UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

CASO DE ESTUDIO DE UN OPERADOR DE TELECOMUNICACIONES EN CHILE: EVALUACIÓN TÉCNICA/ECONÓMICA DEL DESPLIEGUE DEL PROTOCOLO BGP-LU EN UNA RED DE DATOS.

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELÉCTRICO

VICTOR IGNACIO PALMA RODRIGUEZ

PROFESOR GUÍA:
Juan Acevedo Gilmore

MIEMBROS DE LA COMISIÓN:
Daniel Viveros Sepulveda
Alvaro Silva Madrid

SANTIAGO DE CHILE
2023

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE INGENIERO CIVIL ELÉCTRICO
POR: VICTOR IGNACIO PALMA RODRIGUEZ
FECHA: 2023
PROF. GUÍA: Juan Acevedo Gillmore

CASO DE ESTUDIO DE UN OPERADOR DE TELECOMUNICACIONES EN CHILE: EVALUACIÓN TÉCNICA/ECONÓMICA DEL DESPLIEGUE DEL PROTOCOLO BGP-LU EN UNA RED DE DATOS.

Los proveedores de servicios de Internet (ISP) buscan mejorar y optimizar sus redes utilizando tecnologías que logren este objetivo con la menor complejidad posible. El presente informe de memoria de título tiene como objetivo llevar a cabo una evaluación técnica y económica de la implementación del protocolo de enrutamiento BGP-LU, el cual busca optimizar la red de los ISP.

En la evaluación técnica, se realizaron simulaciones del caso de estudio utilizando el software eNSP, obteniendo resultados coherentes en tres escenarios diferentes los cuales son descritos en este trabajo. Desde el punto de vista económico, la implementación de BGP-LU muestra una reducción significativa en los gastos de capital y de los gastos operativos.

Los resultados muestran una clara disminución en las rutas de las tablas de los routers en la red, mostrando que los equipos implementados por los ISP no deben de tener un requerimiento computacional sobredimensionado. Por el lado económico, la implementación de BGP-LU reduce el CAPEX en un 89 % mientras el OPEX disminuye en un 95 %.

Para mi familia, amigos,
el futuro, la esperanza.

Saludos

Tabla de Contenido

Índice de Tablas

Índice de Ilustraciones

Capítulo 1

Introducción

El servicio de acceso a Internet se define como la forma de compartir información de un grupo de personas por medio de dispositivos, los cuales se conectan entre ellos para formar una red de telecomunicaciones. Estos servicios se han transformado en un factor de desarrollo en los países debido al acceso de información al alcance de la mano y al proceso de globalización. En el caso de Chile, el último informe del Banco Central, IPOM, se estima que aporta al 12,6 % del PIB lo que lo transforma en un motor de desarrollo importante en el país tanto como político, económico e incluso cultural [1].

En los informes mensuales del Ministerio de Transporte y Telecomunicaciones, el servicio de acceso a Internet tiene una penetración del 135,1 %; siendo los accesos fijos un 22,4 % y los accesos móviles un 112,7 % [2]. Las conexiones de acceso móvil representan una mayor cantidad que las fijas, esto a causa de que por habitante existe más de 1 dispositivo móvil con servicios de acceso a internet y la facilidad de obtener uno.

Las empresas que se dedican a proveer este servicio, también denominadas Proveedores de Servicios de Acceso a Internet (Internet Service Provider o ISP), continuamente han tenido que implementar tecnologías avanzadas con el fin de satisfacer los crecientes y constantes nuevos requerimientos del servicio, estos van desde un incremento en la cantidad de clientes y una mayor cantidad de información demandada por estos mismos. A esto se le denomina crecimiento en la cantidad de accesos y crecimiento del ancho de banda respectivamente, ambos conceptos son parte del crecimiento de la demanda de un ISP.

Dado que el ISP es una empresa que pertenece a un mercado altamente competitivo, debe implementar tecnologías avanzadas para satisfacer la demanda de los clientes y de esta forma obtener beneficios económicos a través de la comercialización de sus servicios. Los ISP buscan obtener la mayor utilidad alcanzable con la menor inversión posible, discerniendo entre las distintas tecnologías disponibles.

Los ISP están conformados por un conjunto de equipos de telecomunicaciones que permiten el transporte de información de un punto a otro, este conjunto se le denomina red. La red a su vez se divide jerárquicamente en tres partes según su función de Acceso, Agregación y Core. El cómo se organizan e interconectan dispositivos pertenecientes a estas divisiones, se le denomina topología de red.

En el acceso se encuentran equipos que permiten la conexión de los usuarios a la red de un ISP. En Agregación los usuarios son agrupados y transportados al Core.

Una de las principales funciones del Core es realizar el procesamiento final al destino de los usuarios en la red. Para lograr esta función, debe conocer todos los destinos posibles donde son organizados en una tabla, donde cada fila es su vecino al cual debe enviar la información para llegar al destino. Con el fin de crear esta tabla, se usa un lenguaje de comunicación llamado protocolo.

Este protocolo recopila e intercambia información de todos los equipos de la red. De esta manera, los equipos conocen la existencia de sus vecinos y de los equipos remotos que se encuentran en la red. Estos protocolos se denominan protocolo interior (IGP) o protocolo exterior (EGP), dependiendo de si se utilizan dentro o fuera de un sistema autónomo, que es un conjunto de equipos bajo una misma administración.

Cada equipo de red, ya sea de Acceso, Agregación o Core, tiene mínimo tres tablas: Tabla de vecindad, donde conoce todos los vecinos de un determinado protocolo, Tabla de ruteo, que es la elección de un determinado protocolo para llegar a un destino y la Tabla topológica que es la tabla que contiene toda la información de los distintos protocolos configurados en la red.

Cuando se requiere implementar un dispositivo que permita la conexión directa de usuarios a la red de un ISP, es lógico realizar una evaluación del caso, ya que estos equipos tienen ciertas limitaciones en términos de capacidad y alcance, especialmente cuando se trata de áreas rurales con una población demográfica media de hasta 32 mil habitantes en Chile. En estos casos, utilizar un equipo de alto rendimiento en cuanto a capacidad de procesamiento, memoria y dimensiones no resulta viable debido a su elevado costo. Por lo tanto, se busca una alternativa de equipos que cumplan con los requisitos necesarios y ofrezcan un mayor beneficio económico en comparación con los equipos sobredimensionados.

Sin embargo, los equipos de menor tamaño presentan la dificultad de no soportar la cantidad de rutas que se manejan en la red. Debido a esto es necesario encontrar una solución que permita aplicar este escenario sin comprometer el rendimiento y la funcionalidad del sistema.

Debido a que los ISP utilizan MPLS/IP como protocolos base de intercambio de información. En el caso de MPLS, este funciona por medio de los IGP, y junto a LDP (label Discovery Protocol) para el intercambio de etiquetas, hacen que las tablas de rutas sean muy extensas. Con el fin de optimizar el proceso de MPLS, nos centraremos en la evaluación técnica y económica de BGP-LU. BGP-LU es una extensión del protocolo BGP [3], el cual pertenece a la categoría de los EGP, donde su versión 4 es la más usada y difundida en Internet a nivel mundial.

La evaluación de la parte técnica del BGP-LU, se realizará por medio de la simulación de una red con el software eNSP perteneciente a la compañía Huawei. La evaluación del área económica, será analizando el aumento o disminución del CAPEX Y OPEX de un ISP al implementar BGP-LU en una red.

Esta memoria se centrará en esta última etapa, donde se evaluará, si tecnologías avanzadas,

desde un análisis técnico y económico, implementadas en el Core de la red, permiten tener un beneficio económico para un ISP.

1.1. Objetivos

1.1.1. Generales

Realizar una evaluación técnica y económica de la optimización de la red de un proveedor de múltiples servicios de acceso a Internet, con la implementación de nuevas tecnologías en el enrutamiento de paquetes, específicamente con el protocolo BGP-LU.

1.1.2. Específicos

1. Describir el funcionamiento del protocolo BGP-LU, y el cómo se aplica mediante junto a la tecnología actual de la red de un proveedor de servicios con acceso a internet .

2. Evaluar técnicamente el despliegue de configuración del protocolo BGP-LU, utilizando métricas correspondientes, donde se evidencie la optimización del número de rutas en las tablas de cada routers, mejorando también la eficiencia en el momento de enrutamiento de paquetes.

3. Evaluar económicamente, comparando el beneficio de implementar el despliegue protocolo BGP-LU, en comparación a la compra de nuevos routers los cuales soportan estas nuevas rutas.

Capítulo 2

Marco teórico

Las redes de datos de los ISPs estan conformadas por dispositivos de telecomunicaciones, como routers, switches, fibra óptica, entre otros. Estos dispositivos constituyen la topología de la red y se encargan de transportar la información de un punto a otro. La unidad de transporte de la información se define como un paquete o conjunto de paquetes de datos.

Con el fin de que los routers sean capaces de transportar la información, es necesario que conozcan una ruta dentro de la topología de la red que conduzca al destino deseado. Sin embargo, estos dispositivos solo tienen conocimiento de las rutas que están directamente conectadas físicamente a ellos. Por lo tanto, los routers intercambian información de sus tablas de de rutas con otros routers vecinos por medio de protocolos de enrutamiento. De esta forma, los routers determinan a qué vecino enviar el tráfico para llegar a su destino.

Una diferencia importante entre los protocolos de enrutamiento es la ubicación donde se aplican, es decir, si se utilizan dentro de un sistema autónomo se conooce como protocolo interno (IGP), y en el caso que se utilice entre sistemas autónomos distintos, se llama protocolo externo (EGP). Algunos ejemplos de estos protocolos son OSPF, LDP, BGP y RSVP-TE, cada uno de los cuales genera una tabla de enrutamiento única en cada router.

Existen dos tipos de protocolos de enrutamiento, segun el como aprenden las rutas: el estático y el dinámico.

El enrutamiento estático implica la configuración manual de rutas específicas en los routers, lo que requiere que todas las posibles rutas sean explícitamente definidas. Este enfoque no es escalable, es decir, es complicado cuando aumenta el número de routers a configurar. Además, no puede adaptarse a cambios en la red, como la caída de un enlace.

Por otro lado, el enrutamiento dinámico aprende rutas a través de constantes actualizaciones recibidas por routers vecinos, que permiten a los routers conocer cambios en la topología de red y adaptarse. Si un router detecta diferencias en su base de datos en comparación con otros dispositivos, agrega la nueva ruta y calcula el camino óptimo utilizando el algoritmo correspondiente, y si encuentra que la nueva ruta mejora el rendimiento, se actualiza en la tabla de enrutamiento. En caso contrario, no se realizan cambios.

2.1. Protocolo Dinámico

Los protocolos de enrutamiento dinámico al aplicarse en routers generan que estos puedan aprender rutas por medio del intercambio de información entre estos dispositivos. Este cambio se realiza por medio de mensajes que dependerán exclusivamente del protocolo de ruteo que se utilice, la función se realiza de tal forma que cuando se detectan cambios en la red, ya sea, el añadir o quitar un ruta predeterminada, se genera un intercambio

2.2. Internal gateway protocol (IGP)

Como se mencionó anteriormente los IGP actúan dentro de un sistema autónomo, siendo los más conocidos RIP, IS-IS, EIGRP y OSPF [4]. El Protocolo EIGRP es de uso exclusivo por su fabricante (CISCO), RIP e IS-IS son protocolos no tan comunes en las redes, siendo usados en tareas específicas. Mientras OSPF es implementado mayoritariamente por los diferentes proveedores de servicio en Chile.

El protocolo RIP utiliza la métrica de saltos para determinar la cantidad de routers que debe atravesar un paquete para llegar a su destino. Sin embargo, tiene un límite máximo de 16 saltos, lo que puede resultar problemático en redes de gran tamaño, ya que puede considerar una red inalcanzable si supera este límite [5].

IS-IS, cuyo nombre significa Intermediate System to Intermediate System, es un protocolo que se utiliza para el intercambio de información entre routers intermedios. Para compartir tablas de enrutamiento con otros routers, IS-IS sigue una serie de pasos, que incluyen el establecimiento de adyacencia entre dispositivos, el intercambio de tablas de enrutamiento y el cálculo de la ruta óptima en cada caso. Los mensajes deben estar definidos por su tipo, longitud y valor entero de este campo [6].

EIGRP, desarrollado por Cisco como una mejora de su predecesor IGRP, no es un estándar y no es implementado por todos los proveedores de equipos de red, como Juniper, Huawei, Alcatel, entre otros. EIGRP es un protocolo vector de distancia que utiliza parámetros, conocidos como parámetros K, para determinar sus métricas. Estos parámetros incluyen el ancho de banda, el retardo de envío y la confiabilidad, entre otros [7].

2.3. Protocolo OSPF

El protocolo Open Short Path First abreviado como OSPF, pertenece al grupo de los protocolos de enrutamiento dinámico. Siendo su unica área de funcionamiento el interior de un sistema autónomo, perteneciendo al grupo de los protocolos de interior (IGP). Fue desarrollado en el año 1987 por la IETF. La primera versión OSPF v1 está especificada en los documentos RFC 1131. Después en el año 1998 se actualizó a OSPFv2 en RFC 2328. La última actualización es OSPFv3 donde se incorpora compatibilidad con IPv6 en el año 1999 [8].

Este protocolo de enrutamiento utiliza para su comunicación el sistema estado-enlace. El sistema estado-enlace es la valorización del enlace que realiza un router con sus vecinos, entregando un costo asociado al ancho de banda de este. Estos costos se van sumando hasta

tener un costo total origen/destino, además, de evitar las existencias de circulación infinita de la información o los llamados loops de ruta o loop infinitos. Similar a otros protocolos dinámicos, OSPF soporta el Support classless inter domain (CIDR[1]), donde se agrega el uso de máscaras[2] y submascaras (prefijos de direcciones de redes), permitiendo un mayor número de direcciones de IPv4. Soporta la existencia de rutas similares a un destino [9].

2.3.1. Funcionamiento OSPF

OSPF tiene como capacidad parcelar la topología de red en grupos más pequeños llamados áreas, cada una con sus propias bases de datos de rutas. Esto significa que los routers pertenecientes a un área, solo conocen las rutas dentro de su propia área y no rutas de dispositivos externos.

La agrupación en áreas tiene beneficios como reducir el tráfico de información en comparación con tener un único dominio en todo el sistema autónomo. Esto optimiza el envío de paquetes y mejora el rendimiento de la red.

Sin embargo, al tener subconjuntos de áreas, surge la necesidad de establecer comunicación entre ellas. Para esto, se utilizan routers especiales que funcionan como enlaces entre los dominios, permitiendo el intercambio de información. Estos routers son los únicos que tienen la capacidad de enrutar hacia otras áreas.

Para lograr la transmisión de información entre diferentes áreas, se requiere la presencia de un área backbone conocida como "área 0". Esta área es esencial para la comunicación entre otras áreas designadas dentro del mismo sistema autónomo. Por ejemplo, si el área 1 necesita comunicarse con el área 2, es necesario que la comunicación pase a través del área 0 para llevar a cabo este intercambio de datos.

Con el objetivo de disminuir el tamaño de las tablas de ruteo de OSPF, existen tres diferentes tipos de áreas en OSPF: Standard, Stub, Totally stub y NSSA [9].

El área standard no tiene configuración especial en comparación a las siguiente. Sin embargo, existe un área central conocida como Backbone, área 0, la cual siempre debe estar presente en las diferentes redes. Permite la comunicación entre áreas Standards.

La configuración de un área Stub se realiza de manera que los LSA (Link State Advertisements o envío de estado de enlace) provenientes de sistemas autónomos externos no se propaguen hacia los routers que pertenecen a dicha área, incluso aquellos en los límites, por ejmeplo, los routers de borde. En esta configuración, solo se establece una ruta por defecto en el router de borde para alcanzar rutas externas, lo que permite una mejor distribución de los recursos de CPU en los dispositivos.

El área Totally Stub no acepta ningún tipo de LSA, ya sean internos o externos. La única

[1] Técnica utilizada en el enrutamiento de paquetes en redes IP para mejorar la eficiencia en el uso de direcciones IP

[2] Direccionamiento IP el cual indica a qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

ruta conocida en esta área es la ruta por defecto, que se encuentra en el router de borde. A diferencia del área Stub, en el área Totally Stub el router de borde no puede enviar los LSAs a los routers internos del área, pero aún puede enviar LSAs hacia áreas externas.

NSSA (Not So Stubby Area), tiene como objetivo solucionar la limitación de las áreas stub al permitir la recepción de rutas externas. Esto es importante porque en las áreas stub, los routers internos no pueden recibir rutas externas, lo que dificulta el enrutamiento de paquetes hacia la red. Para resolver este problema, se utiliza un tipo específico de LSA (Link-State Advertisement) llamado tipo 7, que permite a los routers de borde en un área NSSA recibir rutas externas.

El funcionamiento de OSPF se debe a dos procesos fundamentales nativos de este protocolo: Hello packet y Sincronización de LSA [10].

2.3.1.1. Hello packet

Es responsable de establecer la conexión entre dos vecinos OSPF lógicamente contiguos, permitiendo una comunicación bidireccional. Para lograr esto, se intercambian constantemente mensajes de saludo, cuyo propósito es descubrir nuevos dispositivos en la red. Cuando se encuentra un nuevo dispositivo, este responde proporcionando parámetros importantes, como el *Time to Live* (tiempo de espera antes de que se desconecte la conexión), el costo del enlace y la dirección IP de destino.

Para mantener el enlace activo, se envían periódicamente estos paquetes de saludo, utilizando una variante del hello packet. Este paquete reinicia los temporizadores de intervalo para mantener la conexión. Si un dispositivo no recibe este tipo de mensaje, la comunicación entre los dispositivos se da de baja.

Dependiendo del tipo de red, se pueden agregar funciones adicionales al hello packet. Por ejemplo, en redes de broadcast y NBMA (non-broadcast multiple access), el protocolo OSPF designa un router central (DR) que recibe la información de los demás routers a través de LSA. Esto ayuda a reducir la cantidad de mensajes enviados en la red. Además, se designa un router de respaldo en caso de fallas [9].

En redes de broadcast, los routers envían periódicamente un hello packet a toda la red para anunciarse a sí mismos. El contenido del mensaje incluye información sobre el router designado y una lista de routers que han enviado hello packets recientemente. En redes NBMA, el router designado envía el mensaje a los demás routers que participan en la topología [9].

2.3.2. Sincronización de LSA

Este protocolo de enrutamiento dinámico se basa en el estado de enlace, por lo que es importante que los LSA, de los routers de la red, estén sincronizados. Para simplificar este proceso, los routers adyacentes permanecen en un estado de sincronización con su dispositivo compañero, y luego estos se sincronizan con los dispositivos adyacentes cercanos, y así sucesivamente.

