PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

RÁPIDA RECONVERGENCIA EN LA INGENIERÍA DE TRÁFICO APLICADA A UN ESCENARIO MPLS VPN

Tesis para optar el grado de Magíster en Ingeniería de las Telecomunicaciones que presenta

DANIEL ROJAS HUAMANI

Dirigido por

MS. ANTONIO OCAMPO ZUÑIGA

Jurado

DR. CARLOS BERNARDINO SILVA CARDENAS

MS. JUAN CARLOS ORTEGA ULLOA

San Miguel, 2015

AGRADECIMIENTO

Al padre Dios, por todo el sostén brindado lo largo de mi existencia y a la Virgen María por guardarme siempre.

INDICE

GLOSARIO

APS: Automatic Protection Switching

ATM: Asynchronous Transfer Mode

BFD: Bi-directional Forwarding Detection

CEF: Cisco Express Forwarding

CSR: Cloud Services Router

FR: Frame Relay

IGP: Interior Gateway Protocol

IOS: Internetworking Operating System

IP: Internet Protocol

IP FRR: Internet Protocol Fast ReRoute

ISPF: Incremental Shortest Path First

LSA: Link State Advertisement

LSP: Label Switched Path

LSR: Label Switching Router

MPLS: Multi Protocol Label Switching

MPLS TE: Multi Protocol Label Switching Traffic Engineering

MPLS TE TUNNEL: Multi Protocol Label Switching Traffic Engineering Tunnel

OSI: Open Standard Internacional

OSPF: Open Shortest Path First

OSPF TE: Open Shortest Path First Traffic Engineering

PCALC: Path Calculation Algorithm

POS: Packet Over SONET

PSTN: Public Switching Telephony Network

RIB: Routing Information Base

RSVP TE: Resource Reservation Protocol Traffic Engineering

SPF: Shortest Path First

TE: Traffic Engineering

VOIP: Voz Internet Protocol

RESUMEN

Con la tendencia actual de transportar cualquier tipo de tráfico sobre IP (datos, voz, video, etc.), el desarrollo tecnológico se orienta a concretar dicho transporte imponiendo IP sobre MPLS, asimismo con la finalidad de obtener un tiempo de reconvergencia de decenas o centenas de milisegundos en la red de núcleo de un proveedor de servicios que ha experimentado una falla en un enlace entre dos enrutadores, se despliegan enlaces ópticos y equipamiento adicional de respaldo para cada enlace a proteger, incluyendo interfaces y tarjetas. Ocurrida la falla de un enlace en la red de núcleo de un proveedor de servicios, dicha red debe ser capaz de reconverger en el menor tiempo posible, lo contrario trae consigo entre otros, pérdidas económicas y la imagen de la empresa se deteriora.

La presente tesis propone simular TE/IP FRR y Optimizaciones para establecer una ruta que reserve un ancho de banda determinado, instalar una ruta y un next-hop de respaldo en la RIB y CEF de un enrutador y estimar un tiempo de reconvergencia menor a 5 segundos luego de ocurrida la falla de un enlace entre dos enrutadores, recuperándose la conectividad sin la necesidad de tener enlaces ópticos ni contar con equipamiento adicional de respaldo para la protección de los mismos.

Para alcanzar el objetivo propuesto se describen los principios de operación de las redes IP, OSPF, IP FRR, TE, MPLS y se simulan 3 topologías porque con ellas se comprueba la hipótesis propuesta. En la primera topología se simuló TE (ingeniería de tráfico), en la segunda se simuló IP FRR (rápido re-enrutamiento IP) y en la tercera topología se simuló TE/IP FRR y Optimizaciones. La finalidad de proponer diferentes topologías es mostrar la posibilidad de configurar TE o IP FRR o TE/IP FRR y Optimizaciones de manera independiente, integrando 2 de ellas o integrando los 3 conceptos en una determinada topología.

En ese orden establecido, en la tercera simulación se valida la hipótesis propuesta concatenando: ***i)*** TE; ***ii)*** TE/IP FRR; y ***iii)*** TE/IP FRR y Optimizaciones, estimando un tiempo de 3 segundos para reconverger o recuperar la conectividad en la topología analizada luego de ocurrida la falla en un enlace entre dos enrutadores. Para ello se utilizó un valor de 20 ms como temporizador de espera para generar el primer LSA luego de detectar un cambio en la topología y un valor menor o igual a 1200 ms como temporizador de espera para la primera actualización del algoritmo SPF.

INTRODUCCION

La tendencia actual de los proveedores de servicios de telecomunicaciones, es mantener y operar una sola red, la cual sea capaz de brindar cualquier servicio, a través de cualquier dispositivo móvil, portátil y/o fijo. Asimismo con la adopción y el uso global del Protocolo de Internet (IP) y las ventajas que ofrecen las redes de paquetes conmutados frente a las de circuitos conmutados, se sigue la tendencia a utilizar redes de transporte basadas en IP, como protocolo dominante en la capa 3 del modelo Internacional de Estándares Abiertos (OSI). Esto conlleva a que las redes basadas en IP, ofrezcan al menos, las mismas características de calidad y disponibilidad que ofrecen las redes de circuitos conmutados, como por ejemplo, la disponibilidad de cinco nueves al año ofrecida por la Red de Telefonía Púbica Conmutada (PSTN) [1,2].

Ofrecer con redes basadas en IP tales características, lleva a plantear escenarios en los que no necesariamente, el camino a seguir por un determinado flujo o paquetes, sea el ofrecido por una tabla de rutas construida en base a algún Protocolo de Gateway Interior (IGP), cuyo paradigma a seguir es el camino con menor métrica [3].

En ese sentido, existen tecnologías que permiten aplicar el concepto de Ingeniería de Tráfico (TE), siendo capaces de ofrecer alternativas de enrutamiento distintas a las ofrecidas por los IGPs, Multi Protocolo de Conmutación de Etiquetas (MPLS) es una de ellas, estrictamente Multi Protocolo de Conmutación de Etiquetas Ingeniería de Tráfico (MPLS TE). Adicionalmente, existen técnicas que aceleran el re-enrutamiento IP conocidas como Protocolo de Internet Rápido re-enrutamiento (IP FRR), dichas tecnologías permiten reducir el tiempo de respuesta ante la falla de un enlace o nodo en una red IP, restableciendo la conectividad y la operatividad en dicha red [3].

La presente tesis permite integrar sobre la topología de red IP analizada, la ingeniería de tráfico, el rápido re-enrutamiento IP y optimizaciones con la finalidad de establecer una ruta preferida, instalar una ruta y un enrutador de respaldo en la Base de Información de Enrutamiento (RIB) y Reenvío Rápido de Cisco (CEF) de un enrutador y restablecer la operatividad en la red ante la falla de un enlace entre dos enrutadores de la ruta establecida por TE, en algunos segundos, sin la necesidad de contar con equipamiento adicional de respaldo para situaciones de fallas en los enlaces entre enrutadores.

CAPITULO 1: MARCO TEORICO

El presente capítulo señala los principios de operación de: IP y el protocolo Primero el Camino más Corto Estándar Abierto (OSPF). Se resume la operación del rápido re-enrutamiento IP y MPLS. Asimismo se señala como MPLS permite transportar información de TE para ser utilizada por OSPF y se señala la manera de optimizar los temporizadores de operación de OSPF para acelerar la reconvergencia ante una situación de falla de un enlace entre enrutadores.

1.1 Problemática

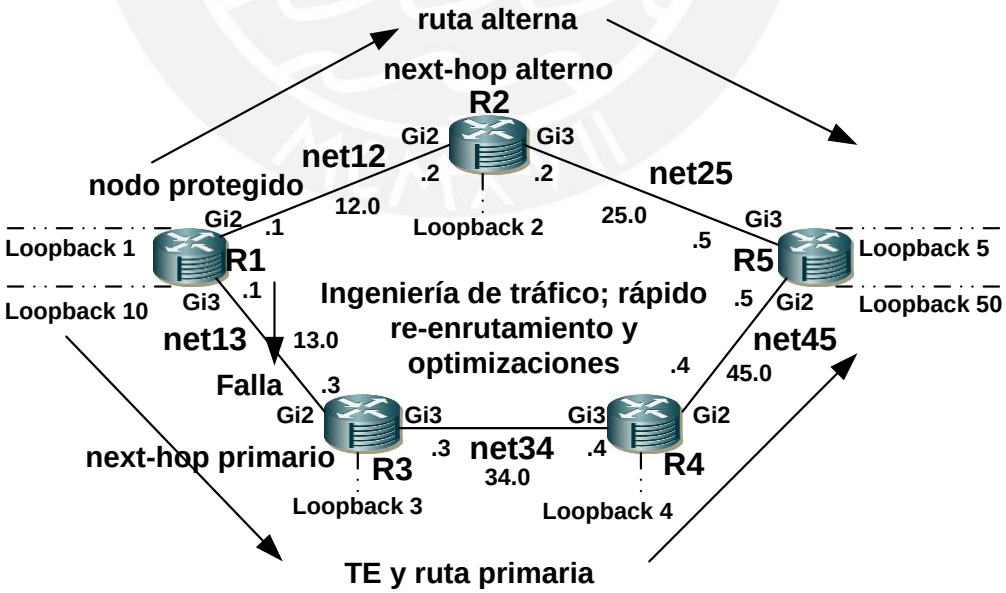

Figura N° 1: Topología de Red IP analizada [3,4].

El enrutamiento IP está gobernado por la necesidad de conmutar paquetes en el menor tiempo posible, estableciéndose la ruta con menor métrica para las redes destinos. Al tener conectividad IP y enrutamiento OSPF en la red de la Figura N° 1 y considerando todos los enlaces de la misma capacidad, OSPF establece la ruta R1-R2-R5 para la conectividad entre las interfaces Loopback 10 y 50 de R1 y R5, respectivamente. No se considera el ancho de banda disponible en las interfaces, y de trabajar dichas interfaces a plena carga, los paquetes serán eliminados por saturación, una consecuencia de ello es tener enlaces sobreutilizados y otros subutilizados [3].

Cambiar enlaces y equipos a capacidades mayores, conlleva a realizar tareas de planificación, programación, etc., demandando tiempo, dinero y otros recursos. Realizar modificaciones en las métricas del IGP es una opción válida, logrando utilizar enlaces subutilizados, esparciendo el tráfico de la red entre los enrutadores R1 y R5, sin embargo al tener tráfico entre otros 2 enrutadores en la red propuesta, se presenta el inconveniente inicial y de modificar nuevamente las métricas del IGP también variará el establecimiento de todas las otras rutas [3].

Se propone utilizar una métrica distinta a la utilizada por OSPF, como por ejemplo el ancho de banda o parte del ancho de banda disponible en la interface, estableciéndose una ruta en base a dicho recurso, es decir una ruta que cumpla con una restricción [3].

En resumen e inicialmente OSPF requiere establecer una relación de vecindad con los enrutadores directamente conectados, para ello según el estándar de operación, se envían paquetes HELLO cada 10 o 30 segundos dependiendo del tipo de red. Sí, un enrutador R1 en un tiempo de 4 veces el HELLO (4xHELLO = DEAD) no recibe ningún paquete HELLO del enrutador vecino, este último pierde adyacencia con R1, OSPF en R1 actualiza la base de datos de estados de enlaces y recalcula el algoritmo Primero el Camino más Corto (SPF) para actualizar las rutas hacia las redes destinos, restableciéndose la conectividad en un tiempo estimado de 40 segundos, es decir reconverge en 40 segundos [5].

Modificar los temporizadores HELLO y DEAD no asegura tener un tiempo de reconvergencia menor a los 40 segundos, ya que intervienen otros temporizadores, tales como el temporizador para la generación de un Anuncio de Estado de Enlace (LSA) luego de ocurrido un cambio en la topología o el temporizador para recalcular el algoritmo SPF luego de recibir dicho LSA, en ese sentido se tendrá que aplicar

optimizaciones para lograr un tiempo de reconvergencia que no supere los 5 segundos para reestablecer la conectividad y operatividad [6].

1.2 Hipótesis

Aplicando la ingeniería de tráfico (TE) se establecerá una ruta que cumpla con una restricción. Así luego de ocurrir la falla de un enlace entre dos enrutadores de esta ruta establecida por TE, se conseguirá reconverger en un tiempo menor a 5 segundos mediante la aplicación del rápido re-enrutamiento IP (IP FRR) y optimizaciones las cuales instalarán rutas de respaldo y alcanzarán el tiempo propuesto.

1.3 OSPF Rápida Convergencia y BFD

OSPF pertenece a la familia de los IGPs, siendo un protocolo de enrutamiento de estado de enlace, el cual es capaz de dividir el dominio de enrutamiento en 2 capas jerárquicas llamadas áreas, la única área y de mayor jerarquía es llamada área backbone y/o área 0; siendo la de menor jerarquía una área no backbone y/o área estándar [5].

OSPF es un estándar abierto basado primariamente en la publicación denominada: Solicitud para Comentarios (RFC) número 2328 del Grupo de Trabajo de Ingeniería de Internet (IETF), su operación incluyen las siguientes características [5]:

a) Respuesta rápida ante cambios en la topología de la red.

b) Actualizaciones desencadenadas por eventos.

c) Actualizaciones periódicas en intervalos de 30 minutos (según estándar).

OSPF genera actualizaciones de enrutamiento solo cuando ocurre un cambio en la topología de la red, al cambiar el estado de un enlace, el enrutador que detecta dicho cambio, crea un LSA con respecto al mismo, el cual es anunciado a todos los enrutadores vecinos dentro del dominio de enrutamiento de OSPF, cada enrutador receptor del LSA en cuestión, almacena ese LSA en una base de datos llamada base de datos de estados de enlaces, y reenvía dicho LSA a sus enrutadores vecinos de la misma área [5].

La base de datos de estados de enlaces de cada enrutador, es usada para calcular la mejor ruta hacia cada prefijo a través de la red aplicando el algoritmo SPF de Dijkstra o

el algoritmo Primero el Camino más Corto Incremental (ISPF). Los resultados de estos cálculos en cada enrutador son ofrecidos a la tabla de enrutamiento del mismo (solo las rutas con menores costos) [5].

Definimos la reconvergencia de red como aquel proceso de sincronización en las tablas de reenvió de todos los enrutadores, luego de producido un cambio en la topología. Dicha reconvergencia toma tiempo y es durante el cual podría producirse loops (lo que significa lazos cerrados de enrutamiento) debido a la inconsistencia en las tablas de reenvió y/o a la topología de la red [6].

Cambios en la topología de un dominio OSPF son anunciados mediante la transmisión de paquetes LSAs, los que tienen que alcanzar a todos los enrutadores pertenecientes al dominio para luego recalcular el algoritmo SPF. Es en este sentido que se optimiza la operación de OSPF para acelerar el tiempo de reconvergencia [6].

Se mencionan los temporizadores a modificar en la simulación de TE/IP FRR y Optimizaciones, tales como son los parámetros para el algoritmo SPF, los cuales constan de 3 valores expresados en milisegundos; el primero indica el retardo para el cálculo del algoritmo SPF una vez recibido un cambio (primer cambio recibido), el segundo indica el retardo para el cálculo entre el primer y segundo algoritmo SPF, y el tercer valor indica el máximo retardo para el cálculo del mismo algoritmo [6].

Los parámetros del LSA son similares a los del SPF, el primero indica el retardo para la generación de la primera ocurrencia generando un LSA luego de ocurrir un cambio en la topología de red, el segundo indica el mínimo retardo para generar la misma LSA y el tercero indica el máximo retardo para volver a originar el LSA en cuestión [6].

El parámetro LSA ARRIVAL indica el mínimo retardo para aceptar el LSA, expresado en milisegundos [6].

El parámetro PACING FLOOD en milisegundos, indica el tiempo mínimo para trasladar el LSA a las interfaces que correspondan [6].

El parámetro PACING RETRANSMISSION también en milisegundos, indica el tiempo mínimo para la transmisión del LSA entre vecinos [6].

Siguiendo con la optimización del tiempo de reconvergencia, se considerará un proceso para detectar la falla de un enlace. En un ambiente real, el tiempo para este

proceso es variable, dependiendo del medio físico y del tipo de encapsulación en la capa 2 del modelo OSI. Como ejemplo tenemos que el Paquete Sobre SONET (POS) tiende a utilizar 50 milisegundos como tiempo de detección de falla considerando las capas 1 y 2 del modelo OSI [7].

La Detección de Reenvío Bidireccional (BFD) estandariza un método (protocolo, dispositivo y enlace) para una rápida detección de falla entre dispositivos, operando en cualquier medio y manteniendo reducida sobrecarga de operación. El BFD opera sobre cualquier medio físico de la capa 1, encapsulaciones, topologías y protocolos de enrutamientos, siendo el mejor escenario, la obtención de un tiempo de detección similar al ofrecido por el POS [7].

Las aplicaciones comunes de BFD incluyen [7]:

- Detección de actividad en el plano de control.

- Detección de actividad en el extremo del túnel.

- Desencadena un mecanismo para IP/MPLS FRR.

- Detección de falla en el plano de datos para MPLS.

BFD verifica la conectividad entre dos dispositivos, en la fase inicial del despliegue, un enrutador CISCO soporta BFD en modo asíncrono, el cual depende de la transmisión de paquetes de control [7].

BFD detecta la falla en la ruta de reenvió entre dos dispositivos adyacentes, incluyendo las interfaces, el enlace de datos y el plano de reenvió. En dispositivos CISCO, el BFD es habilitado en los niveles de interface y protocolo de enrutamiento, habilitado el BFD, se establece la sesión, BFD negocia los temporizadores y envían paquetes de control en el intervalo negociado. BFD es independiente del protocolo de enrutamiento. De presentarse una falla en el enlace de datos, BFD notifica al protocolo de enrutamiento del enrutador local, el cual según instrucciones inicia el proceso de reconvergencia [8].

