56	-	172	16	0	59	255.255.255.252	0.0.0.3	Disponible		172.16.0.57		172.16.0.58
172	16	0	60	-	172	16	0	63	255.255.255.252	0.0.0.3	Disponible		172.16.0.61		172.16.0.62
172	16	0	64	-	172	16	0	67	255.255.255.252	0.0.0.3	Disponible		172.16.0.65		172.16.0.66
172	16	0	68	-	172	16	0	71	255.255.255.252	0.0.0.3	Disponible		172.16.0.69		172.16.0.70

***Fuente*: Elaboración propia**

Tabla Nº 8. **Cuadro de direcciones IPv6 para las interfaces loopback**

Cuadro de direccones IPV6 para las interfaces looback						
Dirección Inicio		Dirección Final	Numero de Bits	Host Disponibles	Router_ID	Dirección Asignada
2001:DDDD:AAAA::0	-	2001:DDDD:AAAA::3	126	2	R1	2001:DDDD:AAAA::1/126
2001:DDDD:AAAA::4		2001:DDDD:AAAA::7	126	2	R2	2001:DDDD:AAAA::5/126
2001:DDDD:AAAA::8		2001:DDDD:AAAA::B	126	2	R3	2001:DDDD:AAAA::9/126
2001:DDDD:AAAA::C		2001:DDDD:AAAA::F	126	2	R4	2001:DDDD:AAAA::D/126
2001:DDDD:AAAA::10		2001:DDDD:AAAA::13	126	2	R5	2001:DDDD:AAAA::11/126
2001:DDDD:AAAA::14		2001:DDDD:AAAA::18	126	2	R6	2001:DDDD:AAAA::15/126
2001:DDDD:AAAA::8		2001:DDDD:AAAA::1B	126	2	R7	2001:DDDD:AAAA::19/126

***Fuente*: Elaboración propia**

Tabla Nº 9. **Cuadro de direcciones IPv4 para las interfaces loopback**

Cuadro de direccones IPV4 para las interfaces looback			
Direccion	Mascara red	Mascara wilcard	Router
10.0.1.1	255.255.255.0	0.0.0.255	R1
10.0.2.1	255.255.255.0	0.0.0.255	R2
10.0.3.1	255.255.255.0	0.0.0.255	R3
10.0.4.1	255.255.255.0	0.0.0.255	R4
10.0.5.1	255.255.255.0	0.0.0.255	R5
10.0.6.1	255.255.255.0	0.0.0.255	R6
10.0.7.1	255.255.255.0	0.0.0.255	R7
10.0.8.1	255.255.255.0	0.0.0.255	R8

***Fuente*: Elaboración propia**

En la siguiente grafica ilustramos el mapa de direcciones IP utilizadas en la red privada de cada abonando del servicio.

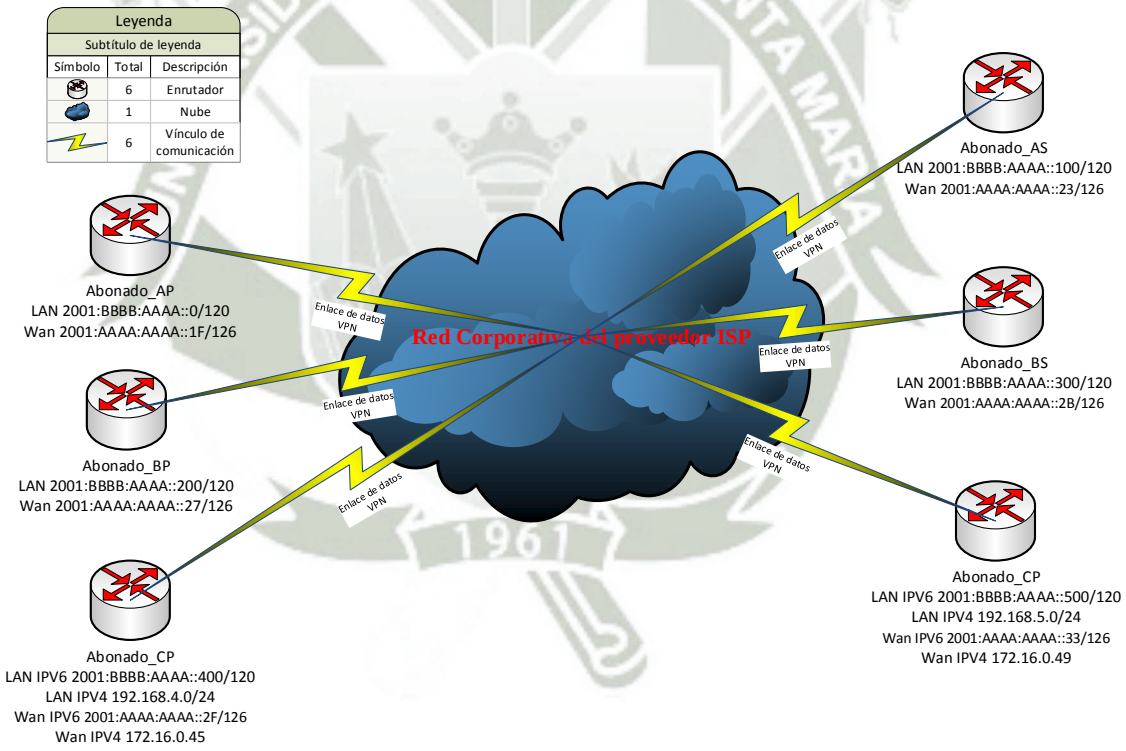

Gráfico Nº 10. **Mapa de direcciones IP utilizadas en la VPN de cada abonado**

***Fuente*: Elaboración propia**

c) Implementación: Formación del usuario; Implantación del sistema.

Ahora ya con toda la documentación en regla procedemos a confeccionar nuestro laboratorio de pruebas, en base a la información recolectada durante las entrevistas realizadas con el personal de TI de Fondesurco y el proveedor de comunicaciones Level 3, para la elaboración de la nube del ISP dispondremos de 7 enrutadores todos enlazados a través del protocolo OSPF, recrearemos 3 escenarios para los diferentes clientes de la empresa en mención, cada sucursal tiene su propio enrutador conectado y se conecta a su sede principal a través de una conexión VPN tal y como se ilustra en la gráfica más adelante.

En paralelo agregaremos a esta configuración las respectivas reservas RSVP y el protocolo MPLS para habilitar ingeniería de tráfico, utilizando uno de los enlaces subutilizados permitiendo de este modo ofrecer un servicio garantizado al abonado_C, quien demanda una mejor calidad en el servicio ofrecido para atender sus planes de crecimiento.

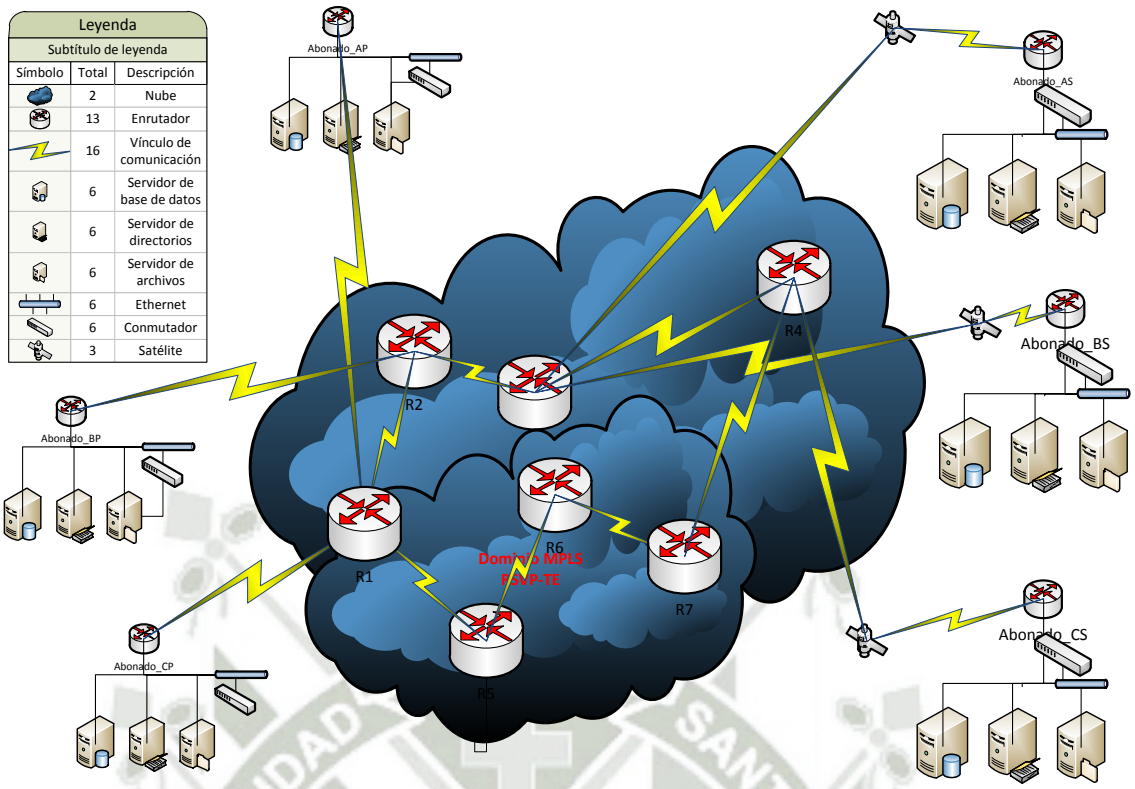

Gráfico Nº 11. **Configuración con las RSVP y MPLS**

Fuente**: Elaboración propia**

6.1.1. Configuración de los equipos

En esta sección iremos detallando paso a paso las configuraciones desplegadas en cada uno de los enrutadores, dividiremos la configuración en dos partes una para los equipos de la red privada de los abonados y otra para la red privada del proveedor de comunicaciones.

6.1.1.1. Configuración de los enrutadores del abonado

Los dispositivos utilizados en nuestra simulación son equipos Cisco 2691 con dos interfaces fast ethernet para permitir la conectividad entre la red WAN y la LAN la versión de IOS utilizada es la 12.4 (4) T7.

Con el cuadro de direccionamiento IP nos permitirá llevar un mejor control de las subredes utilizadas en que equipo, número de interfaz asignada y finalmente las que se encuentran disponibles desplegaremos la configuración de los enlaces WAN de la siguiente manera.

6.1.1.2. Configuración de las interfaces fast Ethernet

```
Abonado_AP#
Abonado_AP#configure terminal
Abonado_AP#(config)#interface fastEthernet 0/0
Abonado_AP#(config-if)# ipv6 address 2001:BBBB:AAAA::1/120
Abonado_AP#(config-if)# no shutdown
Abonado_AP#(config-if)#exit
Abonado_AP#(config-if)# interface fastEthernet 1/1
Abonado_AP#(config-if)# ipv6 address 2001:AAAA:AAAA::1D/126
Abonado_AP#(config-if)# no shutdown
Abonado_AP#(config-if)#exit
```

6.1.1.3. Configuración del túnel VPN

```
Abonado_AP#
Abonado_AP#configure terminal
Abonado_AP#(config)#interface Tunnel0
Abonado_AP#(config-if)# no ip address
Abonado_AP#(config-if)# ipv6 address 2001:CCCC:AAAA::1/126
Abonado_AP#(config-if)#tunnel source FastEthernet1/0
Abonado_AP#(config-if)#tunnel mode gre ipv6
Abonado_AP#(config-if)#tunnel destination 2001:AAAA:AAAA::21
Abonado_AP#(config-if)#exit
```

6.1.1.4. Configuración de las tablas de ruteo

Como paso final nos resta habilitar las tablas de ruteo utilizaremos rutas estáticas para permitir la conexión VPN entre las agencias del abonado.

```
Abonado_AP#
Abonado_AP#configure terminal
Abonado_AP#(config)# ipv6 route 2001:BBBB:AAAA::100/120 Tunnel0
2001:CCCC:AAAA::2
```

Con esto ya tenemos habilitadas todas las rutas para nuestros destinos, atreves de los túneles VPN establecidos con cada una de las agencias, ahora realizamos las pruebas de diagnóstico para evaluar la configuración aplicada.