Existe diferentes tipos de LSA, donde la diferencia principal en su función y qué routers lo

transmite, a continuación se presentan los mas frecuente en una red:

- LSA tipo 1 de router: Paquetes enviados entre routers que pertenecen a la misma área. Llevan información de la conexión de las interfaces.
- LSA tipo 2 de red: Paquete enviado por el router designado del área (DR), con el cual se describe la conexión de los otros routers. Este paquete es enviado a todos los demás, lo que se llama inundación de paquete.
- LSA tipo 3 de sumario: Paquete generado normalmente por routers que limitan entre mas de 2 áreas. Este paquete sumarisa las conexiones.
- LSA tipo 4 de sumario AS externo: Paquete utilizado principalmente para avisar a los demás routers de área la existencia de un sistema autónomo diferente.
- LSA tipo 5 sumario: Paquete generado por un router límite entre sistemas autónomos. En el paquete se advierte de las rutas externas a los routers internos del área.

Cuando un router recibe una actualización de la base de datos, crea una solicitud para determinar si es necesario adquirir la nueva ruta en el dispositivo. En caso afirmativo, un router envía la información y el otro router la recibe. Para indicar el final del proceso, el router maestro utiliza la herramienta M-bits.

2.3.2.1. Plano de control

OSPF es un protocolo que permite la conexión entre nodos de una red sin necesidad de especificar los routers más cercanos al dispositivo configurado. Utiliza los hello packet para establecer enlaces entre los nodos, y asignar un costo a cada conexión. Sin embargo, para el intercambio de información, se debe de generar las tablas de rutas correspondientes en cada router.

Las tablas de rutas de cada router se construyen a partir de LSA (Link State Advertisements) que se intercambian entre los routers. LSA determina la mejor ruta basándose en los LSA recibidos y comparándolos. Este proceso se realiza de manera individual en cada nodo, formando rutas en toda la topología de red al iterar sucesivamente en cada nodo de la red.

2.3.3. Arquitectura de red OSPF

En la figura 2.1, se muestran las clasificaciones de routers que se pueden encontrar en el protocolo OSPF [8], detallando a continuacion sus funciones.

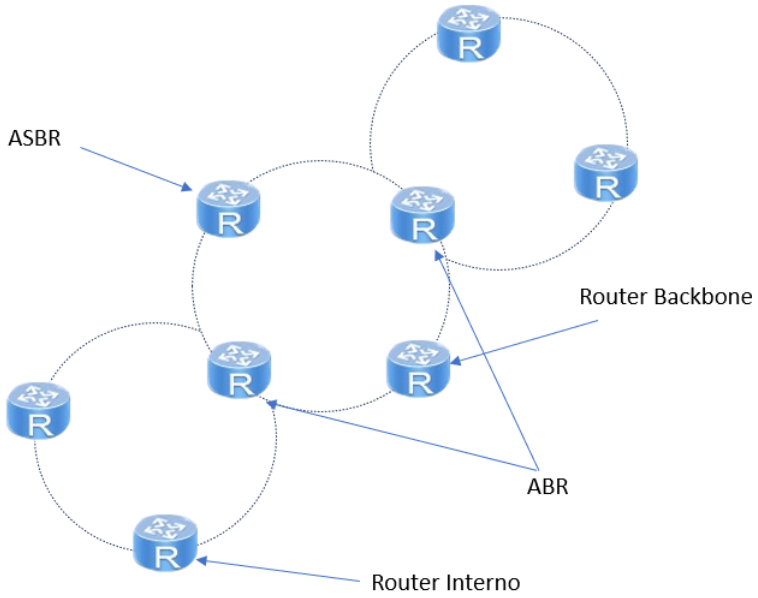

Figura 2.1: Arquitectura de routers OSPF.

Routers internos: Los routers internos se encuentran dentro de las áreas de la red, y están conectados a los ABR y ASBR. Estos routers intercambian LSA tipo 1 y 2 para compartir información sobre las redes dentro de su área.

ABR (Area Border Router): Estos routers se ubican entre las áreas, como se muestra en la figura 2.1, y tienen interfaces conectadas a dos subconjuntos diferentes, como el área 0 y el área 1. Los routers de borde de área intercambian LSA tipo 3 para informar a otras áreas sobre las redes existentes en su área.

Routers Backbone: Estos routers se encuentran en el área 0, que es el área principal de la topología. Tienen la función de enrutar el tráfico entre diferentes áreas dentro del mismo sistema autónomo.

ASBR (Autonomous system border area): Estos routers se encuentran en la frontera del sistema autónomo, generalmente en el área 0. Además de participar en OSPF, también debe manejar otros protocolos como BGP, esto con el fin de comunicarse con otros sistemas autónomos. Estos routers intercambian LSA tipo 5 para compartir información sobre las rutas externas al sistema autónomo.

2.3.4. Formato mensaje OSPF

El header de OSPF o el formato de mensaje de OSPF [9], se muestra en la figura 2.2.

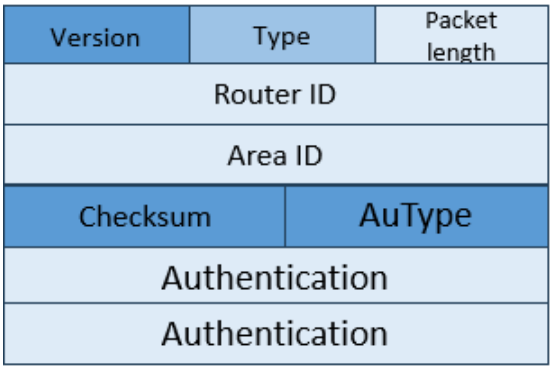

Figura 2.2: Estructura header OSPF.

Versión: Indica el número de versión del protocolo OSPF.

Type: Esta sección especifica qué tipo de mensaje es. OSPF tiene tres diferentes tipos.

Packet Length: Señala la longitud, en bytes, que tiene el paquete.

Router ID: Router ID de la fuente de origen del paquete.

Area ID: Esta sección consta de una longitud de 4 octetos, en donde se indica el área a donde pertenece este mensaje.

Checksum: Esta parte del mensaje verifica las anteriores características del mensaje.

AuType: Indica qué tipo de autenticación se utilizará para el mensaje; puede ser con contraseña, criptográfica y sin ningún tipo.

2.3.5. Hello packet

El header del paquete hello packet [9], se muestra en la figura 2.3.

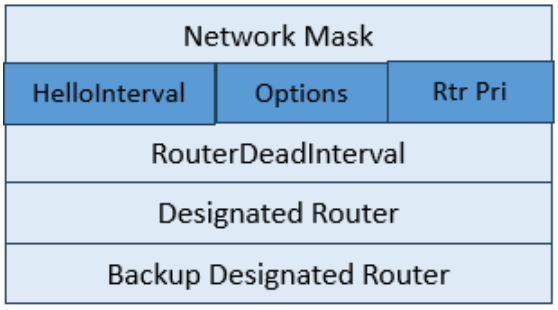

Figura 2.3: Estuctura header hello packet.

Network Mask: Máscara de red asociada a la interfaz del envío del paquete.

Hello interval: Indica el tiempo de espera para mantener la comunicación entre los routers.

Options: Capacidades posibles que puede tener OSPF.

Router Priority: En caso de escoger un router designado, indica la prioridad de cierto router para ser elegido.

RouterDeadInterval: Número de segundos que se debe esperar para que la comunicación se interrumpa.

Designated router: Router designado en la red, siendo identificado aquí con su IP.

Backup Designated Router: Router designado en la red para ser el respaldo del router designado, indicando su IP.

2.3.6. Formato paquete LSA

En la figura 2.4 se muestra el formato del header del paquete LSA de OSPF [9].

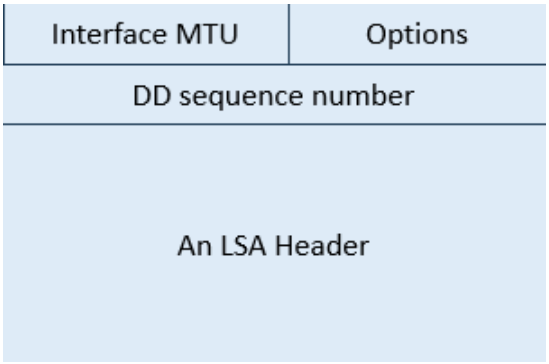

Figura 2.4: Estructura Header LSA.

Interface MTU: Indica por cuál interfaz se hará la sincronización de LSA entre los routers. Si el valor es 0, se realiza por enlace virtual.

Options: Capacidades posibles que puede tener OSPF.

I-bit: Especifica el bit inicial en el intercambio de información de los LSA.

M-bit: Indica cuantos bit quedan por terminar el intercambio de información de los LSAs.

MS-bit: En esta sección se indica que router actuará envia la información y el que recibe la información, en el intercambio de los LSAs.

DD sequence number: Esta sección funciona como indicador de cuántos paquetes faltan por terminar. Se empieza con un valor inicial que va incrementando hasta que se termina el proceso.

2.4. MPLS

La arquitectura de red MPLS (Multiprotocol Label Switching) fue desarrollada por la IETF y se introdujo en 1997 a través de la especificación RFC 3036. MPLS tiene como objetivo principal mejorar el proceso de reenvío de paquetes en las redes. En lugar de basarse únicamente en la dirección IP de destino de cada paquete para su enrutamiento, los routers utilizan etiquetas para simplificar este proceso.

Las etiquetas MPLS son únicas y tienen una longitud numérica menor en comparación con las direcciones IP. Estas etiquetas tienen un significado local y solo son interpretadas por los routers involucrados en el camino de reenvío. Al verificar las etiquetas en lugar de las direcciones IP, los routers pueden realizar el enrutamiento de manera más eficiente y rápida.

Las etiquetas en MPLS tienen diferentes operaciones asociadas, siendo las más frecuentes Push, Pop y Swap.

- Push: Es el proceso de añadir una etiqueta a un paquete.
- Pop: Consiste en remover la etiqueta de un paquete.
- Swap: Implica el intercambio de una etiqueta por otra en un paquete.

A lo largo del tiempo, MPLS ha evolucionado y se ha integrado en otras áreas de las redes, como las redes privadas virtuales (VPN) y la ingeniería de tráfico. Esto se debe a las capacidades y flexibilidad que ofrece MPLS, permitiendo la creación de conexiones seguras y optimizando el flujo de tráfico en la red.

2.4.1. Protocolos participantes en MPLS

Se deben de conocer dos protocolos que permiten el funcionamiento de MPLS: El LDP y RSVP [11].

2.4.1.1. Protocolo LDP

El Protocolo de Distribución de Etiquetas (Label Distribution Protocol o LDP) es un protocolo de enrutamiento utilizado en redes MPLS . Fue desarrollado por la IETF (Internet Engineering Task Force) con el objetivo de mejorar la eficiencia en el uso de los recursos de red y el rendimiento de las redes que lo implementan.

La función principal del protocolo LDP es establecer y distribuir etiquetas para los paquetes de datos que se transmiten a través de la red. Cuando LDP asigna una etiqueta a un paquete o conjunto de paquetes, se crea lo que se conoce como una clase de equivalencia de reenvío (Forwarding Equivalence Class o FEC). En esta función, cada router debe comunicar las etiquetas a los routers vecinos, y estas etiquetas se almacenan en la tabla de reenvío MPLS (FLIB) de cada router, formando así la topología de red MPLS con las etiquetas asignadas a cada dispositivo participante.

Una de las principales ventajas del protocolo LDP es su capacidad de ser compatible con otros protocolos de enrutamiento IGP y BGP (como se verá más adelante). Esto significa que las redes que utilizan los protocolos mencionados anteriormente, pueden incorporar fácilmente

el protocolo LDP en su infraestructura de red, aprovechando sus beneficios en términos de eficiencia y rendimiento.

2.4.1.2. Protocolo RSVP

El protocolo RSVP (Resource Reservation Protocol) permite a los dispositivos de red reservar ancho de banda para garantizar la calidad de servicio en el transporte de datos en tiempo real. Fue desarrollado por la IETF en la década de 1990 como una solución para abordar problemas de congestión en la red.

El objetivo principal de RSVP es permitir que los dispositivos de red establezcan y mantengan rutas de comunicación que asignen un determinado ancho de banda y calidad de servicio en un enlace, según los requisitos específicos de los servicios solicitados por los usuarios. RSVP funciona mediante el intercambio de mensajes entre routers, donde un router solicita a su vecino el uso del enlace y especifica los requerimientos de ancho de banda y calidad de servicio necesarios. A continuación, el dispositivo de destino responde con una confirmación o rechazo al requerimiento. Una vez establecida la conexión, ambos participantes asignan los recursos que fueron previamente aceptados hasta que se finalice el uso del enlace.

De esta manera, RSVP permite asegurar que los recursos de red necesarios para el transporte de datos en tiempo real estén disponibles y sean utilizados de manera eficiente, evitando la congestión y garantizando una experiencia de calidad para los servicios que requieren una transmisión sin interrupciones y en tiempo real.

2.4.2. Estructura MPLS

Para el funcionamiento de la red MPLS esta debe tener una estructura a nivel de routers o dispositivos de capa 2 (switches) que sean capaces de reenviar paquetes. A continuación se muestran los elementos que participan en una red MPLS [12]:

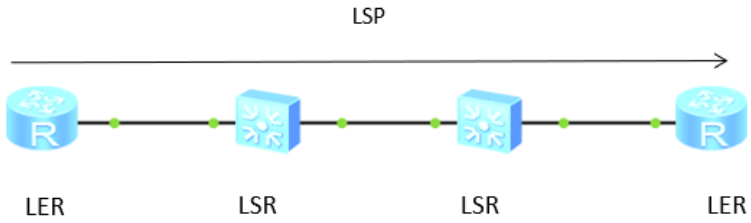

Figura 2.5: Estructura routers/switches MPLS.

LSR : se encuentran en la estructura interna que le da forma a la red, donde se realiza el FEC del protocolo LDP.

LER: se encuentran a los bordes de la red.

Otro tipo de clasificación son los routers P, PE y CE.

P: Provider router, ubicados en el núcleo de la red de un proveedor.

PE: Provider edge, ubicados en los bordes de la red de un proveedor.

CE: Customer router, ubicados específicamente para servicios a los clientes del proveedor.

2.4.3. Funcionamiento de MPLS

Para la optimización en el envío de paquetes, MPLS divide el plano de enrutamiento y el plano de control, con el fin de aligerar la carga de los dispositivos para la conmutación de paquetes [13]. La razón de esto es que la creación de las rutas es un proceso complejo donde se ven factores como el costo y tiempo, mientras el envío es un proceso simple.

2.4.3.1. Plano control

Al igual que los protocolos de enrutamiento dinámico, MPLS requiere generar información para las tablas de etiquetas (LFIB) necesarias para el envío de paquetes. En el caso de MPLS, puede utilizar más de un protocolo para lograr esto debido a la naturaleza de su arquitectura. Se deben distribuir tanto las etiquetas a nivel de LDP (Label Distribution Protocol) como a través de otros protocolos IGP.

Para la distribución de etiquetas entre los diferentes nodos de la red, se utiliza el protocolo LDP. LDP se encarga de asignar etiquetas a los paquetes o flujos de paquetes y luego distribuirlas a otros dispositivos de la red a través de los Label Switched Paths (LSP), que son los caminos utilizados para el intercambio de etiquetas. De esta manera, todos los routers o switches en el dominio MPLS tienen una tabla de enrutamiento de etiquetas.

Si bien RSVP (Resource Reservation Protocol) también puede ser utilizado para la distribución de etiquetas, este protocolo se utiliza principalmente para el control de flujo de tráfico en la red, con el objetivo de ofrecer un mejor servicio mediante la reserva de recursos. En el contexto de la ingeniería de tráfico de MPLS, se utiliza principalmente para la gestión de recursos por parte de los proveedores de servicios.

2.4.3.2. Plano de enrutamiento

El proceso de envío de paquetes dentro del dominio MPLS comienza con la asignación de una etiqueta al flujo de datos entrante. Este proceso se lleva a cabo en los routers conocidos como LER (Label Edge Router). Una vez que se ha asignado la etiqueta, el router LER procede a enrutar el paquete siguiendo la ruta indicada en la tabla de enrutamiento.

En lugar de verificar el encabezado IP del paquete, el dispositivo receptor, que puede ser un router o un switch, examina la etiqueta y la utiliza para cambiarla por otra etiqueta correspondiente antes de enviarlo al siguiente destino. Este proceso se repite de forma sucesiva hasta que el paquete alcanza los límites de la red MPLS.

Finalmente, el router LER en el límite de la red MPLS enruta el paquete externamente utilizando direccionamiento IP y elimina la etiqueta asociada al flujo de paquetes.

2.4.3.3. Formato mensaje MPLS

El header de las etiquetas MPLS, figura 2.6 se encuentra entre el header de capa 2 y el de capa 3. Además, tienen una longitud total de 32 bits [14].

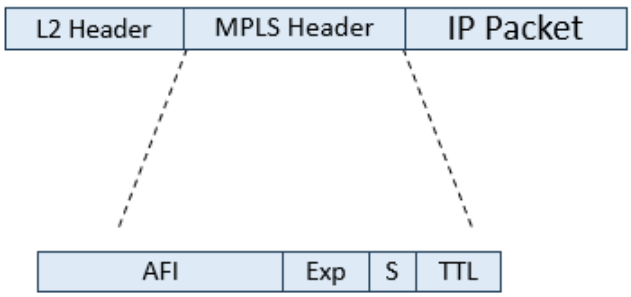

Figura 2.6: Estructura header MPLS.

Label Value: Campo de 20 bits. Identificador de etiquetas para el uso del enrutamiento de MPLS. Utiliza números enteros.

Experimental: Campo de 3 bits, donde se explicita prioridad de los paquetes conocido como clase de servicio.

Stack: Campo de 1 bit. Indica si pertenece a un apilamiento de etiquetas, y en caso de serlo la última etiqueta manda.

TTL: Campo de 8 bits. Corresponde al tiempo en cuanto el mensaje sera descartado.

2.5. Protocolo BGP

El protocolo BGP (Border Gateway Protocol) es un protocolo de enrutamiento dinámico que tiene como objetivo principal interconectar diferentes sistemas autónomos. Se estableció como estándar de protocolo externo en 1990 con la publicación de la RFC 1163, que describe su función y operación básica. A lo largo del tiempo, se han desarrollado diferentes versiones, siendo la última el protocolo BGP-4, descrito en la RFC 4271 [15].

El BGP comparte información sobre las redes cercanas con otros sistemas que utilizan este mismo protocolo, a los cuales se les denomina pares o vecinos BGP. Esto crea una red de conexiones entre los sistemas autónomos. La implementación del BGP ha introducido nuevas características en el envío de paquetes tales como; el soporte de CIDR; el uso del método de path-vector para seleccionar la mejor ruta entre sistemas autónomos; políticas que permiten controlar las tablas de ruta sin modificar la configuración y el uso de atributos, que pueden ser obligatorios u opcionales, dependiendo de las capacidades que se deseen utilizar [16].