BFD en el Sistema Operativo Internetworking (IOS) de CISCO opera con los siguientes parámetros o temporizadores expresados en milisegundos [8]:

- El parámetro INTERVALO indica el temporizador de negociación.

- El parámetro MIN_Rx indica el mínimo tiempo de espera.

- El parámetro MULTIPLIER es usado para establecer el máximo tiempo de espera.

1.4 IP FRR

El concepto de rápido re-enrutamiento IP (IP FRR), permite acelerar el re-enrutamiento IP cuando se produce una falla en un enlace o nodo en la red, sin la necesidad de esperar los tiempos de convergencia tradicionales o manipular los tiempos propios de operación del protocolo en cuestión, referido al establecimiento de adyacencia entre enrutadores (en el caso de OSPF nos referimos a los intervalos: HELLO y DEAD) [9].

IP FRR hace referencia al conjunto de tecnologías que provee la capacidad de rápido re-enrutamiento basado en el reenvío y paradigma IP [9].

IP FRR es la capacidad de un enrutador de soportar las siguientes 2 funcionalidades [10]:

A.- Precalcula una ruta de respaldo para los prefijos destinos (ver Figura N° 2), la cual es accesible vía un siguiente salto (next-hop) de respaldo y se activa cuando la ruta primaria para el prefijo destino no está disponible. Cuando un enrutador no posee una ruta de respaldo para un prefijo y detecta una falla en la conectividad para ese prefijo, para lograr la reconvergencia, intercambia información de enrutamiento con la finalidad de recalcular un nuevo next-hop, sin embargo la ventaja de instalar un next-hop de respaldo, es que el enrutador puede reenviar paquetes durante la reconvergencia antes de que el nuevo next-hop para el prefijo afectado haya sido calculado e instalado [10].

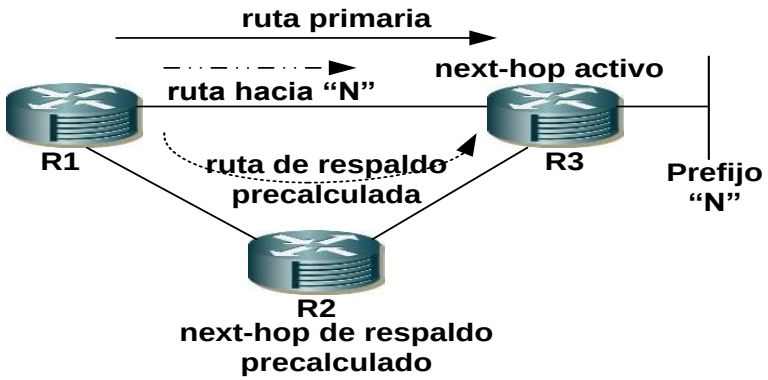

Figura N° 2: Ruta reparada libre de loop [4,11].

B.- Tan pronto como la falla en la ruta primaria es detectada en el plano de reenvío, el enrutador R1 de la Figura N° 3 reemplaza el next-hop activo para el prefijo afectado, por un next-hop de respaldo instalado en algunos cientos de milisegundos, siendo el enrutador R2 en este caso. El tiempo empleado en este proceso dependerá de la tecnología y el hardware utilizado [10].

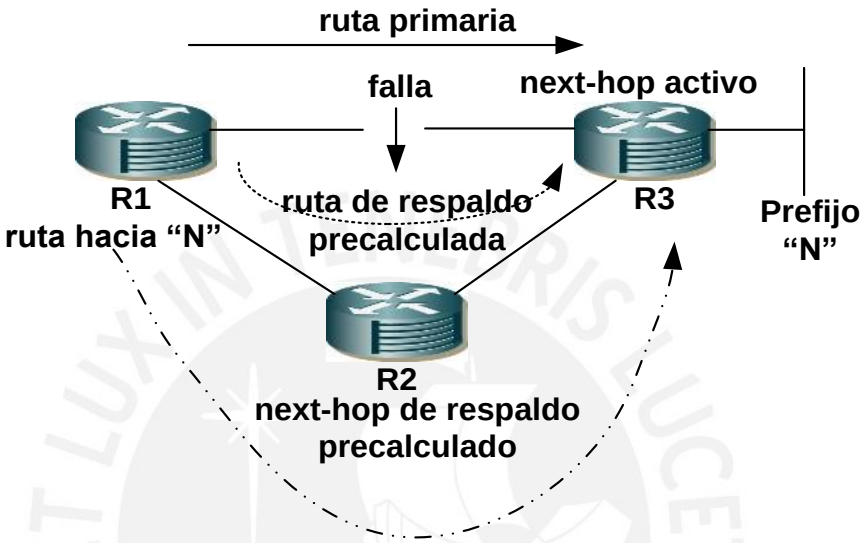

Figura N° 3: Rápido enrutamiento libre de loop [4,11].

1.5 TE

La ingeniería de tráfico, es la capacidad de dirigir el tráfico a lo largo de una red IP, desde la mejor ruta especificada por una tabla de enrutamiento construida en base a algún IGP, hasta una ruta distinta a la especificada por dicho protocolo [12].

La ingeniería de tráfico sitúa el tráfico donde existe disponibilidad de ancho de banda [12].

1.6 MPLS

MPLS define como los enrutadores pueden reenviar paquetes basados en una etiqueta MPLS y amplía el paradigma de reenvío de paquetes del IGP, considerando desde la información para el reenvío de paquetes ofrecida por el IGP en cuestión, hasta permitir decisiones de reenvío considerando otros factores, tales como TE [13].

El MPLS es la implementación de una capa intermedia entre la capa 2 y la capa 3 del modelo de referencia OSI, no es un protocolo de capa 2, ya que el encabezado de dicha capa aún se mantiene, ni es un protocolo de capa 3, por la misma razón [3].

Modelo OSI

Aplicación
Presentación
Sesión
Transporte
Red
Enlace de Datos
Física

Figura N° 4: Modelo de Referencia OSI [3].

MPLS conceptualmente, se dice que opera en la capa 2.5 del modelo de referencia de 7 capas de OSI, es decir opera entre la capa Enlace de Datos y la capa de Red [3].

MPLS integra las ventajas de la conmutación de la capa 2, tales como las ofrecidas por las redes: Modo de Transferencia Asíncrona (ATM) o Frame Relay (FR); con los beneficios del enrutamiento de la capa 3, como las ofrecidas por el protocolo IP [3].

Un enrutador que soporta MPLS es llamado Enrutador de Conmutación de Etiquetas (LSR) y es capaz de entender etiquetas de MPLS, recibiendo y transmitiendo paquetes etiquetados sobre la capa de enlace de datos [3].

Existen 3 tipos de enrutadores LSRs en una red MPLS [3]:

a) LSR de ingreso, el cual recibe un paquete que aún no tiene etiqueta, inserta una etiqueta y reenvía el paquete sobre el enlace de datos.

b) LSR de egreso, el cual recibe un paquete etiquetado, remueve dicha etiqueta o las que hubiere y reenvía el paquete sobre el enlace de datos. Los LSR de Ingreso y Egreso, residen en la frontera de la red MPLS.

c) LSR intermedio, el cual recibe un paquete etiquetado, desarrolla una operación sobre el mismo, conmuta el paquete y lo reenvía sobre el correspondiente enlace de datos.

Si un enrutador LSR recibe un paquete etiquetado, desarrolla una de las siguientes 3 operaciones: ***i)*** POP, ***ii)*** PUSH o ***iii)*** SWAP [3].

Un Ruta de Etiqueta Conmutada (LSP), es una secuencia de enrutadores LSRs que conmuta paquetes etiquetados a través de una red MPLS o parte de ella, el primer LSR de un LSP, es el LSR de ingreso para ese LSP, mientras que el último LSR del LSP, es el LSR de egreso, todos los LSRs entre el LSR de ingreso y el LSR de egreso, son llamados LSRs intermedios [3].

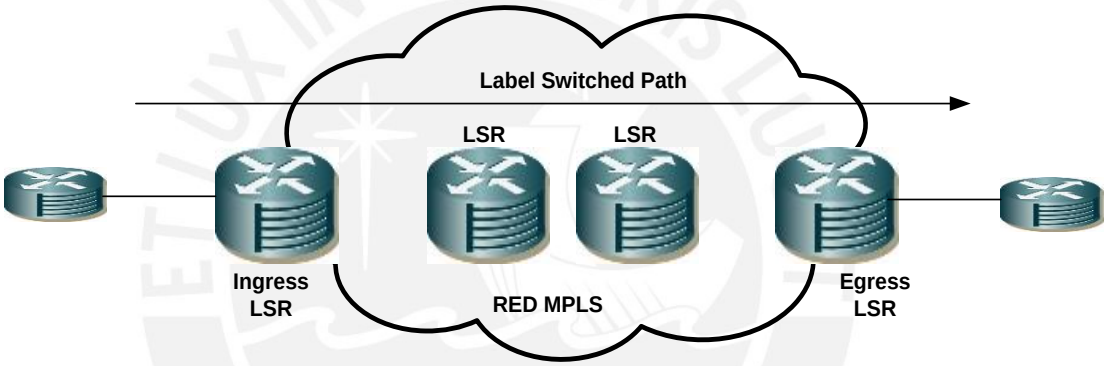

Figura N° 5: Un LSP a través de una red MPLS [3,4].

1.7 MPLS TE

MPLS TE requiere de un IGP de estado de enlace y que sea capaz de transportar información necesaria para TE, por ello OSPF ha sido extendido para transportar dicha información, en consecuencia si OSPF transporta información referida a TE, recibe el nombre de Primero el Camino más Corto Estándar Abierto Ingeniería de Tráfico (OSPF TE) [3].

Para que MPLS TE opere, requiere cumplir las siguientes sentencias [3]:

a) Restricciones de enlaces (cuanto tráfico cada enlace puede soportar y que enlaces pueden ser utilizados por un túnel TE).

b) Distribución de información de TE (habilitando MPLS TE para un IGP de estado de enlace, tal como OSPF).

c) Un algoritmo para calcular la mejor ruta desde el Head End LSR hasta el Tail End LSR, tal como el Algoritmo para Calcular la Ruta (PCALC).

d) Un Protocolo de señalización tal como el Protocolo con Reserva de Recurso Ingeniería de Tráfico (RSVP TE), para señalizar un túnel TE a través de la red.

e) Reenviar tráfico sobre el túnel TE.

MPLS TE puede dirigir el tráfico según los recursos o restricciones, tales como el ancho de banda de los enlaces y otros atributos de los enlaces, dichos atributos son especificados por el operador, estos atributos son configurados en los enlaces y anunciados por el protocolo de enrutamiento de estado de enlace utilizado [3].

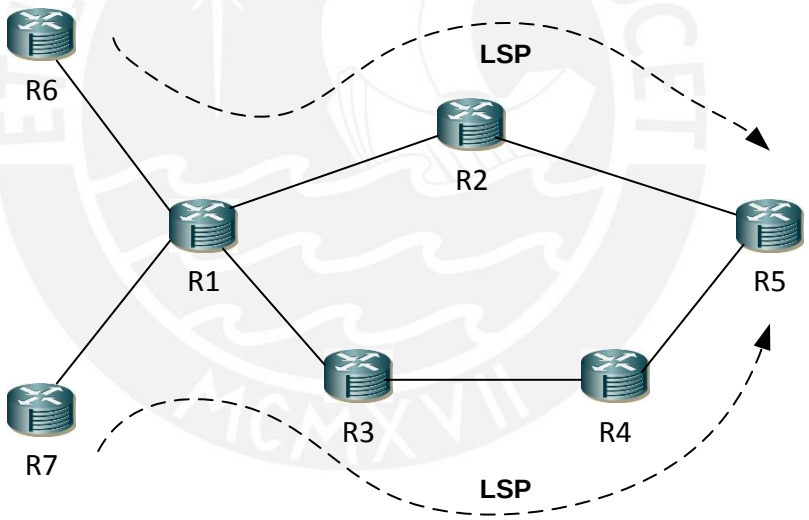

Figura N° 6: Establecimiento de distintos LSPs (Túnel TE) [3,4].

En la Figura N° 6 sí el reenvió del tráfico se basa solo en el paradigma IP y asumiendo que todos los enlaces tienen la misma capacidad, la ruta a seguir desde R6 o R7 hasta R5, será R1-R2-R5, sin importar la configuración realizada en R6 o R7 [3].

Al configurar un túnel TE en algún enrutador LSR, dicho enrutador se convierte en el Head End LSR de ese túnel TE, luego se especifica el LSR destino para el túnel TE en

cuestión, este último LSR es conocido como el Tail End LSR, y necesariamente se adhiere a la restricción declarada en la configuración del túnel, por ejemplo, se puede especificar el ancho de banda requerido para establecer un túnel TE [3].

El algoritmo PCALC busca en una base de datos para TE, la coincidencia del ancho de banda requerido y los atributos para el túnel TE en los enlaces de todas la rutas posibles y escoge la ruta que cumpla con las restricciones, este cálculo es realizado en el Head End LSR [3].

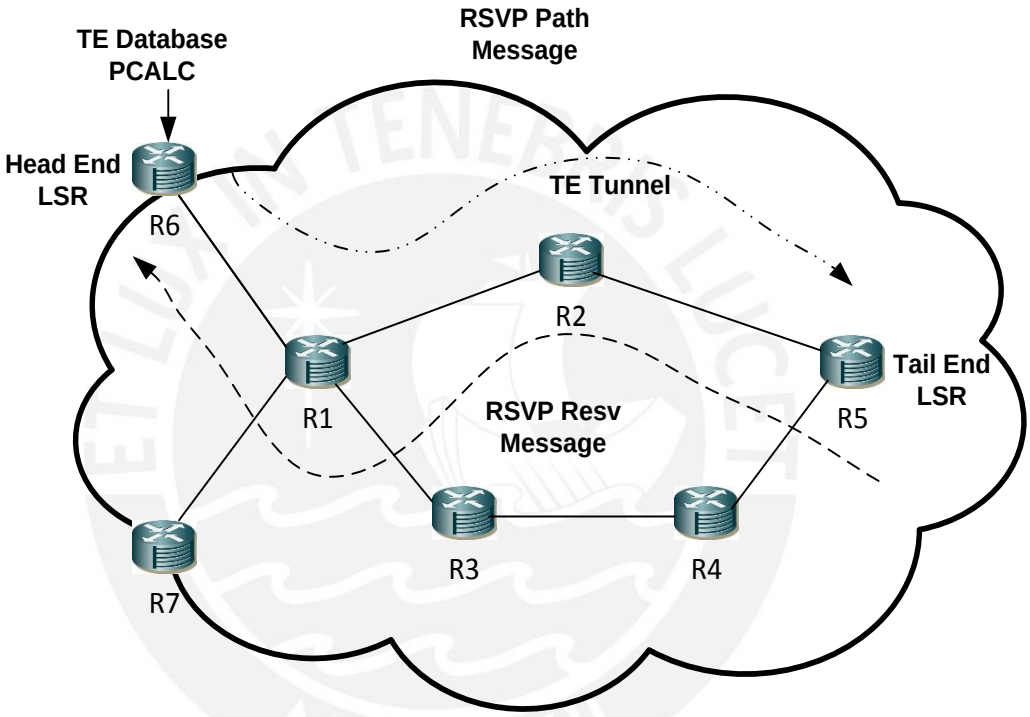

Figura N° 7: Distribución de la información de TE sobre OSPF [3,4].

El protocolo RSVP TE es el encargado de señalar las etiquetas a lo largo de la ruta, desde el Head End LSR hasta el Tail End LSR, creando un túnel TE de manera unidireccional y cumpliendo con las restricciones del mismo [3].

RSVP TE señala el túnel TE mediante el envío del mensaje Path Req desde el Head End LSR hasta el Tail End LSR, transportando una solicitud de etiqueta MPLS, luego el Tail End LSR envía un mensaje de regreso Resv Msg hacia el Head End LSR, verificando que el túnel TE con las restricciones señaladas pueda ser establecido en cada nodo y de no recibir mensaje alguno de error, se establece el túnel TE de manera unidireccional [3].

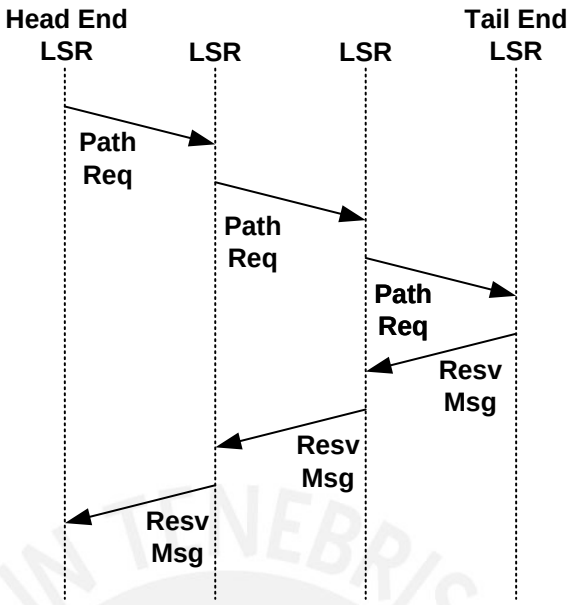

Figura N° 8: Flujos de los mensajes Path Req y Resv Msg en el RSVP [14].

Establecido el túnel TE, es necesario asegurar que el tráfico sea reenviado a través de la ruta señalada o elegida, una forma de lograr esto es instruyendo al Head End LSR a que inserte los prefijos destinos dentro de la tabla de enrutamiento con el túnel TE como next-hop o interface de salida, de manera similar se establece el ruta de retorno [3].

