UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

Tema:

Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales

Autor:

Gian Carlo Banchón Parra

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

MSc. Manuel Romero Paz

Guayaquil, 2 de diciembre del 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

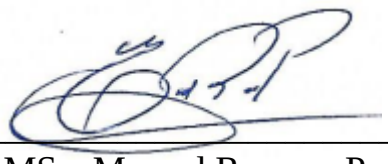
Certificamos que el presente trabajo fue realizado en su totalidad por el Ing. Gian Carlo Banchón Parra, como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, 2 de diciembre del 2020

TUTOR

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA



MSc. Manuel Romero Paz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, Gian Carlo Banchón Parra

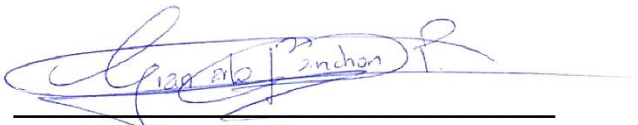
DECLARO QUE:

El trabajo de Titulación "Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales." previa a la obtención del Título de Magíster en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido

Guayaquil, 2 de diciembre del 2020

EL AUTOR



Gian Carlo Banchón Parra

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

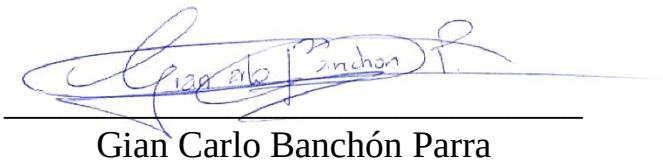
AUTORIZACIÓN

Yo, Gian Carlo Banchón Parra

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: "Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

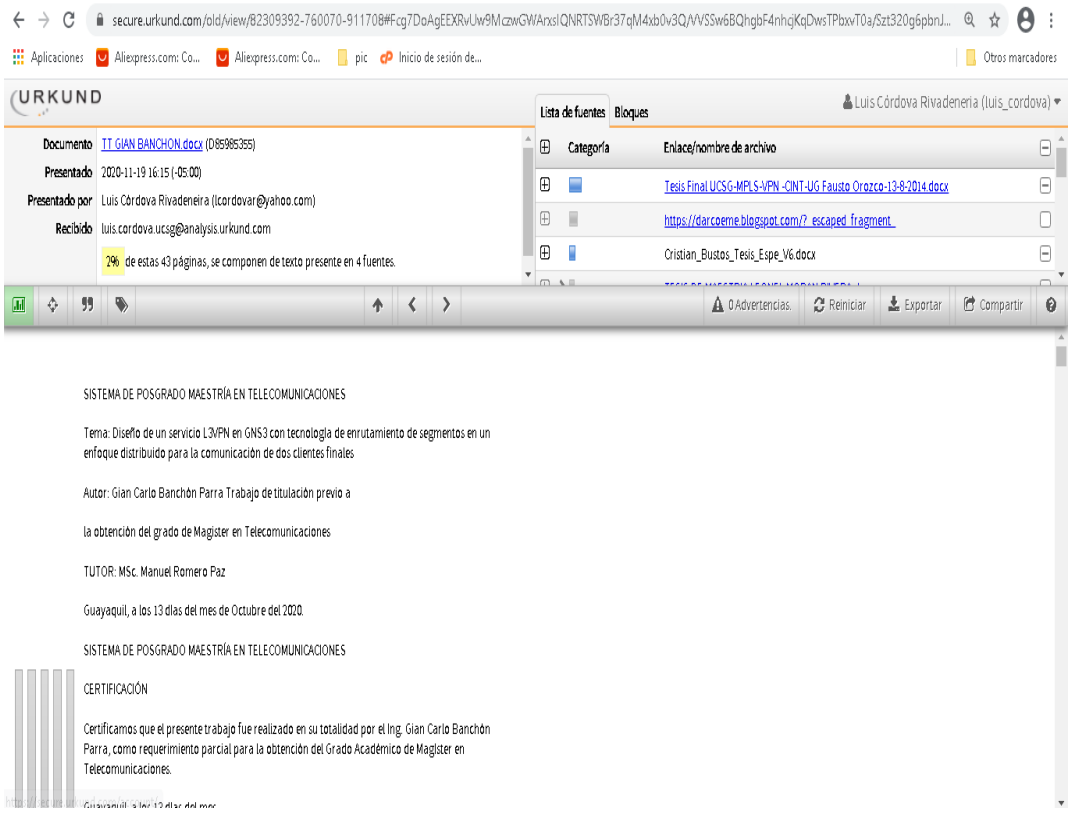
Guayaquil, 2 de diciembre del 2020

EL AUTOR



Gian Carlo Banchón Parra

REPORTE DE URKUND



secure.urkund.com/old/view/82309392-760070-911708#Fcg7DoAgEEXRvUw9MczwGWArxsIQNRTSWBr37qM4xb0v3Q/VVSSw6BQhgbF4nhcjKqDwsTPbxvT0a/Szt320g6pbnJ...

Aplicaciones | Aliexpress.com: Co... | Aliexpress.com: Co... | pic | Inicio de sesión de... | Otros marcadores

URKUND

Lista de fuentes | Bloques

Luis Córdova Rivadeneira (luis_cordova)

Documento	TT GIAN BANCHON.docx (D85985355)
Presentado	2020-11-19 16:15 (-05:00)
Presentado por	Luis Córdova Rivadeneira (lcordovar@yahoo.com)
Recibido	luis.cordova.ucsg@analysis.urkund.com
	2% de estas 43 páginas, se componen de texto presente en 4 fuentes.

Categoría	Enlace/nombre de archivo
	Tesis Final UCSG-MPLS-VPN -CINT-UG Fausto Orozco-13-8-2014.docx
	https://darcoerne.blogspot.com/?_escaped_fragment_
	Cristian_Bustos_Tesis_Espe_V6.docx

0 Advertencias. | Reiniciar | Exportar | Compartir

SISTEMA DE POSGRADO MAESTRÍA EN TELECOMUNICACIONES

Tema: Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales

Autor: Gian Carlo Banchón Parra Trabajo de titulación previo a

la obtención del grado de Magister en Telecomunicaciones

TUTOR: MSc. Manuel Romero Paz

Guayaquil, a los 13 días del mes de Octubre del 2020.

SISTEMA DE POSGRADO MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Ing. Gian Carlo Banchón Parra, como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

DEDICATORIA

Dedico mi tesis a Dios, ya que me ha brindado salud, la cual me ha permitido concluir exitosamente mi trabajo de titulación.

También a mi esposa Xiomara, a mis padres Juan y Yolanda, y mis hermanas, en especial a Karla, quienes han estado brindándome siempre su apoyo y han sido testigos del esfuerzo y sacrificio que se ha hecho para poder cumplir con una meta más en mi vida y siempre han estado ahí brindándome su apoyo incondicional.

Gian Banchón

AGRADECIMIENTOS

Agradezco a Dios ya que en estos momentos tan duros que estamos viviendo a nivel mundial por la pandemia, me ha brindado salud, en especial a mi familia y esposa, ya que siempre los ha cuidado.

También agradezco al Ing. Manuel Romero, ya que ha sido ese apoyo que necesita todo estudiante y mucho más que un tutor, decano o profesor te brinda la confianza de un amigo, lo cual me ayudó mucho para cumplir mis objetivos.

Gian Banchón

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

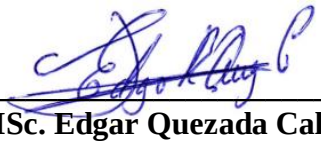
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

MSc. Manuel Romero Paz
Tutor

MSc. Manuel Romero Paz
Director del Programa

MSc. Luis Córdova Rivadeneira
Revisor



MSc. Edgar Quezada Calle
Revisor

RESUMEN

Uno de los nuevos retos a nivel de proveedor, es tener una red de transporte mucho más rápida y eficaz que consuma menos cantidad de recursos en los equipos de red y que se acople a las nuevas tecnologías de digitalización como 5G (Quinta Generación), IOT (Internet of Things), IA (Inteligencia Artificial), SDN (Software Defined Network), etc. A través de una simulación en GNS3 se levanta un servicio L3VPN (Layer3-Virtual Private Network) sobre una red de transporte con tecnología de enrutamiento de segmentos. Esto permite tener un conocimiento básico sobre el funcionamiento y la aplicación de esta nueva tecnología, la cual se basa en el enrutamiento de origen, que permite la reducción de estados en los routers de tránsito ya que la ruta hasta su destino la decide el router de ingreso, quien agrega a la cabecera del paquete el camino adecuado para llegar a su punto final. Por último, con el diseño y simulación de este proyecto de investigación se podrá demostrar los beneficios que presenta la tecnología de enrutamiento de segmentos en comparación con las redes actuales levantadas sobre MPLS.

Palabras Claves: 5G, IOT, IA, SDN, GNS3, L3VPN, MPLS, VPN.

ABSTRACT

One of the new challenges at the provider level is to have a much faster and more efficient transport network that consumes fewer resources in network equipment and that is coupled to new digitization technologies such as 5G (Fifth Generation), IOT (Internet of Things), AI (Artificial Intelligence), SDN (Software Defined Network), etc. Through a simulation in GNS3, an L3VPN (Layer3-Virtual Private Network) service is raised over a transport network with segment routing technology. This allows to have a basic knowledge about the operation and application of this new technology, which is based on source routing, which allows the reduction of states in transit routers since the route to its destination is decided by the router of income, who adds to the header of the packet the appropriate path to reach its end point. Finally, with the design and simulation of this research project it will be possible to demonstrate the benefits of segment routing technology compared to current networks built on MPLS.

Keywords: 5G, IOT, AI, SDN, GNS3, L3VPN, MPLS, VPN.

Índice General

Índice de Tablas

Índice de Figuras

CAPÍTULO 1: Descripción del proyecto de intervención

Con el reto de obtener una red de proveedor convergente, rápida, eficaz y preparada para el uso de nuevas tecnologías como 5G (Quinta Generación), IA (Inteligencia Artificial), IOT (Internet of Things) y SDN (Software Defined Network), se ve la necesidad de implementar una tecnología de transporte como el enrutamiento de segmentos, que elimina los protocolos de señalización que genera MPLS (Multiprotocol Label Switching), y basa su enrutamiento en el enrutador de origen, obteniendo redes óptimas y eficaces para el transporte de nuevas tecnologías.

1.1. Introducción

El desarrollo del tema a tratar en este documento, pretende presentar el beneficio que se puede obtener al aplicar la tecnología de enrutamiento de segmentos y las facilidades que le brinda al operador de red para realizar un troubleshotting, aumentando la efectividad y la rapidez en la solución de problemas en la red.

Una de las ventajas claves del enrutamiento de segmentos es su simplicidad, sólo toma pocas líneas de configuración para habilitarlo en el enrutador. Es particularmente útil en SDN, donde las nuevas necesidades comerciales requieren nuevas tecnologías y una granularidad más fina de ingeniería y diferenciación de tráfico. Se puede implementar en la red paso a paso, no hay necesidad de hacer actualizaciones masivas dentro en ella. Se puede integrar con redes MPLS existentes, ya que es interoperable con su plano de control y datos.

Segment Routing (SR) elimina protocolos de señalización pesados de MPLS y mueve la inteligencia al enrutador de origen, por lo tanto, elimina la complejidad de la red haciéndola más flexible para hacer frente a los patrones de tráfico en constante cambio, en volumen o tiempo. SR brinda un nuevo control sobre su infraestructura de red, usándola para obtener una manera simple y

escalable de enfrentar los desafíos que trae la digitalización con la implementación de nuevas tecnologías.

El enrutamiento de segmentos es una tecnología que está ganando popularidad como una forma de simplificar las redes MPLS. Tiene los beneficios de interactuar con redes definidas por software y usar el enrutamiento basado en la fuente, es decir, permite a los enrutadores de origen incluir instrucciones de enrutamiento en los paquetes IP para definir la ruta que tomarán a través de la red. Todo esto lo hace sin mantener cambios de estado en el núcleo de la red.

Una de las principales motivaciones que permite profundizar el estudio de esta tecnología de enrutamiento, es que, si se tiene como base una red MPLS y a ésta se le implementa SR, se resuelve en gran parte los problemas que actualmente generan sus protocolos, como LDP (Label Distribution Protocol) y RSVP (Resource Reservation Protocol), que demandan alto tráfico de señalización de extremo a extremo por cada LSP (Label Switch Path). SR utiliza un esquema de enrutamiento basado en el origen, en el que un nodo de red dirige un paquete en función de una lista de instrucciones que se encuentran en el encabezado del mismo llamados “segmentos”, por lo que no se necesita ninguna señalización mientras los cambios de estado se mantengan en el paquete, permitiendo así reducir la cantidad de memoria y de procesamiento necesario que requieren los routers para mantener los estados.

SR es un nuevo paradigma de enrutamiento que tiene como objetivo optimizar, simplificar y mejorar la escalabilidad de las redes basadas en IP/MPLS. El enrutador de origen elige una ruta y la inserta directamente en la cabecera del paquete como una lista ordenada de enlaces. Una ruta de SR no depende de la señalización hop-by-hop, del protocolo de distribución de etiquetas (LDP) o del protocolo RSVP, más bien, utiliza "segmentos" para el envío. En general, una red mucho más simple de administrar y operar. El enrutamiento de segmentos también puede funcionar con un plano de datos MPLS o IPv6 y se integra con amplias capacidades de múltiples servicios de estos, incluyendo Layer3 VPN (Virtual Private Network) y Ethernet VPN (EVPN).

En una red SR, los "segmentos" representan enlaces de red, nodos o servicios. Una ruta que atraviesa un paquete IP en una red es similar a una trayectoria de conducción de automóviles que generalmente incluye carreteras, intersecciones y un destino, una intersección representa un segmento de nodo de red, una carretera entre dos intersecciones representa un segmento de enlace y un destino representa un segmento de servicio de red. En una red de transporte IP/MPLS, un segmento de nodo representa un enrutador habilitado para MPLS, un segmento de enlace representa una conexión entre dos enrutadores adyacentes y un segmento de servicio representa un servicio VPN de cliente (una VPN de capa 3 o VPN de capa 2), Ver figura 1.1

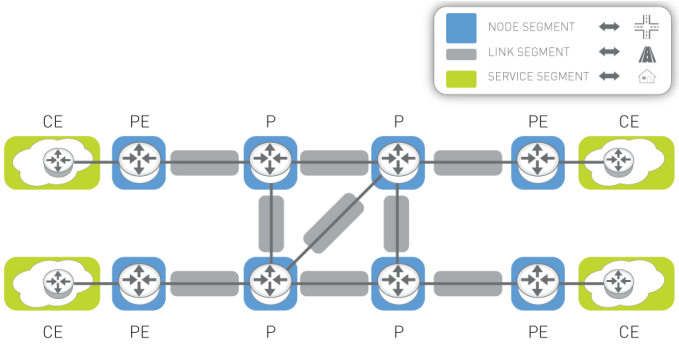


Figura 1.1 Ejemplo de simbología de Segment Routing
Fuente: (Said, 2019)

1.2. Antecedentes

Los proveedores de servicios y las grandes empresas enfrentan desafíos difíciles, la infraestructura de red y sus operaciones están creciendo a un ritmo acelerado y se están volviendo complejos. Las redes IP/MPLS, creadas hace más de 20 años, generan grandes cantidades de procesamiento en la red y se están volviendo muy complicadas en su administración e implementación. Los proveedores de servicios sienten la presión adicional de perder ingresos y tener una dura competencia por parte de los proveedores más importantes, así como el desafío de innovar. Esto hace que los propietarios de la red piensen en una tecnología de transporte que pueda proporcionar convergencia entre capas, y solucione las complejidades en las redes de hoy en términos de escalabilidad, simplicidad y facilidad de operación (Farrel & Bonica, 2017).

En noviembre de 2012 Clarence Filsfils divulgó el concepto de SR a los operadores de red. Un año después la IETF (Internet Engineering Task Force)

forma el Grupo de Trabajo SPRING (Source Packet Routing In Networking) para actividades de investigación y estandarización de SR. Y en 2015 EATCN (European Advanced Networking Test Center) ya condujo el primer evento público de interoperabilidad de SR. Avance rápido hasta entonces ya que esta interoperabilidad proporciona el último punto de prueba para el creciente soporte multi-vendor de SR (Liste, 2018).

Se observó que MPLS-TE (Multi-Protocol Label Switching – Traffic Engineering) requiere de estados explícitos a ser mantenidos en todos los saltos a lo largo de una ruta y esto puede conducir a problemas de escalabilidad en el plano de control y en el de datos. Además, MPLS-TE no explota fácilmente el equilibrio de carga ofrecido por ECMP (Equal Cost Multi-Path Routing), en redes IP simples. Por otro lado, SR puede dirigir el tráfico que fluye a lo largo de una ruta de ingeniería de tráfico, sin mantener el estado por flujo en los nodos a lo largo del camino, explotando el enrutamiento ECMP dentro de cada segmento.

SR es una tecnología de enrutamiento, que ha llamado la atención de los administradores de redes, debido a su potencial para simplificar y unificar la capa de transporte. Es basada en la fuente y permite que las redes IP / MPLS e IPV6 se ejecuten de manera más simple y escalen más fácilmente.

1.3. Planteamiento del problema

El gran crecimiento y la variedad de tráfico IP que actualmente una red de datos debe manejar, genera congestión y provoca lentitud debido a los altos procesamientos y consumos elevados de memoria que demandan los equipos, provocados por el alto tráfico de señalización que Actualmente es producido en una red MPLS por los protocolos que maneja, lo que conlleva a que el cliente tenga problemas y retardos en la recepción de datos, como también dificulta la solución de problemas por parte del operador de red.

Para la aplicación de tecnologías modernas como: conexiones M2M (Machine to Machine) que soportan las aplicaciones del Internet de las Cosas (IoT Internet of Things), hogares inteligentes, los servicios de salud, conectividad con

equipos médicos, automóviles inteligentes, etc., se requieren de redes IP basadas en MPLS mucho más flexibles, escalables y simples de operar. Por lo que se presenta la necesidad de contar con un protocolo de enrutamiento rápido y eficaz, que permita disminuir el consumo de memoria, procesamiento y tráfico de señalización que generan los equipos de Backbone en una red MPLS.

Este trabajo pretende demostrar a través de una simulación, la manera de implementar la tecnología de enrutamiento de segmentos aplicada a una red de proveedor que ofrece servicios L3VPN (Layer3 VPN) para la comunicación de clientes. Lo que conlleva a tener una red menos congestionada por la reducción del tráfico de señalización y, por ende, con menos consumo de recursos en los equipos, permitiendo de esta manera que los servicios que atraviesan la red del proveedor sean mucho más eficientes.

1.4. Definición del problema

Necesidad de implementar un diseño de servicio L3VPN en GNS3 con tecnología de Enrutamiento de Segmentos en un enfoque distribuido para la comunicación de dos clientes finales.

1.5. Justificación

Con los nuevos desafíos que trae la digitalización con la implementación de nuevas tecnologías como 5G, IoT, la inteligencia artificial (IA), SDN, y por la gran demanda de direcciones IP, los proveedores de red tienen que enfocarse en preparar de mejor forma su infraestructura, es así que, según el reciente estudio realizado por Cisco VNI (Visual Networking Index), cuyos pronósticos son claves para el 2022, indican que dentro de 2 años se creará más tráfico que el que se ha creado en las más de tres décadas que lleva internet, es decir que un 60% de la población mundial estará conectado a internet, generando 4.8 mil millones de usuarios o más de 28 mil millones de conexiones y dispositivos en línea. El video, los juegos y multimedia representarán más del 85% de todo el tráfico IP, es por esto que muchas empresas de telecomunicaciones piensan en usar nuevas tecnologías de transporte para mejorar las redes actuales basadas en MPLS.

El crecimiento sobrecargado de conectividad IP, necesita que a la red actual basada en MPLS, la cual ha sido de gran ayuda en estos últimos años debido a la facilidad y rapidez que brinda en los equipos de red al conmutar servicios basados en etiquetas, no ha reducido el alto consumo de recursos debido a la cantidad de caminos de señalización que se generan dentro de ellos por los protocolos LDP y RSVP. Por lo cual se ha tenido que migrar constantemente servicios MPLS como L3VPN (Layer 3 VPN), L2VPN (Layer 2 VPN), etc. a equipos más robustos con mayor performance, que soporten una cantidad mayor de etiquetas, lo cual no es tan factible debido a que los servicios son creados a través de túneles hacia enrutadores que se encuentran lejanos a la red de acceso para la cual fueron creados. Por tales motivos muchos proveedores de red están de acuerdo en implementar una tecnología de transporte que: elimine la necesidad de usar estos protocolos de señalización, obtenga los mismos resultados que MPLS, y prepare su red para nuevas tecnologías de digitalización.

1.6. Objetivos

A continuación, se detallan los objetivos planteados para la investigación.

1.6.1. Objetivo General

Diseñar un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos, en un enfoque distribuido para la comunicación de dos clientes finales.

1.6.2. Objetivos específicos

- ✓ Caracterizar la tecnología SR.
- ✓ Comparar las ventajas que brinda el enrutamiento de segmentos con una red MPLS.
- ✓ Diseñar un servicio L3VPN y simularlo en GNS3 con tecnología de enrutamiento de segmentos.

1.7. Hipótesis

El diseño y simulación en GNS3 de un servicio L3VPN para la comunicación de dos clientes finales sobre una red de transporte con enrutamiento de segmentos, permitirá tener un conocimiento más amplio acerca de esta nueva tecnología para el transporte de nuevos servicios de digitalización (IOT, 5G, SDN, IA), haciendo que éstos se adapten y funcionen rápidamente, sin causar pérdidas de información.

1.8. Metodología de investigación.

Para el desarrollo de este trabajo se utilizará un método descriptivo y experimental, con la finalidad de describir las características técnicas de la tecnología de enrutamiento de segmentos aplicada a un servicio L3VPN y experimental basado en un diseño aplicado a un caso de estudio, donde se recrea una red de un proveedor de servicios sobre la cual se implementará un servicio L3VPN.

Para concluir la investigación se utilizará un análisis explicativo de los resultados obtenidos en la implementación del diseño para demostrar el cumplimiento de los objetivos planteados.

CAPÍTULO 2: Fundamentación Teórica

En este capítulo se abarcará todos los temas y puntos que se debe conocer acerca de esta nueva tecnología de enrutamiento de segmentos, su aplicación y nuevas estructuras de funcionamiento, también se hará una comparación con el protocolo MPLS.

2.1. Introducción al Enrutamiento de Segmentos (SR)

Las actividades de investigación y estandarización de SR se originaron a fines de la década de 2000, principalmente con el objetivo de superar algunos problemas y limitaciones de escalabilidad que habían sido identificados en la Ingeniería de Tráfico con MPLS (MPLS-TE) utilizadas para redes de Backbone.