2.5.1. Funcionamiento BGP

El método de envío de mensajes en BGP se conoce como Path-vector. Este enfoque se diferencia de los métodos de estado de enlace y distancia, ya que utiliza información crucial

como los saltos siguientes a los routers, la red de destino y el camino a seguir.

Aunque la función principal del protocolo BGP es conectar routers de diferentes sistemas autónomos, también se utiliza internamente en los sistemas, lo que se conoce como iBGP. En este caso, el router actúa como un protocolo IGP para compartir información de enrutamiento con sus pares BGP.

Para que BGP funcione correctamente, la conexión entre dos routers diferentes se realiza mediante el protocolo TCP en el puerto 179. Para establecer la conexión con vecinos BGP, se deben cumplir ciertos requisitos. En primer lugar, los pares que deseen establecer una relación BGP deben estar conectados lógicamente mediante otros dispositivos de red, o directamente. En segundo lugar, como BGP no tiene un proceso para descubrir nuevas conexiones, se utiliza un tipo de mensaje BGP llamado OPEN. Este mensaje debe especificar la dirección IP, el ID del router, el tiempo de vida y otros parámetros necesarios para que el mensaje OPEN pueda enlazar directamente dos dispositivos que utilicen BGP.

Una vez establecida la comunicación BGP, el protocolo no utiliza la función nativa de TCP para mantener la sesión en línea. En su lugar, se utilizan mensajes específicos del protocolo BGP. Al igual que otros protocolos de enrutamiento dinámico, BGP debe generar tablas de ruta para compartirlas con sus pares. Siguiendo el ejemplo de OSPF, primero genera las rutas disponibles en el router, utilizando las mejores de ellas sin importar si provienen de otros protocolos utilizados en el dispositivo.

Después de completar estos procesos internos, el protocolo BGP utiliza el mensaje UPDATE para notificar a todos los vecinos BGP, ya sea IBGP o EBGP. En este mensaje se envía la base de datos de la tabla de rutas. El dispositivo receptor del mensaje compara esta tabla con la suya propia y, en caso de encontrar una actualización, repite el proceso interno. Esta vez se revisa si la nueva ruta es óptima en comparación con la existente. Si mejora, se reemplaza; de lo contrario, se mantiene. El router que recibe el mensaje también lo envía a sus vecinos, evitando enviárselo al dispositivo de origen de la actualización para evitar bucles infinitos. BGP utiliza un atributo que permite reconocer el origen del mensaje.

En caso de que se produzca una desconexión entre los vecinos BGP, sin importar la razón, BGP envía un mensaje de UPDATE a los routers adyacentes para indicar que no hay conexión con la otra red. Para esto, utiliza un atributo que permite verificar si existe o no la conexión con el par BGP. En consecuencia, se mantienen o eliminan las rutas que pasan por ese dispositivo, lo que requiere generar una nueva tabla de rutas con esta información.

Aunque el plano de control del protocolo genera las tablas de rutas, BGP puede realizar cambios en el enrutamiento sin necesidad de modificar la configuración del router, gracias al uso de políticas BGP. Estas políticas son instrucciones adicionales que se entregan aparte de la configuración normal de BGP, sin alterar la configuración en sí de BGP. Algunas de estas funciones incluyen NO EXPORT, NO ADVERTISE y NO EXPORT SUBCONFED. La función NO EXPORT implica no enviar avisos a routers que se encuentren fuera del sistema autónomo, sino solo a los dispositivos que estén dentro del sistema. NO ADVERTISE evita que las direcciones se anuncien a vecinos IBGP y eBGP. Por último, NO EXPORT SUBCONFED impide advertir rutas a otros sistemas autónomos.

En resumen, BGP utiliza políticas para filtrar mediante la comparación de dos atributos, NEXT HOP y AS PATH.

2.5.2. Formato mensaje BGP

Como se dijo BGP utiliza protocolo TCP para la conexión entre los peers BGP, teniendo un formato de mensaje que consta de un total de 4096 octetos como tamaño máximo y con un mínimo de 19 [17].

El formato del header BGP se muestra en la figura 2.7.

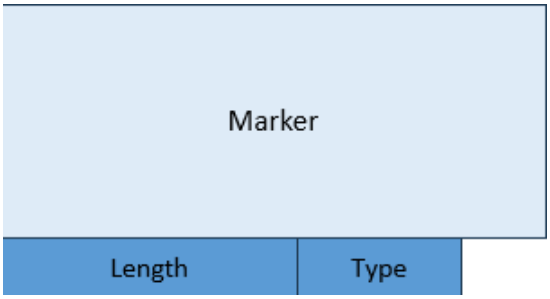

Figura 2.7: Estructura Header BGP.

Marker: Este campo tiene un total de 128 bits, en donde se ve la compatibilidad y la limitación de mensajes BGP. Aquí solo se usa el dígito 1.

Length: Este campo son 24 bits, donde se indica el valor de la longitud del mensaje BGP.

Type: En este campo es 1 bit, donde se indica el tipo de mensaje BGP que es. Existen 5 tipos posibles.

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE
- ROUTE-REFRESH

2.5.2.1. OPEN

Después de establecer la conexión TCP entre dos pares BGP diferentes, y negociar los parámetros de esta acción entre vecinos BGP, se envía el mensaje OPEN como se muestra en la figura 2.8.

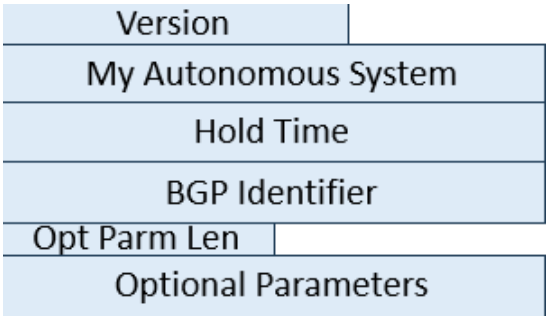

Figura 2.8: Estructura header Open.

Version: Campo de 8 bits, en donde se indica la versión que está utilizando el par BGP. Actualmente es la versión 4.

My Autonomous System: Campo de 16 bits. Indica el sistema autónomo al que pertenece el par BGP responsable del envío, especificando su número en el topología de la red.

Hold Time: Campo de 16 bits. Se especifica el tiempo de espera para recibir respuesta entre los pares BGP, en donde se reinicia el tiempo al valor establecido en caso de recibir antes. En caso contrario, si se excede el tiempo límite establecido, se interrumpe la conexión, y son eliminadas las rutas y se anuncia con actualización (mensaje UPDATE) a los vecinos BGP.

BGP identifier: Campo de 32 bits. BGP identifier es un número, relacionado con la IP, que identifica al BGP que está enviando el mensaje a su vecino BGP. Este parámetro se define previamente para realizar la conexión entre estos pares. Las formas de configuración pueden ser estáticas o dinámica.

Optional Parameters Length: Campo de 8 bits, se puede añadir funciones opcionales en la cual se especifica la longitud de los campos para definir estas cualidades BGP.

Optional Parameters: Cantidad de bits variables. Se muestra en la figura 2.9, el formato del header de este campo con los parámetros opcionales de BGP que se añaden.

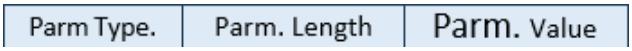

Figura 2.9: Estructura header Optional Parameters.

Parameter Type: Campo de longitud de 8 bits, el cual con un número indica cuál cualidad BGP es.

Parameter Length: Campo de longitud de 8 bits. Indica la longitud de Parameter Value.

Parameter Value: Longitud variable de bits. Indica el cambio de la cualidad BGP escogida previamente, es decir, activa o inactiva.

2.5.2.2. UPDATE

Una vez realizada la conexión entre los pares BGP e identificado los parámetros con el mensaje OPEN, los vecinos comparten información, de rutas factibles y/o rutas cercanas de los BGP, formando de esta forma la topología de relaciones entre diferentes sistemas autónomos.

El formato del header BGP al usar su función UPDATE siempre cambia, y la estructura de este, tal como se muestra en la figura 2.10.

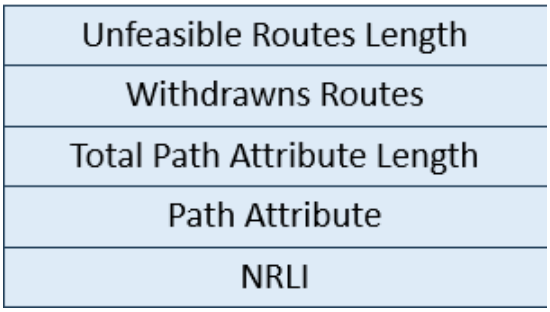

Figura 2.10: Estructura header Update.

Unfeasible Routes Length: Campo de 16 bits. Indica la longitud de mensaje que mostrará las rutas infactibles que tiene el par BGP.

Withdrawn Routes: Campo con longitud variable de bits. Lista de rutas con prefijos IP que serán reiteradas. Está escrita en tuplas, como <longitud y prefijo>.

Total path attribute length: Campo de 16 bits. Indica la longitud del campo de atributos del mensaje UPDATE.

Path attribute: Campo de longitud variable de bits. Siempre está presente en mensajes UPDATE, a excepción del caso de retirar rutas. Esta sección tiene tripleta, las cuales indican la longitud de atributos, los atributos que serán cambiados y el valor que tomarán. El header de estos atributos se muestra en la figura 2.11.

Figura 2.11: Estructura header atributos BGP.

El atributo de ruta siempre está presente cuando se actualiza la información de enrutamiento en los pares BGP. Los atributos BGP son los siguientes:

Origin: Indica cómo se obtuvo la información de enrutamiento, es decir, el protocolo de enrutamiento a través del cual el router adquirió esa información.

AS PATH: Actúa como un filtro que permite o niega rutas en función de una comparación lógica OR. Este atributo se compara con la ruta para determinar si se debe aceptar

o rechazar. Existen diferentes métodos de comparación, como el uso de asteriscos, punto de exclamación, peso, entre otros. Este atributo es relevante en la comparación de políticas BGP.

Next HOP: Indica la dirección IP del siguiente salto para alcanzar el destino de la ruta. Este atributo también participa en la comparación de políticas BGP.

Aggregator: Transmite el número del último sistema autónomo en la ruta agregada.

Network Layer reachability information: Es un campo de longitud variable que contiene los prefijos de direcciones IP. La información se presenta en forma de dupleta, que incluye la longitud y el prefijo de la dirección IP. Este atributo es relevante para verificar la conectividad entre los pares BGP y para agregar o eliminar rutas de la tabla de enrutamiento BGP.

LOCAL PREF: Es un valor configurable a nivel local del router y determina la preferencia de una ruta. Cuanto mayor sea el valor de este atributo, mayor será la preferencia. En BGP, hay un valor predeterminado para este atributo, que es 100, pero se puede modificar según sea necesario. Esta política se utiliza principalmente en iBGP.

MED: Es un valor configurable a nivel local del router y se utiliza para determinar la preferencia de una ruta en caso de tener múltiples rutas hacia el mismo destino. Cuanto menor sea el valor de MED, mayor será la preferencia. El MED es visto solo por los pares BGP del sistema autónomo vecino. Se asemeja al costo de una ruta en caso de OSPF.

Para el atributo opcional de las comunidades también existe un formato, ostrado en la figura 2.12

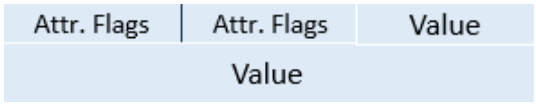

Figura 2.12: Estructura header atributos opcionales.

Type: Indica si la comunidad es normal o extendida. Tiene tanto High como Low debido a los códigos que puede exceder de 1 octetos en el caso de la segunda opción.

Value: Es un código que depende de qué tipo de comunidad es, donde normalmente las comunidades extendidas utilizaran 6 octetos designados.

2.5.2.3. KEEPALIVE

Si bien BGP utiliza TCP, el protocolo no utiliza el formato de este mecanismo para mantener la conexión entre los pares BGP, en cambio, se usa este formato de mensaje.

Ambos vecinos BGP establecen el intervalo de tiempo que se debe de esperar para recibir este mensaje y no cortar comunicaciones. En caso de no existir intervalo de tiempo no se envían. El formato UPDATE puede suplantar este funcionamiento.

2.5.2.4. NOTIFICATION

En casos de existir un error en la conexión de los vecinos BGP, se envía un mensaje de error, para luego ser finalizada el intercambio entre estos dispositivos.

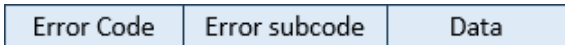

Figura 2.13: Estructura header Notification.

Error code: En este campo tiene 8 bits. Se indica por medio de un número entero el tipo de error que se ha producido.

Error subcode: Campo con longitud de 8 bits. Se especifica el error en el mensaje. Existen diferentes tipos de errores los cuales afectan los mensajes UPDATE, OPEN y KEEPALIVE. Además, de problemas en el header del mensaje BGP y tiempo de intervalo expirado.

Se suelen cometer errores frecuentes en el header de los mensajes BGP, como la falta de sincronización en la conexión y problemas relacionados con la longitud y el tipo del mensaje.

Data: Este campo tiene longitud variable de bits. Esto se debe a que se entrega información adicional del mensaje de notificación.

2.5.2.5. ROUTE-REFRESH

Es una capacidad añadida a BGP, para cuando se quiera actualizar nuevas políticas o características a las rutas entre los vecinos, esto con el fin de reducir el costo que trae el actualizarlas de manera normal utilizando el formato UPDATE del protocolo M-BGP (multi protocolo BGP), la cual será detallada más adelante.

El formato de este tipo de mensaje es el mostra en la figura 2.14

Figura 2.14: Estructura header Route-Refresh.

AFI: Campo con longitud de 16 bits. Indica la Address Family.

RES: Campo de 8 bits. Se identifica quien envía, debido a que el transmisor configura este campo con un 0, mientras el receptor lo ignora.

SAFI: Campo con longitud de 8 bits. Indica la subsequence Address Family.

2.6. Multiprotocolo BGP

Esta categoría de BGP-4 corresponde a una extensión del protocolo BGP, cuyo objetivo principal es proporcionar soporte para diferentes capas de red y tipos de direcciones. Se utiliza el término *Address Family* (AFI) para referirse a las capas de red, como IPv4, IPv6, VPNv4, VPNv6, entre otras. Por otro lado, el término *Subsequence Address Family* (SAFI) se utiliza

para los diferentes tipos de direcciones, como multicast, unicast, broadcast, y demás. Estas categorías están definidas en detalle por IANA, asignando un valor entero a cada una de las funciones posible [18].

Para lograr el objetivo de BGP con múltiples protocolos, se requiere incorporar características del protocolo base, como NRLI (Network Layer Reachability Information), Aggregator y NEXT HOP. Sin embargo, cada una de estas características funciona de manera diferente en el contexto de cada capa y tipo de dirección. La información de NEXT HOP ahora se incluye en la lista de NRLI, junto con las AFI y SAFI correspondientes.

Además de los atributos estándar de BGP, se agregan dos atributos opcionales que hacen uso de las características mencionadas anteriormente: el atributo de accesibilidad multiprotocolo de NRLI y el atributo de inaccesibilidad. El atributo de accesibilidad multiprotocolo tiene dos funciones posibles: indicar la ruta posible a un vecino BGP, junto a la capa de red que se utiliza o quitar de esta lista debido a desconexión con el par BGP.

2.6.1. Formato mensaje M-BGP

MBGP añade la posibilidad de utilizar diferentes capas de red definidas como AFI y diferentes direcciones indicadas por SAFI. Esta informacion se agrega a NRLI, cambiando el fomato de header como se muestra en la figura 2.15 [14]:

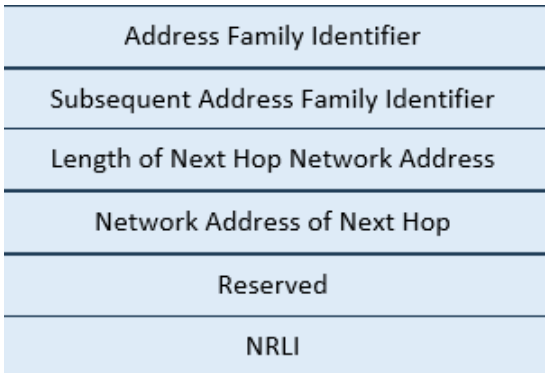

Figura 2.15: Estructura header M-BGP.

Address Family: Campo de longitud de 16 bits. Siempre está en conjunto de una SAFI. Las AFI funcionan como identificador de un grupo de protocolos de capa de red (definidos en una lista por IANA-AF) a usarse en el siguiente salto. Por ejemplo IPv4, IPv6, VPNv4, entre otros.

Subsequent Address Family: Campo de longitud de 8 bits. Se usa conjuntamente con una AFI. Indica como y donde enviaran el mensajes los routers asociados a BGP (definidos en una lista de IANA-AF). Estos pueden ser unicast, multicast, NRLI con MPLS, entre otros.

Length of next hop network address: Este campo es variable en su longitud de bits. Aquí se entregan la longitud de la lista a los **next hop** a diferentes redes.

Network address of next hop: Este campo es variable en su longitud de bits. Se enlistan los

next hop que se deben de realizar a la red.

Network Layer Reachability Information: Campo de longitud variable de bits. El NRLI procesa lo necesario en BGP-v4, principalmente información que contiene los prefijos de dirección IP de los **next hop**. La información se muestra como tupla, <longitud y prefijo IP>. Se agregan las posibilidades de diferentes direcciones de capa de red de las AFI y SAFI, tal como se muestra a continuación.

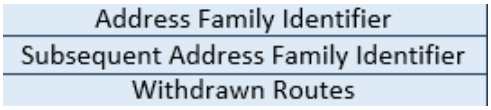

Figura 2.16: Estructura header NRLI.

La funcionalidad del atributo de inaccesibilidad del multiprotocolo NRLI, es retirar de la lista todas las rutas que no se puedan acceder. Tiene la misma estructura que accesibilidad en la distribución del mensaje.

Address Family: Campo de 16 bits. Identificador de un grupo de protocolos de capa de red, que debe, usarse en el siguiente salto, por ejemplo indicar si es IPv4, IPv6, VPNv4, entre otros, definidos en una lista por IANA-AF. 2-octetos

Subsequent Address Family: Campo de 8 bits. Indica como y donde enviaran el mensajes los routers asociados a BGP. Estos pueden ser unicast, multicast, NRLI con MPLS, entre otros, definidos por IANA-AF. 1-octeto

Withdrawn Routes: Campo con longitud variable de bits. Se indican las rutas detectadas que son inalcanzables, por lo que, se enlistan y se procede a eliminar del proceso del plano de control típico de BGP.