Abonado_AP#show ipv6 interface brief
FastEthernet0/0 [up/up]
FE80::C808:1AFF:FE48:8
2001:BBBB:AAAA::1
FastEthernet0/1 [administratively down/down]
Unassigned
FastEthernet1/0 [up/up]
FE80::C808:1AFF:FE48:1C
2001:AAAA:AAAA::1D
FastEthernet1/1 [administratively down/down]
Unassigned
Tunnel0 [up/up]
FE80::C808:1AFF:FE48:8
2001:CCCC:AAAA::1
Abonado_AP#

Abonado_AP#show ipv6 route	
	IPv6 Routing Table - default - 9 entries
	Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
	B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
	I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
	EX - EIGRP external, ND - Neighbor Discovery
	O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
	ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S	::/0 [2/0]
	via FE80::C801:18FF:FEB8:1C, FastEthernet1/0
C	2001:AAAA:AAAA::1C/126 [0/0]
	via FastEthernet1/0, directly connected
L	2001:AAAA:AAAA::1D/128 [0/0]
	via FastEthernet1/0, receive
C	2001:BBBB:AAAA::/120 [0/0]
	via FastEthernet0/0, directly connected
L	2001:BBBB:AAAA::1/128 [0/0]
	via FastEthernet0/0, receive
S	2001:BBBB:AAAA::100/120 [1/0]

	via 2001:CCCC:AAAA::2, Tunnel0
C	2001:CCCC:AAAA::/126 [0/0]
	via Tunnel0, directly connected
L	2001:CCCC:AAAA::1/128 [0/0]
	via Tunnel0, receive
L	FF00::/8 [0/0]
	via Null0, receive

Abonado_AP#

```
Abonado_AP#show interfaces tunnel0 summary

*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count

Interface          IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* Tunnel0            0    0    0    0    0    0    0    0    0
Abonado_AP#
```

Solo para el caso de nuestro estudio Fondesurco quienes mantienen un direccionamiento IPV4 desplegaremos la siguiente configuración tanto para IPV4 e IPV6.

```
Abonado_CP#
Abonado_CP#configure terminal
Abonado_CP(config)#
Abonado_CP(config)#interface fastEthernet 0/0
Abonado_CP(config-if)# ip address 192.168.4.1 255.255.255.0
Abonado_CP(config-if)# ipv6 address 2001:BBBB:AAAA::401/120
Abonado_CP(config-if)# no shutdown
Abonado_CP(config-if)#exit
Abonado_CP(config)#interface fastEthernet 1/1
Abonado_CP(config-if)# ip address 172.16.0.37 255.255.255.252
Abonado_CP(config-if)# ipv6 address 2001:AAAA:AAAA::2D/126
Abonado_CP(config-if)# no shutdown
Abonado_CP(config-if)#exit

Abonado_CP(config)#interface tunnel 2
Abonado_CP(config-if)# no ip address
Abonado_CP(config-if)# ipv6 address 2001:CCCC:AAAA::9/126
```

```
Abonado_CP(config-if)# tunnel source FastEthernet1/1
Abonado_CP(config-if)# tunnel mode gre ipv6
Abonado_CP(config-if)# tunnel destination 2001:AAAA:AAAA::31
Abonado_CP(config-if)#exit
Abonado_CP(config)#interface tunnel 5
Abonado_CP(config)# ip address 10.10.0.9 255.255.255.252
Abonado_CP(config)# tunnel source FastEthernet1/1
Abonado_CP(config)# tunnel destination 172.16.0.49
Abonado_CP(config)#exit
```

6.1.1.5. Configuración de las tablas de ruteo

Como paso final nos resta habilitar las tablas de ruteo utilizaremos rutas estáticas para permitir la conexión VPN entre las agencias del abonado.

```
Abonado_CP(config)# ip route 0.0.0.0 0.0.0.0 FastEthernet1/1
Abonado_CP(config)# ip route 192.168.5.0 255.255.255.0 10.10.0.10
Abonado_CP(config)# ipv6 route 2001:BBBB:AAAA::500/120 Tunnel2
2001:CCCC:AAAA::A
```

Realizamos las pruebas de diagnóstico para evaluar la configuración aplicada.

```
Abonado_CP#show ipv6 interface brief
FastEthernet0/0          [up/up]
FE80::C80C:2FF:FE20:8
2001:BBBB:AAAA::401
FastEthernet0/1          [administratively down/down]
Unassigned
FastEthernet1/0          [administratively down/down]
Unassigned
FastEthernet1/1          [up/up]
FE80::C80C:2FF:FE20:1D
2001:AAAA:AAAA::2D
Tunnel2                  [up/up]
FE80::C80C:2FF:FE20:8
2001:CCCC:AAAA::9
Tunnel5                  [up/up]
Unassigned
Abonado_CP#
```

Abonado_CP#show ip interface brief						
Interface	IP-Address	OK?	Method	Status		Protocol
FastEthernet0/0	192.168.4.1	YES	NVRAM	up		up
FastEthernet0/1	unassigned	YES	NVRAM	administratively	down	down
FastEthernet1/0	unassigned	YES	NVRAM	administratively	down	down
FastEthernet1/1	172.16.0.37	YES	NVRAM	up		up
Tunnel2	unassigned	YES	NVRAM	up		up
Tunnel5	10.10.0.9	YES	NVRAM	up		up
Abonado_CP#						

```
Abonado_CP#show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D – EIGRP
EX - EIGRP external, ND - Neighbor Discovery
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [2/0]
via FE80::C801:18FF:FEB8:1D, FastEthernet1/1
C   2001:AAAA:AAAA::2C/126 [0/0]
via FastEthernet1/1, directly connected
L   2001:AAAA:AAAA::2D/128 [0/0]
via FastEthernet1/1, receive
C   2001:BBBB:AAAA::400/120 [0/0]
via FastEthernet0/0, directly connected
L   2001:BBBB:AAAA::401/128 [0/0]
via FastEthernet0/0, receive
S   2001:BBBB:AAAA::500/120 [1/0]
via 2001:CCCC:AAAA::A, Tunnel2
C   2001:CCCC:AAAA::8/126 [0/0]
via Tunnel2, directly connected
L   2001:CCCC:AAAA::9/128 [0/0]
via Tunnel2, receive
L   FF00::/8 [0/0]
via Null0, receive
Abonado_CP#
```

```
Abonado_CP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter área
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, + - replicated route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, FastEthernet1/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.0.8/30 is directly connected, Tunnel5
L        10.10.0.9/32 is directly connected, Tunnel5
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.36/30 is directly connected, FastEthernet1/1
L        172.16.0.37/32 is directly connected, FastEthernet1/1
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, FastEthernet0/0
L        192.168.4.1/32 is directly connected, FastEthernet0/0
S     192.168.5.0/24 [1/0] via 10.10.0.10
Abonado_CP#
```

```
Abonado_CP#show interfaces tunnel2 summary

*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count

Interface           IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS
TRTL
-----------------------------------------------------------------------
* Tunnel2              0    0    0    0    0    0    0    0    0
Abonado_CP#show interfaces tunnel5 summary

*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count

Interface           IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS
TRTL
-----------------------------------------------------------------------
* Tunnel5              0    0    0    0    0    0    0    0    0
Abonado_CP#
```

6.1.1.6. Configuración de los enrutadores del proveedor ISP

Según las entrevistas sostenidas con el proveedor de comunicaciones nos afirman que utilizan equipos ciscos modelo 7200, son los mismos que hemos utilizado para la realización de nuestra simulación tales equipos están trabajando con la versión de IOS 15.0(1)M, del mismo modo que el anterior utilizaremos el cuadro de direcciones ip para las interfaces Loopback, que serán utilizadas cono ID de los enrutadores, hacemos inca pie que el protocolo de enrutamiento utilizado es OSPF, sobre el cual aplicaremos las optimizaciones que nos brindan los protocolos RSVP y MPLS.

6.1.1.7. Configuración de las Interfaces

Ingresamos al modo de configuración global, en cada interface

```
R1#
R1#configure terminal
R1(config)# interface Loopback0
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 172.16.0.1 255.255.255.252
R1(config-if)#ipv6 address 2001:AAAA:AAAA::1/126
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface FastEthernet0/1
R1(config-if)# ip address 172.16.0.13 255.255.255.252
R1(config-if)#ipv6 address2001:AAAA:AAAA::D/126
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface FastEthernet1/0
R1(config-if)#ip address 172.16.0.30 255.255.255.252
R1(config-if)#ipv6 address 2001:AAAA:AAAA::1E/126
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface FastEthernet1/1
R1(config-if)#ip address 172.16.0.46 255.255.255.252
ipv6 address ipv6 address 2001:AAAA:AAAA::2E/126
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configuración del protocolo OSPF, para el direccionamiento IPV4. Dentro del modo de configuración global.

```
R1(config)#router ospf 10
R1(config)# network 10.0.1.0 0.0.0.255 area 10
R1(config)# network 172.16.0.0 0.0.0.3 area 10
R1(config)# network 172.16.0.12 0.0.0.3 area 10
R1(config)# network 172.16.0.36 0.0.0.3 area 10
R1(config)#exit
```

6.1.1.8. Configuración del protocolo OSPF, para el direccionamiento IPV6

```
R1# configure terminal
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router ospf 1
R1(config)# router-id 10.0.1.1
R1(config)#exit
```

Con esto habilitamos el protocolo de enrutamiento OSPF para IPV6, ahora resta habilitarlo para cada una de las interfaces que vamos a publicar.

```
R1# configure terminal
R1(config)#interface fastEthernet 0/0
R1(config)#ipv6 ospf 1 area 0
R1(config)#router-id 10.0.1.1
R1(config)#exit
```

Con esto tenemos habilitado nuestro equipo, y con las redes publicadas para los vecinos que conformar nuestra red OSPF, ahora procedemos a verificar la configuración.

Nota.- La misma configuración se aplica para los demás equipos de la red corporativa del proveedor.