2.1.1. Enrutamiento de Origen

En contraste con el enrutamiento tradicional basado en el destino, se puede implementar enrutamiento de origen en una red, donde este elige la ruta y la codifica en el encabezado del paquete como una lista ordenada de segmentos, es decir el origen especifica la ruta que debe tomar un paquete a través de la red, así al viajar a través de esta, un enrutador de tránsito dirige el paquete inspeccionando la información de ruta codificada en el paquete por el enrutador de origen, el cual debe conocer el diseño de la red para poder especificar la ruta al destino.

El enrutamiento de origen permite determinar un camino parcial o completo, si el que envía determina el camino exacto, este mecanismo es llamado Strict Source Record Routing (SSRR), este enfoque es raramente usado. Un caso común de Source Routing es llamado Loose Source Recorded Routing (LSRR), donde el que envía proporciona uno o más saltos intermedios que el paquete debe visitar en su camino al destino.

El principal beneficio del enrutamiento de origen es que los nodos intermedios no tienen que mantener la información de ruta en RIB (Routing Information Base) porque los pasos de reenvío se especifican en el paquete de datos, también permite una solución de problemas de red más fácil, mejora el seguimiento de rutas y aumenta el rendimiento general de la red. SDN también se puede mejorar cuando se utiliza el enrutamiento de origen en el plano de datos, puede minimizar la comunicación entre el controlador SDN y enrutadores cuando se configura un nuevo flujo.

2.1.2. Definición del SR

El enrutamiento de segmentos es un método de reenvío de paquetes basados en el paradigma del "source routing", donde una lista de segmentos es agregada en la cabecera del paquete a través del nodo de ingreso (source) que escoge un camino y guía el paquete por una lista ordenada de segmentos (política de SR) hasta su destino alrededor de la red. Los segmentos son un identificador para cualquier tipo de instrucción y son llamados SID (Segment Id).

SR divide la red en "segmentos" donde a cada nodo y enlace se le puede asignar un SID, que se anuncia por cada nodo utilizando extensiones de protocolo de enrutamiento estándar (ISIS / OSPF o BGP), eliminando la necesidad de ejecutar protocolos adicionales de distribución de etiquetas.

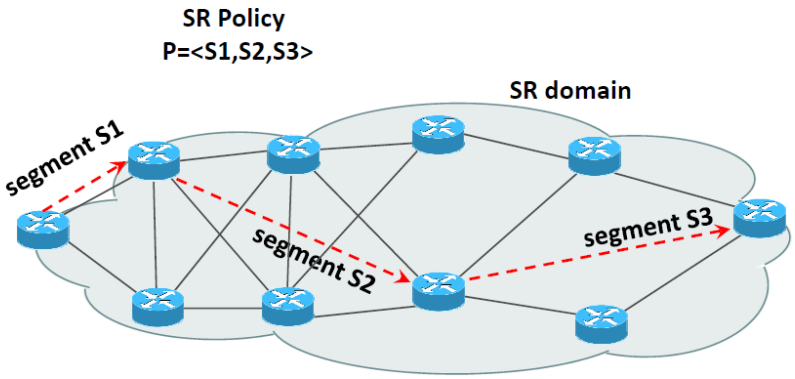


Figura 2.1 Política de SR y segmentos.
Fuente: (Ventre, y otros, 2020)

2.1.3. Beneficios del SR

- ✓ El enrutamiento de segmentos se propone esencialmente como un reemplazo para LDP o RSVP-TE, donde el IGP (Interior Gateway Protocol), actualmente ISIS (Intermediate System to Intermediate System) u OSPF (Open Shortest Path First), se ha extendido para incorporar internamente las funciones de etiquetado y enrutamiento de segmentos, lo que lleva al beneficio obvio de no tener que ejecutar un protocolo adicional junto con el IGP para proporcionar la funcionalidad MPLS, ya que se puede hacer todo dentro de ISIS u OSPF.
- ✓ Tiene la propiedad de simplificar y unificar la capa de transporte, ya que la estructura de SR conduce a una red de envío de extremo a externo más simple, y reduce la cantidad de protocolos necesarios en redes de acceso, metro, núcleo y data center.
- ✓ Se considera de bajo riesgo ya que los principales protocolos descongestionarán en lugar de sobrecargar la red, para que sea más simple.
- ✓ Redes programables, simplificación y reducción de componentes de señalización, balanceo e ingeniería de tráfico

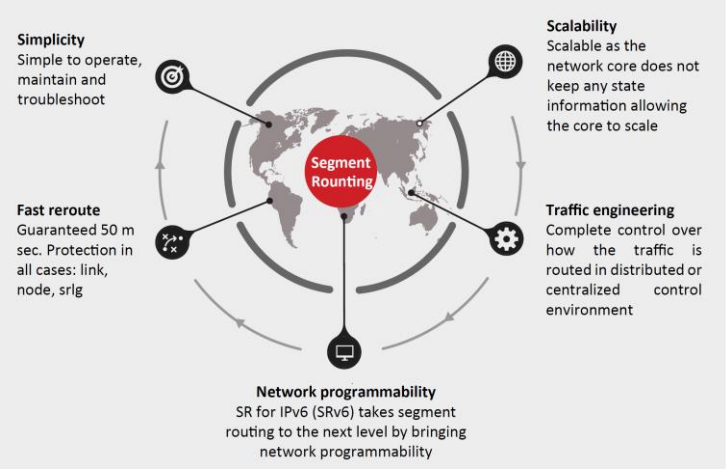


Figura 2.2 Beneficios de Segment Routing
Fuente: (Mota, 2018)

2.1.4. Características del SR

Se puede habilitar en redes operativas que usen MPLS ya que pueden trabajar juntas, hasta que se migre totalmente la red de un Proveedor de Servicios. Se puede aplicar en redes IP/MPLS e IPV6, en la primera se puede aplicar sin

cambiar el plano de datos, donde un segmento equivale a una etiqueta MPLS y la lista de segmentos es equivalente a la pila de etiquetas. En la segunda un segmento representa una dirección IPv6, esto se habilita introduciendo la extensión de encabezado de enrutamiento de segmento que permite que se multipliquen varias direcciones codificadas en el enrutador de origen, por lo que se pueden especificar varios saltos intermedios. Cuando se aplica en IPv6 puede ser llamado SRv6.

SR es escalable porque no se basa en LDP/RSVP-TE, y no es necesario mantener miles de etiquetas en una base de datos LDP y evita miles de LSP de ingeniería de tráfico, como ocurre en MPLS. Además, las tablas de reenvío en SR tienden a ser constantes, una vez que los SIDs (Segment ID) son seteados no hay necesidad de hacer más cambios.

Utiliza extensiones a los protocolos IGP (Interior Gateway Protocol) existentes para fines de señalización, con lo cual tiene otros beneficios, puede tomar ventaja de ECMP para equilibrar la carga en múltiples rutas disponibles en la red y ganar una mejor utilización del ancho de banda. Este tipo de flexibilidad no existe en RSVP-TE actual, que necesitaría complejas configuraciones manuales para la funcionalidad ECMP.

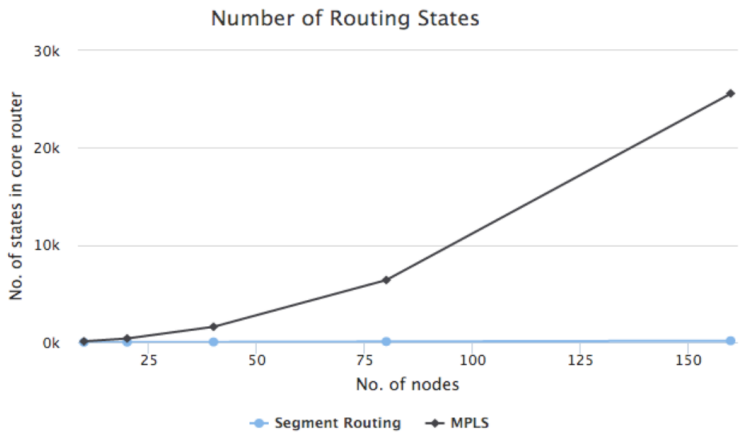


Figura 2.3 Números de estados MPLS vs SR.
Fuente: (Kos, 2015)

2.1.5. Segment Routing vs MPLS

En la red MPLS, la señalización de etiquetas y la reserva de recursos se realizan mediante implementación de los protocolos de señalización, LDP y RSVP-TE (Resource Reservation Protocol – Traffic Engineering). Como se indicó antes, en la red SR es suficiente tener un protocolo IGP y una vez que se configura el enrutamiento de segmentos, IGP tomará etiquetas y las redistribuirá dentro del dominio. No es necesario implementar ningún protocolo de señalización, lo que permite tener un gran beneficio en términos de ancho de banda y simplicidad.

Tabla 2.1 Comparación Segment Routing vs MPLS

Características tecnológicas	SEGMENT ROUTING	MPLS
Señalización con etiquetas	IGP	LDP+RSVP-TE
IGP/LDP Sync	NO requerido	requerido
FAST REROUTE(FRR) /5Oms	IGP	IGP+RSVP-TE
Estados extras por FRR	NO	SI
Optimización BACKUP	SI	NO
Estados TE	Solo en el nodo cabecera	N*N problemas en el CORE
Soporta SDN	SI	NO
Tipo de enrutamiento	Basado en la Fuente	Basado en el destino
Cálculo del PATH	restricciones SPF o PCE	IGP+RSVP-TE
Escalabilidad	ALTA	BAJA
Operación y tshoot	BAJO	ALTO

Fuente: elaborada por el autor

Además, LDP tiene muchos inconvenientes respecto a la sincronización después de que un enlace falla, pues debe sincronizarse con IGP que calcula los nuevos caminos a las rutas más cortas dentro de la red. Como hay un intervalo de tiempo mientras que los LSP se vuelven estables nuevamente, en algunos casos puede causar pérdida de paquetes porque los enrutadores centrales no saben cómo reenviar paquetes que son direccionados a una red externa. En SR solo IGP es usado y no hay necesidad de sincronización con otros protocolos.

Tener una buena protección de ruta es crucial para aplicaciones sensibles. En MPLS en algunos casos, es posible tener una protección de ruta de extremo a extremo, pero calculando una ruta primaria y secundaria. Para ambas rutas, los

recursos deben estar reservados utilizando el protocolo RSVP-TE. Todos los enrutadores incluidos, los de la ruta primaria y secundaria deben mantener el estado de los túneles. Esto garantiza QoS y que el tráfico no se pierda en caso de falla, la ruta está totalmente protegida y se puede redirigir de manera muy rápida <50 ms Fast Re Route (FRR). Sin embargo, la reservación doble de recursos no es eficiente en términos de utilización de la red, especialmente en aquellas de CORE ocupadas. Por otro lado, el enrutamiento de segmentos utiliza caminos postconvergentes que IGP calcula automáticamente cuando falla el enlace y garantiza un camino óptimo en una nueva situación. No hay estados adicionales que debe mantenerse para proteger el camino. El mecanismo FRR en enrutamiento de segmentos se llama Topology Independent Loop-Free Alternate (TI-LFA) y garantiza convergencia <50ms.

El ECMP permite el balanceo de tráfico entre rutas de igual costo entre el origen y el destino. En SR está incorporado, si existen dos rutas entre el mismo principio y fin (el mismo Prefijo-SID), el tráfico tomará caminos diferentes. Esta propiedad es compatible con la estabilidad de la red. En túneles MPLS se determinan estrictamente salto por salto, lo que significa que ECMP no es soportado.

En SR se utiliza el paradigma de enrutamiento de origen (source routing), mientras que en MPLS los paquetes se tunelizan poniendo etiquetas según su dirección IP de destino. En la red de enrutamiento de segmentos los caminos son determinados por el Constrained Shortest Path First (CSPF), es una extensión del algoritmo SPF (Shortest Path First). Primero, el algoritmo de ruta más corta se ejecuta, después se aplican las restricciones (disponibilidad de ancho de banda, latencia, etc.). El cálculo de la ruta generalmente lo realiza una entidad externa como un controlador SDN o PCEP (Path Computation Element Protocol). En MPLS, las rutas se configuran combinando IGP y protocolos RSVP-TE.

El enrutamiento de segmentos fue pensado para tener una red centralizada a nivel de plano de control. MPLS tiene un enfoque de tecnología diferente donde el plano de control es distribuido y los caminos pueden ser seteados y mantenidos

usando protocolos distribuidos. En estos ambientes distribuidos es muy difícil de aplicar control centralizado.

SR simplifica el proceso de operación y reduce la necesidad de mantenimiento de las redes. El plano de datos es altamente simplificado dado que no hay protocolos de señalización. Además, esto facilita la operación para marcar etiquetas constantes sobre la red. Es altamente escalable comparado con MPLS. Primero porque elimina la necesidad de protocolos de señalización que conlleva a reducir la arquitectura general y los procesamientos a nivel de software abaratando el hardware del equipo. Además, el número de estados en la red se reducen en gran medida aplicando enrutamiento de segmentos, cada nodo debería mantener aproximadamente (N-1) + número de adyacencias, donde N es el número total de routers dentro del dominio IGP. En MPLS para LDP cada router mantiene sesiones (estados LSP) de acuerdo al número de vecinos y para RSVP-TE, si una topología incluye N routers en full mesh, habrá la necesidad de mantener un estado de NxN LSP en cada router, lo que conlleva a problemas de escalabilidad en redes grandes.

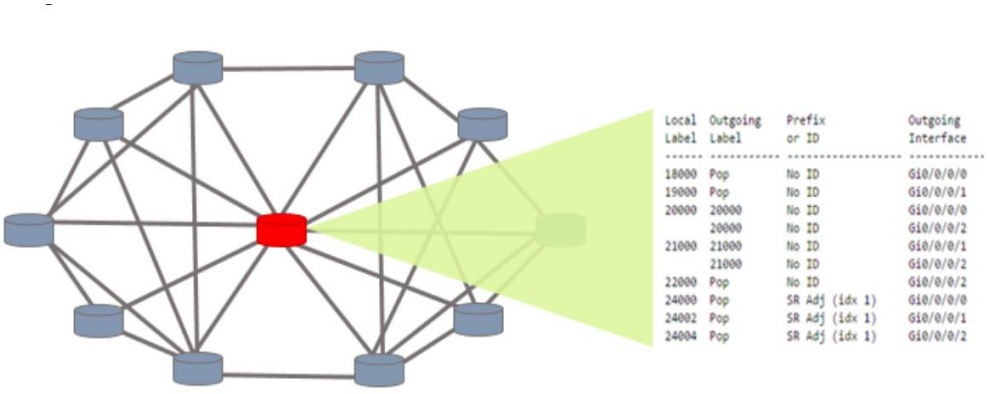


Figura 2.4 Escalabilidad de la Red
Fuente: (Kos, 2015)

2.1.6. Problemas de escalabilidad de RSVP-TE y LDP

Los LDP mantienen el estado de reenvío de toda la Forwarding Information Class (FEC) en la red, porque cada una es accesible por cualquier otro enrutador LDP. RSVP-TE solo mantiene el estado de reenvío de los LSP que lo atraviesan y potencialmente su camino de protección. Desde la perspectiva de

estados de reenvío, LDP corre problemas de escalabilidad si la red se vuelve demasiado grande.

RSVP-TE también puede realizar ingeniería de tráfico en redes IP / MPLS; sin embargo, involucra configuraciones complejas de túneles en interfaces y es difícil de solucionar. LDP no puede hacer ingeniería de tráfico, pero puede perder la sincronización de LDP e IGP porque la una depende de la otra para la convergencia de rutas

2.2. Tecnologías detrás del SR

A continuación, se detallan los conceptos más importantes acerca de las tecnologías que maneja el enrutamiento de segmentos.

2.2.1. Segmento

Es la unidad básica en el SR. Es una instrucción que el nodo ejecuta sobre el paquete de entrada. Por ejemplo, un comando podría ser reenviar el paquete a un nodo de red específico según la ruta más corta, o reenviar paquetes a través de una interfaz específica, o entregar el paquete a una aplicación o servicio dado. Cada segmento es identificado por el SID que consiste en un entero de 20 bit y en el entorno MPLS está codificado en una etiqueta de 32 bits. Un ejemplo de combinación de múltiples segmentos, para una ruta end-to-end puede ser creada de la siguiente manera:

Si el tráfico necesita ir desde el ingreso en “A” al egreso “H” con una derivación en “E”, los 3 segmentos son suficientes para definir el camino. Adicional debería estar algún identificador asociado con los segmentos, este identificador es llamado “segment identifier”.

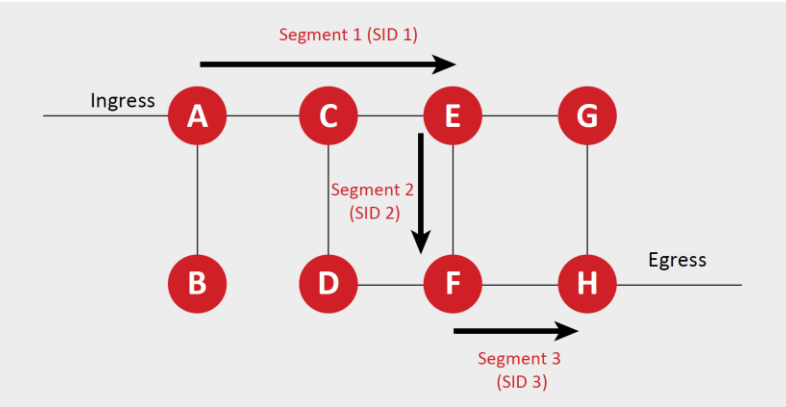


Figura 2.5 Segmentos en SR
Fuente: (Mota, 2018)

2.2.2. Lista SID

Es la unión de algunos Segment Identifier, es decir es el camino end-to-end que recorre un paquete con enrutamiento de segmentos habilitado. En un paquete SR el segmento que especifica la instrucción a ser ejecutada es llamado segmento activo.

En MPLS, un segmento se codifica como una etiqueta, una pila de ellas representa una lista ordenada de segmentos. La etiqueta superior es la que procesa el nodo que lo recibe, al procesar el paquete, esta se saca de la pila.

En IPV6, se define un nuevo encabezado de enrutamiento para habilitar el SR. Un segmento está codificado como una dirección IPV6. Una lista ordenada de direcciones representa una lista de segmentos.

2.2.3. Dominio de SEGMENT ROUTING

Es un set de nodos participando en el modelo de enrutamiento basado en la fuente. El nodo de cabecera puede ser el origen del paquete o un nodo intermedio que realiza una clasificación del tráfico y asocia la política de SR al paquete. En otras palabras, el host puede ser parte de un dominio de SR, pero esto no es requerido y depende del escenario general en el que se aplica. Esto es lo que se espera, que todos los nodos en un dominio SR sean manejados por una misma instancia administrativa. Por ejemplo: Un proveedor de Servicios backbone puede

constituir un dominio de SR y el nodo cabecera será el router de borde de ingreso al backbone (en este caso un host no es parte del dominio de SR).

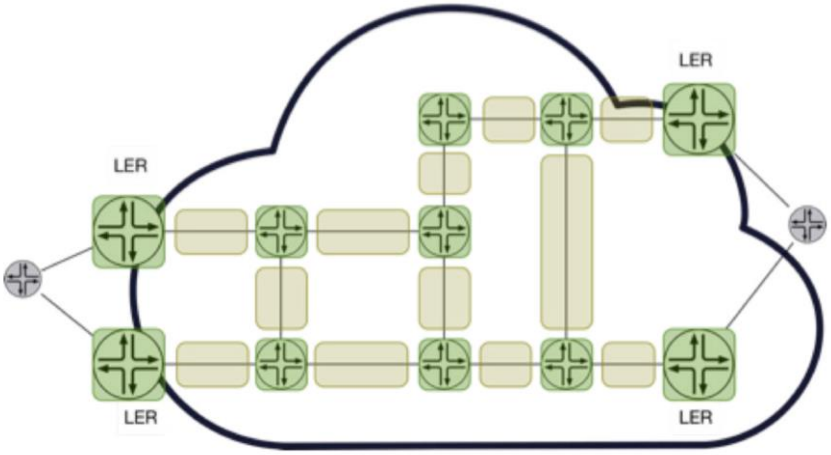


Figura 2.6 Nodo SID y Adyacencia SID en un dominio SR
Fuente: (ARISTA, 2019)

Segmento Global:

El segmento global está relacionado a la instrucción que es compatible con todos los nodos en un dominio IGP y debe ser único en este. Cualquier nodo en un dominio IGP debe tener todos los segmentos globales en su FIB (Forwarding Information Base). El valor de los identificadores de segmento global se toma del Segment Routing Global Block (SRGB) y se le puede asignar un valor absoluto del mismo. Alternativamente, el valor SID puede ser derivado por cada nodo usando un valor de índice y agregando este al valor base de SRGB, este es un sub-espacio de un SID de 32 bits. Un ejemplo típico de un segmento global es una instrucción que reenvía su paquete a lo largo de una red o un nodo de destino IP dado. El segmento de prefijo y el de nodo, tienen importancia en todo el dominio por lo tanto son considerados como Segmentos Globales.

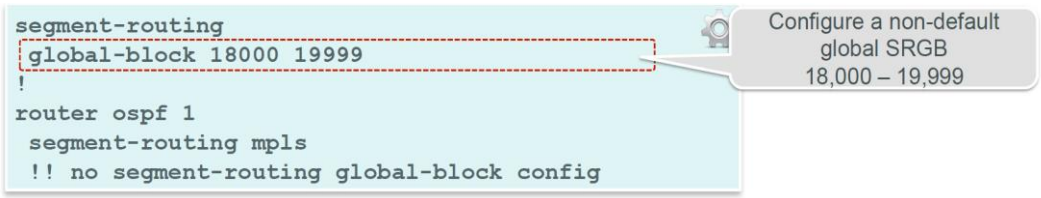


Figura 2.7 Configuración de SRGB Global
Fuente: (Filsfils & Michielsen, Segment Routing IGP Control Plane , 2014)

Figura 2.8 Configuración de SRGB dentro de la instancia IGP
Fuente: (Filsfils & Michielsen, Segment Routing IGP Control Plane , 2014)

Segmento Local:

Es una instrucción soportada por el nodo que lo origina, toman un valor fuera del rango SRGB. Ya que solo tiene un significado local, su valor está relacionado solo a la FIB del enrutador local, el cual no es consciente de los segmentos locales de los otros enrutadores en un dominio, es decir, que no tienen que ser únicos dentro del dominio SR. Los segmentos de adyacencia solo tienen significancia local. Por lo tanto, los routers con capacidad de realizar conmutación por segmentos distribuyen estos SID de forma automática, sin preocuparse por su coordinación en todo el dominio.

2.2.4. Segmentos IGP

Dentro del dominio SR, un IGP distribuye dos tipos de segmentos: Prefijo y Adyacente. Señalar segmentos IGP requiere que los protocolos de estados de enlace, como OSPF o ISIS, utilicen extensiones. A continuación, se detalla cada una de estos:

Figura 2.9 Clasificación de IGP-SID
Fuente: (Kos, 2015)

Segmento Prefijo:

De manera general está asociado con un prefijo IP y representa la ruta IGP de menor costo entre cualquier router y un prefijo especificado, el cual es identificado como Prefijo SID y se configura manualmente desde el rango de etiquetas del SRGB distribuyéndose a través de OSPF o ISIS.