2.6.2. Protocolo BGP-LU

El protocolo conocido como BGP-LU (BGP-label unicast) combina las funcionalidades del protocolo BGP (Border Gateway Protocol) y el protocolo multiprotocolo BGP, además de aprovechar la arquitectura de red MPLS. El objetivo de BGP-LU es permitir el funcionamiento de distribución de etiquetas por medio de BGP [3].

Al utilizar BGP-LU, la ruta en particular se encuentra dentro del contexto de Header BGP, donde se almacena la información necesaria para distribuir el mensaje en el atributo NRLI. Es importante tener en cuenta que se agrega la posibilidad de BGP de distribuir etiquetas, añadiendo esta extensión como distribuidor de etiquetas junto a protocolos IGP y LDP.

Una condicionante del protocolo BGP-LU es que si anuncia diferentes etiquetas en una ruta hacia un mismo destino, se selecciona un protocolo de distribución de etiquetas MPLS (BGP-LU o LDP), descartando los demás protocolos. Además, es importante que las rutas sean independientes entre sí, lo que significa que si selecciona uno de estos protocolos, el otro queda invalidado.

2.6.2.1. Formato Mensaje BGP-LU

Al agregar información de las etiquetas MPLS a las funcionalidades de BGP, se agrega información como el mapeo de las etiquetas y su siguiente salto. Esto es añadido en el campo NRLI específicamente en cada uno que contenga rutas, generando cambios en el formato del header BGP [3], como se muestra en la figura 2.17.

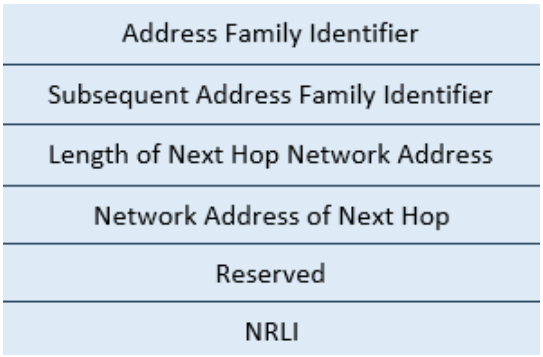

Figura 2.17: Estructura header BGP-LU.

Address Family: Campo de 16 bits. Siempre está en conjunto de una subsecuencia de dirección de familia. Este funciona como identificador de un grupo de protocolos de capa de red, a usar en el **next hop**, como por ejemplo IPv4, IPv6, VPNv4, entre otros.

Subsequent Address Family: Campo de 8 bits. Se usa conjuntamente con dirección de familia, indica como y donde enviaran el mensajes los routers asociados a BGP. Estos pueden ser unicast, multicast, NRLI con MPLS, entre otros.

Length of next hop network address: Campo de 1 bit. Este campo es variable en su longitud de octetos. Aquí se entregan las longitudes de la lista a los siguientes saltos a diferentes redes.

Network address of next hop: Campo longitud variable de bits. Se enlistan las direcciones de los **next hop** que se deben de realizar a la red.

Network Layer Reachability Information: Campo de longitud variable. El NRLI además, de procesar los necesario en BGP-v4, contiene los prefijos de dirección IP. La información se muestra como tupla, <longitud y prefijo IP>. Se agregan las posibilidades de direcciones de capa de red (AFI y SAFI), tales como se muestra a continuación.

- Longitud del mensaje: Campo de 8 bits. Indica la longitud del campo de etiquetas y de los prefijos de dirección IP. .

- Campo de etiquetas: 24 bits. Aquí es donde se encuentran las etiquetas a usar, pudiendo ser 1 o más.

- Prefijo de dirección IP: Campo con longitud variable de bits. Indica el prefijo destino del paquete, se muestra como tupla <longitud y prefijo>.

Address Family: Campo de 16 bits. Identificador de un grupo de protocolos de capa de red, que debe, usarse en el siguiente salto, por ejemplo indicar si es IPv4, IPv6, VPNv4, entre otros.

Subsequent Address Family: Campo de 8 bits. Indica como y donde enviaran el mensajes los routers asociados a BGP. Estos pueden ser unicast, multicast, NRLI con MPLS, entre otros.

Withdrawn Routes: Campo con cantidades variables de bits. En este campo se indican las rutas detectadas que son inalcanzables, por lo que, se enlistan y se procede a eliminar del proceso del plano de control de BGP.

- Longitud del mensaje: Indica la longitud del campo de etiquetas y de los prefijos de dirección IP, para esta parte es necesaria un 1 octeto.

- Campo de etiquetas: Aquí es donde se encuentran las etiquetas a usar, pudiendo ser 1 o más, utiliza 3 octetos.

- Prefijo de dirección IP: El cual es el prefijo destino del paquete, siendo variable la extensión de octetos. <longitud y prefijo>

2.7. Estado de arte

Los ISP deben tener una alta continuidad operacional, esto con el fin de cumplir las demandas de clientes y las exigencias gubernamentales. Actualmente la SUBTEL exige tanto tasa de pérdida de paquetes , como Latencia y tasa de ocupación de un enlace [19]. Para lograr esto los ISP presentan una topología de red con múltiples enlaces redundantes. Estos se concentran principalmente en la capa de agregación y core.

La topología de red se divide por el modelo jerárquico, en tres capas lógicas diferentes: Acceso, Agregación y Core. Estas capas de redes al tener diferentes funciones, se encuentran independiente en la red, como se puede ver en la figura 2.18. Para compensar esto existen protocolos de enrutamiento que permiten la conexión de una capa a otra, sin embargo, esto genera puntos de congestión, debido al cambio de una tecnología a otra, como se puede ver en la figura 2.18.

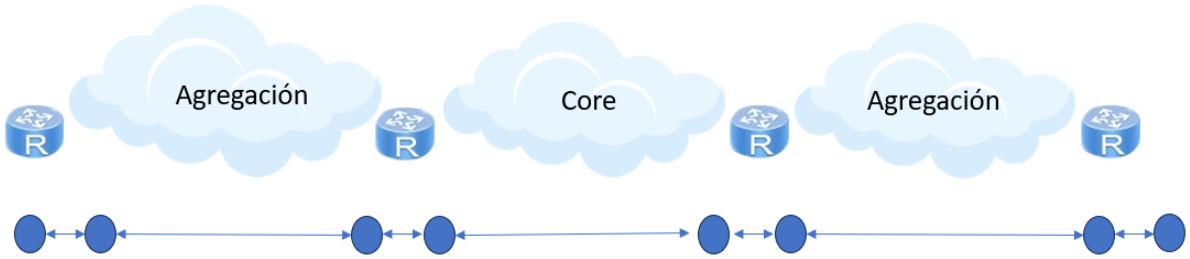

Figura 2.18: Estado actual de la red previo a BGP-LU.

Estos puntos de congestión de la topología de red son consecuencia del cambio de tecnología que debe de existir en el enrutamiento de la información de un punto a otro en la red. Las tecnologías que funcionan al mismo tiempo son los protocolos de enrutamiento OSPF y BGP, y MPLS.

OSPF es usado como protocolo de señalización. Esto significa su principal función es el intercambio de rutas entre routers, que pertenecen al mismo sistema autónomo. Los IGP permiten el funcionamiento de protocolos como LDP [20] y BGP [16].

MPLS es usado en la industria de las telecomunicaciones como técnica de enrutamiento óptimo y mejorando el tiempo de envío de paquetes. Se utiliza en la red con L2VPN usando protocolos de LDP y RSVP, y junto a su funcion de tráfico de ingeniería con RSPV-TE.

Los ISP utilizan el protocolo BGP-v4 en sus equipos de borde, debido a la necesidad de intercambio de rutas con diversos operadores (otros sistemas autónomos) [21]. Además, el uso de políticas permite controlar los anuncios de rutas del proveedor a otros routers, siendo este protocolo, necesario para optimizar el procesamiento e incluso prevenir filtración de información sensible.

El uso de multi-protocolo BGP, es por su ambivalencia al transmitir en diferentes capas de red, tales como, IPv4, IPv6, VPNv4, EVPN, y demas [16]. Si es usado junto a la red MPLS, en temas de VPN se encuentra lo que es L3VPN de MPLS [22].

La optimización de las redes y la prevención de cuellos de botella son aspectos cruciales para los ISP. Sin embargo, los ISP para resolver el tema de los cuellos de botellas, enfrentan desafíos asociados a los protocolos OSPF y LDP, que tienden a generar una sobrecarga en la red debido a la gran cantidad de mensajes que emiten. En el caso de OSPF, esto ocurre con los LSA tipo 3, mientras que el protocolo LDP afecta por los paquetes de descubrimiento. Para abordar esta situación, se busca minimizar al máximo el impacto de estos protocolos en la red.

Además, OSPF presenta otro problema relevante relacionado con la publicación de rutas de interfaces, especialmente cuando se trata de redes extensas pertenecientes a los ISP. Estas redes generan una gran cantidad de rutas que los routers deben ser capaces de gestionar y almacenar. Esta complejidad añade un desafío adicional a la administración y operación de la red, demandando una eficiente gestión de recursos para garantizar el óptimo funcionamiento de la red en su totalidad.

2.8. Metodología

2.8.1. Aplicación BGP-LU

La función de BGP-LU es anunciar etiquetas MPLS a través del protocolo BGP. Esto optimiza la topología de red del ISP al reducir la necesidad de utilizar múltiples protocolos de enrutamiento. Además, esta implementación elimina la necesidad de aplicar el protocolo LDP. Dando como resultado, menos protocolos participando en la ropologia de redy, por ende reduccion en el procesamiento de los router.

El protocolo BGP-LU se implementa en distintas capas de la red, como por ejemplo la capa de Agregación y Core. Esto se realiza con el objetivo de evitar puntos de congestión en la estructura de MPLS. Este protocolo junto a lo que se conoce como RR, se denomina como seamless MPLS. Seamless MPLS aplica todos los servicios que MPLS ofrece en diferentes secciones de la red, como las capas de agregación y core, en una única instancia unificada de MPLS. Esto resulta en una optimización significativa en la transmisión de paquetes al evitar puntos de congestión y mejorar el flujo de datos en la red [23].

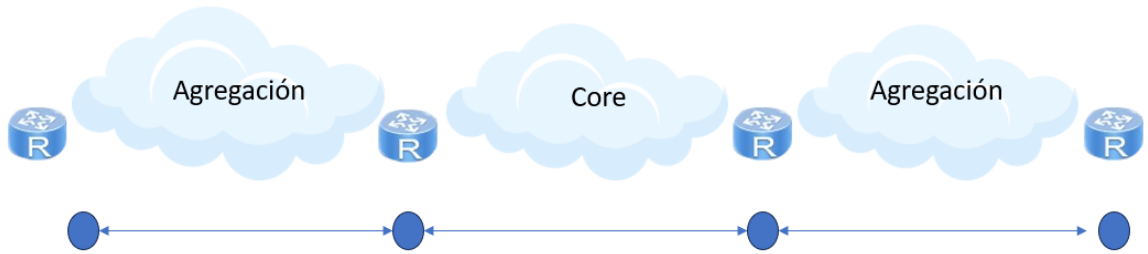

Figura 2.19: Estado de red implementacion BGP-LU.

Los *routers reflectors* (RR) actúan de tal forma que los vecinos BGP envían sus actualizaciones de rutas al RR. Este las transmite a otros routers, además, funciona como receptor de otras rutas externas. De esta manera, los dispositivos del sistema autónomo no necesitan establecer conexiones BGP completas entre sí, lo que reduce la carga y optimiza la red [17]. Existen dos tipos de RR uno en el que un router ya existente en la topología asume esta función (in-line) y otro en el que se agrega un nuevo router a la topología para desempeñar esta función (standalone), siendo in-line una clara opción económica de la aplicación de los RR debido la reutilización de dispositivos para esta función.

Seamless MPLS presenta dos tipos de aplicaciones que difieren según si las capas de la red están en diferentes sistemas autónomos o en el mismo sistema. [24].

- Intra-AS: En este tipo de seamless MPLS la capa de acceso, distribución y núcleo de red, se encuentran en el mismo sistema autónomo. Común en redes móviles

- Inter-AS: En este tipo de seamless MPLS la capa de acceso y distribución se encuentran en el mismo sistema autónomo, mientras que la capa de núcleo de red se encuentra en

un sistema autónomo diferente. Es usualmente como las empresas manejan sus servicios.

Ambas opciones de implementación de seamless MPLS son interesantes para el caso de estudio. Esto se debe principalmente a que la opción intra-AS tiene como objetivo reducir las tablas de rutas de los routers dentro del mismo sistema autónomo, lo cual cumple con los requisitos de bajar las rutas recibidas de un router dentro del sistema.

Por otro lado, la opción inter-AS es necesaria para demostrar la conectividad de este dispositivo con otro ISP, y también permite reducir las tablas de rutas recibidas entrantes del sistema autónomo externo.

2.8.2. Evaluación Técnica

La evaluación técnica se realizará por medio de un simulador, que permite simular topologías de red y compararlas de manera pertinente. La topología de red base se muestra en la figura 2.20.

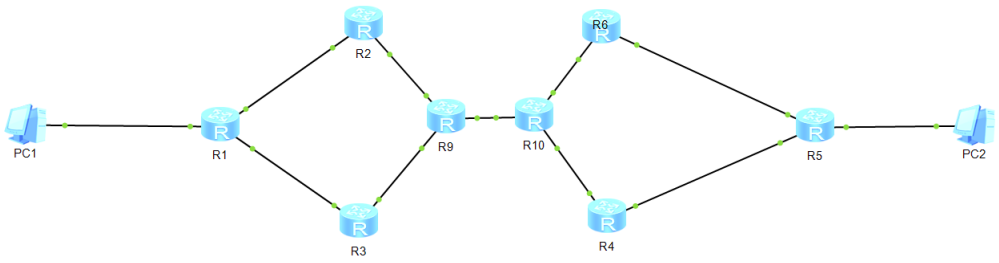

Figura 2.20: Topología de red la evaluación n técnica.

Para llevar a cabo la evaluación técnica necesaria, se realizaron modificaciones en la topología de red anterior. A continuación, se muestran diferentes casos a estudiar:

1. Red de 1 sistema autónomo con OSPF, MPLS e iBGP.
2. Red de 1 sistema autónomo con OSPF, MPLS y BGP-LU.
3. Red con 2 sistemas autónomos con OSPF, MPLS y BGP-LU.

Para cada simulación se comparan las tablas de direcciones de rutas de los routers 1 y 5, con el fin de mantener una línea de comparación. Las topologías de red a simular se presentan con más detalle en cada caso de estudio.

2.8.2.1. Programa eNSP

Para realizar la simulación de las topologías de red propuestas, se utiliza el eNSP. Este es un programa de Huawei que permite simular una topología de red a elección, donde utiliza routers pertenecientes a la empresa. Además, es posible utilizar diferentes configuración de

protocolos, tales como, OSPF, M-BGP, BGP, MPLS y BGP-LU .

En este trabajo se utiliza la siguiente versión del software eNSP v100R003C00SPC100. Como en la mayoría de los softwares de simulación de topologías de red, es necesario complementar con un programa que pueda crear máquinas virtuales, escogiendo VMware en su versión v5.2.26.

Tabla 2.1: Requisitos y herramientas para la simulación en eNSP.

Requisitos	Herramienta
Nodos Backbone	Router Genérico eNSP
Nodos Clientes	Cliente PC
Conexiones entre nodos	Conexión AUTO

La herramienta *Router* se encuentra específicamente en la categoría **Router**. Para realizar conexiones físicas entre los dispositivos en cada topología se utiliza *Auto*, conexión que se encuentra en la categoría de **Connections**. Con el fin de probar el envío de un punto a otro punto de la red, se utiliza el elemento *PC*, perteneciente a la categoría de **End devices**.

2.8.2.2. Configuración generales de los tres casos.

La implementación de cada simulación requiere configuraciones específicas, aunque comparten una base similar. Para asegurar una correcta configuración en cada caso, se sigue el siguiente diagrama:

Figura 2.21: Diagrama general de configuración simulaciones.

La configuración de interfaces y PCs se realiza de manera idéntica en cada una de las simulaciones. Sin embargo, en cada simulación se llevan a cabo configuraciones específicas a nivel de OSPF, MPLS y BGP.

2.8.2.2.1. Configuración PC

Una vez ya conectado todos los elementos de la topología de red, se inicia con el botón de "Start devices". Luego de esto, se ingresa a los PCs para su configuraciones de IPv4, específicamente las direcciones IP, sub-máscaras de red y dirección IP del router (gateway en el programa). A continuación se muestran las direcciones IPs, en la tabla 2.3, para aplicar en los dispositivos finales.

La configuración de estos dispositivos es por medio de la interfaz gráfica del programa. En IPv4 configuration, se selecciona "Static", y se procede a realizar los cambios respectivos de

la tabla 2.2 .

Tabla 2.2: Direcciones IP por usar en PC1 y PC2.

Pc1	*Dirección IP*
Dirección de red	*192.168.1.0 /24*
Dirección del PC	*192.168.1.2 /24*
Dirección de gateway	*192.168.1.1 /24*
Máscara de red	255.255.255.0

Pc2	*Dirección IP*
Dirección de red	*192.168.2.0 /24*
Dirección del PC	*192.168.2.2 /24*
Dirección de gateway	*192.168.2.1 /24*
Máscara de red	255.255.255.0

2.8.2.2.2. Configuración en Interfaces de los routers

Las conexiones físicas entre routers y la interfaz loopback de estos dispositivos tienen que estar definidas por una dirección IP. Se sigue la línea de configuración mostrada en el diagrama 2.22.

Figura 2.22: Diagrama de configuracion de interfaces.

Las interfaces de conexión entre routers se muestran las direcciones a usar en la tabla 2.3.

Tabla 2.3: Tabla de Conexiones router con direcciones de red

Conexión Routers	Dirección de red IP
R1-R2	10.0.0.0 /30
R1-R3	10.0.0.4 /30
R3-R9	10.0.0.16 /30
R2-R9	10.0.0.32 /30
R9-R10	10.0.0.12 /30
R10-R4	10.0.0.36 /30
R10-R6	10.0.0.40 /30
R6-R5	10.0.0.28 /30
R4-R5	10.0.0.24 /30

Las direcciones IP de la interfaz de loopback de los routers en la topología se muestra en la tabla 2.4.

Tabla 2.4: Direcciones IP interfaces loopback de los router.

Router	Dirección IP Loopback
R1	10.0.1.1 /32
R2	10.0.2.1 /32
R3	10.0.3.1 /32
R4	10.0.4.1 /32
R5	10.0.5.1 /32
R6	10.0.6.1 /32
R9	10.0.9.1 /32
R10	10.0.10.1 /32

Una vez ya en la interfaz ethernet 0/0/0 se debe utilizar el comando *ip address X.X.X.X /Y*, el cual definirá que esa es la dirección IPv4 de la interfaz.

