Pontificia Universidad Católica del Ecuador
FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Redes de Comunicaciones

ANÁLISIS COMPARATIVO EN UNA INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO

Autor: Ing. Daniel Arturo Pilicita Escobar

Director: PhD. Gustavo Salazar Chacón

Quito, 2024.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, **DANIEL ARTURO PILICITA ESCOBAR,** con C.I 1718710773**,** autor del trabajo de graduación intitulado: **"ANÁLISIS COMPARATIVO EN UNA INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO"**, previa a la obtención del grado académico de **MAGISTER (MAGÍSTER EN TECNOLOGÍAS DE INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES)** en la Facultad de **INGENIERÍA**:

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, 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 graduación 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 Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Quito, enero 2024

Firmado electrónicamente por:
DANIEL ARTURO
PILICITA ESCOBAR

_____

DANIEL ARTURO PILICITA ESCOBAR
C.I. 1718710773

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

APROBACIÓN DEL TUTOR

En mi carácter de Director – Tutor del Trabajo de Posgrado Titulado: "ANÁLISIS COMPARATIVO EN UNA INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO", presentado por el maestrante DANIEL ARTURO PILICITA ESCOBAR, titular de la Cédula de Identidad Nº 1718710773 para optar al Grado de Magíster en Tecnologías de Información mención Redes de Comunicaciones, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ciencias de la Educación.

En la ciudad de Quito, a los 17 días de enero de 2024

Firmado electrónicamente por:
GUSTAVO DAVID SALAZAR CHACON

PhD. GUSTAVO SALAZAR CHACÓN C.I. 1716104797

gsalazar787@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 2 % índice de similitud con otras fuentes.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

turnitin **Informe de Originalidad Turnitin**

TesisFinal-DPilicita por Daniel Pilicita

Desde EntregaFinal (Tesis-Final-Maestría-DPilicita)

Procesado el 17-ene.-2024 12:51 -05
Identificador: 2272658089
Número de palabras: 21819

Índice de similitud	Similitud según fuente	
2%	Internet Sources:	0%
	Publicaciones:	0%
	Trabajos del estudiante:	4%

fuentes:

1 2% match (trabajos de los estudiantes desde 31-oct.-2023)
Clase: Tesis Maestría - Elizabeth Falconí
Ejercicio: Tesis - Elizabeth Falconí
Nº del trabajo: 2213163841

texto del trabajo:

1**FACULTAD DE INGENIERÍA COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE INGENIERÍA**
Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Redes de Comunicaciones
ANÁLISIS COMPARATIVO EN **UNA**

INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO Autor: Ing. Daniel Arturo Pilicita Escobar Director: PhD. Gustavo Salazar Chacón Quito, 2024. COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR DECLARACIÓN Y AUTORIZACIÓN Yo, DANIEL ARTURO PILICITA ESCOBAR, con C.I 1718710773, autor del trabajo de graduación intitulado: "ANÁLISIS COMPARATIVO EN UNA INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO",

1**previa a la obtención del grado académico de MAGISTER** (MAGÍSTER **EN TECNOLOGÍAS DE INFORMACIÓN MENCIÓN REDES DE**

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Daniel Arturo Pilicita Escobar portador de la cédula de ciudadanía No. 1718710773, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Firmado electrónicamente por:
DANIEL ARTURO
PILICITA ESCOBAR

DANIEL ARTURO PILICITA ESCOBAR
C.I. 1718710773

DEDICATORIA

Este logro está dedicado a mi esposa Carolina quien fue indispensable para su culminación; a mis padres Arturo y Alicia, y a mi hermano Diego, quienes junto con Caro siempre me han apoyado en todo, gracias por su ejemplo, motivación y soporte en cada paso.

AGRADECIMIENTOS

Agradezco a Dios por brindarnos vida, salud y bendiciones cada día.

A mi amada esposa Carolina por su apoyo incondicional prácticamente desde que fuimos unos adolescentes, momento en el que inició nuestra bella historia. Gracias por su amor, esfuerzo, motivación y por todos los sacrificios que implican cada logro.

A mis amados padres Arturo y Alicia por su amor incondicional, su ejemplo, su guía, su motivación para impulsarme a conseguir este logro. Gracias por el enorme esfuerzo que han realizado y realizan día a día simplemente por nuestro bienestar. ¡Son mis héroes!

A mi amado hermano Diego quien ha sido un ejemplo de esfuerzo, dedicación y perseverancia. Sé que conseguirá todo lo que se proponga en la vida.

A mi querida tía Blanca, por estar siempre junto a nosotros desde pequeños y desearnos lo mejor en cada aspecto de nuestras vidas.

A mi director de tesis, PhD. Gustavo Salazar por haberme brindado su guía y apoyo en la elaboración del presente trabajo de titulación y por su motivación para seguir avanzado.

A mis profesores de la maestría por brindar a sus estudiantes lo más valioso que se puede compartir, el conocimiento.

A mis compañeros de la maestría quienes fueron un gran apoyo en todo momento durante esta bonita etapa de nuestras vidas.

Finalmente, a todas aquellas personas que con sus palabras de motivación y apoyo fueron muy importantes para la consecución de este logro.

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

ÍNDICE DE CONTENIDOS

Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647
Quito – Ecuador www.puce.edu.ec

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

ANÁLISIS COMPARATIVO EN UNA INFRAESTRUCTURA IPV4 ENTRE MPLS LDP Y SEGMENT ROUTING: PRUEBA DE CONCEPTO PARA UN PROVEEDOR DE SERVICIO

Autor: Ing. Daniel Arturo Pilicita Escobar

Director -Tutor: PhD. Gustavo Salazar Chacón

Fecha: 17 de enero 2024

RESUMEN

El presente trabajo de titulación consiste en emular una red de transporte IP/MPLS (*Internet Protocol / Multi-Protocol Label Switching)* de un Proveedor de Servicios implementando 2 escenarios en el emulador de red EVE-NG. En el primer escenario, se utilizó MPLS LDP (*Label Distribution Protocol*) como protocolo para la distribución de etiquetas, mientras que, en el segundo se configuró MPLS con *Segment Routing*, como nueva tecnología para el transporte de los datos dentro de la red del proveedor.

El objetivo es realizar una comparación de las ventajas y desventajas de cada una de estas tecnologías a través del análisis de resultados de indicadores como capacidad de Traffic Engineering, Latencia y Jitter al inyectar tráfico en la red, para determinar cuál tecnología presenta mayores beneficios y permite optimizar los recursos de la red.

Con respecto a la red del Proveedor de Servicios, está conformada por 4 equipos de Core (P) y 4 equipos Provider Edge (PE). Se utilizaron imágenes de equipos routers marca Cisco de la familia ASR9K con sistema operativo XR. Se implementó IS-IS como IGP (*Interior Gateway Protocol*) para el enrutamiento dentro del Sistema Autónomo y para la interconexión con los equipos del cliente se utilizó BGP (*Border Gateway Protocol*). Para los equipos del cliente (CE) se optó por imágenes de routers Cisco con sistema operativo IOS.

Se implementaron los 2 escenarios indicados previamente y se inyectó tráfico mediante el uso de la herramienta NetEM, que permite agregar retrasos y producir pérdidas entre otras acciones a los paquetes que salen de una interfaz. Se recopilaron los datos necesarios para cada uno de los indicadores, los cuales fueron procesados de forma estadística, finalmente se analizaron los resultados. Estos resultados muestran que la red implementada con *Segment Routing* presenta un mejor desempeño considerando que brinda opciones más sofisticadas para configurar Traffic Engineering, y además los valores de Latencia y Jitter experimentaron una mejora significativa.

De esta forma, se ha determinado que *Segment Routing* brinda mayores beneficios a la vez que optimiza los recursos de la red de un Proveedor de Servicios ISP.

Palabras clave:

Proveedor de servicios, MPLS, LDP, Segment Routing, Traffic Engineering, Latencia, Jitter

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN Y ADMINISTRACIÓN DE TI

COMPARATIVE ANALYSIS IN AN IPV4 INFRASTRUCTURE BETWEEN MPLS LDP AND SEGMENT ROUTING: PROOF OF CONCEPT FOR A SERVICE PROVIDER

Autor: Ing. Daniel Arturo Pilicita Escobar

Director -Tutor: PhD. Gustavo Salazar Chacón

Fecha: 17 de enero 2024

ABSTRACT

This degree work consists in the emulation of an IP/MPLS (Internet Protocol / Multi-Protocol Label Switching) transport network of a Service Provider by implementing 2 scenarios in the EVE-NG network emulator. In the first scenario, MPLS LDP (Label Distribution Protocol) was used as protocol for label distribution, while in the second, MPLS with Segment Routing was configured as a new technology for data transport within the provider's network.

The goal is to make a comparison of the advantages and disadvantages of each of these technologies through the analysis of results of indicators such as Traffic Engineering capacity, Latency and Jitter when injecting traffic into the network, to determine which technology presents greater benefits and optimize network resources.

Regarding to Service Provider's network, this consists of 4 Core (P) devices and 4 Provider Edge (PE) devices. Images of Cisco brand router equipment from the ASR9K family with XR operating system were used. IS-IS was implemented as IGP (Interior Gateway Protocol) for routing within the Autonomous System and BGP (Border Gateway Protocol) was used for interconnection with client equipment. For the client equipment (CE), images of Cisco routers with IOS operating system were chosen.

The 2 scenarios indicated previously were implemented and traffic was injected through the use of the NetEM tool, which allows adding delays and producing losses among other actions to packets leaving an interface. The necessary data for each of the indicators were collected, which were processed statistically, finally the results were analyzed. These results show that the network implemented with Segment Routing presents better performance considering that it provides more sophisticated options to configure Traffic Engineering, and also the Latency and Jitter values experienced a significant improvement.

In this way, it has been determined that Segment Routing provides greater benefits while optimizing the network resources of an ISP Service Provider.

Keywords:

Service Provider, MPLS, LDP, Segment Routing, Traffic Engineering, Latency, Jitter

INTRODUCCIÓN

Año tras año el acceso a Internet llega a más hogares en todo el mundo razón por la cual, la cantidad de usuarios y dispositivos conectados se incrementa de una manera acelerada. Estos usuarios se conectan a Internet a través de empresas proveedoras de servicio de Internet (*ISP*, por sus siglas en inglés *Internet Service Provider*), las cuales utilizan varias tecnologías para este propósito y lo hacen implementando una infraestructura de red necesaria que les permita garantizar la prestación de los servicios contratados por los usuarios.

Una de las tecnologías más utilizadas entre los ISPs en sus redes de transporte es MPLS (*MultiProtocol Label Switching*), que es un estándar desarrollado por el IETF a finales de los 90. Este protocolo realiza ruteo en base a una etiqueta que se agrega a cada uno de los paquetes en lugar de realizar ruteo en base a la dirección destino como se hacía tradicionalmente. Para este propósito utiliza LDP (*Label Distribution Protocol*), que es el protocolo encargado de distribuir las etiquetas. MPLS es multiprotocolo porque se puede aplicar a cualquier tipo de tráfico como puede ser voz, video, datos, entre otros.

Con el tiempo, MPLS evolucionó en funcionalidades que le brindan la posibilidad de proveer otras aplicaciones como son ingeniería de tráfico (*TE Traffic Engineering*), que tiene el propósito de direccionar el tráfico por rutas diferentes a la seleccionada por el IGP (mejor ruta o ruta más corta) gracias a la inclusión de RSVP (*Resource Reservation Protocol*), de esta manera se puede optimizar los recursos de la red, principalmente la ocupación de los enlaces. MPLS permite también marcar el tráfico para que sea transportado con diferente Calidad de Servicio (*QoS Quality of Service*) y así priorizar el tráfico en base a requerimientos particulares, además permite configurar redes virtuales privadas (*VPN Virtual Private Networks*) que son enlaces entre puntos utilizando una infraestructura compartida y representan la aplicación más extendida de MPLS para proveer servicios a los clientes.

En la figura 1, se muestra la topología de una red MPLS típica de un Proveedor de Servicios (ISP):

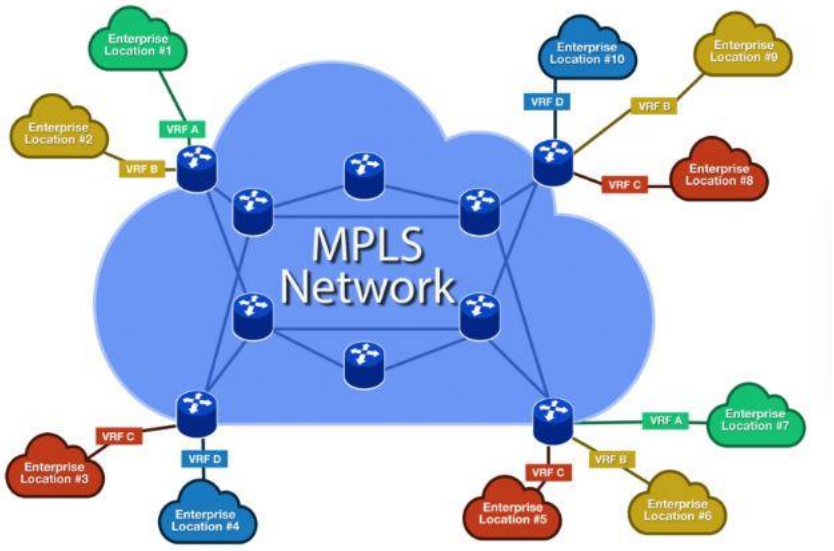


Figura 1. Topología de una Red MPLS de un ISP
Fuente: (IP Specialist, 2019)

Sin embargo, con el desarrollo de nuevas tecnologías, aplicaciones y demás, los usuarios cada vez requieren de mejores prestaciones y mayor ancho de banda por parte de sus Proveedores de Servicio, quienes tienen que adaptar sus redes a esta evolución tecnológica, puesto que las tecnologías tradicionales como MPLS, LDP y RSVP presentan complicaciones especialmente de escalabilidad y

sobrecarga en el performance de los equipos. Es así que, surge *Segment Routing* como una opción que se adapta a estos cambios.

El presente trabajo se realiza con el objetivo de establecer las diferencias entre MPLS con LDP y MPLS utilizando *Segment Routing* para determinar las ventajas y desventajas de cada una de ellas a través del análisis de los resultados obtenidos al emular las topologías diseñadas para un Proveedor de Servicios de telecomunicaciones mediante un emulador de infraestructura de red.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

Las redes IP tradicionales se basan en la información que proveen los protocolos de enrutamiento tales como OSPF (*Open Shortest Path First*), IS-IS (*Intermediate System to Intermediate System*), BGP (*Border Gateway Protocol),* entre otros, o en su defecto, rutas estáticas configuradas en cada router, para tomar la decisión de reenvío de los paquetes, es decir, esta decisión de reenvío se basa única y exclusivamente en la dirección IP de destino. Esto resulta en congestión de ciertas rutas y subutilización de otras.

Actualmente, una gran cantidad de proveedores de servicio de internet ISPs *(Internet Service Provider*) han implementado sus redes utilizando MPLS para el transporte de datos. Una red MPLS (*Multi-Protocol Label Switching*) utiliza etiquetas para el enrutamiento, opera entre las capas 2 y 3 del modelo OSI y puede ser utilizada para transportar diferentes tipos de tráfico, como pueden ser voz, video, paquetes IP, etc. El protocolo creado para asignar dichas etiquetas a los prefijos y anunciarlas a los vecinos es LDP (*Label Distribution Protocol*).

Posteriormente, se introdujo la ingeniería de tráfico TE (*Traffic Engineering*), con la que los routers de ingreso determinan la ruta desde el origen hasta el destino para flujos de tráfico específicos. De esta forma, el tráfico se puede redireccionar a través de rutas subutilizadas descongestionando así las rutas con un elevado nivel de tráfico. Para esto es necesario utilizar el protocolo RSVP (*Resource Reservation Protocol*) que sirve para reservar los recursos a lo largo de toda la ruta que conformarán el túnel de TE.

Los protocolos LDP y RSVP-TE son complicados de implementar, operar y realizar *troubleshooting*. Adicionalmente, crean una gran cantidad de tráfico de señalización en la red y tienen una visualización limitada de la topología, que repercute en la capacidad de *Traffic Engineering* y los tiempos de Latencia y Jitter de forma negativa (Santos, 2019). Otra desventaja de MPLS es el costo del ancho de banda, un cliente que requiera este servicio lo debe obtener a través de un ISP, lo que hace que sea costoso.

Ante los problemas mencionados previamente, surge como alternativa *Segment Routing*, la cual es una tecnología que permite realizar enrutamiento de origen de una forma flexible, sencilla y escalable. Sin embargo, al ser una tecnología relativamente nueva, no se ha implementado a gran escala en las redes de los proveedores de servicios, principalmente por los requisitos a nivel de hardware que se requieren para soportar los nuevos *features* (características, atributos) demandados por esta tecnología.

De lo anterior se puede identificar el siguiente problema principal:

- No se cuenta con un análisis comparativo entre una red IPv4 MPLS que utiliza LDP para el intercambio de etiquetas y una red IPv4 MPLS que utiliza *Segment Routing* mediante un emulador de infraestructura de red para un Proveedor de Servicios de Telecomunicaciones, que permita determinar que *Segment Routing* tiene un mejor rendimiento.

Además, los siguientes problemas secundarios:

- Se carece de un análisis que muestre la diferencia entre MPLS con LDP y MPLS con *Segment Routing*, para determinar las ventajas y desventajas de cada una de ellas.

- No se tiene un diseño de una red IP MPLS utilizando *Segment Routing* para un Proveedor de Servicios de Telecomunicaciones mediante un emulador de infraestructura de red.

- No se cuenta con el análisis de los resultados de MPLS LDP y MPLS con *Segment Routing* utilizando los siguientes indicadores: Capacidad de Traffic Engineering, Latencia y Jitter.

1.2. Objetivos de la Investigación

Objetivo General

Elaborar un análisis comparativo entre una red IPv4 MPLS con LDP y una red IP MPLS utilizando *Segment Routing* para un Proveedor de Servicios de Telecomunicaciones mediante un emulador de infraestructura de red para determinar que *Segment Routing* tiene un mejor rendimiento.

Objetivos Específicos

- Establecer la diferencia entre MPLS con LDP y MPLS con *Segment Routing* para determinar las ventajas y desventajas de cada una de ellas.
- Diseñar una red IP MPLS utilizando *Segment Routing* para un Proveedor de Servicios de Telecomunicaciones mediante un emulador de infraestructura de red.
- Analizar los resultados de MPLS con LDP y MPLS con *Segment Routing* utilizando los siguientes indicadores: capacidad de Traffic Engineering, Latencia y Jitter.

1.3. Justificación de la Investigación

Los requerimientos en cuanto a características que deben garantizar los Proveedores de Servicios de Internet (ISPs) como ancho de banda, disponibilidad, seguridad, redundancia, estabilidad, latencia, entre otras, a los usuarios finales son cada vez mayores. Hoy en día existen muchos más dispositivos conectados a Internet, desde elementos convencionales como computadores, tablets, teléfonos móviles, entre otros, también elementos nuevos pero que resultan cotidianos en el día a día de los usuarios tales como televisores, luces, asistentes inteligentes para el hogar, etc., y que han cambiado la forma de vida de las personas gracias al Internet de las cosas (IoT); hasta recursos más sofisticados como dispositivos médicos, vehículos, sistemas para edificios e incluso ciudades inteligentes. Por otro lado, con la implementación de nuevas tecnologías como las redes móviles 5G e inteligencia artificial, es indispensable contar con mayor capacidad en las redes IP. Las redes de los Proveedores de Servicios, no son una excepción, ya que deben adaptar su infraestructura al continuo desarrollo tecnológico y constante incremento de capacidad, con el objetivo de transportar las grandes cantidades de tráfico generado y atender las nuevas características requeridas, además deben hacerlo de una manera rentable.

Como se había indicado previamente, gran parte de los Proveedores de Servicio de Internet han utilizado MPLS en sus redes para el transporte de los datos, sin embargo, esta tecnología con el paso del tiempo se ha convertido en una solución no escalable por los desafíos que se presentan al implementar nuevos servicios. La tecnología *Segment Routing* puede ser aplicada directamente en la arquitectura MPLS sin afectar el plano de datos. Esta permite utilizar el ancho de banda de la red de una forma más efectiva, a la vez que, optimiza el consumo de los recursos de los equipos que conforman la red. En este sentido, *Segment Routing* se convierte en una opción para los Proveedores de Servicios que buscan simplificar sus redes y hacerlas más escalables, eficientes y rentables.

El propósito de esta investigación es realizar un análisis comparativo del rendimiento entre una red IP MPLS tradicional que utiliza LDP para el intercambio de etiquetas y otra que utiliza *Segment Routing*, del cual se resalten las ventajas y desventajas de cada una de las 2 tecnologías.

Por otro lado, implementar las 2 topologías de redes MPLS, una con LDP y otra con *Segment Routing* en un emulador de red permitirá analizar la viabilidad de una futura implementación de *Segment Routing* en la red de un Proveedor de Servicios y comprobar los beneficios que esta puede ofrecer.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Internet tiene sus orígenes a finales de la década del 60 con la implementación de la primera red de computadoras, ARPANET, por sus siglas en inglés *Advanced Research Projects Agency Network*. Este desarrollo fue llevado a cabo por investigadores estadounidenses y consistió en comunicar 4 nodos ubicados en UCLA, el Stanford Research Institute, la universidad de Utah y la UC de Santa Bárbara, Su propósito fue crear un servicio de mensajes que permitiera a cualquier computadora transmitir un mensaje destinado a cualquier otra y tener la certeza de que fue entregado correctamente (Joskowicz, 2015).

Un ISP (*Internet Service Provider*) por sus siglas en inglés, es un proveedor de servicios de Internet, es decir, su negocio es proveer a los usuarios la conexión a Internet a través de distintas tecnologías ya sean alámbricas o inalámbricas, las cuales han ido evolucionando en el tiempo de acuerdo con los nuevos requerimientos. Entre estas tecnologías se pueden destacar las siguientes: Dial-up (conexión a través de la línea telefónica), ADSL y VDSL (conexión a través de cobre), HFC (soluciones híbridas entre fibra óptica y cable coaxial), FTTH (conexión a través de fibra óptica hasta el hogar) y las redes móviles 3G (HSPA), 4G (LTE) y las de última generación 5G.

En la actualidad, estos proveedores de servicio de Internet (ISPs) utilizan múltiples tecnologías para proporcionar un transporte confiable de los datos a través de sus redes. Una de las tecnologías más comunes para este propósito es MPLS (*Multi-Protocol Label Switching*) que utiliza etiquetas para el enrutamiento y permite proveer servicios que son iguales o funcionalmente equivalentes a los servicios que proveían las empresas de telecomunicaciones tradicionales. Las VPN MPLS son la aplicación más utilizada para proveer servicios a los clientes. Además, se puede implementar características de Calidad de servicio utilizando VPN MPLS de capa 2 con implementación de QoS y se puede optimizar el flujo del tráfico a través de túneles de Ingeniería de Tráfico, entre otras características.

Existen varios protocolos capaces de anunciar etiquetas, pero el principal es LDP (*Label Distribution Protocol*). Gracias a este protocolo, las etiquetas son asignadas a cada dirección en la tabla de enrutamiento global construida y mantenida por el IGP y permite a los routers establecer sesiones entre ellos, crear, anunciar y almacenar *label bindings* (asociaciones entre prefijos y etiquetas), ayudando a rellenar el contenido de la LIB (*Label Information Base*) y LFIB (*Label Forwarding Information Base*).

Para la interconexión entre los distintos equipos que conforman la red MPLS y que se encuentran dispersos geográficamente en diferentes localidades se utiliza DWDM (*Dense Wavelength Division Multiplexing*), multiplexación densa por división de longitud de onda, que es una técnica de transmisión de señales a través de fibra óptica.

Sin embargo, los proveedores de servicio que operan redes IP/MPLS están en la necesidad de adaptar su infraestructura de red existente a los nuevos requerimientos que surgen con el avance de la tecnología y desarrollo de nuevas aplicaciones, sin impactar negativamente en los costos, además de ser escalables, sin que se incremente el grado de complejidad para la administración y operación de la misma.

Ante estas necesidades, aparece *Segment Routing* como una opción bastante atractiva por los beneficios que brinda en general a los proveedores de servicio y que se desarrollarán en el presente trabajo.

2.2. Bases Teóricas

2.2.1. MPLS

En la actualidad la mayoría de ISPs (*Internet Service Providers*) cuentan con tecnología MPLS en sus redes de transporte. Con base en lo indicado en (Cisco, 2014), MPLS proporciona una encapsulación

intermedia entre un encabezado IP de capa 3 de interconexión de sistemas abiertos (OSI) y un encabezado arbitrario de capa 2 de OSI. El reenvío de paquetes a través LSP (*label switched paths)* que se pueden crear utilizando varios métodos y protocolos, según los resultados requeridos y la carga útil puede ser de capa 3 o incluso de capa 2.

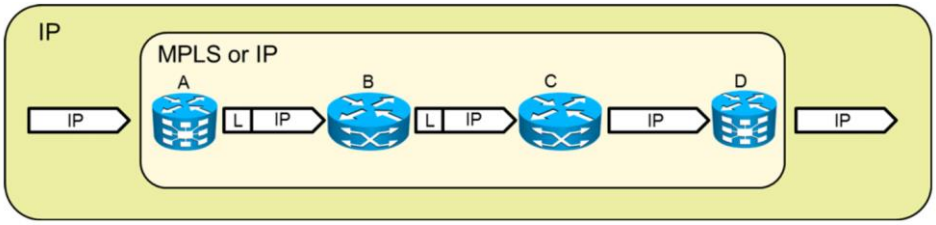


Figura 2. Red MPLS
Fuente: (Cisco, 2014)

MPLS es una tecnología que como se había indicado previamente, se utiliza principalmente en redes de Proveedores de Servicios, la cual mejora el enrutamiento IP clásico mediante el uso de CEF *Cisco Express Forwarding*, con la introducción de un encabezado adicional en los paquetes denominado etiqueta y basa su funcionamiento para el reenvío de paquetes en la búsqueda de etiquetas y no en la búsqueda de direcciones IP. Estas etiquetas generalmente corresponden a las redes IP de destino, es decir, cada destino poseerá una etiqueta correspondiente en cada router que esté habilitado para trabajar con MPLS.

En los proveedores de servicios que hacen uso de MPLS en sus redes de transporte, solamente los routers que se encuentran en el borde del dominio MPLS realizan búsquedas de enrutamiento. Todos los demás routers reenvían los paquetes en base a etiquetas, es decir, el análisis del encabezado de capa 3 se realiza solo una vez, cuando el paquete ingresa al dominio MPLS, luego se agregan las etiquetas al paquete y se reenvía al dominio MPLS.

En la figura 3, se muestra una etiqueta MPLS que se utiliza para el reenvío de los paquetes, esta etiqueta se inserta entre el encabezado de la Capa 2 y la Capa 3 y consta de 32 bits:

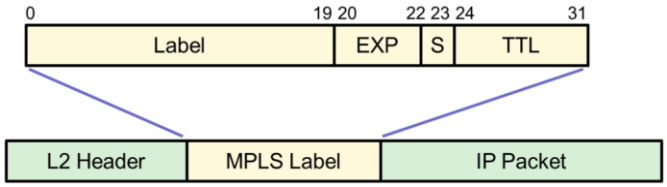


Figura 3. Etiqueta MPLS
Fuente: (Cisco, 2014)

A continuación, se detalla cada uno de sus componentes:

- *Label:* Etiqueta de 20 bits
- EXP: Campo experimental de 3 bits, utilizado para CoS *Class of Service*
- S: Indicador *bottom-of-stack* de 1 bit, determina si la etiqueta es la última insertada en el paquete. Si este bit se establece en 1, indica que esta etiqueta es la última.
- TTL: *Time to Live*, campo de 8 bits, tiene el mismo propósito que el campo TTL (Tiempo de vida) en el encabezado IP.

De acuerdo con lo indicado en (The Cisco Learning Network, 2018), se listan algunas características claves de MPLS:

- Es una tecnología de transporte capaz de llevar un rango amplio de protocolos.
- Sus etiquetas siempre son insertadas entre las capas 2 y 3 del protocolo existente.
- Su transporte está basado en operaciones con etiquetas localmente significativas.
- Las operaciones de sus etiquetas son PUSH, SWAP y POP.
- Se apoya principalmente en *Label Distribution Protocol* (LDP) para anunciar y distribuir *label bindings.*
- Las etiquetas son asignadas a prefijos IP de destino o circuitos virtuales, en general, a caminos hacia un *endpoint* específico y una operación a ser realizada luego de remover dicha etiqueta.
- El rango disponible de etiquetas es de 0 a 1’048.575.
- El rango reservado de etiquetas es de 0 a 15:

ETIQUETA	**PROPÓSITO**
0	Explicit Null Se envía al último LSR para mantener el campo EXP que contiene los valores de QoS, de lo contrario el PHP quitará todas las etiquetas y se perderá el campo EXP
1	Router Alert Label Cuando se requiera que el siguiente LSR ignore la etiqueta y lo procese como un paquete IP normal
2	Explicit Null (IPv6)
3	Implicit Null (*Penultimate Hop Popping* PHP) Indica al siguiente LSR que el paquete saldrá de la red MPLS y deben ser removidas todas las etiquetas y procesar como un paquete IP normal
4 - 12	No están asignadas
13 y 14	GAL Label y OAM Alert Label Usadas para detección de fallas, localización y monitoreo de rendimiento
15	No está asignada

Tabla 1. Etiquetas reservadas en MPLS
Fuente: (Edson Hernández, 2020)

A continuación, se muestra un ejemplo de cómo realiza MPLS el reenvío de paquetes:

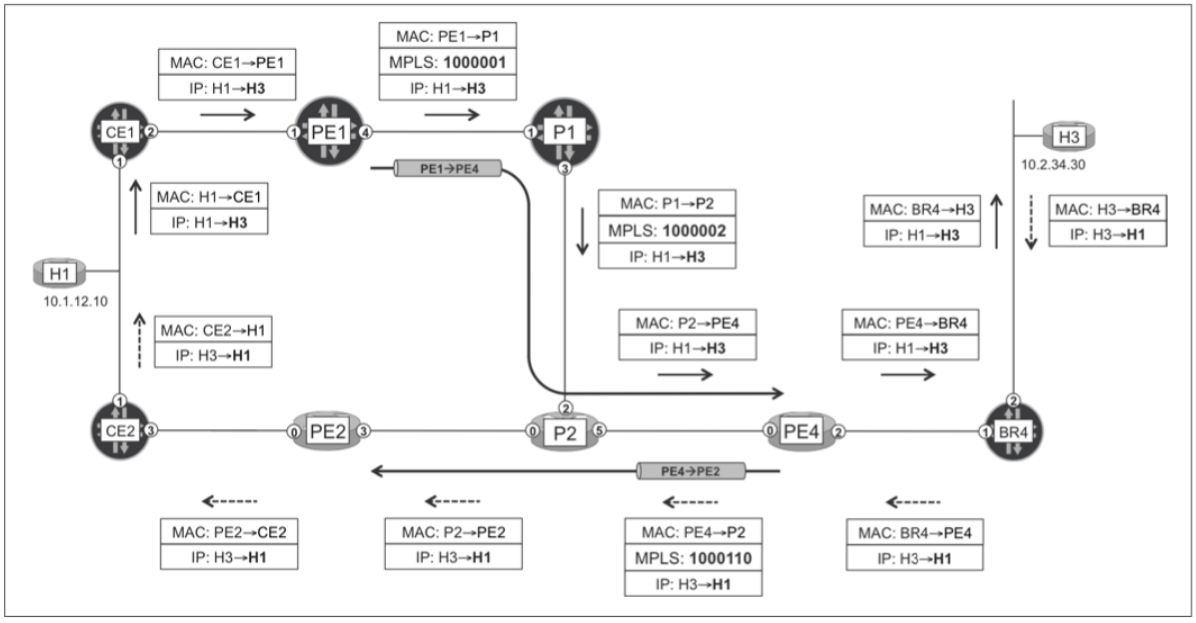


Figura 4. Reenvío de paquetes en MPLS

Fuente: (Sánchez Monge & Szarkowicz, 2015)

(Sánchez Monge & Szarkowicz, 2015) indican mediante un ejemplo como MPLS reenvía los paquetes:

La figura 4 muestra dos *Label-Switched Paths* (LSPs) denominados PE1→PE4 y PE4→PE2. Enfocándose en el primero, un paquete IPv4 H1→H3 (10.1.12.10→10.2.34.30) llega a PE1, lo que conduce a lo siguiente:

1.- H3 es alcanzable a través de PE4, por lo que, PE1 coloca el paquete en el LSP PE1→PE4. Lo hace insertando un nuevo encabezado MPLS entre los encabezados IPv4 y Ethernet del paquete H1→H3. Este encabezado contiene la etiqueta MPLS 1000001, que es localmente significativa para P1. Esta operación es una inserción (*Push)* de etiqueta. Finalmente, PE1 envía el paquete a P1.