1.8 OSPF TE

El principio de operación de OSPF, es enviar y/o reenviar información del estado de sus interfaces o enlaces a los enrutadores vecinos. Dicha información es el costo de cada enlace y su valor numérico por defecto es auto deducido por el protocolo según la capacidad nominal de dicho enlace. La información de todos los enlaces en todos los enrutadores pertenecientes a la misma área de enrutamiento, reside en una base de datos que mantiene cada enrutador, llamada base de datos de estados de enlaces y con los datos contenidos en ella, cada enrutador ejecuta el algoritmo SPF o ISPF para calcular los costos hacia cada prefijo destino escogiendo la ruta con menor costo [3].

Para que OSPF lleve información adicional al estado de los enlaces, tales como máximo ancho de banda reservable, ancho de banda actual, máximo ancho de banda sin reservar, es necesario extender OSPF a OSPF TE, mediante la implementación de

una capa intermedia entre la capa 2 y la capa 3 del modelo de referencia OSI, esta capa intermedia que transporta la información de TE es conocida como MPLS [12].

OSPF necesariamente se extiende para transportar información extra sobre los enlaces para TE, es por ello que OSPF TE requiere [3]:

a) Métrica de TE.

b) Ancho de banda máximo.

c) Máximo ancho de banda reservable.

d) Ancho de banda sin reservar.

e) Grupo Administrativo.

La RFC 2370 describe las extensiones de OSPF donde 3 nuevas LSAs son definidas y llamadas LSAs opacas, las cuales son las que MPLS TE necesita para colocar la información extra de los enlaces dentro de un dominio OSPF, luego OSPF envía o reenvía esta información dentro del dominio de enrutamiento [3].

En el presente documento, analizaremos la incidencia del parámetro descrito en el literal anterior “c”, el cual es el ancho de banda reservado en el enlace para TE, en ese sentido, tenemos que instruir a los enrutadores de la red IP propuesta a reservar cierto ancho de banda. Utilizando el IOS de CISCO se requiere habilitar MPLS TE de manera global y en cada interface de cada enrutador participante, así como en el dominio de enrutamiento de OSPF [3].

1.9 MPLS TE TUNNEL

El Túnel Ingeniería de Tráfico Multi Protocolo de Conmutación de Etiquetas (MPLS TE TUNNEL) es un LSP desde el Head End LSR hasta el Tail End LSR, de manera unidireccional, teniendo los siguientes atributos [3]:

a) Túnel Destino

Es el ID del enrutador destino habilitado para MPLS TE en el Tail End LSR.

b) Ancho de banda deseado

Es el ancho de banda requerido por el túnel.

c) Afinidad

Un enlace puede tener un atributo denominado flag, el cual indica: *i)* el recurso del enlace, *ii)* la capacidad del enlace o *iii)* una política administrativa, indicando la necesidad de que un túnel teniendo un recurso, puede atravesar un enlace. El flag consta de 32 bits sin ninguna sintaxis asociados con ellos, con cualquier significado que el operador de red quisiese asociarle [3].

En el túnel del Head End LSR, es posible configurar bits de afinidad y una máscara para controlar el permiso del túnel a través del enlace con los atributos del flag. Los bits de afinidad tienen una longitud de 32 bits y están coincidiendo uno a uno con los bits del atributo flag. La máscara de los bits de afinidad, indican si cada bit especificado, necesita ser verificado con el bit correspondiente en el campo flag del enlace [3].

En consecuencia, sí el n-enésimo bit en la máscara de afinidad es establecido, entonces el n-enésimo bit en el atributo flag necesariamente coincide con el n-enésimo en la longitud de los bits de afinidad. Sí el n-enésimo bit en la máscara de afinidad no se establece, no importa si los dos bits en la misma posición en los campos de bits de afinidad y bits de atributos flag coinciden [3].

d) Prioridades Setup y Holding

En el establecimiento de un túnel o LSP, el Setup define el nivel de preferencia, desde el más preferible con valor 0, hasta el menos preferible con valor 7. El holding define la probabilidad de que una vez establecido el túnel, este sea reemplazado por un nuevo LSP [12].

e) Reoptimización

La reoptimización motiva al túnel a ser reenrutado por la red, sobre una ruta que no es la mejor ruta o la ruta más óptima, al no tener el enlace suficiente ancho de banda para ser reservado en el momento en que el túnel haya sido señalizado, es decir la reserva de ancho de banda no es suficiente para el establecer túnel TE [3].

Existen 3 eventos que desencadenan la reoptimización: ***i)*** reoptimización periódica, ***ii)*** reoptimización producida por evento, y ***iii)*** reoptimización manual [3].

f) Opción de Ruta

Es el camino que deberá seguir el túnel, y se puede establecer de dos formas: ***i)*** Explicita, donde se especifica cada enrutador de la ruta en forma manual, desde el next-hop hasta el Tail End LSR; y ***ii)*** Dinámica, donde solo se indica el destino o Tail End LSR, cuya ruta es calculada en el Head End LSR mediante el algoritmo PCACL, siendo el PCALC el algoritmo SPF de OSPF modificado para OSPF TE [3].

En general los atributos tales como bits de afinidad, flag, reoptimización, prioridad Setup, Holding y la opción ruta, son los factores usados para calcular la ruta de un túnel TE [3].

1.10 Estado del Arte

MPLS es comúnmente habilitado en el núcleo de una red IP de un Proveedor de Servicios, si un enlace o enrutador falla, el tráfico es reenrutado alrededor de la falla, dicho re-enrutamiento sucede para MPLS y para IP, lo que significa que el tráfico es eliminado durante la transición, siendo perjudicial para un tráfico sensible a pérdidas de paquetes, como por ejemplo el tráfico de Voz sobre IP (VOIP) [3].

Existen mecanismos para protección en la capa 1 del modelo OSI, conocidos como Conmutación para Protección Automática (APS), los cuales tienen connotación en enlaces ópticos, teniendo como desventaja que para cada enlace protegido, se requiere un enlace de respaldo y una tarjeta adicional con la respectiva interface en cada extremo del enlace, estando a la espera de que se produzca la falla [3].

Enlaces y nodos protegido con MPLS TE FRR, no requieren de un enlace de respaldo, se crea un túnel de respaldo para cada enlace o nodo protegido por adelantado, lo que lleva a omitir el tiempo empleado en señalar el túnel de respaldo, cuando el dispositivo o enlace protegido falla [3].

En una red MPLS TE con rápido re-enrutamiento (MPLS TE FRR), si se realiza configuración manual y enrutamiento explícito para cada túnel de respaldo, brinda la posibilidad de reenrutar el tráfico etiquetado alrededor del enlace o del dispositivo que se hizo indisponible en 50 ms siempre, contando con enlaces ópticos y APS [3].

Algunos proveedores de servicios de telecomunicaciones, tales como T-Mobile UK, Verizon, TI y Vodafone están implementando MPLS TE FRR [2].

Asimismo la característica de OSPF/IP FRR permite reenrutar el tráfico alrededor del enlace cuando se produce una falla en el mismo, para lo cual se preestablece una ruta alternativa por prefijo y se instala dicha ruta en el CEF y en la RIB del enrutador. Producida la falla en el enrutador protegido, dicho enrutador desvía el tráfico hacia la ruta alterna almacenada, sin que los equipos pertenecientes al dominio de enrutamiento, recalculen la ruta para el prefijo afectado o incluso noten que la topología de la red haya cambiado [11].

En la actualidad existe la tendencia en los proveedores de servicios de implementar redes IP/MPLS. De contar con enlaces ópticos, es posible proteger los mismos mediante APS requiriendo equipamiento adicional. Asimismo es posible implementar MPLS FRR o MPLS TE FRR requiriendo realizar ruteo explícito para la protección de los enlaces así como contar con enlaces ópticos [3].

En el presente documento se establece una ruta que cumpla con reservar un valor de ancho de banda en las interfaces participantes y se protege un enlace en la ruta establecida sin la necesidad de contar con enlaces ópticos ni equipamiento adicional de respaldo para cada enlace. Es decir se propone simular TE/IP FRR y Optimizaciones, en donde mediante TE se establecerá una ruta preferida, con IP FRR se instalará una ruta y un next-hop de respaldo en la RIB y CEF de un enrutador y con optimizaciones se propone obtener la reconvergencia o restablecimiento de la conectividad en un tiempo que no supere los 5 segundos luego de presentarse la falla en un enlace entre 2 enrutadores en la ruta establecida, sin la necesidad de realizar ruteo explícito (manual) para establecer una ruta de respaldo. Teniendo como aporte ponderar la necesidad de requerir equipamiento de respaldo adicional y el tiempo para el restablecimiento de la conectividad en la red analizada.

CAPITULO 2: SIMULACIONES DE OSPF TE, IP FRR, TE/IP FRR y Optimizaciones

En el presente capítulo se proponen 3 topologías distintas. En la primera de ellas se simulará OSPF TE, para lo cual se utilizará la topología de la Figura N° 9, ya que esta topología ofrece 3 rutas entre los puntos de interés, en una de estas rutas se realizará una reserva del ancho de banda en las interfaces participantes, así OSPF TE establecerá la ruta que cumpla con dicha reserva. En la segunda topología se simulará IP FRR utilizando la topología de la Figura N° 14, ya que esta topología ofrece un enrutador de respaldo y una ruta alterna entre los puntos de interés, así IP FRR instalará la ruta y el next-hop de respaldo en la RIB y CEF de los enrutadores involucrados con la finalidad de reducir el tiempo de reconvergencia ante una falla del enlace entre dos enrutadores.

En la tercera topología se simulará TE/IP FRR y Optimización, utilizando la topología de la Figura N° 18, ya que dicha topología ofrece 2 rutas entre los puntos de interés, así como una ruta y un next-hop de respaldo. En este escenario TE elegirá la ruta que cumpla con la reserva del ancho de banda señalado en las interfaces participantes. IP FRR instalará una ruta y un next-hop de respaldo en la RIB y CEF de un enrutador. Con las optimizaciones se intentará obtener un tiempo de reconvergencia que no supere a los 5 segundos para restablecer la conectividad entre los puntos de interés luego de ocurrir una falla del enlace entre 2 enrutadores en la ruta establecida por TE.

2.1 Metodología

La metodología se basa en la obtención de resultados a través de la simulación de tres topologías de redes distintas, se realizará configuraciones en el IOS de CISCO sobre máquinas virtuales, utilizando la versión 12.4(19) para la simulación de OSPF TE; y la versión 15.5(1)S para las simulaciones de: *i)* IP FRR; y *ii)* TE/IP FRR y Optimizaciones.

Al tener que simular TE/IP FRR y Optimizaciones, se propone simular una topología para TE, una para IP FRR y una para las optimizaciones, con la finalidad de mostrar la posibilidad de implementar TE, IP FRR y Optimizaciones en cualquier topología de manera independiente o integrar 2 de ellas o integrar las 3 en cualquier topología. Se precisa que la base y el conocimiento teórico es único para las 3 tecnologías, siendo la configuración dependiente de una topología particular.

Para la simulación de OSPF TE se construirá una topología de red compuesta por nueve enrutadores, utilizando la versión 12.4(19) del IOS de CISCO, se simulará una red MPLS TE con la finalidad de transportar información adicional del estado del enlace de cada enrutador, esta información adicional es la reserva del ancho de banda en la interface, la misma que será utilizado por OSPF TE para elegir una ruta que cumpla con la reserva señalada. Se configurará máquinas virtuales en las cuales se establecerá el direccionamiento IP y el dominio de enrutamiento OSPF para tener conectividad IP. Se simulará una red MPLS y la aplicación MPLS TE, en consecuencia se simulará TE sobre el dominio de enrutamiento OSPF, convirtiéndose el dominio OSPF en un dominio OSPF TE. Se discutirá el establecimiento de rutas en base a la reserva del ancho de banda de las interfaces en los enrutadores participantes de la ruta elegida en la red propuesta. Se utilizará una laptop de tercera generación, con sistema operativo Windows 8.1 a 64 bits, con 8 GB de RAM y 2.5 GHz de procesador.

Para la simulación de IP FRR se construirá una topología de red compuesta por tres enrutadores, utilizando la versión 15.5(1)S del IOS de CISCO, se simulará una red IP con dominio de enrutamiento OSPF para tener conectividad IP. Se realizará configuraciones en máquinas virtuales en las cuales se establecerá IP FRR con la finalidad de instalar una ruta y un next-hop de respaldo en la RIB del OSPF y en el CEF de los enrutadores involucrados. En esta simulación se utilizará una laptop de cuarta generación, con sistema operativo Windows 8.1 a 64 bits, con 12 GB de RAM y 3.5 GHz de procesador.

Para la simulación de TE/IP FRR y Optimizaciones se construirá una topología de red compuesta por cinco enrutadores, se utilizará la versión 15.5(1)S del IOS de CISCO, se simulará una red IP, OSPF, MPLS TE, OSPF TE e IP FRR con la finalidad de tener conectividad IP, elegir una ruta que reserve un ancho de banda señalado y tener instalada una ruta y un next-hop de respaldo en la RIB y CEF en los enrutadores de interés. Se optimizará los temporizadores de OSPF, referidos a la generación del primer LSA luego de ocurrido un cambio en la topología, así como el temporizador para la actualización del algoritmo SPF luego de recibir dicho LSA. Se establecerán los enlaces entre enrutadores como redes punto a punto para evitar que OSPF genere LSAs del tipo 2 y se establecerá el protocolo BFD para la detección de adyacencia entre enrutadores vecinos. Con estas optimizaciones se intentará estimar el tiempo de reconvergencia luego de ocurrir la falla del enlace entre 2 enrutadores en la ruta establecida. Esta simulación se realizará utilizando una laptop de cuarta generación, con sistema operativo Windows 8.1 a 64 bits, con 12 GB de RAM y 3.5 GHz de procesador.

2.2 Primera Simulación: Topología de red utilizada para la simulación de OSPF TE

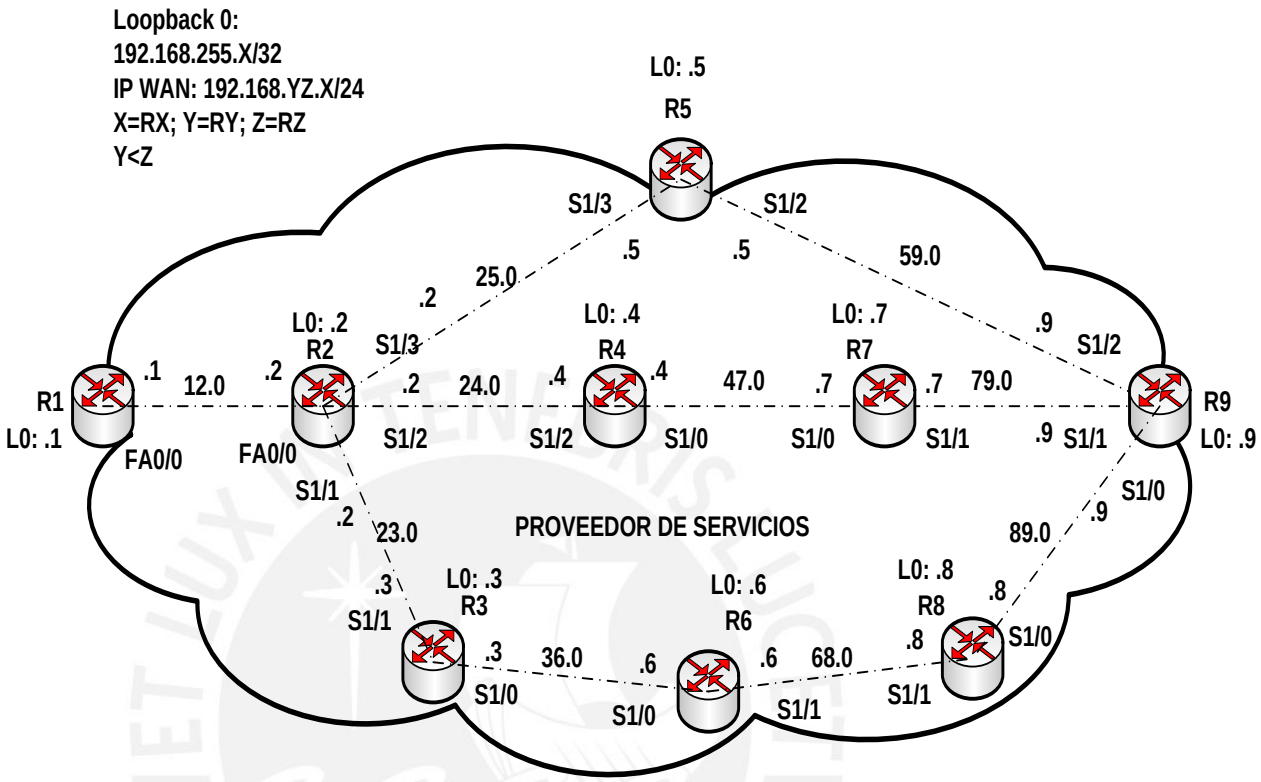

Figura N° 9: Simulación de MPLS TE sobre OSPF (OSPF TE).

La presente simulación se realizó en Dynamips 0.2.8-RC2-x86. Esta simulación tiene como objetivo establecer una ruta entre las interfaces Loopbacks 0 de los enrutadores R1 y R9 con direcciones IP: 192.168.255.1 y 192.168.255.9 respectivamente siguiendo la ruta R1-R2-R3-R6-R8-R9. Se consideró la reserva del ancho de banda en las interfaces de los enrutadores pertenecientes a la ruta elegida, para lo cual se instruyó a los mismos a realizar la reserva del ancho de banda en cada interface. En esta simulación se observó que para OSPF TE la ruta difiere a la ofrecida por OSPF, asimismo se requiere el soporte de MPLS para transportar información de TE.