```
R1#show ipv6 route
    IPv6 Routing Table - default - 18 entries
    Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
    B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
    I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D – EIGRP
    EX - EIGRP external, ND - Neighbor Discovery
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
C    2001:AAAA:AAAA::/126 [0/0]
     via FastEthernet0/0, directly connected
L    2001:AAAA:AAAA::1/128 [0/0]
     via FastEthernet0/0, receive
O    2001:AAAA:AAAA::4/126 [110/2]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
O    2001:AAAA:AAAA::8/126 [110/3]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
C    2001:AAAA:AAAA::C/126 [0/0]
     via FastEthernet0/1, directly connected
L    2001:AAAA:AAAA::D/128 [0/0]
     via FastEthernet0/1, receive
O    2001:AAAA:AAAA::10/126 [110/2]
     via FE80::C805:14FF:FE64:6, FastEthernet0/1
O    2001:AAAA:AAAA::14/126 [110/3]
     via FE80::C805:14FF:FE64:6, FastEthernet0/1
O    2001:AAAA:AAAA::18/126 [110/4]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
     via FE80::C805:14FF:FE64:6, FastEthernet0/1
C    2001:AAAA:AAAA::1C/126 [0/0]
     via FastEthernet1/0, directly connected
L    2001:AAAA:AAAA::1E/128 [0/0]
     via FastEthernet1/0, receive
O    2001:AAAA:AAAA::20/126 [110/3]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
O    2001:AAAA:AAAA::24/126 [110/2]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
O    2001:AAAA:AAAA::28/126 [110/3]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
C    2001:AAAA:AAAA::2C/126 [0/0]
     via FastEthernet1/1, directly connected
L    2001:AAAA:AAAA::2E/128 [0/0]
     via FastEthernet1/1, receive
O    2001:AAAA:AAAA::30/126 [110/4]
     via FE80::C802:13FF:FE9C:8, FastEthernet0/0
L    FF00::/8 [0/0]
     via Null0, receive
R1   #
R1#show ip route
                    Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B –
                    BGP
                    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter área
                    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, + - replicated route

                Gateway of last resort is not set

                10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C               10.0.1.0/24 is directly connected, Loopback0
L               10.0.1.1/32 is directly connected, Loopback0
O               10.0.2.1/32 [110/2] via 172.16.0.2, 01:11:52, FastEthernet0/0
O               10.0.3.1/32 [110/3] via 172.16.0.2, 01:11:52, FastEthernet0/0
O               10.0.4.1/32 [110/4] via 10.0.4.1, 01:11:52, Tunnel10
                [110/4] via 10.0.4.1, 01:11:52, Tunnel12
O               10.0.5.1/32 [110/2] via 172.16.0.14, 01:11:52, FastEthernet0/1
O               10.0.6.1/32 [110/3] via 172.16.0.14, 01:11:52, FastEthernet0/1
O               10.0.7.1/32 [110/4] via 172.16.0.14, 01:11:52, FastEthernet0/1
                172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
C               172.16.0.0/30 is directly connected, FastEthernet0/0
L               172.16.0.1/32 is directly connected, FastEthernet0/0
O               172.16.0.4/30 [110/2] via 172.16.0.2, 01:11:53, FastEthernet0/0
O               172.16.0.8/30 [110/3] via 172.16.0.2, 01:11:53, FastEthernet0/0
C               172.16.0.12/30 is directly connected, FastEthernet0/1
L               172.16.0.13/32 is directly connected, FastEthernet0/1
O               172.16.0.16/30 [110/2] via 172.16.0.14, 01:11:53, FastEthernet0/1
O               172.16.0.20/30 [110/3] via 172.16.0.14, 01:11:53, FastEthernet0/1
O               172.16.0.24/30 [110/4] via 172.16.0.14, 01:11:53, FastEthernet0/1
                [110/4] via 10.0.4.1, 01:11:53, Tunnel10
                [110/4] via 10.0.4.1, 01:11:53, Tunnel12
C               172.16.0.36/30 is directly connected, FastEthernet1/1
L               172.16.0.38/32 is directly connected, FastEthernet1/1
O               172.16.0.48/30 [110/4] via 10.0.4.1, 01:11:53, Tunnel10
                [110/4] via 10.0.4.1, 01:11:53, Tunnel12
R1#
```

```
R1#show ipv6 interface brief
FastEthernet0/0         [up/up]
FE80::C801:18FF:FEB8:8
2001:AAAA:AAAA::1
FastEthernet0/1         [up/up]
FE80::C801:18FF:FEB8:6
2001:AAAA:AAAA::D
FastEthernet1/0         [up/up]
FE80::C801:18FF:FEB8:1C
2001:AAAA:AAAA::1E
FastEthernet1/1         [up/up]
FE80::C801:18FF:FEB8:1D
2001:AAAA:AAAA::2E
Loopback0               [up/up]
```

```
Unassigned
Tunnel10               [up/up]
Unassigned
Tunnel12               [up/up]
Unassigned
R1#
```

```
R1#show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/0        172.16.0.1      YES NVRAM   Up        up
FastEthernet0/1        172.16.0.13     YES NVRAM   Up        up
FastEthernet1/0        unassigned      YES NVRAM   Up        up
FastEthernet1/1        172.16.0.38     YES NVRAM   Up        up
Loopback0              10.0.1.1        YES NVRAM   Up        up
Tunnel10               172.16.0.38     YES TFTP    Up        up
Tunnel12               172.16.0.38     YES TFTP    Up        up
R1#
```

6.1.2. Configuración de los equipos aplicando MPLS y RSVP

En esta sección iremos especificando las configuraciones aplicadas en los diferentes equipos durante el proceso de introducción de RSVP y MPLS en las alineaciones actuales de los equipos, los cambios se pueden aplicar en caliente (en producción) no afectando al rendimiento ni presentando un impacto negativo al negocio, los cambios dados deben aplicarse en los equipos de comunicaciones del ISP. Sin más preámbulo pasemos a la configuración de los equipos.

Como primer paso debemos habilitar MPLS en todos las enrutadores que conformaran nuestro dominio MPLS, ingresamos al modo de configuración global y debemos introducir los siguientes comandos.

```
R1(config)#ip cef
R1(config)#mpls label protocol ldp
R1(config)#mpls traffic-eng tunnels
R1(config)#ipv6 cef
```

Por cada interface del router tenemos que habilitar para que soporte MPLS y RSVP, esta configuración la realizamos de la siguiente manera:

Nota.- Para nuestro caso aplicaremos la configuración en todas las interfaces activas de todos los equipos que conformar la red del ISP, la configuración es la misma por lo solo citamos un equipo como referencia.

```
R1(config)#
R1(config)#interface fastEthernet 0/0
R1(config-if)#mpls ip
R1(config-if)#mpls traffic-eng tunnels
R1(config-if)#ip rsvp bandwidth 8000
R1(config-if)#exit
R1(config)#
```

Como siguiente paso debemos permitir que OSPF también sea compatible con MPLS, esto se lleva a cabo de la siguiente manera y se aplica a todos los casos.

```
R1(config)#
R1(config)#router ospf 10
R1(config-router)#mpls traffic-eng router-id Loopback0
R1(config-router)#mpls traffic-eng area 10
R1(config-router)#exit
R1(config)#
```

Ahora procedemos a evaluar los cambios aplicados en los equipos de comunicaciones. Esta labor la podemos realizar haciendo uso del comando show mpls, el cual dispone de varias opciones que las podemos investigar de la siguiente manera como se muestra a continuación:

R1#show mpls ?	
discovery	Information about LSP discovery
Flow	MPLS netflow information
forwarding-table	Show the Label Forwarding Table
interfaces	Per-interface MPLS forwarding information
Ip	MPLS IP information
l2transport	MPLS circuit transport info
Label	Label information
Ldp	Label Distribution Protocol information

```
memory          Memory usage information
oam             OAM information
static          Show MPLS static information
traffic-eng     Traffic engineering information

R1#show mpls
```

Como primer paso vamos a revisar rápidamente que interfaces están funcionando con MPLS.

```
R1#show mpls interfaces
Interface              IP         Tunnel   BGP     Static  Operational
FastEthernet0/0        Yes (ldp)  Yes      No      No      Yes
FastEthernet0/1        Yes (ldp)  Yes      No      No      Yes
FastEthernet1/0        Yes (ldp)  Yes      No      No      Yes
FastEthernet1/1        Yes (ldp)  Yes      No      No      Yes
Tunnel10               No         No       No      No      Yes
Tunnel12               No         No       No      No      Yes
R1#
```

Verificando la información de LDP como identificativo del router MPLS y sus vecinos.

```
R1#show mpls ldp discovery
Local LDP Identifier:
10.0.1.1:0
Discovery Sources:
Interfaces:
FastEthernet0/0 (ldp):                  xmit/recv
LDP Id: 10.0.2.1:0
FastEthernet0/1 (ldp):                  xmit/recv
LDP Id: 10.0.5.1:0
FastEthernet1/0 (ldp):                  xmit
FastEthernet1/1 (ldp):                  xmit
R1#
```

Desplegamos en pantalla la detección de las adyacencias LDP y el estado de las conexiones establecidas, con los enrutadores vecinos en nuestra red MPLS que se está habilitando, esta tabla debe crecer a medida que vayamos agregando dispositivos.

```
R1#show mpls ldp neighbor
Peer                    LDP Ident: 10.0.2.1:0; Local LDP Ident 10.0.1.1:0
                        TCP connection: 10.0.2.1.21316 - 10.0.1.1.646
                        State: Oper; Msgs sent/rcvd: 40/39; Downstream
                        Up time: 00:18:28
                        LDP discovery sources:
                        FastEthernet0/0, Src IP addr: 172.16.0.2
                        Addresses bound to peer LDP Ident:
                        172.16.0.2      10.0.2.1        172.16.0.5
Peer                    LDP Ident: 10.0.5.1:0; Local LDP Ident 10.0.1.1:0
                        TCP connection: 10.0.5.1.24995 - 10.0.1.1.646
                        State: Oper; Msgs sent/rcvd: 39/39; Downstream
                        Up time: 00:18:19
                        LDP discovery sources:
                        FastEthernet0/1, Src IP addr: 172.16.0.14
                        Addresses bound to peer LDP Ident:
                        172.16.0.17     10.0.5.1        172.16.0.14
R1#
```

Con la introducción de MPLS cada uno de nuestros ruteadores usa como identificador la dirección IP de su interface loopback, con la configuración introducida cada router actúa como LSR (Label Switch Router) y ejecutan LDP, para visualizar la tabla LDP usamos el siguiente mandato.

```
R1#show mpls ldp bindings
Lib                     entry: 10.0.1.0/24, rev 8
                        local binding:  label: imp-null
Lib                     entry: 10.0.1.1/32, rev 26
                        remote binding: lsr: 10.0.2.1:0, label: 28
                        remote binding: lsr: 10.0.5.1:0, label: 23
Lib                     entry: 10.0.2.0/24, rev 23
                        remote binding: lsr: 10.0.2.1:0, label: imp-null
Lib                     entry: 10.0.2.1/32, rev 14
                        local binding:  label: 18
                        remote binding: lsr: 10.0.5.1:0, label: 22
Lib                     entry: 10.0.3.1/32, rev 12
                        local binding:  label: 17
                        remote binding: lsr: 10.0.2.1:0, label: 20
                        remote binding: lsr: 10.0.5.1:0, label: 21
Lib                     entry: 10.0.4.1/32, rev 10
                        local binding:  label: 16
                        remote binding: lsr: 10.0.2.1:0, label: 19
                        remote binding: lsr: 10.0.5.1:0, label: 20
```

Lib	entry: 10.0.5.0/24, rev 35
	remote binding: lsr: 10.0.5.1:0, label: imp-null
Lib	entry: 10.0.5.1/32, rev 32
	local binding: label: 25
	remote binding: lsr: 10.0.2.1:0, label: 33
Lib	entry: 10.0.6.1/32, rev 30
	local binding: label: 24
	remote binding: lsr: 10.0.2.1:0, label: 27
	remote binding: lsr: 10.0.5.1:0, label: 19
Lib	entry: 10.0.7.1/32, rev 29
	local binding: label: 23
	remote binding: lsr: 10.0.2.1:0, label: 26
	remote binding: lsr: 10.0.5.1:0, label: 18
Lib	entry: 172.16.0.0/30, rev 2
	local binding: label: imp-null
	remote binding: lsr: 10.0.2.1:0, label: imp-null
	remote binding: lsr: 10.0.5.1:0, label: 30
Lib	entry: 172.16.0.4/30, rev 22
	local binding: label: 22
	remote binding: lsr: 10.0.2.1:0, label: imp-null
	remote binding: lsr: 10.0.5.1:0, label: 27
Lib	entry: 172.16.0.8/30, rev 20
	local binding: label: 21
	remote binding: lsr: 10.0.2.1:0, label: 23
	remote binding: lsr: 10.0.5.1:0, label: 26
Lib	entry: 172.16.0.12/30, rev 4
	local binding: label: imp-null
	remote binding: lsr: 10.0.2.1:0, label: 31
	remote binding: lsr: 10.0.5.1:0, label: imp-null
Lib	entry: 172.16.0.16/30, rev 34
	local binding: label: 27
	remote binding: lsr: 10.0.2.1:0, label: 30
	remote binding: lsr: 10.0.5.1:0, label: imp-null
Lib	entry: 172.16.0.20/30, rev 33
	local binding: label: 26
	remote binding: lsr: 10.0.2.1:0, label: 32
	remote binding: lsr: 10.0.5.1:0, label: 29
Lib	entry: 172.16.0.24/30, rev 18
	local binding: label: 20
	remote binding: lsr: 10.0.2.1:0, label: 22
	remote binding: lsr: 10.0.5.1:0, label: 28
Lib	entry: 172.16.0.36/30, rev 6
	local binding: label: imp-null
	remote binding: lsr: 10.0.2.1:0, label: 29
	remote binding: lsr: 10.0.5.1:0, label: 25
Lib	entry: 172.16.0.48/30, rev 16