2.- P1 recibe el paquete, lo inspecciona y elimina el encabezado MPLS original. Luego, P1 agrega un nuevo encabezado MPLS con la etiqueta 1000002, que es localmente significativo para P2, y envía el paquete a P2. Esta operación se denomina intercambio (*swap*) de etiquetas.

3.- P2 recibe el paquete, lo inspecciona y elimina el encabezado MPLS, posteriormente, envía el paquete IPv4 puro hacia PE4. Esta operación se denomina *pop*.

4.- PE4 recibe el paquete IPv4 sin encabezados MPLS. Esto debido a que, en este caso PE4 habla BGP y conoce todas las rutas IPv4, por lo que sabe cómo reenviar el paquete hacia su destino.

Como se puede apreciar, el LSP PE1→PE4 comienza en PE1, atraviesa P1 y P2 y termina en PE4. Al colocar el paquete en el LSP, PE1 básicamente lo envía a PE4. De hecho, cuando P2 recibe un paquete con la etiqueta 1000002, la instrucción de reenvío es clara: abre la etiqueta y envía el paquete fuera de la interfaz correspondiente (Gi 0/0/0/5).

El paquete H1→H3 llega sin etiquetar a PE4 en virtud de un mecanismo llamado *Penultimate Hop Popping (PHP)* ejecutado por P2.

Penultimate Hop Popping (PHP), el penúltimo router antes de que salga el paquete de la red MPLS es responsable de eliminar la etiqueta MPLS y reenviar el tráfico al PE de salida. El PE de salida luego realiza una búsqueda de ruta IP y reenvía el tráfico.

En cuanto al paquete H3→H1, este viaja de PE4 a PE2 en un LSP más corto donde solo se llevan a cabo dos operaciones MPLS: inserción (*push*) de etiquetas en PE4 y extracción (*pop*) de etiquetas en P2. No hay intercambio de etiquetas.

2.2.1.1. Roles de los enrutadores en la red MPLS

En base a la figura 4, se pueden indicar los siguientes roles de los enrutadores desde el punto de vista del LSP PE1→PE4:

- **PE1: (*Ingress LSR)***, el término ingreso (*ingress)* se refiere al hecho de que los paquetes de usuario como H1→H3 ingresan al LSP en PE1, que actúa como punto de entrada o ingreso. Éste LSR está en el borde de la red MPLS y es el primero en insertar un encabezado y una etiqueta MPLS en un paquete.

- **P1 (o P2): (*Intermediate LSR*)**, Provider Router. Son los LSR que existen dentro de la red y son responsables de poner, quitar e intercambiar las etiquetas según el enrutamiento en la red MPLS.

- **PE4: (*Egress LSR*)**, el término egreso (*egress)* proviene del hecho de que los paquetes de usuario como H1→H3 salen del LSP en este PE. Éste LSR está en el borde de la red y es el

último punto antes de salir de ella. Por lo tanto, elimina todas las etiquetas y encabezados MPLS.

2.2.2. LDP Label Distribution Protocol

De acuerdo con la información proporcionada en (Hesselbach et al., 2014) un protocolo de distribución de etiquetas es un conjunto de procedimientos a través del cual un router LSR informa a otro de la relación etiqueta/FEC que ha formado. Dos routers LSR que utilizan un protocolo de distribución de etiquetas para intercambiar información se conocen como "puertos de distribución de etiquetas". Si dos routers LSR son puertos de distribución de etiquetas, se puede indicar que hay una "distribución de etiquetas adyacente" entre ellos.

El intercambio de mensajes entre LSR´s se realiza mediante el envío de PDU´s de LDP. Este envío se basa en la utilización de sesiones LDP que se establecen sobre conexiones TCP. Es importante indicar que cada LDP PDU puede transportar más de un mensaje LDP, sin que estos mensajes deban tener relación entre ellos. El protocolo LDP utiliza un esquema de codificación de mensajes conocido como TLV (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura:

- **U:** Campo de un bit que indica el comportamiento en caso de recibir un mensaje desconocido. Si U=0 indica que se debe responder con un mensaje de notificación al LSR origen, si U=1 se ignora el mensaje y se continúa procesando el PDU.

- **F:** Campo de un bit. Este campo solamente se utiliza si el bit U=1. Si se recibe un mensaje desconocido que debe propagarse y el bit F está en cero, este mensaje no avanza al siguiente LSR, en caso contrario si se hace.

- **Tipo:** Campo de 14 bits que define el tipo de mensaje y, por lo tanto, indica cómo debe ser interpretado el campo valor.

- **Longitud**: campo de 2 octetos que especifica la longitud del campo valor.

- **Valor:** Campo de longitud variable que contienen la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

Ahora, según lo indicado en (Sánchez Monge & Szarkowicz, 2015), LDP puede señalar tres tipos de *transport Label-Switched Paths (LSPs),* rutas de transporte conmutadas por etiqueta: multipunto a punto (MP2P), punto a multipunto (P2MP) y multipunto a multipunto (MP2MP).

LDP posee varias características que lo hacen altamente escalable desde el punto de vista operativo como son:

- La señalización de etiquetas tiene lugar en las conexiones TCP. Esto permite una entrega confiable con una actualización.

- Por otro lado, los LSP de MP2P implican una reducción de estado significativa.

- Adicionalmente, cuando se trata de configurar LSP de transporte, LDP es plug-and-play, es decir, simplemente se habilita LDP en las interfaces principales y listo.

A continuación, se muestra un ejemplo breve de la habilitación de LDP tanto en un equipo Cisco IOS XR, así como, en un equipo Juniper:

Configuración de LDP en IOS XR
mpls ldp interface GigabitEthernet0/0/0/3 interface GigabitEthernet0/0/0/4

Tabla 2. Configuración de LDP en IOS XR
Fuente: (Sánchez Monge & Szarkowicz, 2015)

Configuración de LDP en JUNOS:

protocols {
ldp {
track-igp-metric;
interface ge-0/0/3.0;
interface ge-0/0/4.0;
}}

Tabla 3. Configuración de LDP en JUNOS
Fuente: (Sánchez Monge & Szarkowicz, 2015)

Descubrimiento y sesiones LDP

Una vez que se habilita LDP en una interfaz, comienza un proceso llamado *LDP Discovery*, descubrimiento básico. El LSR empieza a enviar y recibir mensajes LDP de *hello* en cada una de las interfaces configuradas según se muestra en la siguiente figura:

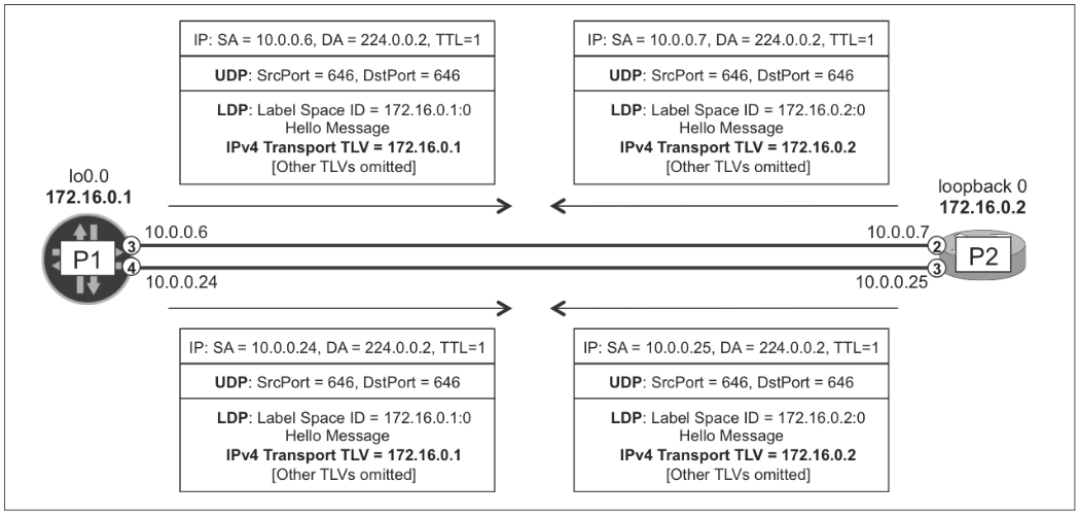


Figura 5. Mensajes Hello en LDP
Fuente: (Sánchez Monge & Szarkowicz, 2015)

Los mensajes de *hello* LDP se encapsulan de la siguiente manera:

- Primero, en una cabecera UDP, con puerto de origen y destino 646.
- Luego, en un encabezado IPv4 con TTL=1 y dirección de destino multicast 224.0.0.2.

Estos paquetes no son enrutables y su único propósito es establecer adyacencias entre vecinos conectados directamente. Cabe indicar que para los vecinos que no se encuentran directamente conectados, existe otro método llamado descubrimiento extendido *extended discovery* o *targeted LDP*, en el cual los *hellos* LDP son unicast y multisalto (TTL>1).

El proceso de descubrimiento básico genera *hellos* LDP de adyacencias, uno por cada interfaz habilitada para LDP, por esta razón, en la figura 5 establecen dos adyacencias *hello* entre P1 y P2.

***Hellos* de adyacencias LDP en P1 (Junos):**

juniper@P1> **show ldp neighbor**

Address	Interface	Label space ID	Hold time
10.0.0.2	ge-2/0/1.0	172.16.0.11:0	13
10.0.0.7	**ge-2/0/3.0**	**172.16.0.2:0**	12
10.0.0.25	**ge-2/0/4.0**	**172.16.0.2:0**	12
10.0.0.9	ge-2/0/6.0	12 172.16.0.33:0	14

***Hellos* de adyacencias LDP en P2 (IOS XR):**

RP/0/0/CPU0:P2#**show mpls ldp discovery brief**
Local LDP Identifier: 172.16.0.2:0

Discovery Source	VRF Name	Peer LDP ID	Hold time	Session
Gi0/0/0/0	default	172.16.0.22:0	15	Y
Gi0/0/0/2	default	**172.16.0.1:0**	15	Y
Gi0/0/0/3	default	**172.16.0.1:0**	15	Y
Gi0/0/0/5	default	172.16.0.44:0	15	Y

El descubrimiento LDP desencadena el establecimiento de una sesión LDP sobre TCP entre cada par de LSRs vecinos. Los puntos finales de estas sesiones TCP multisalto son las direcciones de transporte codificadas en los *hellos* basados en UDP.

Aunque P1 y P2 tienen más de un *hello* LDP de adyacencia, solo establecen una sesión LDP entre sus direcciones de loopback.

Una vez establecida la conexión TCP a través del *three-way handshake*, P1 y P2 intercambian mensajes de inicialización LDP y, finalmente, la información de la etiqueta.

Sesiones LDP en P1 (Junos):

juniper@P1> **show ldp session**

Address	State	Connection	Hold time	Adv. Mode
172.16.0.2	Operational	Open	24	DU
172.16.0.11	Operational	Open	21	DU
172.16.0.33	Operational	Open	20	DU

Sesiones LDP en P2 (IOS XR):

RP/0/0/CPU0:P2#**show mpls ldp neighbor brief**

Peer	GR	NSR	Up time	Discovery	Address	IPv4 Label
172.16.0.22:0	N	N	1d04h	1	6	25
172.16.0.22:0	N	N	1d04h	1	5	23
172.16.0.1:0	N	N	0:02:02	2	6	10

En LDP existe dos tipos de mecanismos de *heartbeat*:

- Mensajes *LDP-over-UDP* para mantener las adyacencias *hello* LDP.
- *Keepalives LDP-over-TCP* para mantener las sesiones LDP.

Asignación de etiquetas LDP

Una vez que dos vecinos establecen una sesión LDP, inicia el intercambio de mensajes de mapeo de etiquetas para asociar prefijos IPv4 a etiquetas MPLS. Esta asignación de etiquetas permite la formación de la *Label Information Base* (LIB).

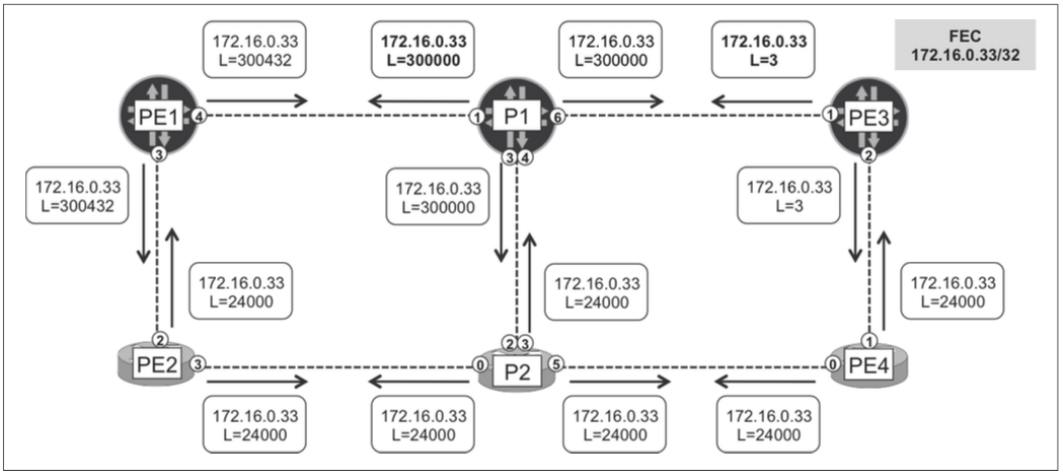


Figura 6. Mensajes LDP label mapping para 172.16.0.33
Fuente: (Sánchez Monge & Szarkowicz, 2015)

En base a la topología de la figura 6, PE1 necesita un LSP que termine en PE3 para enviar paquetes más allá de PE3. La FEC *Forwarding Equivalence Class* asociada a ese LSP está representada por 172.16.0.33/32, la dirección de loopback de PE3. El PE de ingreso PE1 no canaliza necesariamente el tráfico destinado a la propia FEC, generalmente, el paquete coincide con una ruta en PE1 cuyo siguiente salto BGP es 172.16.0.33. Esta es la asociación entre el paquete y la FEC.

Centrándose en el prefijo IPv4 o FEC, la dirección loopback de PE3 (172.16.0.33/32), se observa que todos los routers centrales de la red anuncian una asignación de etiquetas para este prefijo y se determina que cada router anuncia la misma asignación de etiquetas en cada sesión LDP. Así, P1 anuncia la asignación para la FEC 172.16.0.33/32 la etiqueta 300000 a todos sus vecinos. Esta etiqueta tiene significado local en P1. Es decir, P1 vincula localmente la etiqueta 300000 a 172.16.0.33/32, y dice a sus pares LDP que, si desean que envíe un paquete por el túnel hacia PE3, se lo envíen con un encabezado MPLS que contenga la etiqueta 300000.

Esta asignación solo tiene significado local y debe interpretarse en el contexto del espacio de etiquetas 172.16.0.1:0. El primer campo es el ID del router P1 y el segundo campo (cero) representa un espacio de etiqueta de plataforma. En este sentido, la búsqueda de etiquetas se lleva a cabo en P1, independientemente de la interfaz a la que llegue el paquete MPLS. Si P1 recibe un paquete cuya etiqueta MPLS externa es 300000, sin importar la interfaz de entrada, P1 lo colocará en un LSP hacia PE3. El mapeo (172.16.0.33/32, 3000000) tiene un significado para toda la plataforma dentro de P1.

Cabe recalcar que, debido a que las etiquetas MPLS tienen un significado local, cada router generalmente anuncia una asignación de etiquetas diferente para una FEC determinada. Sin embargo, no existe ninguna regla que obligue a que las etiquetas sean diferentes. Por ejemplo, PE2, P2 y PE4 anuncian la misma etiqueta para 172.16.0.33/32 (24000), esto es posible y está correcto porque cada etiqueta pertenece a un espacio de etiqueta de plataforma diferente (LSR).

2.2.3. Aplicaciones MPLS

Según lo indicado en (Cisco, 2023), existen varios tipos de aplicaciones con las que puede utilizar MPLS:

- Enrutamiento IP unicast, es la aplicación más común para MPLS.
- Enrutamiento IP multicast, posee diferentes requerimientos de reenvío.
- MPLS TE (*Traffic Engineering*), es un complemento de MPLS para optimizar la utilización de los enlaces.
- VPN MPLS, permiten la superposición (*overlapping)* de direcciones entre VPNs.
- QoS (*Quality of Service*), se puede proporcionar una calidad de servicio diferenciada.

A continuación, se amplían algunas de estas aplicaciones antes mencionadas:

2.2.3.1. Enrutamiento IP MPLS

Antes de hablar sobre el enrutamiento IP MPLS, es necesario indicar como se lleva a cabo el enrutamiento IP tradicional:

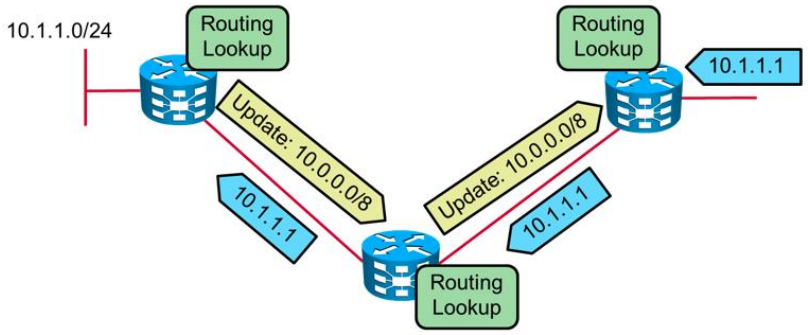


Figura 7. Enrutamiento IP tradicional
Fuente: (Cisco, 2014)

Como se puede observar en la figura 7, el enrutamiento IP basa su funcionamiento en direcciones IP, es decir, se utiliza para distribuir información de enrutamiento de capa 3.

Cada router analiza el encabezado de capa 3 de cada paquete, lo compara con la tabla de enrutamiento local y toma una decisión sobre dónde reenviar el paquete. Independientemente del protocolo de enrutamiento, los router reenvían paquetes dependiendo de la búsqueda basada en la dirección de destino. Finalmente, esta búsqueda se realiza de forma independiente en cada router de la red.

Con este antecedente, el enrutamiento IP MPLS proporciona una mejora con respecto al enrutamiento IP tradicional ya que ofrece los siguientes beneficios:

- Utiliza etiquetas para el reenvío de paquetes incrementado la eficiencia de la red, puesto que, la operación de intercambio de etiquetas consume menos recursos de CPU que una búsqueda de enrutamiento.
- MPLS puede proporcionar servicios orientados a la conexión al tráfico IP, debido al reenvío basado en FEC. La FEC (*Forwarding Equivalence Class*) corresponde a una dirección de destino almacenada en la tabla de enrutamiento IP.
- MPLS soporta también enrutamiento IP multicast, sin la necesidad de un protocolo dedicado, simplemente, se utiliza PIM (*Protocol Independent Multicast*) versión 2 con extensiones para MPLS para propagar la información de enrutamiento y etiquetas. En este caso, la FEC es igual a una dirección de destino muticast.

MPLS simple utiliza solamente una etiqueta en cada paquete. Sin embargo, también es posible insertar varias etiquetas en un paquete a través de una pila de etiquetas (*Label Stack*). Este apilamiento consiste en la encapsulación de un paquete MPLS dentro de otro paquete MPLS cuyo resultado brinda la capacidad de tunelizar un LSP MPLS dentro de otro LSP.

Entre otras aplicaciones que agregan etiquetas adicionales a los paquetes se tienen: MPLS VPN, MPLS TE, MPLS QoS. Para habilitar estos servicios y otras funciones avanzadas se requiere la inserción de dos o más etiquetas en un paquete.

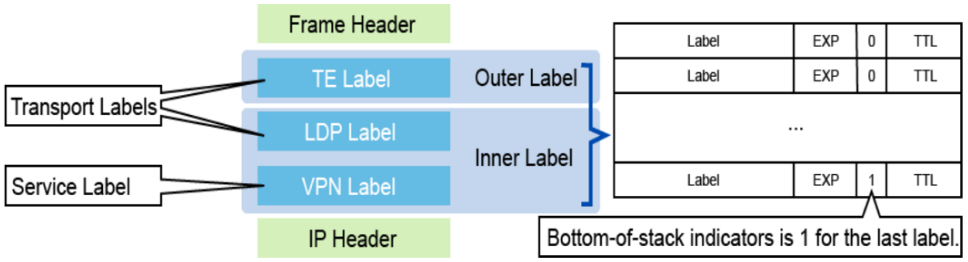


Figura 8. Apilamiento de Etiquetas MPLS
Fuente: (Cisco, 2023)

La etiqueta exterior se usa para conmutar un paquete MPLS a través de la red. En la figura 8, la capa exterior corresponde a una etiqueta de *Traffic Enginnering* que tiene como destino el punto final de un túnel de TE. Los routers intermedios ignoran las etiquetas internas. En este ejemplo, las etiquetas internas se utilizan para apuntar al router de salida y para identificar la VPN del paquete. El bit *bottom-of-stack* determina si una etiqueta es la última que se halla inserta en el paquete, si este bit es (1), indica que es la última etiqueta.

2.2.3.2. MPLS TE Traffic Engineering, Ingeniería de tráfico

El objetivo de utilizar MPLS TE *Traffic Engineering*, es controlar el flujo de tráfico que cursa por la red, optimizando el uso de los recursos y, por ende, reduciendo la congestión que se puede producir en ciertos enlaces que tienen preferencia por el algoritmo del IGP.

Figura 9. MPLS Traffic Engineering
Fuente: (Cisco, 2023)

MPLS TE requiere de los siguientes requisitos:

- Cada LSR debe ver la topología completa de la red. En este punto, solamente OSPF e IS-IS tienen una visión de la topología completa.

- Cada LSR necesita información adicional sobre los enlaces en la red. Esta información incluye los recursos disponibles y las limitaciones. OSPF e IS-IS tienen extensiones para propagar esta

información adicional.

- RSVP es utilizado para establecer los túneles de TE y propagar las etiquetas. Los túneles siempre son unidireccionales.

En base a lo indicado en (The Cisco Learning Network, 2018), MPLS-TE *(MPLS Traffic Engineering)* comprende un grupo de extensiones de ingeniería de tráfico para los IGPs de *link-state (OSPF e IS-IS)* que permiten llevar información sobre el ancho de banda total y reservable en cada enlace entre los routers de una red. Adicionalmente, MPLS-TE utiliza el protocolo RSVP para realizar el anuncio y conteo del ancho de banda utilizado por los túneles TE en los enlaces individuales, y anuncia las etiquetas MPLS para esos túneles TE.

En este sentido, el IGP busca el camino más corto que cumpla los requerimientos de ancho de banda de un túnel en particular, luego, entrega la secuencia exacta de routers y enlaces a RSVP para que realice el conteo del ancho de banda usado y disponible a lo largo de este camino, y anuncie la etiqueta correspondiente. Estos caminos son conocidos como túneles TE y son siempre unidireccionales desde el *headend* hasta el *tailend*.

MPLS-TE es una de las aplicaciones más importantes de MPLS, sin embargo, surgen inconvenientes con respecto a su escalabilidad. Primero, presenta cierto grado de complejidad es su configuración y operación, ya que cada túnel posee propiedades únicas como con el destino, ancho de banda requerido, camino a seguir, entre otros, y debe ser configurado en el router *headend* obligatoriamente. En una red de un Proveedor de Servicios existirán cientos de túneles, además pueden existir túneles múltiples con diferentes requerimientos entre los mismos *endpoints*. Otra complicación es el uso de RSVP para la señalización que representa una carga adicional en los equipos y por ende en la escalabilidad. Finalmente, otro aspecto a considerar de MPLS-TE al momento de una implementación, son las responsabilidades adicionales de los IGPs, OSPF o IS-IS, que como se indicó previamente, han sido extendidos con una característica adicional conocida como *Constrained Shortest Path First* (CSPF), la cual permite determinar el camino más corto y también toma en cuenta el ancho de banda disponible, para asegurar que el camino más corto calculado pueda contener un túnel con un ancho de banda requerido.

2.2.3.3. VPN MPLS

Las VPN MPLS hacen referencia a un enlace punto - punto o punto – multipunto que utiliza una infraestructura compartida o red pública y permiten tener escalabilidad dividiendo en segmentos más pequeños a las redes. Son de gran utilidad ya que permiten proveer redes aisladas a departamentos de un cliente o entre clientes utilizando una infraestructura única.

Las VPN MPLS son muy escalables y permiten el soporte de servicios IP como:

- Unicast
- Multicast
- Calidad del servicio QoS
- Servicios centralizados

Las redes son aprendidas vía IGP o BGP desde los clientes o a través de MP-BGP desde otros PEs. Se utilizan dos etiquetas:

- La etiqueta superior (LDP) sirve para vincular los LSR de borde con un único túnel LSP.
- La etiqueta interior se utiliza para propagar la información y las etiquetas de enrutamiento de

VPN a través del dominio MPLS por medio del MP-BGP *Multiprotocol Border Gateway Protocol*.

2.2.3.3.1. VPNs MPLS de Capa 3

Conforme con la información proporcionada en (Cisco, 2023), la principal característica de las VPNs MPLS de capa 3 es que la conexión entre el proveedor de servicios y los clientes es a través de IP, es decir, es necesario establecer un enrutamiento IP, sea estático o dinámico para poder intercambiar información de enrutamiento entre los sitios de los clientes que pertenezcan a la misma VPN.

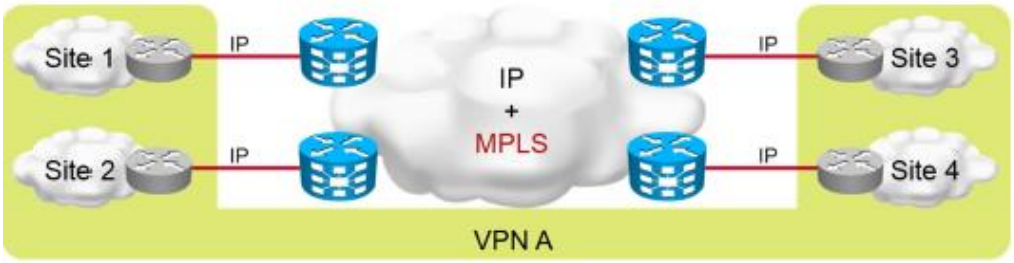


Figura 10. VPN MPLS de capa 3
Fuente: (Cisco, 2014)

En las redes de los proveedores de Servicios van a existir cientos o miles de clientes, los cuales pueden utilizar rangos de direcciones IP privadas iguales, en este sentido, no pueden realizar un reenvío normal puesto que existirían problemas por duplicación de IPs (*overlapping*), más bien, deben garantizar el aislamiento en el plano de datos entre los paquetes que pertenecen a diferentes clientes.

Las VRFs *(Virtual and Routing Forwarding)* permiten aislar la información de enrutamiento de cada cliente, y lo hacen a través de la expansión de los prefijos IPv4 marcándolos con un identificador de 64 bits llamado RD *(Route Distinguisher)*, que los convierte en únicos dentro de cada VRF.

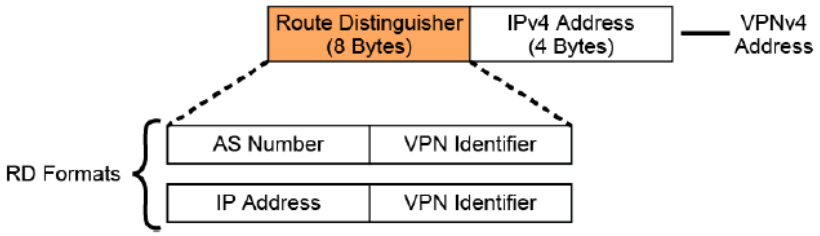


Figura 11. Route Distinguisher
Fuente: (Cisco, 2023)

El resultado de añadir el RD a la dirección IPv4 da como resultado la formación de una dirección VPNv4 de 96 bits. Estas direcciones VPNv4 son intercambiadas entre routers PEs mediante el protocolo MP-BGP. En IPv6, el proceso de añadir el RD es similar y el prefijo pasará a llamarse VPNv6.

Cuando existe la necesidad de que varios sitios participen en más de una VPN, el RD no es suficiente, es así que, se introduce el concepto de RT (*Route Target*). Los RTs son comunidades extendidas que permiten a una VRF participar en múltiples VPNs, es decir, identifican la membresía VPN de rutas aprendidas de un sitio en particular.

Los RT se implementan mediante el uso de comunidades extendidas, donde los 16 bits de orden superior de la comunidad extendida (64 bits en total) están codificados con un valor correspondiente a la membresía VPN del sitio específico.

Los RT son agregados a una ruta de un cliente en particular, cuando esta es convertida en prefijo VPNv4 por el router PE. Los RT insertados a la ruta se denominan **RT de exportación** y se configuran por separado para cada tabla de enrutamiento virtual en el router PE.

Cuando las rutas VPNv4 se propagan a otros routers PE, esos routers deben seleccionar las rutas para importar a sus tablas de enrutamiento virtuales. Esta selección se basa en el **RT de importación**. Cada tabla de enrutamiento virtual en el router PE puede tener varios RTs de importación configurados que identifican el conjunto de VPNs desde las cuales se deben aceptar las rutas.

2.2.3.3.2. VPNs MPLS de Capa 2

Las VPNs MPLS de capa 2 permiten a los proveedores de servicios ofrecer conexiones de capa 2 punto a punto o multipunto entre sitios de clientes distantes. Consolidan el tráfico de capa 2, como Ethernet, Frame Relay, ATM, entre otros, a través de una red IP o MPLS (Cisco, 2014).

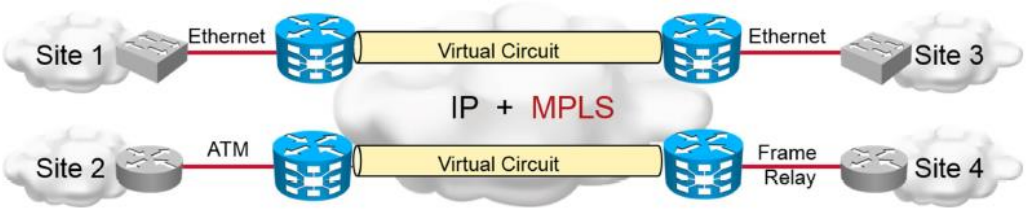


Figura 12. VPN MPLS de capa 2
Fuente: (Cisco, 2014)

La principal característica de las VPN MPLS de capa 2 es que no se requiere señalización IP entre el cliente y el proveedor de servicios.

EoMPLS se puede implementar de dos maneras:

1. Ethernet punto a punto sobre MPLS, donde todo el tráfico Ethernet se intercambia a través de un único circuito virtual (LSP). Existen 2 modos:

   - Modo de puerto: Las tramas Ethernet completas se encapsulan en un LSP MPLS. Esta opción permite enrutar una interfaz física a un único sitio remoto distante, pero puede usar VLAN IEEE 802.1Q de extremo a extremo.