Tabla 2.5: Configuración dirección IP interfaz R1

Interfaz R1	Dirección IP
Ethernet 0/0/0	*Interface ethernet 0/0/0* *ip address 192.168.1.2 /24*
Ethernet 0/0/1	*Interface ethernet 0/0/1* *ip address 10.0.0.1 /30*
Giga Ethernet 0/0/0	*Interface Gi 0/0/0* *ip address 10.0.0.5 /30*

Este proceso se repite en cada interfaz de routers conectada a otro router. Las interfaces por configurar se muestran en la figura 2.29.

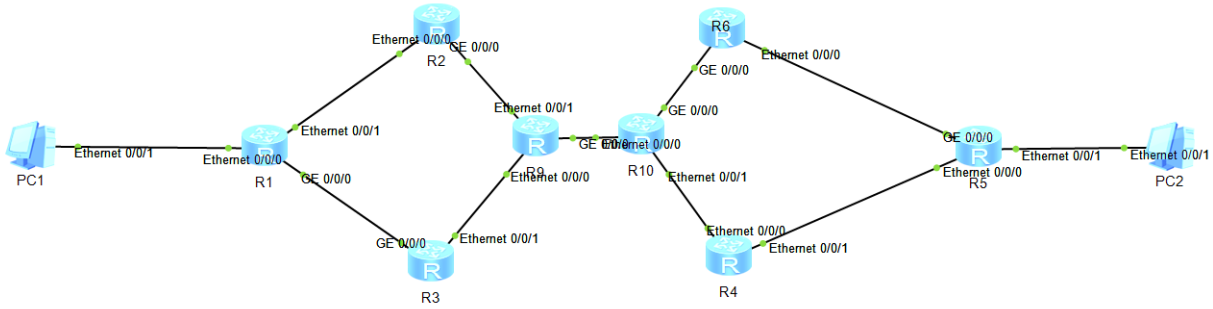

Figura 2.23: Topología de red con interfaces detalladas por router.

2.8.2.3. Simulación 1: Red de 1 sistema autónomo con OSPF, MPLS e iBGP

En este caso de estudio solo existe un sistema autónomo y solo un área OSPF, tal como se muestra en la figura 2.24.

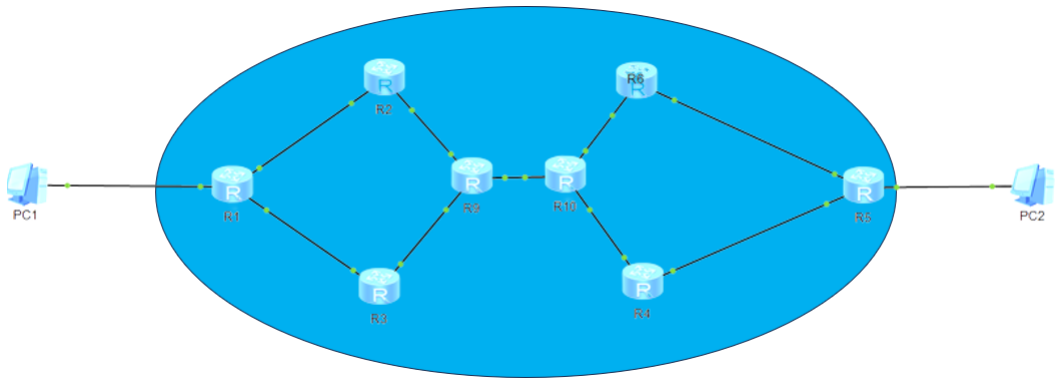

Figura 2.24: Topología de red de Simulación 1.

2.8.2.3.1. OSPF

Para la configuración de OSPF, se tiene que tener en cuenta que se aplica dentro de los sistemas autónomos, implicando que solo se configura un área de OSPF. Dentro de esta área los routers intercambian las rutas OSPF entre todos.

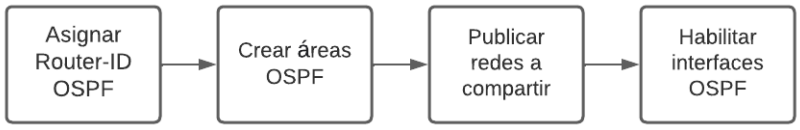

Figura 2.25: Diagrama configuración OSPF.

En la configuración central del router se debe inicializar el proceso OSPF indicando tanto

los router-ID, las IPs loopback y el área a la cual pertenecen los dispositivos. En este caso de estudio los routers de la topología pertenecen a la misma área.

Se utilizan los comandos *ospf 1 router-id X.X.X.X*, donde X.X.X.X es la IP de dirección de la interfaz de loopback del router que está siendo configurado. Con este comando se inicia el proceso de OSPF. Con el comando area 0 se establece en el router el funcionamiento del área.

Por último, se publican las redes que este router anunciara a sus vecinos conectados, utilizando el comando *network X.X.X.X* (dirección IP de la red) *Y.Y.Y.Y* (dirección wildcard[3] de la red). Las redes por publicar son las Interfaces de loopback y las direcciones de red de ambos PCs.

Tabla 2.6: Configuración de comandos OSPF R1.

OSPF R1	Comandos
Router-ID	*OSPF router-id 10.0.1.1 /32*
Área	*area 0*
	network 10.0.1.1 0.0.0.0
Anunciar redes	*network 10.0.0.0 0.0.0.3*
	network 192.168.1.0 0.0.0.255

Ahora se procede a activar OSPF en cada interfaz que se conecta a otro router, donde se utilice este protocolo. Se usan los siguiente comandos *ospf network-type p2p* y *ospf enable 1 area 0*.

Tabla 2.7: Configuración de comandos OSPF en interfaces.

R1	Comandos
GI 0/0/0	*ospf network-type p2p*
	ospf enable 1 area 0
Ethernet 0/0/1	*ospf network-type p2p*
	ospf enable 1 area 0

2.8.2.3.2. MPLS

Es importante que la configuración del protocolo IGP sea primero que la de MPLS, ya que, es necesario que los routers ruteen información entre ellos. Esto se hace con el fin de conectar MPLS por medio de las interfaces de loopbacks. Además, MPLS se configura de tal manera, que existe dentro de cada sistema autónomo de manera independiente, es decir, que en esta topología propuesta, con tres sistemas autónomos, son tres sistemas de MPLS.

[3] Es una sub-mascara de red de 32 bits, la cual esta invertida con respecto a la mascara de red. Esta sub-mascara indica dirección de IP utilizada en *Access-list* y *publicación OSPF*

Figura 2.26: Diagrama configuración MPLS.

El primer paso para la configuración MPLS es inicializar el proceso en el modo system-view, usando el comando mpls lsr-id X.X.X.X (IP de loopback del router la cual funciona como identificador de MPLS). Este proceso se realiza en cada router de la topología.

Luego se debe usar el comando mpls para que se active la configuración en el router generalizado. Seguido de esto, se utiliza el comando *mpls ldp* para activar el protocolo LDP para el intercambio de etiquetas. Este proceso se realiza en cada router de la topología. Como paso final, es necesario acceder a cada interfaz de la topología que se dirija hacia su propio sistema autónomo.

Tabla 2.8: Configuración comandos MPLS.

R1	Comandos
MPLS ID	*mpls lsr-id 10.0.1.1*
Activando MPLS globalmente	*mpls* *mpls ldp*
Activando MPLS interfaz	*interface gi 0/0/0* *mpls* *mpls ldp*

2.8.2.3.3. BGP

Para la inicialización del proceso BGP, se debe de ingresar a la configuración central de cada router que utiliza este protocolo, usando el comando system-view.

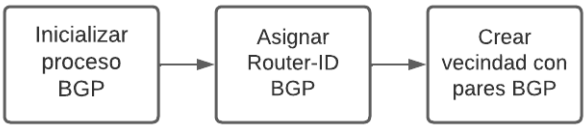

Figura 2.27: Diagrama configuración BGP.

Luego, se debe indicar el sistema autónomo al que pertenece el dispositivo, para esto se usa bgp X, donde X es un número entero que indica el identificador del sistema autónomo, en esta topología la única opción posible es AS-100.

Las conexiones iBGP de este sistema autónomo son por adyacencia, es decir, el R1 se conectará a la interfaz de loopback del R2 y R3, mientras R2 se conecta a R1, R3 y R9. Siguiendo

este patrón se configuran los demás routers de la topología de red. Para que un router aledaño a R3 pueda realizar una conexión con este dispositivo, se debe aplicar el comando *peer X.X.X.X as-number 100* y *peer X.X.X.X connect-interface loopback 1*. Donde X.X.X.X es la dirección de loopback del router 3.

Tabla 2.9: Configuración comandos BGP.

R1	Comandos
Designación numero de AS	*bgp 100*
BGP-ID	*router-id 10.0.1.1*
Conectándose a otros pares	*peer 10.0.2.1 as-number 100* *peer 10.0.2.1 connect-interface loopback 1*

Este proceso se realiza de forma análoga en los demás routers, la lista a continuación indica las conexión iBGP, que deben realizarse desde el primer router hacia los otros:

- R3 con R1, R2 y R9.
- R9 con R3, R2 y R10.
- R10 con R9, R4 y R6
- R6 con R10, R4 y R5
- R4 con R10, R6 y R5
- R5 con R6 y R4

2.8.2.3.4. Verificación de resultados

Con el fin de comparar las direcciones de tablas de rutas recibidas en R1 y R5, se debe ingresar a la configuración central de cada router con system-view, y escribir el siguiente comando *display ip routing-table*, así obtendremos las direcciones de enrutamiento de cada router, donde se indica: el siguiente salto de enrutamiento, con que protocolo aprendió la ruta, el costo asociado a usar la ruta, la interfaz de conexión, entre otros.

2.8.2.4. Simulación 2: Red de 1 sistema autónomo con OSPF, MPLS y BGP-LU

En este caso de estudio solo existe un sistema autónomo, sin embargo, y a diferencia del caso de estudio 1, este tiene un router reflector en la topología, cambiando la configuración de BGP. La topología de red se muestra en la figura 2.28

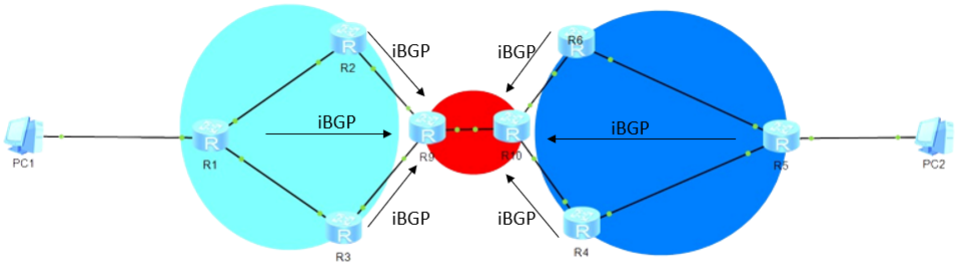

Figura 2.28: Topologia de red Simulacion 2.

R9 y R10 son confgurados como routers reflector en esta simulacion de la topología de red.

2.8.2.4.1. OSPF

Para la configuración de OSPF se tiene que tener en cuenta que se aplica dentro de los sistemas autónomos. Un cambio con respecto a la simulación 1, es que la simulación 2 consta de tres áreas de OSPF. Aquellas corresponden al área 0, área 1 y área 2.

En la configuración central del router se debe inicializar el proceso OSPF indicando tanto los router-ID las IPs loopback como el área a la cual pertenecen los dispositivos, en este caso de estudio los routers de la topología pertenecen a la misma área.

Se utilizan los comandos *ospf 1 router-id X.X.X.X*, donde X.X.X.X es la IP de dirección de la interfaz de loopback del router que está siendo configurado. Con este comando se inicia el proceso de OSPF. Con el comando *area 0*, *area 1* y *area 2* se establecen estas áreas.

Por último, se publican las redes que este router anunciará a sus vecinos conectados utilizando el comando *network X.X.X.X* (dirección IP de la red) *Y.Y.Y.Y* (dirección wildcard de la red, complemento de la submascara de red). Las redes por publicar son las loopback y conexiones entre routers.

Se deben publicar las redes de las interfaces de conexión con *network 10.0.0.0 0.0.0.3*. Este caso es para la conexión entre R1 y R9.

Tabla 2.10: Configuraciones con comandos OSPF 2 áreas en R3.

R3	Comandos
Router-ID	*ospf router-id 10.0.3.1 /32*
Area	*area 0* *area 1*
Publicando rutas Area 1	*network 10.0.0.4 0.0.0.3*
Publicando rutas Area 0	network 10.0.0.16 0.0.0.3

Similarmente se muestra cómo se debe configurar R4 siendo sus conexiones directas R10 y

R5.

Tabla 2.11: Configuraciones con comandos OSPF 2 áreas en R4.

R4	Comandos
Router-ID	*ospf router-id 10.0.3.1 /32*
Area	*area 0* *area 2*
Publicando rutas Area 2	*network 10.0.0.24 0.0.0.3*
Publicando rutas Area 0	network 10.0.0.36 0.0.0.3

Ahora se procede a activar OSPF en cada interfaz que se conecta a otro router, donde se utilice este protocolo. Se usan los siguiente comandos ospf network-type p2p y *ospf enable 1 area 1*. Los router centrales el comando es *area 0*, y los de la derecha *area 2*.

Tabla 2.12: Configuraciones con comandos OSPF en interfaces R3.

R3	Comandos
GI 0/0/0	*ospf network-type p2p* *ospf enable 1 area 1*
Ethernet 0/0/1	*ospf network-type p2p* *ospf enable 1 area 0*

Los comandos a utilizar en la interfaz de R4 también cambian como se muestra en la tabla 2.13.

Tabla 2.13: Configuraciones con comandos OSPF en interfaces R4.

R4	Comandos
Ethernet 0/0/0	*ospf network-type p2p* *ospf enable 1 area 0*
Ethernet 0/0/1	*ospf network-type p2p* *ospf enable 1 area 2*

Con el fin de filtrar las rutas de las direcciones entre las conexiones de los routers, se utiliza un access-list (ACL). En este se procede a solo permitir las rutas de direcciones IP de las loopbacks de los routers. Luego, se procede a aplicar un filtro con este ACL, resultando en una filtración satisfactoria. Este proceso de filtración también se puede lograr con políticas BGP, sin embargo, estas rutas deben ser publicadas junto a la política.

2.8.2.4.2. MPLS

El primer paso para la configuración MPLS es inicializar el proceso en el modo *system-view*, usando el comando *mpls lsr-id X.X.X.X* (dirección IP de loopback del router que se esta configurando). Este proceso se realiza en cada router de la topología.

Luego, se utiliza el comando *mpls* para que se active la configuración en el router generalizado y *mpls ldp* para activar el protocolo LDP para el intercambio de etiquetas. Este proceso se

realiza en cada router de la topología.

Como paso final, es necesario acceder a cada interfaz de la topología que se dirija hacia su propio sistema autónomo. Una vez que se hayan identificado las interfaces que requieren configuración, se accede a ellas mediante los comandos *int ethernet 0/0/0* o *int gi 0/0/0*. Después de ingresar a las interfaces, se utilizan dos comandos importantes: *mpls* para activar la función MPLS y *mpls ldp* para activar el protocolo de transporte de etiquetas.

Tabla 2.14: Configuración con comandos MPLS R1.

R1	Comandos
MPLS ID	*mpls lsr-id 10.0.3.1*
Activando MPLS globalmente	*mpls* *mpls ldp*
Activando MPLS interfaz	*interface Ethernet 0/0/0* *mpls* *mpls ldp*

2.8.2.4.3. BGP

El diagrama a continuación muestra los pasos a seguir para configurar iBGP de manera correcta en este caso de estudio:

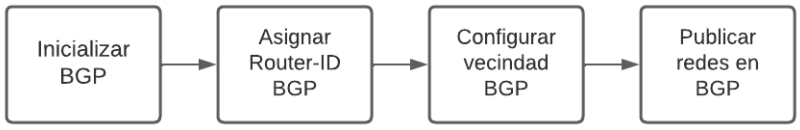

Figura 2.29: Diagrama configuración BGP.

La inicialización del proceso BGP, se debe de ingresar a la configuración central de cada router que utiliza este protocolo, usando el comando system-view. Luego, indicar el sistema autónomo al que pertenece el dispositivo, para esto se usa *bgp X*, donde X es un número entero que indica el identificador del sistema autónomo, en esta topología la única opción posible es AS-100.

Al estar en presencia de dos RR, las conexiones iBGP de este sistema autónomo se realizan de la siguiente forma:

- R10 se conectará por iBGP a R1, R2, R3 y R9.
- R1 a R10.
- R2 a R10.
- R3 a R10.

- R9 a R4, R5, R6 y R10.
- R4 a R9.
- R5 a R9.
- R8 a R9.

La configuración de R9 y R10 como routers reflector (RR) se realiza en el proceso de BGP de cada router. A continuación, se especifica qué dispositivos de enrutamiento actuarán como clientes del RR. En el caso de R9, sus clientes son R10, R3, R2 y R1. Para lograr esto, es necesario configurar el RR para que publique las rutas de estos routers clientes. Para ello, se utiliza el comando *peer X.X.X.X reflect-client*, donde X.X.X.X representa las direcciones IP de R10, R3, R2 y R1.

Para R10, sus clientes son R9, R4, R5 y R6. En este caso, se utiliza el mismo comando *peer X.X.X.X reflect-client*, pero ahora X.X.X.X representa las direcciones IP de R9, R4, R5 y R6.

Además, es importante configurar la capacidad de los RR para publicar las rutas de R2, R3, R10 y R1. Esto se logra mediante el comando *peer X.X.X.X next-hop-local* en cada uno de los routers clientes de R9. Para R10, se realiza de manera similar con el mismo comando, pero publicando las rutas de R9, R4, R5 y R6.

Tabla 2.15: Configuración con comandos de R10 como Router reflector.

R10	Comandos
Designación numero de AS	*bgp 100*
BGP-ID	*router-id 10.0.10.1*
	peer 10.0.2.1 reflect-client
Conectándose a otros pares	*peer 10.0.2.1 next-hop-local*
	peer 10.0.2.1 label-route-capability

Luego, se deben de publicar las redes que se desean transmitir a través de BGP, que corresponden a las direcciones de los PCs en la red. Por ejemplo, para la red de PCs, se utiliza el comando *network 192.168.1.0 24* en R1 y el comando *network 192.168.2.0 24* en R5. De esta manera, se configuran adecuadamente las redes respectivas en cada uno de los routers.

Tabla 2.16: Configuración con comandos de publicación de redes en BGP en R1.