En la Figura N° 9 se tienen las siguientes interfaces: fastethernet (FA) a 100 Mb/s y seriales (S1/0, S1/1, S1/2 y S1/3) a 1544 Kb/s. Se configuró el direccionamiento IP de acuerdo a las direcciones señaladas así como OSPF para tener conectividad IP. Considerando OSPF, se tiene que la ruta desde la interface Loopback 0 en R1 hacia la Loopback 0 en R9 seguirá R1-R2-R5-R9 (192.168.12.2; 192.168.25.5; 192.168.59.9), lo cual es comprobado con la herramienta traceroute ("traceroute IP-Final source IP-

Inical") desde R1. Se precisa que en OSPF, una interface tiene un costo asociado a ella y que al tener todas las interface seriales de la misma capacidad, todas tienen el mismo costo, asimismo el estándar OSPF elegirá la ruta con menor costo, en consecuencia elegirá la ruta con menor número de enrutadores, sin tener en cuenta la reserva de ancho de banda en las interfaces, por consiguiente se establece la ruta R1-R2-R5-R9 tal como se muestra en la Figura N° 10. Cabe precisar que la herramienta "traceroute" muestra el rastro o seguimiento de ruta desde un origen hasta un destino.

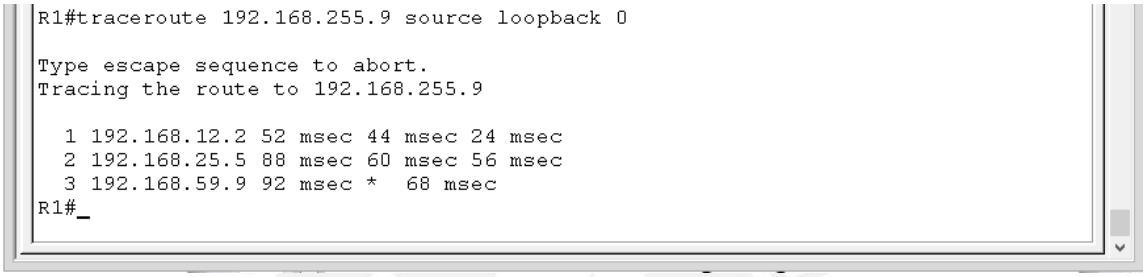

Figura N° 10: La simulación muestra la ruta desde la Loopback 0 en R1 hacia la Loopback 0 en R9, sin tener en cuenta la reserva de ancho de banda.

Se simuló MPLS TE para transportar la información de reserva de ancho de banda en cada interface, así OSPF TE tomará en cuenta dicha restricción. Se configuró la ruta R1-R2-R4-R7-R9 (192.168.12.2; 192.168.24.4; 192.168.47.7; 192.168.79.9 - ruta A) con reserva de 300 Kb/s y la ruta R1-R2-R3-R6-R8-R9 (192.168.12.2; 192.168.23.3; 192.168.36.6; 192.168.68.8; 192.168.89.9 - ruta B) con reserva de 500 Kb/s, se configuró un TE TUNNEL desde R1 hacia R9 y viceversa; y se estableció una ruta con reserva de 300 Kb/s.

Las rutas A y B cumplen con el requerimiento de reservar 300 Kb/s, así OSPF TE discriminó la ruta que contenga un menor número de enrutadores, en consecuencia la ruta A será la elegida, lo cual es comprobado con la herramienta "traceroute" y mostrado en la Figura N° 11. Obsérvese las etiquetas impuestas por MPLS y la ruta establecida R1-R2-R4-R7-R9 en la respectiva figura.

```
R1#traceroute 192.168.255.9 source 192.168.255.1

Type escape sequence to abort.
Tracing the route to 192.168.255.9

  1 192.168.12.2 [MPLS: Label 30 Exp 0] 156 msec 172 msec 136 msec
  2 192.168.24.4 [MPLS: Label 32 Exp 0] 124 msec 152 msec 152 msec
  3 192.168.47.7 [MPLS: Label 32 Exp 0] 124 msec 200 msec 140 msec
  4 192.168.79.9 152 msec *  184 msec
R1#
```

Figura N° 11: La simulación muestra la ruta desde la Loopback 0 en R1 hacia la Lopback 0 en R9 y las etiquetas utilizadas por MPLS.

Ahora se requiere establecer una ruta con reserva de 500 Kb/s, de acuerdo a lo anterior se observa que la ruta B es la que cumple con dicha reserva, para visualizar esto se utiliza nuevamente la herramienta “traceroute” desde R1 hacia R9 y desde R9 hacia R1.

Se precisa que la ruta B vista desde R1 corresponde a R1-R2-R3-R6-R8-R9 (192.168.12.2; 192.168.23.3; 192.168.36.6; 192.168.68.8; 192.168.89.9). Asimismo la ruta B vista desde R9 corresponde a R9-R8-R6-R3-R2-R1 (192.168.89.8; 192.168.68.6; 192.168.36.3; 192.168.23.2; 192.168.12.1).

Con la herramienta “traceroute” se observa la ruta desde R1 hacia R9, tener presente que dicha ruta reserva 500 Kb/s. La Figura N° 12 muestra la ruta seguida desde la interface Loopback 0 en R1 hasta la interface Loopback 0 en R9, visto desde R1.

```
R1#traceroute 192.168.255.9 source 192.168.255.1

Type escape sequence to abort.
Tracing the route to 192.168.255.9

  1 192.168.12.2 [MPLS: Label 32 Exp 0] 136 msec 188 msec 144 msec
  2 192.168.23.3 [MPLS: Label 33 Exp 0] 172 msec 160 msec 192 msec
  3 192.168.36.6 [MPLS: Label 33 Exp 0] 152 msec 196 msec 144 msec
  4 192.168.68.8 [MPLS: Label 33 Exp 0] 136 msec 216 msec 172 msec
  5 192.168.89.9 172 msec *  180 msec
R1#
```

Figura N° 12: La simulación muestra la ruta desde la Loopback 0 en R1 hacia la Lopback 0 en R9. En este caso se reserva 500 Kb/s, comprobando la aplicación de TE.

Con la herramienta “traceroute se observa la ruta desde R9 a R1 con reserva de 500 Kb/s, tal como se muestra en la Figura N° 13, visto desde R9.

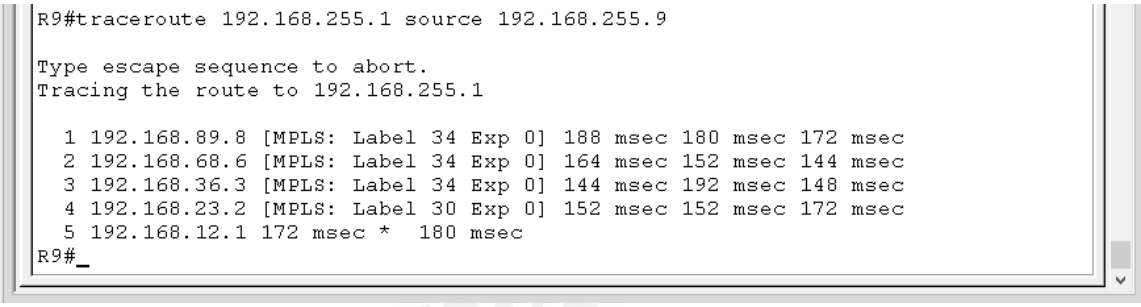

Figura N° 13: La simulación muestra la ruta desde la Loopback 0 en R9 hacia la Lopback 0 en R1. Se reserva 500 Kb/s y se comprueba la aplicación de TE.

La reserva de 500 Kb/s es para observar la operación de OSPF TE y/o la aplicación de TE. En general es posible reservar cualquier valor que no supere la capacidad de la interface involucrada.

Para mayores detalles de configuración, véase el Anexo I.

2.3 Segunda Simulación: Topología de red utilizada para la simulación de IP FRR

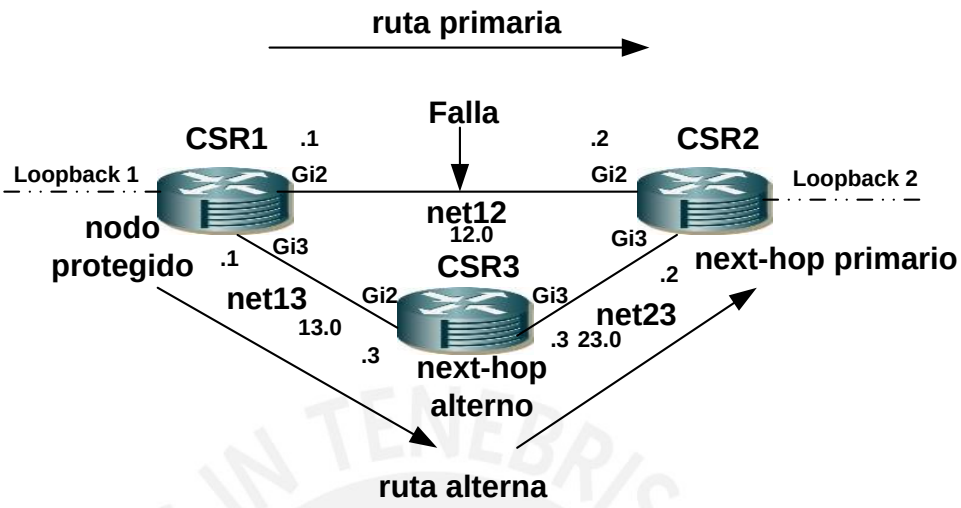

Figura N° 14: Simulación de OSPF Fast Reroute (IP FRR) [4,10,14].

La presente simulación se realizó en ESXi 5.5 con vSphere Client 5.5. Esta simulación tiene como objetivo instalar un next-hop de respaldo precalculado, para tener una ruta alterna instalada en la RIB del OSPF y en el CEF de un enrutador, con la finalidad de mantener conectividad entre la Loopback 1 en el Enrutador para Servicios en la Nube 1 - CSR1 con dirección IP: 10.0.1.1 y la Loopback 2 en CSR2 con dirección IP: 10.0.2.2.

Se tiene que al configurar el direccionamiento indicado en la Figura N° 14 y OSPF para tener conectividad IP, la ruta desde la Loopback 1 en CSR1 hacia la Loopback 2 en CSR2 seguirá CSR1-CSR2 (192.168.12.2). Y de suceder una falla en el enlace entre CSR1 y CSR2, OSPF detecta dicha falla, actualiza el algoritmo SPF, las tablas de enrutamiento y reestablecer la conectividad entre las Loopback 1 y 2. De acuerdo a los temporizadores del estándar de operación de OSPF, se estima 40 segundos para la reconvergencia, asimismo en dicho estándar no se tiene una ruta de respaldo instalada en la RIB ni CEF de los enrutadores.

Es necesario precisar que en el IOS de CISO la tabla de reenvió conocida como CEF deriva de la base de información de enrutamiento de OSPF conocida como RIB. Asimismo CEF es una tecnología desarrollada por CISCO para el reenvío de paquetes.

Se configuró IP FRR en CSR1 para tener una ruta y un next-hop de respaldo instalado en la CEF siendo dicho next-hop CSR3, el cual visto desde CSR1 tiene la IP 192.168.13.3. En la Figura N° 15 se observa la CEF de CSR1, se visualiza a CSR2 como enrutador primario con IP 192.168.12.2 (véase: next-hop 192.168.12.2) y a CSR3 como enrutador alterno con IP 192.168.13.3 (véase: repair: attached-nexthop).

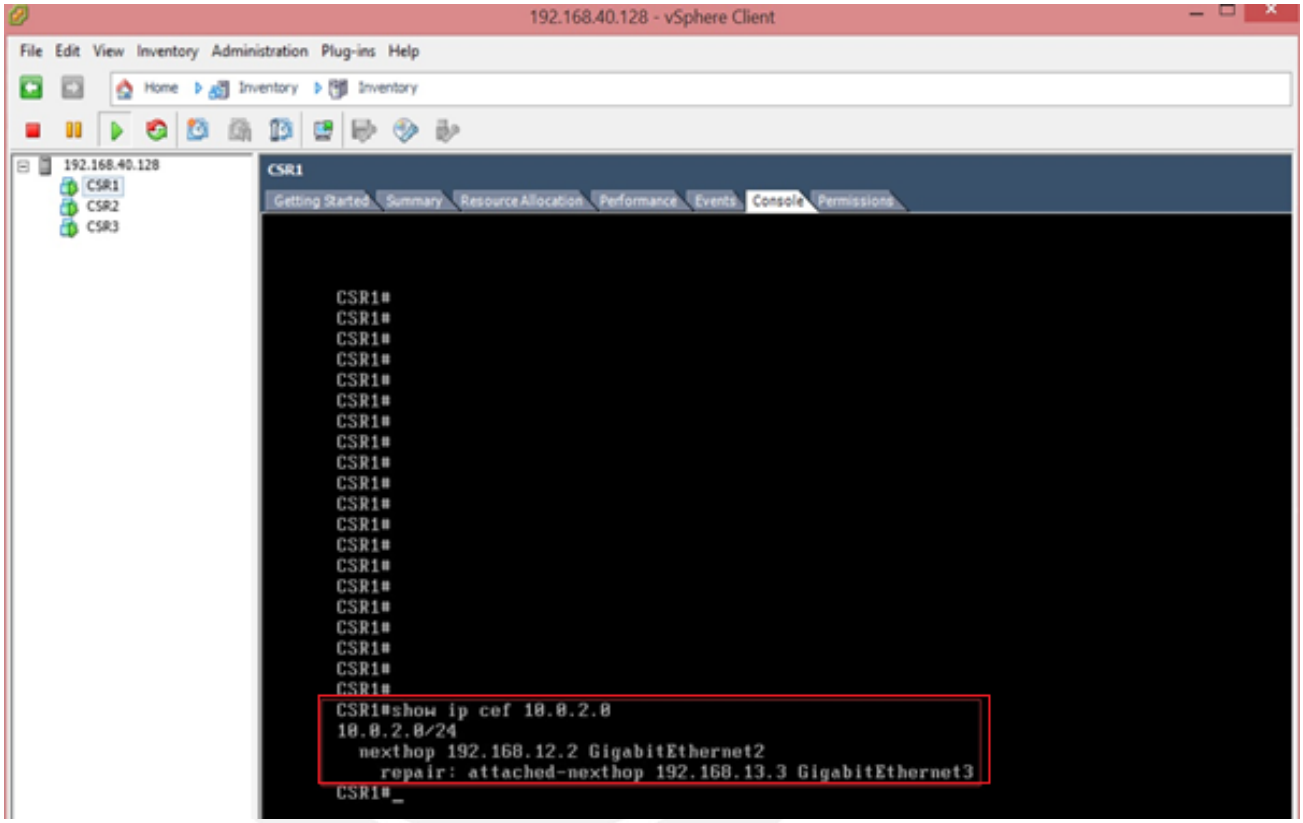

Figura N° 15: De acuerdo con la simulación, en CSR1 se observa un enrutador de respaldo con IP 192.168.13.3 (CSR3) instalado en la CEF, ofreciendo una ruta alterna para la red 10.0.2.0/24.

Se configuró IP FRR en CSR2, teniendo al enrutador CSR1 con IP 192.168.12.1 como next-hop primario (véase: next-hop 192.168.12.1) y al enrutador CSR3 con IP 192.168.23.3 como next-hop alterno (véase: repair: attached-nexthop). La Figura N° 16 muestra la CEF de CSR2.