```
                                local binding:  label: 19
                                remote binding: lsr: 10.0.2.1:0, label: 21
                                remote binding: lsr: 10.0.5.1:0, label: 24
R1#
```

Finalmente si deseamos consultar la tabla FIB creada automáticamente durante la configuración de MPLS debemos hacer uso del siguiente mandato en la línea de comandos de nuestro enrutador, como se aprecia en la siguiente captura.

```
        R1#show mpls forwarding-table
Local   Outgoing   Prefix                Bytes Label   Outgoing    Next Hop
Label   Label      or Tunnel Id          Switched      interface
16      [T]  Pop Label  10.0.4.1/32      0             Tu10        point2point
        [T]  Pop Label  10.0.4.1/32      0             Tu12        point2point
17      20         10.0.3.1/32           0             Fa0/0       172.16.0.2
18      No Label   10.0.2.1/32           0             Fa0/0       172.16.0.2
19      [T]  No Label   172.16.0.48/30   0             Tu10        point2point
        [T]  No Label   172.16.0.48/30   0             Tu12        point2point
20      28         172.16.0.24/30        0             Fa0/1       172.16.0.14
        [T]  No Label   172.16.0.24/30   0             Tu10        point2point
        [T]  No Label   172.16.0.24/30   0             Tu12        point2point
21      23         172.16.0.8/30         0             Fa0/0       172.16.0.2
22      Pop Label  172.16.0.4/30         0             Fa0/0       172.16.0.2
23      18         10.0.7.1/32           0             Fa0/1       172.16.0.14
24      19         10.0.6.1/32           0             Fa0/1       172.16.0.14
25      No Label   10.0.5.1/32           0             Fa0/1       172.16.0.14
26      29         172.16.0.20/30        0             Fa0/1       172.16.0.14
27      Pop Label  172.16.0.16/30        0             Fa0/1       172.16.0.14

[T]     Forwarding through a LSP tunnel  .
        View additional labelling info   with the 'deta  il' option
R1#
```

```
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::0/126
                Outgoing   Prefix          Bytes
Local           Label                      Outgoing          Next Hop
Label           Label      or Tunnel Id    Switched          interface
                No Label
None            2001:AAAA:AAAA::/126  \
                0                          Punt
```

```
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::4/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::4/126    \
                0                        Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::8/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::8/126    \
                0                        Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::C/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::C/126    \
                0                        Punt
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::10/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::10/126   \
                0                        Fa0/1           FE80::C805:14FF:F
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::14/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::14/126   \
                0                        Fa0/1           FE80::C805:14FF:F
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::18/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
                No Label
None            2001:AAAA:AAAA::18/126   \
                0                        Fa0/0           FE80::C802:13FF:F
                No Label
                2001:AAAA:AAAA::18/126   \
                0                        Fa0/1           FE80::C805:14FF:F
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::1C/126
                Outgoing  Prefix          Bytes
Local           Label                    Outgoing        Next Hop
Label           Label     or Tunnel Id   Switched        interface
```

```
                No Label
None            2001:AAAA:AAAA::1C/126  \
                0                       Punt
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::20/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                No Label
None            2001:AAAA:AAAA::20/126  \
                0                       Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::24/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                No Label
None            2001:AAAA:AAAA::24/126  \
                0                       Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::28/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                No Label
None            2001:AAAA:AAAA::28/126  \
                0                       Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::2C/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                No Label
None            2001:AAAA:AAAA::2C/126  \
                0                       Punt
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::30/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                No Label
None            2001:AAAA:AAAA::30/126  \
                0                       Fa0/0           FE80::C802:13FF:FE9C:8
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::34/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::38/126
                Outgoing  Prefix        Bytes
Local           Label                   Outgoing        Next Hop
Label           Label     or Tunnel Id  Switched        interface
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::60/126
```

```
                Outgoing   Prefix          Bytes
Local           Label                      Outgoing        Next Hop
Label           Label      or Tunnel Id    Switched        interface
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::64/126
                Outgoing   Prefix          Bytes
Local           Label                      Outgoing        Next Hop
Label           Label      or Tunnel Id    Switched        interface
                mpls forwarding-table
R1#show         2001:AAAA:AAAA::68/126
                Outgoing   Prefix          Bytes
Local           Label                      Outgoing        Next Hop
Label           Label      or Tunnel Id    Switched        interface
R1#
```

```
R1#show
mpls
memory
Allo        cator-Name                  In-use/Allocated        Count
----        ----------                  ----------------        -----     -----
LDP:        Cap Block           :       240/0       0%      [    10]    Chunk
LDP:        Cap CCB Block       :       48/0        0%      [     2]    Chunk
LDP:        Cap LCB Block       :       28/144      -19%    [     1]    Chunk
LDP:        LDP LSR addrinf     :       216/0       0%      [     6]    Chunk
            LDP Message TLV
LDP:        Indi                :       0/0         0%      [     0]    Chunk
LDP:        LDP Session DB Entry:       88/0        0%      [     2]    Chunk
LDP:        LDP TCB info        :       80/0        0%      [     2]    Chunk
LDP:        LDP peer addrinf    :       240/0       0%      [     6]    Chunk
LDP:        LDP swidb           :       780/1092    -71%    [     6]
LDP:        TAGCON peer         :       704/808     -87%    [     2]
LDP:        TDP adjacency       :       344/448     -76%    [     2]
LDP:        TDP context block   :       304/356     -85%    [     1]
LDP:        TDP interface       :       224/432     -51%    [     4]
LDP:        TDP large PIE chunk :       0/0         0%      [     0]    Chunk
LDP:        TDP max PIE chunk   :       0/0         0%      [     0]    Chunk
LDP:        TDP ptcl adj        :       432/536     -80%    [     2]
LDP:        TDP small PIE chunk :       0/0         0%      [     0]    Chunk
LDP:        TIB RB binding array:       2520/3508   -71%    [    19]
LDP:        TIB RB binding info :       652/1640    -39%    [    19]
LDP:        TIB adv bmap        :       572/1560    -36%    [    19]
LDP:        TIB entry           :       3952/152    (2600%  ) [    19    ] Chunk
LDP:        Tagcon peer uid tabl:       68/120      -56%    [     1]
LDP:        local addr table    :       64/116      -55%    [     1]
LFD:        AToM pwid           :       0/0         0%      [     0]    Chunk
LFD:        FIB feature         :       480/2484    -19%    [    15]    Chunk
LFD:        LTE                 :       1088/864    -125%   [    16]    Chunk
LFD:        LT_WALK             :       0/0         0%      [     0]    Chunk
LFD:        non-IP info         :       480/432     -111%   [     4]    Chunk
LSD:        intf                :       1440/0      0%      [     6]    Chunk
```

```
LSD:  label tbl   :  768/576   -133%  [  16]  Chunk
LSD:  label tbl   :  84/0      0%     [   1]  Chunk
MFI:  Clnt CMsg   :  0/0       0%     [   0]  Chunk
MFI:  Clnt SMsg   :  87616/0   0%     [   4]  Chunk
MFI:  Frr intf Q  :  0/1132    0%     [   0]  Chunk
MFI:  InfoReq     :  0/0       0%     [   0]  Chunk
MFI:  InfoRply    :  0/0       0%     [   0]  Chunk
MFI:  vrf table info  :  0/0   0%     [   0]  Chunk

Tota  l allocated: 0.015 Mb,  16 Kb, 16400 bytes
R1#
```

Hasta este momento tenemos habilitado MPLS en los enrutadores y en todas las interfaces del mismo modo tenemos habilitada la ingeniería de tráfico, finalmente hemos corroborado que todo este funcionado correctamente, este es el momento para permitir la configuración de MPSL-TE.

```
R1#
R1#configure terminal
R1(config)#interface tunnel 10
R1(config-if)#
R1(config-if)#ip unnumbered FastEthernet1/1
R1(config-if)#ip load-sharing per-packet
R1(config-if)#tunnel mode mpls traffic-eng
R1(config-if)#tunnel destination 10.0.4.1
R1(config-if)#tunnel mpls traffic-eng autoroute announce
R1(config-if)#tunnel mpls traffic-eng priority 1 1
R1(config-if)#tunnel mpls traffic-eng bandwidth 1500
R1(config-if)#tunnel mpls traffic-eng path-option 1 explicit name ruta10
R1(config-if)#tunnel mpls traffic-eng load-share 10
R1(config-if)# exit
```

Procedemos a crear nuestro path con el destino especificado

```
R1(config)#ip explicit-path name ruta10 enable
R1(cfg-ip-expl-path)#next-address 172.16.0.14
R1(cfg-ip-expl-path)#next-address 172.16.0.18
R1(cfg-ip-expl-path)#next-address 172.16.0.22
```

Procedemos a verificar que nuestro túnel de ingeniería de tráfico MPLS se encuentre administrativamente arriba, operacionalmente en línea, el destino sea alcanzable y el path sea válido.

Disponemos de los siguientes comandos de verificación:

```
R1#show mpls traffic-eng?
auto-tunnel                 Automatically created tunnel interfaces
Autoroute                   Autorouted tunnel destination information
Exp                         MPLS traffic-eng tunnel exp information
fast-reroute                Fast Reroute information
forwarding-adjacency        forwarding-adjacency tunnel destination information
link-management             Link Management information
Lsp                         Show LSP information
Topology                    Show topology Commands
Tunnels                     MPLS traffic-eng tunnel status

R1#show mpls traffic-eng
```

Nota.- Resaltaremos las líneas que nos muestran el resultado de lo anteriormente descrito que debemos verificar.