   - Modo VLAN: Las VLANs seleccionadas se extraen y encapsulan en LSPs MPLS dedicados. Esta opción permite que el sitio central de un cliente utilice un único enlace físico con múltiples VLANs que luego se enrutan a múltiples sitios remotos individuales en diferentes ubicaciones.

2. VPLS, permiten la interconexión de múltiples sitios a través de una malla completa de circuitos virtuales.

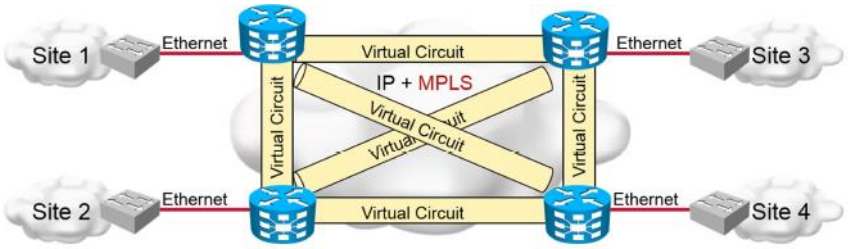


Figura 13. VPLS
Fuente: (Cisco, 2014)

2.2.3.4. Calidad de servicio MPLS QoS

La calidad de servicio QoS (*Quality of Service*) permite proporcionar servicios diferenciados a través de una red MPLS, clasificando los paquetes y de esta manera previniendo la generación de congestión.

MPLS no define una nueva arquitectura de QoS, sino que más bien, se ha adaptado para soportar las Arquitecturas de QoS IP actuales. El objetivo principal del modelo Cisco DiffServ (*Differentiated Services*) es proporcionar escalabilidad y un nivel de QoS similar al del modelo IntServ (*Integrated Services*) sin necesidad de un control por flujo. La red simplemente identifica una clase y aplica las medidas apropiadas.

Una QoS diferenciada se obtiene mediante el uso de bits MPLS experimentales o mediante la creación de túneles LSP separados para diferentes clases. Las extensiones de LDP se utilizan para crear múltiples túneles LSP para el mismo destino (uno para cada clase).

La clasificación y el condicionamiento se realizan en el borde. Los nodos centrales implementan un comportamiento de reenvío.

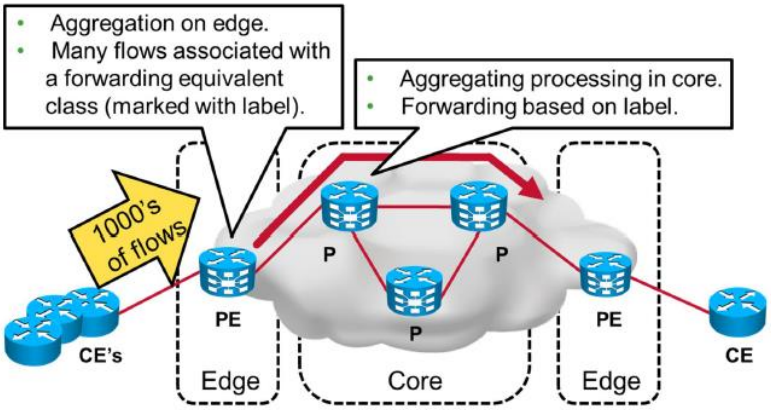


Figura 14. MPLS QoS
Fuente: (Cisco, 2014)

Los paquetes MPLS necesitan llevar la marca del paquete en sus encabezados porque los LSRs no examinan el encabezado IP durante el reenvío. Para esto se utiliza un campo EXP de 3 bits en el encabezado MPLS.

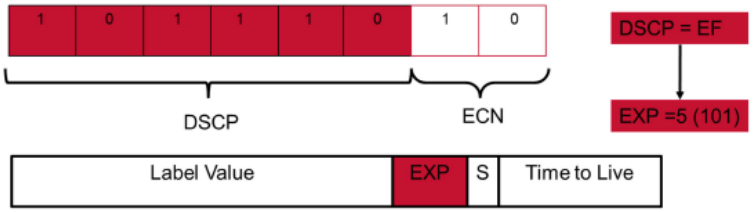


Figura 15. Campo EXP para QoS
Fuente: (Cisco, 2014)

El valor DSCP se asigna al valor EXP en el router PE.

2.2.4. Segment Routing

De acuerdo con lo indicado en (Cisco, 2023), *Segment Routing* es una forma flexible y escalable de realizar enrutamiento de origen. Es una tecnología que aprovecha la infraestructura MPLS existente y que brinda la posibilidad de definir el camino que por donde se enrutará el tráfico de una forma más precisa y sencilla. Esta mejora además permite introducir soluciones de red definidas por software en

la red de un proveedor de servicios.

En *Segment Routing* el origen elige una ruta que se codifica en el encabezado del paquete como una lista ordenada de segmentos. Un segmento se puede definir como un identificador para un nodo, una ruta, un servicio, una instrucción o un identificador de una política de ingeniería de tráfico.

Estos segmentos pueden tener un significado global o local. Los de significado global son válidos para todo el dominio de enrutamiento del segmento y son identificados por un *Segment Identifier* SID, el cual se elige de un rango de etiquetas conocido como *Segment Routing Global Block SRGB.* Este bloque global es un rango de etiquetas que está reservado para *Segment Routing* y comprende desde 16.000 hasta 23.999. Por otro lado, los segmentos con un significado local se aplican y tienen sentido solo para el router emisor e identifican enlaces hacia otros routers, rutas alternas, etc.

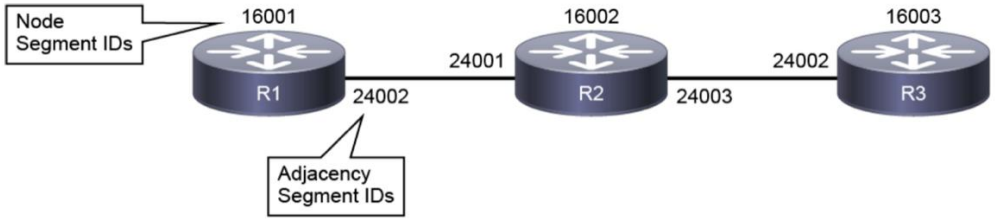


Figura 16. Segments ID
Fuente: (Cisco, 2023)

Los *Segment Identifiers* SIDs deben ser asignados a los routers de forma manual, puesto que tienen un alcance global, son válidos en todo el dominio y por lo tanto deben ser únicos. En la figura 16, se puede observar que R1 tiene el SID 16001, R2 el SID 16002 y R3 el SID 16003 y se verifica que son únicos. Generalmente, estas etiquetas no cambian en caso de reinicio de los equipos.

También se asignan etiquetas a los enlaces entre routers, se las conoce como *Adjacency Segment IDs*. En este caso son únicas localmente y pueden configurarse de forma manual o asignarse automáticamente. A diferencia de las anteriores, estas si pueden cambiar en caso de reinicio del router.

Adicionalmente, existe un *Segment ID* de prefijo el cual identifica a cada prefijo, similar al MPLS regular.

2.2.4.1. Reenvío de paquetes en Segment Routing

Segment Routing define en el origen la ruta de un paquete para que sea transportado a través de la red. La red entregará el paquete de acuerdo con las instrucciones, también conocidas como segmentos.

En la siguiente figura, las etiquetas se establecen en el router de origen, es decir, en donde el paquete ingresa a la red, en este caso, el router R1.

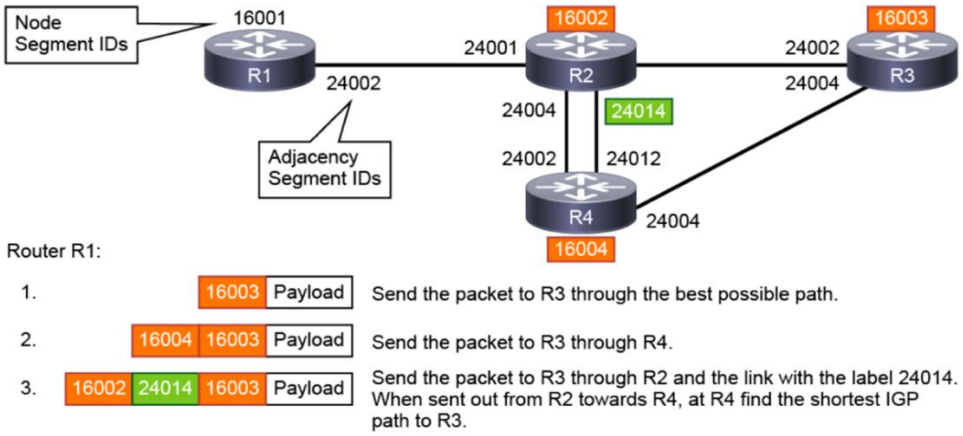


Figura 17. Segments ID asignados a prefijos
Fuente: (Cisco, 2023)

Existen algunas posibilidades sobre cómo las etiquetas de *Segment Routing* trabajan para el reenvío de paquetes, dependiendo de las etiquetas y del conjunto de etiquetas con las que se inserten en el paquete. En el ejemplo de la Figura 17, se puede indicar lo siguiente:

- Cuando R1 recibe un paquete etiquetado con una etiqueta de *Segment Routing*, este enviará el paquete a R3 a través de la mejor ruta posible que haya determinado el IGP.
- Cuando R1 recibe un paquete etiquetado con una pila de etiquetas (*stack of labels*) que identifiquen a los routers R4 y R3, se enviará el paquete hacia el router R3 a través de R4.
- Cuando el router R1 recibe un paquete etiquetado con una pila de etiquetas que identifican al router R2 y a un enlace con el *Adjacency Segment ID* 24014, enviará el paquete hacia el router R3 a través de R2 y luego por el enlace correspondiente a esa etiqueta. Cuando el paquete llega a R4, este debe reenviarle hacia R3 utilizando la ruta IGP más corta.

2.2.4.2. Plano de datos en Segment Routing

Segment Routing se puede aplicar directamente sobre una arquitectura MPLS sin cambios en el plano de reenvío, es decir, puede ser implementado utilizando tecnología y hardware MPLS existente. De hecho, existe interoperabilidad completa con MPLS LDP, en otras palabras, LDP y *Segment Routing* pueden coexistir, pero se preferirá LDP. Para preferir las etiquetas de *Segment Routing* sobre las de LDP se requiere utilizar la ejecutar el comando SR-prefer.

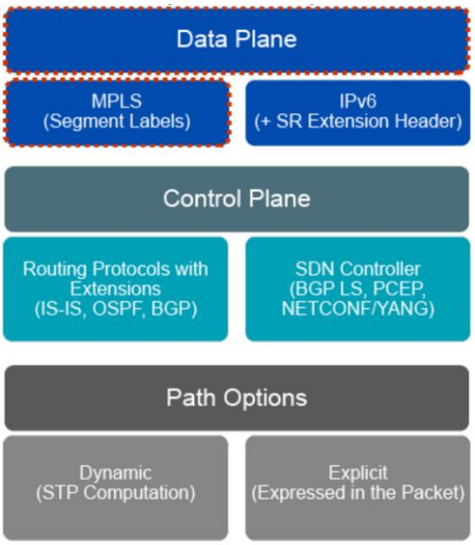


Figura 18. Plano de datos en SR
Fuente: (Cisco, 2023)

Un segmento es equivalente a una etiqueta, una lista de segmentos equivale a una pila de etiquetas, el segmento a procesar se encuentra en la parte superior de la pila y las funcionalidades PHP y Explicit-Null son soportadas.

Un router inserta una etiqueta de prefijo-SID en un paquete si:

- El destino mismo, o el siguiente salto en el que se resuelve el destino, hace coincidir un FEC con un Prefijo-SID
- El vecino de downstream está habilitado para SR
- El nodo está configurado para preferir la imposición de la etiqueta SR o el FEC
- No tiene una etiqueta LDP asociada

Con respecto a IPv6, *Segment Routing* (SRv6) utiliza el plano de datos IPv6 nativo, es decir, permite una implementación pura de IPv6 puesto que está basado en encabezados de extensión IPv6. Un segmento es una dirección IPv6 y una lista de segmentos equivale a una lista de direcciones IPv6.

2.2.4.3. Plano de control en Segment Routing

Segment Routing basa su funcionamiento en unas extensiones de los protocolos *Intermediate System-to-Intermediate System* (IS-IS), utiliza nuevos TLVs y *Open Shortest Path First* (OSPF) con la implementación de LSAs Opaque. Puede operar con un MPLS o un plano de datos IPv6, y se integra con las aplicaciones de MPLS como son VPN capa 3 (L3VPN), *Private Wire Service* (VPWS), *Virtual Private LAN Service* (VPLS), y Ethernet VPN (EVPN).

Existe menos carga para el plano de control puesto que no es necesario utilizar otros protocolos como LDP y RSVP, ya que, del intercambio y la configuración de etiquetas se encarga el mismo IGP.

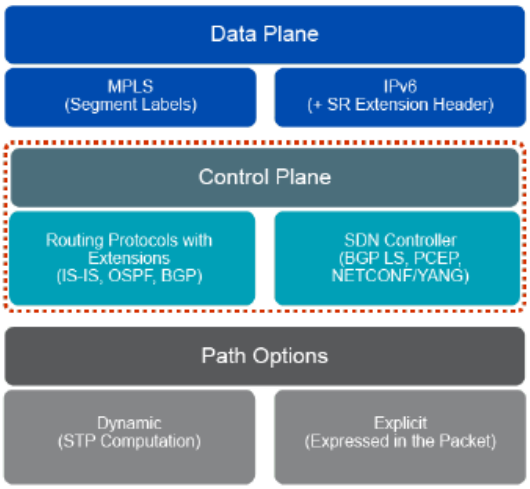


Figura 19. Plano de control en SR
Fuente: (Cisco, 2023)

Adicionalmente, brinda la posibilidad de utilizar un Controlador SDN, el cual facilita las tareas de:

- SR-TE multidominio
- BGP-LS
- PCEP

2.2.4.4. Segment Routing TE

Acorde a la información proporcionada en (Filsfils & Michielsen, 2017), SR-Traffic-Engineering proporciona una arquitectura simple, automatizada y escalable para controlar el flujo del tráfico dentro de una red para optimizar el consumo de los recursos, principalmente la utilización de los enlaces.

Además de la opción de configurar túneles de Ingeniería de Tráfico a través de interfaces Túnel de forma similar a la configuración en MPLS TE, *Segment Routing* brida la posibilidad de trabajar con Políticas (*Policies*).

SR Policy

Una *SR Policy* se identifica de forma única mediante una tupla que está conformada por una cabecera, un color y un punto final.
La cabecera hace referencia al nodo donde se implementará la Política de *Segment Routing*, el color es un valor numérico que permite diferenciar múltiples políticas entre los mismos nodos (origen y destino) y el punto final representa el destino de la política SR.

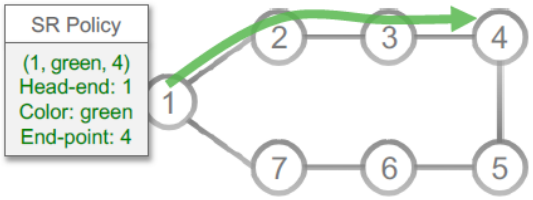


Figura 20. Política SR
Fuente: (Filsfils & Michielsen, 2017)

SR Policy Color

Cada Política SR tiene asociado un color para indicar un determinado tratamiento que se aplicará al paquete y únicamente puede existir con un color determinado para una política SR entre un par de nodos (origen y destino), es decir, la combinación de cabecera, color y punto final es única.

Por ejemplo, en la siguiente figura se puede apreciar que existen 2 políticas una "azul" que tiene como prioridad un costo bajo y otra "verde" que considera en cambio un delay bajo. El objetivo de la primera es direccionar el tráfico hacia 1.1.1.0/24 a través del Nodo 4 y con bajo costo (1, azul, 4), mientras que, la segunda busca direccionar el tráfico hacia 2.2.2.0/24 a través del Nodo4 con un delay bajo (1, verde, 4).

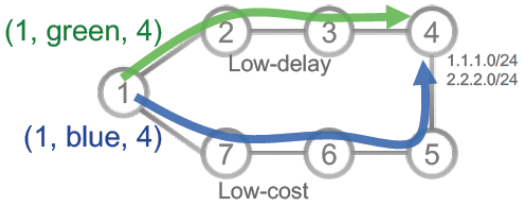


Figura 21. Política SR con color
Fuente: (Filsfils & Michielsen, 2017)

Al igual que en MPLS TE existen dos opciones para direccionar el tráfico, una de forma dinámica y la otra de forma estática.

Path dinámico

El *Head-end* calcula la mejor ruta optimizando los recursos como una lista de SID o un conjunto de listas de SID.

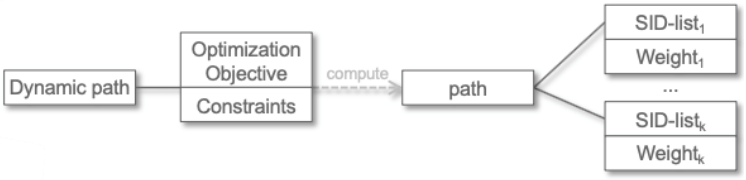


Figura 22. Path dinámico
Fuente: (Filsfils & Michielsen, 2017)

Cuando el *Head-end* no posee suficiente información topológica como, por ejemplo, un problema multidominio, puede delegar el cálculo a un PCE (*Path Computation Element*).

Cada vez que existe un cambio de la topología de la red, se vuelve a calcular la ruta.

Path estático

Una ruta explícita es una lista de SIDs o un conjunto de listas de SIDs que se especifican explícitamente.

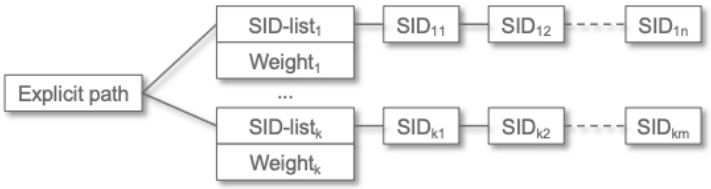


Figura 23. Path estático
Fuente: (Filsfils & Michielsen, 2017)

En el ejemplo de la siguiente figura, se enrutará el tráfico de manera explícita desde el router 1 hacia el router 4 a través del SID 16002, el adjacency SID 30203 y finalmente el SID 16004.

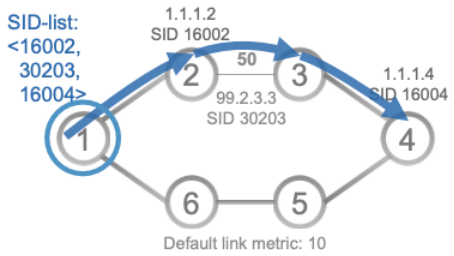


Figura 24. Policy – Path estático
Fuente: (Filsfils & Michielsen, 2017)

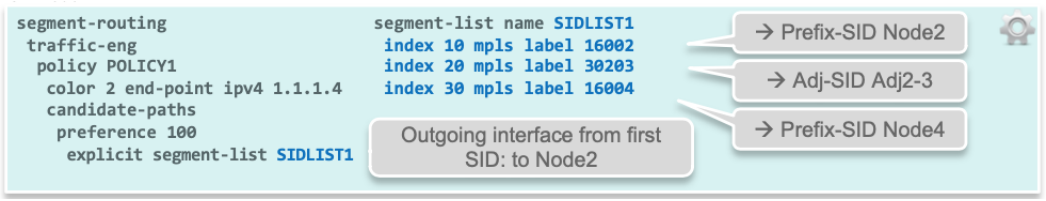


Figura 25. SR Policy – Configuración de política con path estático
Fuente: (Filsfils & Michielsen, 2017)

2.2.5. IS-IS Intermediate System to Intermediate System

Inicialmente, en redes pequeñas se utilizaba enrutamiento estático para habilitar la conectividad entre los equipos que las conforman, sin embargo, esta no era una solución escalable sobre todo en redes grandes como son las de los proveedores de servicio. Es así que surgen los protocolos de enrutamiento dinámico. Para el presente trabajo de titulación se ha optado por utilizar IS-IS (*Intermediate System to*

Intermediate System) por sus características, su simplicidad y robustes que brinda para una red de un proveedor de servicios. Adicionalmente, se han desarrollado extensiones que le permiten trabajar con *Segment Routing*.

En base a la información detallada en (Cisco, 2023), entre las principales características de este protocolo se tienen las siguientes:

- Es un protocolo de enrutamiento de estado de enlace.
- Es estable y escalable, con una convergencia muy rápida.
- Fue diseñado originalmente como el IGP para el servicio de red sin conexión (CLNS) parte del conjunto de protocolos OSI.
- El protocolo de Capa 3 del conjunto de protocolos OSI es el CLNP.
- Es flexible y ampliable para adaptarse a aplicaciones futuras.
- IS-IS admite una jerarquía de dos niveles para administrar y escalar el enrutamiento en redes grandes. Un área es un grupo de redes contiguas y hosts conectados que un administrador de red los especifica como parte de dicha área. Un router siempre está en una sola área y el límite entre áreas está en el enlace que conecta dos routers que se encuentran en zonas diferentes. Esta adyacencia es siempre de Nivel 2. Un dominio es un conjunto de áreas conectadas. Los dominios de enrutamiento brindan conectividad total a todos los sistemas finales dentro de ellos.
- El enrutamiento de Nivel 1 es un enrutamiento dentro de un área de Nivel 1, mientras que el enrutamiento de Nivel 2 es un enrutamiento entre áreas de Nivel 1.

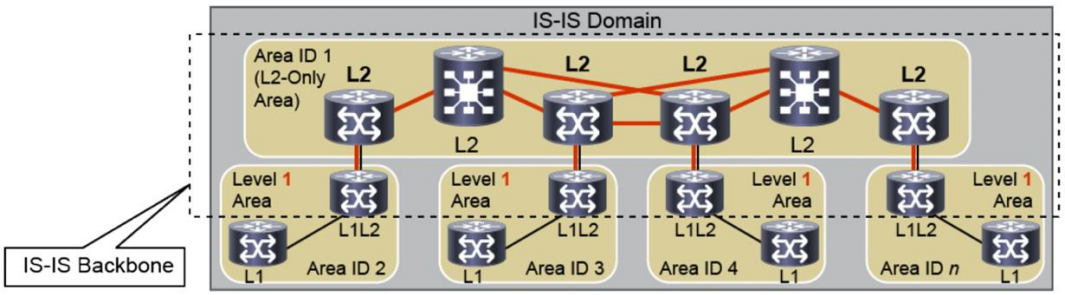


Figura 26. Jerarquía en IS-IS
Fuente: (Cisco, 2023)

- Los routers IS-IS establecen adyacencias mediante el uso Hellos e intercambian información del estado del enlace mediante el uso de paquetes de estado del enlace (*LSP Link State Packets*) en toda un área para construir la LSDB *Link State Data Base*. Luego, cada router ejecuta el algoritmo *Shortest Path First* (SPF) de Dijkstra contra su LSDB para elegir el mejor camino.
- Cada router contiene la información de topología únicamente para su propia área.
- IS-IS es parte de OSI y originalmente se usaba únicamente con CLNS; ampliado más adelante para su uso con IP. IS-IS todavía usa CLNS para mantener adyacencias y construir un árbol SPF.
- El IS-IS integrado también puede transportar información de enrutamiento IPv4 e IPv6.

- Existen 2 tipos de métricas: Amplia (*Wide)* y Angosta *(Narrow)*. La métrica amplia es el nuevo tipo de métrica y se utiliza para redes grandes de proveedores de servicios de alta velocidad, mientras que, la métrica angosta es antigua e insuficiente para redes grandes y otras funcionalidades como Ingeniería de Tráfico, etc.

- El costo del enlace por defecto es 10.

- Cada router se identifica mediante una dirección NSAP única. A diferencia de las direcciones IP, las direcciones CLNS se aplican a nodos completos y no a interfaces. Debido a que IS-IS se diseñó originalmente para CLNS, IS-IS requiere direcciones CLNS, incluso si el router solo se usa para enrutar IP. Las direcciones CLNS que utilizan los routers se denominan NSAP. Una parte de una dirección NSAP es el byte del selector NSAP (NSEL). Cuando se especifica un NSAP con un NSEL de 0, el NSAP se denomina NET.

  Existen varios formatos de direcciones NSAP.

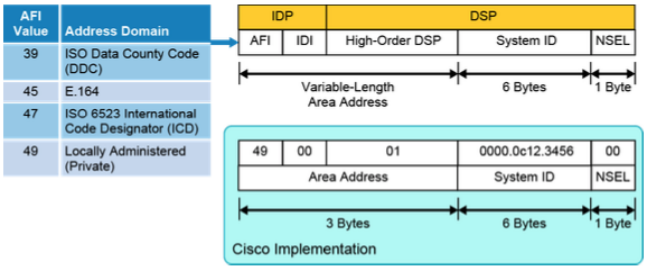


Figura 27. Formato de dirección NSAP
Fuente: (Cisco, 2023)

Donde:

- El byte AFI especifica el formato de la dirección y la autoridad asignada a esa dirección.

- El IDI identifica un subdominio bajo la AFI.

- La parte específica del dominio (DSP) contribuye al enrutamiento dentro de un dominio de enrutamiento IS-IS. El

- DSP comprende la parte específica del dominio de alto orden (HO-DSP), el ID del sistema y el NSEL:

  - El HO-DSP subdivide el dominio en áreas. El HO-DSP es aproximadamente el equivalente OSI de una subred en IP.

  - La ID del sistema identifica un dispositivo OSI individual. En OSI, un dispositivo tiene una dirección, tal como ocurre en DECnet, mientras que, en IP cada interfaz tiene una dirección.

  - El NSEL identifica un proceso en el dispositivo y corresponde aproximadamente a un puerto o socket en IP. El NSEL no se utiliza en las decisiones de enrutamiento.

El formato NSAP más simple, utilizado por la mayoría de las empresas que ejecutan IS-IS como IGP, comprende lo siguiente:

- Dirección de área: Debe tener al menos 1 byte, separada en dos partes:

  - El AFI, fijado en 49, lo que significa que el AFI se administra localmente y; por lo

tanto, la empresa puede asignar direcciones individuales

- El identificador de área (ID); los octetos de la dirección de área que siguen al AFI.

- ID del sistema: Los routers Cisco que cumplen con los estándares del perfil de interconexión de sistemas abiertos (GOSIP) versión 2.0 del gobierno de EE. UU. requieren una identificación del sistema de 6 bytes.

- NSEL: NSEL siempre debe establecerse en 0 para un router.

Como se indicó en el numeral anterior (2.2.4), *Segment Routing* basa su funcionamiento en nuevas extensiones para el protocolo IS-IS, es decir, se definen nuevos TLVs.

El primero, se denomina sub-TLV del *Prefix Segment Identifier* (Prefix-SID) y transporta el IGP-Prefix-SID de *Segment Routing*.

El segundo, es el sub-TLV para el *Adjacency Segment ID* (Adj-SID). Es un sub-TLV opcional que transporta el IGP-Adjacency-SID de *Segment Routing.*

El tercero corresponde al sub-TLV SID/Label que contiene un SID o una etiqueta MPLS.

Para utilizar *Segment Routing* con IS-IS es necesario utilizar la métrica extendida (*metric-style wide*).

2.2.6. BGP Border Gateway Protocol

De acuerdo con la información proporcionada en (Edgeworth et al., 2015), el RFC 4271 define el protocolo BGP *(Border Gateway Protocol)*, como un protocolo de enrutamiento *path vector* que proporciona escalabilidad, flexibilidad y sobretodo estabilidad a la red. BGP es el único protocolo utilizado para intercambiar redes en Internet, y priorizó la estabilidad puesto que, por el gran tamaño de las tablas BGP, de presentarse una falla en un enlace podría resultar en un recálculo de miles de rutas.

BGP está diseñado para el intercambio de información entre diferentes sistemas autónomos AS *Automonous System*, los cuales se identifican mediante un número de AS único. Desde la perspectiva de BGP, un sistema autónomo es una colección de routers bajo un mismo control de la organización, que utilizan uno o más IGPs para enrutar paquetes dentro del sistema autónomo.

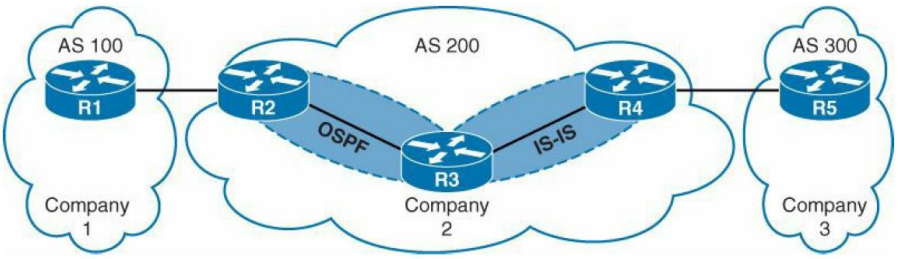


Figura 28. Sistemas Autónomos
Fuente: (Edgeworth et al., 2015)

Los números de sistema autónomo eran originalmente de 2 bytes (16 bits) que proporcionaba 65.535 ASN, pero por su agotamiento se amplió a 4 bytes (32 bits), esto permitió ampliar el rango a 4.294.967.295 ASN únicos.

Existen dos bloques de ASN privados disponibles para uso de cualquier organización, los cuales no pueden ser intercambiados públicamente en Internet. Los ASN 64.512 a 65.534 son ASN privados dentro del sistema de 16 bits y del 4.200.000.000 al 4.294.967.294 son ASN privados dentro del rango extendido de 32 bits. Los ASN privados son similares al espacio de direcciones IPv4 del RFC 1918 y se utilizan exclusivamente para enrutamiento privado.

La IANA (*Internet Assigned Numbers Authority)* es la autoridad responsable de asignar todos los ASN públicos con el objetivo de asegurar que sean globalmente únicos.

Sesiones BGP

Una sesión BGP se refiere a la adyacencia que se establece entre dos routers BGP. Las sesiones BGP siempre son punto a punto (P2P) y pueden ser de dos tipos:

- iBGP - *Internal BGP*: Son sesiones establecidas con entre routers BGP que se encuentran dentro del mismo sistema autónomo o que participa en la misma confederación BGP. Se considera que las sesiones iBGP son más seguras, por lo que, algunas de las medidas de seguridad de BGP se reducen en comparación con las sesiones eBGP. A los prefijos iBGP se les asigna una distancia administrativa (AD) de 200 al instalarlos en la tabla RIB del router.

- eBGP - *External BGP*: Se refiere a sesiones establecidas entre routers BGP que se encuentran en sistemas autónomos diferentes. A los prefijos eBGP se les asigna una distancia administrativa (AD) de 20 al instalarlos en la tabla RIB del router.

2.2.7. Route Reflectors

BGP tiene la limitante de anunciar un prefijo aprendido de un par iBGP hacia otro par iBGP como mecanismo de prevención de lazos. Esto puede desencadenar en problemas de escalabilidad dentro de la red del Proveedor de Servicios, puesto que para que exista una conectividad completa, sería necesario que se habiliten sesiones BGP entre todos y cada uno de los routers parte del AS, es decir, se requiere habilitar sesiones *Full-Mesh.*

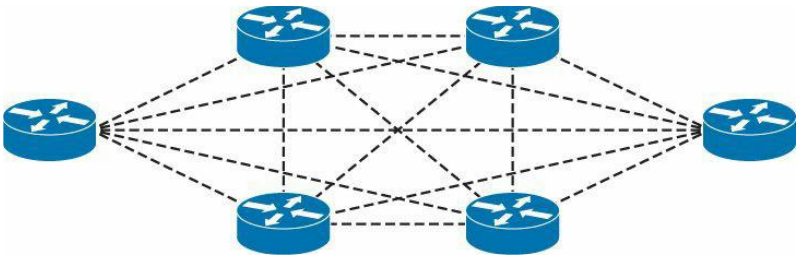


Figura 29. Sesiones Full-Mesh de iBGP
Fuente: (Edgeworth et al., 2015)

La fórmula n(n-1)/2 permite calcular el número de sesiones requeridas para tener un Full Mesh entre todos los equipos integrantes de la red, donde n representa el número de routers existentes, por ende, se tendría un crecimiento exponencial a medida que aumente la cantidad de equipos en la red.