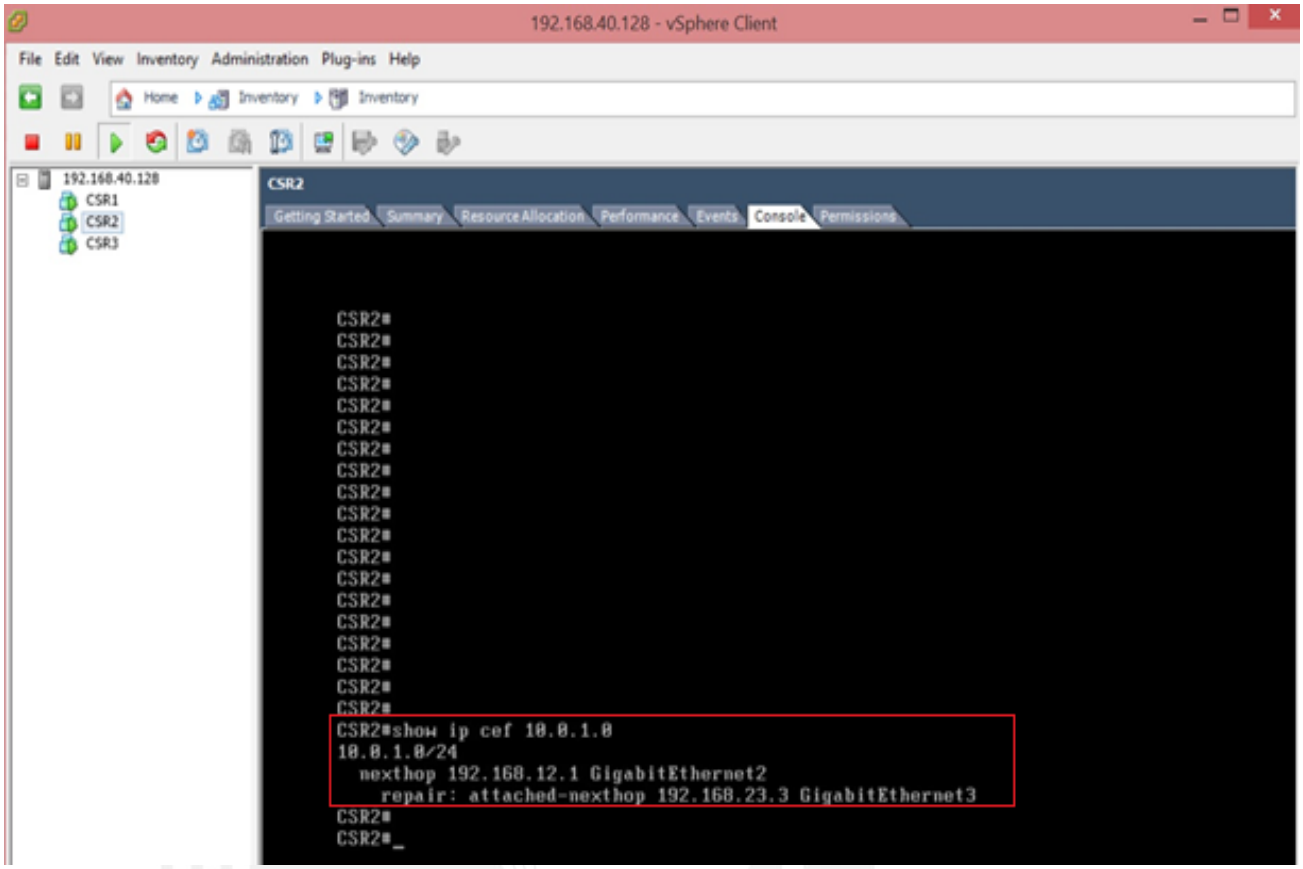

Figura N° 16: De acuerdo con la simulación, en CSR2 se observa un enrutador de respaldo con IP 192.168.23.3 (CSR3) instalado en la CEF, ofreciendo una ruta alterna para la red 10.0.1.0/24

Desde CSR1 y con la finalidad de estimar el tiempo de reconvergencia luego de ocurrir la falla del enlace entre CSR1 y CSR2, se simula una prueba de conectividad con la herramienta “ping” con destino en la Loopback 2 de CSR2 y con origen en la Loopback 1 de CSR1; y simulando la falla del enlace entre estos enrutadores. En la Figura N° 17 se observa 3 puntos (véase: **!!!...!!!**), los cuales indican 3 paquetes perdidos antes de restablecerse la conectividad en la topología propuesta.

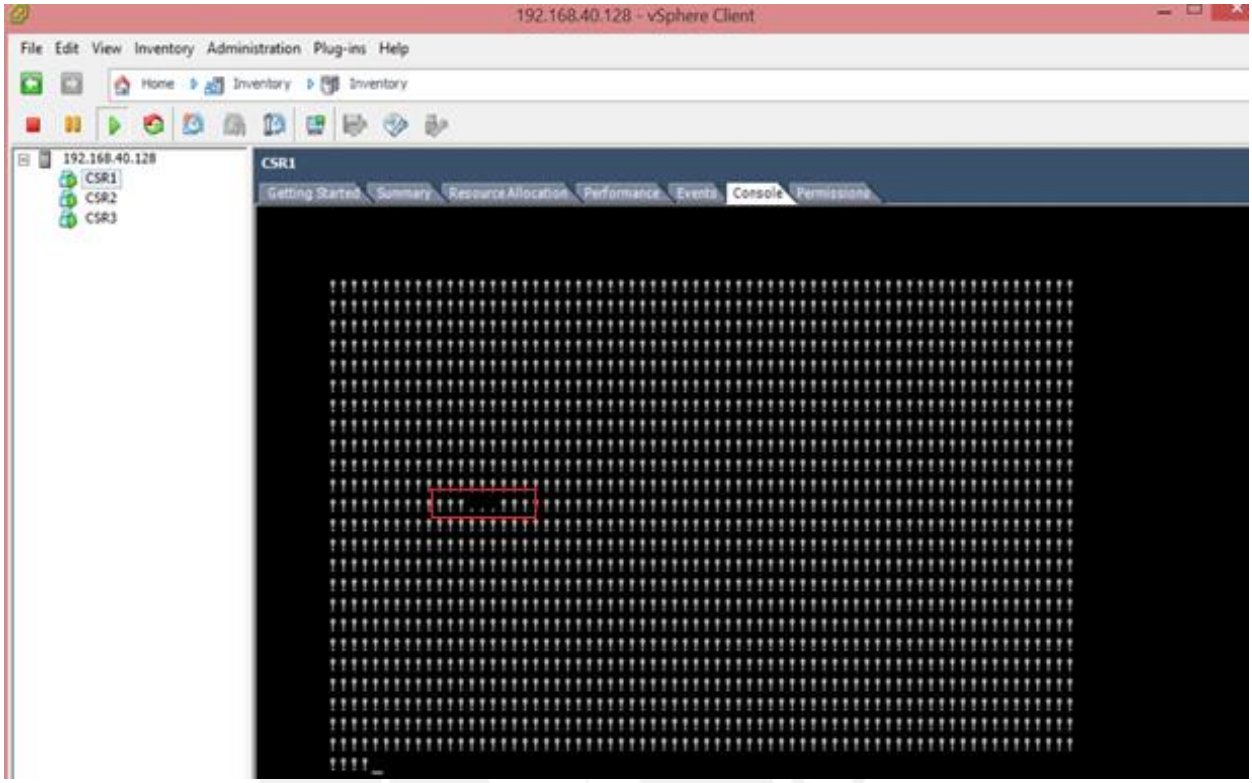

Figura N° 17: En la simulación se realizó una prueba de conectividad desde CSR1 hacia CSR2. Se observa 3 puntos (…) lo cual significa que se perdieron 3 paquetes antes de recuperar la conectividad.

Se precisa que en una prueba de conectividad con la herramienta “ping”, un enrutador CISCO envía paquetes icmp. De recibir respuesta al mismo en un tiempo menor o igual a 2 segundos, el IOS muestra el signo (**!**) y de no recibir la respuesta en el intervalo de tiempo señalado, el IOS muestra un punto (**.**) y declara el paquete como paquete perdido.

En la Figura N° 17 se observa 3 paquetes perdidos (véase 3 puntos: **…**), en consecuencia se estima un tiempo de reconvergencia de 7 segundos antes de restablecerse la conectividad entre las interfaces Loopbacks de interés. Se estimó un tiempo de reconvergencia similar al realizar la prueba de conectividad entre las Loopback 2 en CSR2 y la Loopback 1 en CSR1. El tiempo estimado obtenido se logró al tener instalado en CSR1 y CSR2 un next-hop alterno en la CEF de ambos enrutadores, siendo dicho next-hop CSR3 para ambos en la presente topología.

Para mayores detalles de configuración, véase el Anexo II.

2.4 Tercera Simulación: Topología de red utilizada para la simulación de TE/IP FRR y Optimizaciones

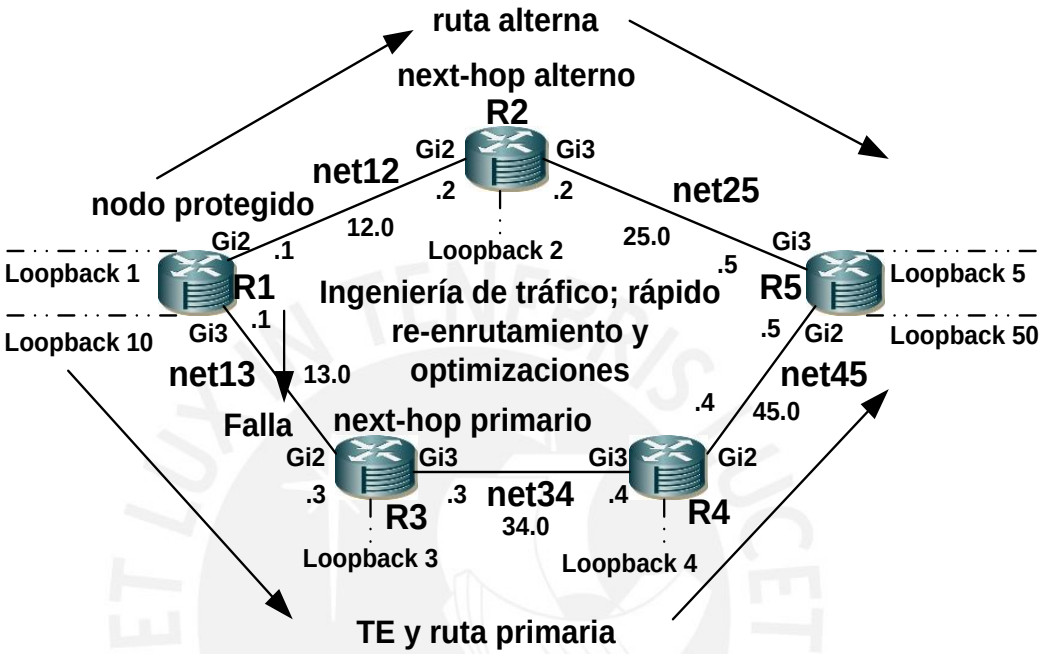

Figura N° 18: Simulación de TE/IP FRR y Optimizaciones [3,4].

La presente simulación se realizó en ESXi 5.5 con vSphere Client 5.5. Esta simulación propone establecer una ruta con reserva de ancho de banda, instalar un next-hop de respaldo en la CEF del enrutador R3 y restablecer la conectividad en un tiempo menor o igual a 5 segundos luego de ocurrida la falla del enlace entre 2 enrutadores en la ruta establecida. Se precisa que las interfaces en los 5 enrutadores son GigabitEthernet (a 1000 Mb/s).

Se configuró el direccionamiento IP de acuerdo a las direcciones señaladas en la Figura N° 18, se configuró OSPF para tener conectividad IP. Se configuró MPLS y MPLS TE para transportar información de reserva de ancho de banda en las interfaces de los enrutadores involucrados con la finalidad de que OSPF TE utilice dicha información para el establecimiento de la ruta. Se configuró IP FRR en R3 para que R3 instale en la CEF un next-hop de respaldo.

Tal como se observó IP FRR restableció la conectividad en un tiempo estimado de 7 segundos. Para lograr un tiempo de reconvergencia que no supere los 5 segundos luego de ocurrir la falla en el enlace entre 2 enrutadores de la ruta establecida, es necesario optimizar la operación de OSPF referidos a: ***i)*** el temporizador para la generación de un LSA luego de ocurrido en cambio en la topología; y ***ii)*** el temporizador para actualizar el algoritmo SPF luego de recibir dicho LSA. Así como establecer los enlaces como redes punto a punto para OSPF con la finalidad de que no se generan LSA del tipo 2 y el protocolo BFD con la finalidad de detectar la adyacencia entre enrutadores vecinos directamente conectados.

Sin la información de TE, la ruta desde la Loopback 10 en R1 hacia la Loopback 50 en R5 seguirá R1-R2-R5 (192.168.12.2; 192.168.25.5).

Se configuró un TE TUNNEL desde R1 hacia R5 y desde R5 hacia R1 para tener TE, se reservaron en las interfaces: Gi3 de R1; Gi2 y Gi3 de R3 y R4; y en Gi2 de R5 30 Mb/s y con TE se estableció una ruta desde R1 hacia R5 y desde R5 hacia R1 con reserva de 30 Mb/s, así se estableció desde R1 hacia R5 la ruta R1-R3-R4-R5 (192.168.13.3; 192.168.34.4; 192.168.45.5) y desde R5 hacia R1 la ruta R5-R4-R3-R1 (192.168.45.4; 192.168.34.3: 192.168.13.1).

Desde R1 se observa la ruta utilizando la herramienta “traceroute” con destino en la Loopback 50 (192.168.50.5) y origen en la Loopback 10 (192.168.10.1) tal como se muestra en la Figura N° 19.

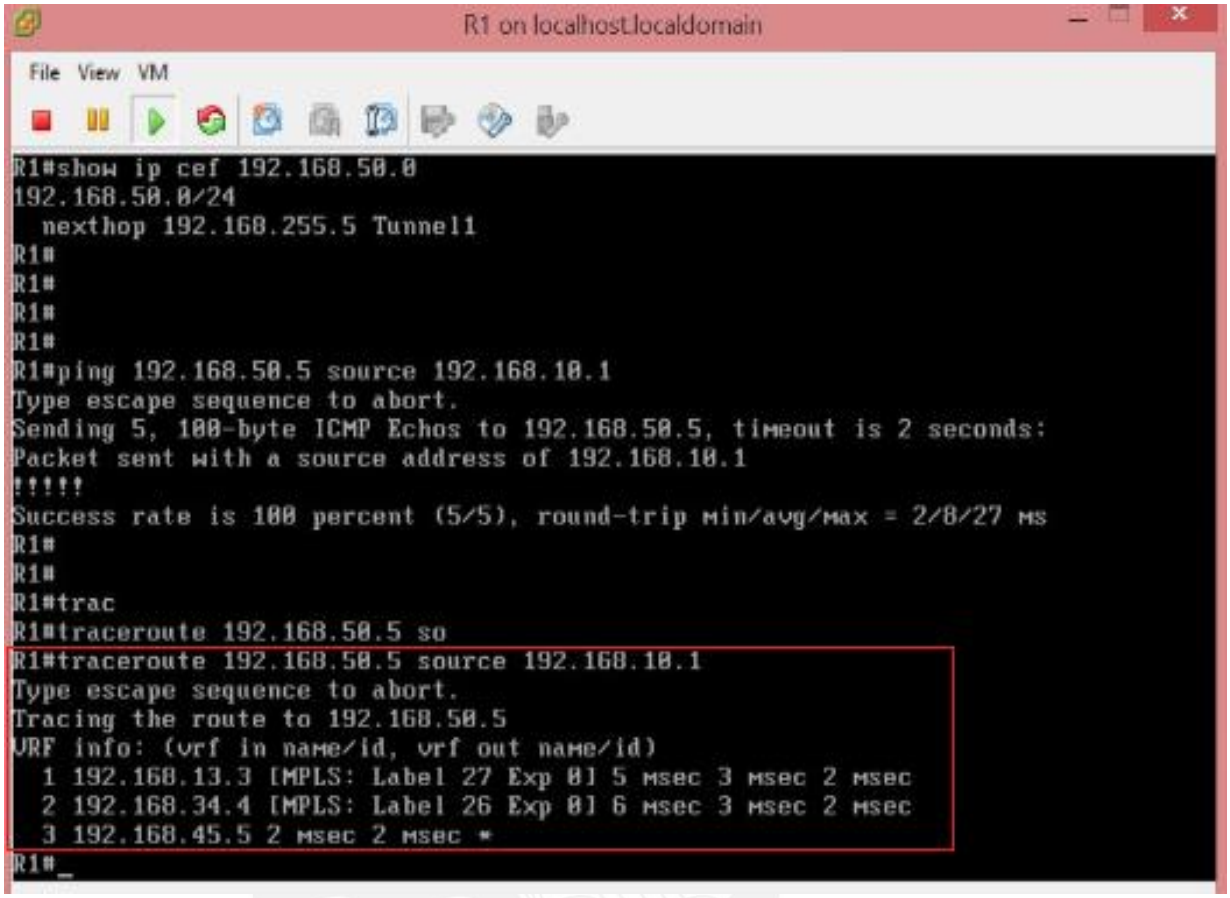

Figura N° 19: La simulación muestra la ruta seguida desde la Loopback 10 en R1 hacia la Loopback 50 en R5 con reserva de 30 Mb/s, lo cual es posible debido al soporte de MPLS.

Análogamente desde R5 hacia R1 se observa la ruta utilizando la herramienta “traceroute” con destino en la Loopback 10 (192.168.10.1) y origen en la Loopback 50 (192.168.50.5) tal como se muestra en la Figura N° 20.

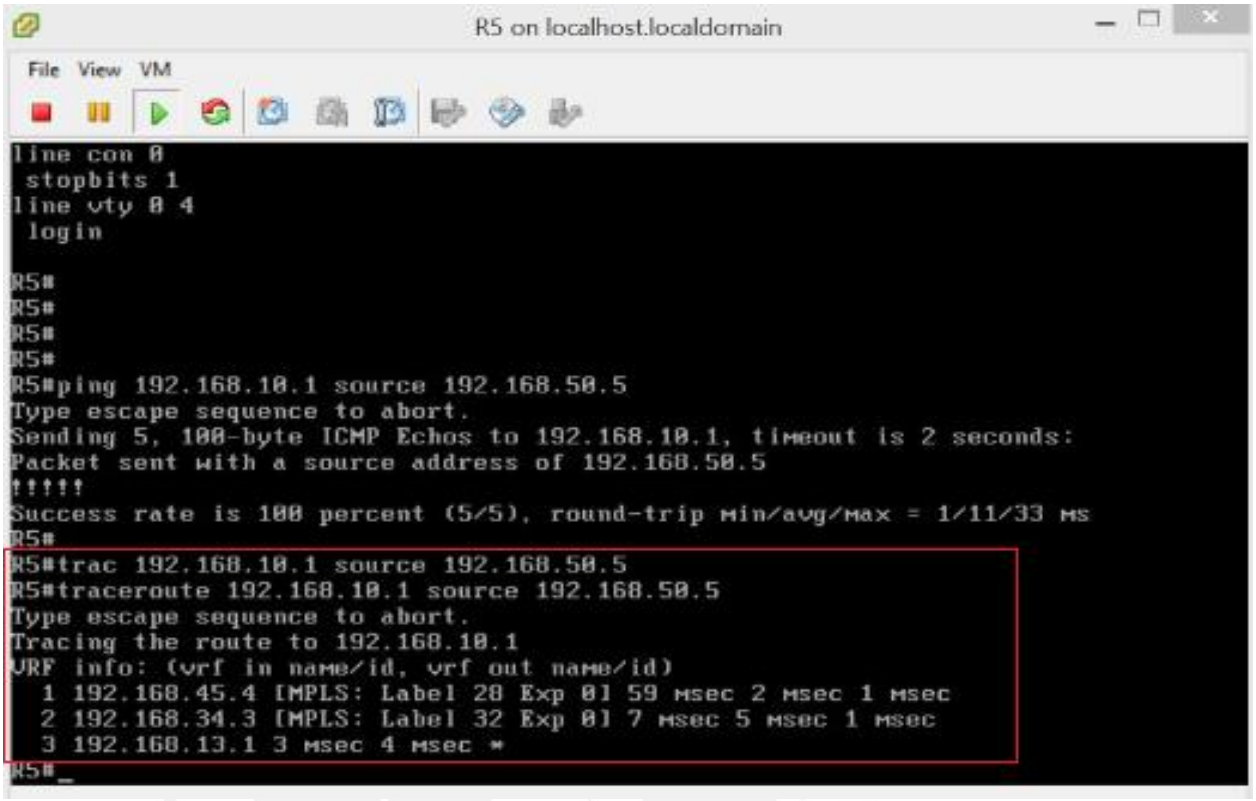

Figura N° 20: La simulación muestra la ruta seguida desde la Loopback 50 en R5 hacia la Loopback 10 en R1 con reserva de 30 Mb/s, lo cual es posible debido al soporte de MPLS.