```
R1#show mpls traffic-eng tunnels

Name: R1_t10                          (Tunnel10) Destination: 10.0.4.1
Status:
Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit ruta10 (Basis for Setup, path weight 4)

Config Parameters:
    Bandwidth: 1500     kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 10
auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


InLabel  :  -
  OutLabel : FastEthernet0/1, 17
  RSVP Signalling Info:
       Src 10.0.1.1, Dst 10.0.4.1, Tun_Id 10, Tun_Instance 16
RSVP Path Info:
      My Address: 172.16.0.13
      Explicit Route: 172.16.0.14 172.16.0.17 172.16.0.18 172.16.0.21
                    172.16.0.22 172.16.0.25 172.16.0.26 10.0.4.1
      Record   Route:   NONE
      Tspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
```

```
RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
History:
   Tunnel:
      Time since created: 50 minutes, 17 seconds
      Time since path change: 49 minutes, 13 seconds
      Number of LSP IDs (Tun_Instances) used: 16
Current LSP:
      Uptime: 49 minutes, 13 seconds

Name: R1_t12                          (Tunnel12) Destination: 10.0.4.1
Status:
Admin: up         Oper: up     Path: valid       Signalling: connected
   path option 1, type explicit ruta12 (Basis for Setup, path weight 3)

Config Parameters:
   Bandwidth: 1500     kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
Metric Type: TE (default)
   AutoRoute:  enabled   LockDown: disabled  Loadshare: 12
auto-bw: disabled
  Active Path Option Parameters:
   State: explicit path option 1 is active
   BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled

InLabel  :  -
  OutLabel : FastEthernet0/0, 24
  RSVP Signalling Info:
       Src 10.0.1.1, Dst 10.0.4.1, Tun_Id 12, Tun_Instance 10
RSVP Path Info:
      My Address: 172.16.0.1
      Explicit Route: 172.16.0.2 172.16.0.5 172.16.0.6 172.16.0.9
                  172.16.0.10 10.0.4.1
      Record   Route:   NONE
      Tspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
History:
   Tunnel:
      Time since created: 50 minutes, 17 seconds
      Time since path change: 49 minutes, 22 seconds
      Number of LSP IDs (Tun_Instances) used: 10
Current LSP:
      Uptime: 49 minutes, 22 seconds
```

```
LSP Tunnel R4_t11 is signalled, connection is up
InLabel  : FastEthernet0/1, implicit-null
 OutLabel :  -
 RSVP Signalling Info:
      Src 10.0.4.1, Dst 10.0.1.1, Tun_Id 11, Tun_Instance 24
RSVP Path Info:
     My Address: 10.0.1.1
     Explicit Route:  NONE
     Record   Route:   NONE
     Tspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
RSVP Resv Info:
     Record   Route:   NONE
     Fspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits

LSP Tunnel R4_t13 is signalled, connection is up
InLabel  : FastEthernet0/0, implicit-null
 OutLabel :  -
 RSVP Signalling Info:
     Src 10.0.4.1, Dst 10.0.1.1, Tun_Id 13, Tun_Instance 18
RSVP Path Info:
     My Address: 10.0.1.1
     Explicit Route:  NONE
     Record   Route:   NONE
     Tspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
RSVP Resv Info:
     Record   Route:   NONE
     Fspec: ave rate=1500 kbits, burst=1000 bytes, peak rate=1500 kbits
R1#
```

```
R1#show mpls traffic-eng autoroute
MPLS TE autorouting enabled
 destination 10.0.4.1, area ospf 10  area 10, has 2 tunnels
   Tunnel12    (load balancing metric 166666666, nexthop 10.0.4.1)
(flags: Announce)
   Tunnel10    (load balancing metric 200000000, nexthop 10.0.4.1)
(flags: Announce)
R1#
```

```
R1#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel            In-label Out intf/label            FRR intf/label Status

LSP midpoint frr information:
LSP identifier              In-label Out intf/label            FRR intf/label Status
```

```
R1#
R1#show mpls traffic-eng topology path tunnel
10
Query Parameters:
Destination: 10.0.4.1
Bandwidth: 1500
Priorities: 1 (setup), 1 (hold)
Affinity: 0x0 (value), 0xFFFF (mask)
Query Results:
Min Bandwidth Along Path: 6500 (kbps)
Max Bandwidth Along Path: 6500 (kbps)


                                    : affinity                  6500
Hop  0: 172.16.0.1                  00000000,       bandwidth   (kbps)
                                    : affinity                  6500
Hop  1: 172.16.0.2                  00000000,       bandwidth   (kbps)
                                    : affinity                  6500
Hop  2: 172.16.0.5                  00000000,       bandwidth   (kbps)
                                    : affinity                  6500
Hop  3: 172.16.0.6                  00000000,       bandwidth   (kbps)
                                    : affinity                  6500
Hop  4: 172.16.0.9                  00000000,       bandwidth   (kbps)
                                    : affinity                  6500
Hop  5: 172.16.0.10                 00000000,       bandwidth   (kbps)
Hop  6: 10.0.4.1
R1#
```

```
R1#show mpls traffic-eng topology path
destination                         10.0.4.1
Query Parameters:
Destination: 10.0.4.1
Bandwidth: 0
Priorities: 0 (setup), 0 (hold)
Affinity: 0x0 (value), 0xFFFFFFFF (mask)
Query Results:
Min Bandwidth Along Path: 8000 (kbps)
Max Bandwidth Along Path: 8000 (kbps)
                                    : affinity
Hop  0: 172.16.0.1                  00000000,       bandwidth   8000 (kbps)
                                    : affinity
Hop  1: 172.16.0.2                  00000000,       bandwidth   8000 (kbps)
                                    : affinity
Hop  2: 172.16.0.5                  00000000,       bandwidth   8000 (kbps)
                                    : affinity
Hop  3: 172.16.0.6                  00000000,       bandwidth   8000 (kbps)
                                    : affinity
Hop  4: 172.16.0.9                  00000000,       bandwidth   8000 (kbps)
                                    : affinity
Hop  5: 172.16.0.10                 00000000,       bandwidth   8000 (kbps)
Hop  6: 10.0.4.1
R1#
```

d) Pruebas: Introducción a las pruebas del software; Técnicas de prueba; Documentación del proceso de prueba del software; Otras técnicas de verificación y validación.

Con la finalidad de poder analizar el rendimiento en las comunicaciones en base a los cambios aplicados tomaremos muestras de ambos modelos simulados e iremos interpretando cada uno de ellos, se efectuaron pruebas de stress en los enlaces de la red corporativa del proveedor, para denostar la eficiencia de la ingeniería de tráfico, en colaboración con la reserva de recursos, pruebas de ping, se efectuó un ping con 500 paquetes enviados, con un tamaño de 1000 bytes cabe señalar que todas las pruebas se efectuaron desde la sede principal con destino a las sedes remotas.

Pruebas de ping en un enlace con enrutamiento tradicional

AbonadoAP con destino Abonado_AS:

```
Abonado_AP#ping 2001:BBBB:AAAA::101 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::101, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 44/105/236 ms
Abonado_AP#
```

Pruebas de ping en un enlace con enrutamiento tradicional

AbonadoBP con destino Abonado_BS:

```
Abonado_BP#ping 2001:BBBB:AAAA::301 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::301, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 28/88/200 ms
Abonado_BP#
```

Pruebas de ping en un enlace con enrutamiento tradicional

AbonadoCP con destino Abonado_CS:

```
Abonado_CP#ping 2001:BBBB:AAAA::501 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::501, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 56/123/312 ms
Abonado_CP#
```

Así mismo si nos apoyamos con la herramienta WireShark para realizar un sniffer al estado del enlace del router 1 y el router 5 podemos apreciar que no presenta tráfico alguno de los paquetes ICMP enviados por los tres abonados, quedando subutilizada esta conexión.

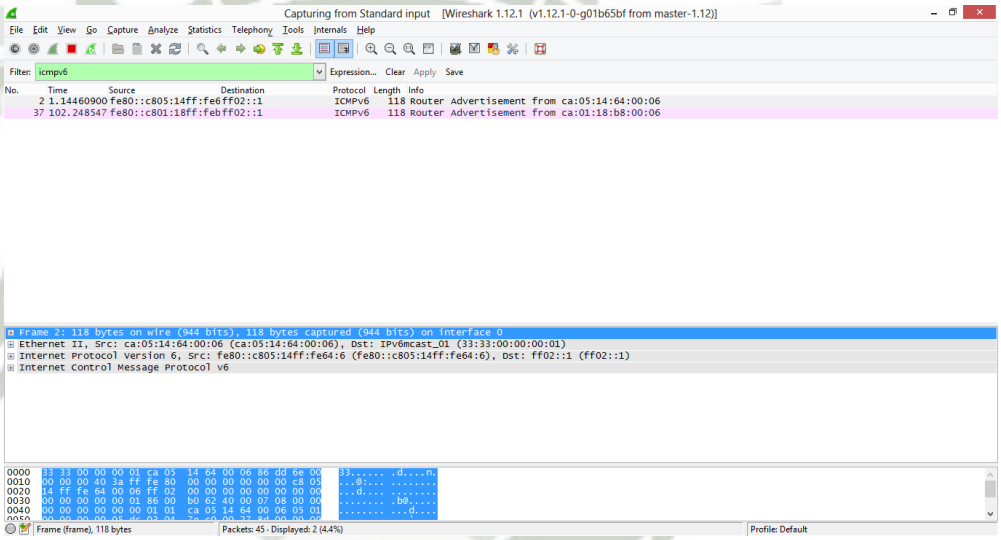

Gráfico Nº 12. **Captura de tráfico entre R1-R5**

Fuente**: Elaboración propia**

Todo el tráfico está fluyendo a través del enlace disponible entre R1 y R2 como se muestra en la siguiente gráfica.

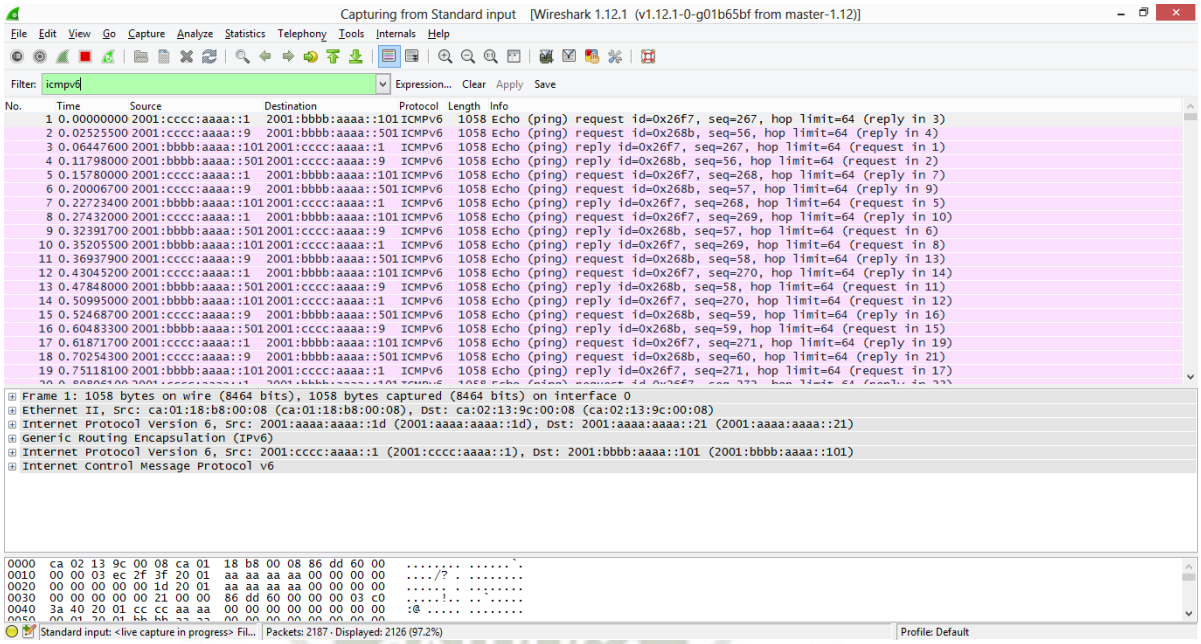

Gráfico Nº 13. Captura de tráfico entre R1-R2

Fuente: **Elaboración propia**

Ahora procedemos a efectuar la misma prueba de stress para medir el rendimiento obtenido con la ayuda de la tecnología de conmutación de etiquetas MPLS, haciendo uso de reservas a través del protocolo RSVP, empleado Ingeniería de Tráfico. Para ofrecer un servicio de calidad garantizada al enlace de la conexión VPN del Abonado_C.

Pruebas de ping en un enlace con enrutamiento MPLS-Te

AbonadoAP con destino Abonado_AS:

Abonado_AP#ping 2001:BBBB:AAAA::101 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::101, timeout is 2 seconds:
!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 44/83/152 ms
Abonado_AP#

Pruebas de ping en un enlace con enrutamiento MPLS-Te

AbonadoBP con destino Abonado_BS:

Abonado_BP#ping 2001:BBBB:AAAA::301 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::301, timeout is 2 seconds:
!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 40/67/116 ms
Abonado_BP#

Pruebas de ping en un enlace con enrutamiento MPLS-Te

AbonadoCP con destino Abonado_CS:

Abonado_CP#ping 2001:BBBB:AAAA::501 size 1000 repeat 500
Type escape sequence to abort.
Sending 500, 1000-byte ICMP Echos to 2001:BBBB:AAAA::501, timeout is 2 seconds:
!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 48/93/188 ms
Abonado_CP#

Del mismo modo que anterior procedemos a realizar una Sniffer al estado de la conexión entre el router R1 y R5, logrando los siguientes resultados, existe tráfico únicamente entre las redes privadas que conforman la conexión VPN del Abonado_C dirección origen 10.10.0.9 con destino 192.168.5.1 y viceversa.

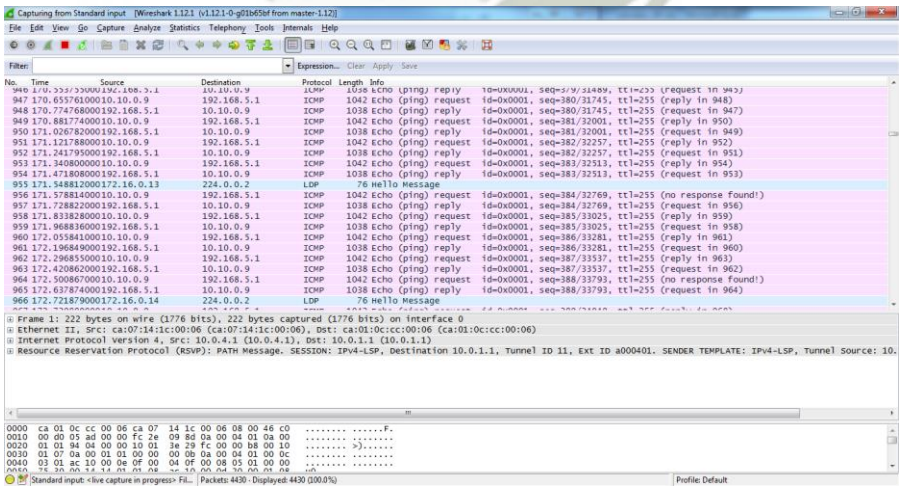

Gráfico Nº 14. **Captura de tráfico entre R1-R5**

Fuente**: Elaboración propia**

No se utiliza en ningún momento el enlace congestionado entre los enrutadores R1 y R2, puesto que nuestro Túnel MPLS posee una ruta explicita para alcanzar nuestro destino.

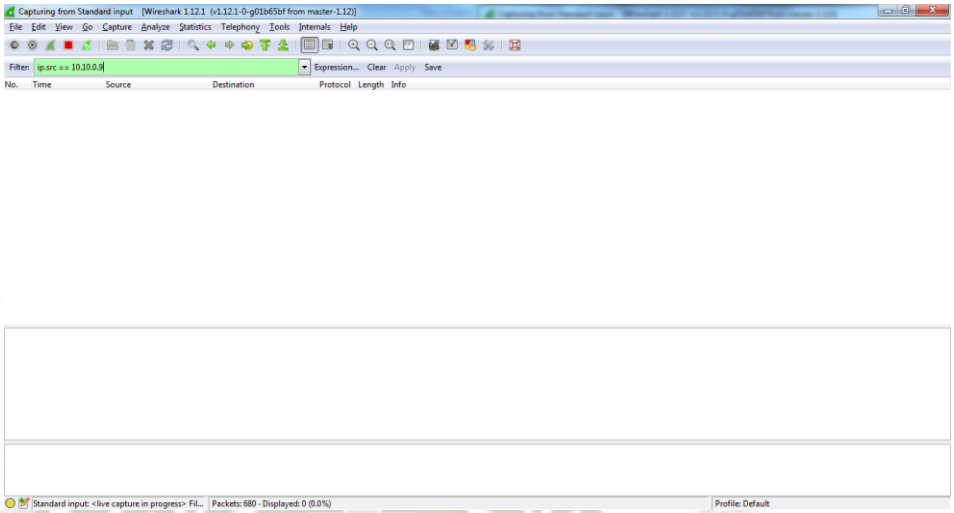

Gráfico Nº 15. **Captura de tráfico entre R1-R2**

Fuente**: Elaboración propia**

Análisis comparativo para los enlaces del Abonado_A

Podemos apreciar una pequeña descongestión en las líneas de comunicaciones para este abonado, el tráfico generado por el Abonado_C, ya no fluye por este camino.

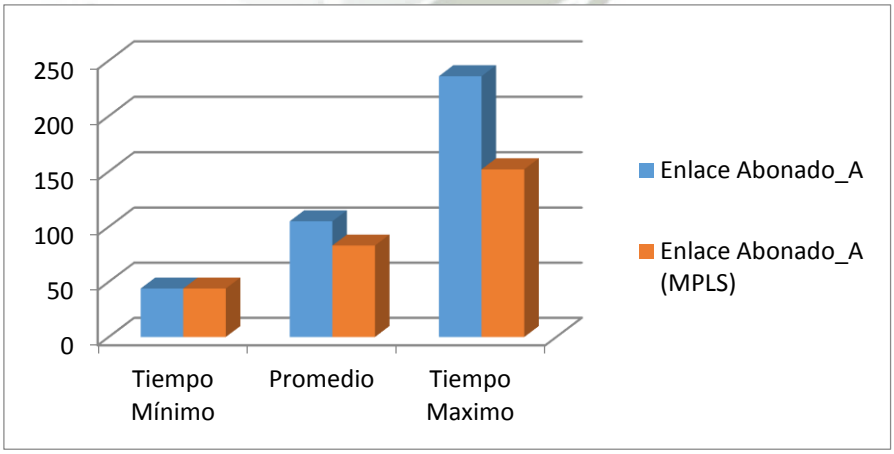

Gráfico Nº 16. **Cuadro comparativo para los enlaces del Abonado_A**

Fuente: **Elaboración propia**

Análisis comparativo para los enlaces del Abonado_B

Del mismo modo que el anterior se aprecia una descongestión en las líneas de comunicaciones para este abonado, el tráfico generado por el Abonado_C, ya no fluye por este camino.

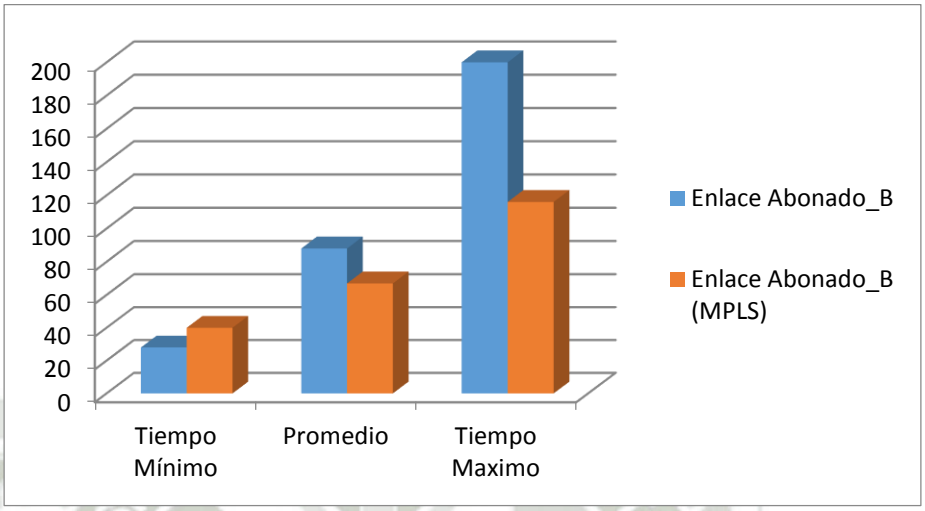

Gráfico Nº 17. **Cuadro comparativo para los enlaces del Abonado_B**

Fuente: **Elaboración propia**

Análisis comparativo para los enlaces del Abonado_C

Con este cliente se está aplicando ingeniería de tráfico, se observa notablemente una mejora sustancial de 124 milisegundos en sus líneas de comunicaciones aplicando MPLS.

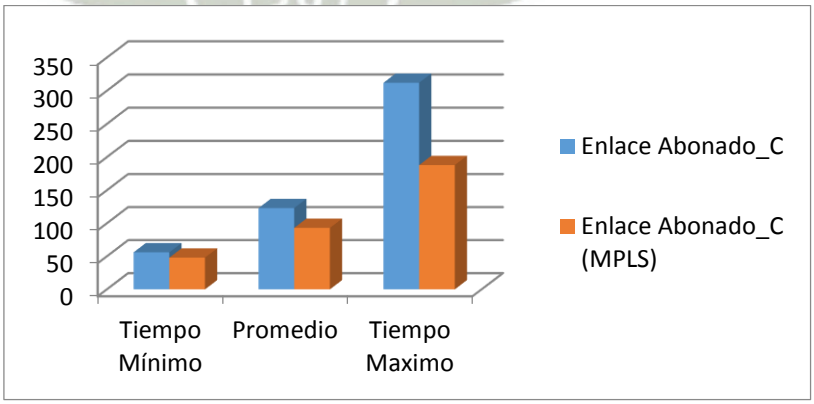

Gráfico Nº 18. **Cuadro comparativo para los enlaces del Abonado_C**

Fuente: **Elaboración propia**

Por último tenemos un cuadro comparativo de los tres abonados.

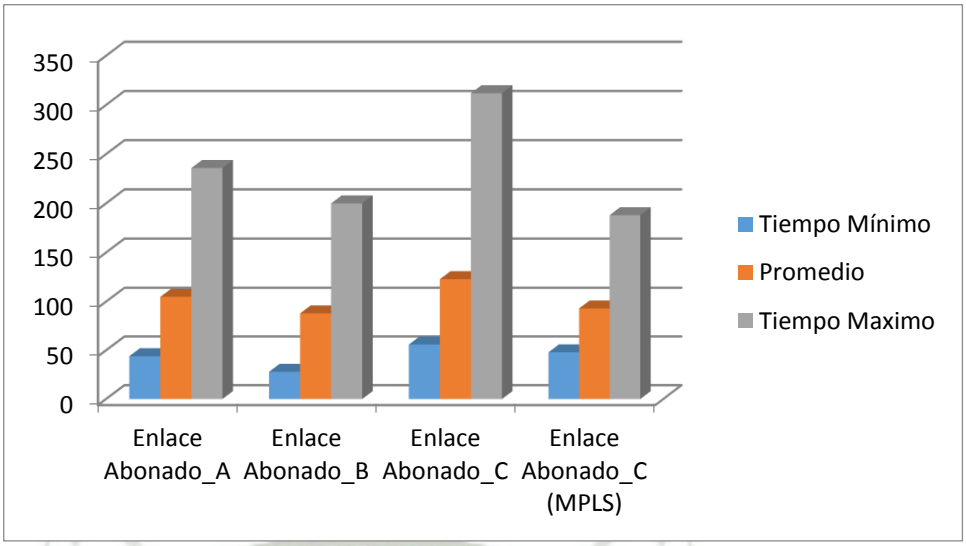

Gráfico Nº 19. **Cuadro comparativo de los tres abonados**

Fuente**: Elaboración propia**

Logrando aplicar esta tecnología logramos mejorar los tiempos de respuesta para nuestros enlaces según cuadro adjunto.

	Promedio red estándar en milisegundos	Promedio red MPLS en milisegundos	Mejora en milisegundos
Abonado_A	115	83	32
Abonado_B	98	67	31
Enlace Abonado_C (MPLS)	133	93	40

Gráfico Nº 20. Cuadro promedio mejora de tiempos

Fuente: **Elaboración propia**

Pruebas de stress realizadas con un tamaño de paquete de 3000 bytes con 2000 paquetes enviados

	Promedio red estándar en milisegundos	Promedio red MPLS en milisegundos	Mejora en milisegundos
Abonado_A	900	645	255
Abonado_B	760	530	230
Enlace Abonado_C (MPLS)	1020	610	410

Gráfico Nº 21. **Cuadro promedio muestra la mejora en milisegundos**

Fuente: **Elaboración propia**

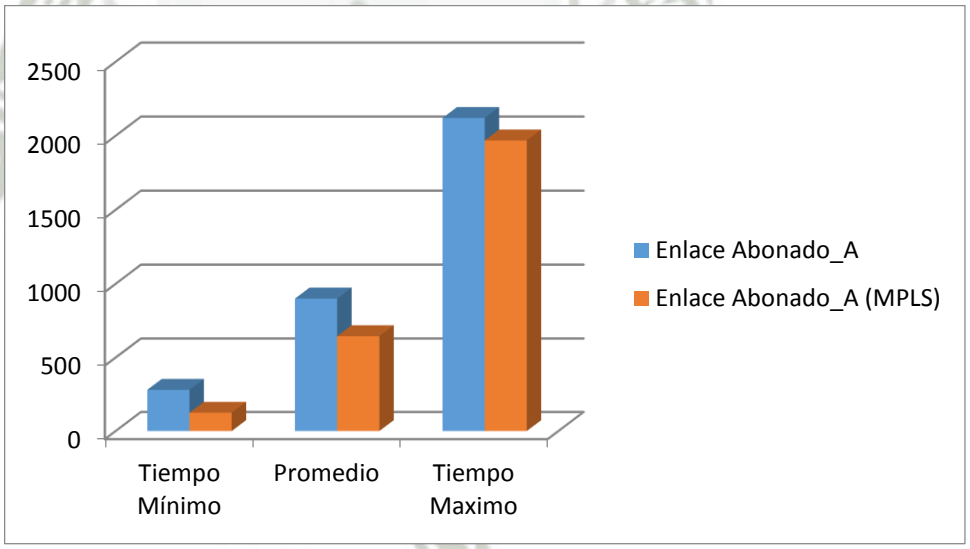

Gráfico Nº 22. **Cuadro comparativo para el Abonado_A**

Fuente: **Elaboración propia**

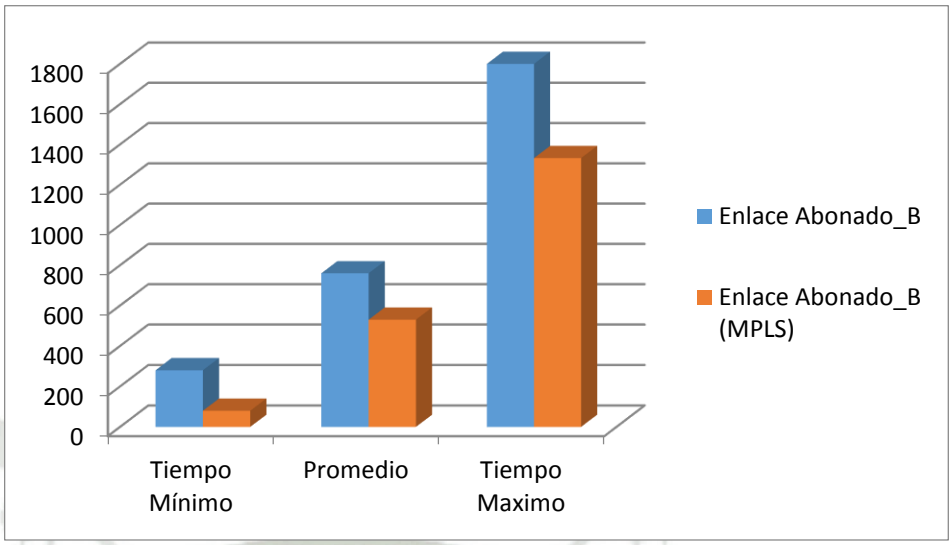

Gráfico Nº 23. **Cuadro comparativo para el Abonado_B**

Fuente: **Elaboración propia**

Cuadro comparativo general muestra la mejora del abonado C con MPLS

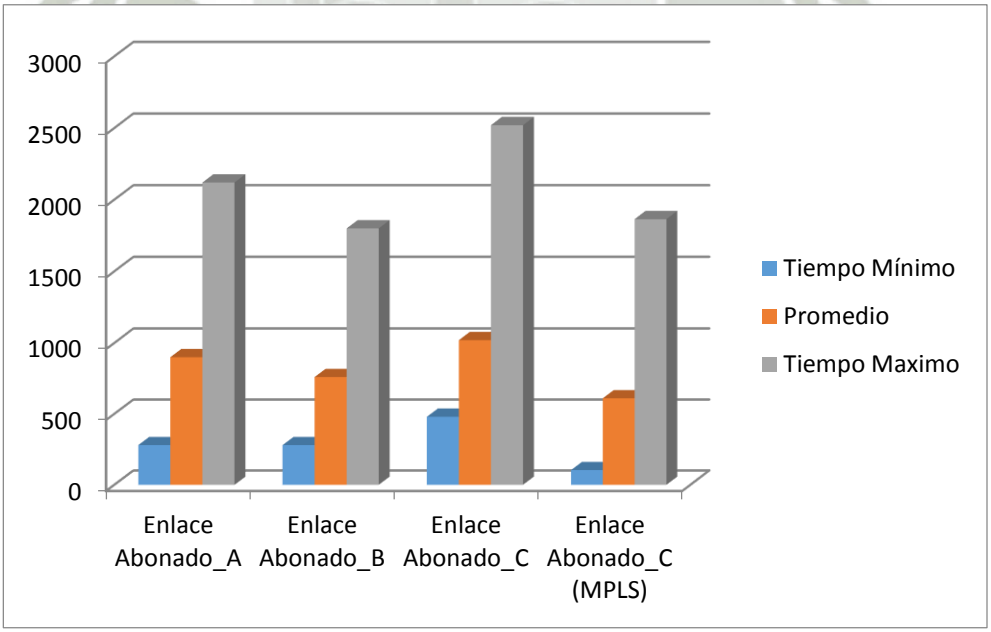

Gráfico Nº 24. **Cuadro general de mejoría del Abonado_C con MPLS**

Fuente: **Elaboración propia**