R1	Comandos
BGP	*bgp100*
Router-ID	*router-id 10.0.1.1*
Publicar rutas en BGP	*network 192.168.1.0 /24 route-policy 1 export*

2.8.2.4.4. Verificaciones de resultados

Al igual que en la simulación 1, necesitamos obtener las tablas de enrutamiento recibidas en R1 y R5. Sin embargo, en esta ocasión, compararemos estas tablas con las obtenidas en la primera simulación. Para obtener las tablas de enrutamiento en la simulación 2, debemos acceder a la configuración central de cada enrutador utilizando el comando *system-view*. Luego, ejecutamos el comando *display ip routing-table* para visualizar las tablas de enrutamiento. Esto nos permitirá obtener información detallada sobre las rutas presentes en cada router y compararlas con las obtenidas en la simulación anterior.

Ahora vamos a verificar si la función de envío de etiquetas MPLS, a través del protocolo BGP, se está cumpliendo correctamente. Para ello, utilizaremos el comando *display mpls lsp*, el cual mostrará las direcciones que están siendo publicadas por BGP-LU. Este comando nos permitirá examinar y confirmar que las etiquetas MPLS se están propagando adecuadamente a través del protocolo BGP. Ahora se quitara el funcionamiento del protocolo LDP como caso de interés, utilizando el comando *undo mpls ldp* en la configuración central de R1, y después veremos el resultado con *display mpls lsp*.

2.8.2.5. Simulación 3: Red con 2 sistemas autónomos con OSPF, MPLS y BGP-LU

2.8.2.5.1. Consideraciones

Existen dos sistemas autónomos diferentes en la simulación. Uno donde se encuentras dispositivos de Agregación y Acceso, serán azules. Y el de Core, de color rojo, tal como, se muestra en la figura 2.30

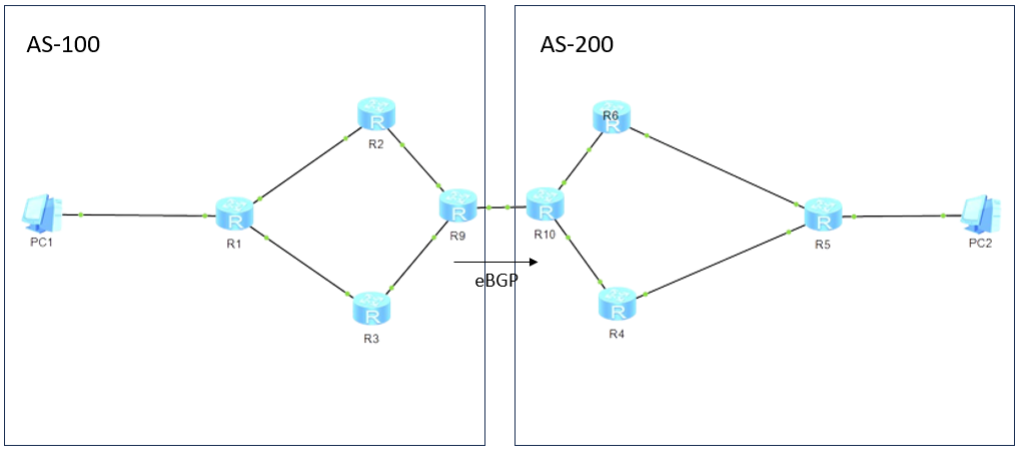

Figura 2.30: Topología de red Simulación 3.

- AS-100: R1, R2, R3 y R9.
- AS-200: R10, R4, R5 Y R6.

2.8.2.5.2. OSPF

En esta simulación, se tiene dos áreas OSPF, sin embargo, estas no se conectan entre si, debido a estar en diferentes sistemas autonomos. Estas áreas, que se encuentran en diferentes sistemas autónomos, son áreas de backbone.

Se debe ingresar al modo *system-view*, luego en cada interfaz que se conecte a otro dispositivo y que utilice OSPF, debe dividirse lógicamente con los comandos ospf network-type p2p y *ospf enable 1 area 0*.

Ahora en la configuración central del router se debe inicializar el proceso OSPF indicando tanto los router-ID (las cuales son las direcciones IPs loopback), como el área que pertenece esta configuración.

Por último, dentro del área OSPF, se publican las redes que este router anunciará a sus vecinos conectados utilizando el comando *network X.X.X.X* (dirección IP de la red) *Y.Y.Y.Y* (dirección wildcard de la red). Las direcciones por publicar son las conexiones entre routers y loopbacks de cada router.

Tabla 2.17: Configuración de comandos OSPF R1.

OSPF R1	Comandos
Router-ID	*OSPF router-id 10.0.1.1 /32*
Área	*area 0*
Anunciar redes	*network 10.0.1.1 0.0.0.0* *network 10.0.0.0 0.0.0.3*

2.8.2.5.3. MPLS

Para el caso de estudio de BGP-LU la configuración es bastante similar, con cambios específicos en las interfaces que se conectan a otro sistema autónomo. Esto se hace para activar el intercambio de etiquetas MPLS entre dos diferentes sistemas.

El primer paso para la configuración MPLS es inicializar el proceso en el modo *system-view*, usando el comando *mpls lsr-id X.X.X.X* (IP de loopback del router la cual funciona como identificador de MPLS). Este proceso se realiza en cada router de la topología.

Luego, se debe usar el comando *mpls* para que se active la configuración MPLS en el router. Segudo de eso se hace uso del comando *mpls ldp* para activar el protocolo LDP para el intercambio de etiquetas. Este proceso se realiza en cada router de la topología.

Se debe ingresar a cada interfaz de la topología que se encuentre en dirección a su propio sistema autónomo. Una vez identificadas las interfaces a configurar, se ingresa a ellas con el comando *int ethernet 0/0/0* o *gi 0/0/0*. Luego de haber ingresado, se utilizan los comandos *mpls* para activar la función MPLS y mpls ldp en la interfaz.

Por último, la configuración de interfaces entre sistemas autónomos, siendo la conexión entre

los routers R9 a R10. Ya identificada esta interfaces, se procede a configurar solo *mpls*, ya que se desea que BGP realice esta distribución de etiquetas.

Tabla 2.18: Configuración conexión MPLS de R9 a R19.

R9	Comandos
MPLS ID	*mpls lsr-id 10.0.9.1*
Activando MPLS globalmente	*mpls*
Activando MPLS en la interfaz	*int gi 0/0/0* *mpls*

2.8.2.5.4. BGP

La configuración BGP de sistemas autónomos es diferente que en el caso base, ya que, se debe configurar eBGP entre el AS100 y AS-200. En la configuración de los routers reflector, esto se deben configura uno por cada sistema autónomo, es decir, AS-100 y AS-200, se le asigna R9 y R10 como RR respectivamente.

En cuanto a la configuración de iBGP, el cambio principal es que los routers clientes del RR ya no se comunicarán entre sí mediante iBGP. Ahora, es el RR el encargado de enrutar entre ellos para establecer la comunicación.

La configuración en ambos routers se realiza utilizando el comando *peer IP 10.0.0.34 AS-number X*, donde X representa el número del sistema autónomo al que pertenece la interfaz objetivo. En el caso de R2 a R9, el comando se modifica de la siguiente manera, *peer 10.0.0.33 AS-number 100*.

La configuración de R9 y R10 como Routers Reflectors (RR) se realiza en el proceso de BGP de cada router. Para ello, se ingresa el comando *bgp 100* en cada uno de los routers. Luego, se indica qué dispositivos de enrutamiento serán clientes del RR. Además, se debe configurar el RR para publicar las rutas de los routers clientes.

En R9, se utiliza el comando *peer 10.0.1.1 reflect-client* para indicar que R1 es cliente de R9. Este mismo comando se aplica en R3 y R2. A continuación, se configura la capacidad de los RR como publicadores de las rutas de R1 utilizando el comando *peer 10.0.1.1 next-hop-local*, este comando es similar en R2 como en R3.

Para la configuración de iBGP en el caso de AS-100, se establece la conexión de R9 a R1, R9 a R2 y R9 a R3. Luego, cada uno de ellos establecerá una sesión iBGP hacia R9.

R10 identifica que sus clientes reflector R4, R5 y R6. El comando para indicar es el mismo, *peer 10.0.6.1 reflect-client*, el cual indica que R5 es cliente de R10. Se utiliza el mismo comando, ahora con direcciones de loopback de R5 y R6. A continuación, se configura la capacidad de los RR como publicadores de las rutas de R10 utilizando el comando *peer 10.0.6.1 next-hop-local*, este comando es similar en R4 como en R5.

Tabla 2.19: Configuración con comandos de R9 como Router reflector.

R9	Comandos
Designación numero de AS	*bgp 100*
BGP-ID	*router-id 10.0.9.1*
Conectándose a otros pares	*peer 10.0.2.1 as-number 100*
	peer 10.0.2.1 reflect-client
	peer 10.0.2.1 next-hop-local
	peer 10.0.2.1 label-route-capability

Para la configuración de iBGP en el caso de AS-200, se establece la conexión de R4 a R10, R10 a R5 y R10 a R6. Luego, cada uno de ellos establecerá una sesión iBGP hacia R10. Para el caso de eBGP que se aplica desde R9 a R10.

Tabla 2.20: Configuración con comandos de R10 a R9

R10	Comandos
Designación numero de AS	*bgp 100*
BGP-ID	*router-id 10.0.10.1*
Conectándose a otros pares	*peer 10.0.9.1 as-number 100*
	peer 10.0.9.1 coonect-interface loopback 1
	peer 10.0.9.1 label-route-capability check-tunnel-reachable

Ahora R1 y R5 deben publicar las rutas de PC en BGP, respectivamente, con comando *network 192.168.1.0 24 route-policy 1 export* en la configuración central de BGP.

Tabla 2.21: Configuración con comandos de publicación de redes en BGP R1.

R1	Comandos
BGP	*bgp100*
Router-ID	*router-id 10.0.1.1*
Publicar rutas en BGP	*network 192.168.1.0 /24 route-policy 1 export*

2.8.2.5.5. Verificaciones de resultados

Para obtener las tablas de enrutamiento en la simulación 3, debemos acceder a la configuración central de cada enrutador utilizando el comando system-view. Luego, ejecutamos el comando *display ip routing-table* para visualizar las tablas de enrutamiento. Esto nos permitirá obtener información detallada sobre las rutas presentes en cada router.

Ahora vamos a verificar si la función de envío de etiquetas MPLS a través del protocolo BGP se está cumpliendo correctamente. Para ello, utilizaremos el comando *display mpls lsp*, el cual mostrará las direcciones que están siendo publicadas por BGP-LU. Este comando nos permitirá examinar y confirmar que las etiquetas MPLS se están propagando adecuadamente a través del protocolo BGP.

2.8.3. Evaluación económica

La evaluación económica que se llevará a cabo en este informe consiste en contrastar los beneficios en términos de reducción del CAPEX y OPEX de dos proyectos en particular. El primer proyecto implica la aplicación del protocolo BGP-LU utilizando un router en una versión compacta. Por otro lado, el segundo proyecto implica el uso de un router sin la implementación del protocolo, pero con capacidad para manejar una mayor cantidad de rutas.

- CAPEX (Gasto de Capital): Se refiere a los costos asociados a la adquisición inicial de activos fijos necesarios para la implementación de los proyectos. Esto incluye la compra de equipos, infraestructura de red, licencias de software y cualquier otro gasto de inversión inicial.
- OPEX (Gastos Operativos): Se refiere a los gastos operativos asociados al funcionamiento continuo de los proyectos. Esto puede incluir gastos como el mantenimiento y soporte técnico, los costos de energía y climatización, los gastos de personal, los contratos de servicios, entre otros.

Al tener en cuenta estos aspectos, se podrá realizar una evaluación exhaustiva de los costos de inversión inicial y los costos operativos a largo plazo de los proyectos, lo que permitirá una comparación adecuada de su viabilidad económica.

2.8.3.1. Consideraciones

En el análisis del CAPEX (gasto de capital) de los proyectos mencionados anteriormente, excluiremos los módulos ópticos, tarjetas de servicios y switches de esta sección. Este mismo análisis se realiza con respecto al costo del equipo de climatización, ya que representa una variación del 1 % con respecto al costo de los router a evaluar.

En el caso del OPEX (gasto operativo), al igual que en el CAPEX, no se considerará el costo de importación de los bienes ni los trabajos de ingeniería relacionados con la instalación y puesta en servicio de los equipos. Además, se considera que los trabajos de emplazamiento, canalización de energía y servicios de ingeniería en terreno para el despliegue de los equipos

protocolo y obras civiles. Se consideran similares tanto en tema de espacio como uso de recursos.

El análisis principal de esta sección se centra en dos aspectos fundamentales. En primer lugar, se evaluará la energía requerida por los equipos, medida en Watts consumidos. En segundo lugar, se tendrá en cuenta la climatización mediante aire acondicionado necesaria para mantener los equipos dentro de las temperaturas de funcionamiento adecuadas.

2.8.3.1.1. Proyecto con cambio de router y aplicación de BGP-LU

El router a utilizar es, Huawei NetEngine 8000 F1A. Este router tiene capacidad de almacenamiento bajas a lo requerido actualmente en la red, sin embargo, con la aplicación del protocolo BGP-LU, este dispositivo tiene la posibilidad de estar conectado en la red.

Especificaciones técnicas del equipo Huawei NetEngine 8000 F1-8H20Q [25].

- Dimensiones: Altura = 43.6 mm profundidad = 420 mm y ancho = 442 mm.
- 325 Watts de consumo típico del equipo.
- 1054.44 BTU /h de climatización de consumo tipo del equipo.
- Por confidencialidad, tanto para la empresa fabricante como el operador, el precio de este equipo se mantendrá oculto, asignando un valor proporcional al router Huawei NE40E-X16A, el cual es $ 11.11X CLP.

2.8.3.1.2. Proyecto de cambio de Router con mayor procesamiento y tabla de rutas posibles

El router a utilizar en la comparación económica del OPEX y CAPEX, específicamente en el proyecto de dispositivo con mayor procesamiento de recursos computacionales y de memoria, es el router Huawei NE40E-X16A. Este equipo tiene que tenert un total 12 tarjetas de servicios para cumplir su función de enrutamiento.

Especificaciones técnicas del equipo Huawei NE40E-X16A [26]:

- Dimensiones: Altura = 1778 mm Profundidad = 650 mm y Ancho = 442 mm.
- 7,720 Watts de consumo típico del equipo.
- 25,046.9 BTU/h de climatización de consumo tipo del equipo.
- Por confidencialidad, tanto para la empresa fabricante como el operador, el precio de este equipo se mantendrá oculto, asignando su valor como $ X CLP. Este precio considera 4 tarjetas de unidad de procesamiento y 8 tarjetas de enrutamiento, con puertos necesarios para el funcionamiento de la red.

2.8.3.2. Evaluación CAPEX

Para la evaluación de CAPEX de ambos routers se utiliza la siguiente ecuación:

$$\%_C = \frac{P_{F1A}}{P_{NE40E}} \cdot 100 \tag{2.1}$$

Donde:

%c = Es el porcentaje que representa el router NE 8000 F1A con respecto al NE40E-X16A.

P_{NE40E} = El costo asociado al router NE40E-X16A.

P_{F1A} = El costo asociado al router 8000 F1A.

Para calcular la tasa de reducción se utiliza la ecuación 2.2.

$$T_RC = 100 - \%_C \tag{2.2}$$

Donde:

T_RC = La tasa de reducción de costo.

%c = El porcentaje calculado en la ecuacion .

2.8.3.3. Evaluación OPEX

Ya que el consumo de los equipos se encuentra en Watts, el único valor que queda es lo consumido para su climatización. Con el fin de obtener el consumo energético de ambos router se utiliza la siguiente conversión 1 $BTU = 0.2931$ Watts

Una vez realizada esta conversión con la ecuación 2.3 se calcula los Watts consumidos.

$$W/h_{total} = W_{Consumidos} + W_{BTU} \tag{2.3}$$

Luego, de calcular el valor total de Watts consumidos, se procede a calcular el gasto operacional utilizando la ecuación 2.4. Para esto se extrae el precio medio del mercado eléctrico nacional, dato de la Comisión nacional de energía (CNE), el cual en el mes de Julio del año 2023 es \$106.49 CLP/W [27].

$$G_{CE} = 106.49 \cdot W/h_{toal} \tag{2.4}$$

Ahora para tener la tasa de reducción del gasto operacional, se procede a utilizar la siguiente ecuación.

$$T_{RO} = \frac{G_{CENE40E} - G_{CEF1A}}{G_{CENE40E}} \cdot 100 \tag{2.5}$$

Capítulo 3

Resultados

3.1. Resultado evaluación técnica

En este capitulo se presentan los resultados obtenidos de las siguiente simulaciones: Caso base, Seamless MPLS intra-AS y Seamless MPLS inter-AS.

Se presentan las tablas de direcciones de rutas, en caso de las tres simulaciones, y las etiquetas MPLS transmitidas por BGP, en el caso de las simulación de Seamless MPLS. Estas mediciones se aplican a los tres casos.

3.1.1. Simulación 1: Topología de red caso base: OSPF, MPLS e iBGP.

Se presentan a continuación las direcciones de interfaces que aprende el router 1 y añade en su tabla de rutas tal como se muestra en la figura 3.1, con un total de 39 rutas almacenadas.

```
Routing Tables: Public
         Destinations : 26        Routes : 39

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/30  Direct  0    0           D   10.0.0.1        Ethernet0/0/1
        10.0.0.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
        10.0.0.4/30  Direct  0    0           D   10.0.0.5        GigabitEthernet
0/0/0
        10.0.0.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
        10.0.0.8/30  OSPF    10   2           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   2           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.12/30  OSPF    10   3           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   3           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.16/30  OSPF    10   2           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.20/30  OSPF    10   5           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   5           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.24/30  OSPF    10   5           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   5           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.28/30  OSPF    10   5           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   5           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.32/30  OSPF    10   2           D   10.0.0.2        Ethernet0/0/1
       10.0.0.36/30  OSPF    10   4           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   4           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.40/30  OSPF    10   4           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   4           D   10.0.0.6        GigabitEthernet
```

Figura 3.1: Tabla de rutas interfaces R1.

En la figura 3.2 se muestran las direcciones de interfaz de loopback aprendidas por el router 1.

```
     10.0.0.40/30  OSPF    10   4           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   4           D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack1
      10.0.2.1/32  OSPF    10   1           D   10.0.0.2        Ethernet0/0/1
      10.0.3.1/32  OSPF    10   1           D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.4.1/32  OSPF    10   4           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   4           D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.5.1/32  OSPF    10   5           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   5           D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.6.1/32  OSPF    10   4           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   4           D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.9.1/32  OSPF    10   2           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   2           D   10.0.0.6        GigabitEthernet
0/0/0
     10.0.10.1/32  OSPF    10   3           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   3           D   10.0.0.6        GigabitEthernet
0/0/0
     127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.1.0/24  Direct  0    0           D   192.168.1.1     Ethernet0/0/0
   192.168.1.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
   192.168.2.0/24  OSPF    10   6           D   10.0.0.2        Ethernet0/0/1
                   OSPF    10   6           D   10.0.0.6        GigabitEthernet
0/0/0
```

Figura 3.2: Tabla de rutas R1.