Se configuró IP FRR en R3 con la finalidad de tener instalado un next-hop de respaldo en la RIB y en el CEF de R3 con lo cual se protege el enlace entre los enrutadores R1 y R3 considerado en un inicio como un punto de falla o de mayor vulnerabilidad.

Obsérvese que de acuerdo a la presente topología, el next-hop de respaldo para R3 deberá ser R5 y no R4 por lo siguiente, ocurrida la falla del enlace entre R1 y R3, R4 intentará aún reenviar paquetes destinados hacia la Loopback 10 de R1 mediante R3; y si R3 tendría a R4 como el next-hop de respaldo, se producirá un loop de enrutamiento, por esta razón el next-hop de respaldo para R3 deberá ser R5. La realización de esta tarea es posible gracias al protocolo de señalización conocido como Protocolo de Distribución de Etiquetas (LDP) de MPLS.

En R3 se observa la RIB para la ruta 192.168.10.0/24 (véase: OSPF local RIB) y el next-hop instalado en el CEF de dicho enrutador, tal como se muestra en la Figura N° 21.

Obsérvese que el next-hop instalado tiene la IP 192.168.255.5 la cual se encuentra en R5 (véase: repair path via 192.168.255.5 y repair: attached-next-hop 192.168.255.5).

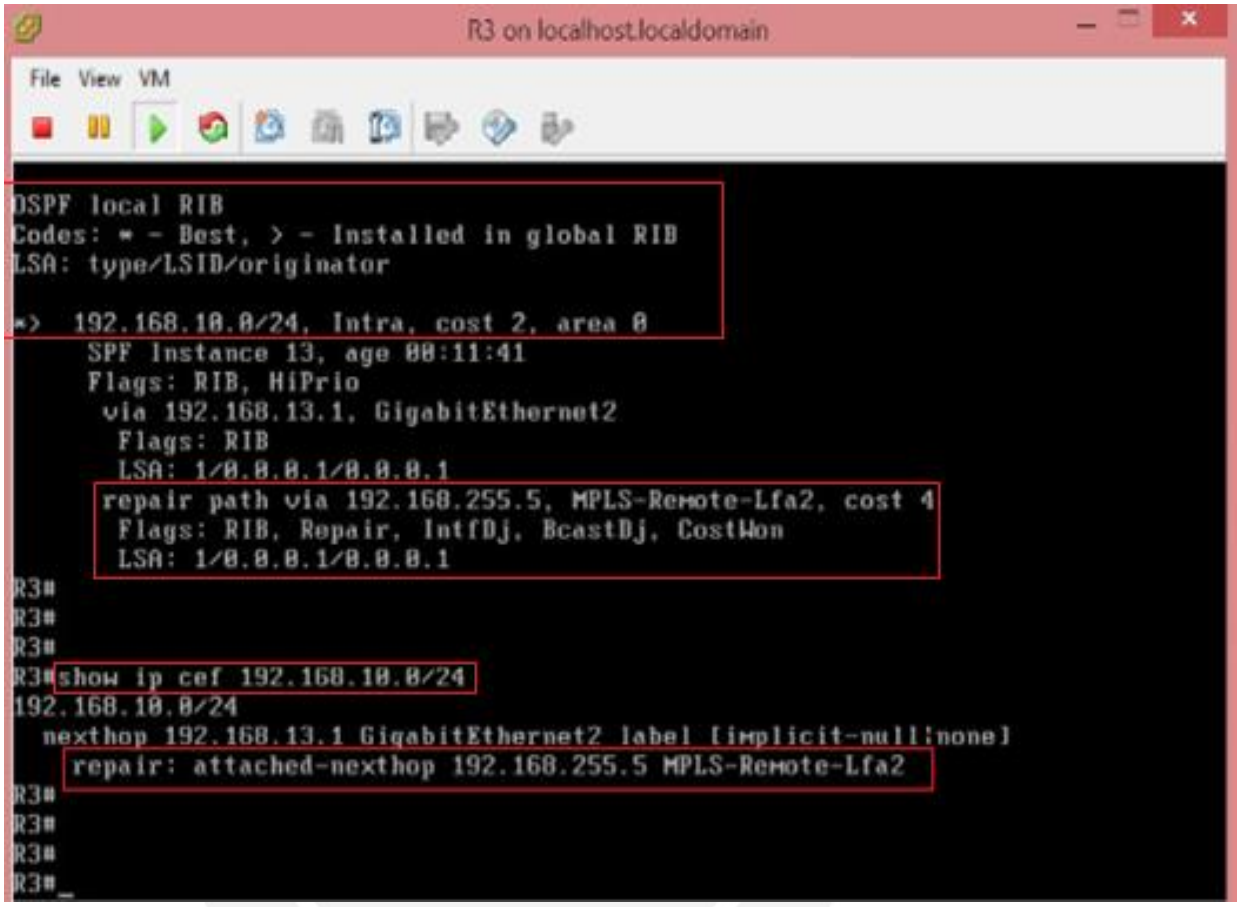

Figura N° 21: La simulación muestra que en la RIB y CEF de R3 se tiene una ruta de respaldo para la red 192.168.10.0/24 apuntando al enrutador R5 (192.168.255.5).

Adicionalmente en la Figura N° 22 se observa en R3 el IP FRR con la opción remota habilitada (véase: Interface MPLS-Remote-Lfa2), se observa la señalización utilizada en el túnel (véase: Tunnel type: MPLS-LDP) y la terminación en la IP 192.168.255.5 (véase: Termination IP address). Obsérvese que al no existir en la presente topología conectividad directa entre R3 y R5, la opción remota habilitada es necesaria, ya que para R3 el next-hop de respaldo no es R4 sino R5, evitando de esta manera un loop de enrutamiento, tal como se ha señalado.

Asimismo desde R3 se observa que el primer enrutador para alcanzar R5 es el enrutador con dirección IP 192.168.34.4 que corresponde a R4, ya que para que R3

alcance a R5 tiene que transitar por R4. Obsérvese que de esta manera se protege el enlace entre R1 y R3 (véase: Protects: 192.168.13.1).

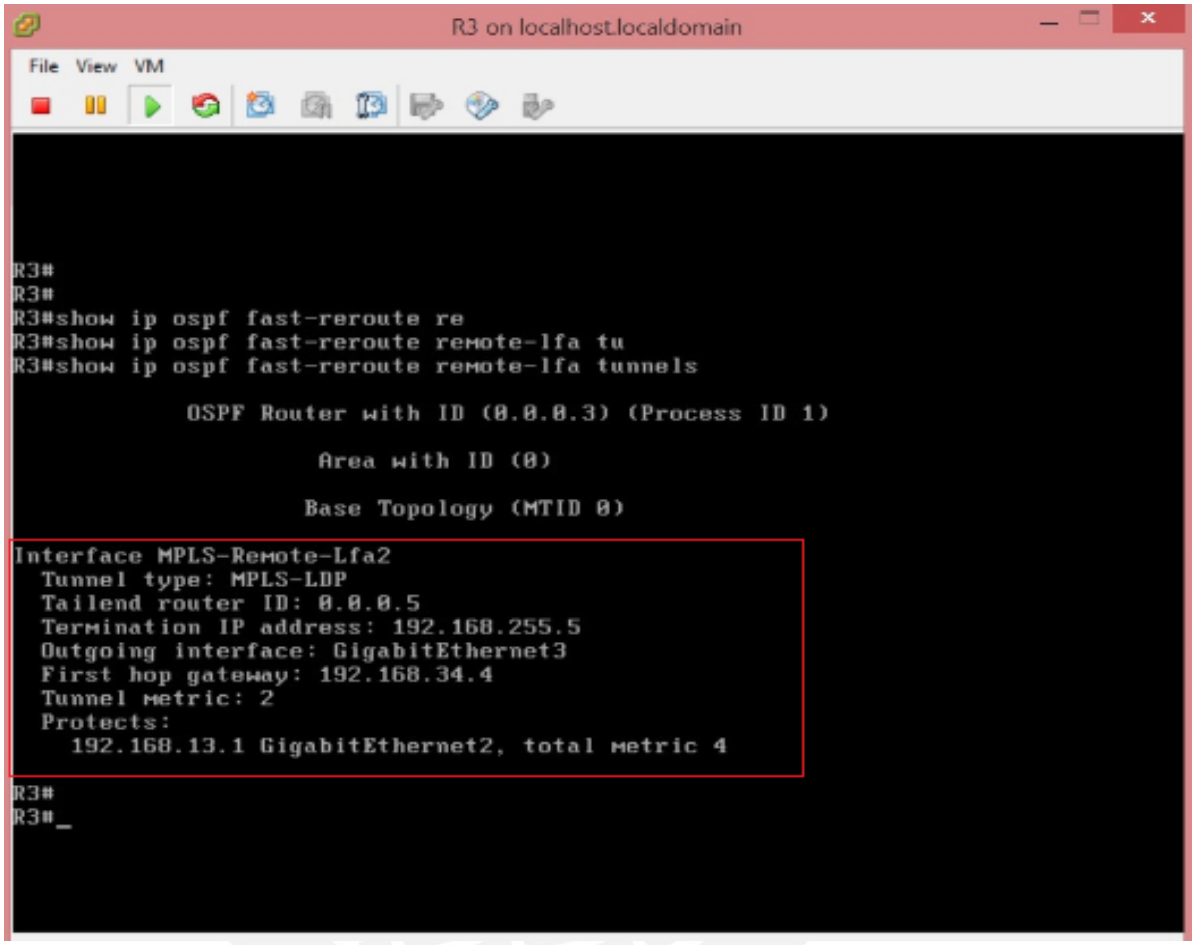

Figura N° 22: En el proceso de simulación se observa en R3 el funcionamiento del IP FRR con la opción remota necesariamente habilitada para la topología propuesta.

Con la finalidad de estimar un tiempo de reconvergencia que no supere a los 5 segundos luego de ocurrir una falla en el enlace entre 2 enrutadores de la ruta establecida, se optimizó los temporizadores de OSPF modificando los valores para: **timers throttle spf** y **timers throttle lsa**.

Se modificó el primer valor de **timers throttle spf** igual a 50 ms el cual indica el tiempo de espera para actualizar el algoritmo SPF luego de recibir un cambio en la topología. Se modificó el primer valor de **timers throttle lsa** igual a 20 ms el cual indica el tiempo de espera para generar un LSA luego de ocurrido un cambio en la topología.

En la Figura N° 23 se observa los valores utilizados para los temporizadores de OSPF, se establecieron todas las interfaces como redes punto a punto para OSPF, para evitar la generación de LSAs del tipo 2, se configuró BFD para la detección de adyacencia entre enrutadores directamente conectados en OSPF (véase: bfd all-interfaces). Dicha configuración se extendió a todos los enrutadores de la presente topología.

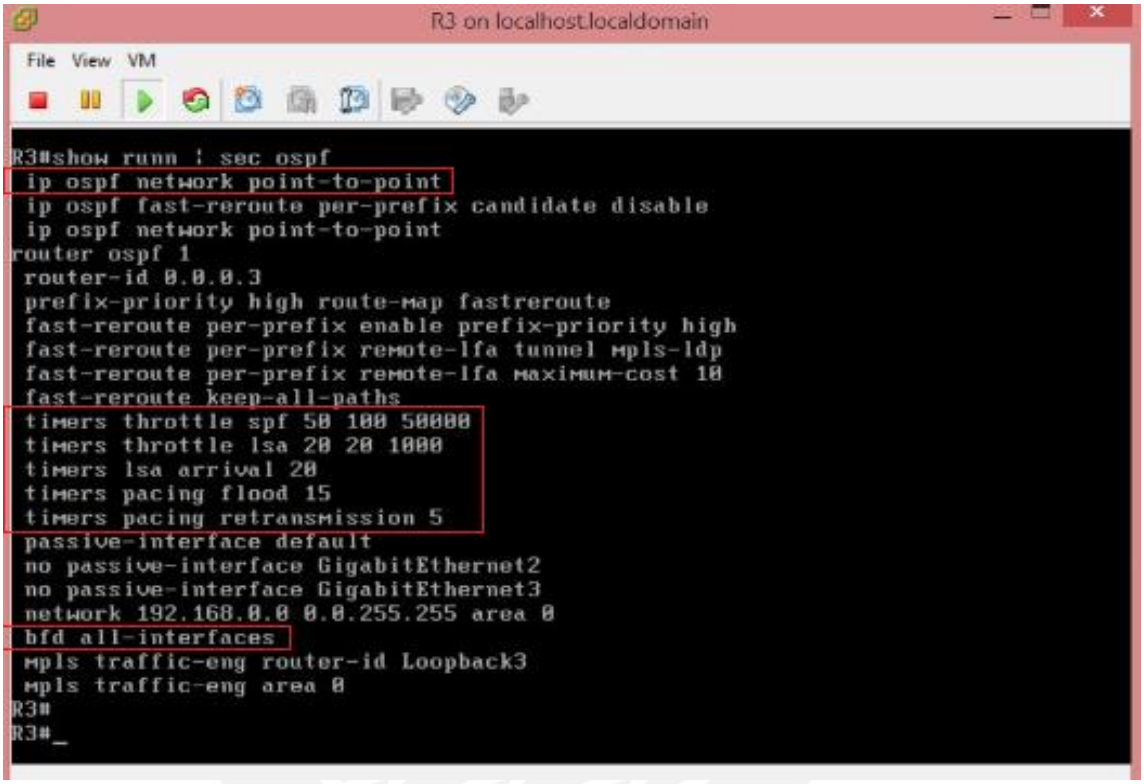

Figura N° 23: En la simulación se modificaron los temporizadores de operación de OSPF y uso del protocolo BFD, lo cual es observado en R3 y replicado a todos los enrutadores de la presente topología.

Asimismo se configuró BFD en las interfaces (véase: bfd interval 50 min_rx 150 multiplier 3) tal como se observa en la Figura N° 24.

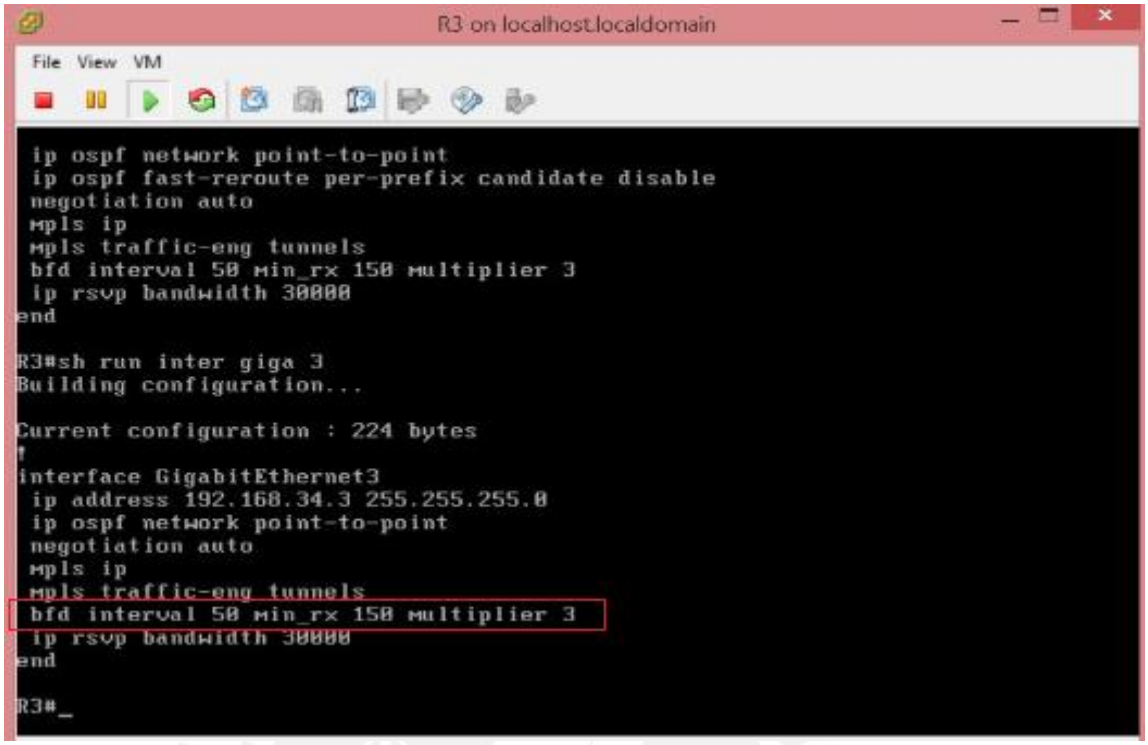

Figura N° 24: En la simulación se modificaron los valores de operación del protocolo BFD en las interfaces de todos los enrutadores, tal como se muestra en R3.