El Prefijo SID es un segmento global, entonces es globalmente único dentro del dominio de SR, cuando se utiliza en MPLS, el SID de prefijo se asigna en forma de una etiqueta y si se usa en IPv6, se asigna como una dirección IPv6.

- Node SID. - Subtipo del segmento de prefijo, que identifica un nodo en específico (ejemplo un loopback) en dominio IGP, es identificado como un Nodo SID, el cual es único en el dominio SR. Este es configurado debajo de la interfaz de loopback con la loopback address del nodo como prefijo.

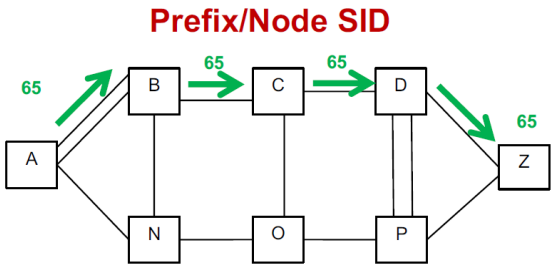


Figura 2.10 Ejemplo prefix/Nodo SID
Fuente: (Jaksic, 2018)

- Anycast SID. - Es un tipo especial del segmento de prefijo que muestra una ruta consciente por ECMP al nodo más cercano del conjunto anycast. Es un Segment ID compartido que usa un grupo de enrutadores con un valor de SID común llamado Anycast SID.

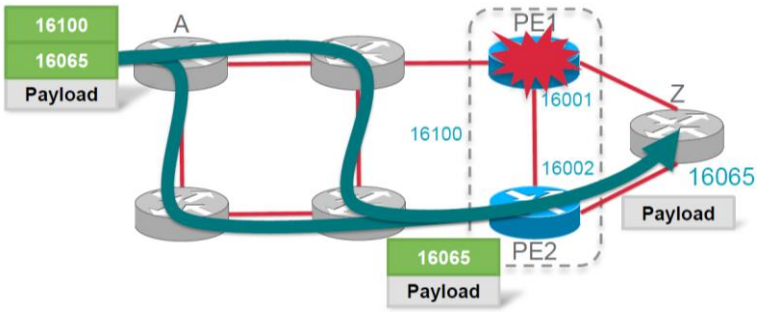


Figura 2.11 Operación de Prefix SID anycast
(Filsfils & Michielsen, Segment Routing IGP Control Plane , 2014)

Segmento de Adyacencia:

Se identifica por una etiqueta llamada Adjacency SID, que representa una adyacencia IGP entre dos routers o la interfaz de salida a un router vecino. Los Adj SID son locales para cada nodo y son instalados y anunciados en vecinos

conectados directamente, se asigna dinámicamente por un nodo (fuera del bloque SRGB) y dirige el tráfico a una adyacencia específica.

Por ejemplo, si un router tiene 4 enlaces adyacentes, este localizará un único Adj SID para cada uno de ellos, una vez que observa que Adj SID se encuentra en la entrada de la pila de etiquetas, éste sabe a qué enlace el tráfico deberá ser reenviado.

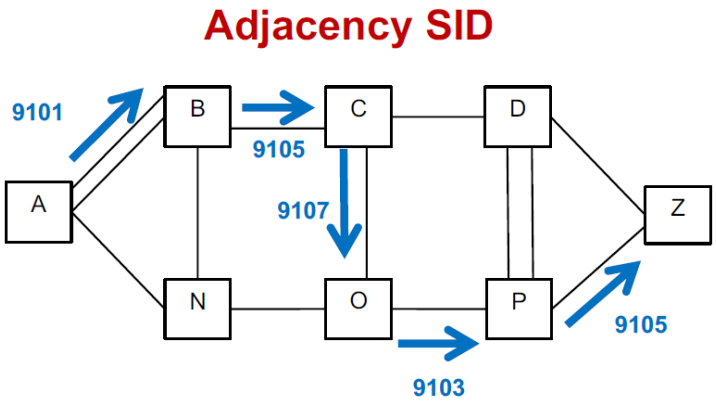


Figura 2.12 Ejemplo de Adyacencia SID
Fuente: (Jaksic, 2018)

2.2.5. Segmento BGP

En caso de ingeniería de tráfico multidominio, el segmento IGP no es suficiente para realizar esta tarea, pues está configurado para un dominio simple IGP y un router no puede pasar el tráfico a los próximos dominios ya que no sabe su SID, si no hay enrutamiento IGP entre routers en diferentes dominios, la única manera de resolver esto es usando un protocolo BGP (Border Gateway Protocol) y sus segmentos.

Los segmentos se anuncian utilizando los protocolos de enrutamiento IGP y BGP. Para ambos protocolos, las extensiones de SR son definidas para incluir su Información. En otras palabras, los protocolos de enrutamiento habilitan señalización de segmentos a través de la red. Permitiendo ahora considerar un sistema autónomo que consta de múltiples áreas IGP, en cada una IS-IS u OSPF está corriendo. Éstos son responsables de anunciar segmentos dentro de un dominio IGP. Sin embargo, para implementar ingeniería de tráfico entre Sistemas autónomos, Intercambio de Segmentos entre peers, BGP debe estar habilitado.

Segmento de Prefijo BGP:

Para fines de SR, BGP prefix SID es definido para identificar el segmento de prefijos BGP, el cual es siempre global dentro de un área BGP/SR. Un enrutador que recibe un paquete con BGP-Prefix-SID enrutará un paquete de acuerdo con la ruta más corta, compatible con ECMP, al prefijo BGP especificado.

Segmento Peer BGP:

Ayuda a identificar un enlace peer BGP particular entre varios enlaces disponibles. Esto ayuda mucho en BGP EPE (Egress Peer Engineering), uno de estos, habilitado en el enrutador de salida puede anunciar segmentos correspondientes a sus peers conectados. Estos segmentos se denominan segmentos de interconexión BGP (BGP Peering SID)

Ejemplo: Existe un requerimiento para diseñar una ruta para que una aplicación particular de baja latencia desde un DC atraviese una WAN y luego salga por el camino preferido que es a través de AS2. Para llegar desde un DC ("a") a un peer de egreso particular (AS2) necesitará de 3 segmentos los cuales van apilados como etiquetas: {16001,16002 y 25000}.

- 16001-> BGP prefix SID, para alcanzar desde 'a' A 'b'
- 16002-> IGP Prefix SID, para alcanzar desde 'b' A 'c'
- 25000-> BGP Peer SID, para seleccionar un enlace particular que este directamente conectando 'c' a 'AS2'.

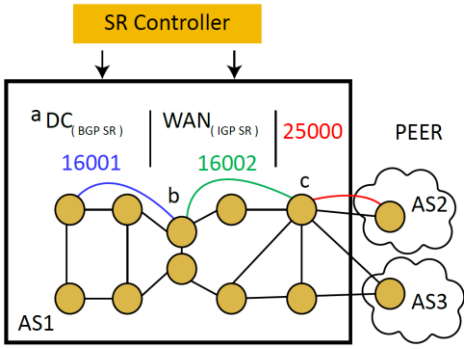


Figura 2.13 Esquema de BGP con un controlador SR.
Fuente: (Mota, 2018)

2.2.6. Operación de Ruteo

Un nodo origen dirige una lista ordenada de SIDs adjuntada a la cabecera de un paquete. Para el plano de datos SR-MPLS, un SID es una etiqueta, mientras que para SR-IPv6 es un direccionamiento IPv6. El segmento superior es uno de los primeros en ser ejecutados, al hacerlo el paquete alcanza un destino intermedio y el próximo segmento será procesado y así sucesivamente. Cuando el último segmento es procesado, el flujo alcanza su destino, o simplemente sale del dominio de SR y continúa a ser ruteado dependiendo de su IP de destino.

Hay tres operaciones que se podrían realizar sobre segmentos en nodos con SR habilitado. Sin embargo, están estrechamente relacionadas con las operaciones realizadas en etiquetas MPLS sobre sus redes. Las operaciones de SR son:

1. PUSH**:** Se asemeja a MPLS PUSH. Consiste en la inserción de un segmento sobre el Top de la pila de segmentos en un paquete SR.
2. NEXT**:** Se asemeja a MPLS POP. Consiste cuando un segmento activo es completado y es removido de la pila de segmentos. La operación NEXT también cubre el caso del último nodo de una política de SR, en la cual la operación NEXT generalmente resulta en el procesamiento del paquete de acuerdo con el reenvío de IP regular.
3. CONTINUE**:** Se asemeja al MPLS SWAP. Consiste cuando un segmento activo aún no es completado y éste permanece activo. Es realizado por los nodos que están en el camino entre los dos segmentos. Naturalmente esta operación se usa en segmentos globales, que desde su ejecución podría incluir algunos saltos. Segmentos locales (adyacencias) son ejecutados con un único salto.

Por ejemplo, en la fig. 2.14 una política de SR **P** que consiste en dirigir un paquete a lo largo de tres segmentos con SID S1, S2 y S3, pueden ser representados como P = <S1, S2, S3>. Tres operaciones han sido definidas sobre esta lista de segmentos para un genérico SR dataplane:

El PUSH se ejecuta en el orden: PUSH(S3), PUSH(S2), PUSH(S1), donde el nodo cabecero envía el paquete con el Segmento activo S1. El nodo identificado con S1 recibe el paquete y realiza la operación NEXT, el siguiente segmento es S2, el cual se convierte en activo y el paquete es reenviado a lo largo de S2. Los nodos intermedios en el camino entre S1 y S2 realizan el CONTINUE. El camino entre S1 y S2 no es precisado por el SR policy y será escogido considerando el enrutamiento IP regular a lo largo de S2 en el dominio SR. Si hay múltiples rutas de igual costo entre los nodos S1 y S2 y el mecanismo ECMP es compatible para el enrutamiento IP en el dominio SR, este puede convenientemente ser explotado por SEGMENT ROUTING. Y así continúa su camino según la política SR hasta llegar al S3, donde aplicará un NEXT para que el paquete sea entregado a su destino.

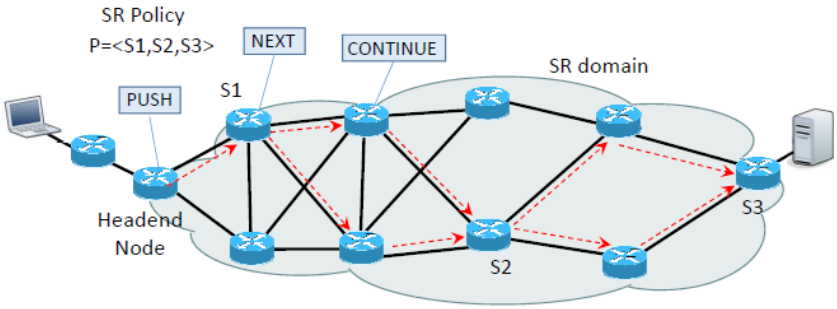


Figura 2.14 Ejemplo de una política SR y sus operaciones.
Fuente: (Ventre, y otros, 2020)

2.3. Intermediate System to Intermediate System

ISIS es un protocolo IGP estandarizado por la Organización Internacional de Normalización en 1992, para la comunicación entre dos dispositivos de red llamados IS (Intermediate System). Junto con OSPF pertenecen al grupo de protocolos de estado de enlace, los cuales permiten una rápida convergencia, así como un buen rendimiento de escalabilidad en comparación con protocolos de vector de distancia. Las características principales de IS-IS son:

- Red sin clase.
- Inundaciones rápidas
- Convergencia rápida
- Enrutamiento jerárquico
- Escalabilidad
- Ajuste flexible de temporizador

La operación IS-IS se basa en la inundación de la información del estado de enlace dentro de un dominio administrativo (de enrutamiento). Un enrutador inunda periódicamente una red con paquetes de estado de enlace (LSP) que contienen esa información, la cual es recopilada y cualquier nodo de red puede obtener una imagen completa de la topología de la red. Al aplicar ciertos algoritmos, un enrutador puede calcular la ruta más corta a otros nodos en el dominio. IS-IS utiliza el algoritmo Dijkstra. Tras el cálculo, un enrutador almacena los resultados en su FIB, una nueva entrada es añadida para cada ruta de destino contenida en el nodo, la dirección del siguiente salto y la interfaz de salida.

El enrutamiento IS-IS utiliza el esquema jerárquico que se diferencia a través de niveles, su enrutador puede ser de L1, L2 o L1/L2. El primero no es un router del área de backbone, crea adyacencia con vecinos en su misma área. Solo la información que tiene un enrutador de L1 con respecto a las otras áreas es una ruta por defecto más cercana al enrutador de L1/L2. El L2 es un enrutador de backbone y construye sus adyacencias solo con los de L2, que pueden estar en la misma área o en otras. Los enrutadores de L2 son responsables del encaminamiento entre dominios y tienen toda la información sobre la topología. El enrutador de L1/L2 crea adyacencia con enrutadores L1 y L2. Se comportan como puertas de acceso a enrutadores L1 que desean enviar el tráfico fuera del dominio, la arquitectura jerárquica de IS-IS se presenta en la figura 2.15.

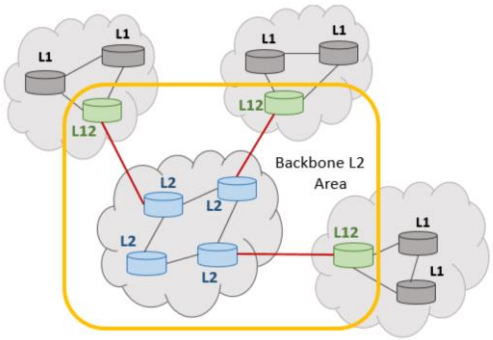


Figura 2.15 Arquitectura Jerárquica ISIS
Fuente: (Kos, 2015)

En general, un flujo de operación de un enrutador IS-IS:

1. Envía mensajes de saludo y construye adyacencias

2. Crea paquetes de estado de enlace e inunda a sus vecinos
3. Recibe toda la información del estado del enlace de sus vecinos
4. Ejecuta el primer algoritmo de la ruta más corta (Dijkstra) y el cálculo de ruta parcial
5. El procedimiento se repite cuando se reciben nuevos LSP

IS-IS junto con OSPF son esenciales para las redes de enrutamiento de segmentos. IGP permite la redistribución de segmentos a través de la red, lo que elimina la necesidad de protocolos de señalización como LDP. En comparación con OSPF, IS-IS se convirtió cada vez más popular entre los proveedores de servicios por su rendimiento en grandes topologías. Eso motiva a implementarlo en este proyecto como IGP. En el siguiente subcapítulo se verá qué extensiones de IS-IS ordinarias son esenciales para el enrutamiento de segmentos

2.3.1. Extensiones de ISIS para SR

Puede habilitar el enrutamiento de segmentos para IGP, lo puede hacer en el submodo de configuración del enrutador a través de comandos. Sin embargo, se habilita solo después de configurar SR globalmente.

El enrutamiento de segmento requiere que cada enrutador anuncie su capacidad de plano de datos de SR y rango de valores de etiqueta MPLS, que se utilizan en el caso de que se asignen SID globales. Dichas capacidades se anuncian utilizando SR sub-TLV (Type Lenght Value) insertados en TLV-242 del enrutador IS-IS.

SR permite una definición flexible de caminos de extremo a extremo dentro de topologías IGP, codificando rutas como secuencias de subcaminos topológicos, llamados "segmentos", los cuales son anunciados por los protocolos de enrutamiento de estado de enlace (IS-IS y OSPF). Dos tipos de segmentos son definidos, de prefijo y de adyacencia. Los primeros representan una ruta más corta a un prefijo por ECMP, según el estado de la topología IGP. Los sgundos representan un salto sobre una adyacencia específica entre dos nodos en el IGP. Un segmento de prefijo es típicamente una ruta de múltiples saltos

mientras que el de adyacencia, en la mayoría de los casos, es una ruta de un salto. En SR el plano de control se puede aplicar a los planos de datos IPv6 y MPLS, y no requieren ninguna señalización adicional (que no sea el IGP normal). Por ejemplo, cuando se usa en redes MPLS, las rutas SR no requieren ninguna señalización LDP o RSVP-TE. Aun así, SR puede interoperar en presencia de LSP establecidos con RSVP o LDP.

IS-IS usa elementos Type-Length-Value (TLV) dentro de un protocolo mensaje, estos hacen que un protocolo sea fácilmente extensible. Una vez que los datos adicionales deban ser codificados en el mensaje se agrega un nuevo TLV y no hay necesidad de rediseñar un protocolo. Para admitir el enrutamiento de segmentos, nuevos IS-IS Sub-TLV son definidos, los cuales se colocan dentro de los TLV y utilizan los mismos conceptos que el ordinario.

Los TLV existen dentro de los paquetes IS-IS, mientras que los sub-TLV en los TLV, estos se utilizan para agregar información adicional a IS-IS paquetes, Sub-TLV se utilizan para particular TLVs. En IS-IS, permiten anunciar las capacidades TLV dentro de un nivel de ISIS o en un dominio de enrutamiento.

```
TYPE: 242
  LENGTH: from 5 to 255
  VALUE:
    Router ID (4 octets)
    Flags (1 octet)
    Set of optional sub-TLVs (0-250 octets)

Flags

            0 1 2 3 4 5 6 7
            +-+-+-+-+-+-+-+-+
            | Reserved  |D|S|
            +-+-+-+-+-+-+-+-+
```

Figura 2.16 Formato del enrutador ISIS con capacidades TLV 242
Fuente: (Network Working Group, 2007)

Flag Scope (S). - si se establece, entonces inunda los TLV a través de todo el dominio de enrutamiento.

Flag Down (D). - si se establece, entonces permite que se filtre capacidades TLV de enrutador ISIS de nivel 2 (L2) a nivel 1 (L1).

Prefix-SID Sub-TLV:

Se define para transportar información sobre el Identificador de prefijo de segmento. Como se mencionó anteriormente debe ser único dentro de dominio IGP. Contiene los indicadores necesarios para desambiguar el prefijo IP a las asignaciones de nodos. Además, si un nodo dado tiene varias direcciones IP de 'transporte estable' hay banderas para diferenciar estos otros Prefijos IP advertidos desde un nodo dado. Tiene el siguiente formato:

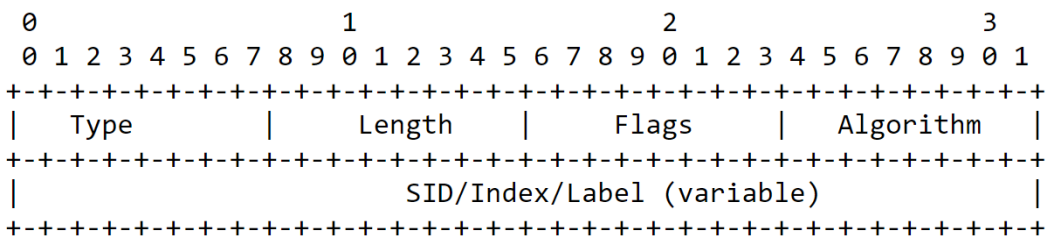


Figura 2.17 Formato de un Prefix SID Sub-TLV de un mensaje ISIS
Fuente: (Filsfils, y otros, 2015)

```
interface Loopback0
 ipv4 address 1.1.1.1 255.255.255.255
 ipv6 address 2001::101:101/128
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  segment-routing mpls
 !
 address-family ipv6 unicast
  metric-style wide
  segment-routing mpls
 !
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid absolute 16001
   !! Or: prefix-sid index 1
  !
  address-family ipv6 unicast
   prefix-sid absolute 17001
   !! Or: prefix-sid index 1001
 !
```

Figura 2.18 Configuración de Prefijo SID en SR
Fuente: (Filsfils & Michielsen, Segment Routing IGP Control Plane , 2014)

Los primeros cuatro campos tienen una longitud de 8 bits cada uno. Se definen seis banderas para Prefix-SID sub-TLV: de reenvío, Node-SID, no-PHP, explicit-Null, de valor y local.

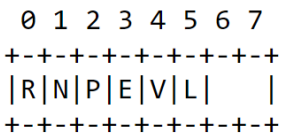


Figura 2.19 Banderas de un Prefix SID Sub-TLV
Fuente: (Filsfils, y otros, 2015)

1. Bandera de Reenvío (R): si se establece, el prefijo al cual este Prefix SID es asociado, es propagado por el enrutador desde otro nivel (L1 a L2 o viceversa) o desde otro protocolo (redistribución).
2. Bandera de Node SID (N): si se establece el prefijo al cual este Prefeix SID es asociado, corresponde a la dirección loopback de un router.
3. Bandera no-PHP (P): si se establece, el penúltimo hop no debería hacer POP al prefix-SID antes de entregar el paquete al nodo que advierte el Prefix-SID.
4. Bandera Explicitt-Null: si se establece, el penúltimo hop debería reemplazar el Prefix-SID con un Explicit-Null, ya que el router que origina el prefijo quiere recibir el paquete con una etiqueta MPLS para usar el bit EXP/TC para la clasificación. Se lo configura sobre el router que origina el prefijo localmente.
5. Bandera de valor (V): si se establece, el Prefix-SID lleva un valor (en lugar de un index)
6. Bandera Local: Si se establece, entonces el valor o el index llevado por el prefix-SID tiene una significancia local.

Los otros bits deberían ser 0, cuando son recibidos son ignorados. Dependiendo de su valor, estas banderas podrían influir en dónde y cómo se distribuirá el sub-TLV dentro del dominio IGP. El campo de **Algoritmo** contiene un identificador del que un enrutador debería usar para calcular la ruta más corta (SPF basado en métrica, SPF restringido, etc.). El campo **SID/Index/Label** contiene información sobre SID. Hay dos maneras cómo se puede codificar SID en este campo. El valor SID se puede codificar directamente, y en ese caso se usan tres octetos de cuatro. Las banderas de valor y locales deben establecerse, lo que significa que sub-TLV lleva el valor SID real. De lo contrario, la información SID podría ser llevada debajo de su valor índice, el cual es un desplazamiento en rango de etiqueta SID para un enrutador determinado. Una vez que recibe un índice, un enrutador lo usa para recuperar un valor SID real. Esta codificación utiliza todos los 32 bits, y requiere que banderas locales y de valor no estén establecidas.

Adjacency-SID Sub-TLV:

Es codificado y distribuido por el Adjacency-SID con banderas y campos que podrían ser usados, en futuras extensiones de SR, para llevar otros tipos de SIDs. Puede anunciar adyacencia de un solo nodo o un conjunto de ellas referidas a un enrutador designado. Esto se lo obtiene a través de un IS-neighbor TLV que tiene un formato similar a un Prefix-SID sub-TLV.