En la figura 3.3, se observa las tablas de dirección de rutas de interfaces recibidas por el router 5, además, la información de almacenamiento de 38 de rutas aprendidas.

```
Routing Tables: Public
         Destinations : 26        Routes : 38

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.0.0.0/30  OSPF    10   5           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   5           D   10.0.0.29       GigabitEthernet
0/0/0
       10.0.0.4/30  OSPF    10   5           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   5           D   10.0.0.29       GigabitEthernet
0/0/0
       10.0.0.8/30  OSPF    10   5           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   5           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.0.12/30  OSPF    10   3           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   3           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.0.16/30  OSPF    10   4           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   4           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.0.20/30  OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
      10.0.0.24/30  Direct  0    0           D   10.0.0.26       Ethernet0/0/0
      10.0.0.26/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
      10.0.0.28/30  Direct  0    0           D   10.0.0.30       GigabitEthernet
0/0/0
      10.0.0.30/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
      10.0.0.32/30  OSPF    10   4           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   4           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.0.36/30  OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
      10.0.0.40/30  OSPF    10   2           D   10.0.0.29       GigabitEthernet
```

Figura 3.3: Tabla de rutas R5 interfaces de conexión.

A continuación se muestran las direcciones IP de las interfaces loopback que aprende Router 5, figura 3.4

```
      10.0.0.40/30  OSPF    10   2           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.1.1/32   OSPF    10   5           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   5           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.2.1/32   OSPF    10   4           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   4           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.3.1/32   OSPF    10   4           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   4           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.4.1/32   OSPF    10   1           D   10.0.0.25       Ethernet0/0/0
      10.0.5.1/32   Direct  0    0           D   127.0.0.1       LoopBack1
      10.0.6.1/32   OSPF    10   1           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.9.1/32   OSPF    10   3           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   3           D   10.0.0.29       GigabitEthernet
0/0/0
     10.0.10.1/32   OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   2           D   10.0.0.29       GigabitEthernet
0/0/0
     127.0.0.0/8    Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   6           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   6           D   10.0.0.29       GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     Ethernet0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
```

Figura 3.4: Tabla de rutas R5 interfaces loopback.

En la figura 3.5 se ve las etiquetas MPLS distribuidas por el protocolo LDP tanto del router 1 como el router 5.

```
                LSP Information: LDP LSP
--------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
10.0.2.1/32         NULL/3        -/Eth0/0/1
10.0.2.1/32         1024/3        -/Eth0/0/1
10.0.3.1/32         NULL/3        -/GE0/0/0
10.0.3.1/32         1025/3        -/GE0/0/0
10.0.1.1/32         3/NULL        -/-
10.0.4.1/32         NULL/1030     -/Eth0/0/1
10.0.4.1/32         1030/1030     -/Eth0/0/1
10.0.4.1/32         NULL/1030     -/GE0/0/0
10.0.4.1/32         1030/1030     -/GE0/0/0
10.0.5.1/32         NULL/1028     -/Eth0/0/1
10.0.5.1/32         1028/1028     -/Eth0/0/1
10.0.5.1/32         NULL/1028     -/GE0/0/0
10.0.5.1/32         1028/1028     -/GE0/0/0
10.0.6.1/32         NULL/1029     -/GE0/0/0
10.0.6.1/32         1029/1029     -/GE0/0/0
10.0.6.1/32         NULL/1029     -/Eth0/0/1
10.0.6.1/32         1029/1029     -/Eth0/0/1
10.0.9.1/32         NULL/1026     -/Eth0/0/1
10.0.9.1/32         1026/1026     -/Eth0/0/1
10.0.9.1/32         NULL/1026     -/GE0/0/0
10.0.9.1/32         1026/1026     -/GE0/0/0
10.0.10.1/32        NULL/1027     -/GE0/0/0
10.0.10.1/32        1027/1027     -/GE0/0/0
10.0.10.1/32        NULL/1027     -/Eth0/0/1
10.0.10.1/32        1027/1027     -/Eth0/0/1
```

(a) Tabla etiquetas R1.

```
                LSP Information: LDP LSP
--------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
10.0.1.1/32         NULL/1024     -/GE0/0/0
10.0.1.1/32         1024/1024     -/GE0/0/0
10.0.2.1/32         NULL/1025     -/GE0/0/0
10.0.2.1/32         1025/1025     -/GE0/0/0
10.0.3.1/32         NULL/1026     -/GE0/0/0
10.0.3.1/32         1026/1026     -/GE0/0/0
10.0.9.1/32         NULL/1027     -/GE0/0/0
10.0.9.1/32         1027/1027     -/GE0/0/0
10.0.10.1/32        NULL/1028     -/GE0/0/0
10.0.10.1/32        1028/1028     -/GE0/0/0
10.0.5.1/32         3/NULL        -/-
10.0.6.1/32         NULL/3        -/GE0/0/0
10.0.6.1/32         1029/3        -/GE0/0/0
10.0.4.1/32         NULL/3        -/Eth0/0/0
10.0.4.1/32         1030/3        -/Eth0/0/0
10.0.1.1/32         NULL/1026     -/Eth0/0/0
10.0.1.1/32         1024/1026     -/Eth0/0/0
10.0.2.1/32         NULL/1027     -/Eth0/0/0
10.0.2.1/32         1025/1027     -/Eth0/0/0
10.0.3.1/32         NULL/1028     -/Eth0/0/0
10.0.3.1/32         1026/1028     -/Eth0/0/0
10.0.9.1/32         NULL/1029     -/Eth0/0/0
10.0.9.1/32         1027/1029     -/Eth0/0/0
10.0.10.1/32        NULL/1030     -/Eth0/0/0
10.0.10.1/32        1028/1030     -/Eth0/0/0
```

(b) Tabla etiquetas R5.

Figura 3.5: Tabla de etiquetas Caso base.

3.1.2. Análisis de resultados de Simulación 2: Topología de red caso base: OSPF, MPLS e iBGP.

Los resultados obtenidos en esta simulación son consistentes con las expectativas. En primer lugar, se observa que tanto el Router 1 como el Router 5 tienen 38 rutas aprendidas. Además, tanto R1 como R5 aprenden todas las rutas a través del protocolo OSPF, a pesar de la presencia de iBGP. Esto indica que el protocolo IGP es preferido en esta configuración interna del sistema autónomo.

En cuanto a la distribución de etiquetas MPLS, los resultados obtenidos son acordes a lo esperado. El protocolo LDP se encarga de distribuir las etiquetas MPLS, especialmente para las direcciones IP de las interfaces de loopback. Sin embargo, es importante señalar que no

es capaz de transmitir etiquetas para las direcciones IP de los PCs ubicados en los extremos.

3.1.3. Simulación 2: Topología de red caso Seamless MPLS intra-AS: OSPF, MPLS e iBGP-LU.

En la simulación del caso Seamless MPLS intra-AS, se presentan los siguiente resultado de interfaces de conexión de R1, como se muestra en la figura 3.6, con un total de 16 rutas.

```
Routing Tables: Public
         Destinations : 16        Routes : 18

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.0.0.0/30  Direct  0    0           D   10.0.0.1        Ethernet0/0/1
       10.0.0.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
       10.0.0.4/30  Direct  0    0           D   10.0.0.5        GigabitEthernet
0/0/0
       10.0.0.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
       10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack1
       10.0.2.1/32  OSPF    10   300         D   10.0.0.2        Ethernet0/0/1
       10.0.3.1/32  OSPF    10   300         D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.5.1/32  IBGP    255  0          RD   10.0.9.1        GigabitEthernet
0/0/0
       10.0.9.1/32  OSPF    10   301         D   10.0.0.2        Ethernet0/0/1
                    OSPF    10   301         D   10.0.0.6        GigabitEthernet
0/0/0
      10.0.10.1/32  OSPF    10   302         D   10.0.0.2        Ethernet0/0/1
                    OSPF    10   302         D   10.0.0.6        GigabitEthernet
0/0/0
     10.125.0.0/24  Static  60   0           D   0.0.0.0         NULL0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     Ethernet0/0/0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
    192.168.2.0/24  IBGP    255  0          RD   10.0.9.1        GigabitEthernet
0/0/0
```

Figura 3.6: Tabla de rutas R1 interfaces de conexión.

```
                LSP Information: BGP  LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
10.0.1.1/32         1027/NULL     -/-
192.168.1.0/24      1028/NULL     -/-
192.168.2.0/24      NULL/1038     -/-
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
10.0.3.1/32         NULL/3        -/GE0/0/0
10.0.3.1/32         1024/3        -/GE0/0/0
10.0.2.1/32         NULL/3        -/Eth0/0/1
10.0.2.1/32         1025/3        -/Eth0/0/1
10.0.1.1/32         3/NULL        -/-
10.0.4.1/32         NULL/1035     -/GE0/0/0
10.0.4.1/32         1037/1035     -/GE0/0/0
10.0.5.1/32         NULL/1036     -/GE0/0/0
10.0.5.1/32         1038/1036     -/GE0/0/0
10.0.6.1/32         NULL/1037     -/GE0/0/0
10.0.6.1/32         1039/1037     -/GE0/0/0
10.0.10.1/32        NULL/1038     -/GE0/0/0
10.0.10.1/32        1040/1038     -/GE0/0/0
10.0.4.1/32         NULL/1035     -/Eth0/0/1
10.0.4.1/32         1037/1035     -/Eth0/0/1
10.0.5.1/32         NULL/1036     -/Eth0/0/1
10.0.5.1/32         1038/1036     -/Eth0/0/1
10.0.6.1/32         NULL/1037     -/Eth0/0/1
10.0.6.1/32         1039/1037     -/Eth0/0/1
10.0.9.1/32         NULL/1026     -/Eth0/0/1
10.0.9.1/32         1026/1026     -/Eth0/0/1
10.0.9.1/32         NULL/1026     -/GE0/0/0
10.0.9.1/32         1026/1026     -/GE0/0/0
10.0.10.1/32        NULL/1038     -/Eth0/0/1
10.0.10.1/32        1040/1038     -/Eth0/0/1
```

Figura 3.7: Tabla de etiquetas R1.

En la figura 3.7, se observa las etiquetas MPLS, distribuidas tanto por el protocolo LDP

como BGP-LU.

Las direcciones de interfaces de conexión perteneciente la tabla de rutas del router 5, se muestran a continuación en la figura 3.8.

```
Routing Tables: Public
         Destinations : 14        Routes : 15

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.24/30  Direct  0    0           D   10.0.0.26       Ethernet0/0/0
      10.0.0.26/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
      10.0.0.28/30  Direct  0    0           D   10.0.0.30       GigabitEthernet
0/0/0
      10.0.0.30/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
       10.0.1.1/32  IBGP    255  0          RD   10.0.10.1       GigabitEthernet
0/0/0
       10.0.4.1/32  OSPF    10   1           D   10.0.0.25       Ethernet0/0/0
       10.0.5.1/32  Direct  0    0           D   127.0.0.1       LoopBack1
       10.0.6.1/32  OSPF    10   1           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.10.1/32  OSPF    10   2           D   10.0.0.29       GigabitEthernet
0/0/0
                    OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  IBGP    255  0          RD   10.0.10.1       GigabitEthernet
0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     Ethernet0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
```

Figura 3.8: Tabla de rutas interfaces de conexión R5.

Se procede a mostrar, en la figura 3.9, las etiquetas MPLS que aprende router 5 por medio del protocolo LDP y BGP-LU.

```
------------------------------------------------------------------------------
                LSP Information: BGP  LSP
------------------------------------------------------------------------------
FEC               In/Out Label  In/Out IF                     Vrf Name
10.0.5.1/32       1026/NULL     -/-
192.168.2.0/24    1027/NULL     -/-
192.168.1.0/24    NULL/1038     -/-
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC               In/Out Label  In/Out IF                     Vrf Name
10.0.5.1/32       3/NULL        -/-
10.0.6.1/32       NULL/3        -/GE0/0/0
10.0.6.1/32       1024/3        -/GE0/0/0
10.0.4.1/32       NULL/3        -/Eth0/0/0
10.0.4.1/32       1025/3        -/Eth0/0/0
10.0.1.1/32       NULL/1035     -/GE0/0/0
10.0.1.1/32       1037/1035     -/GE0/0/0
10.0.2.1/32       NULL/1036     -/GE0/0/0
10.0.2.1/32       1038/1036     -/GE0/0/0
10.0.3.1/32       NULL/1037     -/GE0/0/0
10.0.3.1/32       1039/1037     -/GE0/0/0
10.0.9.1/32       NULL/1038     -/GE0/0/0
10.0.9.1/32       1040/1038     -/GE0/0/0
10.0.1.1/32       NULL/1035     -/Eth0/0/0
10.0.1.1/32       1037/1035     -/Eth0/0/0
10.0.2.1/32       NULL/1036     -/Eth0/0/0
10.0.2.1/32       1038/1036     -/Eth0/0/0
10.0.3.1/32       NULL/1037     -/Eth0/0/0
10.0.3.1/32       1039/1037     -/Eth0/0/0
10.0.9.1/32       NULL/1038     -/Eth0/0/0
10.0.9.1/32       1040/1038     -/Eth0/0/0
10.0.10.1/32      NULL/1030     -/Eth0/0/0
10.0.10.1/32      1032/1030     -/Eth0/0/0
10.0.10.1/32      NULL/1030     -/GE0/0/0
10.0.10.1/32      1032/1030     -/GE0/0/0
```

Figura 3.9: Tabla de rutas interfaces de loopback R5.

3.1.4. Análisis de Simulación 2: Topología de red escenario Seamless MPLS intra-AS: OSPF, MPLS e iBGP-LU

Las tablas de rutas en las interfaces de conexión entre los routers ya no son aprendidas por los dispositivos de la topología de red, lo que resulta en una reducción del tamaño de la tabla de rutas. Sin embargo, las interfaces de loopback de los dispositivos dentro del sistema autónomo siguen siendo transmitidas, incluso si se encuentran en diferentes áreas. A pesar de esto, al disminuir el tamaño de la tabla de rutas, se logra un menor consumo de recursos de procesamiento y memoria en estos equipos.

La dirección IP del PC2 se aprende a través del protocolo iBGP en R1, mientras que R5 está conectado directamente. Este resultado es esperado y confirma el correcto funcionamiento de BGP en la red. De manera similar, el PC1 está conectado directamente a R1, mientras que R5 aprende la ruta a través de BGP. Las interfaces de loopback de cada dispositivo se aprenden mediante OSPF, a pesar de estar en diferentes áreas. En el caso de áreas standrad (área 1), solo aprenden las rutas del área backbone, y no de la otra área standrad (area 2).

En la tabla que muestra los caminos de las etiquetas MPLS (LSP), se puede observar que la dirección de los PCs ya no es transmitida a través del protocolo LDP, sino a través de iBGP, lo que indica que se ha implementado BGP-LU, que tiene la capacidad de distribuir etiquetas. Además, al deshabilitar LDP en los routers, BGP-LU sigue siendo capaz de enviar estas etiquetas.

3.1.5. Simulación 3: Topología de red escenario Seamless MPLS inter-AS: OSPF, MPLS y BGP-LU

La figura 3.10, se muestra los resultados de las direcciones IP de las interfaces de loopback de la topologia de red, que aprende R1.

```
Routing Tables: Public
         Destinations : 18        Routes : 20

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/30  Direct  0    0           D   10.0.0.1        Ethernet0/0/1
        10.0.0.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
        10.0.0.4/30  Direct  0    0           D   10.0.0.5        GigabitEthernet
0/0/0
        10.0.0.5/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
       10.0.0.12/30  OSPF    10   3           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   3           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.16/30  OSPF    10   2           D   10.0.0.6        GigabitEthernet
0/0/0
       10.0.0.32/30  OSPF    10   2           D   10.0.0.2        Ethernet0/0/1
        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack1
        10.0.2.1/32  OSPF    10   1           D   10.0.0.2        Ethernet0/0/1
        10.0.3.1/32  OSPF    10   1           D   10.0.0.6        GigabitEthernet
0/0/0
        10.0.5.1/32  IBGP    255  0          RD   10.0.9.1        Ethernet0/0/1
        10.0.9.1/32  OSPF    10   2           D   10.0.0.2        Ethernet0/0/1
                     OSPF    10   2           D   10.0.0.6        GigabitEthernet
0/0/0
      10.125.0.0/24  Static  60   0           D   0.0.0.0         NULL0
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     192.168.1.0/24  Direct  0    0           D   192.168.1.1     Ethernet0/0/0
     192.168.1.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
     192.168.2.0/24  IBGP    255  0          RD   10.0.9.1        Ethernet0/0/1
```

Figura 3.10: Tabla de rutas interfaces de loopback R1.

La tabla de etiquetas MPLS que aprende R1, tanto en el protocolo LDP como el BGP, se muestran a continuación en la figura 3.11

```
                LSP Information: BGP  LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
10.0.1.1/32        1027/NULL     -/-
192.168.1.0/24     1029/NULL     -/-
10.0.5.1/32        NULL/1029     -/-
192.168.2.0/24     NULL/1032     -/-
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
10.0.2.1/32        NULL/3        -/Eth0/0/1
10.0.2.1/32        1024/3        -/Eth0/0/1
10.0.3.1/32        NULL/3        -/GE0/0/0
10.0.3.1/32        1025/3        -/GE0/0/0
10.0.1.1/32        3/NULL        -/-
10.0.9.1/32        NULL/1026     -/GE0/0/0
10.0.9.1/32        1026/1026     -/GE0/0/0
10.0.9.1/32        NULL/1026     -/Eth0/0/1
10.0.9.1/32        1026/1026     -/Eth0/0/1
```

Figura 3.11: Tabla de LSP R1.

De manera similar, se presentan las direcciones IP de loopbacks aprendidas por R5 en la figura 3.12

```
Routing Tables: Public
         Destinations : 16        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.24/30  Direct  0    0           D   10.0.0.26       Ethernet0/0/0
      10.0.0.26/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
      10.0.0.28/30  Direct  0    0           D   10.0.0.30       GigabitEthernet
0/0/0
      10.0.0.30/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
      10.0.0.36/30  OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
      10.0.0.40/30  OSPF    10   2           D   10.0.0.29       GigabitEthernet
0/0/0
       10.0.1.1/32  IBGP    255  0          RD   10.0.10.1       Ethernet0/0/0
       10.0.4.1/32  OSPF    10   1           D   10.0.0.25       Ethernet0/0/0
       10.0.5.1/32  Direct  0    0           D   127.0.0.1       LoopBack1
       10.0.6.1/32  OSPF    10   1           D   10.0.0.29       GigabitEthernet
0/0/0
      10.0.10.1/32  OSPF    10   2           D   10.0.0.25       Ethernet0/0/0
                    OSPF    10   2           D   10.0.0.29       GigabitEthernet
0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  IBGP    255  0          RD   10.0.10.1       Ethernet0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     Ethernet0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
```

Figura 3.12: Tabla de rutas interfaces de loopback R5.