Se precisa que la finalidad es mantener la conectividad entre la interface Loopback 10 con IP 192.168.10.1 en R1 y la Loopback 50 con IP 192.168.50.5 en R5, tratando de obtener un tiempo de reconvergencia o recuperación que no supere los 5 segundos luego de ocurrir una falla del enlace entre 2 enrutadores de la ruta establecida por TE.

Para realizar la prueba de conectividad se utilizó la herramienta “ping” desde R1 con destino en la IP 192.168.50.5 y con origen en la IP 192.168.10.1 (desde R1 hacia R5), se simuló una falla del enlace entre R1 y R3 deshabilitando la interface Gi2 en R3 y observándose la pérdida de 1 paquete antes de restablecerse la conectividad, en consecuencia se estimó un tiempo de reconvergencia de 3 segundos.

De manera simultánea con la herramienta “ping” se realizó la prueba de conectividad desde R5 con destino en la IP 192.168.10.1 y con origen en la IP 192.168.50.5 (desde R5 hacia R1), observándose 1 paquete perdido y estimando 3 segundos para la reconvergencia.

En la Figura N° 25 se observa que se deshabilita la interface Gi2 en R3 simulando la falla del enlace entre R1 y R3.

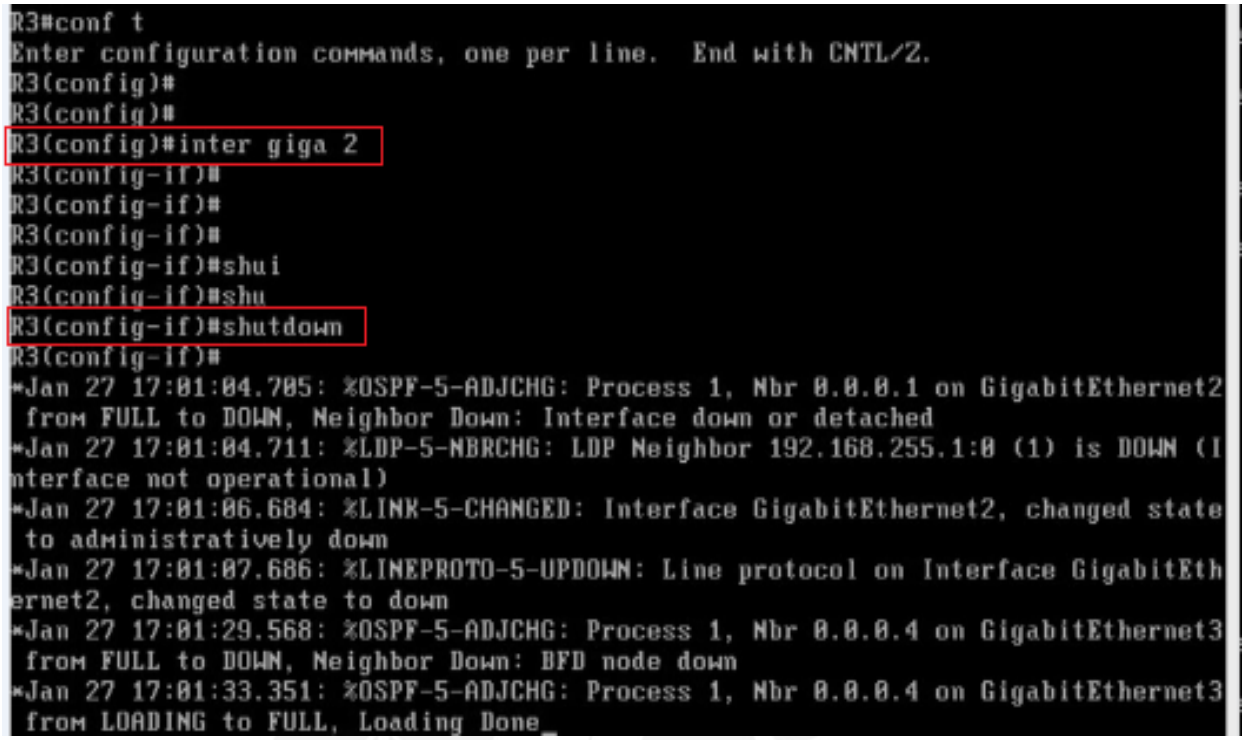

Figura N° 25: En la simulación de la prueba de conectividad, se simuló una falla del enlace entre R1 y R3, deshabilitando la interface Giga2 en R3.

En la Figura N° 26 se simuló el restablecimiento de la conectividad desde R1 hacia R5, se observa 1 paquete perdido (véase: **!!!.!!!** y **299/300**), se estimó un tiempo de reconvergencia de 3 segundos para el restablecimiento de la conectividad. Obsérvese que se reconverge o, lo que significa que se recupera la conectividad siguiendo la ruta R1-R2-R5 (192.168.12.2; 192.168.25.5), visto desde R1 (véase: traceroute).

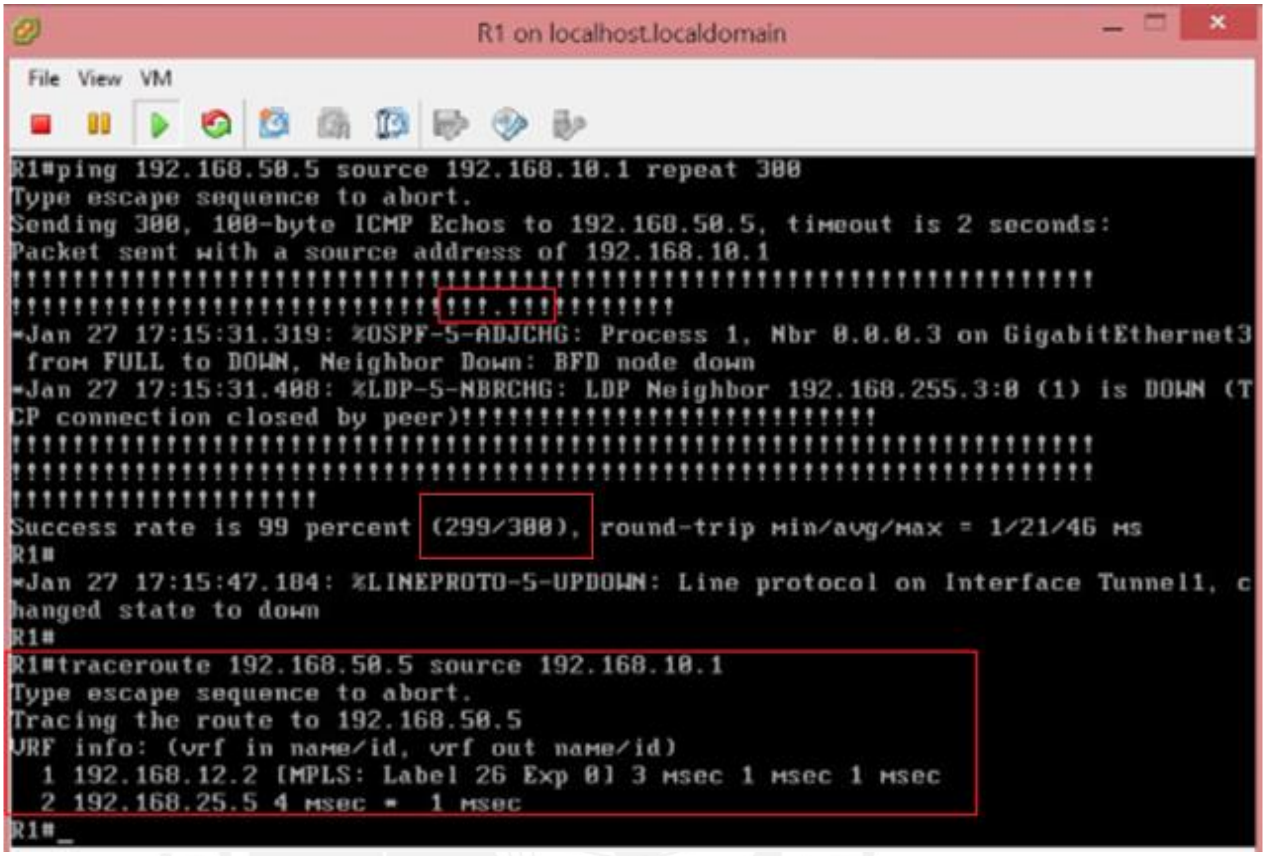

Figura N° 26: En la simulación de la prueba de conectividad realizada desde R1 hacia R5 se observa 1 punto (**.**) lo cual significa que se perdió 1 paquete antes de recuperar la conectividad, es decir la red reconverge luego de perder 1 paquete.

Análogamente se simuló el restablecimiento de la conectividad desde R5 hacia R1, se observó 1 paquete perdido (véase: **!!!.!!!** y **299/300**), se estimó un tiempo de reconvergencia de 3 segundos para el restablecimiento de la conectividad. Obsérvese que se reconverge siguiendo la ruta R5-R2-R1 (192.168.25.2; 192.168.12.1), visto desde R5 (véase: traceroute), tal como se observa en la Figura N° 27.

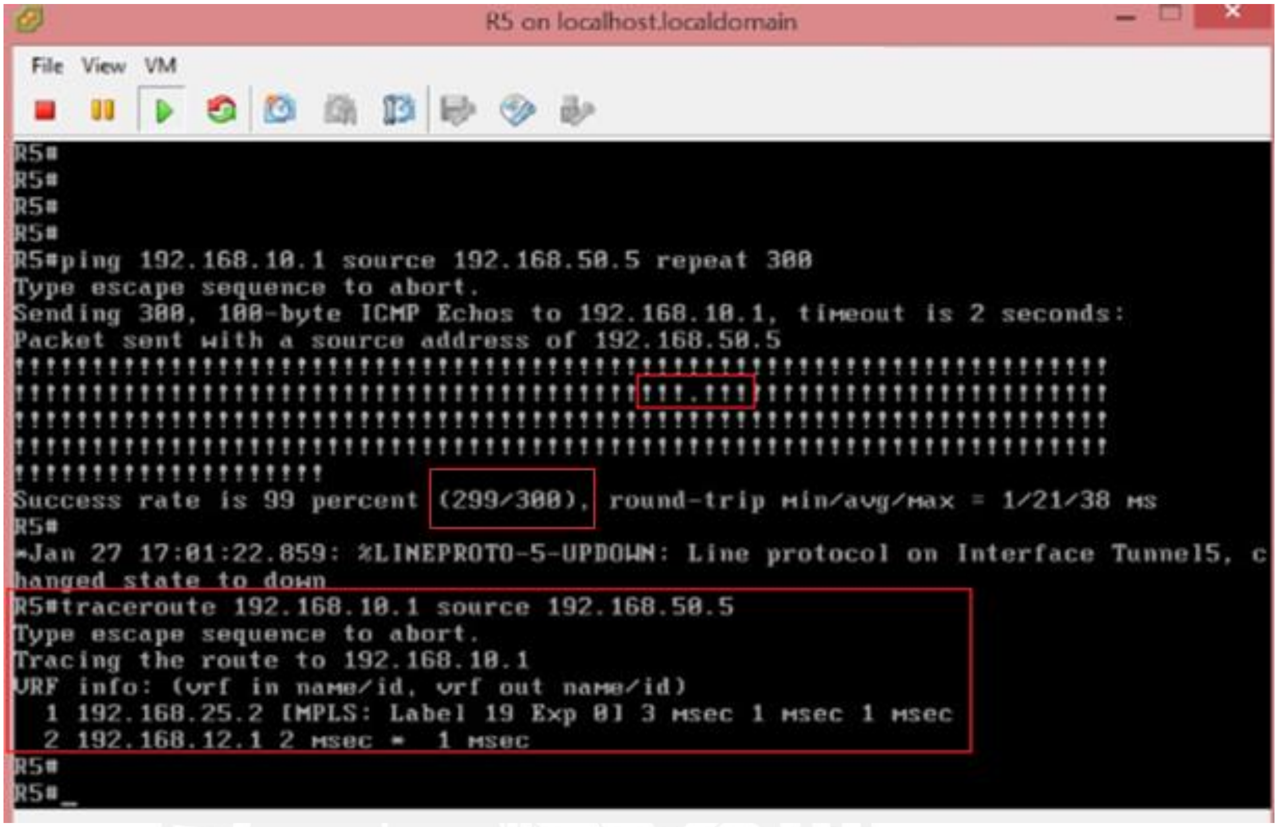

Figura N° 27: En la simulación de la prueba de conectividad realizada desde R5 hacia R1 se observa 1 punto (**.**) lo cual significa que se perdió 1 paquete antes de recuperar la conectividad, es decir la red reconverge luego de perder 1 paquete.

Así se observó que luego de simular la falla del enlace entre R1 y R3, se logró la reconvergencia en un tiempo estimado de 3 segundos, reestableciéndose o recuperándose la conectividad entre los puntos de interés.

Se reitera que el primer valor de **timers throttle spf** indica el tiempo de espera para iniciar la primera actualización del algoritmo SPF luego de recibir un LSA que notifica un cambio en la topología. Con la finalidad de estimar la variabilidad del tiempo de reconvergencia, se probaron los siguientes valores: **timers throttle spf 1200 2400 30000** y se entendió la misma configuración a los demás enrutadores.

Asimismo se reitera que se fijó el primer valor de **timers throttle lsa** en 20 ms, el valor en mención refiere al temporizador de espera para generar el primer LSA luego de ocurrir un cambio en la topología, en consecuencia al utilizar dicho valor en todas las pruebas de conectividad anula el uso del BFD.

Cabe precisar que se utilizó la siguiente configuración para el BFD en todas las interfaces: **bfd interval 50 min_rx 150 multiplier 3**, por tanto los 20 ms incluido en el primer parámetro de **timers throttle lsa** adelantan a los 50 ms para la detección de adyacencia del BFD (primer valor de: **bfd interval**). Bajo estas condiciones, el uso del BFD no interviene en la estimación del tiempo de reconvergencia.

En la Figura N° 28 se observa los valores utilizados para: **timers throttle lsa 1200 2400 30000** en R2, recordar que se extendió la misma configuración hacia los otros enrutadores.

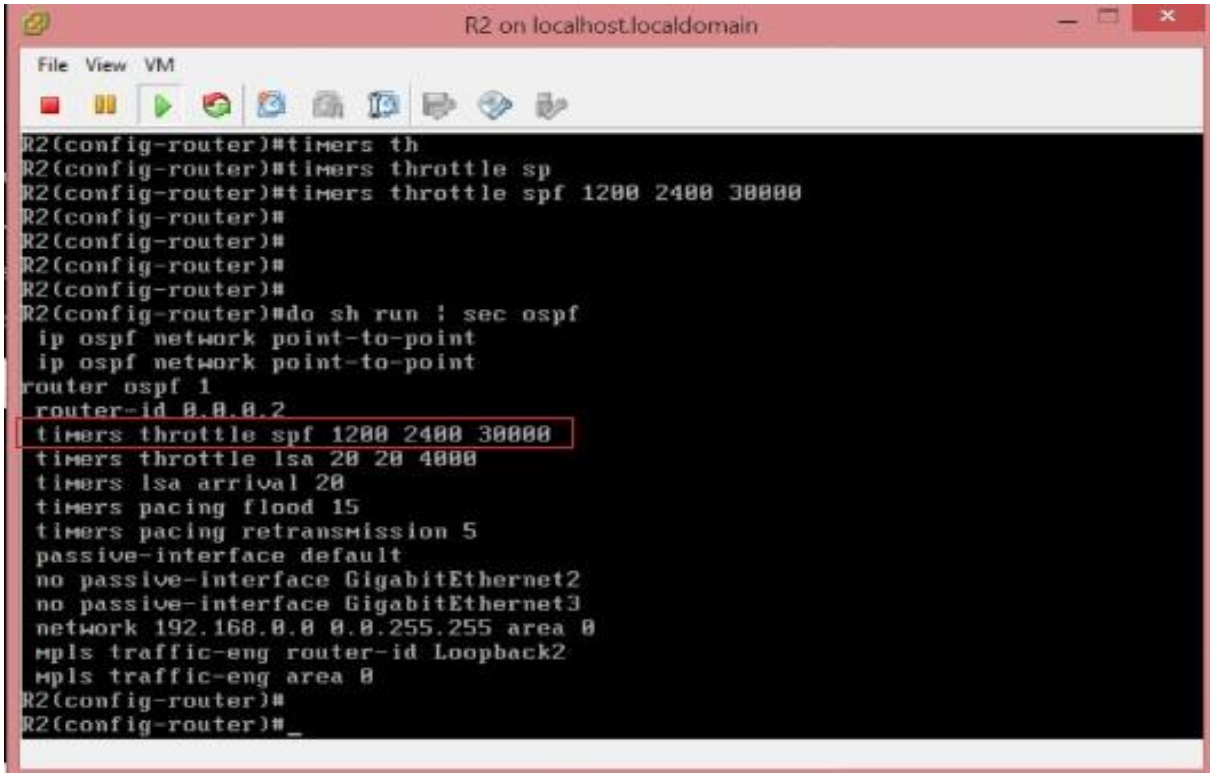

Figura N° 28: En la simulación se modificaron los temporizadores de operación de OSPF en los parámetros que corresponden a: timers throttle spf 1200 2400 30000.