Como solución a este inconveniente, en el RFC 1966 se introdujo el concepto de *Route Reflectors* RR, que permite que un router iBGP refleje rutas a otro equipo iBGP, donde el router que refleja rutas se conoce como *Route Reflector* y el router que recibe las rutas reflejadas es un *Route Reflector Client*.

Existen 3 reglas básicas que rigen el comportamiento de los *RR*:

1. Si un *RR* recibe una ruta de un equipo que no es *RR client*, el *RR* anunciará la ruta a un *RR client*, pero no anunciará la ruta a los routers que no sea *RR client.*

2. Si un *RR* recibe una ruta de un *RR client*, anunciará la ruta a los *RR clients* y a los no *RR clients*. Incluso el *RR client* que envió el anuncio recibirá una copia de la ruta, pero la descartará porque se ve a sí mismo como el creador de la ruta.

3. Si un *RR* recibe una ruta de un par eBGP, anunciará la ruta a los *RR clients* y a los no *RR clients.*

CAPÍTULO III: METODOLOGÍA

3.1. Tipo de Investigación

En este trabajo de titulación se realizará la emulación de la red de un proveedor de servicios ISP (*Internet Service Provider*), a través de un emulador de infraestructura de red. Se utilizará IS-IS (*Intermediate System-to-Intermediate System*) como IGP (*Interior Gateway Protocol*) y MPLS (*MultiProtocol Label Switching*) para el transporte de datos. Se implementarán 2 topologías, una utilizando LDP (*Label Distribution Protocol*) como protocolo de señalización y otra utilizando *segment routing* como mejora a la tecnología para realizar enrutamiento. Se analizará paso a paso la configuración requerida para implementar cada una de las topologías con el objetivo de comparar su rendimiento en base al problema planteado. Finalmente, se realizará un análisis de los resultados obtenidos para cada uno de los casos, para dar un resultado en base a las pruebas propuestas respecto a la implementación LDP y *segment routing* sobre la red de transporte MPLS de un Proveedor de Servicios.

La metodología utilizada en el presente capítulo será experimental, ya que se implementarán las topologías partiendo desde cero y se definirán diferentes aspectos a ser considerados tales como cantidad de equipos, roles que tendrán cada uno de ellos dentro de la red, conexiones físicas, requerimientos lógicos, protocolos de ruteo, entre otros. Se emularán cada uno de los escenarios propuestos con el objetivo de obtener datos del comportamiento de la red, para realizar el análisis comparativo que permita determinar si efectivamente *Segment Routing* tiene un mejor desempeño con respecto a LDP.

3.2. EVE-NG (Emulated Virtual Enviroment – Next Generation)

Para implementar las 2 topologías planteadas se utilizará el emulador de red EVE-NG (*Emulated Virtual Enviroment – Next Generation*). Esta herramienta permite emular infraestructuras de redes de TI, realizar pruebas de concepto, simular topologías utilizando sistemas operativos multiproveedor como son Cisco, Juniper, CheckPoint, entre otros.

Figura 30. Emulador de infraestructura de red EVE-NG
Fuente: (EVE-NG, 2023)

En su portal web, se puede encontrar documentación respecto a temas relacionados al mundo del networking. Su uso brinda grandes ventajas entre las cuales se pueden destacar:

- Aprendizaje, puesto que permite implementar laboratorios haciendo uso de sistemas operativos de varias marcas.

- Diseño, ya que brinda la posibilidad de construir redes de acuerdo con diferentes requerimientos y validar su correcto desempeño.

- Eficiencia, porque se trabaja en un ambiente seguro, sin el riesgo de manipular equipos de una red real.

- Flexibilidad, puesto que es posible una interacción multivendor.

Adicionalmente, dentro de sus principales características se pueden indicar las siguientes:

- Diseñador de topología
- Importación / exportación de configuraciones
- Formato de archivos de laboratorio xml
- Importación de imágenes y mapas
- Soporte de kernel personalizado para protocolos L2
- Optimización de memoria (UKSM)
- Watchdog de la CPU
- Interfaz completa de usuario HTML5
- Capacidad de uso sin herramientas adicionales
- Multiusuarios
- Interacción con una red real
- Instancias de laboratorio simultáneas
- Derivado del servidor Ubuntu LTS 20.04 para soporte a largo plazo. (EVE-NG, 2023)

EVE-NG puede ser instalada a través de una VM (*Virtual Machine*) en un servidor, un computador personal o en el Cloud. En el presente trabajo de titulación se utilizará Google Cloud por los beneficios que brinda en cuanto a recursos si se compara a una PC, ya que los requerimientos de CPU y memoria dependiendo de los modelos de equipos con los que se desea trabajar pueden ser bastante exigentes.

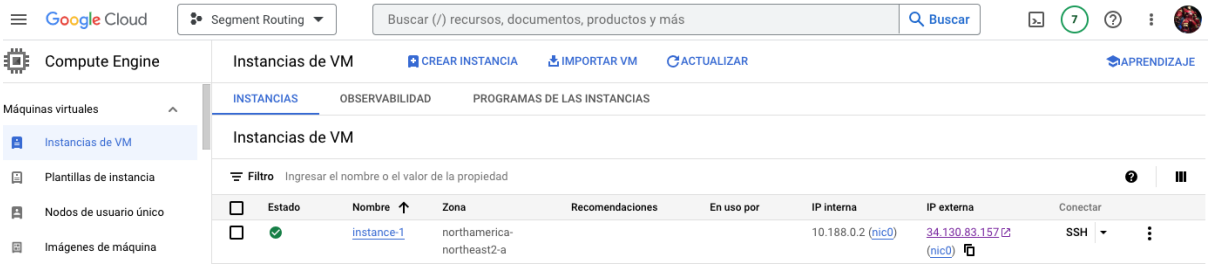


Figura 31. Instancia (EVE-NG) creada en Google Cloud
Fuente: Autor

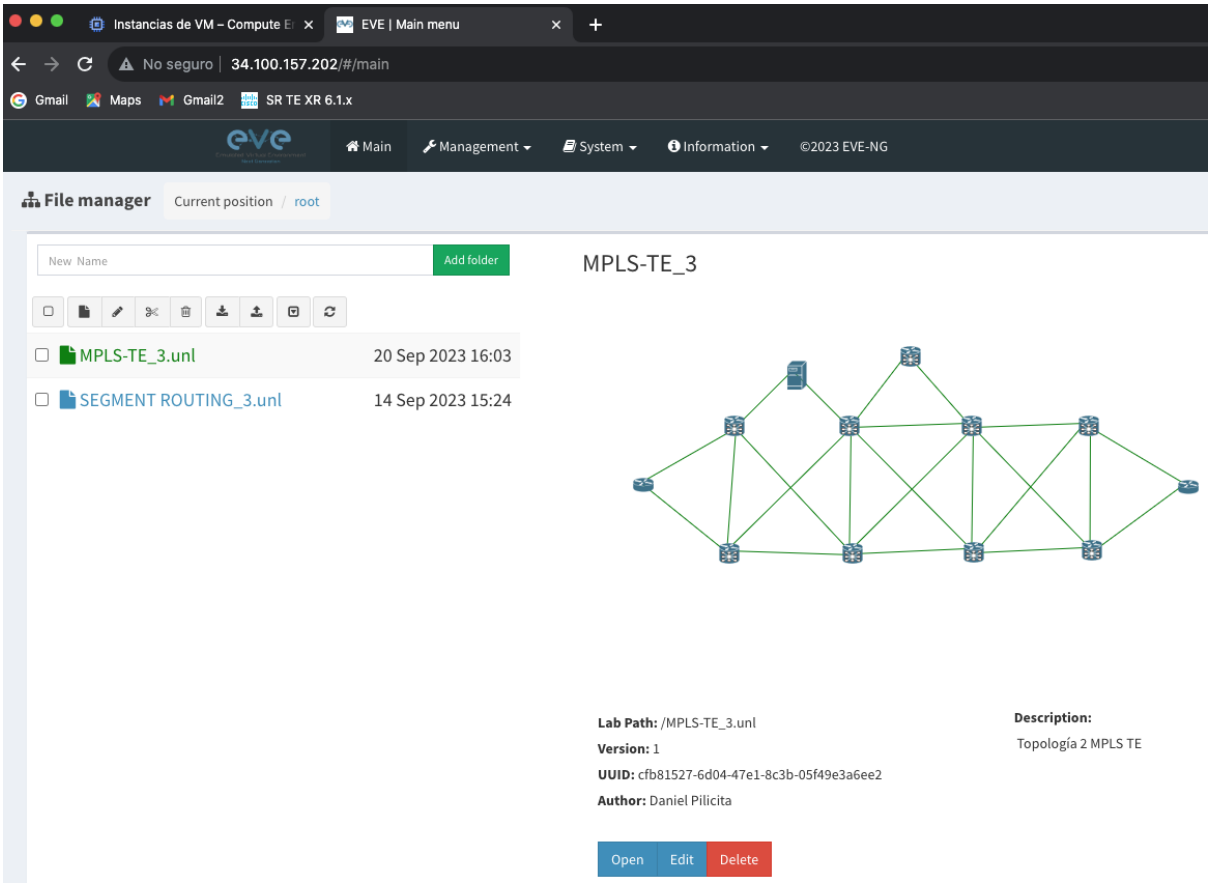


Figura 32. Pantalla principal de EVE-NG
Fuente: Autor

En el Anexo 1 se detalla la instalación de EVE-NG en Google Cloud, así como la carga de las imágenes de los sistemas operativos de los equipos a utilizar en la emulación.

En el presente trabajo de titulación se utilizarán imágenes de equipos routers marca Cisco, de los siguientes modelos:

- Equipos del proveedor de servicios:

  Para la red del ISP se utilizarán routers Cisco de la familia ASR9000 cuyo sistema operativo es XR con la versión de release es la 6.1.3.

Qemu folder name EVE	Vendor	Qemu image .qcow2 name
xrv-	XRv Cisco Router	hda

Tabla 4. Imagen de Router Cisco XRv
Fuente: (EVE-NG, 2023)

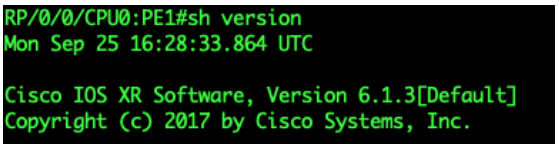


Figura 33. Router Cisco XRv
Fuente: Autor

- Equipos del cliente:

  Como equipos del cliente se utilizarán routers Cisco con sistema operativo IOSv Software

(VIOS-ADVENTERPRISEK9-M), Version 15.6(2)T.

Qemu folder name EVE	Vendor	Qemu image .qcow2 name
vios-	L3 vIOS Cisco Router	virtioa

Tabla 5. Imagen de Router Cisco vIOS
Fuente: (EVE-NG, 2023)

Figura 34. Router Cisco IOSv
Fuente: Autor

3.3. Variables e indicadores

Variable Independiente:

Diseño de una red IP MPLS para un proveedor de servicios.

Variable Dependiente:

Rendimiento de la red IP MPLS con LDP y Segment Routing.

Indicadores:

- Capacidad de Traffic Engineering
- Latencia
- Jitter

3.4. Operacionalización de variables

En base a las variables definidas se puede realizar el sigueinte análisis:

VARIABLES	TIPO	CONCEPTO	INDICADORES
Diseño de una red IP MPLS para un proveedor de servicios	Variable Independiente	Arquitectura física y lógica de la red transporte IP MPLS de un proveedor de servicios. Los aspectos por considerar entre otros son: seguridad, escalabilidad, redundancia y disponibilidad	1. Capacidad de TE 2. Latencia 3. Jitter
Rendimiento de la red IP MPLS: LDP vs Segment Routing	Variable Dependiente	El rendimiento de una red está directamente relacionado con la fiabilidad y consistencia de cada uno de los servicios provistos a través de esta.	

Tabla 6. Operacionalización de variables
Fuente: Autor

3.5. Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	¿Cómo el análisis comparativo entre una red IP MPLS con LDP y una red IP MPLS utilizando Segment Routing permite determinar que Segment Routing brinda un mejor rendimiento en este tipo de redes?
OBJETIVO GENERAL	Elaborar un análisis comparativo entre una red IPv4 MPLS LDP y una red IP MPLS utilizando Segment Routing para un proveedor de servicios de telecomunicaciones mediante un emulador de infraestructura de red para determinar que Segment Routing tiene un mejor rendimiento.

HIPÓTESIS GENERAL	El Diseño de una red IP MPLS utilizando Segment Routing para un proveedor de servicios mejorará el rendimiento de la red en comparación a utilizar LDP
VARIABLES	- Diseño de una red IP MPLS para un proveedor de servicios - MPLS: LDP vs Segment Routing
INDICADORES	- Capacidad de Traffic Engineering - Latencia - Jitter
METODOLOGÍA	- Se realizará un estudio descriptivo que permitirá definir la topología a utilizar, los modelos de equipos, un emulador de redes, imágenes de sistemas operativos de los equipos. - Se emularán las 2 topologías, una con MPLS LDP y otra con MPLS utilizando Segment Routing a través de un emulador de infraestructura de red. Se configurarán cada uno de los equipos, se probará que exista comunicación entre ellos y se realizarán las pruebas correspondientes para obtener los resultados. - Se realizará un análisis comparativo de los resultados obtenidos en los 2 casos de modo que se pueda definir que tecnología brinda un mejor rendimiento
TÉCNICAS	- Observaciones - Cálculos estadísticos
INSTRUMENTOS	- Emulador de infraestructura de red - Software de análisis de datos en una red

Tabla 7. Matriz de consistencia
Fuente: Autor

3.6. Diseño de la red IP MPLS de un Proveedor de Servicios

Para diseñar una red de un Proveedor de Servicios es de suma importancia tener en consideración varios parámetros como son la seguridad, la escalabilidad, redundancia y la disponibilidad con el objetivo de garantizar la continuidad de los servicios ofertados. Es necesario también contar con equipamiento actualizado que cumpla con los estándares de la industria. Disponer de equipos de última tecnología permite contar con soporte por parte del fabricante en casos de presentarse bugs o fallas en dichos equipos.

Se requiere elaborar una ingeniería de detalle en la que se incluyan todos los aspectos a considerar para la implementación y el despliegue de la red. Toda esta información debe ser documentada con el objetivo de facilitar la habilitación de nuevos servicios, integración de plataformas, la resolución de problemas por parte del personal de Operación y Mantenimiento, además de mantener abierta la posibilidad de crecimiento y expansión de la red.

3.6.1. Topología de la red IP MPLS del Proveedor de Servicios

Aspectos importantes a considerar para implementar la topología de un Proveedor de Servicios son la cantidad de equipos, modelos, el rol que tendrán dentro de la red, las localidades principales que concentren gran cantidad de tráfico, la escalabilidad, la segmentación, el flujo del tráfico, entre otros.

En base a los aspectos antes mencionados, para efectos de la emulación, la red se segmentará en 2 capas: Core y Agregación.

La capa de core estará conformada por 4 equipos P (*Provider*), los cuales cumplen el rol de LSR (*Label Switch Router*) y son responsables de insertar, extraer e intercambiar las etiquetas según el enrutamiento en la red MPLS.

La capa de agregación dispondrá de 4 equipos PE (*Provider Edge*), 2 en cada extremo de la red, los cuales como su nombre lo indica se encuentran en los límites de la red MPLS. En función del flujo de tráfico pueden ser: *Ingress label switch router*, LSR de entrada, es el primer equipo en insertar un encabezado y una etiqueta MPLS en un paquete; o *Egress label switch router*, LSR de salida, que es el último punto antes de salir de la red, por lo tanto, elimina todas las etiquetas y encabezados MPLS.

Adicionalmente, se utilizará un equipo *Route Reflector* que se encargará de emular un establecimiento full-mesh entre todos los equipos de la red MPLS facilitando así la operación y transporte de los servicios a nivel de MPLS VPNs.

Finalmente, todos los equipos tendrán habilitados enlaces redundantes hacia sus equipos vecinos.

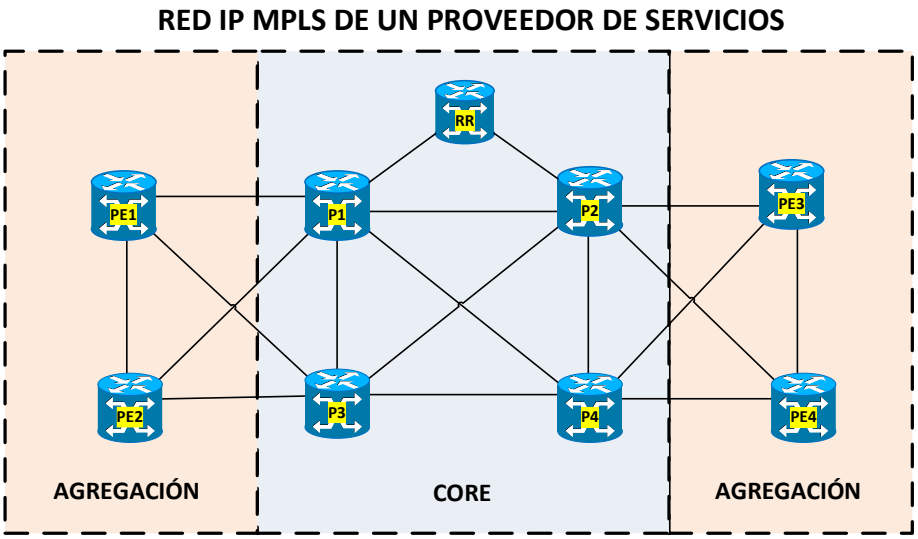


Figura 35. Topología de un Proveedor de Servicios
Fuente: Autor

3.6.2. Direccionamiento

En base a la topología considerada en el numeral anterior, se ha planificado el siguiente direccionamiento para cada uno de los equipos de la red a emular teniendo en cuenta las siguientes consideraciones:

- Cada equipo debe tener un direccionamiento para ser administrado y debe ser configurado preferentemente en un interfaz que permanezca activa incluso si se llegarán a presentar problemas físicos, por ende, se configura generalmente en una interfaz Loopback. El direccionamiento asignado a este tipo de interfaces tiene una máscara 32.
  Es de suma importancia que no exista duplicidad de este direccionamiento para evitar conflictos entre los equipos y por ende fallas en la operación de la red.

- Para habilitar cada uno de los enlaces de la Figura 35 y las conexiones hacia los equipos del cliente, se deben considerar los recursos físicos a nivel de interfaces que posee cada uno de los equipos que conforman la red. A cada interfaz se asignará una subred con máscara 30 para habilitar los enlaces WAN correspondientes.

HOSTNAME	INTERFAZ	DIRECCIONAMIENTO	SISTEMA AUTÓNOMO
P1	Lo0	10.0.0.1/32	64512
	Gi0/0/0/0	10.1.2.1/30	
	Gi0/0/0/1	10.1.4.1/30	
	Gi0/0/0/2	10.1.3.1/30	
	Gi0/0/0/3	10.1.12.1/30	
	Gi0/0/0/4	10.1.11.1/30	
	Gi0/0/0/5	10.1.99.1/30	
	NET	49.0000.0100.0000.0001.00	

	Node ID (SR)	16001	
P2	Lo0	10.0.0.2/32	
	Gi0/0/0/0	10.1.2.2/30	
	Gi0/0/0/1	10.2.3.1/30	
	Gi0/0/0/2	10.2.4.1/30	
	Gi0/0/0/3	10.2.14.1/30	
	Gi0/0/0/4	10.2.13.1/30	
	Gi0/0/0/5	10.2.99.1/30	
	NET	49.0000.0100.0000.0002.00	
	Node ID (SR)	16002	
P3	Lo0	10.0.0.3/32	
	Gi0/0/0/0	10.3.4.1/30	
	Gi0/0/0/1	10.2.3.2/30	
	Gi0/0/0/2	10.1.3.2/30	
	Gi0/0/0/3	10.3.11.1/30	
	Gi0/0/0/4	10.3.12.1/30	
	NET	49.0000.0100.0000.0003.00	
	Node ID (SR)	16003	
P4	Lo0	10.0.0.4/32	
	Gi0/0/0/0	10.3.4.2/30	
	Gi0/0/0/1	10.1.4.2/30	
	Gi0/0/0/2	10.2.4.2/30	
	Gi0/0/0/3	10.4.13.1/30	
	Gi0/0/0/4	10.4.14.1/30	
	NET	49.0000.0100.0000.0004.00	
	Node ID (SR)	16004	
PE1	Lo0	10.0.0.11/32	
	Gi0/0/0/1	10.11.10.1/30	
	Gi0/0/0/2	10.11.12.1/30	
	Gi0/0/0/3	10.3.11.2/30	
	Gi0/0/0/4	10.1.11.2/30	
	NET	49.0001.0100.0000.0011.00	
	Node ID (SR)	16011	
PE2	Lo0	10.0.0.12/32	
	Gi0/0/0/1	10.12.10.1/30	
	Gi0/0/0/2	10.11.12.2/30	
	Gi0/0/0/3	10.1.12.2/30	
	Gi0/0/0/4	10.3.12.2/30	
	NET	49.0001.0100.0000.0012.00	
	Node ID (SR)	16012	
PE3	Lo0	10.0.0.13/32	
	Gi0/0/0/1	10.13.10.1/30	

	Gi0/0/0/2	10.13.14.1/30	
	Gi0/0/0/3	10.4.13.2/30	
	Gi0/0/0/4	10.2.13.2/30	
	NET	49.0002.0100.0000.0013.00	
	Node ID (SR)	16013	
PE4	Lo0	10.0.0.14/32	
	Gi0/0/0/1	10.14.10.1/30	
	Gi0/0/0/2	10.13.14.2/30	
	Gi0/0/0/3	10.2.14.2/30	
	Gi0/0/0/4	10.4.14.2/30	
	NET	49.0002.0100.0000.0014.00	
	Node ID (SR)	16014	
CE1	Lo0	1.1.1.1/32	64513
	Gi0/1	10.11.10.2/30	
	Gi0/2	10.12.10.2/30	
CE2	Lo0	2.2.2.2/32	64514
	Gi0/1	10.13.10.2/30	
	Gi0/2	10.14.10.2/30	

Tabla 8. Direccionamiento
Fuente: Autor

3.6.3. IGP Interior Gateway Protocol

Como protocolo de enrutamiento dentro de la red del Proveedor de Servicios, se ha optado por utilizar IS-IS (*Intermediate System to Intermediate System*), ya que, por sus características, simplicidad y robustez es una opción ampliamente utilizada dentro de los ISPs. Además, de que se han desarrollado extensiones al mismo que le permiten trabajar con *Segment Routing*.

Dado que en la topología existen varias áreas se configurarán todos los enlaces como L2.

En base a la información detallada en el numeral 2.2.5 del presente trabajo, se desarrollará la dirección NET para el router PE1: 49.0001.0100.0000.0011.00 como ejemplo explicativo:

- Lo0 PE1: 10.0.0.11/32
- AFI: 49
- Área ID: 0001
- ID del sistema: se obtiene a partir de la dirección Lo0: 10.0.0.11 y debe ser de 6 bytes.

  010.000.000.011

  0100 0000 0011
  0100.0000.0011
- NSEL: 00

Por lo tanto, el NET para PE1 es: 49.0001.0100.0000.0011.00

Configuración de *Segment Routing* en IS-IS:

Configuración de *Segment Routing* en IS-IS
router isis MTI is-type level-2-only net 49.0001.0100.0000.0011.00 log adjacency changes address-family ipv4 unicast metric-style wide mpls traffic-eng level-2-only mpls traffic-eng router-id Loopback0 router-id Loopback0 segment-routing mpls ! interface Loopback0 passive address-family ipv4 unicast prefix-sid absolute 16011 ! ! interface GigabitEthernet0/0/0/1 circuit-type level-2-only address-family ipv4 unicast ! ! interface GigabitEthernet0/0/0/2 circuit-type level-2-only address-family ipv4 unicast ! ! interface GigabitEthernet0/0/0/3 circuit-type level-2-only address-family ipv4 unicast ! ! interface GigabitEthernet0/0/0/4 circuit-type level-2-only address-family ipv4 unicast ! ! interface GigabitEthernet0/0/0/5 circuit-type level-2-only address-family ipv4 unicast !

```
!
!
```

Tabla 9. Configuración de *Segment Routing* en IS-IS
Fuente: Autor

Verificación de vecinos IS-IS

```
RP/0/0/CPU0:PE1#sh isis neighbors
Sat Nov 18 13:12:40.766 UTC

IS-IS MTI neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
P1             Gi0/0/0/4        5000.0001.0005 Up    24       L2   Capable
P3             Gi0/0/0/3        5000.0003.0004 Up    27       L2   Capable
PE2            Gi0/0/0/2        5000.0006.0003 Up    7        L2   Capable
```

Figura 36. Verificación de vecinos IS-IS
Fuente: Autor

Verificación de *Segment Routing* en ISIS

```
RP/0/0/CPU0:PE1#sh isis database level 2 verbose PE3.00
Wed Nov 29 02:25:38.628 UTC

IS-IS MTI (Level-2) Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
PE3.00-00             0x00000007   0x1f50        1122            0/0/0
  Area Address:   49.0002
  NLPID:          0xcc
  Hostname:       PE3
  IP Address:     10.0.0.13
  Router ID:      10.0.0.13
  Router Cap:     10.0.0.13, D:0, S:0
    Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
  Metric: 10         IS-Extended PE3.05
    Affinity: 0x00000000
    Interface IP Address: 10.4.13.2
    Neighbor IP Address: 10.4.13.2
    Physical BW: 1000000 kbits/sec
    Reservable Global pool BW: 0 kbits/sec
    Global Pool BW Unreserved:
      [0]: 0        kbits/sec          [1]: 0        kbits/sec
      [2]: 0        kbits/sec          [3]: 0        kbits/sec
      [4]: 0        kbits/sec          [5]: 0        kbits/sec
      [6]: 0        kbits/sec          [7]: 0        kbits/sec
    Admin. Weight: 10
    Ext Admin Group: Length: 32
      0x00000000    0x00000000
      0x00000000    0x00000000
      0x00000000    0x00000000
      0x00000000    0x00000000
    LAN-ADJ-SID: F:0 B:1 V:1 L:1 S:0 weight:0 Adjacency-sid: 24002 System ID:P4
    LAN-ADJ-SID: F:0 B:0 V:1 L:1 S:0 weight:0 Adjacency-sid: 24003 System ID:P4
```

Figura 37. Verificación de *Segment Routing* en ISIS
Fuente: Autor

3.6.4. Conectividad con el cliente - BGP

Para la conectividad entre la red MPLS del Proveedor de Servicios y el cliente se utilizó BGP (*Border Gateway Protocol*). Como se había indicado previamente, BGP está diseñado para el intercambio de información entre sistemas autónomos diferentes y cada uno se identifica a través de un número de AS único, los cuales son asignados por la IANA. Para efectos de la emulación, se ha asignado el AS 64512 para la red del Proveedor de Servicios, mientras que los sitios de los clientes se utilizarán los ASs 64513 y 64514.

Configuración de sesiones BGP:

Configuración de sesión BGP en PE1
router bgp 64512 address-family ipv4 unicast network 10.0.0.11/32 ! neighbor 10.0.0.99 remote-as 64512 update-source Loopback0 address-family ipv4 unicast ! ! neighbor 10.11.10.2 remote-as 64513 address-family ipv4 unicast route-policy RPL_PASS_BGP in route-policy RPL_PASS_BGP out ! ! !

Tabla 10. Configuración de sesión BGP en PE1
Fuente: Autor

Configuración de sesión BGP en CE1
router bgp 64513 bgp log-neighbor-changes network 1.1.1.1 mask 255.255.255.255 neighbor 10.11.10.1 remote-as 64512 neighbor 10.12.10.1 remote-as 64512 !

Tabla 11. Configuración de sesión BGP en CE1
Fuente: Autor

3.6.5. Sesiones iBGP - Route Reflector

Con el objetivo de solventar la limitante de BGP al momento de anunciar un prefijo aprendido entre pares iBGP como mecanismo de prevención de lazos, y que por ende, requiere que todos los elementos establezcan sesiones entre sí, se ha optado por utilizar un Route-Reflector. Todos los routers de la red del Proveedor de Servicios (clientes) establecerán conexiones iBGP con el RR y éste reflejará las rutas hacia los todos clientes simulando una conexión *full-mesh,* por lo tanto, ya no es necesario establecer conexiones iBGP entre todos los equipos de la red.

Configuración de sesiones iBGP entre el RR y los Equipos de la red MPLS
router bgp 64512 address-family ipv4 unicast network 10.0.0.99/32 ! neighbor 10.0.0.1 remote-as 64512 update-source Loopback0 address-family ipv4 unicast route-reflector-client ! ! neighbor 10.0.0.2 remote-as 64512 update-source Loopback0 address-family ipv4 unicast route-reflector-client ! ! neighbor 10.0.0.3 remote-as 64512 update-source Loopback0 address-family ipv4 unicast route-reflector-client ! ! …

Tabla 12. Configuración de sesiones iBGP entre el RR y los Equipos de la red MPLS
Fuente: Autor

3.6.6. Topología 1 – Red IP MPLS con LDP

Además de las consideraciones indicadas en secciones previas de este documento, en este escenario se implementará una red IP MPLS para un Proveedor de Servicios utilizando LDP como protocolo de asignación y distribución de etiquetas.