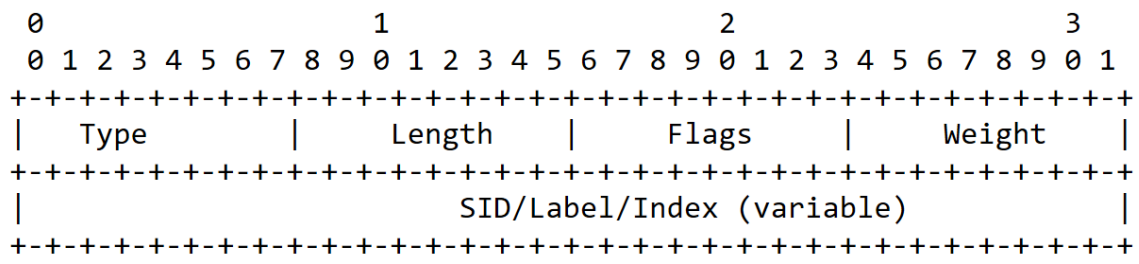


Figura 2.20 Formato de Adyacencia SID Sub-TLV de un mensaje ISIS
Fuente: (Filsfils, y otros, 2015)

Adjacency-SID sub-TLV tiene cinco banderas definidas: Address-family, Back-up, Valor, local y conjunto. A diferencia de Prefix-SID sub-TLV, tiene un campo de peso que lleva el del enlace, con el fin de equilibrar la carga.

```
interface GigabitEthernet0/0/0/0
 ipv4 address 99.1.2.1 255.255.255.0
 ipv6 address 2001::9901:201/120
!
router isis 1
 address-family ipv4 unicast
  metric-style wide
  segment-routing mpls
 !
 address-family ipv6 unicast
  metric-style wide
  segment-routing mpls
 !
 interface GigabitEthernet0/0/0/0
  point-to-point
  address-family ipv4 unicast
  address-family ipv6 unicast
```

Figura 2.21 Configuración de Adyacencia SID en SR
Fuente: (Filsfils & Michielsen, Segment Routing IGP Control Plane , 2014)

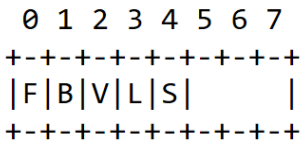


Figura 2.22 Banderas de un Adyacencia SID Sub-TLV

Fuente: (Filsfils, y otros, 2015)

1. Bandera Adrress Family (F): si no está establecida se refiere a una adyacencia con encapsulación de salida IPv4. Si lo está el Adj-SID hace referencia a IPv6.
2. Bandera Backup (B): Si se establece, el Adj-SID es elegible para protección (por ejemplo: usando IPFRR o MPLS-FRR).
3. Bandera Valor (V): si se establece, el Adj-SID lleva un valor. Por defecto la bandera es establecida.
4. Bandera Local (L): si se establece, el Valor/index llevado por el ADj-SID tienen una significancia local. Por defecto esta bandera es establecida.
5. Bandera Conjunto (S): cuando se establece, la bandera S indica que el Adj-SID se refiere a un conjunto de adyacencias, y por lo tanto también puede ser asignado a otras.

Weight: 1 octeto. El valor representa el peso de un Adj-SID para el balanceo de carga.

El campo SID/Index/Label puede contener uno de tres valores: de etiqueta (3 octetos), de índice (4 octetos) o dirección IPv6 (en el caso de que se implemente SR en el plano de datos IPv6). La combinación de bits: locales y de valor, indica cuál de esos tres valores están dentro del campo SID/Index/Label. Por ejemplo:

- V y L seteadas, usa los 3 octetos donde los 20 bits más a la derecha son usados para codificar la etiqueta.
- V y L no seteadas, usa los 4 octetos donde el index es definido por el valor de desplazamiento en el espacio SID/LABEL advertidas por el enrutador.
- V=1 y L=0, usa 16 octetos y un ipv6 address, donde es globalmente único.

En las subredes LAN, un enrutador designado es elegido y, junto con sus nodos adyacentes forman un pseudo-nodo que puede anunciar un conjunto de adyacencias para sus "nuevos" vecinos. Este tipo de publicidad es compatible con LAN-Adj-SID que tiene propiedades similares a un Adj-SID ordinario sub-TLV.

SID/LABEL Sub-TLV:

Son usados para añadir información extra a un particular TLV. Están formados por los siguientes campos: 1 octeto para Tipo, un octeto para Longitud, y de cero o más octetos para el de valor. Contiene un SID o una etiqueta MPLS.

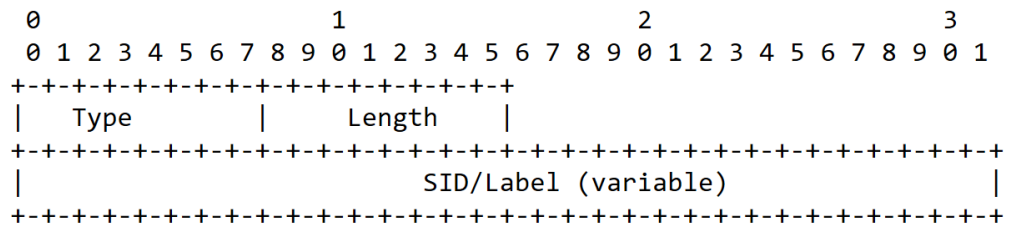


Figura 2.23 Formato de SID/LABEL sub TLV
Fuente: (Filsfils, y otros, 2015)

Seteado con los valores por defecto:

- Type: TDB, valor sugerido 1
- Longitud: variable
- SID/LABEL: Si la longitud se setea a 3 entonces los 20 bits más a la derecha representan una etiqueta MPLS

SID/Label BINDING TLV:

Podría ser originado por cualquier router en un dominio IS-IS. Hay múltiples usos de SID/Label Binding TLV. El enrutador puede anunciar un Binding SID/Label a lo largo de una FEC con al menos un simple 'next hop style'. El protocolo soporta más de un anclaje 'next hop style' para adjuntar a un binding SID/Label, que da como resultado una ruta simple. En analogía con RSVP, la terminología para esto se llama ERO (Explicit Route Object). Dado que el camino con el formato estilo ERO permite ser el pilar de Binding SID/label para direcciones de nodos IP y enlaces de cualquier ruta de camino etiquetado. Además, binding SID/Label desde protocolos externos pueden ser fácilmente anunciados.

Otra aplicación de Binding SID/Label puede ser usado para unir un direccionamiento IP a un valor SID. Esto es importante si en un dominio no todos los nodos son capaces de advertir SIDs. Otro propósito es advertir Binding SID/LABEL y sus rutas primarias y de respaldo serán asociadas. Si un router quiere advertir múltiples caminos entonces puede generar varios TLV para el

mismo Prefijo/FEC. Cada aparición de un TLV vinculante con respecto a un prefijo FEC tiene significado acumulativo y no cancelador. Debido a restricciones de espacio en los TLV IS-IS de 8 bits, un enrutador de origen puede codificar una ruta primaria ERO en un Binding SID/label TLV y la ruta de respaldo ERO en un segundo Binding SID/Label TLV. El prefijo FEC y el SID/Label sub-TLV deben ser idénticos en ambos TLV.

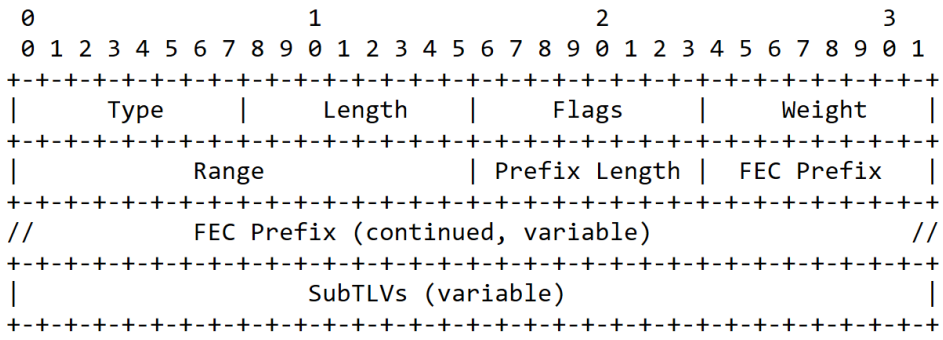


Figura 2.24 Formato de SID/LABEL BINDING TLV
Fuente: (Filsfils, y otros, 2015)

Type: TBD sugerido 149

Longitud: variable

Flags: 1 octeto

Weight: 1 octeto

Range: 2 octetos

Longitud de prefijo: 1 octeto

Prefijo FEC: 0 -16 octetos

Sub TLVs: Donde cada Sub TLV consiste en la secuencia de:

- 1 octeto de Tipo de Sub TLV
- 1 octeto de longitud en el campo de valor de SUB TLV
- 0-243 octetos de valor

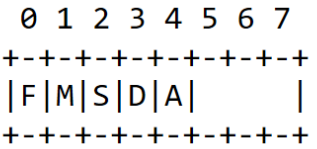


Figura 2.25 Banderas de SID/LABEL BINDING TLV9
Fuente: (Filsfils, y otros, 2015)

1. Bandera Adrress Family (F): si no está establecida el prefijo FEC lleva un prefijo IPv4. Si está establecida lleva uno IPv6.

2. Bandera Mirror (M): si se establece, advierte el SID/path correspondiente a un contexto espejo. Por lo general se usa en PLR (Point Local Repair) cuando necesita proteger una ruta.
3. Flag Scope(S): si se establece, inunda los TLV a través de todo el dominio de enrutamiento.
4. Flag Down (D): si se establece, permite que se filtre capacidades TLV de enrutador ISIS de nivel 2 (L2) a nivel 1 (L1).
5. Flag adjunto (A): si se establece, indica que los prefijos y los SIDs anunciados en el Binding SID/Label TLV están directamente conectados a quienes los originan. Si el Binding TLV es filtrado a otras áreas/niveles entonces el bit A no debe estar seteado.

Capacidades SR Sub TLV:

Están incluidas dentro de las capacidades TLV. El SR data plane y los valores de rango de etiquetas, son advertidos por capacidades sub TLV insertadas dentro de ellas de router ISIS en caso de que global SID sean localizados. Capacidades sub TLV incluyen todos los rangos de SRGB reservados.

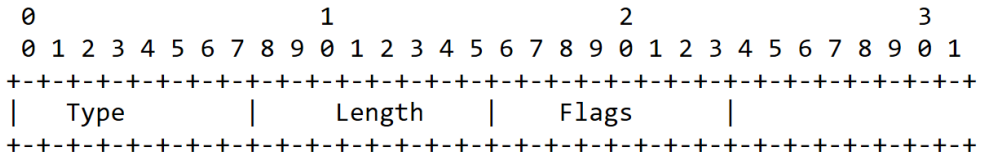


Figura 2.26 Formato de Capacidad SR SUB TLV
Fuente: (Filsfils, y otros, 2015)

Banderas:

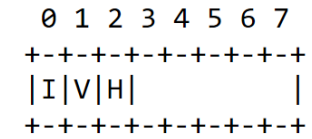


Figura 2.27 Banderas de Capacidad SR SUB TLV
Fuente: (Filsfils, y otros, 2015)

1. Flag I: si se establece, el router es capaz de procesar SR MPLS encapsulado en paquetes IPV4 en todas las interfaces
2. Flag V: si se establece, el router es capaz de procesar SR MPLS encapsulado en paquetes IPV6 en todas las interfaces.

3. Flag H: si se establece, el router es capaz de procesar cabeceras SR ipv6 en todas las interfaces

Las capacidades SR sub TLV contiene: Bandera (8 bits) y uno o más descriptores SRGB. Un descriptor contiene:

- Rango (24 bits),
- SID/LABEL (variable, de 32 bits si es MPLS) indica el inicio de SRGB

El SID/LABEL Sub TLV contiene el primer valor del SRGB, mientras que el rango contiene el número de elementos de SRGB.

2.4. Casos y Usos de SR

La tecnología SR, brinda un nuevo control sobre la infraestructura de red, haciéndola mucho más flexible y escalable, lo cual permite su uso y aplicación en los siguientes casos:

2.4.1. Coexistencia de Enrutamiento de Segmentos y MPLS:

Coexistencia del Plano de control:

- El plano de control MPLS coexiste desde los inicios de MPLS (LDP, TDP, RSVP-TE,BGP,etc)
- El "Administrador de etiquetas" y el plano de control MPLS garantizan la funcionalidad de que etiquetas locales usadas por diferentes protocolos de distribución no colisionen.
- Los segmentos globales necesitan usar un rango protegido, exclusivamente para ellos.

Coexistencia del Plano de datos:

- Para el plano de reenvío no hay diferencia de donde esta venga una etiqueta, (static, LDP, RSVP-TE, BGP o SR)
- Mientras el plano de control no use sobreposición de etiquetas en el espacio del plano de datos coexiste bien.

Figura 2.28 Coexistencia del SR/LDP en el Plano de Datos
Fuente: (Kramer, 2017)

Modelos de desarrollo para Intercomunicación SR/LDP:

Existen diferentes formas en las que se pueden intercomunicar una red MPLS con SR o viceversa, como se observa en la figura 30, adicionalmente en esta figura se indica si se necesita del uso de Mapping Server.

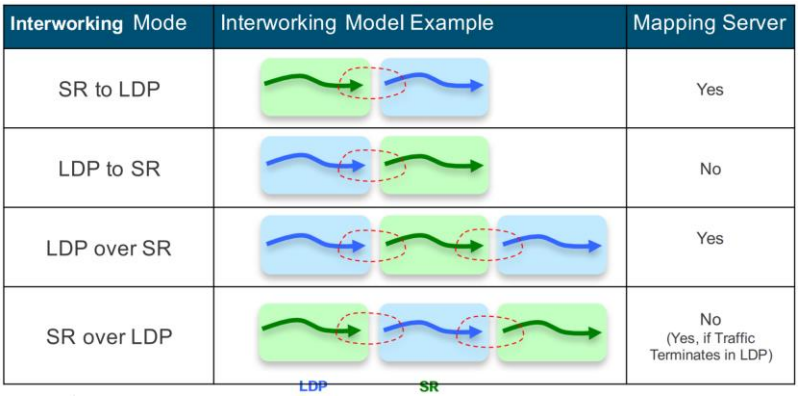


Figura 2.29 Modelos de interconexiones LDP/SR
Fuente: (Kramer, 2017)

- **Intercomunicando LDP a SR.-** Cuando un nodo soporta LDP, pero su próximo salto a lo largo del camino más corto a su destino no habla LDP, entonces la etiqueta de salida para el nuevo nodo no es LDP. En este caso, el LSP formado por LDP está conectado a un segmento de prefijo. Donde el nodo de borde C (LDP/SR) instala en su FIB, para que se comunique de un protocolo a otro (en este caso de LDP a SR) lo siguiente:

Etiqueta de entrada: una etiqueta del LDP binding para la FEC Z

Etiqueta de salida: un segmento de prefijo unido a FEC Z

Interfaz de salida: D

Esta entrada FIB es automáticamente derivada a la capa de enrutamiento, no se necesita de configuración.

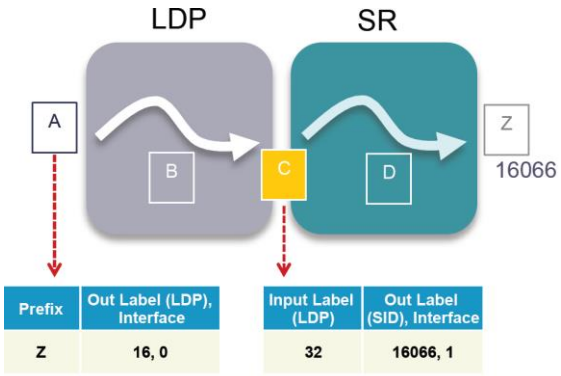


Figura 2.30 Intercomunicando LDP a SR
Fuente: (Jaksic, 2018)

- **Intercomunicando SR a LDP. -** Cuando un nodo soporta SR, pero su próximo salto a lo largo del camino más corto a su destino no habla SR, entonces la etiqueta de salida para el próximo nodo no es SR. En este caso, el segmento de prefijo está conectado a un LDP LSP. Donde cualquier nodo en el borde SR/LDP instala entradas SR-to-LDP a la FIB.

Para el ejemplo, A quiere enviar tráfico a Z, pero Z no habla SR, por lo tanto, no advierte cualquier Prefix-SID. Con ayuda del Mapping Server advierte el SID mapeado para routers que no hablan SR. Por ejemplo, este advierte que Z es 16066.

A y B instalan normalmente un prefijo SR para 16066. C se da cuenta de que el próximo salto a lo largo de SPT hacia Z no habla SR, por lo tanto, instala entradas SR-to-LDP a la FIB:

Etiqueta de entrada: prefix-SID unida a Z (16066)

Etiqueta de salida: LDP binding desde D para FEC Z

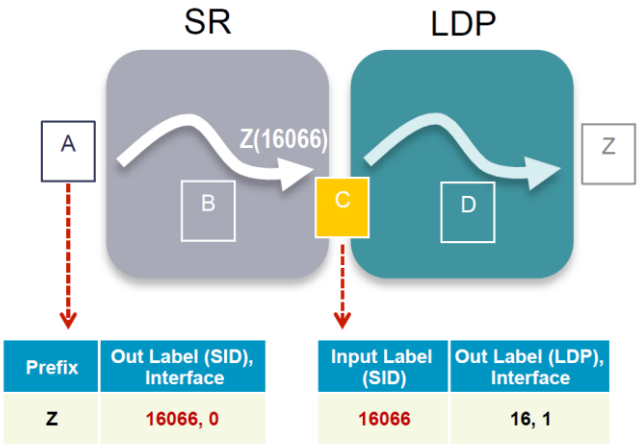


Figura 2.31 Intercomunicando SR a LDP
Fuente: (Jaksic, 2018)

- **Mapping Server. -** Advierte Prefix SID mapeados en IGP para nodos que no hablan SR, los cuales son configurados en el Mapping Server. Es decir, habilita a los nodos SR para que se puedan intercomunicar con nodos LDP que no hablan SR. El Mapping Server solo es requerido para hablar de SR a LDP.

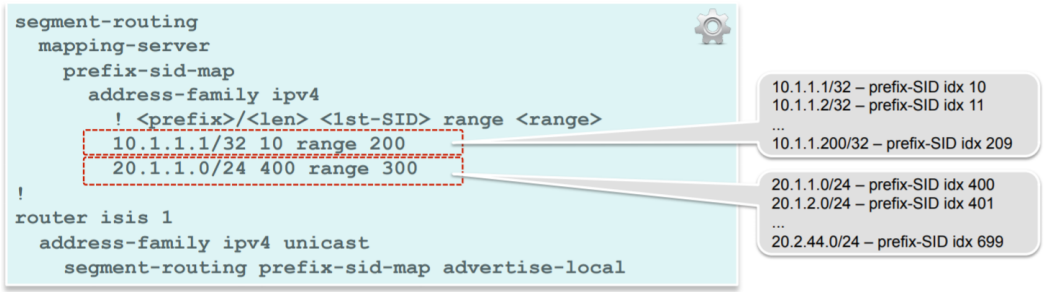


Figura 2.32 Configuración para un Mapping Server con SR/LDP
Fuente: (Filsfils & Michielsen, Segment Routing, 2015)

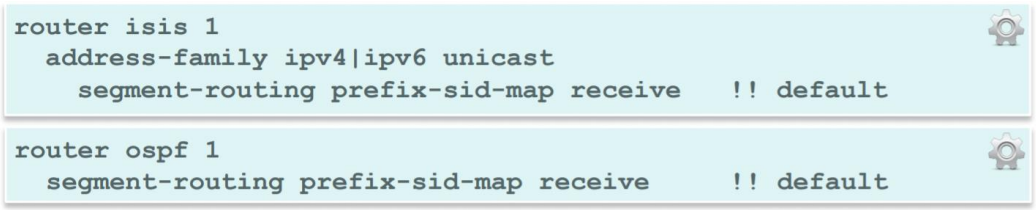


Figura 2.33 Configuración para un Mapping Client con SR/LDP
Fuente: (Filsfils & Michielsen, Segment Routing, 2015)

2.4.2. SRTE (SR Traffic Engineering)

SRTE se ha convertido en uno de los casos de uso ampliamente adoptados para el enrutamiento de segmentos, debido a la simplicidad y escalabilidad que proporciona. La ingeniería de tráfico en MPLS hasta ahora rara vez se ha implementado en grandes servicios de proveedores de red debido a la

complejidad. SRTE no solo proporciona simplicidad y escalabilidad, sino también proporciona una forma nativa de SR de implementar rutas de ingeniería de tráfico que aprovechan el comportamiento ECMP de redes IP. La complejidad se reduce aún más en la red debido a los beneficios adicionales de la automatización a través de la implementación de políticas de SR bajo demanda y la dirección automatizada del tráfico en la red.

SRTE provee, enrutamiento explícito y enrutamiento basado en restricciones, así políticas flexibles pueden ser automáticamente creadas en un ambiente distribuido y centralizado (SDN), basados en la latencia, jitter, ancho de banda, caminos diferentes y preferidos, etc. No usa RSVP-TE, porque este protocolo usado para ingeniería de tráfico en IP/MPLS, no es popular debido a la necesidad de crear configuraciones de túneles para las políticas de TE que conlleva rápidamente a problemas de escalabilidad.

SRTE mantiene el CORE rápido y escalable (sin estados). Uno de los principales beneficios es la tunelización sin señales RSVP y LDP, como también el ECMP aplicado al enrutamiento dentro de cada segmento y cero estados por flujo en routers de tránsito. Contrario a lo que se observa en MPLS-TE que mantiene un estado explícito en todos los saltos a lo largo de una ruta, lo que conduce a problemas de escalabilidad en el plano de control y de datos. Además, el modelo de tráfico guiado con conexión de MPLS-TE no explota fácilmente el equilibrio de carga que ofrece el enrutamiento ECMP en redes IP simples.

SRTE Policy:

Es una lista ordenada de segmentos, la cual es añadida a la cabecera del paquete en un nodo de borde, que guía el paquete a través de la política SR hasta su destino. El color es un valor numérico arbitrario que muestra diferentes tipos de políticas, por ejemplo, el verde para caminos de baja latencia o el rojo para caminos de alto ancho de banda.

Por ejemplo, en este caso hay dos políticas diferentes configuradas: verde para baja latencia y rojo para alto ancho de banda (una política tiene muchos

candidatos). La roja tiene dos caminos. El preferido a lo largo de múltiples candidatos es identificado por el número más alto de preferencia (uno de los parámetros del camino candidato).