Se simuló nuevamente la prueba de conectividad entre los puntos de interés, siguiendo la secuencia señala para dicha prueba, se obtuvo 1 paquete perdido tanto desde R1 hacia R5 como desde R5 hacia R1, estimándose un tiempo de reconvergencia de 3 segundos para el restablecimiento de la conectividad entre los puntos de interés.

Asimismo de acuerdo a las simulaciones realizadas, se estimó un tiempo de reconvergencia de 3 segundos para restablecer la conectividad entre los puntos de interés, simulando una falla en cualquier enlace de la ruta R1-R3-R4-R5. Para ello se utilizó 20 ms como temporizador de espera para generar el primer LSA luego de detectar un cambio en la topología y un valor menor o igual a 1200 ms como temporizador de espera para la primera actualización del algoritmo SPF.

Se varió los valores de operación a: **timers throttle spf 1500 3000 15000** en todos los enrutadores de la red propuesta, se simuló la prueba de conectividad entre los puntos de interés (desde la Loopback 10 en R1 hacia la Loopback 50 en R5 y viceversa) simulándose la falla del enlace entre R1 y R3, obteniéndose 2 paquetes perdidos y estimándose un tiempo de 5 segundos para el restablecimiento de la conectividad. En la Figura N° 29 se observa 2 paquetes perdidos (véase: **!!!..!!!** y **598/600**) y se estimó un tiempo de reconvergencia de 5 segundos.

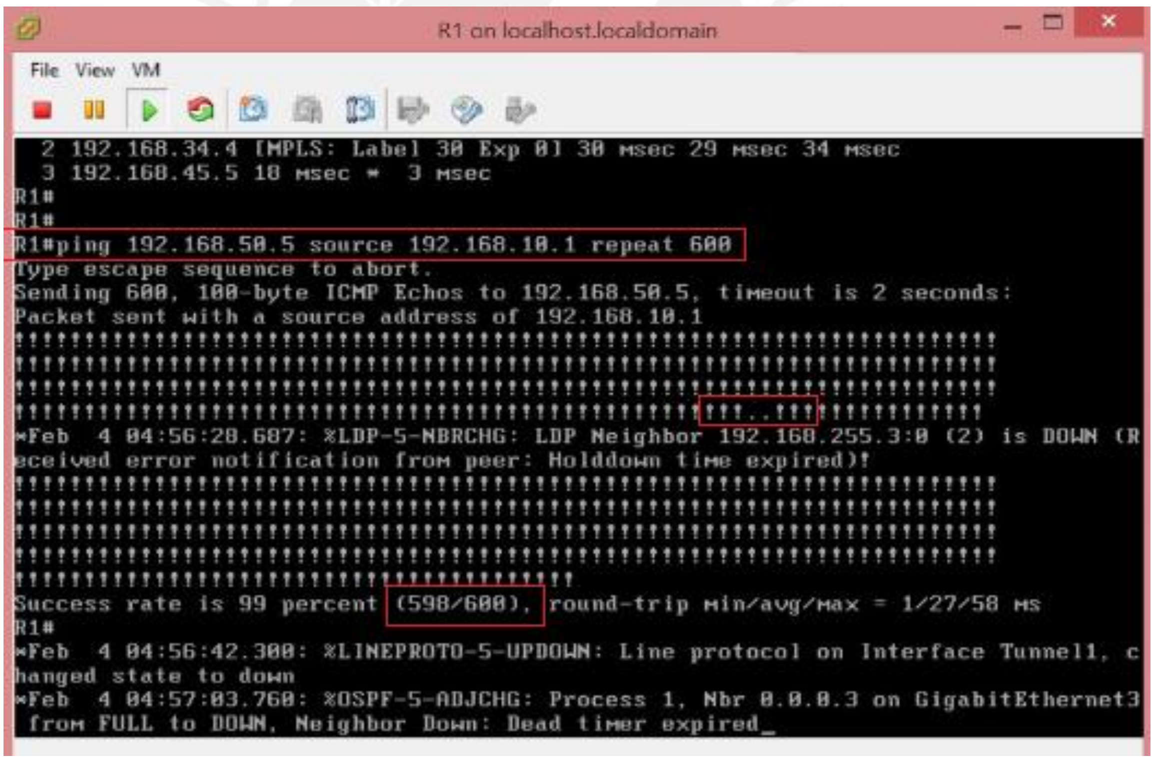

Figura N° 29: En la simulación de la prueba de conectividad realizada desde R1 hacia R5 se observa en este caso 2 puntos (**..**) lo cual significa que se perdió 2 paquetes antes de recuperar la conectividad, es decir la red reconverge luego de perder 2 paquetes.

Análogamente se simuló la prueba de conectividad desde R5 hacia R1, observando 2 paquetes perdidos (véase: **!!!..!!!** y **298/300**) y estimándose un tiempo de 5 segundos para la reconvergencia, tal como se muestra en la Figura N° 30.

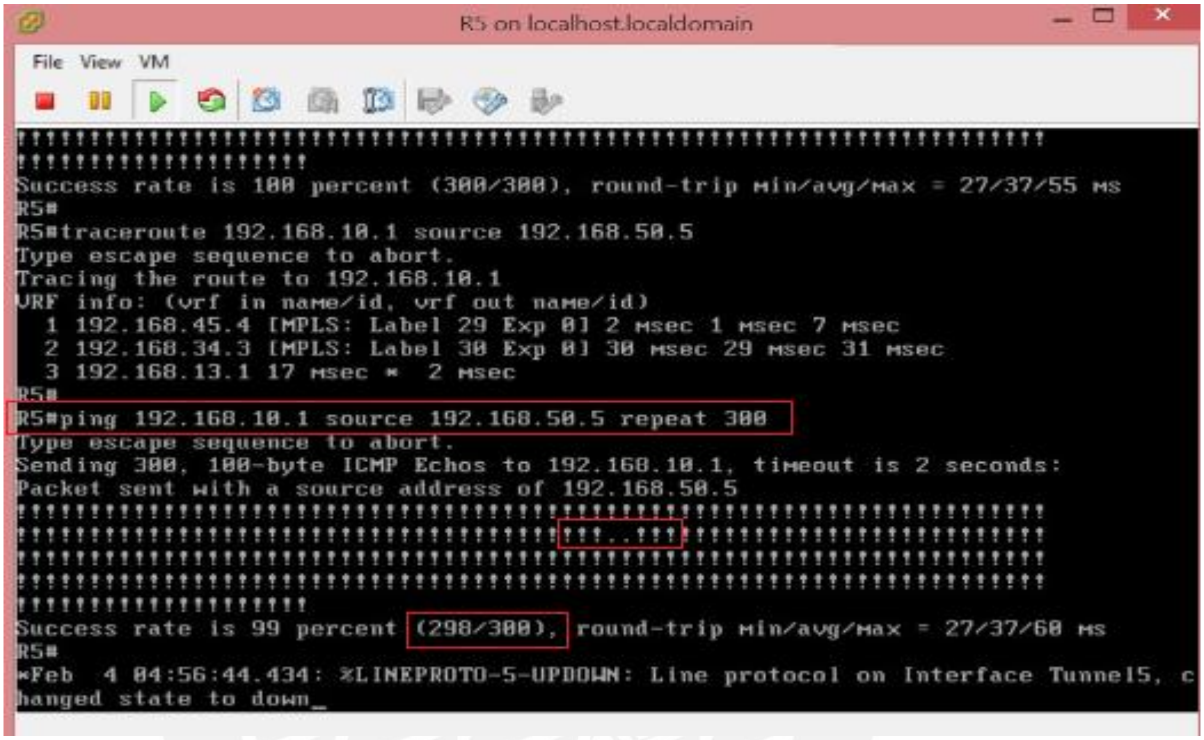

Figura N° 30: En la simulación de la prueba de conectividad realizada desde R5 hacia R1 se observa en este caso 2 puntos (**..**) lo cual significa que se perdió 2 paquetes antes de recuperar la conectividad, es decir la red reconverge luego de perder 2 paquetes.

Al variar los valores de operación a: **timers throttle spf 2000 4000 10000** en todos los enrutadores de la red propuesta y al simularse la prueba de conectividad entre los puntos de interés, se observó 2 paquetes perdidos y se estimó un tiempo de 5 segundos para el restablecimiento de la conectividad.

Asimismo al variar los valores de operación a: **timers throttle spf 3000 6000 50000** en todos los enrutadores de la red propuesta y al simularse la prueba de conectividad entre los puntos de interés, se observó 3 paquetes perdidos y se estimó un tiempo de 7 segundos para el restablecimiento de la conectividad.

En general al utilizar hasta 1200 ms como primer valor de: **timers throttle spf** y al simular la falla de cualquier enlace entre 2 enrutadores de la ruta establecida por TE

(R1-R3-R4-R5), se observó 1 paquete perdido y se estimó un tiempo de reconvergencia de 3 segundos para el restablecimiento de la conectividad entre los puntos de interés.

Se precisa que se utilizó en todas las simulaciones para las pruebas de conectividad, el valor de 20 ms como primer valor de: **timers throttle lsa** así dicho valor anula el uso del protocolo BFD, tal como se explicó anteriormente.

Asimismo al tener configurado el primer valor de 50 ms (valor mínimo posible de acuerdo con el IOS de CISCO) para la detección de adyacencia del protocolo BFD y que el primer valor en los parámetros de: **timers throttle lsa** corresponde al tiempo de espera para generar el primer LSA luego de ocurrir un cambio en la topología, en consecuencia al utilizar valores menores a los 50 ms como primer valor de **timers throttle lsa**, anula la participación del protocolo BFD en la estimación del tiempo de reconvergencia, motivo por el cual se escogió el valor de 20 ms, con la posibilidad de escoger un valor entero entre 0 y 50 ms.

Asimismo se reitera que la reconvergencia de una red es el proceso mediante el cual se sincroniza las tablas de reenvió de todos los enrutadores, luego de producido un cambio en la topología y restableciéndose la conectividad en la red [6].

Para mayores detalles de configuración, véase el Anexo III.

CONCLUSIONES y OBSERVACIONES

a) De acuerdo al valor mínimo posible de 50 ms para la detección de adyacencia en el protocolo BFD (según el IOS de CISCO) y debido a que el primer valor de: **timers throttle lsa** corresponde al tiempo de espera para generar el primer LSA luego de ocurrir un cambio en la topología, se concluye que al utilizar valores menores a los 50 ms como primer valor de **timers throttle lsa**, anula la participación del protocolo BFD en la estimación del tiempo de reconvergencia, con la posibilidad de escoger un valor entero entre 0 y 50 ms. Motivo por la cual se escogió 20 ms, el cual se utilizó en todas las simulaciones de las pruebas de conectividad realizadas.

b) Con un valor menor o igual a 1200 ms, como temporizador de espera para la primera actualización del algoritmo SPF, asegura la reconvergencia en un tiempo estimado de 3 segundos. Lo que significa que se recupera la conectividad en la red luego de 3 segundos de ocurrida la falla del enlace entre dos enrutadores de la ruta establecida mediante TE. Sin estas optimizaciones la reconvergencia se da en tiempos que superan los 5 segundos, no considerando APS.

c) Con un valor mayor o igual a 1500 ms, como temporizador de espera para la primera actualización del algoritmo SPF, se estimó un tiempo de reconvergencia 5 segundos. Asimismo se estimó un tiempo de reconvergencia entre 3 y 5 segundos al utilizar valores entre 1200 y 2000 ms como temporizador para la primera actualización del algoritmo SPF. Así al utilizar valores mayores o iguales a 3000 ms, como temporizador de espera para la primera actualización del algoritmo SPF, se estimó un tiempo de reconvergencia que superan los 5 segundos.

d) Simulando TE/IP FRR y Optimizaciones, se estableció mediante TE una ruta que cumpla con reservar un ancho de banda determinado, con IP FRR se instaló una ruta y un next-hop de respaldo en la RIB y CEF de un enrutador. Mediante optimizaciones se estimó 3 segundos para restablecer la conectividad en la topología luego de ocurrida la falla de un enlace entre dos enrutadores, teniendo como aporte recuperar la conectividad en algunos segundos sin la necesidad de requerir equipamiento adicional de respaldo ni enlaces ópticos, utilizando 20 ms como temporizador para generar el primer LSA luego de detectar un cambio en la topología y un valor menor o igual a 1200 ms como temporizador para la primera actualización del algoritmo SPF.

e) Este método de rápida reconvergencia utilizó protocolos estándares como OSPF y MPLS, en ese sentido es posible extenderlo hacia equipos de otros fabricantes. Con OSPF es posible optimizar otros temporizadores tal como el temporizador para la ejecución del algoritmo SPF luego de haber recibido un indicativo de cambio de topología. En el presente trabajo las optimizaciones de realizaron en la simulación del IOS y equipamiento CISCO. Se deberá evaluar los valores para estos temporizadores en cada plataforma y el modo de operación dentro de ellas, con la finalidad de optimizar la respuesta del protocolo ante situaciones de fallas.

f) Tal como se visto, la rápida reconvergencia descrita en el presente documento, se condiciona hacia la falla repentina de un solo enlace en la ruta establecida. De considerar fallas sucesivas en los enlaces de la ruta establecida, el tiempo de reconvergencia será mayor al logrado, incrementándose de acuerdo con la manera de operación, con los valores establecidos en la optimización de OSPF y de acuerdo al instante de tiempo donde ocurriría la falla luego de haber ocurrido el primer fallo en un enlace.

g) En la presente simulación, el tráfico de control tal como es el tráfico de operación del protocolo de enrutamiento utilizado, transita por el mismo enlace físico entre los enrutadores de la topología, así al tener todas las interfaces trabajando a plena carga (por ejemplo al 100% de su capacidad) indudablemente impactaría en la transmisión de dicho tráfico, el cual estará sujeto a retardos adicionales y pérdidas, impactando en el tiempo de reconvergencia de manera impredecible. En ese sentido, la solución propuesta está limita a seguir las llamadas buenas prácticas, teniendo en consideraciones factores de utilización del orden de 80 a 85% de la capacidad nominal de cada interface.

BIBLIOGRAFIA

[1] MARCANO, Diógenes
2011 *IMS IP Multimedia Subsystem*. Material de enseñanza. Lima: Pontifica Universidad Católica del Perú, Escuela de Postgrado. Consulta 04 de diciembre de 2014.

[2] GARCIA, Fernando
s/a *MPLS TE Fast Reroute* [diapositivas].S/c:S/e. Consulta 04 de diciembre de 2014. <ftp://ftp.registro.br/pub/gter/gter23/08-TE-FRR.pdf>

[3] DE GHEIN, Luc
2007 *MPLS Fundamentals*: *A Comprehensive Introduction to MPLS Theory and Practice.* Indianapolis: Cisco Press.

[4] CISCO SYSTEM
2006 *Packet Icon Library: Current as of February 2, 2006* [diapositivas]. S/c: Cisco System. Consulta 04 de diciembre de 2014. <http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/Proyecto%20final/GaleriadeIconosCISCO.pdf>

[5] TEARE, Diane
2010 *Implementing Cisco IP Routing (ROUTE): Foundation Learning Guide, Foundation learning for the CCNP ROUTE 642-902 Exam*. Indianapolis: Cisco Press.

[6] LAPUKHOV, Petr
2010 Comentario del 02 de junio de “OSPF Fast Converge”. Blog de INE. “Ospf-Fast-Converge”. Consulta 28 de enero de 2015. <http://blog.ine.com/2010/06/02/ospf-fast-convergenc>

[7] CISCO SYSTEM
2005 *“Bidirectional Forwarding Detection for OSPF”*. San Jose, CA, páginas 1-2, 7-8. Consulta 28 de enero de 2015. <http://www.cisco.com/en/US/technologies/tk648/tk365/tk480/technologies_white_paper0900aecd80244005.pdf>

[8] CISCO SYSTEM
2004-2007 *“Bidirectional Forwarding Derection”*. San Jose, CA, página 3-4, 8, 17-20. Consulta 28 de enero de 2015. <http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.pdf>

[9] PREVIDI, Stefano
2006 *IP Fast ReRoute Technologies* [diapositivas]. S/c:S/e. Consulta 04 de diciembre de 2014. <http://www.apricot.net/apricot2006/slides/conf/thursday/Stefano_Previdi_IPFRR-Apricot.pdf >

[10] Ericsson INC
2014 Fa*st Re-Route in IP/MPLS Networks Using ERICSSON'S IP Operating System* [diapositivas]. San Jose, CA: Ericsson Inc. Consulta 04 de diciembre de 2014. <http://archive.ericsson.net/service/internet/picov/get?DocNo=01/28701-FGB1010192>

[11] CISCO SYSTEM
2001 *"OSPFv2 Loop-Free Alternate Fast Reroute"*. Páginas 1-14. Consulta 04 de diciembre de 2014. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-lfa-frr-xe.pdf>

[12] ALCATEL-LUCENT SRA N°1
2010 *Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Serices: An Advanced Guide for VPLS and VLL*. Indiana: Wiley Publishing, Inc.

[13] CISCO SYSTEM
2010 *CCIE Routing and Switching: Certification Guide, Four Edition*. Indianapolis: Cisco Press.

[14] GARCIA YAGUE, Adolfo
2005 *Redes MPLS y GMPLS Servicios y Aplicaciones. Servicios y Aplicaciones* [diapositivas]. S/c: UNITRONICS COMUNICACOONES. Consulta 04 de diciembre de 2014. <http://www.ccapitalia.net/descarga/docs/2005-mpls-gmpls-v4.pdf>