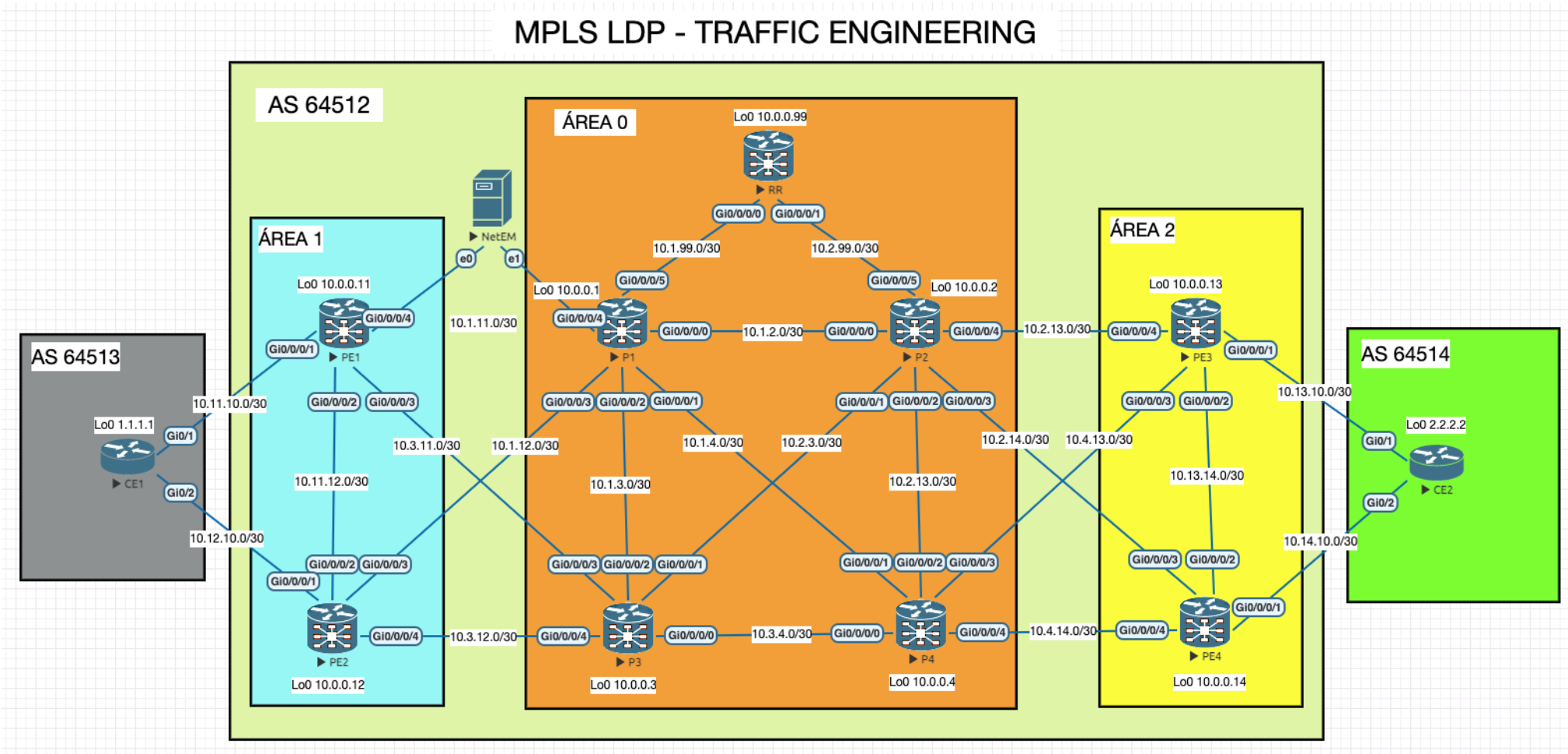


Figura 38. Escenario 1 - Red IP MPLS con LDP de un Proveedor de Servicios
Fuente: Autor

Configuración general de MPLS con LDP y RSVP para TE:

Configuración general de MPLS + LDP y RSVP para TE
interface Loopback0 ipv4 address 10.0.0.11 255.255.255.255 ! mpls ldp router-id 10.0.0.11 interface GigabitEthernet0/0/0/1 ! interface GigabitEthernet0/0/0/2 ! interface GigabitEthernet0/0/0/3 ! interface GigabitEthernet0/0/0/4 ! ! mpls label range table 0 24000 24999 end ! rsvp interface GigabitEthernet0/0/0/1 bandwidth 800000 ! interface GigabitEthernet0/0/0/2 bandwidth 800000 ! interface GigabitEthernet0/0/0/3 bandwidth 800000 ! interface GigabitEthernet0/0/0/4 bandwidth 800000 ! ! mpls traffic-eng interface GigabitEthernet0/0/0/1 ! interface GigabitEthernet0/0/0/2 ! interface GigabitEthernet0/0/0/3 ! interface GigabitEthernet0/0/0/4 ! ! explicit-path name PE1_P1_P2_PE3 index 1 next-address strict ipv4 unicast 10.1.11.2

```
 index 2 next-address strict ipv4 unicast 10.1.2.2
 index 3 next-address strict ipv4 unicast 10.2.13.2
!
interface tunnel-te1213
 ipv4 unnumbered Loopback0
 destination 10.0.0.13
 record-route
 path-option 30 explicit name PE1_P1_P2_PE3
 path-option 40 dynamic
!
```

Tabla 13. Configuración general de MPLS + LDP y RSVP para TE
Fuente: Autor

Verificación de parámetros MPLS:

```
RP/0/0/CPU0:PE1#sh mpls ldp parameters
Fri Sep 29 04:50:12.586 UTC

LDP Parameters:
  Role: Active
  Protocol Version: 1
  Router ID: 10.0.0.11
  Null Label:
    IPv4: Implicit
  Session:
    Hold time: 180 sec
    Keepalive interval: 60 sec
    Backoff: Initial:15 sec, Maximum:120 sec
    Global MD5 password: Disabled
  Discovery:
    Link Hellos:     Holdtime:15 sec, Interval:5 sec
    Targeted Hellos: Holdtime:90 sec, Interval:10 sec
    Quick-start: Enabled (by default)
    Transport address:
      IPv4: 10.0.0.11
  Graceful Restart:
    Disabled
  NSR: Disabled, Not Sync-ed
  Timeouts:
    Housekeeping periodic timer: 10 sec
    Local binding: 300 sec
    Forwarding state in LSD: 15 sec
  Delay in AF Binding Withdrawl from peer: 180 sec
  Max:
    1500 interfaces (1200 attached, 300 TE tunnel), 2000 peers
  OOR state
    Memory: Normal
```

Figura 39. Verificación de parámetros MPLS
Fuente: Autor

Verificación de vecinos MPLS resumen:

```
RP/0/0/CPU0:PE1#sh mpls ldp neighbor  brief
Fri Sep 29 04:51:20.722 UTC

Peer               GR  NSR  Up Time     Discovery   Addresses     Labels
                                          ipv4  ipv6  ipv4  ipv6  ipv4   ipv6
-----------------  --  ---  ----------  ----------  ----------  ------------
10.0.0.1:0         N   N    00:19:16    1     0     7     0     31     0
10.0.0.3:0         N   N    00:06:13    1     0     6     0     31     0
10.0.0.12:0        N   N    00:06:13    1     0     5     0     31     0
```

Figura 40. Verificación de vecinos MPLS resumen
Fuente: Autor

Verificación de vecino MPLS en una interfaz:

```
RP/0/0/CPU0:PE1#sh mpls ldp neighbor gigabitEthernet 0/0/0/3
Fri Sep 29 04:53:36.762 UTC

Peer LDP Identifier: 10.0.0.3:0
  TCP connection: 10.0.0.3:646 - 10.0.0.11:29119
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 44/43; Downstream-Unsolicited
  Up time: 00:08:29
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/3
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (6)
      10.0.0.3        10.1.3.2        10.2.3.2        10.3.4.1
      10.3.11.1       10.3.12.1
    IPv6: (0)
```

Figura 41. Verificación de Vecino MPLS en una interfaz específica
Fuente: Autor

Verificación de LIB:

```
RP/0/0/CPU0:PE1#sh mpls ldp bindings brief
Fri Sep 29 04:59:52.097 UTC

Prefix              Local      Advertised  Remote Bindings
                    Label        (peers)      (peers)
------------------  ---------  ----------  ---------------
10.0.0.1/32         24000               3                3
10.0.0.2/32         24001               3                3
10.0.0.3/32         24002               3                3
10.0.0.4/32         24003               3                3
10.0.0.11/32        ImpNull             3                3
10.0.0.12/32        24004               3                3
10.0.0.13/32        24006               3                3
10.0.0.14/32        24007               3                3
10.0.0.99/32        24005               3                3
10.1.2.0/30         24008               3                3
10.1.3.0/30         24011               3                3
10.1.4.0/30         24014               3                3
10.1.11.0/30        ImpNull             3                3
10.1.12.0/30        24018               3                3
10.1.99.0/30        24020               3                3
10.2.3.0/30         24010               3                3
10.2.4.0/30         24013               3                3
10.2.13.0/30        24023               3                3
10.2.14.0/30        24027               3                3
10.2.99.0/30        24019               3                3
10.3.4.0/30         24012               3                3
10.3.11.0/30        ImpNull             3                3
10.3.12.0/30        24017               3                3
10.4.13.0/30        24022               3                3
10.4.14.0/30        24026               3                3
10.11.10.0/30       ImpNull             3                3
10.11.12.0/30       ImpNull             3                3
10.12.10.0/30       24015               3                3
10.13.10.0/30       24021               3                3
10.13.14.0/30       24025               3                3
10.14.10.0/30       24024               3                3

RP/0/0/CPU0:PE1#sh mpls ldp bindings summary
Fri Sep 29 05:00:23.365 UTC

LIB Summary:
  Total Prefix    : 31
  Revision No     : Current:67, Advertised:67
  Local Bindings : 31
      NULL     : 5 (implicit:5, explicit:0)
      Non-NULL: 26 (lowest:24000, highest:24027)
  Remote Bindings: 93
```

Figura 42. Verificación de LIB
Fuente: Autor

Verificación de FIB:

```
RP/0/0/CPU0:PE1#sh cef
Fri Sep 29 05:02:12.777 UTC

Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
1.1.1.1/32          10.11.10.2/32       <recursive>
2.2.2.2/32          10.13.10.2/32       <recursive>
10.0.0.1/32         10.1.11.1/32        GigabitEthernet0/0/0/4
10.0.0.2/32         10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.0.0.3/32         10.3.11.1/32        GigabitEthernet0/0/0/3
10.0.0.4/32         10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.0.0.11/32        receive             Loopback0
10.0.0.12/32        10.11.12.2/32       GigabitEthernet0/0/0/2
10.0.0.13/32        10.0.0.13/32        tunnel-te3413
10.0.0.14/32        10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.0.0.99/32        10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.2.0/30         10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.3.0/30         10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.4.0/30         10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.11.0/30        attached            GigabitEthernet0/0/0/4
10.1.11.0/32        broadcast           GigabitEthernet0/0/0/4
10.1.11.1/32        10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.11.2/32        receive             GigabitEthernet0/0/0/4
10.1.11.3/32        broadcast           GigabitEthernet0/0/0/4
10.1.12.0/30        10.11.12.2/32       GigabitEthernet0/0/0/2
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.1.99.0/30        10.1.11.1/32        GigabitEthernet0/0/0/4
10.2.3.0/30         10.3.11.1/32        GigabitEthernet0/0/0/3
10.2.4.0/30         10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.2.13.0/30        10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.2.14.0/30        10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.2.99.0/30        10.3.11.1/32        GigabitEthernet0/0/0/3
                    10.1.11.1/32        GigabitEthernet0/0/0/4
10.3.4.0/30         10.3.11.1/32        GigabitEthernet0/0/0/3
10.3.11.0/30        attached            GigabitEthernet0/0/0/3
10.3.11.0/32        broadcast           GigabitEthernet0/0/0/3
10.3.11.1/32        10.3.11.1/32        GigabitEthernet0/0/0/3
10.3.11.2/32        receive             GigabitEthernet0/0/0/3
10.3.11.3/32        broadcast           GigabitEthernet0/0/0/3
 --More--
```

Figura 43. Verificación de FIB
Fuente: Autor

Verificación de LFIB:

```
RP/0/0/CPU0:PE1#sh mpls forwarding
Fri Sep 29 05:03:39.411 UTC
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
Label  Label       or ID             Interface                    Switched
------ ----------- ----------------- ------------ --------------- ------------
24000  Pop         10.0.0.1/32       Gi0/0/0/4    10.1.11.1       5810
24001  33013       10.0.0.2/32       Gi0/0/0/3    10.3.11.1       0
       31012       10.0.0.2/32       Gi0/0/0/4    10.1.11.1       0
24002  Pop         10.0.0.3/32       Gi0/0/0/3    10.3.11.1       2058
24003  33024       10.0.0.4/32       Gi0/0/0/3    10.3.11.1       0
       31023       10.0.0.4/32       Gi0/0/0/4    10.1.11.1       0
24004  Pop         10.0.0.12/32      Gi0/0/0/2    10.11.12.2      2000
24005  31002       10.0.0.99/32      Gi0/0/0/4    10.1.11.1       3462
24006  Pop         10.0.0.13/32      tt3413       10.0.0.13       0
24007  33017       10.0.0.14/32      Gi0/0/0/3    10.3.11.1       0
       31016       10.0.0.14/32      Gi0/0/0/4    10.1.11.1       0
24008  Pop         10.1.2.0/30       Gi0/0/0/4    10.1.11.1       0
24010  Pop         10.2.3.0/30       Gi0/0/0/3    10.3.11.1       0
24011  Pop         10.1.3.0/30       Gi0/0/0/3    10.3.11.1       0
       Pop         10.1.3.0/30       Gi0/0/0/4    10.1.11.1       0
24012  Pop         10.3.4.0/30       Gi0/0/0/3    10.3.11.1       0
24013  33016       10.2.4.0/30       Gi0/0/0/3    10.3.11.1       0
       31015       10.2.4.0/30       Gi0/0/0/4    10.1.11.1       0
24014  Pop         10.1.4.0/30       Gi0/0/0/4    10.1.11.1       0
24015  Pop         10.12.10.0/30     Gi0/0/0/2    10.11.12.2      0
24017  Pop         10.3.12.0/30      Gi0/0/0/2    10.11.12.2      0
       Pop         10.3.12.0/30      Gi0/0/0/3    10.3.11.1       0
24018  Pop         10.1.12.0/30      Gi0/0/0/2    10.11.12.2      0
       Pop         10.1.12.0/30      Gi0/0/0/4    10.1.11.1       0
24019  33011       10.2.99.0/30      Gi0/0/0/3    10.3.11.1       0
       31006       10.2.99.0/30      Gi0/0/0/4    10.1.11.1       0
24020  Pop         10.1.99.0/30      Gi0/0/0/4    10.1.11.1       0
24021  Unlabelled  10.13.10.0/30     tt3413       10.0.0.13       0
24022  33023       10.4.13.0/30      Gi0/0/0/3    10.3.11.1       0
       31022       10.4.13.0/30      Gi0/0/0/4    10.1.11.1       0
24023  33015       10.2.13.0/30      Gi0/0/0/3    10.3.11.1       0
       31014       10.2.13.0/30      Gi0/0/0/4    10.1.11.1       0
24024  33018       10.14.10.0/30     Gi0/0/0/3    10.3.11.1       0
       31017       10.14.10.0/30     Gi0/0/0/4    10.1.11.1       0
24025  Unlabelled  10.13.14.0/30     tt3413       10.0.0.13       0
       33019       10.13.14.0/30     Gi0/0/0/3    10.3.11.1       0
       31018       10.13.14.0/30     Gi0/0/0/4    10.1.11.1       0
24026  33020       10.4.14.0/30      Gi0/0/0/3    10.3.11.1       0
       31019       10.4.14.0/30      Gi0/0/0/4    10.1.11.1       0
24027  33014       10.2.14.0/30      Gi0/0/0/3    10.3.11.1       0
       31013       10.2.14.0/30      Gi0/0/0/4    10.1.11.1       0
```

Figura 44. Verificación de LFIB
Fuente: Autor

Verificación de Rutas aprendidas en PE1:

```
RP/0/0/CPU0:PE1#sh route
Fri Sep 29 05:05:14.635 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

B    1.1.1.1/32 [20/0] via 10.11.10.2, 00:33:03
B    2.2.2.2/32 [200/0] via 10.13.10.2, 00:33:03
i L2 10.0.0.1/32 [115/20] via 10.1.11.1, 00:32:20, GigabitEthernet0/0/0/4
i L2 10.0.0.2/32 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                 [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.0.0.3/32 [115/20] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
i L2 10.0.0.4/32 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                 [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
L    10.0.0.11/32 is directly connected, 00:33:25, Loopback0
i L2 10.0.0.12/32 [115/20] via 10.11.12.2, 00:20:03, GigabitEthernet0/0/0/2
i L2 10.0.0.13/32 [115/40] via 10.0.0.13, 00:31:01, tunnel-te3413
i L2 10.0.0.14/32 [115/40] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                  [115/40] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.0.0.99/32 [115/30] via 10.1.11.1, 00:32:20, GigabitEthernet0/0/0/4
i L2 10.1.2.0/30 [115/20] via 10.1.11.1, 00:32:20, GigabitEthernet0/0/0/4
i L2 10.1.3.0/30 [115/20] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                 [115/20] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.1.4.0/30 [115/20] via 10.1.11.1, 00:32:20, GigabitEthernet0/0/0/4
C    10.1.11.0/30 is directly connected, 00:33:24, GigabitEthernet0/0/0/4
L    10.1.11.2/32 is directly connected, 00:33:24, GigabitEthernet0/0/0/4
i L2 10.1.12.0/30 [115/20] via 10.11.12.2, 00:20:03, GigabitEthernet0/0/0/2
                  [115/20] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.1.99.0/30 [115/20] via 10.1.11.1, 00:32:20, GigabitEthernet0/0/0/4
i L2 10.2.3.0/30 [115/20] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
i L2 10.2.4.0/30 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                 [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.2.13.0/30 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.2.14.0/30 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.2.99.0/30 [115/30] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 00:20:03, GigabitEthernet0/0/0/4
i L2 10.3.4.0/30 [115/20] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
C    10.3.11.0/30 is directly connected, 00:20:06, GigabitEthernet0/0/0/3
L    10.3.11.2/32 is directly connected, 00:20:06, GigabitEthernet0/0/0/3
i L2 10.3.12.0/30 [115/20] via 10.11.12.2, 00:20:03, GigabitEthernet0/0/0/2
                  [115/20] via 10.3.11.1, 00:20:03, GigabitEthernet0/0/0/3
```

Figura 45. Verificación de rutas aprendidas en PE1
Fuente: Autor

Verificación de túneles de TE configurados en el PE1:

```
RP/0/0/CPU0:PE1#sh mpls traffic-eng tunnels brief
Fri Sep 29 05:26:15.378 UTC

                  TUNNEL NAME          DESTINATION      STATUS  STATE
                tunnel-te1213            10.0.0.13          up  up
                tunnel-te1414            10.0.0.14          up  up
                tunnel-te3413            10.0.0.13          up  up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 3 up, 0 down, 0 recovering, 0 recovered heads
```

Figura 46. Verificación de túneles de TE configurados en el PE1
Fuente: Autor

Verificación de configuración del túnel 3413 configurado en el PE1:

```
RP/0/0/CPU0:PE1#sh mpls traffic-eng tunnels 3413
Fri Sep 29 05:28:55.927 UTC


Name: tunnel-te3413  Destination: 10.0.0.13  Ifhandle:0x90
  Signalled-Name: PE1_t3413
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 20,  type dynamic  (Basis for Setup, path weight 30)
    path option 10,  type explicit PE1_P3_P4_PE3
    Last PCALC Error: Fri Sep 29 04:34:12 2023
      Info: Explicit path has unknown address, 10.3.11.2
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Sep 29 04:31:48 2023 (00:57:08 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (global)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute:  enabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
  History:
    Tunnel has been up for: 00:54:43 (since Fri Sep 29 04:34:13 UTC 2023)
    Current LSP:
      Uptime: 00:54:43 (since Fri Sep 29 04:34:13 UTC 2023)

  Path info (IS-IS MTI level-2):
  Node hop count: 3
  Hop0: 10.1.11.1
  Hop1: 10.1.2.1
  Hop2: 10.1.2.2
  Hop3: 10.2.13.1
  Hop4: 10.2.13.2
  Hop5: 10.0.0.13
Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Figura 47. Verificación de túnel 3413 configurado en el PE1
Fuente: Autor

Verificación del estado y direccionamiento de las interfaces:

```
RP/0/0/CPU0:PE1#sh ip int brief
Fri Sep 29 05:26:26.178 UTC

Interface                  IP-Address      Status          Protocol Vrf-Name
Loopback0                  10.0.0.11       Up              Up       default
tunnel-te1213              unassigned      Up              Up       default
tunnel-te1414              unassigned      Up              Up       default
tunnel-te3413              unassigned      Up              Up       default
MgmtEth0/0/CPU0/0          unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/1     10.11.10.1      Up              Up       default
GigabitEthernet0/0/0/2     10.11.12.1      Up              Up       default
GigabitEthernet0/0/0/3     10.3.11.2       Up              Up       default
GigabitEthernet0/0/0/4     10.1.11.2       Up              Up       default
GigabitEthernet0/0/0/5     unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6     unassigned      Shutdown        Down     default
```

Figura 48. Verificación del estado y direccionamiento de las interfaces
Fuente: Autor

Verificación de conectividad entre CE1 – CE2:

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 17/19/24 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 15/18/26 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 15/19/27 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 17/19/23 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 16/19/24 ms
CE1#
```

Figura 49. Verificación de conectividad entre CE1 – CE2
Fuente: Autor

Traceroute entre CE1 – CE2:

```
CE1#traceroute 2.2.2.2 source 1.1.1.1 numeric
Type escape sequence to abort.
Tracing the route to 2.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.11.10.1 8 msec 4 msec 5 msec
  2 10.1.11.1 [MPLS: Label 31025 Exp 0] 55 msec *  *
  3 10.1.2.2 [MPLS: Label 32026 Exp 0] 46 msec *  38 msec
  4 10.2.13.2 43 msec *  *
  5 10.13.10.2 41 msec *  *
CE1#
```

Figura 50. Traceroute entre CE1 – CE2
Fuente: Autor

Como herramienta para controlar el tráfico que cursa por la red y manipularlo se utilizará NetEm, que según la información mostrada en su página web, es una mejora de las funciones de control de tráfico de Linux que permite agregar retrasos, pérdida de paquetes, duplicación y otras características a los paquetes que salen de una interfaz de red seleccionada.

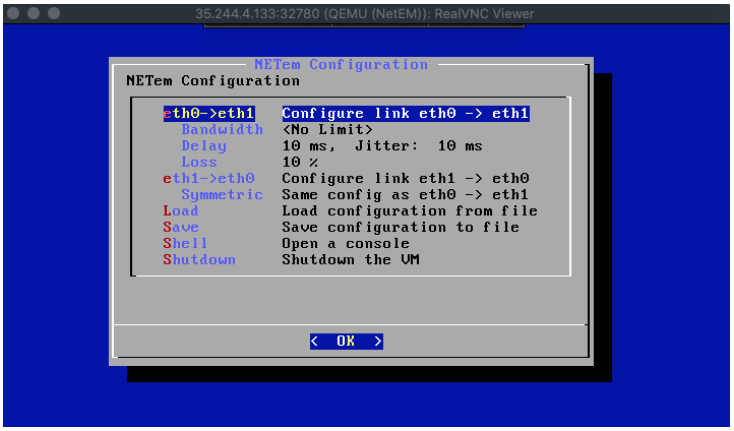


Figura 51. Herramienta NetEM
Fuente: Autor

Conectividad entre CE1 – CE2; Delay=10 ms:

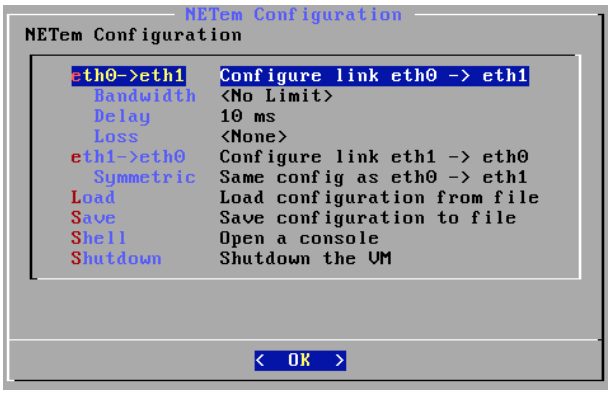


Figura 52. Seteo de Delay=10 ms
Fuente: Autor

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 37/39/47 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 37/39/44 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 36/39/43 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 35/39/45 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 35/39/48 ms
CE1#
```

Figura 53. Pruebas de ping con Delay=10 ms
Fuente: Autor

Conectividad entre CE1 – CE2; Delay=10 ms, Jitter=10ms:

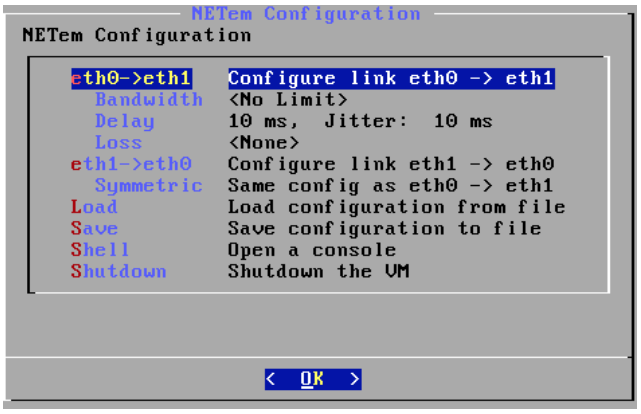


Figura 54. Seteo de Delay=10 ms, Jitter=10ms
Fuente: Autor

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 22/38/64 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 25/39/54 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 21/39/59 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 20/40/57 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 22/37/62 ms
```

Figura 55. Pruebas de ping con Delay=10 ms, Jitter=10ms
Fuente: Autor

Conectividad entre CE1 – CE2; Delay=10 ms, Jitter=10ms, Lost=10%:

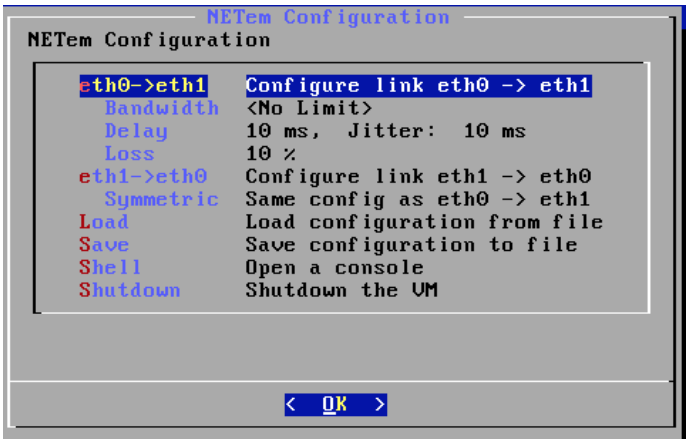


Figura 56. Seteo de Delay=10 ms, Jitter=10ms, Lost=10%
Fuente: Autor

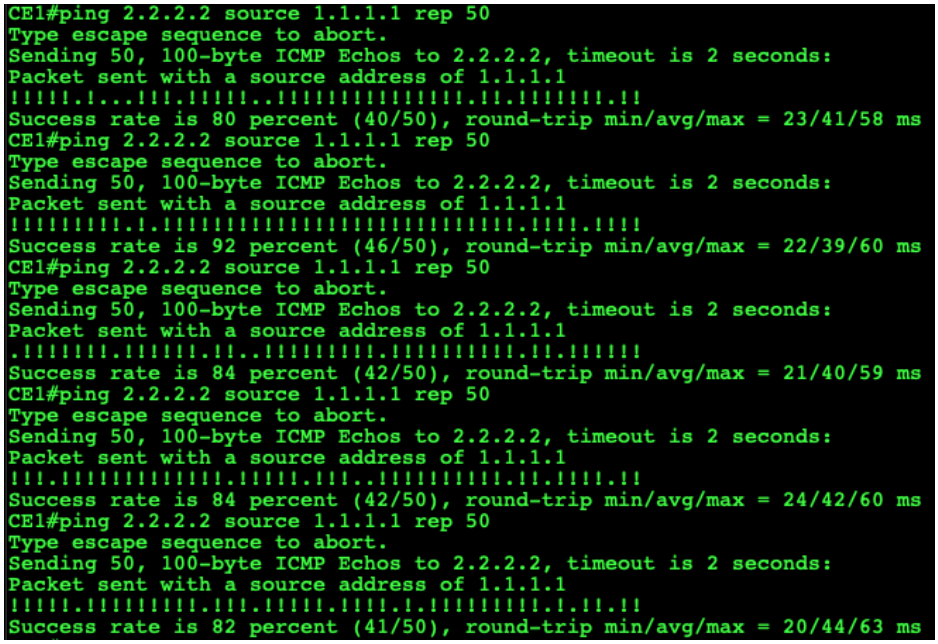


Figura 57. Pruebas de ping con Delay=10 ms, Jitter=10ms, Lost=10%
Fuente: Autor

3.6.7. Topología 2 – Red IP MPLS con *Segment Routing*

Al igual que en el numeral 3.6.6, adicionalmente a las consideraciones generales planteadas, en este escenario se implementará una red IP MPLS utilizando *Segment Routing* como protocolo para realizar el routeo de los paquetes dentro de la red del proveedor.