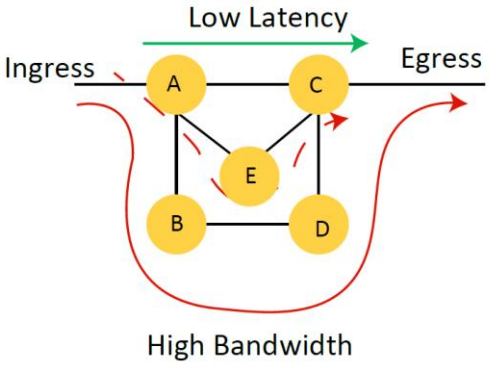


Figura 2.34 Disponibilidad de caminos según el tipo de restricción
Fuente: (Mota, 2018)

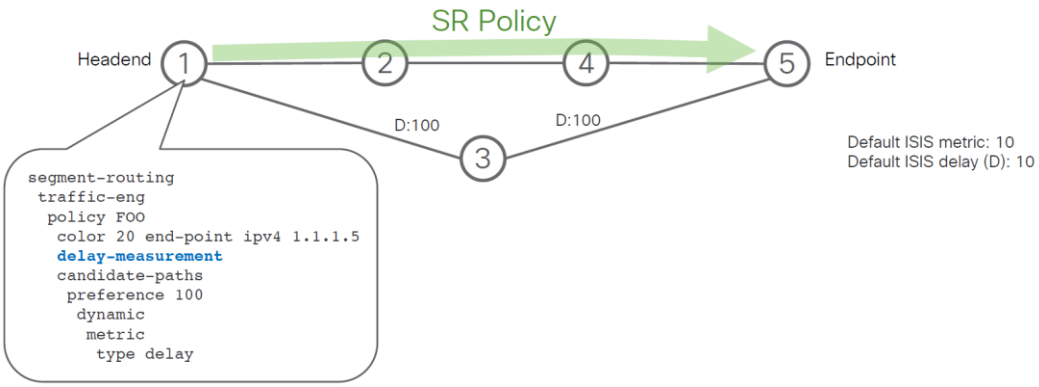


Figura 2.35 Aplicación de una SRTE POLICY
Fuente: (Filsfils & Fellow, SEGMENT ROUTING, 2019)

Binding Segment (BSID):

Es un nuevo tipo de segmento para ingeniería de tráfico, fundamental para SRTE y trae escalabilidad e independencia de servicio para SR. Es usado para asociar una política SR (lista de segmentos) a un SID (llamado BSID) en un nodo dado. Es decir que el nodo que procesa el BSID reemplaza el segmento con una lista de estos: un paquete recibido con el BSID como segmento activo será guiado sobre la política SR asociada, eso significa que el paquete será reenviado usando la correspondiente lista de segmentos.

Usando el BSID es posible separar los procesos de clasificación de paquetes por la aplicación de una política específica de SR la cual se puede cambiar a través del tiempo y se puede ejecutar en un nodo diferente, sin

necesidad de cambiar el proceso de clasificación. Esto mejora la escalabilidad, la resistencia y la independencia de servicios de soluciones basadas en SR.

El SR PCE (Path Computation Element) aprovecha las políticas SR existentes para fines de tránsito al incluir su BSID como parte de una lista SID para una política SR de extremo a extremo, creando una jerarquía de políticas de SR. El BSID permite, que la lista SID sea más corta y la unión entre dominios aislados. Inclusive si la ruta secundaria entre METRO – WAN cambia, el BSID relacionado es constante.

Un BSID es fundamental para construir bloques SRTE. Tiene una significancia local. Identifica una política de SRTE, la cual es asociada 1 a 1 con un BSID. Puede ser asignado automáticamente o estáticamente como parte de una política SRTE.

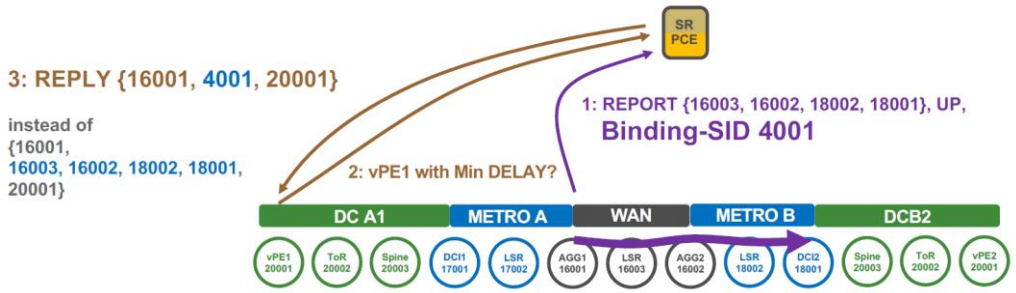


Figura 2.36 Ejemplo de políticas SR para comunicación de un punto a otro
Fuente: (Filsfils & Fellow, SEGMENT ROUTING, 2019)

SR Nativo:

En lugar de usar algoritmos de RSVP-TE para calcular la mejor ruta basada en restricciones, SRTE usa el algoritmo Nativo SR. Se reduce la pila de etiquetas y un camino que balancea carga debido a que SR tiene la capacidad nativa de ECMP.

Los mecanismos de TE convecional son comparados con los de SR nativo para encontrar el path entre A y F, que no pase a través del enlace en rojo. En el convencional el camino mas simple es calculado a través de los routers B-C-D-E. Lo que es más enfocado para ser aplicado en una tecnología TDM, en la cual un path es utilizado para transferir tráfico y no toma ventaja del balanceo de carga a

través de enlaces de costos iguales (para tener ECMP en RSVP-TE tendría que recurir a configuraciones adicionales y complejas).

Debido a que SR nativo soporta ECMP, utiliza todos los caminos de igual costo, lo cual resulta en una pequeña lista de SID. Por ejemplo solo se apunta al prefijo E, lo que balanceará el tráfico a través de los 3 enlaces disponibles, pero usando solo 2 SIDs (E Y F) como labels stacks, y el tráfico podrá llegar a su destino F usando 3 caminos.

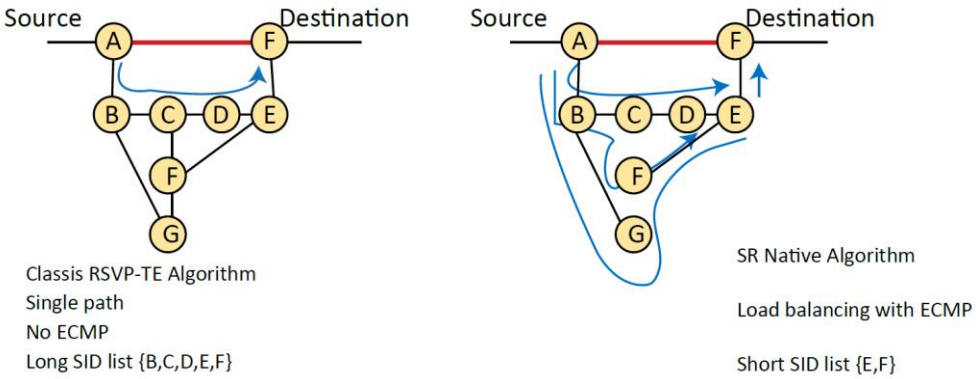


Figura 2.37 Comparación entre Algoritmo RSVP-TE vs Algoritmo SR Nativo
Fuente: (Mota, 2018)

2.4.3. FAST RE-ROUTE (Topology Independent LFA)

SR corre en proveedores de red que manejan servicios de misión crítica, los cuales requieren recuperación a fallas de la manera más rápida, simple y predecible. Es un requisito predeterminado tener recuperación de fallas en menos de 50 milisegundos.

Hay mejoras continuas en los mecanismos de resistencia en redes IP/MPLS: RSVP-TE FRR, loop free alternate (LFA) y LFA remoto, los cuales han sido ampliamente adoptados. Aunque los mecanismos han mejorado, no hay ninguno que pueda garantizar una cobertura del 100% para todos los escenarios de falla. No es común que LFA converja por la ruta más óptima, lo cual si sucede con TI-LFA que siempre busca el IGP más óptimo como mejor camino.

SR resuelve el problema de micro-bucles que puede suceder en LFA. SR utiliza Topology Independent LFA (TI-LFA) que proporciona y garantiza

caminos de respaldo sin bucles y protección contra fallas de enlaces, nodos y Shared Risk Link Group (SRLG) en el 100% de los casos.

Para entender las ventajas del TI-LFA, es importante entender las deficiencias de LFA y REMOTE LFA.

LFA no puede resolver problemas de microloops:

- LFA tiene problemas en una topología de anillos con más de 3 nodos.
- Cuando el enlace primario entre R1 y R5 falla, el tráfico es inmediatamente derivado a R2
- Sin embargo, R2 enviará el tráfico de regreso a R1 debido a que el camino más corto de R2 a R5 es a través de R1. Lo que creará microloops hasta que el tráfico IGP converja.

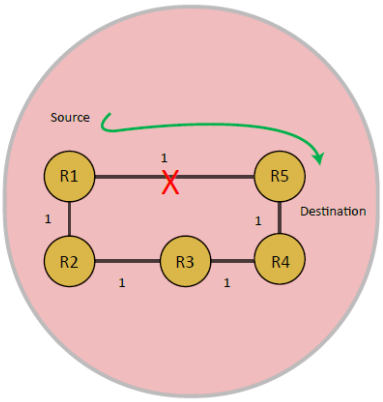


Figura 2.38 Problema de LFA: Microloops
Fuente: (Mota, 2018)

Cómo LFA REMOTO resuelve el problema de LFA:

- LFA remoto escoge el próximo salto del router protegiendo el tráfico a través de un túnel, lo que no lo enviará de retorno a sí mismo.
- Esto va 2 saltos más allá del router R1, por ejemplo, R3 (también llamado nodo PQ).
- Para el camino de backup, el router R1 creará una sesión Target LDP a R3 para que pueda enviar tráfico a través de R2.
- Una vez que el tráfico alcance a R3, este puede fácilmente llegar a R5 como el camino con menor métrica.

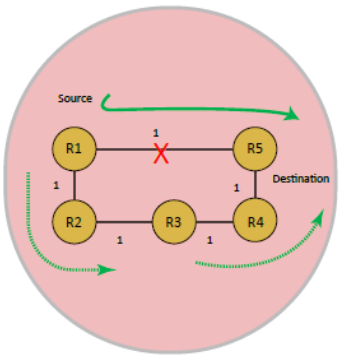


Figura 2.39 Sesión target LDP entre R1 y R3
Fuente: (Mota, 2018)

Qué no puede resolver el LFA REMOTO:

- En el escenario en que la métrica entre R3 y R4 se incremente a 10 (conocido como ejemplo de doble segmento)
- No hay un nodo PQ. Si R1 envía el tráfico a R3 a través del target LDP, éste enviará de regreso a R1 porque es el camino con métrica más corta desde R3 a R5 a través de R1.
- LFA remoto no es capaz de resolver esto.

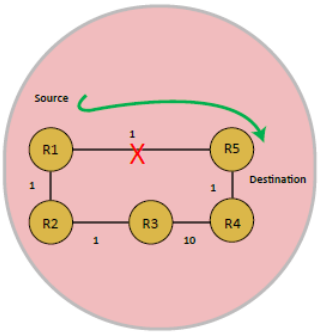


Figura 2.40 Problema cuando aumenta la métrica en un enlace
Fuente: (Mota, 2018)

Entonces LFA no cubre el 100% de convergencia. Sin embargo, TI-LFA con SR no necesita sesiones Target LDP. Esto hace al protocolo muy simple y escalable.

En el escenario con SR para proteger una ruta basada en la misma topología, en el nodo de ingreso R1, tres segmentos son construidos usando 3 labels SID.

1. Etiqueta del prefijo R3 para enviar el tráfico a R3
2. Etiqueta para Adj. R3-R4 para enviar tráfico desde R3 a R4

3. Etiqueta del prefijo R5 para enviar tráfico de R4 a su destino R5

Usando Adj-SID en el nodo R3 se resuelve el problema de cruzar el enlace de métrica alta desde R3 a R4, cuando el tráfico llega a R3 y ve la etiqueta de adyacencia SID Adj R3-R4, inmediatamente sabe que necesita enviar el tráfico en el enlace adyacente a R4, independientemente de la métrica en este enlace. El enrutamiento de segmentos ha resuelto el problema de protección fácilmente, al construir tres pilas de etiquetas sin necesidad de una sesión específica de LDP.

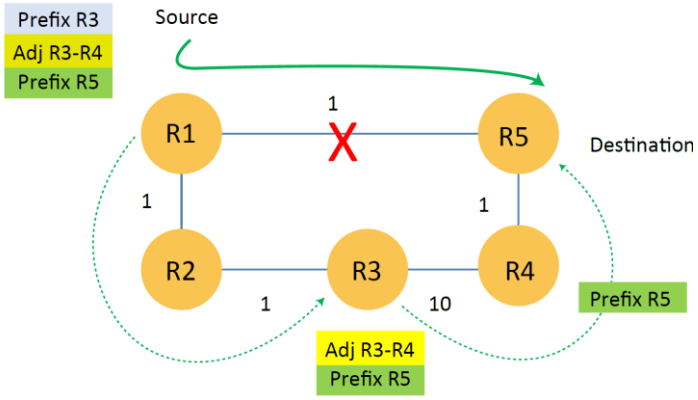


Figura 2.41 Solución para métricas altas con SR
Fuente: (Mota, 2018)

TI-LFA – Ruta De Post Convergencia:

Es la ruta de respaldo utilizada por el PLR, que es la misma que toma un paquete una vez que el protocolo IGP converja, cuando existe un escenario de falla de enlace.

Esta es una ventaja muy importante, ya que automáticamente el camino de respaldo es creado por el IGP de la red, convirtiéndolo en fácil y simple de entender. Además, previene la congestión en la red, aprovechando el camino de Post-Convergencia que es por donde se enviará el tráfico.

Con LFA si hay problema en un enlace a nivel de CORE, todo el tráfico es protegido por los nodos y enlaces de borde, ya que tiene una sesión LDP más directa entre routers de borde. Con TI-LFA el tráfico conmutaría por los enlaces de CORE y aplicaría una pila de PREFIX-SID, siguiendo el camino natural de la convergencia IGP.

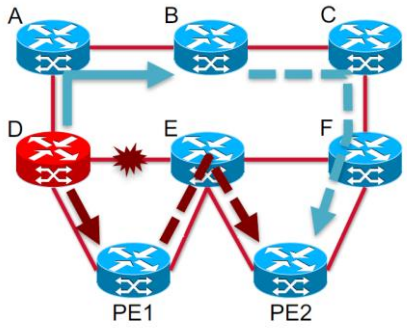


Figura 2.42 Camino optimo Post convergencia
Fuente: (Jaksic, 2018)

2.4.4. Software Define Network

SR se puede utilizar en un entorno centralizado, distribuido e híbrido. En un escenario **distribuido**, los segmentos son asignados y señalizados por IS-IS, OSPF o BGP, permitiendo simplificación en las operaciones y protocolos comparados con MPLS, otro uso sería la protección de 50ms que ofrece en enlaces L3. En un escenario **centralizado**, los segmentos se asignan por un controlador SR de SDN. Un escenario **híbrido** es la combinación de la inteligencia distribuida y centralizada, por ejemplo, distribuido se puede utilizar en el mismo dominio IGP, pero cuando el destino está fuera del dominio IGP, el controlador puede calcular una política enrutada en el origen en nombre de un nodo IGP.

SR no requiere un controlador SDN en la red, pero esta tecnología de enrutamiento fue creada para un control centralizado en mente, por lo que SR y SDN son tecnologías complementarias. Es decir, si no se usa SDN, SR funciona con un enfoque distribuido, al habilitar las dos tecnologías juntas se aprovecha al máximo los beneficios que ofrece la tecnología de enrutamiento de segmentos.

Cuando se utiliza en un entorno centralizado, el enrutamiento de segmentos proporciona una arquitectura SDN simple, ya que no hay estados en la red (solo en el router de borde de entrada), y los caminos son calculados y programados por un controlador centralizado, el cual es usualmente un PCE.

Para la mayoría de los operadores, el controlador SDN es el final del juego, incluso si ellos solamente están usando un control distribuido para sus desarrollos iniciales.

Las redes IP tradicionales consideran los planos de control y datos estrechamente acoplados e incrustados en el mismo nodo de red. En otras palabras, la función de control es distribuida a través de dispositivos de red, lo que significa que cada uno es responsable de tomar una decisión de reenvío de forma autónoma. En las primeras etapas de las redes IP, desarrollar esto se consideró un buen aspecto porque garantizaba la resistencia de la red. Sin embargo, cualquier variación en el plano de control descentralizado requiere cambios en todos los dispositivos de red manualmente. La falta de automatización en la gestión de redes hace que las redes actuales sean estáticas y no puedan adaptarse a demandas de tiempo real.

Para superar tales limitaciones, se ha propuesto un nuevo paradigma de red: SDN, que se puede definir como "una arquitectura donde el plano de control de red está desacoplado y separado del mecanismo de reenvío y es directamente programable" (Kos, 2015). Esta tecnología trae un control centralizado lógico llamado controlador SDN, el cual tiene una vista global de la red. Los dispositivos se convierten en elementos de reenvío de bajo nivel sin función de control. Todas las instrucciones las reciben del controlador a través de interfaces especiales. Las características fundamentales de SDN son:

1. Separar el plano de control con el de datos, convirtiendo a los dispositivos en simples elementos de reenvío.
2. La funcionalidad de control es manejada por el controlador SDN
3. Las redes son programables a través de aplicaciones corriendo sobre el controlador

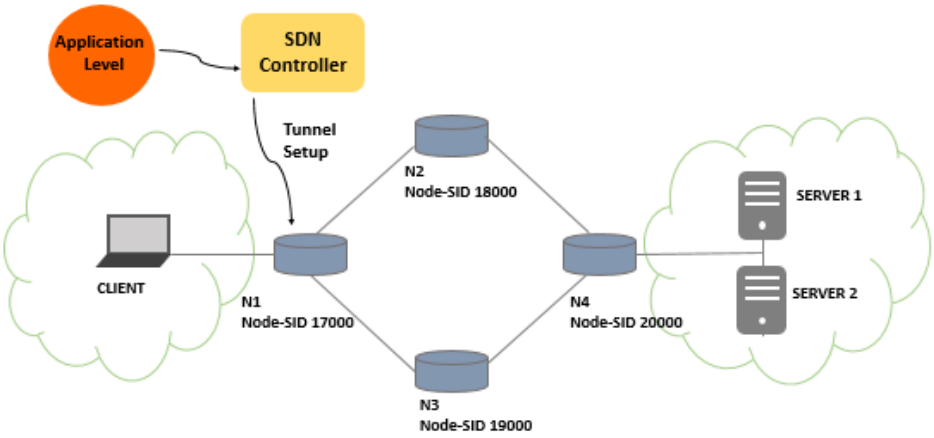


Figura 2.43 Esquema de comunicación usando controlador SDN
Fuente: (Kos, 2015)

La principal característica de una solución SR con SDN es que solo el enrutador cabecera debe mantener el estado para aplicar una política de SR determinada, mientras que los nodos internos no necesitan mantenerlos por política SR, lo que conduce a una escalabilidad mejorada y menos consumo de recursos en los equipos de red.

SDN es la plataforma perfecta para el enrutamiento diseñado para Application Engineering Routing (AER). Da la opción de que una aplicación requiera una ruta específica, en términos de latencia, ancho de banda, SLA (Service Level Agreement), parámetros que empujan los paquetes a través de ese camino, sin tener que informar a la red al respecto. Eso tiene un beneficio recíproco tanto para la aplicación como para el funcionamiento de la red. La aplicación puede especificar directamente sus requisitos y empujar el tráfico en la trayectoria óptima. Por otro lado, la capa de datos es ligera porque no tiene que mantener las rutas de tráfico, ya que se especifican directamente desde la aplicación.

La combinación de SR con un controlador SDN permite que los caminos de TE puedan ser definidos a través de múltiples dominios, definiendo caminos desde una red metro a una red de CORE, también puede conectar DATA CENTERS a la WAN. Mientras algunas otras técnicas de enrutamiento de origen se asocian con OpenFlow basado en SDN, estas técnicas últimamente se limitan

para operar solamente donde OPENFLOW está presente en la red. Con SR definido por IETF, la limitación no existe.

El controlador SDN debe admitir los protocolos esenciales para SR, los cuales son: BGP-LS y PCEP, entonces se comporta como PCE y puede calcular el camino en términos de segmentos y agregarlos de regreso al PCC (Path computation Client). Como propiedad del PCE, el controlador SDN puede iniciar la sesión PCEP y realizar la optimización de flujo, si es necesario. La topología de la red se obtiene mediante la comunicación entre el BGP-LS y los vecinos BGP en cada dominio IGP. Cada dominio IGP debería tener al menos una sesión BGP que redistribuirá la LSDB al controlador SDN.

Elementos y protocolos del SR con un controlador SDN:

PCE: realiza el cálculo de la ruta de manera centralizada y la información de los estados de la red. Es conocido como controlador SDN.

PCC: (Path Computation Client) Se refiere a los PE (Provider Edge).

PCEP: (Path Computation Element Protocol), permite que un controlador SDN programe esencialmente el PCC con una ruta, por ejemplo, aplica una política de SR.

BGP-LS (BGP-LINK STATE): extensión de BGP, permite que la información IGP se inyecte en BGP. Los IGP solo se limitan generalmente al dominio dentro del cual operan, por ejemplo, para una red grande con muchos dominios IGP o MPLS entre dominios, la visión del IGP se vuelve mucho más limitada. BGP, por otro lado, puede cerrar muchas de estas brechas, y cuando se programa con la capacidad de transportar información IGP, puede ser bastante útil.

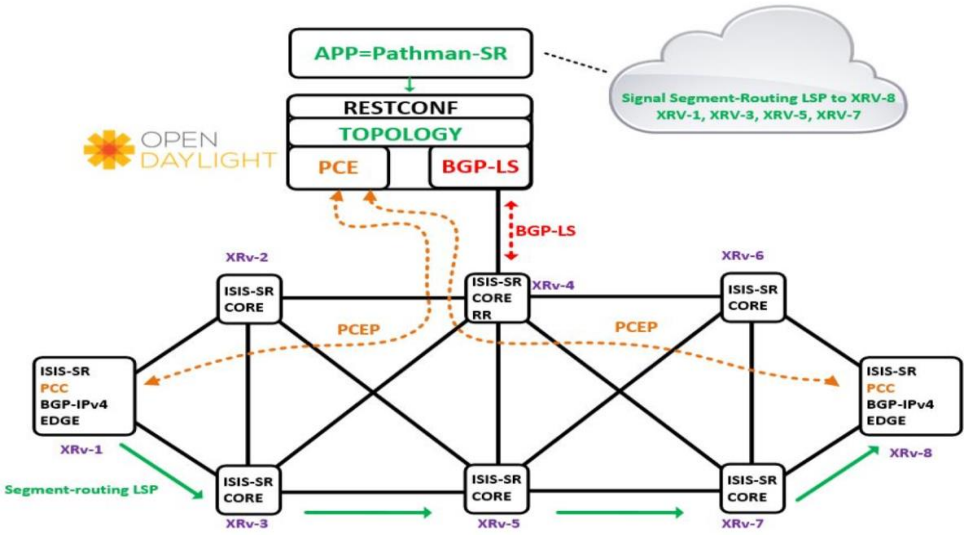


Figura 2.44 Esquema de comunicación usando controlador SDN
Fuente: (Gregory, 2016)

CAPÍTULO 3: Diseño y Simulación de un servicio L3VPN con SR

En este capítulo se diseña y simula la comunicación de dos clientes finales a través de un servicio L3VPN levantado en una red de transporte con tecnología de enrutamiento de segmento, para lo cual se usa la plataforma GNS3. Los equipos a usar son: Cisco IOS XRv a nivel de backbone y Cisco 3725 a nivel de acceso. Los de backbone permiten implementar la tecnología SR, mientras que los de acceso van a funcionar como CE (Customer Edge).