Haciendo uso de la herramienta WireShark realizamos un análisis del tráfico suscitado en el router 1 con destino al router 2 y al router 5.

Podemos apreciar que nuestros túneles MPLS construidos están realizando un balanceo de cargas al utilizar los dos enlaces disponibles del mismo modo tenemos habilitado la alta disponibilidad para la comunicación en caso que llegara a fallar un túnel el trafico MPLS es enrutado por el túnel de respaldo.

Captura de tráfico entre el router 1 y el router 2

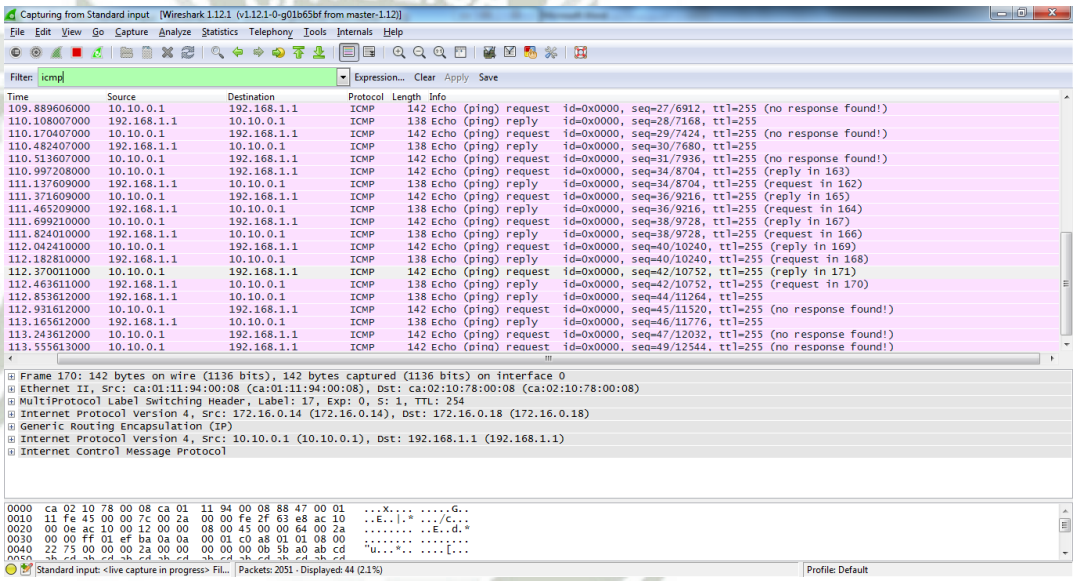

Gráfico Nº 25. **Captura de tráfico entre el router 1 y el router 2**

Fuente: **Elaboración propia**

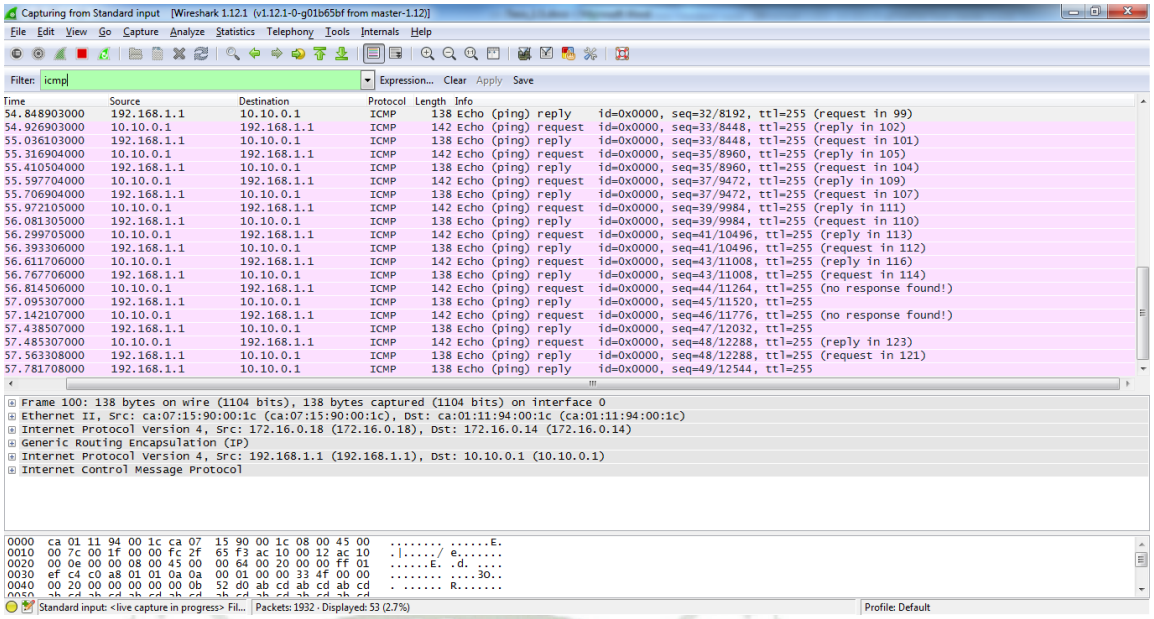

Gráfico N° 26. **Captura de tráfico entre el router 1 y el router 5**

Fuente: **Elaboración propia**

6.2. Conclusión general de la simulación

Según la información que hemos logrado recabar producto de la simulación realizada se puede apreciar una mejora en las ráfagas de tiempo de las comunicaciones sobre todo al reducir los picos elevados de tráfico que es donde se genera la latencia en las comunicaciones, esto se puede apreciar sustancialmente en el tráfico de voz (UDP) puesto que es una ráfaga continua de datos que fluyen por la red y deben ser enrutados sin problemas de congestión.

Para efectos de resultados se utilizó el software de simulación GNS3 y se recreó la red, por limitantes del producto nuestras pruebas se basan en él envío de paquetes ICMP. Se logró una mejora en promedio de 94 milisegundos para el envío constante de 500 paquetes, con un tamaño de 1000 bytes.

Tenemos conocimiento que ya se está aplicando esta tecnología en nuestra ciudad tal es el caso de la compañía Misticom es una empresa peruana de telecomunicaciones que utilizan una red MPLS Cuenta con redes en Lima, Cusco,

Tacna, Chincha, Ica, Juliaca, Puno, Arequipa, y Moquegua. http://misticom.com/somos.html.

7. PLAN DE TRABAJO

Tabla N° 10. **Plan de Trabajo**

NOMBRE DE LA TAREA	DURACION
FORMULACION DEL PROBLEMA	6 días
DETERMINACION DE OBJETIVOS	2 días
ELABORACION DEL PLAN DE TESIS	5 días
PRESENTACION DEL PLAN DE TESIS	1 día
INVESTIGACION TEORICA: CAP. I	15 días
INVESTIGACION TEORICA: CAP. II	15 días
INVESTIGACION TEORICA: CAP. III	15 días
PROPUESTA DE METRICAS	30 días
COMPROBACION DE LA PROPUESTA	30 días
CONCLUSIONES Y RECOMENDACIONES	2 días
PRUEBAS DE EVALUACION	20 días
REDACCIÓN, REVISIÓN Y DEPURACIÓN	3 días
IMPRESIÓN Y ENTREGA DE EJEMPLARES	2 días

Fuente: Elaboración propia

CONCLUSIONES

1. Se realizó la implantación de MPLS en las interfaces de los enrutadores así mismo realizó la habilitación de los túneles MPLS-TE.

2. Antes de aplicar RSVP debe existir un análisis previo entre el ancho de banda disponible y la solicitud de reserva. En nuestro caso aplicamos una reserva de 8000 kbps para cuatro túneles de 1500 kbps, la reserva de los TUNELES-TE no pueden superar a la reserva definida en los enlaces.

3. La Ingeniería de tráfico (TE), permite el establecimiento de los LSP como tuberías de explícitos anchos de banda entre dos puntos utilizando rutas preestablecidas optimizando el performance de los enlaces de comunicaciones.

4. En una red habilitada con MPLS y RSVP los paquetes son identificados, separa el tráfico en diferentes clases, descartando los paquetes mal formados para garantizar la integridad de la red, marca el tráfico, asigna el valor que le corresponde, prioriza protege y aísla el tráfico, llevando un control de la ráfagas que lo conforman.

   Al habilitar un túnel de ingeniería de tráfico se mejoramos notablemente la calidad de servicio del abonado_AP con destino abonadoAS.

5. La Ingeniería del Trafico (TE) no necesita calcular las rutas, brinda mayor confiabilidad en caso de fallas utilizando su capacidad FAST REROUTE (FRR); que permite el uso de rutas alternas definidas.

6. Se observa mejoras en el acceso para cada uno de los enlaces de prueba habilitados, en nuestro caso simulado de logró una mejora entre 22, 21 y 30ms para el envío de 500 paquetes ICMPV6 con un tamaño de 1500 bytes.

7. La simulación permitirá que los proveedores de servicios cuenten con una plataforma versátil para introducir nuevos servicios de valor agregado tales como videoconferencia y mensajes unificados, del mismo modo los proveedores de

servicios de internet (ISP) pueden mejorar sus márgenes de ganancias al introducir MPLS para brindar un valor agregado y distinguirse de sus competidores.

RECOMENDACIONES

1. Según las características específicas de las cuales disponen algunas redes se deben adoptar incuestionables parámetros de configuración para logar una correcta migración a la arquitectura MPLS
2. Realizar la actualización del IOS en los enrutadores de ser necesario para que estos soporten la tecnología MPLS, teniendo en cuenta los requisitos técnicos antes de efectuar la actualización.
3. Efectuar la simulación de este proyecto en un ambiente de laboratorio con equipos reales antes de salir a producción, según la versión de IOS del router puede variar la configuración del mismo.
4. En casos reales, efectuar el análisis, diseño y configuración de los protocolos de enrutamiento, que deberá trabajar y soportar la nueva tecnología