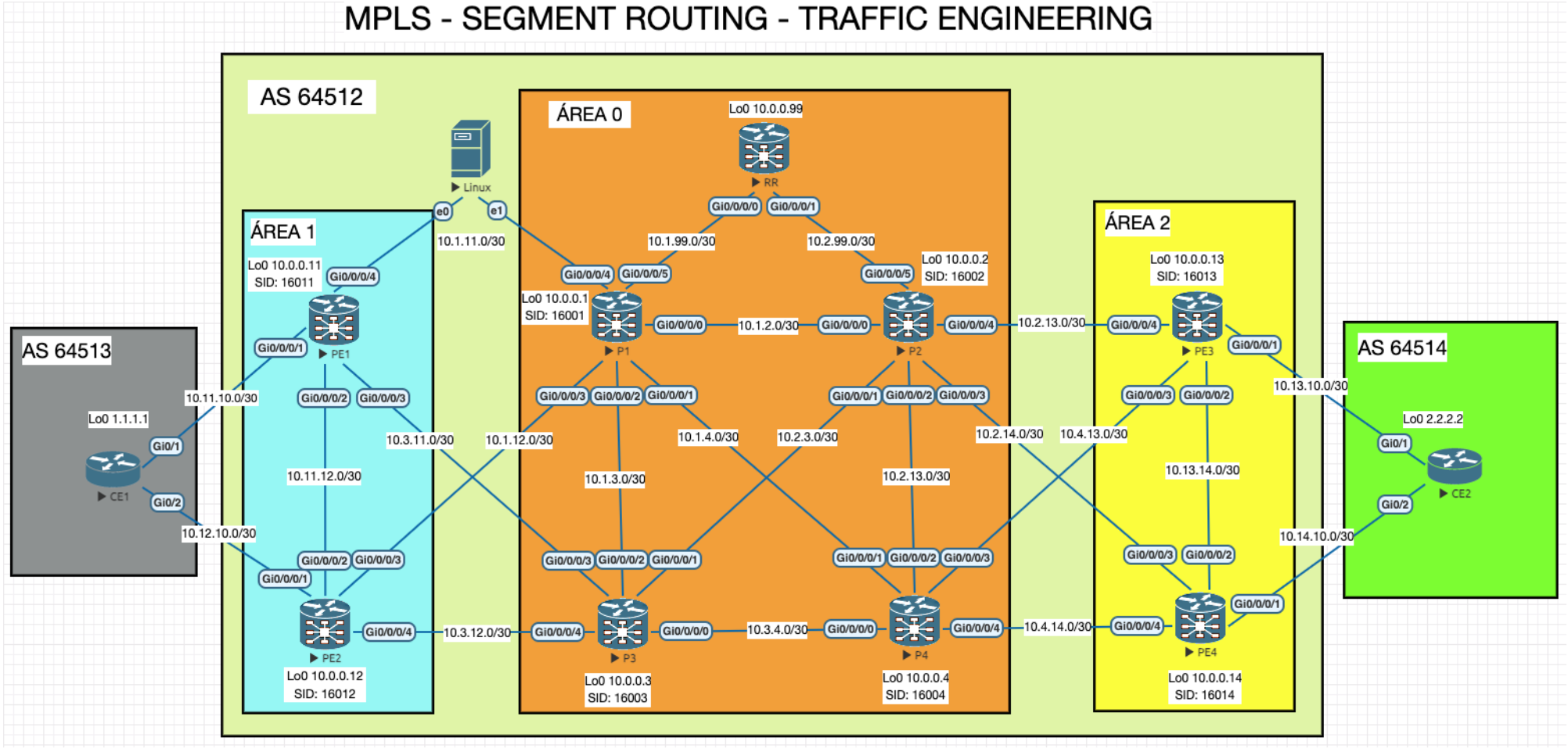


Figura 58. Red IP MPLS con Segment Routing de un Proveedor de Servicios
Fuente: Autor

Asignación de SIDs para cada equipo que conforma la red del Proveedor de Servicios:

HOSTNAME	NODE ID SR
P1	16001
P2	16002
P3	16003
P4	16004
PE1	16011
PE2	16012
PE3	16013
PE4	16014

Tabla 14. Asignación de SIDs
Fuente: Autor

Configuración general de MPLS con *Segment Routing* para TE:

Configuración de MPLS + SR para TE

```
interface Loopback0
 ipv4 address 10.0.0.11 255.255.255.255
!
router isis MTI
 is-type level-2-only
 net 49.0001.0100.0000.0011.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  router-id Loopback0
  segment-routing mpls
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
   prefix-sid absolute 16011
  !
 !
mpls traffic-eng
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
segment-routing
 global-block 16000 23999
!
explicit-path name 1213
```

```
 index 1 next-label 16001
 index 2 next-label 16002
 index 3 next-label 16013
!
interface tunnel-te1213
 ipv4 unnumbered Loopback0
 autoroute announce
 !
 destination 10.0.0.13
 path-option 1 explicit name 1213 segment-routing
!
```

Tabla 15. Configuración de MPLS + SR para TE
Fuente: Autor

Verificación de vecinos MPLS LDP resumen:

```
RP/0/0/CPU0:PE1#sh mpls ldp neighbor  brief
Thu Oct 26 21:43:29.282 UTC

RP/0/0/CPU0:PE1#
```

Figura 59. Verificación de vecinos MPLS resumen
Fuente: Autor

Verificación de tabla de etiquetas Segment Routing:

```
RP/0/0/CPU0:PE1#sh mpls label table detail
Wed Nov 29 02:19:11.985 UTC
Table Label   Owner                           State  Rewrite
----- ------- ------------------------------- ------ -------
0     0       LSD(A)                          InUse  Yes
0     1       LSD(A)                          InUse  Yes
0     2       LSD(A)                          InUse  Yes
0     13      LSD(A)                          InUse  Yes
0     16000   ISIS(A):MTI                     InUse  No
              BGP-VPNv4(A):bgp-default        InUse  No
  (Lbl-blk SRGB, vers:0, (start_label=16000, size=8000)
0     24000   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=1, type=0, intf=Gi0/0/0/2, nh=10.11.12.2)
0     24001   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=3, type=0, intf=Gi0/0/0/2, nh=10.11.12.2)
0     24002   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=1, type=0, intf=Gi0/0/0/3, nh=10.3.11.1)
0     24003   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=3, type=0, intf=Gi0/0/0/3, nh=10.3.11.1)
0     24004   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=1, type=0, intf=Gi0/0/0/4, nh=10.1.11.1)
0     24005   ISIS(A):MTI                     InUse  Yes
  (SR Adj Segment IPv4, vers:0, index=3, type=0, intf=Gi0/0/0/4, nh=10.1.11.1)
0     24006   TE-Control(A)                   InUse  Yes
  (TE Binding, vers:0, identifier=1213, type=0)
0     24007   TE-Control(A)                   InUse  Yes
  (TE Binding, vers:0, identifier=1414, type=0)
0     24008   TE-Control(A)                   InUse  Yes
  (TE Binding, vers:0, identifier=3413, type=0)
0     24009   TE-Control(A)                   InUse  Yes
  (TEv4 SR, vers:0, 'default':4U, src=10.0.0.11, dst=10.0.0.13, tun_id=1213, ext_tun_id=0xb00000a, lsp_id=2)
0     24010   TE-Control(A)                   InUse  Yes
  (TEv4 SR, vers:0, 'default':4U, src=10.0.0.11, dst=10.0.0.14, tun_id=1414, ext_tun_id=0xb00000a, lsp_id=2)
0     24011   TE-Control(A)                   InUse  Yes
  (TEv4 SR, vers:0, 'default':4U, src=10.0.0.11, dst=10.0.0.13, tun_id=3413, ext_tun_id=0xb00000a, lsp_id=2)
0     24012   LDP(A)                          InUse  Yes
  (IPv4, vers:0, 'default':4U, 10.0.0.13/32)
RP/0/0/CPU0:PE1#
```

Figura 60. Verificación de tabla de etiquetas Segment Routing
Fuente: Autor

Verificación de LIB:

```
RP/0/0/CPU0:PE1#sh mpls ldp bindings brief
Thu Oct 26 21:45:32.504 UTC

Prefix             Local      Advertised  Remote Bindings
                   Label        (peers)       (peers)
-----------------  ---------  ----------  --------------
10.0.0.13/32       24009                0               0

RP/0/0/CPU0:PE1#
```

Figura 61. Verificación de LIB
Fuente: Autor

Verificación de LFIB:

```
RP/0/0/CPU0:PE1#sh mpls forwarding
Thu Oct 26 21:47:38.965 UTC
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
Label  Label       or ID             Interface                    Switched
------ ----------- ----------------- ------------ --------------- ------------
16001  Pop         SR Pfx (idx 1)    Gi0/0/0/4    10.1.11.1       0
16002  16002       SR Pfx (idx 2)    Gi0/0/0/3    10.3.11.1       0
       16002       SR Pfx (idx 2)    Gi0/0/0/4    10.1.11.1       0
16003  Pop         SR Pfx (idx 3)    Gi0/0/0/3    10.3.11.1       0
16004  16004       SR Pfx (idx 4)    Gi0/0/0/3    10.3.11.1       0
       16004       SR Pfx (idx 4)    Gi0/0/0/4    10.1.11.1       0
16012  Pop         SR Pfx (idx 12)   Gi0/0/0/2    10.11.12.2      0
16013  16013       SR Pfx (idx 13)   Gi0/0/0/4    10.1.11.1       0
       16013       SR Pfx (idx 13)   Gi0/0/0/3    10.3.11.1       0
16014  16014       SR Pfx (idx 14)   Gi0/0/0/3    10.3.11.1       0
       16014       SR Pfx (idx 14)   Gi0/0/0/4    10.1.11.1       0
24000  Pop         SR Adj (idx 1)    Gi0/0/0/2    10.11.12.2      0
24001  Pop         SR Adj (idx 3)    Gi0/0/0/2    10.11.12.2      0
24002  Pop         SR Adj (idx 1)    Gi0/0/0/4    10.1.11.1       0
24003  Pop         SR Adj (idx 3)    Gi0/0/0/4    10.1.11.1       0
24004  Pop         SR Adj (idx 1)    Gi0/0/0/3    10.3.11.1       0
24005  Pop         SR Adj (idx 3)    Gi0/0/0/3    10.3.11.1       0
24006  Pop         No ID             tt13         point2point     0
24008  Pop         No ID             tt1414       point2point     0
24009  Pop         10.0.0.13/32      tt13         10.0.0.13       0
24010  Pop         No ID             tt3413       point2point     0
RP/0/0/CPU0:PE1#
```

Figura 62. Verificación de LFIB
Fuente: Autor

Verificación de rutas aprendidas en PE1:

```
RP/0/0/CPU0:PE1#sh route
Thu Oct 26 21:48:10.313 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

B    1.1.1.1/32 [20/0] via 10.11.10.2, 04:42:38
B    2.2.2.2/32 [200/0] via 10.13.10.2, 04:42:23
i L2 10.0.0.1/32 [115/10] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.0.0.2/32 [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.0.0.3/32 [115/10] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
i L2 10.0.0.4/32 [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
L    10.0.0.11/32 is directly connected, 04:47:26, Loopback0
i L2 10.0.0.12/32 [115/10] via 10.11.12.2, 04:13:13, GigabitEthernet0/0/0/2
i L2 10.0.0.13/32 [115/30] via 10.0.0.13, 03:11:08, tunnel-te13
i L2 10.0.0.14/32 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.0.0.99/32 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.1.2.0/30 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.1.3.0/30 [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.1.4.0/30 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
C    10.1.11.0/30 is directly connected, 04:47:26, GigabitEthernet0/0/0/4
L    10.1.11.2/32 is directly connected, 04:47:26, GigabitEthernet0/0/0/4
i L2 10.1.12.0/30 [115/20] via 10.11.12.2, 04:13:13, GigabitEthernet0/0/0/2
                  [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.1.99.0/30 [115/20] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.2.3.0/30 [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
i L2 10.2.4.0/30 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                 [115/30] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.2.13.0/30 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.2.14.0/30 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.2.99.0/30 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
                  [115/30] via 10.1.11.1, 04:13:13, GigabitEthernet0/0/0/4
i L2 10.3.4.0/30 [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
C    10.3.11.0/30 is directly connected, 04:47:26, GigabitEthernet0/0/0/3
L    10.3.11.2/32 is directly connected, 04:47:26, GigabitEthernet0/0/0/3
i L2 10.3.12.0/30 [115/20] via 10.11.12.2, 04:13:13, GigabitEthernet0/0/0/2
                  [115/20] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
i L2 10.4.13.0/30 [115/30] via 10.3.11.1, 04:13:13, GigabitEthernet0/0/0/3
```

Figura 63. Verificación de rutas aprendidas en PE1
Fuente: Autor

Verificación de túneles de TE configurados en el PE1:

```
RP/0/0/CPU0:PE1#sh mpls traffic-eng tunnels brief
Thu Oct 26 21:55:06.435 UTC

                  TUNNEL NAME          DESTINATION      STATUS  STATE
                tunnel-te1213            10.0.0.13          up  up
                tunnel-te1414            10.0.0.14          up  up
                tunnel-te3413            10.0.0.13          up  up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 3 up, 0 down, 0 recovering, 0 recovered heads
```

Figura 64. Verificación de túneles de TE configurados en el PE1
Fuente: Autor

Verificación de túnel 1213 configurado en el PE1:

```
RP/0/0/CPU0:PE1#sh mpls traffic-eng tunnels 1213
Thu Oct 26 21:56:31.189 UTC


Name: tunnel-te1213  Destination: 10.0.0.13  Ifhandle:0x110
  Signalled-Name: PE1_t1213
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1, (Segment-Routing) type explicit 1213 (Basis for Setup)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Thu Oct 26 21:54:41 2023 (00:01:50 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (global)
    Path Selection:
      Tiebreaker: Min-fill (default)
      Protection: any (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute:  enabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Disabled
  History:
    Tunnel has been up for: 00:01:50 (since Thu Oct 26 21:54:41 UTC 2023)
    Current LSP:
      Uptime: 00:01:50 (since Thu Oct 26 21:54:41 UTC 2023)

  Segment-Routing Path Info (IS-IS MTI level-2)
    Segment0[Node]: 10.0.0.1, Label: 16001
    Segment1[Node]: 10.0.0.2, Label: 16002
    Segment2[Node]: 10.0.0.13, Label: 16013
Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Figura 65. Verificación de túnel 1213 configurado en el PE1
Fuente: Autor

Enrutamiento desde PE1 (10.0.0.11) hacia PE3 (10.0.0.13) a través del túnel te1213:

```
RP/0/0/CPU0:PE1#sh route 10.0.0.13
Thu Oct 26 21:57:33.974 UTC

Routing entry for 10.0.0.13/32
  Known via "isis MTI", distance 115, metric 30, labeled SR, type level-2
  Installed Oct 26 21:54:41.396 for 00:02:52
  Routing Descriptor Blocks
    10.0.0.13, from 10.0.0.13, via tunnel-te1213
      Route metric is 30
  No advertising protos.
```

Figura 66. Enrutamiento entre PE1 - PE3 a través del túnel te1213
Fuente: Autor

Traceroute entre PE1 (10.0.0.11) - PE3 (10.0.0.13):

```
RP/0/0/CPU0:PE1#traceroute 10.0.0.13
Thu Oct 26 21:57:21.565 UTC

Type escape sequence to abort.
Tracing the route to 10.0.0.13

 1  10.1.11.1 [MPLS: Labels 16002/16013 Exp 0] 9 msec  0 msec  0 msec
 2  10.1.2.2 [MPLS: Label 16013 Exp 0] 0 msec  0 msec  0 msec
 3  10.2.13.2 0 msec  *  0 msec
RP/0/0/CPU0:PE1#
```

Figura 67. Traceroute entre PE1 - PE3
Fuente: Autor

Verificación del estado y direccionamiento de las interfaces:

```
RP/0/0/CPU0:PE1#sh ip int brief
Thu Oct 26 21:59:40.886 UTC

Interface                      IP-Address      Status          Protocol Vrf-Name
Loopback0                      10.0.0.11       Up              Up       default
tunnel-te1213                  10.0.0.11       Up              Up       default
tunnel-te1414                  10.0.0.11       Up              Up       default
tunnel-te3413                  10.0.0.11       Up              Up       default
MgmtEth0/0/CPU0/0              unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/0         unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/1         10.11.10.1      Up              Up       default
GigabitEthernet0/0/0/2         10.11.12.1      Up              Up       default
GigabitEthernet0/0/0/3         10.3.11.2       Up              Up       default
GigabitEthernet0/0/0/4         10.1.11.2       Up              Up       default
GigabitEthernet0/0/0/5         unassigned      Shutdown        Down     default
GigabitEthernet0/0/0/6         unassigned      Shutdown        Down     default
```

Figura 68. Estado y direccionamiento de las interfaces
Fuente: Autor

Verificación de conectividad entre CE1 – CE2:

```
CE1#ping 2.2.2.2 source 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/12/14 ms
```

Figura 69. Verificación de conectividad entre CE1 – CE2
Fuente: Autor

Traceroute desde CE1 (1.1.1.1) hacia CE2 (2.2.2.2):

```
CE1#traceroute 2.2.2.2 source 1.1.1.1 numeric
Type escape sequence to abort.
Tracing the route to 2.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.11.10.1 4 msec 3 msec 3 msec
  2 10.1.11.1 [MPLS: Labels 16002/16013 Exp 0] 10 msec 10 msec 10 msec
  3 10.1.2.2 [MPLS: Label 16013 Exp 0] 9 msec 9 msec 9 msec
  4 10.2.13.2 9 msec 9 msec 9 msec
  5 10.13.10.2 12 msec *  14 msec
CE1#
```

Figura 70. Traceroute entre CE1- CE2
Fuente: Autor

Conectividad entre CE1 – CE2 50 repeticiones:

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/11/14 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/11/15 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/11/13 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/11/14 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/11/13 ms
```

Figura 71. Conectividad entre CE1 – CE2 50 repeticiones
Fuente: Autor

Conectividad entre CE1 – CE2 con un Delay=10 ms:

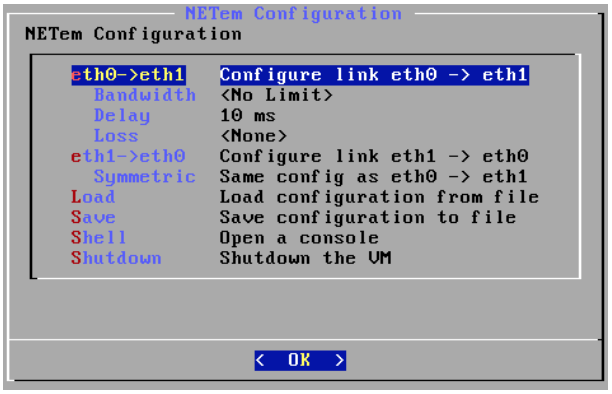


Figura 72. Seteo de Delay=10 ms
Fuente: Autor

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 21/21/24 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 21/21/23 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 22/22/24 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 21/21/23 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 21/21/23 ms
```

Figura 73. Pruebas de ping con Delay=10 ms
Fuente: Autor

Conectividad entre CE1 – CE2; Delay=10 ms, Jitter=10ms:

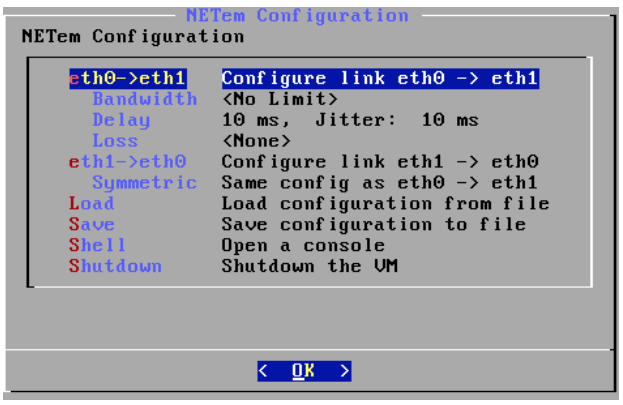


Figura 74. Seteo de Delay=10 ms, Jitter=10ms
Fuente: Autor

```
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 12/21/33 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 12/21/31 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 12/22/32 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 12/21/32 ms
CE1#ping 2.2.2.2 source 1.1.1.1 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 11/20/32 ms
```

Figura 75. Pruebas de ping con Delay=10 ms, Jitter=10ms
Fuente: Autor

Conectividad entre CE1 – CE2; Delay=10 ms, Jitter=10ms, Lost=10%:

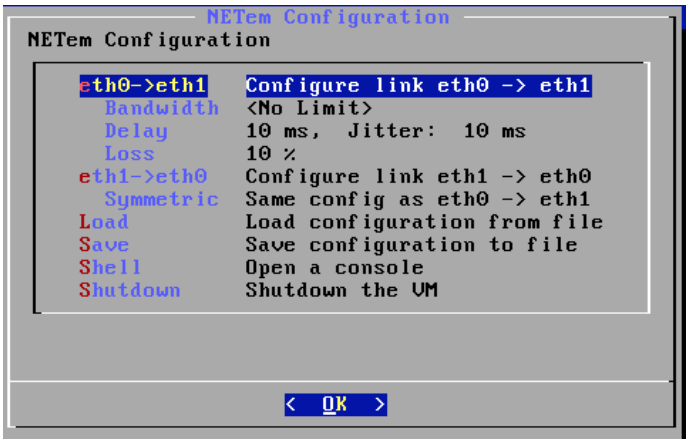


Figura 76. Seteo de Delay=10 ms, Jitter=10ms, Lost=10%
Fuente: Autor

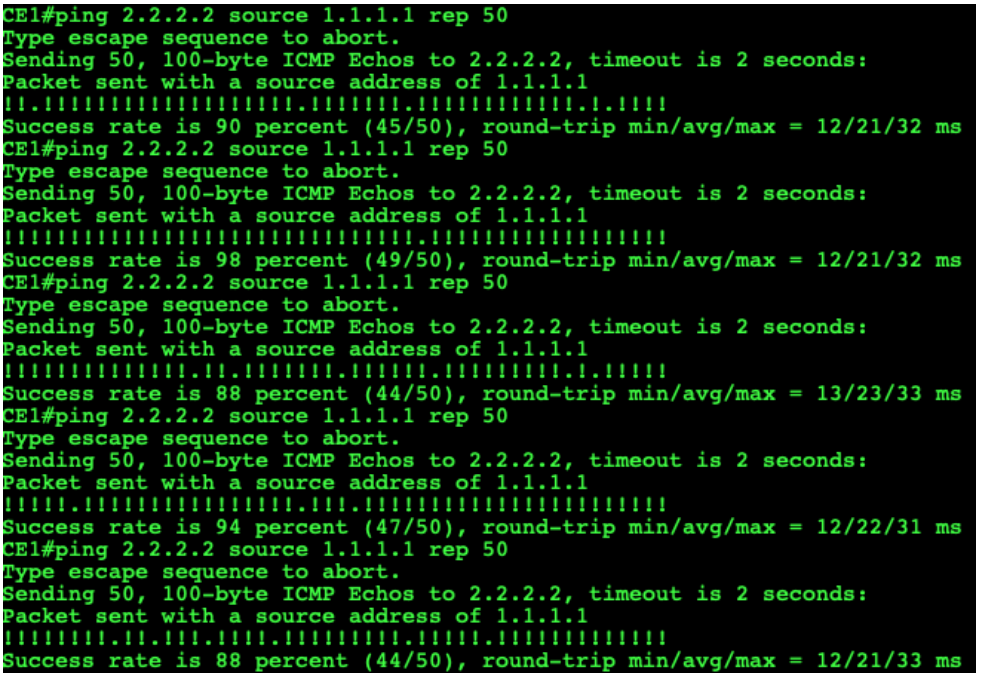


Figura 77. Pruebas de ping con Delay=10 ms, Jitter=10ms, Lost=10%
Fuente: Autor

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE DATOS

Para el análisis de la latencia y jitter se realizaron pruebas con el uso del comando ping con 50 repeticiones entre los equipos del cliente instalados en cada sitio (CE1 y CE2), es decir, atravesando toda la red MPLS del Proveedor de Servicios para los 2 escenarios (MPLS + LDP y MPLS + SEGMENT ROUTING). A través de la herramienta NetEM se modificaron los parámetros de delay, jitter y pérdida de paquetes. Los resultados se muestran en la siguiente tabla:

	ESCENARIO 1: MPLS + LDP			**ESCENARIO 2: MPLS + SEGMENT ROUTING**		
PRUEBA	**MIN**	**AVG**	**MAX**	**MIN**	**AVG**	**MAX**
Ping Normal						
1	17	19	24	11	11	14
2	15	18	26	11	11	15
3	15	19	27	11	11	13
4	17	19	23	11	11	14
5	16	19	24	11	11	13
6	16	18	23	11	11	13
7	17	19	26	11	11	14
8	15	18	23	11	11	14
9	17	19	25	11	11	15
10	17	19	27	11	11	13
Ping agregando un Delay de 10 ms						
1	37	39	47	21	21	24
2	37	39	44	21	21	23
3	36	39	43	22	22	24
4	35	39	45	21	21	23
5	35	39	48	21	21	23
6	35	39	45	21	21	23
7	37	39	44	22	22	24
8	36	39	47	21	21	23
9	37	39	44	21	22	24
10	36	39	43	21	21	23
Ping agregando un Delay de 10 ms y un Jitter de 10 ms						
1	22	38	64	12	21	33
2	25	39	54	12	21	31
3	21	39	59	12	22	32
4	20	40	57	12	31	32
5	22	37	62	11	20	32
6	21	38	59	12	22	32
7	21	37	61	11	21	32
8	20	40	57	12	22	32
9	21	38	59	12	21	31
10	23	40	55	12	20	31
Ping agregando un Delay de 10 ms, un Jitter de 10 ms y una pérdida de paquetes del 10%						
1	23	41	58	12	21	32

2	22	39	60	12	21	32
3	21	40	59	13	23	33
4	24	42	60	12	22	31
5	20	44	63	12	21	33
6	20	42	59	13	23	33
7	20	44	63	12	22	33
8	22	40	60	12	21	21
9	21	41	59	13	23	32
10	23	42	60	12	21	33

Tabla 16. Pruebas de Ping para Latencia y Jitter
Fuente: Autor

A continuación, se presentan los promedios de los valores obtenidos para cada una de las pruebas y las gráficas correspondientes en los 2 escenarios:

ESCENARIO 1: MPLS + LDP			**ESCENARIO 2: MPLS + SEGMENT ROUTING**		
MIN	**AVG**	**MAX**	**MIN**	**AVG**	**MAX**
Ping Normal					
16,2	18,7	24,8	11	11	13,8
Ping agregando un Delay de 10 ms					
36,1	39	45	21,2	21,3	23,4
Ping agregando un Delay de 10 ms y un Jitter de 10 ms					
21,6	38,6	58,7	11,8	22,1	31,8
Ping agregando un Delay de 10 ms, un Jitter de 10 ms y una pérdida de paquetes del 10%					
21,6	41,5	60,1	12,3	21,8	31,3

Tabla 17. Promedio - Pruebas de Ping para Latencia y Jitter
Fuente: Autor

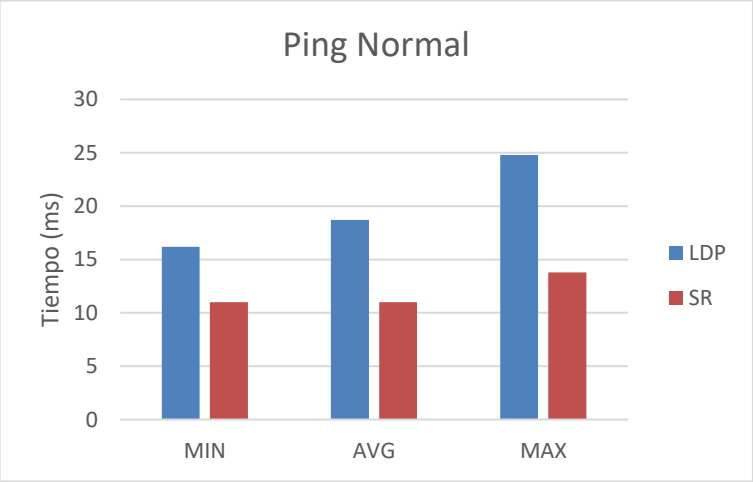


Figura 78. Pruebas de ping normal
Fuente: Autor

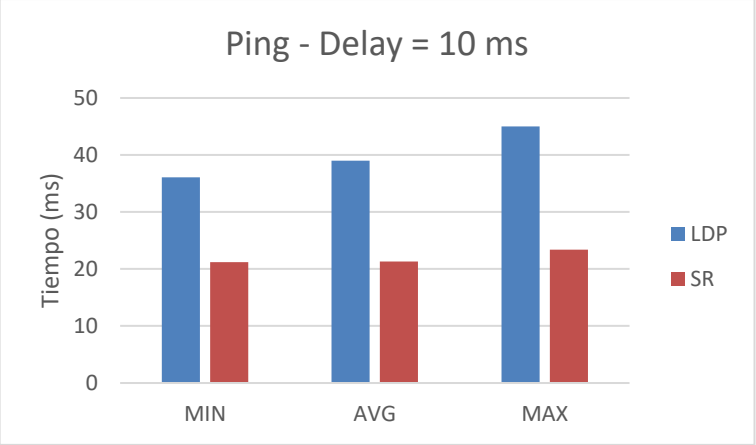


Figura 79. Pruebas de Ping – Delay = 10ms
Fuente: Autor

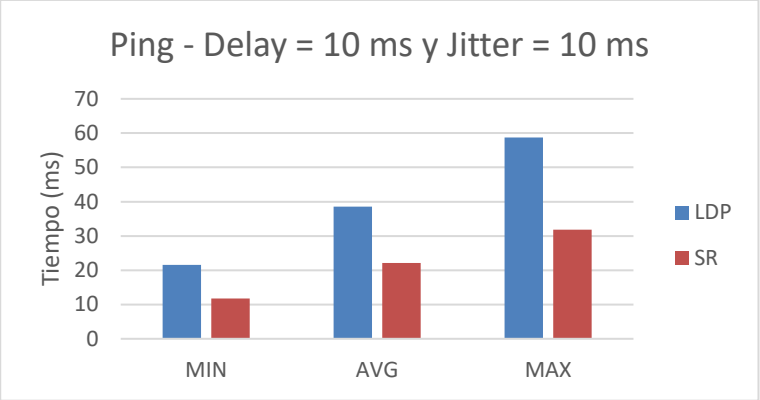


Figura 80. Pruebas de Ping – Delay=10ms; Jitter=10ms
Fuente: Autor

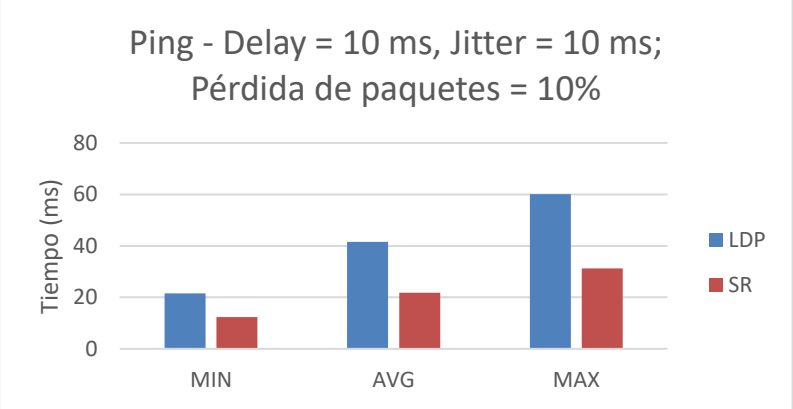


Figura 81. Pruebas de Ping – Delay=10ms; Jitter=10ms, Perdida de paquetes=10%
Fuente: Autor

Como se puede apreciar, en todos los casos de las pruebas realizadas, siempre son mayores los valores de MPLS con LDP en comparación a los valores obtenidos con *Segment Routing*, por ende, se tiene una mejora sustancial en el desempeño de la red del Proveedor de Servicios utilizando MPLS con *Segment Routing*.

Con respecto a Ingeniería de Tráfico, se puede indicar que a pesar de que *Segment Routing* brinda la posibilidad de configurar políticas (***SR Policies***) para controlar el flujo de mejor manera y optimizar la ocupación de los enlaces, para efectos de la emulación se trabajó con una imagen de equipos Cisco

ASR9K con versión de sistema operativo XR 6.1.3. Cabe indicar que con esta versión no fue posible configurar las políticas SR para *Traffic Engineering* como se lo realizaría en un equipo real, razón por la cual únicamente se configuraron interfaces túnel.

Ante esta limitante, se incluye de forma teórica un ejemplo de la configuración requerida para una política de *Segment Routing* para *Traffic Engineering*.

El comando que se muestra a continuación habilita la alimentación de la *database* de *Segment Routing* para *Traffic Engineering* en el router Head-end:

```
router isis 1
 distribute link-state
```

Figura 82. Comando para alimentar la SRTE DB en el Head-end
Fuente: (Filsfils & Michielsen, 2017)

Los siguientes comandos forman parte de la configuración de una Política de *Segment Routing* para *Traffic Engineering* (*SR Policy*):

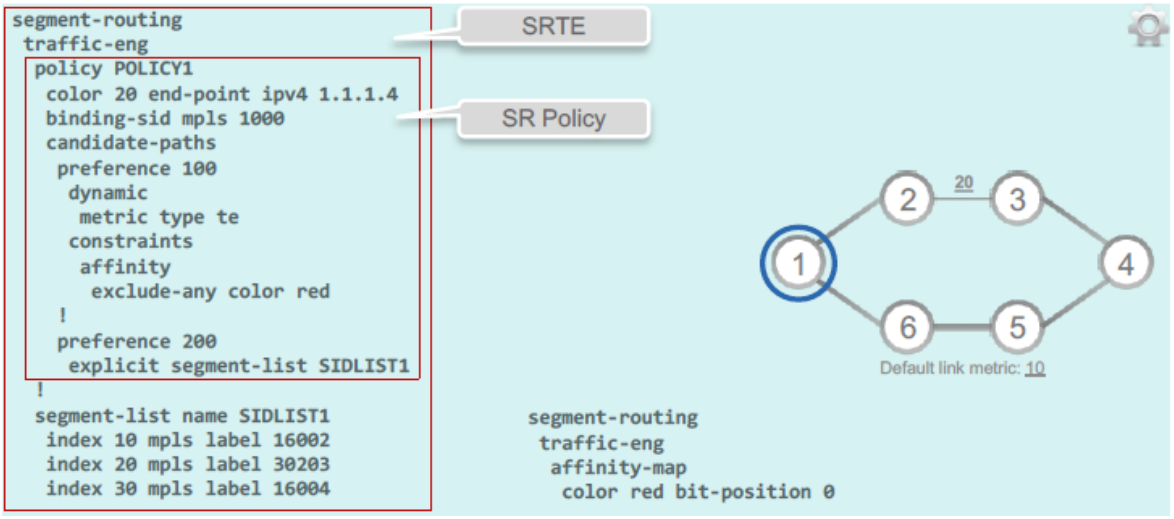


Figura 83. Configuración de la SR Policy
Fuente: (Filsfils & Michielsen, 2017)

En la siguiente figura, se remarcan los comandos para elección de los *paths* candidatos, el primero tendrá una preferencia de 100 y será dinámico, mientras que, el segundo tendrá una preferencia de 200 y seguirá un *path* explicito, cuyos saltos se listan en el *segment-list SIDLIST1*.

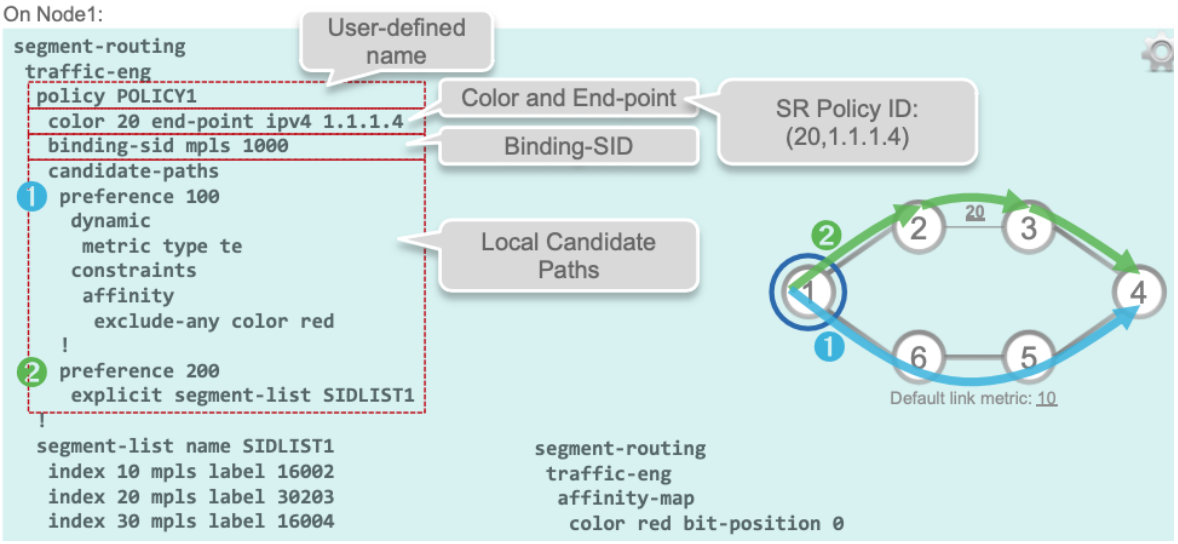


Figura 84. Configuración de paths en la SR Policy
Fuente: (Filsfils & Michielsen, 2017)

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Luego de haber realizado la investigación bibliográfica se concluye que, *Segment Routing* presenta grandes ventajas para las redes de transporte de los Proveedores de Servicios, puesto que gracias sus características no es necesario utilizar protocolos adicionales a MPLS como son LDP para la asignación y transporte de etiquetas o RSVP para proveer aplicaciones como por ejemplo *Traffic Engineering*. Por lo tanto, el rendimiento de los equipos mejora puesto que deben procesar menor cantidad de datos para el reenvío de los paquetes y además se evita inundar la red con etiquetas innecesarias.

- *Segment Routing* basa su funcionamiento en extensiones que se han agregado a los protocolos *link-state* IS-IS y OSPF. En el caso de IS-IS utiliza nuevos TLVs como son el *Prefix Segment Identifier* (Prefix-SID), *Adjacency Segment ID* (Adj-SID) y el SID/Label que contiene un SID o una etiqueta MPLS.

- Luego del desarrollo de la prueba de concepto se concluye que es factible el diseño de una red IP MPLS utilizando *Segment Routing* para un Proveedor de Servicios de Telecomunicaciones mediante un emulador de infraestructura de red, puesto que, se ha implementado la red y comprobado que existe conectividad entre cada sitio del cliente sin la necesidad de utilizar LDP para la asignación y reenvío de etiquetas.

- El diseño propuesto fue exitoso ya que, es posible brindar las mismas funcionalidades de una red MPLS tradicional, pero aprovechando las ventajas que representa utilizar *Segment Routing* ya que, del análisis realizado se evidencia que los valores latencia y jitter tienen una mejora sustancial, lo cual representa una optimización en el rendimiento de la red del Proveedor de Servicios. Además, para *Traficc Engineering* brinda la posibilidad de trabajar con interfaces túnel, así como también, permite trabajar con políticas, lo que amplía las opciones para controlar el flujo del tráfico y permite optimizar la utilización de los recursos existentes.

- La implementación de MPLS con *Segment Routing* resulta ser más sencilla que MPLS con LDP y RSVP, puesto que, no hace falta configurar los protocolos adicionales, reduciendo de esta manera la cantidad de comandos a configurar y por ende la complejidad.

- *Segment Routing* y LDP pueden coexistir dentro de una red MPLS, sin embargo, LDP siempre tendrá preferencia a menos que explícitamente se dé preferencia a *Segment Routing*.

RECOMENDACIONES

- Se recomienda que los Proveedores de Servicios analicen la posibilidad de implementar en sus redes MPLS la tecnología *Segment Routing*, con el objetivo de optimizar los recursos de la red y el proceso de reenvío de la información, puesto que como se ha podido evidenciar, esta tecnología presenta grandes ventajas con respecto a utilizar MPLS con LDP de forma tradicional.

- Se recomienda realizar investigaciones sobre la implementación de otras aplicaciones en las redes de los Proveedores de Servicios utilizando *Segment Routing*. Esto permitirá profundizar el presente estudio y atender la demanda de nuevos servicios de acuerdo con el avance de la tecnología o requerimientos de los clientes.

- Para la emulación de las topologías se recomienda utilizar una máquina virtual con mínimo 16 Gb de memoria RAM, que permita implementar la cantidad de equipos requeridos, principalmente para trabajar con los equipos Cisco ASR9K que tienen el sistema operativo XR y que requieren gran cantidad de memoria para arrancar.

- *Segment Routing Mapping Server* (SRMS) es un componente clave para la inter-operabilidad entre LDP y *Segment Routing*, puesto que permite que los nodos con capacidad SR interactúen con los nodos normales LDP. En este sentido, se recomienda realizar una investigación profunda de este tema con el objetivo de realizar una transición entre estas 2 tecnologías, con miras a una migración total a *Segment Routing*.

REFERENCIAS

Cisco. (2014). *SP CORE - Implementing Cisco Service Provider Next-Generation Core Network Services*.

Cisco. (2023). *Implementing and Operating Cisco Service Provider Network Core Technologies (SPCORE)*.

Edgeworth, B., Foss, A., & Garza Ríos, R. (2015). *IP Routing on Cisco IOS, IOS XE, and IOS XR*.

Edson Hernández. (2020). *Cisco MPLS LDP Rango de etiquetas especiales o reservadas*. https://www.youtube.com/watch?v=YZV9uKAyjYo

Hesselbach, X., Huerta, M., & Calderón, O. (2014). *Problemas abiertos en MPLS. Migración, Protección, Gestión de Recursos y Balanceo de Carga*.

IP Specialist. (2019, June). *Will MPLS go End of Life (EOL) soon?* https://medium.com/@ipspecialist/will-mpls-go-end-of-life-eol-soon-a7e4e4a9c21

Joskowicz, J. (2015). *Breve historia de las Telecomunicaciones*.

Sánchez Monge, A., & Szarkowicz, K. (2015). *MPLS in the SDN Era*.

The Cisco Learning Network. (2018). *Introducción a Segment Routing*. https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKD4EAO/introducci%C3%B3n-a-segment-routing

Salazar-Chacón, G. (2022). *Hybrid Networking SDN and SD-WAN: Traditional Network Architectures and Software-Defined Networks Interoperability in digitization era. Journal of Computer Science and Technology*.

Filsfils, C., & Michielsen, K. (2017). *SR Traffic-Engineering*.

EVE-NG. (2023). *EVE-NG*. https://www.eve-ng.net/

Ch, G. D. S., Naranjo, E. F., & Marrone, L. (2018, November). *SDN-Ready WAN networks: Segment Routing in MPLS-Based Environments. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*.

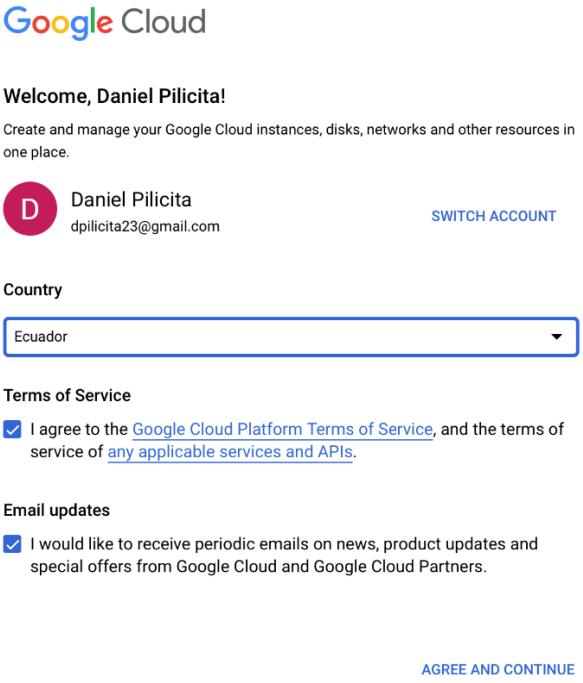
Santos, V. (2019, April 3). *Simplifique su red IP con Segment Routing centralizado, que es parte de Adaptive IP de Ciena*. https://www.ciena.com.mx/insights/articles/Simplify-your-IP-network-with-centralized-Segment-Routing-part-of-Cienas-Adaptive-IP_es_LA.html

Salazar-Chacón, G. D., & García, A. R. R. (2021, April). *Segment-Routing Analysis: Proof-of-Concept Emulation in IPv4 and IPv6 Service Provider Infrastructures.* In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

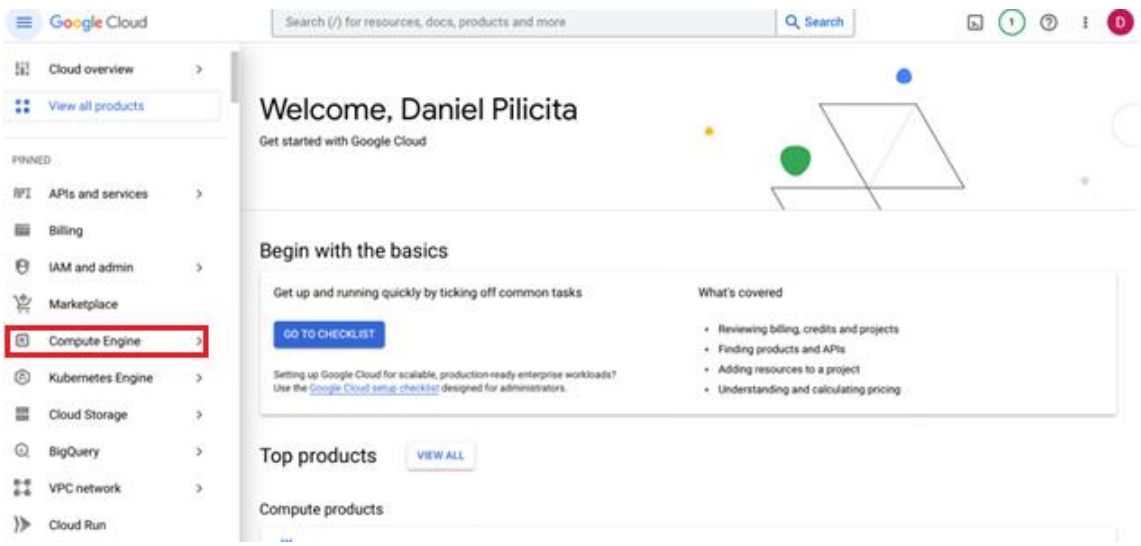
ANEXO 1

INSTALACIÓN DE EVE-NG

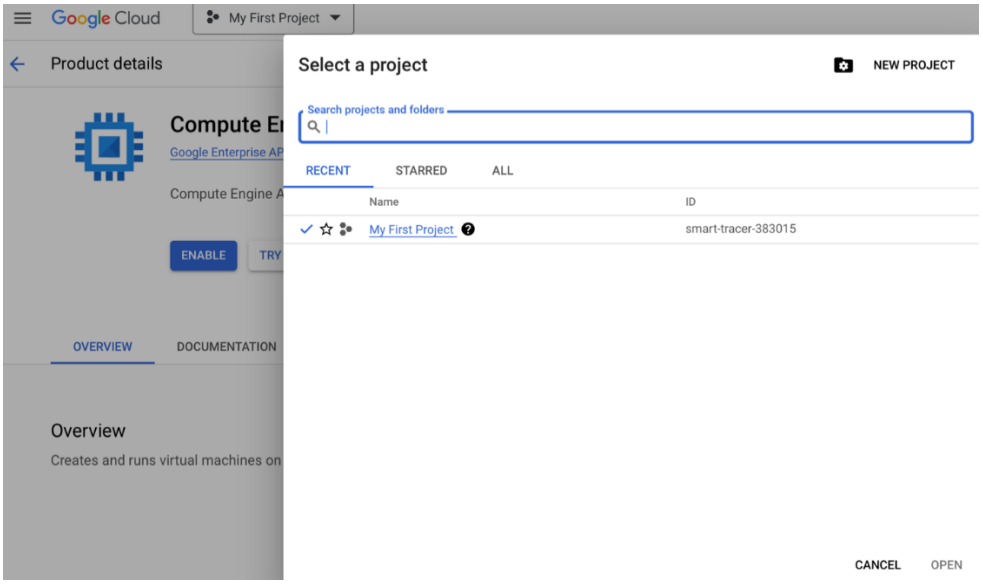
Creación de la cuenta de Google Cloud:



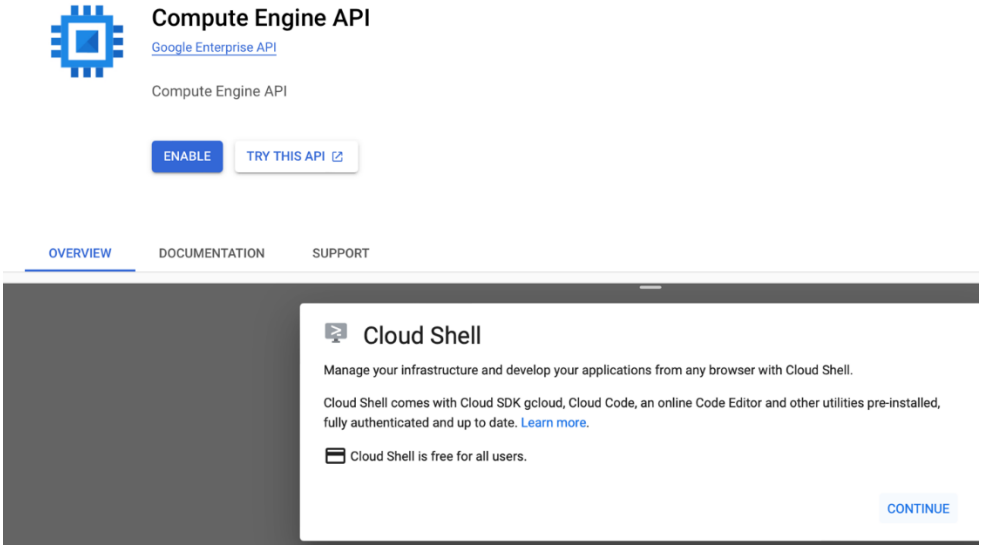
Pantalla principal de Google Cloud:



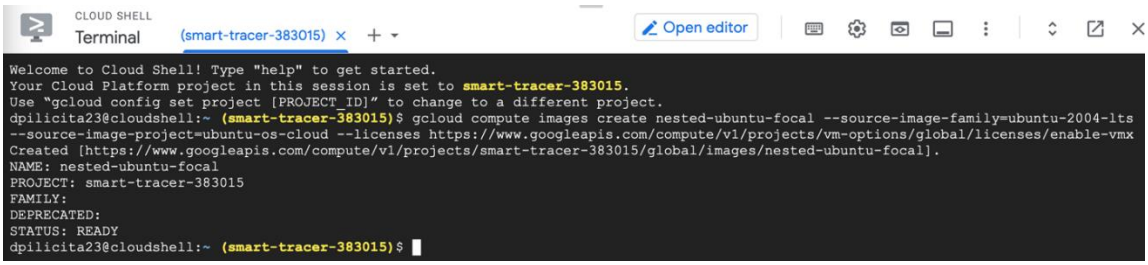
Creación de un proyecto



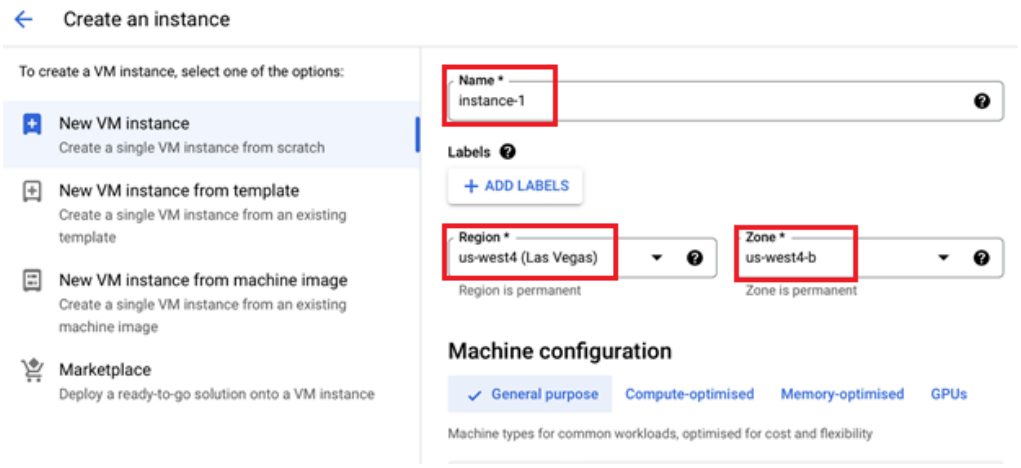
Acceso al Cloud Shell



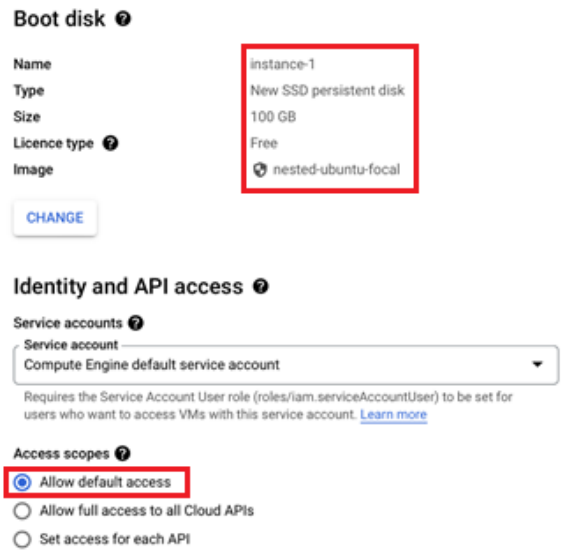
Cargando imagen desde el Cloud Shell:



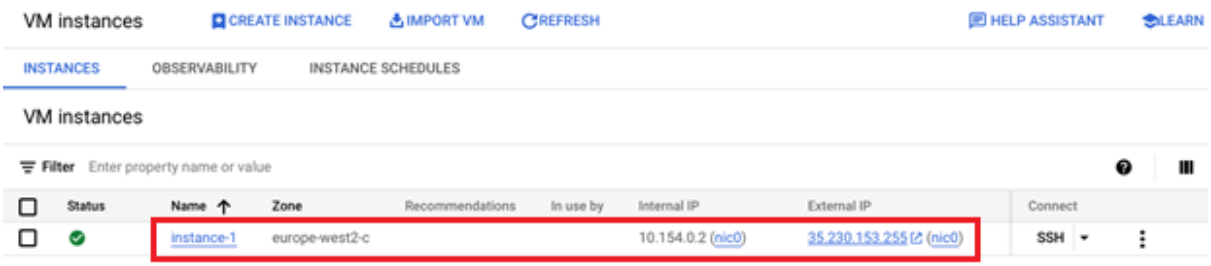
Creación de una instancia:



Configuración del Disco de Arranque:



Instancia creada:



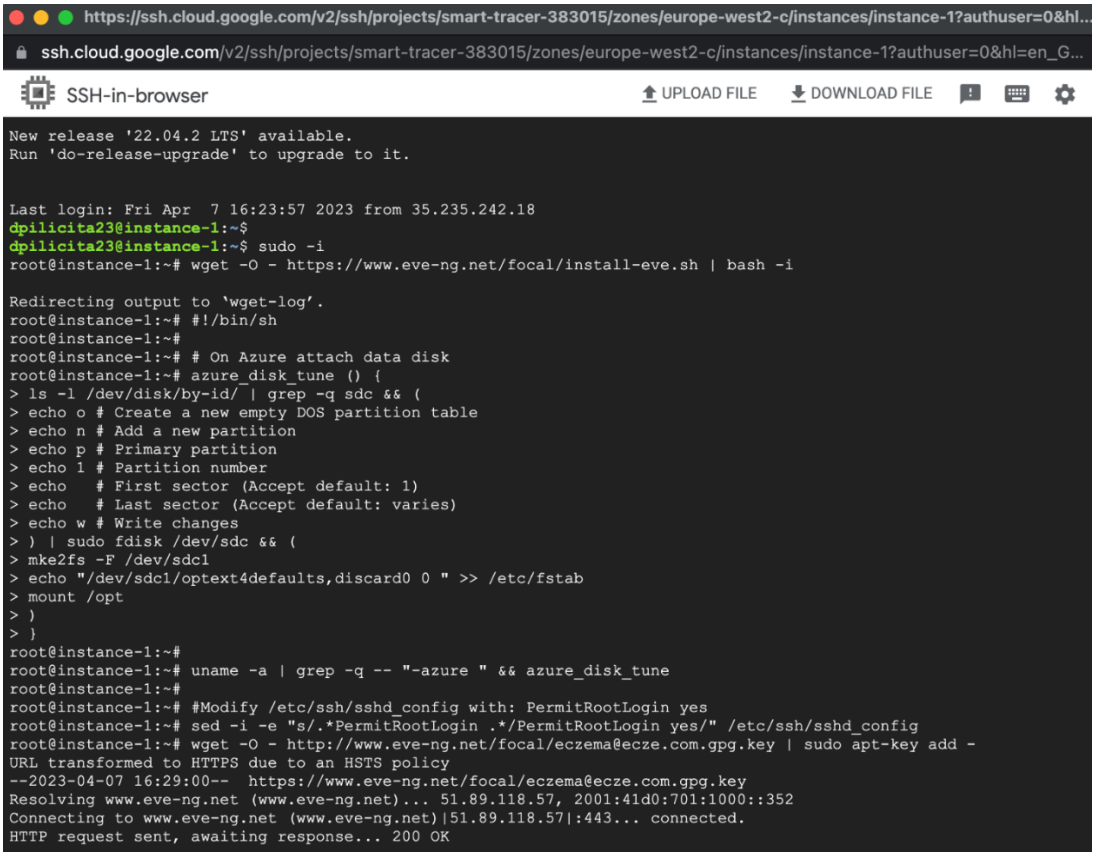
Instalación de EVENG

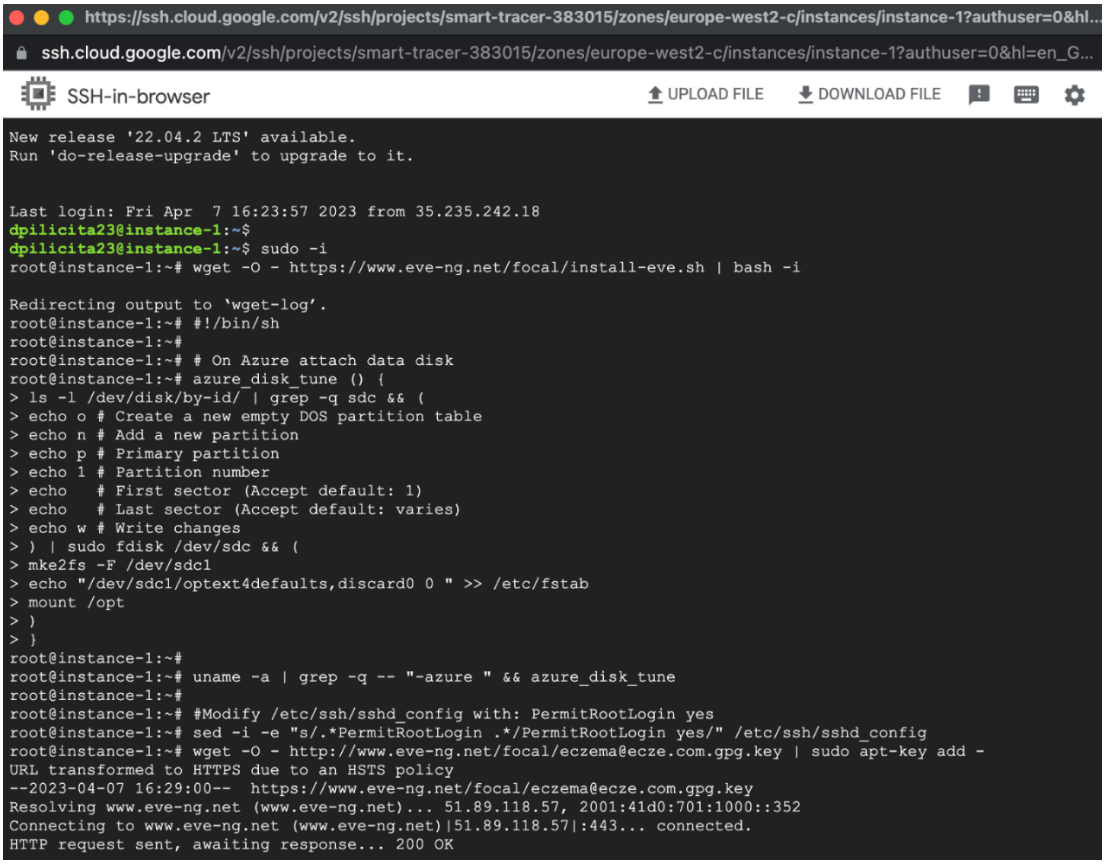
Mediante el ingreso del siguiente comando se cambia a usuario **root**:

sudo -i

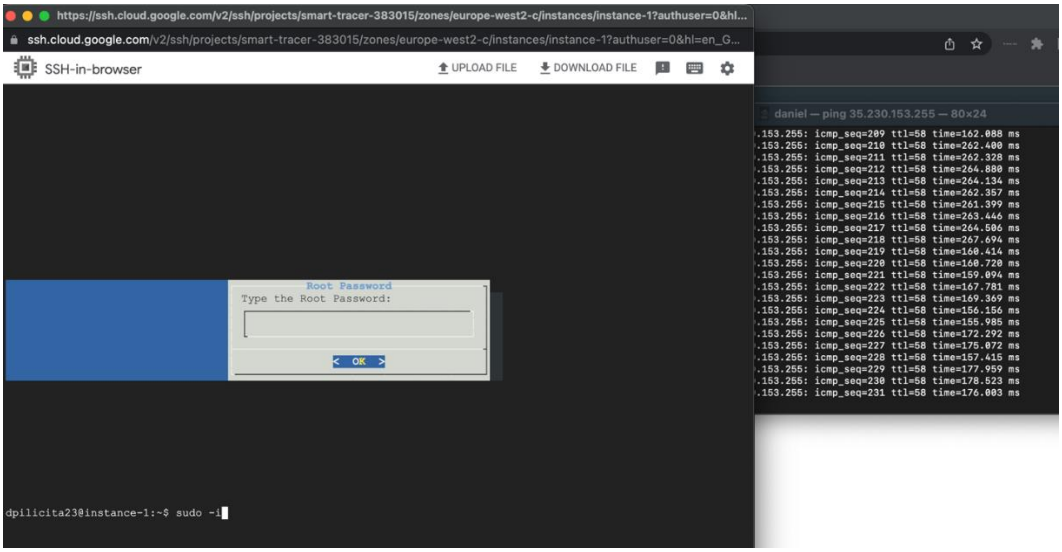
Comando para iniciar la instalación de EVE-NG:

wget -O - https://www.eve-ng.net/focal/install-eve.sh | bash -i

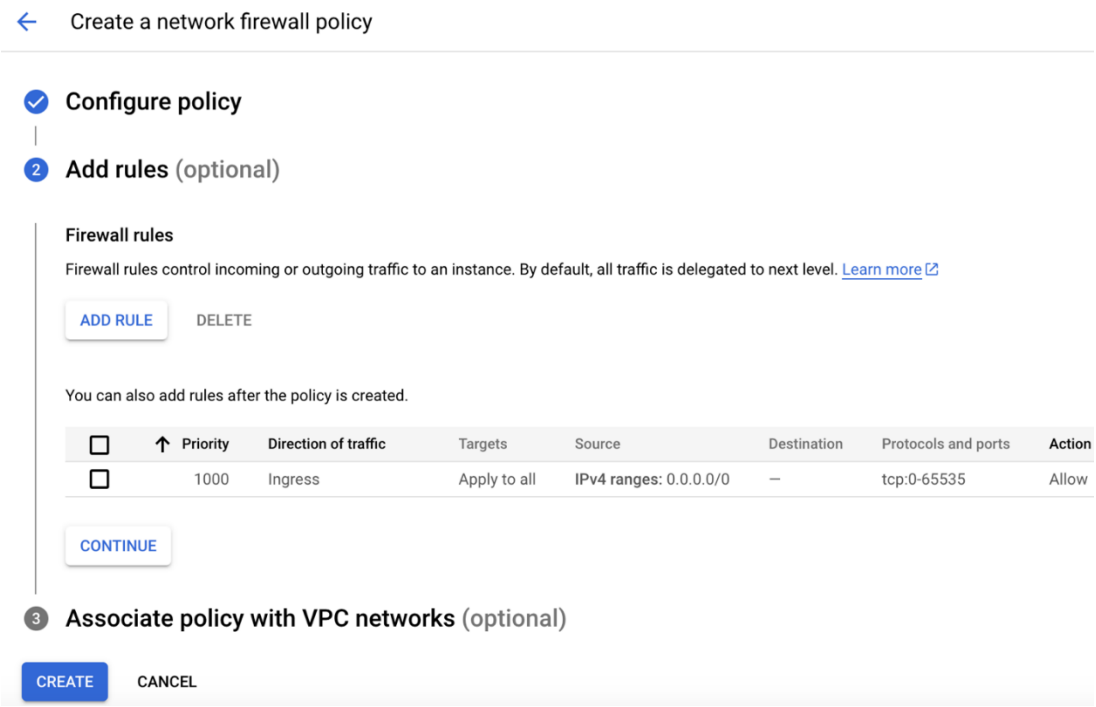




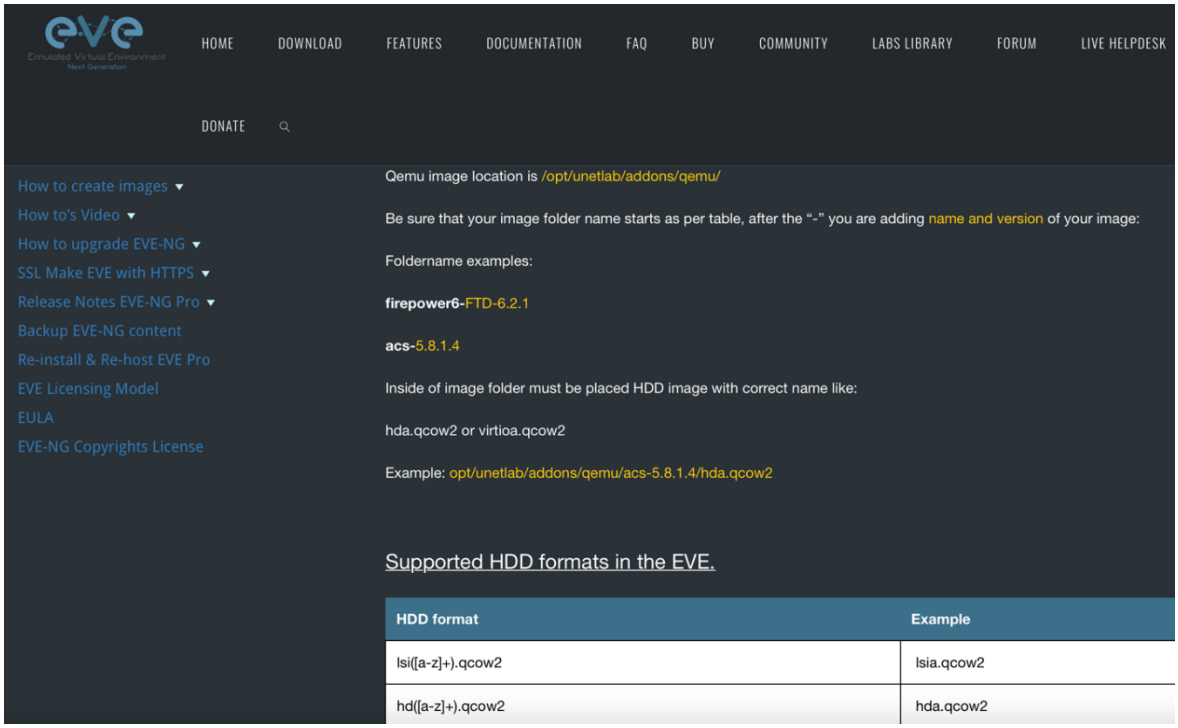
Seteo de contraseña para conexión con el servidor FTP:



Configuración de políticas de entrada y salida en el Firewall:

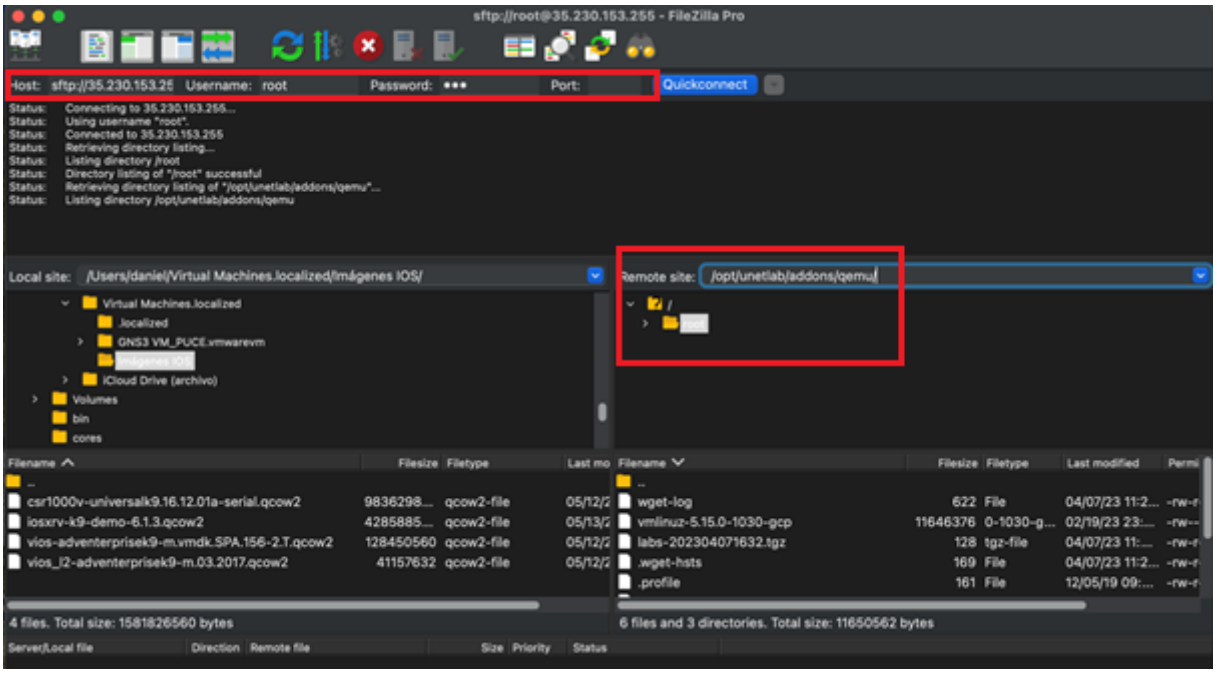


Documentación de EVENG para la carga de imágenes de equipos a utilizar donde se indica los nombres de las carpetas contenedoras y las extensions que los archivos deben tener (EVE-NG, 2023):

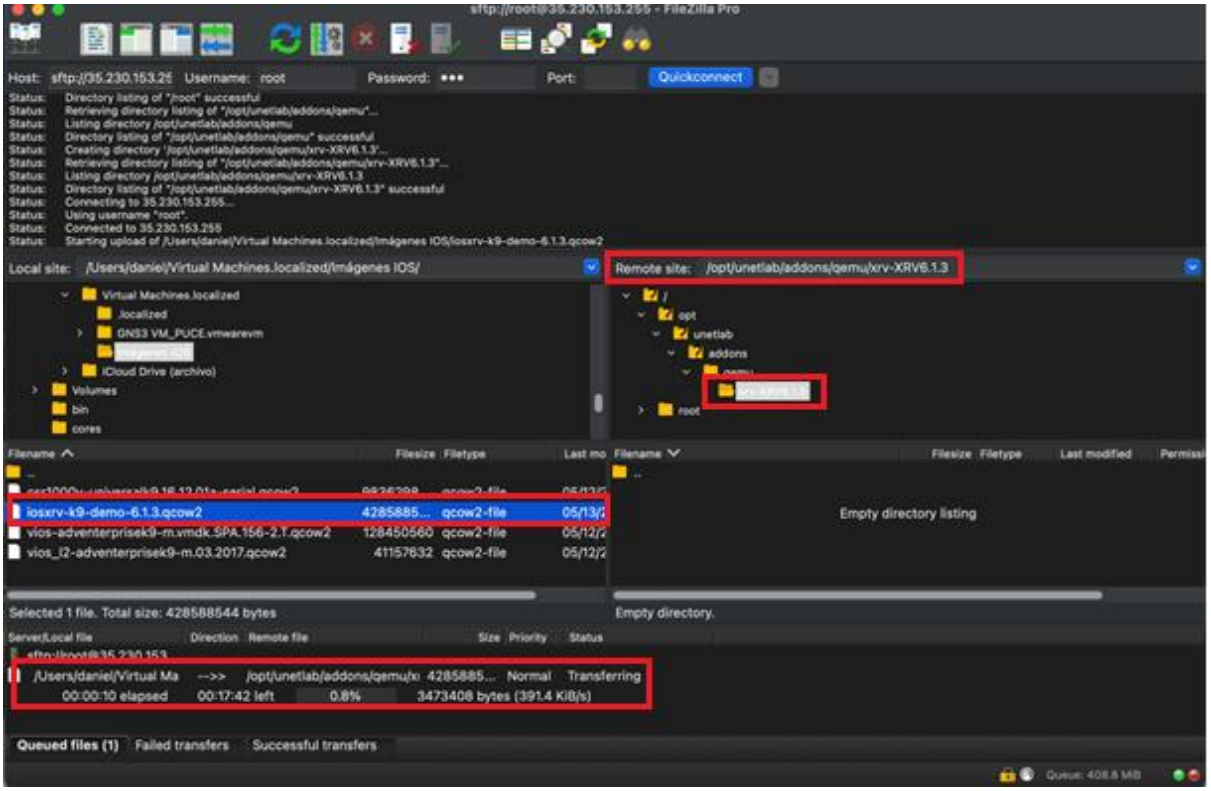


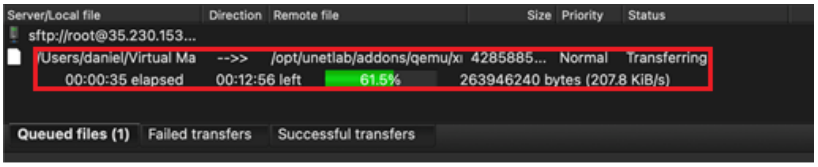
Qemu folder name EVE	Vendor	Qemu image .qcow2 name
vios-	L3 vIOS Cisco Router	virtioa
xrv-	XRv Cisco router	hda

Carga de imágenes mediante FileZilla de equipos a utilizar:

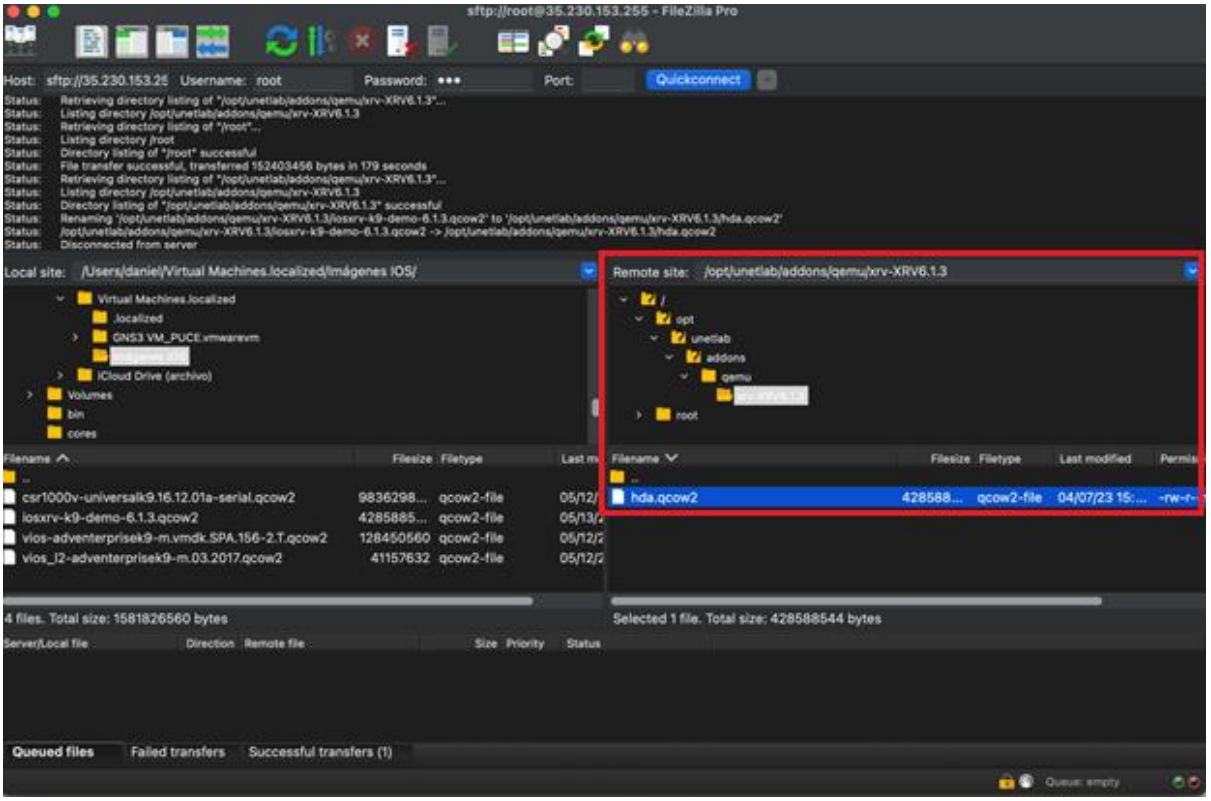


Carga de imagen del equipo Cisco ASR9K con Sistema Operativo XR:

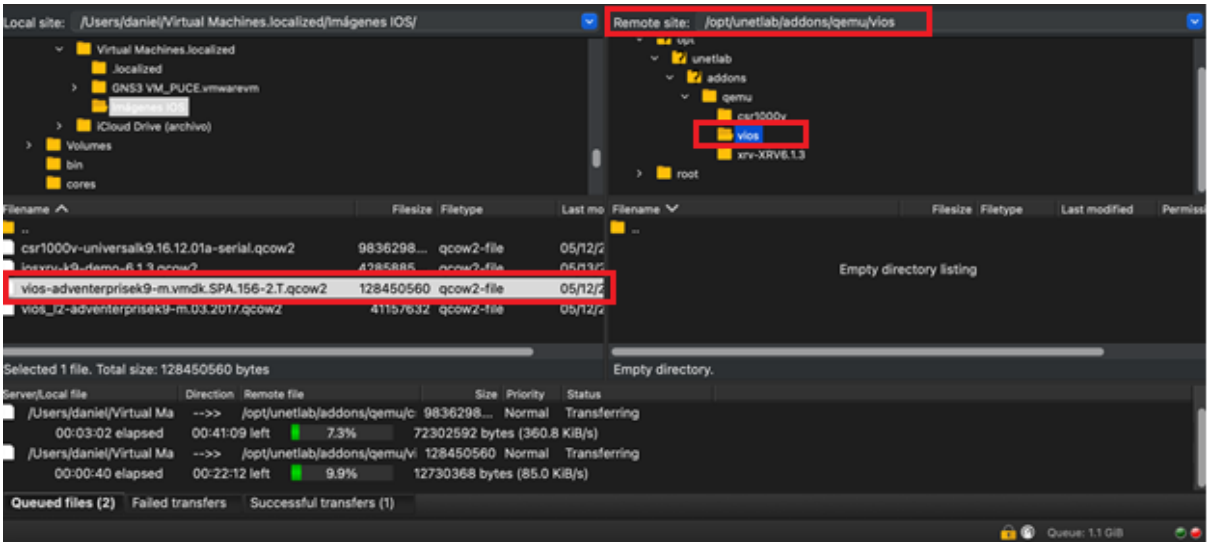




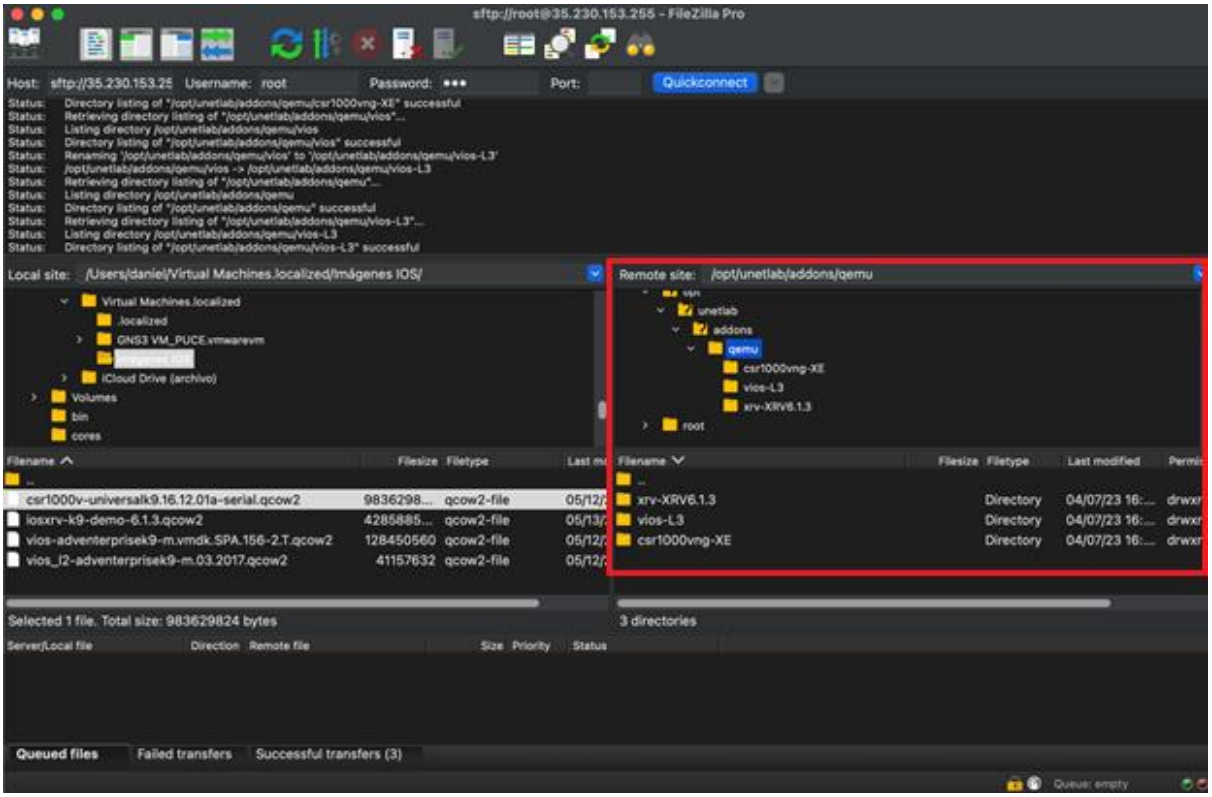
Instalación completa:



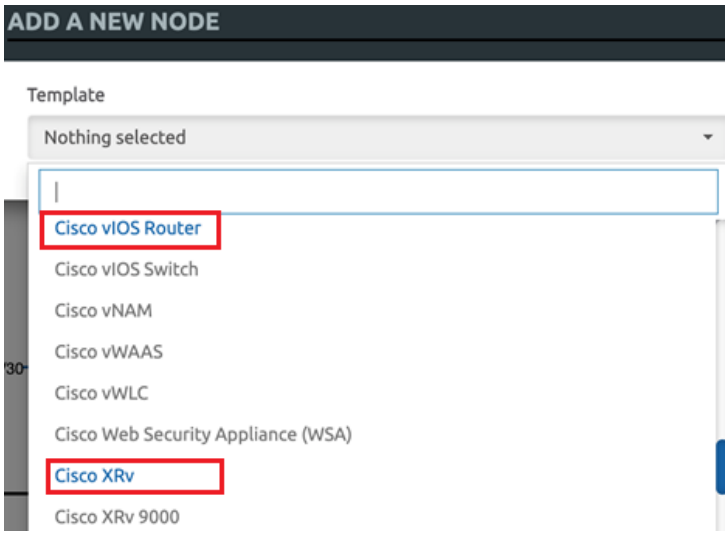
Carga de equipo Cisco con Sistema Operativo IOS:



Imágenes instaladas de equipos a utilizar en la emulación:



Verificación de imágenes cargadas:



El color azul en la descripción de los equipos indica que se encuentran disponibles para utilizar en el emulador.

ANEXO 2

CONFIGURACIÓN DE EQUIPOS MPLS

ESCENARIO 1: MPLS + LDP

Router Provider Edge PE1:

```
hostname PE1
banner motd /
******************************************************************************
 ADVERTENCIA!

 EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO!!

 El acceso esta restringido unicamente para usuarios autorizados y con
 propositos autorizados. El uso no autorizado o indebido puede resultar
 en acciones administrativas disciplinarias asi como en sanciones
 civiles y penales.
 Al continuar utilizando este sistema, usted indica que es consiente
 Y acepta los terminos y condiciones de uso de este sistema

******************************************************************************

================================================================================

  *****  *   *   ****   *****   | PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
  *   * *   *  *     *     *    |              PUCE
  *****  *   *  *     ****    | MAESTRIA EN TECNOLOGIAS DE LA INFORMACION
  *     *   *  *     *     *    |         REDES DE COMUNICACIONES
  *     ****   ****   *****  |               PE1

================================================================================
/
explicit-path name PE1_P1_P2_PE3
 index 1 next-address strict ipv4 unicast 10.1.11.2
 index 2 next-address strict ipv4 unicast 10.1.2.2
 index 3 next-address strict ipv4 unicast 10.2.13.2
!
explicit-path name PE1_P1_P4_PE4
 index 1 next-address strict ipv4 unicast 10.1.11.2
 index 2 next-address strict ipv4 unicast 10.1.4.2
 index 3 next-address strict ipv4 unicast 10.4.14.2
!
explicit-path name PE1_P3_P4_PE3
 index 1 next-address strict ipv4 unicast 10.3.11.2
```

```
 index 2 next-address strict ipv4 unicast 10.3.4.2
 index 3 next-address strict ipv4 unicast 10.4.13.2
!
interface Loopback0
 ipv4 address 10.0.0.11 255.255.255.255
!
interface tunnel-te1213
 ipv4 unnumbered Loopback0
 destination 10.0.0.13
 record-route
 path-option 30 explicit name PE1_P1_P2_PE3
 path-option 40 dynamic
!
interface tunnel-te1414
 ipv4 unnumbered Loopback0
 destination 10.0.0.14
 record-route
 path-option 10 explicit name PE1_P1_P4_PE4
 path-option 20 dynamic
!
interface tunnel-te3413
 ipv4 unnumbered Loopback0
 autoroute announce
 !
 destination 10.0.0.13
 record-route
 path-option 10 explicit name PE1_P3_P4_PE3
 path-option 20 dynamic
!
interface MgmtEth0/0/CPU0/0
 shutdown
!
interface GigabitEthernet0/0/0/0
 shutdown
!
interface GigabitEthernet0/0/0/1
 description ###LINK_TO_CE1_Gi0/1_1G###
 mtu 2014
 ipv4 address 10.11.10.1 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 description ###LINK_TO_PE2_Gi0/0/0/2_1G###
 mtu 2014
 ipv4 address 10.11.12.1 255.255.255.252
```

```
!
interface GigabitEthernet0/0/0/3
 description ###LINK_TO_P3_Gi0/0/0/3_1G###
 mtu 2014
 ipv4 address 10.3.11.2 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 description ###LINK_TO_P1_Gi0/0/0/4_1G###
 mtu 2014
 ipv4 address 10.1.11.2 255.255.255.252
!
interface GigabitEthernet0/0/0/5
 shutdown
!
interface GigabitEthernet0/0/0/6
 shutdown
!
route-policy RPL_PASS_BGP
  pass
end-policy
!
router isis MTI
 is-type level-2-only
 net 49.0001.0100.0000.0011.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  mpls ldp auto-config
 !
 interface Loopback0
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/1
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/2
  circuit-type level-2-only
  address-family ipv4 unicast
  !
```

```
 !
 interface GigabitEthernet0/0/0/3
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/4
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/5
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
!
router bgp 64512
 address-family ipv4 unicast
  network 10.0.0.11/32
 !
 neighbor 10.0.0.99
  remote-as 64512
  update-source Loopback0
  address-family ipv4 unicast
  !
 !
 neighbor 10.11.10.2
  remote-as 64513
  address-family ipv4 unicast
   route-policy RPL_PASS_BGP in
   route-policy RPL_PASS_BGP out
  !
 !
!
rsvp
 interface GigabitEthernet0/0/0/1
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/2
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/3
  bandwidth 800000
```

```
 !
 interface GigabitEthernet0/0/0/4
  bandwidth 800000
 !
!
mpls traffic-eng
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
mpls ldp
 router-id 10.0.0.11
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
 mpls label range table 0 24000 24999
 end
```

Router Provider P1:

```
 hostname P1
 banner motd /
 ******************************************************************************
   ADVERTENCIA!

   EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO!!

   El acceso esta restringido unicamente para usuarios autorizados y con
   propositos autorizados. El uso no autorizado o indebido puede resultar
   en acciones administrativas disciplinarias asi como en sanciones
   civiles y penales.
   Al continuar utilizando este sistema, usted indica que es consiente
   Y acepta los terminos y condiciones de uso de este sistema
```

```
 ***************************************************************************

=============================================================================================

   *****  *   *   ****   *****   | PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
   *   * *   * *     *     |              PUCE
   *****  *   * *     ****   | MAESTRIA EN TECNOLOGIAS DE LA INFORMACION
   *     *   * *     *     |         REDES DE COMUNICACIONES
   *      ****   ****   *****  |               P1

=============================================================================================
/
interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255
!
interface MgmtEth0/0/CPU0/0
 shutdown
!
interface GigabitEthernet0/0/0/0
 description ###LINK_TO_P2_Gi0/0/0/0_1G###
 mtu 2014
 ipv4 address 10.1.2.1 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 description ###LINK_TO_P4_Gi0/0/0/1_1G###
 mtu 2014
 ipv4 address 10.1.4.1 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 description ###LINK_TO_P3_Gi0/0/0/2_1G###
 mtu 2014
 ipv4 address 10.1.3.1 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 description ###LINK_TO_PE2_Gi0/0/0/3_1G###
 mtu 2014
 ipv4 address 10.1.12.1 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 description ###LINK_TO_PE1_Gi0/0/0/4_1G###
 mtu 2014
 ipv4 address 10.1.11.1 255.255.255.252
```

```
!
interface GigabitEthernet0/0/0/5
 description ###LINK_TO_RR_Gi0/0/0/0_1G###
 mtu 2014
 ipv4 address 10.1.99.1 255.255.255.252
!
interface GigabitEthernet0/0/0/6
 shutdown
!
router isis MTI
 is-type level-2-only
 net 49.0000.0100.0000.0001.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  mpls ldp auto-config
 !
 interface Loopback0
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/1
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/2
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/3
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
```

```
 interface GigabitEthernet0/0/0/4
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/5
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
!
router bgp 64512
 address-family ipv4 unicast
  network 10.0.0.1/32
 !
 neighbor 10.0.0.99
  remote-as 64512
  update-source Loopback0
  address-family ipv4 unicast
  !
 !
!
rsvp
 interface GigabitEthernet0/0/0/0
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/1
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/2
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/3
  bandwidth 800000
 !
 interface GigabitEthernet0/0/0/4
  bandwidth 800000
 !
!
mpls traffic-eng
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
```

```
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
mpls ldp
 router-id 10.0.0.1
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
mpls label range table 0 31000 31999
end
```

Router Customer Edge CE1 (Cliente):

```
hostname CE1
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 description ###LINK_TO_PE1_Gi0/0/0/1_1G###
 ip address 10.11.10.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
```

```
 description ###LINK_TO_PE2_Gi0/0/0/1_1G###
 ip address 10.12.10.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
router bgp 64513
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 neighbor 10.11.10.1 remote-as 64512
 neighbor 10.12.10.1 remote-as 64512
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CCCCC
**************************************************************************
  ADVERTENCIA!
  EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO!!
  El acceso esta restringido unicamente para usuarios autorizados y con
  propositos autorizados. El uso no autorizado o indebido puede resultar
  en acciones administrativas disciplinarias asi como en sanciones
  civiles y penales.
  Al continuar utilizando este sistema, usted indica que es consiente
  Y acepta los terminos y condiciones de uso de este sistema
 **************************************************************************
==========================================================================================

   *****  *   *   ****   *****   | PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
   *   * *   *  *      *      |              PUCE
   *****  *   *  *      ****    | MAESTRIA EN TECNOLOGIAS DE LA INFORMACION
   *      *   *  *      *      |         REDES DE COMUNICACIONES
   *      ****   ****   *****  |               CE1
```

```
==========================================================================================
^C
!
line con 0
line aux 0
line vty 0 4
 login
 transport input none
!
no scheduler allocate
!
end
```

ESCENARIO 2: MPLS + SEGMENT ROUTING

Router Provider Edge PE1:

```
hostname PE1
banner motd /
**************************************************************************
  ADVERTENCIA!

  EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO!!

  El acceso esta restringido unicamente para usuarios autorizados y con
  propositos autorizados. El uso no autorizado o indebido puede resultar
  en acciones administrativas disciplinarias asi como en sanciones
  civiles y penales.
  Al continuar utilizando este sistema, usted indica que es consiente
  Y acepta los terminos y condiciones de uso de este sistema

 **************************************************************************

==========================================================================================

   *****  *   *   ****   *****   | PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
   *   * *   * *     *     |              PUCE
   *****  *   *  *     ****   | MAESTRIA EN TECNOLOGIAS DE LA INFORMACION
   *     *   *  *     *     |         REDES DE COMUNICACIONES
   *     ****   ****   *****  |              PE1

==========================================================================================
/
explicit-path name 1213
 index 1 next-label 16001
```

```
 index 2 next-label 16002
 index 3 next-label 16013
!
explicit-path name 1414
 index 1 next-label 16001
 index 2 next-label 16004
 index 3 next-label 16014
!
explicit-path name 3413
 index 1 next-label 16003
 index 2 next-label 16004
 index 3 next-label 16013
!
interface Loopback0
 ipv4 address 10.0.0.11 255.255.255.255
!
interface tunnel-te1213
 ipv4 unnumbered Loopback0
 autoroute announce
 !
 destination 10.0.0.13
 path-option 1 explicit name 1213 segment-routing
!
interface tunnel-te1414
 ipv4 unnumbered Loopback0
 destination 10.0.0.14
 path-option 1 explicit name 1414 segment-routing
!
interface tunnel-te3413
 ipv4 unnumbered Loopback0
 destination 10.0.0.13
 path-option 1 explicit name 3413 segment-routing
!
interface MgmtEth0/0/CPU0/0
 shutdown
!
interface GigabitEthernet0/0/0/0
 shutdown
!
interface GigabitEthernet0/0/0/1
 description ###LINK_TO_CE1_Gi0/1_1G###
 mtu 2014
 ipv4 address 10.11.10.1 255.255.255.252
!
```

```
interface GigabitEthernet0/0/0/2
 description ###LINK_TO_PE2_Gi0/0/0/2_1G###
 mtu 2014
 ipv4 address 10.11.12.1 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 description ###LINK_TO_P3_Gi0/0/0/3_1G###
 mtu 2014
 ipv4 address 10.3.11.2 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 description ###LINK_TO_P1_Gi0/0/0/4_1G###
 mtu 2014
 ipv4 address 10.1.11.2 255.255.255.252
!
interface GigabitEthernet0/0/0/5
 shutdown
!
interface GigabitEthernet0/0/0/6
 shutdown
!
route-policy RPL_PASS_BGP
  pass
end-policy
!
router isis MTI
 is-type level-2-only
 net 49.0001.0100.0000.0011.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  router-id Loopback0
  segment-routing mpls
 !
 interface Loopback0
  passive
  address-family ipv4 unicast
   prefix-sid absolute 16011
  !
 !
 interface GigabitEthernet0/0/0/1
  circuit-type level-2-only
```

```
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/2
 circuit-type level-2-only
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/3
 circuit-type level-2-only
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/4
 circuit-type level-2-only
 address-family ipv4 unicast
 !
!
interface GigabitEthernet0/0/0/5
 circuit-type level-2-only
 address-family ipv4 unicast
 !
!
!
router bgp 64512
 address-family ipv4 unicast
  network 10.0.0.11/32
 !
 neighbor 10.0.0.99
  remote-as 64512
  update-source Loopback0
  address-family ipv4 unicast
  !
 !
 neighbor 10.11.10.2
  remote-as 64513
  address-family ipv4 unicast
   route-policy RPL_PASS_BGP in
   route-policy RPL_PASS_BGP out
  !
 !
!
mpls traffic-eng
 interface GigabitEthernet0/0/0/2
```

```
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
segment-routing
 global-block 16000 23999
!
end
```

Router Provider P1:

```
hostname P1
banner motd /
**************************************************************************
 ADVERTENCIA!

 EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO!!

 El acceso esta restringido unicamente para usuarios autorizados y con
 propositos autorizados. El uso no autorizado o indebido puede resultar
 en acciones administrativas disciplinarias asi como en sanciones
 civiles y penales.
 Al continuar utilizando este sistema, usted indica que es consiente
 Y acepta los terminos y condiciones de uso de este sistema

**************************************************************************

==========================================================================================

  *****  *   *   ****   *****   | PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
  *   * *   *  *     *     |              PUCE
  *****  *   *  *     ****   | MAESTRIA EN TECNOLOGIAS DE LA INFORMACION
  *     *   *  *     *     |         REDES DE COMUNICACIONES
  *      ****   ****   *****  |              P1

==========================================================================================
/
interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255
!
interface MgmtEth0/0/CPU0/0
 shutdown
!
```

```
interface GigabitEthernet0/0/0/0
 description ###LINK_TO_P2_Gi0/0/0/0_1G###
 mtu 2014
 ipv4 address 10.1.2.1 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 description ###LINK_TO_P4_Gi0/0/0/1_1G###
 mtu 2014
 ipv4 address 10.1.4.1 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 description ###LINK_TO_P3_Gi0/0/0/2_1G###
 mtu 2014
 ipv4 address 10.1.3.1 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 description ###LINK_TO_PE2_Gi0/0/0/3_1G###
 mtu 2014
 ipv4 address 10.1.12.1 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 description ###LINK_TO_PE1_Gi0/0/0/4_1G###
 mtu 2014
 ipv4 address 10.1.11.1 255.255.255.252
!
interface GigabitEthernet0/0/0/5
 description ###LINK_TO_RR_Gi0/0/0/0_1G###
 mtu 2014
 ipv4 address 10.1.99.1 255.255.255.252
!
interface GigabitEthernet0/0/0/6
 shutdown
!
router isis MTI
 is-type level-2-only
 net 49.0000.0100.0000.0001.00
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  router-id Loopback0
  segment-routing mpls
 !
```

```
 interface Loopback0
  passive
  address-family ipv4 unicast
   prefix-sid index 1
  !
 !
 interface GigabitEthernet0/0/0/0
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/1
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/2
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/3
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/4
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/0/0/5
  circuit-type level-2-only
  address-family ipv4 unicast
  !
 !
!
router bgp 64512
 address-family ipv4 unicast
  network 10.0.0.1/32
 !
 neighbor 10.0.0.99
  remote-as 64512
  update-source Loopback0
```

```
  address-family ipv4 unicast
  !
 !
!
mpls traffic-eng
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
segment-routing
 global-block 16000 23999
!
end
```