En la implementación se analiza, vía comando CLI, lo siguiente: conectividad punto a punto entre clientes finales, revisión de la cantidad de protocolos habilitados en los routers de backbone, revisión de las etiquetas implementadas para los prefix SID a nivel de routers de Borde (PE) y la revisión del consumo de memoria y estado del CPU en los equipos de red.

3.1. Bloques Funcionales

Consiste en un diseño de red con 5 routers distribuidos de la siguiente manera:

Tabla 3.1 Equipos usados en el diagrama de bloques funcional

No.	Hostname	Modelo	Función
1	CORE	IOS-XRv	Router Core
2	PE1	IOS-XRv	Router Borde
3	PE2	IOS-XRv	Router Borde

4	CE1	Cisco 3725	Router de acceso al cliente
5	CE2	Cisco 3725	Router de acceso al cliente

Fuente: elaborada por el autor

Se ha dividido la red en dos bloques funcionales, el principal o de backbone y el secundario o de acceso. Los routers que conforman la de backbone se encuentran dentro del mismo dominio de enrutamiento, por consiguiente, para este diseño corresponden a un solo proveedor.

Uno de los objetivos de los bloques funcionales, es dar a entender de forma general lo que se va a implementar en el diseño de la red, cuyo objetivo principal es la comunicación de dos clientes finales ubicados en la red de acceso, a través de la red de transporte con tecnología SR implementada en la red de backbone.

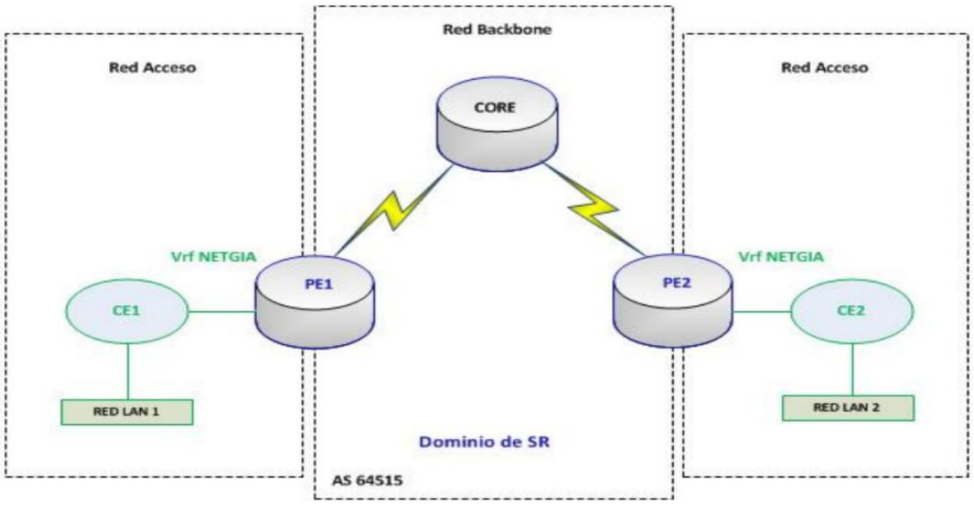


Figura 3.1 Bloques Funcionales del diseño de red
Elaborada por el autor

3.2. Topología de la red con tecnología SR

La topología muestra los protocolos que se van a implementar para la comunicación de dos clientes finales sobre un servicio L3VPN, el cual está levantado a través de una red de transporte con tecnología de enrutamiento de segmentos. Todo este diseño se debe a la implementación a nivel de acceso de tecnologías de última generación, las cuales necesitan que los proveedores estén preparados con una red de transporte más rápida y escalable.

A nivel de backbone se levantan sesiones ISIS entre el router de CORE y los PE, seguido de eso, dentro del IGP se habilita Segment Routing. Las sesiones iBGP se levantan entre los PE. De la misma manera se levantan las sesiones MPBGP entre los PE, para luego configurar la VRF hacia la interfaz que se conecta con los equipos de acceso al cliente y levantar el servicio L3VPN. De esta manera se logra la comunicación entre clientes finales.

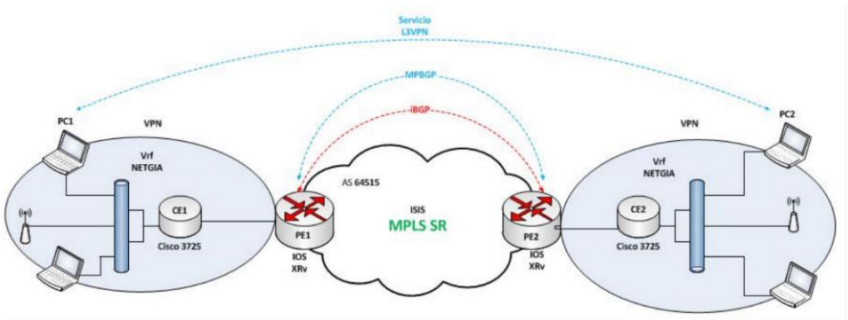


Figura 3.2 Topología de red con los protocolos a implementar
Elaborada por el autor

3.3. Virtualización de la red

GNS3 es un simulador gráfico creado por Cisco que, para este proyecto, se usará en conjunto con máquinas virtuales, lo cual permitirá realizar diseños de topologías de red avanzadas para la aplicación de protocolos de última generación como la tecnología SR.

De Luz, 2016 mencionó que las últimas versiones de GNS3 incorpora GNS3 VM, su propia máquina virtual que trabaja sobre VMware o Virtual Box, es una máquina virtual que funciona con el sistema operativo Ubuntu Linux, con todas las dependencias de GNS3 instaladas por defecto. La compatibilidad de VM con GNS3 está disponible y se puede descargar directamente de la página web oficial.

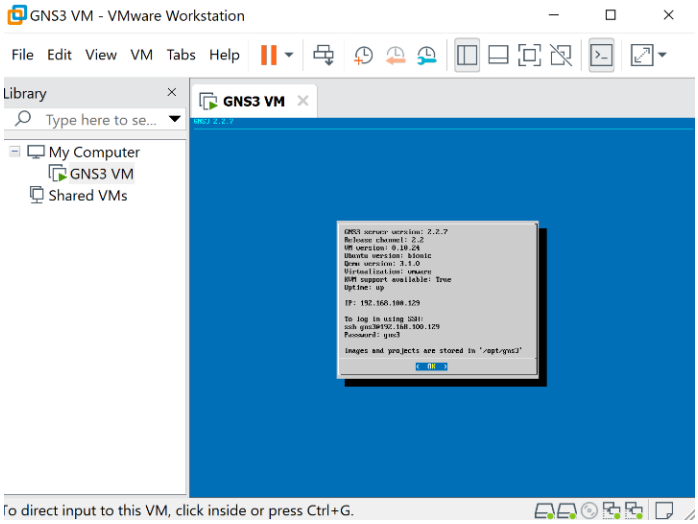


Figura 3.3 Instalación GNS3 VM
Elaborada por el autor

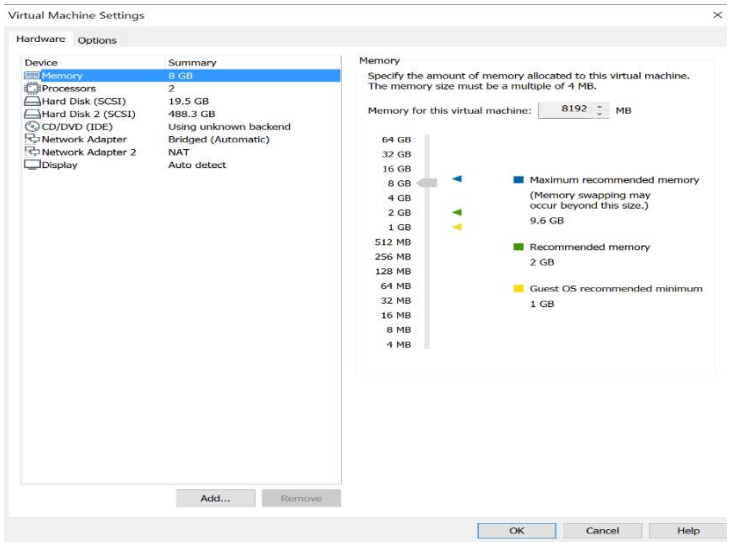


Figura 3.4 Configuración de recursos para la máquina virtual
Elaborada por el autor

La virtualización de la red se basa en el uso de dispositivos virtuales, por lo cual se usaron routers virtuales cuyo software corre dentro de máquinas virtuales ubicadas sobre el mismo hypervisor (administra el hardware del equipo y separa los recursos físicos desde un ambiente virtual).

Para construir la red se usa el router virtual Cisco IOS XRv, del cual se usa la versión DEMO (iosxrv-k9-demo-6.0.1.qcow2) que se encontraba libre en las páginas de cisco. Es importante indicar que a pesar de que la tecnología de enrutamiento de segmentos puede implementarse en versiones IOS XR o IOS XE, casi todas las versiones de IOS tienen un precio en el mercado.

La máquina virtual se encarga de administrar el plano de control y el de datos de Cisco IOS XRv, como también las interfaces de red con sus correspondientes funcionalidades.

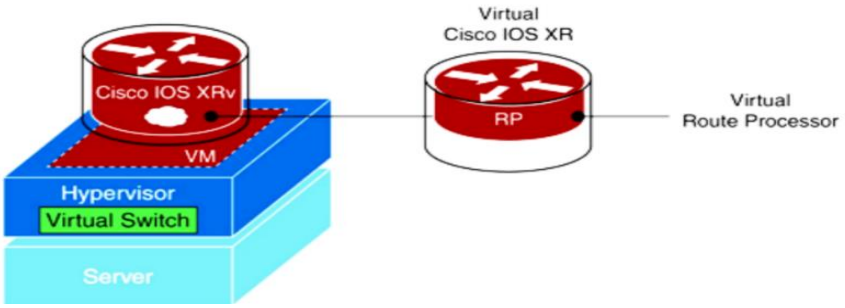


Figura 3.5 Recursos administrados por la Máquina Virtual dentro de Cisco IOS XRv
Fuente: (Kos, 2015)

3.4. Diseño de la red en GNS3

La red se diseñó en GNS3 para montar un prototipo con equipos robustos y de alta gama a nivel de Backbone, usando dispositivos con IOS XRv, para la comunicación de dos clientes a través de SR. Este diseño es aplicado en un solo dominio de red (un solo proveedor).

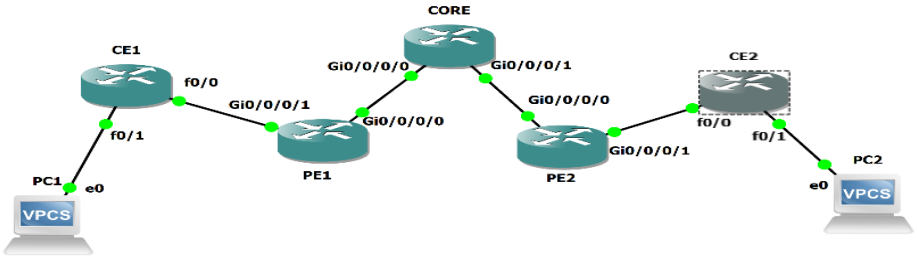


Figura 3.6 Diseño de red en GNS3
Elaborada por el autor

Con este diseño de red se demostrará que es posible la comunicación de dos clientes finales a través de una red con domino SR puro, sin necesidad de protocolos tradicionales de MPLS (LDP, RSVP), esto permite preparar la red para las tecnologías de última generación (IA, IOT, 5G, etc.).

Para este diseño, la red del proveedor va a estar formada por 3 routers (IOSXRv): 1 a nivel de CORE y 2 a nivel de Borde (PE), la red de acceso va estar formada por 2 routers CE (C3725) y 2 PC. El router de Core se conecta a los PE, éstos a su vez se conectan a los CE, a los cuales están conectadas las PC.

Tabla 3.2 Distribución de conexiones entre los equipos de red

Hostname	Interfaces	Descripción

CORE	Gi0/0/0/0 Gi0/0/0/1	###LINK_TO_PE1_Gi0/0/0/0_### ###LINK_TO_PE2_Gi0/0/0/0_###
PE1	Gi0/0/0/0 Gi0/0/0/1	###LINK_TO_CORE_Gi0/0/0/0_### ###LINK_TO_CE1_Fa0/0_###
PE2	Gi0/0/0/0 Gi0/0/0/1	###LINK_TO_CORE_Gi0/0/0/1_### ###LINK_TO_CE2_Fa0/0_###
CE1	Fa0/0 Fa0/1	###LINK_TO_PE1_Gi0/0/0/1_### ###LINK_TO_Pc1_eth0_###
CE2	Fa0/0 Fa0/1	###LINK_TO_PE2_Gi0/0/0/1_### ###LINK_TO_Pc2_eth0_###

Elaborada por el autor

3.5. Configuración de la red

En esta sección se describe en detalle cómo se aplican los comandos vía CLI, en cada uno de los equipos de red. Como se puede observar en la figura 3.2 el objetivo es comunicar dos clientes finales a través de una red de transporte con tecnología SR. Este objetivo se resume cumpliendo los siguientes pasos.

1. Configurar las interfaces de los equipos de red:
   - Loopbacks
   - Gigabitethernet
2. Configurar el protocolo IGP para la red de Backbone (se implementa ISIS).
3. Configurar SR:
   - **Habilitar SR** de manera global en el address-family dentro del IGP.
   - **Habilitar Prefijo-SID** dentro de cada Loopback.
4. Configurar iBGP entre los routers PE.
5. Configurar MP-BGP entre los routers PE.
6. En los routers PE, configurar las vrfs y asociarlas a las interfaces que se conectan a los equipos de acceso.
7. En los routers PE, dentro de las vrfs, enrutar estáticamente las redes LAN que se quieren alcanzar desde un punto al otro.
8. En los CE configurar las loopbacks y enrutar estáticamente la ruta por defecto.
9. Comprobar conectividad desde PC1 a PC2 y viceversa.

3.5.1. Configuración de las interfaces Loopback y Gigabitethernet

En primer lugar, se configuran las interfaces loopbacks y las interfaces WAN que permiten la comunicación y conectividad entre equipos adyacentes.

Tabla 3.3 Loopbacks en el diseño de red

Hostname	Descripciones	Loopback address
CORE	###Loopback 300##	10.30.30.30/32
PE1	###Loopback 100##	10.10.10.10/32
PE2	###Loopback 200##	10.20.20.20/32

Elaborada por el autor

Tabla 3.4 Direccionamientos de interfaces Wan en los equipos de Backbone

Hostname	Interfaces	Direccionamiento
CORE	Gi0/0/0/0	10.10.10.1/30
	Gi0/0/0/1	10.20.20.1/30
PE1	Gi0/0/0/0	10.10.10.2/30
	Gi0/0/0/1	10.11.11.1/30
PE2	Gi0/0/0/0	10.20.20.2/30
	Gi0/0/0/1	10.22.22.1/30

Elaborada por el autor

A continuación, la configuración de las Loopbacks e interfaces WAN de cada equipo de Backbone:

Tabla 3.5 Plantilla de configuración de Loopback e interfaces de CORE

Configuración de Loopback e interfaces de CORE
interface Loopback300 description ### LOOPBACK 300### ipv4 address 10.30.30.30 255.255.255.255 ! interface GigabitEthernet0/0/0/0 description ###LINK TO PE1 Gi0/0/0/0 #### ipv4 address 10.10.10.1 255.255.255.252 ! interface GigabitEthernet0/0/0/1 description ###LINK TO PE2 Gi0/0/0/0 #### ipv4 address 10.20.20.1 255.255.255.252

Elaborada por el autor

Tabla 3.6 Plantilla de configuración de Loopback e interfaces de PE1

Configuración de Loopback e interfaces de PE1
interface Loopback100 description ### LOOPBACK 100### ipv4 address 10.10.10.10 255.255.255.255 ! interface GigabitEthernet0/0/0/0 description ### LINK TO CORE Gi0/0/0/0 #### ipv4 address 10.10.10.2 255.255.255.252 ! interface GigabitEthernet0/0/0/1 description #### LINK TO CE1 Fa0/0#### ipv4 address 10.11.11.1 255.255.255.252

Elaborada por el autor

Tabla 3.7Plantilla de configuración de Loopback e interfaces de PE2

Configuración de Loopback e interfaces de PE2
interface Loopback200 description ### LOOPBACK 200### ipv4 address 10.20.20.20 255.255.255.255 ! interface GigabitEthernet0/0/0/0 description ### LINK TO CORE Gi0/0/0/1 ### ipv4 address 10.20.20.2 255.255.255.252 ! interface GigabitEthernet0/0/0/1 description ###LINK TO CE2 FA 0/0### ipv4 address 10.22.22.1 255.255.255.252

Elaborada por el autor

Comandos de verificación: Se verifica conectividad en los enlaces de Backbone.

Enlace entre CORE – PE1:

RP/0/0/CPU0:CORE#ping 10.10.10.2 source 10.10.10.1
Thu Sep 17 01:38:59.760 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/19 ms

Enlace entre CORE – PE2:

RP/0/0/CPU0: CORE#ping 10.20.20.2 source 10.20.20.1
Thu Sep 17 01:39:05.849 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.2, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/19/69 ms
RP/0/0/CPU0: CORE#

3.5.2. Configuración en la red de Backbone de: Protocolo ISIS, Enrutamiento de Segmento y Prefix-SID.

Como se mencionó al inicio, se usa el protocolo ISIS en los routers de la red de backbone como protocolo IGP, para lo cual se nombra la instancia ISIS "1". Se configura el nivel del área para el cual la instancia fue asignada, en este diseño se trabaja en un solo dominio de red, por lo que es suficiente si se hubiera configurado como "level-1", sin embargo, se lo configura como "level-2". Luego se configura el NET que permite identificar al router dentro del dominio del área.

Dentro del address-family se configura el "metric-style wide" que permite la distribución de nuevos tipos de TLVs. El ISPF es parecido al SPT, la diferencia está en que el ISPF solo recalcula la parte afectada por algún cambio en la topología de red, a diferencia del SPT que recalcula toda la topología por cualquier cambio en la red, lo cual resulta muchas veces innecesario ya que reduce el perfomance de la red y consume recursos como el CPU del equipo de red.

A continuación, se habilita "segment-routing mpls" el cual permite la propagación de las etiquetas con ayuda de los TLVs, a través del IGP. Posterior a eso, se configura las interfaces que serán advertidas por ISIS, en primer lugar la interface Loopback y dentro del address-family su Prefix-SID, el cual ayuda a identificar cada router con una sola etiqueta en todo el dominio SR; por último, se configuran las interfaces Gigabitehternet que tienen como vecinos a otros equipos de backbone.

Tabla 3.8Asignación de Prefijo SID para loopback de Backbone

Hostname	Interface Loopback	Prefix-SID
CORE	###Loopback 300##	19000
PE1	###Loopback 100##	17000
PE2	###Loopback 200##	18000

Elaborada por el autor

Tabla 3.9 Plantilla de configuración de protocolo ISIS, SR y Prefijo SID en CORE

Configuración de protocolo ISIS, enrutamiento de Segmento y Prefijo SID en CORE

```
router isis 1
 is-type level-2-only
 net 49.0001.0100.3003.0030.00
 address-family ipv4 unicast
  metric-style wide
  ispf
  segment-routing mpls
 !
 interface Loopback300
  address-family ipv4 unicast
   prefix-sid absolute 19000
  !
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/1
  address-family ipv4 unicast
```

Elaborada por el autor

Tabla 3.10 Plantilla de Configuración de protocolo ISIS, SR y Prefijo SID en PE1

Configuración de protocolo ISIS, enrutamiento de Segmento y Prefijo SID en PE1

```
router isis 1
 is-type level-2-only
 net 49.0001.0100.1001.0010.00
 address-family ipv4 unicast
  metric-style wide
  ispf
  segment-routing mpls
 !
 interface Loopback100
  address-family ipv4 unicast
   prefix-sid absolute 17000
  !
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv4 unicast
```

Elaborada por el autor

Tabla 3.11 Plantilla de Configuración de protocolo ISIS, SR y Prefijo SID en PE2

Configuración de protocolo ISIS, enrutamiento de Segmento y Prefijo SID en PE2

```
router isis 1
 is-type level-2-only
 net 49.0001.0100.2002.0020.00
 address-family ipv4 unicast
  metric-style wide
  ispf
```

```
 segment-routing mpls
!
interface Loopback200
 address-family ipv4 unicast
  prefix-sid absolute 18000
 !
!
interface GigabitEthernet0/0/0/0
 address-family ipv4 unicast
 !
```

Elaborada por el autor

Comandos de verificación: se comprueba que se aprendan todas las redes por IS-IS y las adyacencias se encuentren establecidas.