5. Realizar la migración en forma parcial de la red, certificar la estabilidad. Validar que los enrutadores sean capaces de enviar paquetes etiquetados con los encabezados MPLS. Antes de habilitar los trabajos de migración de debe tomar muestras de rendimiento de los equipos y las líneas de comunicación en momentos bajos medios y altos de tráfico, esta información recopilada servirá para detectar algún comportamiento desfavorable durante la migración.
6. Se recomienda operar con paquetes con carga útil de datos de más de 65.355 bytes para verificar la no fragmentación en los routers alineados a 64 bits y con una cabecera de longitud fija, más simple, y probar que agiliza su procesado.

REFERENCIAS BIBLIOGRAFICAS

Barberá, J. (2000). MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Madrid, España: Actas del V Congreso de Usuarios de Internet. Mundo Internet.

Blake , S. (diciembre de 1998). An Arquitecture for differentiated services RFC 2475 DICIEMBRE 1998.

Braden , R. (1994). Integrated Services In the internet arquitectura an Overview RFC.

Corral, G., & Abella, J. (1997). ADSL y MPLS. Madrid - España: Editorial Ingeniería La Salle.

Cuevas Casado , A. (2006). Contribución al desarrollo de soluciones para la integración de métodos de establecimiento de sesión en redes 4G. Madrid: Tesis para optar el grado de doctor, Universidad Carlos III de Madrid.

García Tomas, J., Raya Cabrera, J. L., & Rodrigo Raya, V. (2002). Alta velocidad y calidad de servicio en redes IP. Madrid : Primera Edición Ra-ma.

Guevara, A. (s.f.). Nivel de Desmpeño en Redes IPv4 con respect a redes IPv6 con MPLS y RSVP.

Guevara, A., & Cuevas Casado , A. (2010). Nivel de Desempeño en Redes IPv4 con respecto a redes IPv6 con MPLS y RSVP. Bogota.

Hinojosa, M., & Herrera, F. (2009). Diseño de una red MPLS utilizando el protocol IPv6 para proveedores de servicios de telecomunicaciones. Quito: Julio.

Leon-Garcia , A., & Widjaja, I. (2001). Communication Newtworks. McGraw Hill.

Ojeda, G. A., & Carrión, D. A. (Noviembre 2011). Identificación y levantamiento de las plataformas de gestión y monitoreo para la elaboración de un manual de usuario que será utilizado en la aplicación y ejecución de procesos en la red backbone IP/MPLS de la Corporación Nacional de Telecomuniaciones. Quito.

Ortega, B., & Torres, J. (s.f.). Analisis, Diseño de una red MPLS con IPV6 en las UTICS de la escuela politecnica del ejercito. Ecuador.

ANEXO 1: Glosario de términos

ATM: Asyncronous Transfer Mode. Modo de Transferencia Asíncrona.

BackBone: Conexión de alta velocidad dentro una red que interconecta los principales sitios de la Internet.

BGP: Border Gateway Protocol. Protocolo de Intercambio de Borde.

Capa 2 o de Enlace de Datos: Capa 2 del modelo de referencia OSI. Proporciona tránsito confiable de datos a través de un enlace físico.

Capa 3 o de Red: Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

CBR: Constraint-based Routing. Enrutamiento basado en restricciones

CoS: Class of Service. Clases de Servicio

DWDM: Dense Wavelength Division Multiplexing. División de Multiplexaje por Largo de Onda.

EIGRP: Enhanced Interior Gateway Routing Protocol. Protocolo de Puerta de enrutamiento mejorado

EGP: Exterior Gateway Protocol. Protocolo de Puerta exterior.

Etiqueta: Es un identificador corto, de longitud fija y con significado local empleado para identificar un FEC.

FEC: Forwarding Equivalence Class. Clase de Equivalencia de Reenvió.

FR: Frame Relay. Intercambio de Tramas. Una técnica de transmisión eficiente

IETF: Internet Engineering Task Force. Grupo voluntario que investiga y resuelve problemas técnicos.

IGP: Interior Gateway Protocol. Protocolo de Intercambio Interior.

IGRP: Interior Gateway Routing Protocol). Protocolo de enrutamiento de puerta de enlace interior.

IP: Internet Protocol. Protocolo De Internet.

IPsec: Internet Protocol Security. Protocolo de Internet Seguro.

ISP: Internet Service Provider. Proveedor de servicios de internet

LAN: Local Área Network. Red De Área Local.

LDP: Label Distribution Protocol. Protocolo de Distribución de Etiquetas.

LER: Label Edge Router. Router de Etiqueta de Borde.

LSP: Label Switched Path. Camino de Intercambio de Etiquetas.

LSR: Label Switching Router. Enrutador de Intercambio de Etiquetas.

MPLS: Multi-Protocol Label Switching. Intercambio De Etiquetas Multiprotocolares.

NSP: Network Service Provider. Proveedor de Servicio de Red.

OSI, Modelo de referencia: Open Systems Interconnection o Interconexión de Sistemas Abiertos.

OSPF: Open Shortest Path First. El primer camino más corto.

PPP: Point to Point Protocol. Protocolo Punto a Punto. Protocolo que le permite a un computador el uso de protocolos TCP/IP.

PVC: Permanent Virtual Circuit. Circuito Virtual Permanente.

QoS: (Quality of Service). Calidad de servicio.

RSVP: Resource Reservation Protocol. Protocolo de Reservación de Recursos.

SDH: Synchronous Digital Hierarchy. Jerarquia Digital Síncrona.

SONET: Syncronous Optical Network. Red Óptica Síncrona.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protocolo para Control de Trasmisión/protocolo Inter red.

TE: Traffic Engineering. Ingeniería de tráfico.

TTL: Time-To-Live. Es un campo dentro del encabezado IP que indica el tiempo de vida del paquete cuando este viaja por la red.

VPN: Virtual Private Network. Red Privada Virtual.

WAN: Wide Area Network. Red de Area Amplia.