En CORE:

```
RP/0/0/CPU0:CORE#sh ip route isis
Thu Sep 17 03:06:59.218 UTC
i L2 10.10.10.10/32 [115/20] via 10.10.10.2, 01:30:09, GigabitEthernet0/0/0/0
i L2 10.20.20.20/32 [115/20] via 10.20.20.2, 01:30:05, GigabitEthernet0/0/0/1
RP/0/0/CPU0:CORE#

RP/0/0/CPU0:CORE#sh isis neighbors
Thu Sep 17 01:48:20.141 UTC
IS-IS 1 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
PE2            Gi0/0/0/1        0c1d.8b43.2a01 Up    27       L2   Capable
PE1            Gi0/0/0/0        0c1d.8bbd.4a01 Up    7        L2   Capable
Total neighbor count: 2
```

En PE1:

```
RP/0/0/CPU0:PE1#sh ip route isis
Thu Sep 17 03:05:14.946 UTC
i L2 10.20.20.0/30 [115/20] via 10.10.10.1, 01:28:20, GigabitEthernet0/0/0/0
i L2 10.20.20.20/32 [115/30] via 10.10.10.1, 01:16:47, GigabitEthernet0/0/0/0
i L2 10.30.30.30/32 [115/20] via 10.10.10.1, 01:15:33, GigabitEthernet0/0/0/0
RP/0/0/CPU0:PE1#
RP/0/0/CPU0:PE1#sh isi neighbors
Thu Sep 17 01:49:48.006 UTC
IS-IS 1 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
CORE           Gi0/0/0/0        0c1d.8b9c.9a01 Up    29       L2   Capable
Total neighbor count: 1
```

En PE2:

```
RP/0/0/CPU0:PE2#sh ip route isis
Thu Sep 17 03:08:46.801 UTC

i L2 10.10.10.0/30 [115/20] via 10.20.20.1, 01:31:55, GigabitEthernet0/0/0/0
i L2 10.10.10.10/32 [115/30] via 10.20.20.1, 01:31:48, GigabitEthernet0/0/0/0
i L2 10.30.30.30/32 [115/20] via 10.20.20.1, 01:19:05, GigabitEthernet0/0/0/0
RP/0/0/CPU0:PE2#

RP/0/0/CPU0:PE2#sh isi neighbors
Thu Sep 17 01:49:51.965 UTC
IS-IS 1 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
CORE           Gi0/0/0/0        0c1d.8b9c.9a02 Up    8        L2   Capable
Total neighbor count: 1
```

Este comando proporciona en detalle la información de SR propagada a través del protocolo IS-IS, entre los principales datos se tiene: capacidad TLV (D,S), SubTLV (I,V), SRGB, Prefix-SID index.

```
RP/0/0/CPU0:PE1#sh isis database verbose PE2
Thu Sep 17 02:56:31.601 UTC
IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
PE2.00-00             0x0000000c   0xd77f        824           0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname:     PE2
  IP Address:   10.20.20.20
  Router Cap:   10.20.20.20, D:0, S:0
    Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Metric: 10         IS-Extended CORE.03
    LAN-ADJ-SID: F:0 B:1 V:1 L:1 S:0 weight:0 Adjacency-sid: 24000 System ID:CORE
    LAN-ADJ-SID: F:0 B:0 V:1 L:1 S:0 weight:0 Adjacency-sid: 24001 System ID:CORE
  Metric: 10         IP-Extended 10.20.20.0/30
  Metric: 10         IP-Extended 10.20.20.20/32
    Prefix-SID Index: 2000, Algorithm:0, R:0 N:1 P:0 E:0 V:0 L:0
 Total Level-2 LSP count: 1     Local Level-2 LSP count: 0
RP/0/0/CPU0:PE1#sh isis database verbose CORE
Thu Sep 17 02:55:25.126 UTC
IS-IS 1 (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
CORE.00-00            0x0000000b   0xadd3        582           0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
```

```
  Hostname:     CORE
  IP Address:   10.30.30.30
  Router Cap:   10.30.30.30, D:0, S:0
    Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Metric: 10         IS-Extended CORE.03
    LAN-ADJ-SID: F:0 B:1 V:1 L:1 S:0 weight:0 Adjacency-sid: 24000 System ID:PE2
    LAN-ADJ-SID: F:0 B:0 V:1 L:1 S:0 weight:0 Adjacency-sid: 24001 System ID:PE2
  Metric: 10         IS-Extended PE1.01
    LAN-ADJ-SID: F:0 B:1 V:1 L:1 S:0 weight:0 Adjacency-sid: 24002 System ID:PE1
    LAN-ADJ-SID: F:0 B:0 V:1 L:1 S:0 weight:0 Adjacency-sid: 24003 System ID:PE1
  Metric: 10         IP-Extended 10.10.10.0/30
  Metric: 10         IP-Extended 10.20.20.0/30
  Metric: 10         IP-Extended 10.30.30.30/32
    Prefix-SID Index: 3000, Algorithm:0, R:0 N:1 P:0 E:0 V:0 L:0
CORE.03-00          0x00000006   0xb6ee        454           0/0/0
  Metric: 0          IS-Extended CORE.00
  Metric: 0          IS-Extended PE2.00
 Total Level-2 LSP count: 2     Local Level-2 LSP count: 0
```

3.5.3. Configuración del iBGP y MPBGP en los PE

Como siguiente punto se levanta la sesión iBGP entre los PE. En primer lugar, la instancia BGP "64515" (sistema autónomo privado). Luego se especifica la interfaz loopback como router-id. Se habilita globalmente el "address-family ipv4 unicast" donde se propaga la interfaz loopback y posterior a eso se habilita el "address-family vpnv4".

El BGP neighbor debe estar levantado sobre el mismo sistema autónomo "64515" y sus actualizaciones se deben hacer sobre la loopback. Por último, se habilita el "address-family ipv4 unicast" y el "address-family vpnv4 unicast" para levantar la sesión MPBGP.

Tabla 3.12 Plantilla de configuración de iBGP y MP-BGP en PE1

Configuración de iBGP y MP-BGP en PE1
router bgp 64515 bgp router-id 10.10.10.10 address-family ipv4 unicast network 10.10.10.10/32 ! address-family vpnv4 unicast ! neighbor 10.20.20.20 remote-as 64515 update-source Loopback100

```
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
!
```

Elaborada por el autor

Tabla 3.13 Plantilla de configuración de iBGP y MP-BGP en PE2

Configuración de iBGP y MP-BGP en PE2

```
router bgp 64515
 bgp router-id 10.20.20.20
 address-family ipv4 unicast
  network 10.20.20.20/32
 !
 address-family vpnv4 unicast
 !
 neighbor 10.10.10.10
  remote-as 64515
  update-source Loopback200
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
 !
```

Elaborada por el autor

Comandos de verificación: Con este comando se observa que la sesión iBGP haya subido y se encuentre establecida, lo cual indica que está lista para recibir servicios vpnv4.

```
RP/0/0/CPU0:PE1#show bgp sessions
Tue Aug 25 02:53:35.221 UTC
Neighbor        VRF             Spk    AS  InQ  OutQ  NBRState     NSRState
10.20.20.20     default           0 64515    0     0  Established  None
```

Con este comando se observa que el MP-BGP se ha levantado, ya que se puede ver la cantidad de 0 prefijos aprendidos, lo que indica que se encuentra a la espera de que se inyecten prefijos desde su vecino.

```
RP/0/0/CPU0:PE1#sh bgp vpnv4 unicast summary
Thu Sep 10 03:58:10.929 UTC
BGP router identifier 10.10.10.10, local AS number 64515
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
```

Table ID: 0x0 RD version: 0
BGP main routing table version 19
BGP NSR Initial initsync version 9 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.

Process	RcvTblVer	bRIB/RIB	LabelVer	ImportVer	SendTblVer	StandbyVer
Speaker	19	19	19	19	19	0

Neighbor	Spk	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	St/PfxRcd
10.20.20.20	0	64515	36	36	19	0	0	00:29:48	**0**

3.5.4. Configuración de las VRF en los PE

Para poder comunicar un cliente con otro se necesita configurar la VRF solo en los equipos PE, lo cual permite levantar los servicios vpnv4 con ayuda de las sesiones MPBGP previamente levantadas sobre la red de transporte de enrutamiento de segmentos.

Primero a la VRF se le asigna un nombre, luego dentro del "address-family ipv4 unicast" se configura los **RT** de importación y exportación que se forman del "Número de AS=64515" y el "Client-id=0" en el siguiente formato "**NumAS:Cid".** Dentro del BGP se configura la VRF y se le asigna un RD, que es el identificador de la VRF. Seguido de eso, se ingresa al "address-family ipv4 unicast" y se redistribuyen las rutas estáticas y conectadas a través de BGP.

Tabla 3.14 Asignación de VRF

VRF	RD	RT
NETGIA	64515:0	64515:0

Elaborada por el autor

Tabla 3.15 Plantilla de Configuración de VRF en PE1

Configuración de VRF en PE1
vrf NETGIA address-family ipv4 unicast import route-target 64515:0 ! export route-target 64515:0 ! router bgp 64515 vrf NETGIA

```
 rd 64515:0
 address-family ipv4 unicast
  redistribute connected
  redistribute static
!
```

Elaborada por el autor

Tabla 3.16 Plantilla de Configuración de VRF en PE2

Configuración de VRF en PE2

```
vrf NETGIA
 address-family ipv4 unicast
  import route-target
   64515:0
  !
  export route-target
   64515:0
!
router bgp 64515
 vrf NETGIA
  rd 64515:0
  address-family ipv4 unicast
   redistribute connected
   redistribute static
!
```

Elaborada por el autor

Comandos de verificación:

```
RP/0/0/CPU0:PE1#sh vrf NETGIA
Thu Sep 17 03:17:51.004 UTC
VRF             RD              RT                  AFI   SAFI
NETGIA          64515:0
                                import  64515:0     IPV4  Unicast
                                export  64515:0     IPV4  Unicast

RP/0/0/CPU0:PE2#sh vrf NETGIA
Thu Sep 17 03:16:44.478 UTC
VRF             RD              RT                  AFI   SAFI
NETGIA          64515:0
                                import  64515:0     IPV4  Unicast
                                export  64515:0     IPV4  Unicast
```

3.5.5. Asociación de la VRF hacia la interfaz que se conecta al cliente y configuración de rutas estáticas en el PE

En cada PE, se asocia la vrf NETGIA a la interfaz que se conecta hacia el CE. Adicional a eso dentro del "router static" se configura la VRF con las rutas estáticas que pertenecen al cliente y a las cuales se quiere alcanzar.

Tabla 3.17 Plantilla de configuración de interfaz que se conecta al cliente y de rutas estáticas en PE1

Configuración de interfaz que se conecta al cliente y de rutas estáticas en PE1
interface GigabitEthernet0/0/0/1 description #### LINK TO CE1 Fa0/0#### vrf NETGIA ipv4 address 10.11.11.1 255.255.255.252 router static vrf NETGIA address-family ipv4 unicast 1.1.1.1/32 GigabitEthernet0/0/0/1 10.11.11.2 10.100.100.0/24 GigabitEthernet0/0/0/1 10.11.11.2

Elaborada por el autor

Tabla 3.18 Plantilla de Configuración de interfaz que se conecta al cliente y de rutas estáticas en PE2

Configuración de interfaz que se conecta al cliente y de rutas estáticas en PE2
interface GigabitEthernet0/0/0/1 description ###LINK TO CE2 FA 0/0### vrf NETGIA ipv4 address 10.22.22.1 255.255.255.252 router static vrf NETGIA address-family ipv4 unicast 2.2.2.2/32 GigabitEthernet0/0/0/1 10.22.22.2 10.200.200.0/24 GigabitEthernet0/0/0/1 10.22.22.2 !

Elaborada por el autor

Comandos de verificación: Con este comando se puede observar las redes que se aprenden con la vrf NETGIA, entre las cuales hay: directamente conectadas, estáticas, locales y por BGP.

En PE1:

```
RP/0/0/CPU0:PE1#show route vrf NETGIA
Thu Sep 17 03:19:51.975 UTC
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
      U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
      A - access/subscriber, a - Application route
      M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is not set

S    1.1.1.1/32 [1/0] via 10.11.11.2, 01:43:04, GigabitEthernet0/0/0/1
C    10.11.11.0/30 is directly connected, 01:43:04, GigabitEthernet0/0/0/1
L    10.11.11.1/32 is directly connected, 01:43:04, GigabitEthernet0/0/0/1
B    10.22.22.0/30 [200/0] via 10.20.20.20 (nexthop in vrf default), 01:39:02
S    10.100.100.0/24 [1/0] via 10.11.11.2, 01:43:04, GigabitEthernet0/0/0/1
RP/0/0/CPU0:PE1#
```

En PE2:

```
RP/0/0/CPU0:PE2#show route vrf NETGIA
Thu Sep 17 03:23:06.982 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
      U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
      A - access/subscriber, a - Application route
      M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is not set

S    2.2.2.2/32 [1/0] via 10.22.22.2, 01:46:21, GigabitEthernet0/0/0/1
B    10.11.11.0/30 [200/0] via 10.10.10.10 (nexthop in vrf default), 01:42:19
C    10.22.22.0/30 is directly connected, 01:46:21, GigabitEthernet0/0/0/1
L    10.22.22.1/32 is directly connected, 01:46:21, GigabitEthernet0/0/0/1
S    10.200.200.0/24 [1/0] via 10.22.22.2, 01:46:21, GigabitEthernet0/0/0/1
RP/0/0/CPU0:PE2#
```

3.5.6. Configuración en los CE de Interfaz Fastethernet, loopback, ruta por defecto y configuración de las PC

Como último punto se configura la interfaz loopback, fastethernet y ruta por defecto en los CE, como también la thernet en las PC, lo cual va a permitir la comunicación con los clientes finales.

Tabla 3.19 Direccionamiento de loopback en los CE

Hostname	Descripciones	Loopback address
CE1	###Loopback 101##	1.1.1.1/32
CE2	###Loopback 102##	2.2.2.2/32

Elaborada por el autor

Tabla 3.20 Direccionamiento de interfaces en los CE y PC

Hostname	Interfaces	Direccionamiento
CE1	Fa0/0	10.11.11.2/30
	Fa0/1	10.100.100.1/24
CE2	Fa0/0	10.22.22.2/30
	Fa0/1	10.200.200.1/24
PC1	eth0	10.100.100.2/24
PC2	eth0	10.200.200.2/24

Elaborada por el autor

Tabla 3.21 Plantilla de Configuración de la loopback, interfaces Fastethernet y ruta por defecto en CE1

Configuración de la loopback, interfaces Fastethernet y ruta por defecto en CE1
interface Loopback101 ip address 1.1.1.1 255.255.255.255 ! interface FastEthernet0/0 description #### LINK TO PE1 Gi0/0/0/1### ip address 10.11.11.2 255.255.255.252 duplex auto speed auto ! interface FastEthernet0/1 description #### LINK_TO_Pc1_eth0_### ip address 10.100.100.1 255.255.255.0 duplex auto speed auto ! ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 10.11.11.1

Elaborada por el autor

Tabla 3.22 Plantilla de Configuración de la loopback, interfaces Fastethernet y ruta por defecto en CE2

Configuración de la loopback, interfaces Fastethernet y ruta por defecto en CE2
interface Loopback102 ip address 2.2.2.2 255.255.255.255 ! interface FastEthernet0/0 description ### LINK TO PE2 Gi0/0/0/1 ### ip address 10.22.22.2 255.255.255.252 duplex auto speed auto

```
!
interface FastEthernet0/1
 description #### LINK_TO_Pc2_eth0_###
 ip address 10.200.200.1 255.255.255.0
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 10.22.22.1
```

Elaborada por el autor

Tabla 3.23 Plantilla de configuración de la PC1

Configuración de la PC1
PC1> ip 10.100.100.2/24 10.100.100.1 Checking for duplicate address... PC1 : 10.100.100.2 255.255.255.0 gateway 10.100.100.1

Elaborada por el autor

Tabla 3.24 Plantilla de configuración de la PC2

Configuración de la PC2
PC2> ip 10.200.200.2/24 10.200.200.1 Checking for duplicate address... PC2 : 10.200.200.2 255.255.255.0 gateway 10.200.200.1

Elaborada por el autor

Comandos de verificación:

Se observa que estén seteados correctamente los valores en las PC.

PC1:

```
PC1> show ip
NAME        : PC1[1]
IP/MASK     : 10.100.100.2/24
GATEWAY     : 10.100.100.1
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10002
RHOST:PORT  : 127.0.0.1:10003
MTU:        : 1500
```

PC2:

```
PC2> show ip
NAME        : PC2[1]
IP/MASK     : 10.200.200.2/24
GATEWAY     : 10.200.200.1
```

DNS :
MAC : 00:50:79:66:68:01
LPORT : 10004
RHOST:PORT : 127.0.0.1:10005
MTU: : 1500

Se observa que se tiene conectividad desde PE1 con la vrf NETGIA hacia las redes LAN locales.

En PE1:

RP/0/0/CPU0:PE1#ping vrf NETGIA 10.11.11.2
Thu Sep 17 01:41:25.410 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.11.11.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/29 ms
RP/0/0/CPU0:PE1#

RP/0/0/CPU0:PE1#ping vrf NETGIA 1.1.1.1
Thu Sep 17 03:26:47.747 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/13/29 ms
RP/0/0/CPU0:PE1#

RP/0/0/CPU0:PE1#ping vrf NETGIA 10.100.100.2
Thu Sep 17 03:27:50.633 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/21/29 ms
RP/0/0/CPU0:PE1#

En PE2:

RP/0/0/CPU0:PE2#ping vrf NETGIA 10.22.22.2
Thu Sep 17 01:41:03.001 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.22.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/49 ms

```
RP/0/0/CPU0:PE2#

RP/0/0/CPU0:PE2#ping vrf NETGIA 2.2.2.2
Thu Sep 17 03:28:43.269 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/15/39 ms
RP/0/0/CPU0:PE2#


RP/0/0/CPU0:PE2#ping vrf NETGIA 10.200.200.2
Thu Sep 17 03:28:56.568 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.200.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/27/39 ms
RP/0/0/CPU0:PE2#
```

3.6. Resultados finales

Se demostrará vía comando CLI, los objetivos logrados con la implementación de esta tecnología SR, en comparación con MPLS.

3.6.1. Prueba de conectividad entre clientes.

Se necesita en primer lugar validar que se estén aprendiendo las redes remotas, a través del protocolo MPbgp.

Comandos de verificación:

En PE1: Se observa que se anuncian 3 redes a través del protocolo MP-BGP desde PE2.

```
RP/0/0/CPU0:PE1#show bgp vpnv4 unicast summary
Thu Sep 17 03:32:04.355 UTC
BGP router identifier 10.10.10.10, local AS number 64515
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 19
BGP NSR Initial initsync version 9 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
```

BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 19 19 19 19 19 0

Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.20.20.20 0 64515 121 121 19 0 0 01:55:00 **3**

Se observan 3 redes aprendidas vía iBGP, anunciadas desde PE2 y levantadas sobre un servicio L3VPN.

RP/0/0/CPU0:PE1#show bgp vrf NETGIA
Mon Sep 7 23:23:12.125 UTC
BGP VRF NETGIA, state: Active
BGP Route Distinguisher: 64515:0
VRF ID: 0x60000002
BGP router identifier 10.10.10.10, local AS number 64515
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000011 RD version: 17
BGP main routing table version 17
BGP NSR Initial initsync version 7 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 64515:0 (default for vrf NETGIA)
*> 1.1.1.1/32 10.11.11.2 0 32768 ?
*>i2.2.2.2/32 10.20.20.20 0 100 0 ?
*> 10.11.11.0/30 0.0.0.0 0 32768 ?
*>i10.22.22.0/30 10.20.20.20 0 100 0 ?
*> 10.100.100.0/24 10.11.11.2 0 32768 ?
***>i10.200.200.0/24 10.20.20.20 0 100 0 ?**
Processed 6 prefixes, 6 paths

RP/0/0/CPU0:PE1#sh ip route vrf NETGIA | i B
Thu Sep 17 03:35:37.751 UTC
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path

```
      M - mobile route, r - RPL, (!) - FRR Backup path
B    2.2.2.2/32 [200/0] via 10.20.20.20 (nexthop in vrf default), 01:54:48
B    10.22.22.0/30 [200/0] via 10.20.20.20 (nexthop in vrf default), 01:54:48
B    10.200.200.0/24 [200/0] via 10.20.20.20 (nexthop in vrf default), 01:54:48
RP/0/0/CPU0:PE1#
```

Se comprueba conectividad desde PC1 hacia PC2.

PC1:

```
PC1> ping 10.200.200.2
84 bytes from 10.200.200.2 icmp_seq=1 ttl=59 time=155.057 ms
84 bytes from 10.200.200.2 icmp_seq=2 ttl=59 time=90.304 ms
84 bytes from 10.200.200.2 icmp_seq=3 ttl=59 time=81.366 ms
84 bytes from 10.200.200.2 icmp_seq=4 ttl=59 time=214.132 ms
84 bytes from 10.200.200.2 icmp_seq=5 ttl=59 time=77.916 ms
```

En PE2: Se observa que se anuncian 3 redes a través del protocolo MP-BGP desde PE1.

```
RP/0/0/CPU0:PE2#show bgp vpnv4 unicast summary
Thu Sep 17 03:37:30.793 UTC
BGP router identifier 10.20.20.20, local AS number 64515
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 20
BGP NSR Initial initsync version 10 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker            20         20         20         20          20           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.10.10.10       0 64515     126     126       20    0    0 02:00:28          3
```

Se observan 3 redes aprendidas vía iBGP, anunciadas desde PE1 y levantadas sobre un servicio L3VPN.

```
RP/0/0/CPU0:PE2#sh bgp vrf NETGIA
```

```
Mon Sep  7 23:18:51.333 UTC
BGP VRF NETGIA, state: Active
BGP Route Distinguisher: 64515:0
VRF ID: 0x60000002
BGP router identifier 10.20.20.20, local AS number 64515
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000011   RD version: 17
BGP main routing table version 17
BGP NSR Initial initsync version 7 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64515:0 (default for vrf NETGIA)
*>i1.1.1.1/32       10.10.10.10              0    100      0 ?
*> 2.2.2.2/32       10.22.22.2               0         32768 ?
*>i10.11.11.0/30    10.10.10.10              0    100      0 ?
*> 10.22.22.0/30    0.0.0.0                  0         32768 ?
*>i10.100.100.0/24  10.10.10.10              0    100      0 ?
*> 10.200.200.0/24  10.22.22.2               0         32768 ?
Processed 6 prefixes, 6 paths

RP/0/0/CPU0:PE2#sh ip route vrf NETGIA | i B
Thu Sep 17 03:36:41.136 UTC
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       M - mobile route, r - RPL, (!) - FRR Backup path
B    1.1.1.1/32 [200/0] via 10.10.10.10 (nexthop in vrf default), 01:55:53
B    10.11.11.0/30 [200/0] via 10.10.10.10 (nexthop in vrf default), 01:55:53
B    10.100.100.0/24 [200/0] via 10.10.10.10 (nexthop in vrf default), 01:55:53
RP/0/0/CPU0:PE2#
```

Se comprueba conectividad desde PC2 hacia PC1.

PC2:

```
PC2> ping 10.100.100.2
84 bytes from 10.100.100.2 icmp_seq=1 ttl=59 time=168.495 ms
84 bytes from 10.100.100.2 icmp_seq=2 ttl=59 time=129.044 ms
84 bytes from 10.100.100.2 icmp_seq=3 ttl=59 time=89.428 ms
84 bytes from 10.100.100.2 icmp_seq=4 ttl=59 time=85.204 ms
84 bytes from 10.100.100.2 icmp_seq=5 ttl=59 time=76.843 ms
```

3.6.2. Validación y comparación, contra MPLS, de la cantidad de protocolos habilitados en routers de Backbone.

Se puede validar que para SR disminuye la cantidad de protocolos habilitados con respecto a si se hubiera usado MPLS. En SR se observa que ya no se habilita LDP ni tampoco RSVP para la formación de túneles de TE. Permitiendo la disminución de consumo de recursos en los equipos de red.

MPLS:

```
RP/0/0/CPU0:PE1#sh mpls interfaces
Wed Aug 12 16:30:14.901 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------
GigabitEthernet0/0/0/2     Yes      Yes      No       Yes
```

Enrutamiento de Segmentos:

```
RP/0/0/CPU0:PE1#sh mpls interfaces
Fri Aug 28 05:01:15.577 UTC
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------
GigabitEthernet0/0/0/0     No       No       No       Yes
```

3.6.3. Revisión de las etiquetas implementadas en los prefix SID a nivel de routers de Borde.

A continuación, se valida que, en SR para llegar al loopback del PE remoto, se usa la misma etiqueta en todo su dominio. Lo contrario sucede en MPLS donde se usan etiquetas diferentes por cada salto. Con lo cual se comprueba que con SR se reduce el consumo de recursos en los equipos de red ya que maneja la misma etiqueta en todo el camino.

MPLS:

```
RP/0/0/CPU0:PE1#sh mpls forwarding
Tue Aug 25 02:47:17.097 UTC
Local  Outgoing    Prefix           Outgoing     Next Hop        Bytes
Label  Label       or ID            Interface                    Switched
------ ----------- ---------------- ------------ --------------- ------------
24000  Pop         10.30.30.30/32   Gi0/0/0/2    10.10.10.1      1316
24001  24000       10.20.20.20/32   Gi0/0/0/2    10.10.10.1      2652
```

```
24002  Pop         10.20.20.0/30      Gi0/0/0/2    10.10.10.1      0
24003  Unlabelled  1.1.1.1/32[V]      Gi0/0/0/0.100 10.11.11.2      500
24004  Aggregate   NETGIA: Per-VRF Aggr[V]   \
                           NETGIA                  174400
RP/0/0/CPU0:PE1#
```

SR:

```
RP/0/0/CPU0:PE1#sh mpls forwarding
Thu Sep 10 03:58:30.708 UTC
Local  Outgoing    Prefix           Outgoing     Next Hop        Bytes
Label  Label       or ID            Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
18000  18000       SR Pfx (idx 2000)  Gi0/0/0/0    10.10.10.1      4067
19000  Pop         SR Pfx (idx 3000)  Gi0/0/0/0    10.10.10.1      0
24000  Pop         SR Adj (idx 1)     Gi0/0/0/0    10.10.10.1      0
24001  Pop         SR Adj (idx 3)     Gi0/0/0/0    10.10.10.1      0
24002  Unlabelled  1.1.1.1/32[V]      Gi0/0/0/1    10.11.11.2      0
24003  Aggregate   NETGIA: Per-VRF Aggr[V]   \
                           NETGIA                  0
24004  Unlabelled  10.100.100.0/24[V] Gi0/0/0/1    10.11.11.2      0
RP/0/0/CPU0:PE1#
```

Comandos adicionales para ver etiquetas propagadas en SR:

```
RP/0/0/CPU0:PE1#sh bgp vpnv4 unicast labels
Thu Sep 17 03:48:41.417 UTC
BGP router identifier 10.10.10.10, local AS number 64515
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 19
BGP NSR Initial initsync version 9 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network          Next Hop      Rcvd Label      Local Label
Route Distinguisher: 64515:0 (default for vrf NETGIA)
*> 1.1.1.1/32       10.11.11.2     nolabel         24002
*>i2.2.2.2/32       10.20.20.20    24002           nolabel
```

```
*> 10.11.11.0/30      0.0.0.0         nolabel         24003
*>i10.22.22.0/30      10.20.20.20     24003           nolabel
*> 10.100.100.0/24    10.11.11.2      nolabel         24004
*>i10.200.200.0/24    10.20.20.20     24004           nolabel

Processed 6 prefixes, 6 paths
RP/0/0/CPU0:PE1#

RP/0/0/CPU0:PE1#sh cef vrf NETGIA 10.200.200.2
Thu Sep 17 03:49:56.622 UTC
10.200.200.0/24, version 10, internal 0x5000001 0x0 (ptr 0xa142e174) [1], 0x0
(0x0), 0x208 (0xa14c9258)
 Updated Sep 17 01:40:49.272
 Prefix Len 24, traffic index 0, precedence n/a, priority 3
   via 10.20.20.20/32, 3 dependencies, recursive [flags 0x6000]
    path-idx 0 NHID 0x0 [0xa15317f4 0x0]
    recursion-via-/32
    next hop VRF - 'default', table - 0xe0000000
    next hop 10.20.20.20/32 via 18000/0/21
     next hop 10.10.10.1/32 Gi0/0/0/0    labels imposed {18000 24004}
RP/0/0/CPU0:PE1#

CE1#traceroute 10.200.200.2
Type escape sequence to abort.
Tracing the route to 10.200.200.2

  1 10.11.11.1 76 msec 76 msec 76 msec
  2 10.10.10.1 [MPLS: Labels 18000/24004 Exp 0] 144 msec 152 msec 148 msec
  3 10.20.20.2 [MPLS: Label 24004 Exp 0] 144 msec 80 msec 100 msec
  4 10.22.22.2 144 msec 144 msec 112 msec
  5 10.200.200.2 144 msec 144 msec 108 msec
CE1#
```

3.6.4. Revisión del consumo de memoria y estado de CPU en los equipos de red

Por último, se comprueba que gracias a los grandes beneficios que presenta SR, como el etiquetamiento incorporado en el protocolo IGP, permite descongestionar la red ya que no se usa protocolos de señalización (LDP y RSVP), reduciendo el consumo de memoria y recursos en los equipos de red, permitiendo que ésta sea más escalable y eficiente.

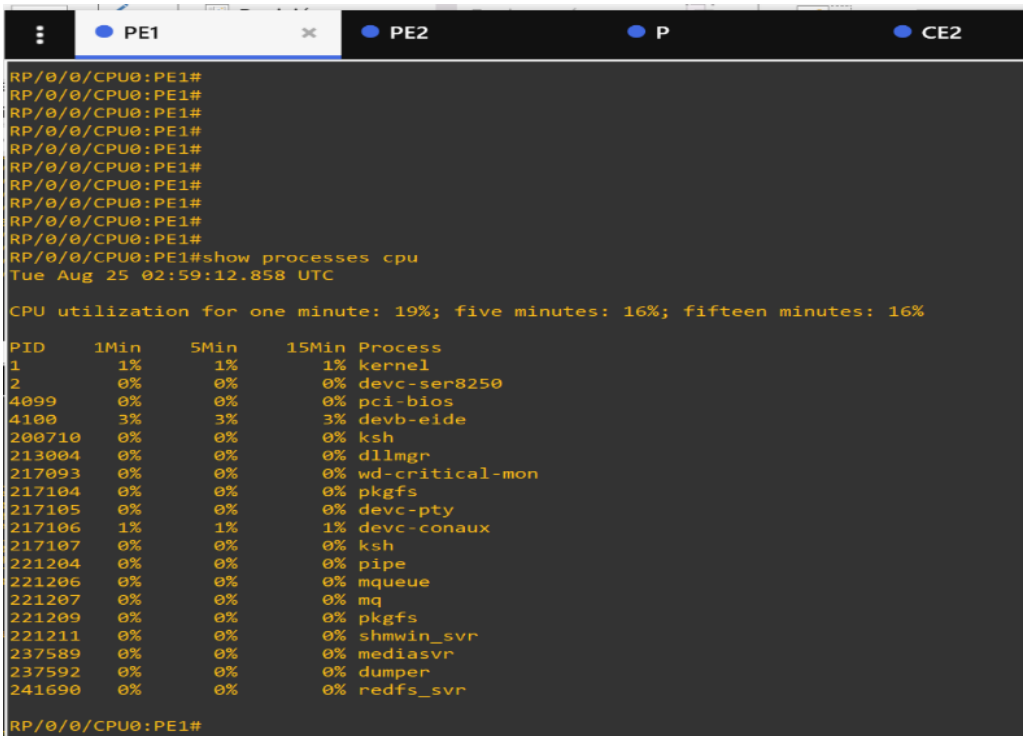


Figura 3.7 Consumo de CPU con MPLS
Elaborada por el autor

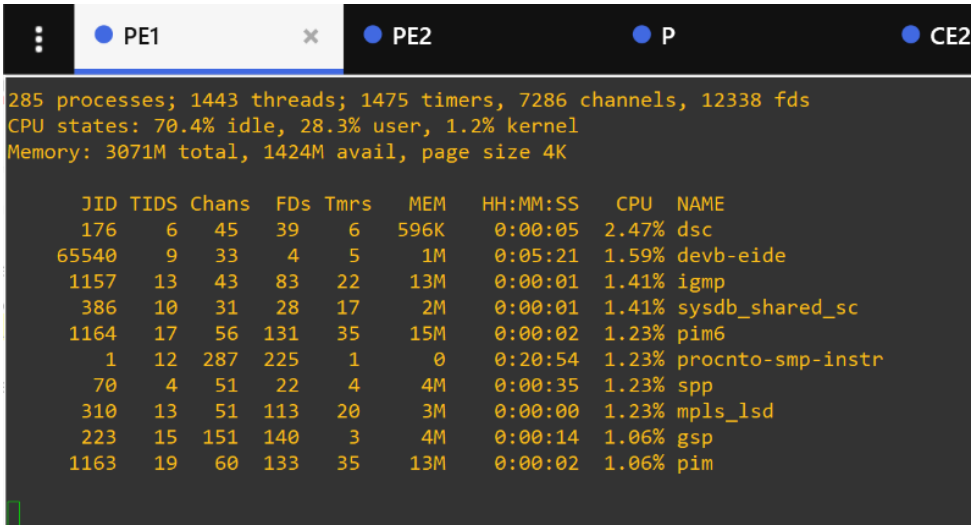


Figura 3.8 Consumo de memoria con MPLS
Elaborada por el autor

SR:

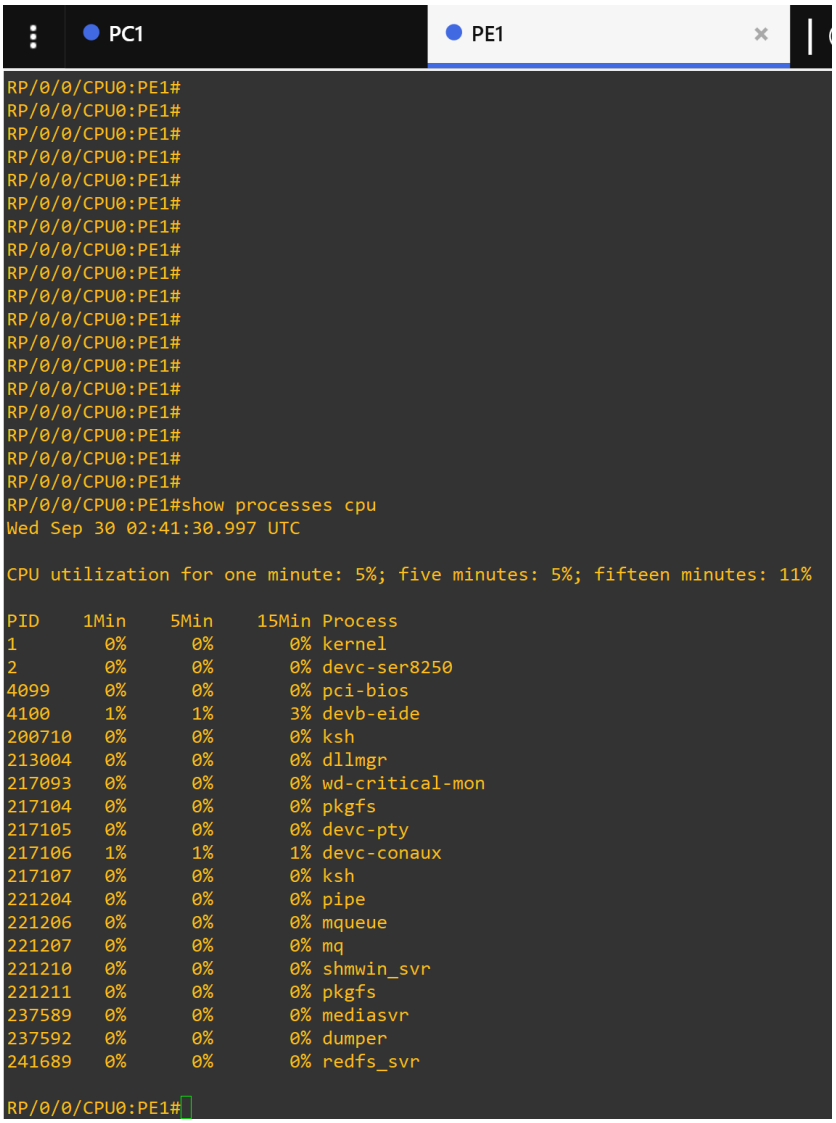


Figura 3.9 Consumo de CPU con SR
Elaborada por el autor

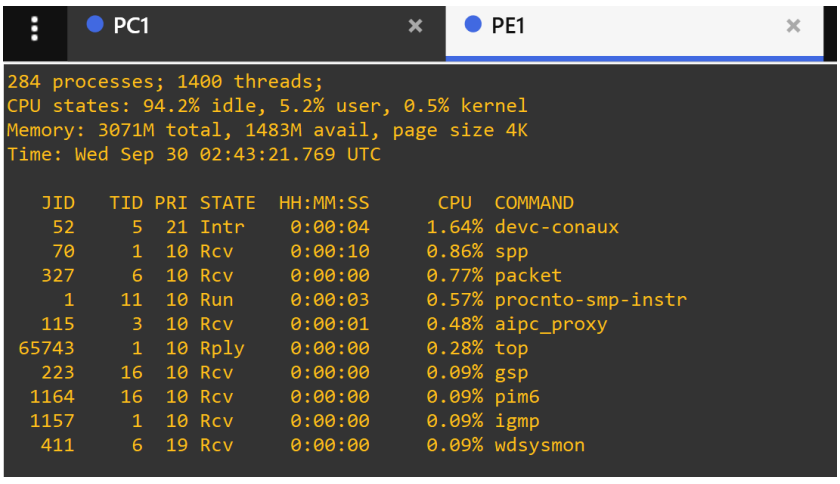


Figura 3.10 Consumo de memoria con SR
Elaborada por el autor

Conclusiones

El diseñar y simular un servicio L3VPN sobre un dominio de SR puro, abre nuevas opciones de configuración una red MPLS ya saturada, obteniendo una red con menos protocolos de señalización y que permite la aplicación de tecnologías de última generación.

Los atributos de simplicidad y escalabilidad junto con la protección avanzada que ofrece Segment Routing, hacen de esta una opción atractiva para diseñar redes de transporte MPLS de próxima generación que admitan servicios y tecnologías modernas como IOT, 5G, IA, SDN, etc.

El enrutamiento de segmento es un nuevo paradigma de reenvío de paquetes que se basa en el enrutamiento de origen, donde el router de entrada SR elige la ruta y la encapsula en la cabecera del paquete, lo que hace que el paquete viaje segmento por segmento hasta llegar a su nodo SR destino, lo cual evita que los routers de tránsito manejen los cambios de estado de la red.

Enrutamiento de segmentos usando el plano de datos MPLS, no requiere LDP o RSVP-TE. Las etiquetas se distribuyen usando Interior Gateway Protocol. Ejecutar menos protocolos dentro del La red ya hace que la red sea más eficaz y facilita el TSHOOT.

Recomendaciones

Para migrar una red MPLS a una con tecnología SR de manera controlada, se recomienda realizar una migración por fases, comenzando con los equipos de CORE (fase 1) hasta terminar con los equipos de acceso (fase n), para de esta manera tener un menor impacto al que si se migrara todos los equipos de la red en una sola fase, para esto se recomienda usar Mapping Server, lo cual ayudará a que los equipos que solo hablen MPLS se entiendan con los equipos que ahora hablan SR.

Se recomienda al operador, que luego de haber tenido un control distribuido de la red, evolucione a un control centralizado, a través de un controlador SDN, donde aprovechará la tecnología SR en su totalidad.

Se recomienda que previo a la implementación de tecnologías de última generación como el IOT, 5G, IA, etc. exista una red de transporte como SR, que vaya a soportar este abrumador crecimiento de tráfico IP.

Se recomienda usar equipos de vendors con amplia experiencia que permita a los analistas implementar nuevos proyectos con esta tecnología de transporte SR, que incluyan soporte técnico y equipos altamente garantizados por parte del proveedor.

Glosario de Términos

5G: Quinta Generación

IA: Inteligencia Artificial

IOT: Internet of Things

SDN: Software Defined Network

MPLS: Multi-Protocol Label Switching

SR: Segment Routing

LDP: Label Distribution Protocol

RSVP: Resource Reservation Protocol

LSP: Label Switch Path

IP: Internet Protocol

VPN: Virtual Private Network

L3VPN: Layer 3 VPN

L2VPN: Layer 2 VPN

EVPN: Ethernet VPN

IETF: Internet Engineering Task Force

SPRING: Source Packet Routing In Networking

EATCN: European Advanced Networking Test Center

MPLS-TE: Multi-Protocol Label Switching – Traffic Engineering

ECMP: Equal Cost Multi-Path

VNI: Visual Networking Index

SSRR: Strict Source Record Routing

LSRR: Loose Source Recorded Routing

RIB: Routing Information Base

ISIS: Intermediate System to Intermediate System

OSPF: Open Shortest Path First

BGP: Border Gateway Protocol

IGP: Interior Gateway Protocol

FRR: Fast Re Route

TI-LFA: Topology Independent Loop-Free Alternate

CSPF: Constrained Shortest Path First

SPF: Shortest Path First

PCEP: Path Computation Element Protocol

SRGB: Segment Routing Global Block

TLV: Type Lenght Value

TDP: Tag Distribution Protocol

SRTE: Segment Routing Traffic Engineering

AER: Application Engineering Routing

PE: Provider Edge

CE: Customer Edge

BGP-LS: BGP Link State

Referencias Bibliográficas

ARISTA. (2019). *MPLS Segment RoutingDriving a modern approach to MPLS transport* . Obtenido de Arista Networks, Inc.: https://www.arista.com/assets/data/pdf/Whitepapers/MPLSSegmentRouting_Whitepaper.pdf

De Luz, S. (2016). *RZ redes zone*. Obtenido de GNS3 lanza la versión 1.4 con importantes mejoras incluyendo GNS3 VM: https://www.redeszone.net/2016/01/17/gns3-lanza-la-version-1-4-con-importantes-mejoras-incluyendo-gns3-vm/

Farrel, A., & Bonica, R. (2017). *IETF Journal*. Obtenido de Enrutamiento por segmentos: descubriendo un tesoro de innovacIón en el IETF: https://www.ietfjournal.org/enrutamiento-por-segmentos-descubriendo-un-tesoro-de-innovacion-en-el-ietf/

Filsfils, C., & Fellow, C. (2019). *SEGMENT ROUTING.* Obtenido de Segment Routing: Technology deep-dive and advanced use cases: https://www.segment-routing.net/images/20190130-bcn-cl-BRKRST-3122-rev7f-km2.pdf

Filsfils, C., & Michielsen, K. (2014). *Segment Routing IGP Control Plane* . Obtenido de Cisco.com: https://www.segment-routing.net/images/0040-SR-TOI-SR_IGP_control_plane_v11a.pdf

Filsfils, C., & Michielsen, K. (2015). *Segment Routing.* Obtenido de Segment Routing Mapping server: http://www.segment-routing.net/tutorials/2016-09-27-segment-routing-mapping-server/

Filsfils, C., Bashandy, A., Gredler, H., Litkowski, S., Decraene, B., & Tantsura, J. (2015). *IS-IS Extensions for Segment Routing draft-ietf-isis-segment-routing-extensions-06.* Obtenido de IETF Tools : https://tools.ietf.org/html/draft-ietf-isis-segment-routing-extensions-06

Gregory, T. (2016). *Segment-routing + Opendaylight SDN + Pathman-SR + PCEP*. Obtenido de PACKETS AND STUFF: https://tgregory.org/2016/12/01/segment-routing-opendaylight-sdn-pathman-sr-pcep/

Jaksic, D. (2018). *Cisco connect: Segment Routing in Service Provider networks.* Obtenido de Cisco : https://www.cisco.com/c/dam/m/hr_hr/training-events/2018/cisco-connect/pdf/Segment_Routing_in_Service_Provider_Network_-_Dejan_Jaksic.pdf

Kos, A. (2015). *Segment Routing principles and applications for SDN.* Milan: Politecnico Di Milano.

Kramer, T. (2017). *Segment Routing Migration Strategies and Case Studies.* Obtenido de ciscolive.com: https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2017/pdf/BRKSPG-2540.pdf

Liste, J. (2018). *@XRDOCS*. Obtenido de MPLS + SDN + NFV World @ Paris2018 – Cisco IOS XR participation at Interoperability Showcase: https://xrdocs.io/cloud-scale-networking/blogs/2018-05-03-cisco-ios-xr-at-mplswc2018-interop/

Mota, R. (2018). *The versatility of segment routing in terms of deployment, distributed versus centralized, network types, data centers/WANs/access, and use cases makes it a solid option for end-to-end network deployment.* (A. R. PAPER, Editor) Obtenido de Segment Routing: https://www.segment-routing.net/images/ACG_Segment_Routing_201808.pdf

Network Working Group. (2007). *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*. Obtenido de RFC 4971 : https://tools.ietf.org/html/rfc4971

Said, J. (2019). *Segment Routing 101 and the Future of MPLS* . Obtenido de Aviat Networks: https://aviatnetworks.com/blog/segment-routing-101-and-the-future-of-mpls/

Ventre, P., Salsano, S., Polverini, M., Cianfrani, A., Abdelsalam, A., Filsfils, C., . . . Clad, F. (2020). *Segment Routing; a Comprehensive Survey of Research Activities, Standardization Efforts and Implementation Results.* Obtenido de Cornell University: https://arxiv.org/abs/1904.03471

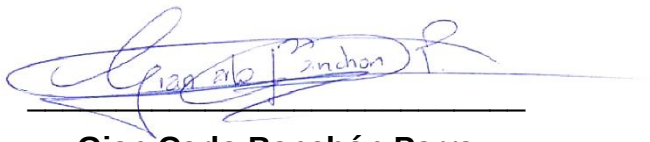
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Gian Carlo Banchón Parra**, con C.C: # **0925379406** autor/a del trabajo de titulación: **Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales,** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 2 de diciembre del 2020



Gian Carlo Banchón Parra

C.C: 0925379406

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	Diseño de un servicio L3VPN en GNS3 con tecnología de enrutamiento de segmentos en un enfoque distribuido para la comunicación de dos clientes finales	
AUTOR(ES)	Gian Carlo Banchón Parra	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz	
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	**Guayaquil, 2 de diciembre del 2020**	**No. DE PÁGINAS: 100**
ÁREAS TEMÁTICAS:	Enrutamiento de Segmentos, Segmentos IGP, Segmento BGP, Intermediate System to Intermediate System, SR Traffic Engineering, Software Define Network, Diseño de red en GNS3	
PALABRAS CLAVES/ KEYWORDS:	5G, IOT, IA, SDN, GNS3, L3VPN, MPLS, VPN	

RESUMEN/ABSTRACT: Uno de los nuevos retos a nivel de proveedor, es tener una red de transporte mucho más rápida y eficaz que consuma menos cantidad de recursos en los equipos de red y que se acople a las nuevas tecnologías de digitalización como 5G (Quinta Generación), IOT (Internet of Things), IA (Inteligencia Artificial), SDN (Software Defined Network), etc. A través de una simulación en GNS3 se levanta un servicio L3VPN (Layer3-Virtual Private Network) sobre una red de transporte con tecnología de enrutamiento de segmentos. Esto permite tener un conocimiento básico sobre el funcionamiento y la aplicación de esta nueva tecnología, la cual se basa en el enrutamiento de origen, que permite la reducción de estados en los routers de tránsito ya que la ruta hasta su destino la decide el router de ingreso, quien agrega a la cabecera del paquete el camino adecuado para llegar a su punto final. Por último, con el diseño y simulación de este proyecto de investigación se podrá demostrar los beneficios que presenta la tecnología de enrutamiento de segmentos en comparación con las redes actuales levantadas sobre MPLS.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO AUTOR/ES:	**Teléfono:** +593-990794134	**E-mail:** gika_3189@hotmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	