En la figura 3.13 se muestran las etiquetas MPLS aprendidas por R5, donde se da detalle las direccionnes IP aprendidas, por protocolo LDP y BGP.

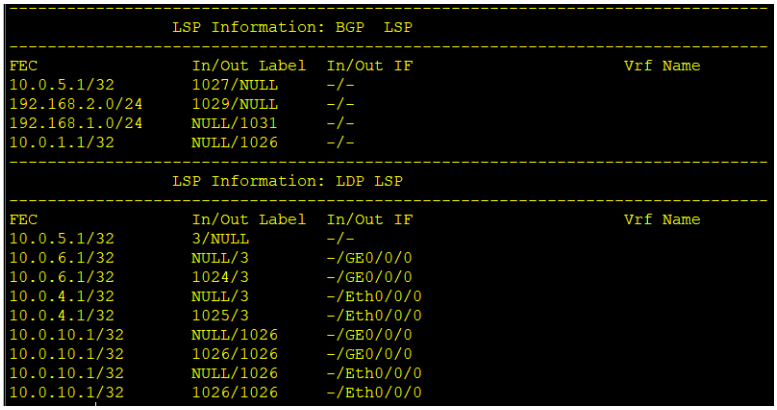

Figura 3.13: Tabla de LSP R5.

3.1.6. Análisis de Simulación 3: Topología de red escenario Seamless MPLS inter-AS: OSPF, MPLS y BGP-LU

Los resultados de la simulación de la topología son coherentes, ya que la implementación de BGP-LU ha resultado en una reducción de la tabla de rutas tanto en el Router 1 como en el Router 5. Las direcciones IP de las interfaces de conexión entre los routers no son aprendidas por routers de áreas diferentes. En cuanto a las interfaces de loopback, los dispositivos solo aprenden las rutas del mismo sistema autónomo.

Es importante destacar que, como se muestra en la figura 3.12, R1 aprende la dirección del PC2 a través de iBGP, lo cual es un resultado esperado y relevante. Este análisis puede continuar si se agregan más direcciones de anuncio de BGP. De manera similar, se puede observar que PC2 es aprendido en R1 a través de iBGP. Por otro lado, en el caso de OSPF, solo se aprenden las interfaces de loopback del mismo sistema autónomo, lo que significa que R1 solo conocerá las interfaces del AS-100 y R5 solo conocerá las del AS-200.

En la figuras 3.11 y 3.13, la cuales muestran los caminos de las etiquetas MPLS (LSP). Se evidencia que las direcciones de los PCs ya no son transmitidas a través del protocolo LDP, sino a través de BGP, lo que indica que se ha implementado BGP-LU, que tiene la capacidad de distribuir etiquetas. Además, al deshabilitar LDP en los routers, BGP-LU sigue siendo capaz de enviar estas etiquetas.

3.2. Resultados evaluación económica

3.2.1. CAPEX

Se procede a calcular el porcentaje de diferencia entre los precios de los dos diferentes modelos de Huawei, para esto se utiliza la ecuación 2.1, reemplazando los valores se obtiene un 11.11 % como se puede ver en la ecuación 3.1.

$$\%_C = \frac{0.1111X}{X} \cdot 100 = 11.11\,\% \tag{3.1}$$

Una vez obtenido se puede calcular el porcentaje de reducción del CAPEX entre ambos routers, utilizando la ecuación 2.2, obteniendo como resultado una tasa de reducción del

88.89 %, calculo realizado en la ecuación 3.2.

$$T_{RC} = 100 - 11.11 = 88.89\,\% \tag{3.2}$$

3.2.2. OPEX

Utilizando la formula general 2.3, para transformar previamente las BTU a Watts consumidos, se obtienen lo siguiente. Watts consumidos de climatización por NE40E es de 7,336.23 Watts. Mientras para 8000 F1A el resultado es de 308.84 Watts.

Utilizando la formula 2.4 se procede a calcular los Watts totales consumido por ambos routers. La ecuación 3.3 representa el total del equipo NE40E .

$$W/h_{total} = 7,720 + 7,336.23 = 15,056.23W \tag{3.3}$$

Mientras la ecuación 3.4 representa el consumo energético total del router NetEngine 8000 F1A.

$$W/h_{total} = 350 + 308.84 = 658.84W \tag{3.4}$$

Ahora se tiene que calcular el gasto operacional relacionado con el consumo energético de cada proyecto (G_{CE}). Con los datos obtenido en la ecuación 3.3 y 3.4, y con el dato extraído del costo de la barra promedio en Chile en CLP/W

$$G_{CE} = 106.49x15,056.23 = 1,603,313.44CLP/W/h \tag{3.5}$$

$$G_{CE} = 106.49x658.84 = 70,159.87CLP/W/h \tag{3.6}$$

En la ecuación 3.7 se procede a calcular la reducción en lo que respecta al OPEX del despliegue del router 8000 F1A, en vez de NE40E.

$$T_{RO} = \frac{1,573,225.46 - 68,842.19}{1,573,225.46} \cdot 100 = 95.62\,\% \tag{3.7}$$

3.2.3. Análisis Económico CAPEX y OPEX

Los resultados obtenidos en la comparación de los costos de adquisición (CAPEX) entre el router NE40E-X16A y el NE8000-F1A son coherentes con las expectativas. Se ha demostrado una reducción significativa del 88.89 % en el costo del equipo al elegir el segundo router, lo cual lo convierte en una opción de inversión muy atractiva. No obstante, para tomar una decisión informada, también es fundamental considerar el costo operativo (OPEX).

En cuanto al OPEX, se observa que el NE40E-X16A, al ser un router de mayor tamaño, presenta un alto consumo de energía y requiere de una climatización costosa, lo que se traduce en un mayor gasto operacional. Por el contrario, el NE8000-F1A tiene un consumo de energía más bajo y un gasto operacional reducido, alcanzando una reducción del 95 % en el costo de la energía consumida. Esto demuestra que la aplicación del equipo de menor tamaño es más rentable desde el punto de vista económico.

Además, al optar por el equipo de menor tamaño, existe un costo asociado a su incorporación

dentro del espacio construido o arrendado, lo cual sería problemático en el caso de utilizar un equipo sobredimensionado.

En resumen, la elección del equipo de menor tamaño no solo implica ahorros significativos en términos de consumo de energía y gasto operacional, sino que también evita costos adicionales relacionados con la infraestructura necesaria para su instalación.

Capítulo 4

Conclusiones

El objetivo principal de este estudio es realizar una evaluación técnica y económica de la optimización de la red de un proveedor de servicios de acceso a Internet mediante la implementación del protocolo BGP-LU. El protocolo BGP-LU permite la transmisión unicast de etiquetas MPLS dentro de una red que utiliza ambas tecnologías. Al combinar este protocolo con un router reflector, se logra una integración sin cuellos de botellas en la red, la reduciendo la cantidad de protocolos utilizados en la red.

En la evaluación técnica, se realizó una simulación del caso de estudio utilizando el software eNSP, obteniendo resultados coherentes en tres escenarios diferentes. En primer lugar, se observa una reducción significativa en las rutas aprendidas en la tabla de enrutamiento de los routers cuando se implementa el protocolo BGP-LU en comparación con el caso base, que utiliza únicamente el protocolo OSPF. En segundo lugar, la aplicación de este protocolo permite prescindir del uso del protocolo LDP en la distribución de etiquetas MPLS, lo que reduce los recursos computacionales y de almacenamiento requeridos.

Es importante tener en cuenta algunas precauciones al implementar el protocolo BGP-LU. Debido a la utilización de router reflectors, la configuración BGP difiere, ya que los routers solo se conectan a ellos mediante iBGP, lo cual implica que el router da preferencia a las tablas de rutas aprendidas por OSPF, ya que se tiene prioridad sobre BGP. Por esto se deben aplicar filtros y/o políticas BGP previas para la implementación de BGP-LU en redes de gran tamaño.

Desde el punto de vista económico, BGP-LU muestra una reducción en los gastos de capital (CAPEX) y en los gastos operativos (OPEX). Se compararon dos proyectos: uno que utiliza equipos con mayor capacidad de procesamiento y almacenamiento de rutas, y otro en el que se implementa el protocolo BGP-LU en equipos de menor tamaño para reducir las tablas de rutas y los requisitos computacionales mencionados anteriormente. Los resultados mostraron una reducción del 90 % en el CAPEX, considerando chasis de router y tarjetas de enrutamiento para el equipo de mayor tamaño, y solo chasis con tarjetas integradas para el equipo de menor tamaño. Además, se obtuvo una reducción del 95 % en los gastos operativos (OPEX).

La optimización de CAPEX y OPEX no solo hace que la implementación de proyectos rurales sea atractiva para los operadores en Chile, sino que también les permite concentrar sus

inversiones en áreas más desafiantes. En contraste, hay proyectos en los que la optimización no aporta beneficios significativos, lo que hace imperativo reducir los costos y gastos en esas áreas.

Para trabajos futuros se recomienda el aplicar el protocolo BGP-LU en un ambiente controlado como un laboratorio de pruebas e ir verificando su funcionamiento, ya que técnicamente se satisface la funcionalidad y, con el fin de evitar problemas en la red viva. Una vez completetada satisfactoriamente estas pruebas, implementar el protocolo BGP-LU en lugares sectorizados de la red para no crear fallas masivas en la red.

Dado el beneficio técnico y económico que ofrece BGP-LU, al reducir las tablas de rutas y los protocolos utilizados, los proveedores de servicios de Internet (ISPs) tienen un incentivo para invertir en áreas rurales de menor tamaño, donde un dispositivo puede operar de manera eficiente en la red y lograr una mayor cobertura a nivel país.

Glosario

AFI Address Family

BGP Border Gateway Protocol

BTU British Thermal Unit

CAPEX Capital Expenditure

CIDR Classless Inter-Domain Routing

EGP Exterior Gateway Protocol

IANA Internet Assigned Numbers Authority

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IGRP Interior Gateway Routing Protocol

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

IS-IS Intermediate System to intermediate System

ISP Internet Service Provider

L2VPN Layer 2 Virtual Private Network

L3VPN Layer 3 Virtual Private Network

LDP Label Distribution Protocol

LSA Link State Advertise

LSP Label Switch Path

MPLS Multi Protocol Label Switching

MP-BGP Multi Protocol Border Gateway Protocol

OSPF Open Short Path First

OPEX Operational Expenditures

RIP Routing Information Protocol

RFC Request For Comments

RR Route Reflector

RSVP Resource Reservation Protocol

SAFI Subsequence Address Family

VPNv4 Virtual Private Network Version 4

Bibliografía

[1] Cuentas Nacionales de Chile, "Evaluación de la actividad económica primer trimestre," 2023.

[2] Subsecretaría de telecomunicaciones, "Sector telecomunicaciones primer trimestre 2023," 2023.

[3] Rosen, Y. R., "Rfc 3107: Carrying label information in bgp-4," 2006.

[4] Juniper NETWORKS, "Descripción general de protocolos de enrutamiento.", https://www.juniper.net/documentation/mx/es/software/junos/routing-overview/topics/concept/routing-protocols-routing-databases-overview.html (visitado el 2023-01-10).

[5] Verma, A. y Bhardwaj, N., "A review on routing information protocol (rip) and open shortest path first (ospf) routing protocol," International Journal of Future Generation Communication and Networking, vol. 9, no. 4, pp. 161–170, 2016.

[6] Gredler, H. y Goralski, W., The complete IS-IS routing protocol. Springer Science & Business Media, 2005.

[7] Medhi, D. y Ramasamy, K., Network routing: algorithms, protocols, and architectures. Morgan kaufmann, 2017.

[8] Huawei Technologies Co., Ltd, "What is ospf and how is it configured?.", https://support.huawei.com/enterprise/en/doc/EDOC1100082074 (visitado el 2022-09-13).

[9] Moy, J., "Rfc2328: Ospf version 2," 1998.

[10] Juniper NETWORKS, "Guía del usuario de ospf.", https://www.juniper.net/documentation/mx/es/software/junos/ospf/topics/topic-map/configuring-ospf-interfaces.html (visitado el 2023-02-20).

[11] Juniper NETWORKS, "Guía del usuario de aplicaciones mpls.", https://www.juniper.net/documentation/mx/es/software/junos/mpls/topics/topic-map/rsvp-overview.html (visitado el 2023-07-08).

[12] Huawei Technologies Co., Ltd, "What is mpls?.", https://support.huawei.com (visitado el 2023-04-14).

[13] Canalis, M. S., "Mpls "multiprotocol label switching": Una arquitectura de backbone para la internet del siglo xxi," Opto Informática Universidad Nacional del Nordeste. Argentina, 2003.

[14] Rosen, E., Viswanathan, A., y Callon, R., "Rfc3031: Multiprotocol label switching architecture," 2001.

[15] Huawei Technologies Co., Ltd, "Bgp configuration.", https://support.huawei.com/enterprise/en/doc/EDOC1100034072/b5abc35a/bgp-configuration (visitado el 2022-12-20).

[16] Juniper NETWORKS, "Guía del usuario del bgp, url = https://www.juniper.net/documentation/mx/es/software/junos/bgp/topics/topic-map/multiprotocol-bgp.html, urldate = 2023-06-02.".

[17] Bates, T., Chen, E., y Chandra, R., "Bgp route reflection: An alternative to full mesh internal bgp (ibgp)," rep. tec., 2006.

[18] Bates, T., Chandra, R., Katz, D., y Rekhter, Y., "Rfc 4760: Multiprotocol extensions for bgp-4," 2007.

[19] Subsecretaría de telecomunicaciones, "Resolucion 698 exenta fija indicadores de calidad de los enlaces de conexion para cursar el trafico nacional de internet y sistema de publicidad de los mismos," 2011-12-29.

[20] Juniper NETWORKS, "Guía del usuario de is-is.", https://www.juniper.net/documentation/mx/es/software/junos/is-is/topics/concept/ldp-igp-synchronization.html (visitado el 2023-04-16).

[21] CISCO System, "Border gateway protocol (bgp).", https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/119001-configure-aigp-00.html (visitado el 2023-05-27).

[22] Juniper NETWORKS, "Guía del usuario de vpn de capa 3 para dispositivos de enrutamiento.", https://www.juniper.net/documentation/mx/es/software/junos/vpn-l3/topics/example/mpls-qfx-series-vpn-layer3.html (visitado el 2023-03-15).

[23] Juniper NETWORKS, "Building multi-generation scalable networks with end-to-end mpls juniper enables service flexibility and scalability with seamless mpls.", https://www.juniper.net/content/dam/www/assets/white-papers/us/en/building-multi-generation-scalable-networks-with-end-to-end.pdf (visitado el 2012).

[24] Huawei Technologies Co., Ltd, "Seamless mpls configuration.", https://support.huawei.com/enterprise/es/doc/EDOC1000089040/28ecd062/principles (visitado el 2023-03-07).

[25] Huawei Technologies Co., Ltd, "Netengine 8000 f1a technical specifications.", https://info.support.huawei.com/info-finder/enterprisesearch/ (visitado el 2023-04-14).

[26] Huawei Technologies Co., Ltd, "Ne40e-x16a technical specifications.", https://info.support.huawei.com/info-finder/enterprisesearch (visitado el 2023-05-29).

[27] Ministerio de Energía, Comisión Nacional de Energía Gobierno de Chile, "Precio medio de mercado sistema eléctrico nacional," rep. tec., 2023-07.

Anexos

Anexo A. Configuración routers Simulación 1

A.1. Router 1

```
    #
sysname router1
#
mpls lsr-id 10.0.1.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher ~=3;Hj'/0F]@l3D+mKgU@[+#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 10.0.0.1 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
```

```
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.5 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.80.2 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.1.1 255.255.255.255
#
bgp 100
 router-id 10.0.1.1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.3.1 as-number 100
 peer 10.0.3.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  import-route static
  peer 10.0.2.1 enable
  peer 10.0.3.1 enable
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.0.0.4 0.0.0.3
```

```
  network 10.0.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.2. Router 2

```
    #
sysname router2
#
mpls lsr-id 10.0.2.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher seE%HB*Zz==H)H2[EInBG[2#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
```

```
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.33 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.2.1 255.255.255.255
#
bgp 100
 router-id 10.0.2.1
 peer 10.0.0.1 as-number 100
 peer 10.0.1.1 as-number 100
 peer 10.0.1.1 connect-interface LoopBack1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 10.0.0.32 255.255.255.252
  peer 10.0.0.1 enable
  peer 10.0.1.1 enable
  peer 10.0.2.1 enable
  peer 10.0.9.1 enable
#
ospf 1 router-id 10.0.2.1
 area 0.0.0.0
  network 10.0.0.8 0.0.0.3
```

```
  network 10.0.0.0 0.0.0.3
  network 10.0.2.1 0.0.0.0
  network 10.0.0.32 0.0.0.3
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.3. Router 3

```
   #
sysname router3
#
mpls lsr-id 10.0.3.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher MF\AMJHap@;BH^68NhwO([*#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
 ip address 10.0.0.17 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
```

```
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.6 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.3.1 255.255.255.255
#
bgp 100
 router-id 10.0.3.1
 peer 10.0.1.1 as-number 100
 peer 10.0.1.1 connect-interface LoopBack1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.1.1 enable
  peer 10.0.2.1 enable
  peer 10.0.9.1 enable
#
ospf 1 router-id 10.0.3.1
 area 0.0.0.0
  network 10.0.0.4 0.0.0.3
  network 10.0.0.8 0.0.0.3
  network 10.0.3.1 0.0.0.0
  network 10.0.0.16 0.0.0.3
```

```
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.4. Router 4

```
   #
sysname router4
#
mpls lsr-id 10.0.4.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher L@mz+H[^kVbL^B&WSBiQI[[#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.37 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.25 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1.1
#
interface Ethernet0/0/1.2
#
```

```
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.4.1 255.255.255.255
#
bgp 100
 router-id 10.0.4.1
 peer 10.0.5.1 as-number 100
 peer 10.0.5.1 connect-interface LoopBack1
 peer 10.0.6.1 as-number 100
 peer 10.0.6.1 connect-interface LoopBack1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.5.1 enable
  peer 10.0.6.1 enable
  peer 10.0.10.1 enable
#
ospf 1 router-id 10.0.4.1
 area 0.0.0.0
  network 10.0.0.20 0.0.0.3
  network 10.0.0.24 0.0.0.3
  network 10.0.4.1 0.0.0.0
```

```
  network 10.0.0.36 0.0.0.3
#
snmp-agent
snmp-agent local-engineid 800007DB035489986E4379
snmp-agent sys-info version v3
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.5. Router 5

```
   #
sysname router5
#
mpls lsr-id 10.0.5.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher \26W,Ls|NSbL^B&WSBiQY[0#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.26 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface Serial0/0/0
 link-protocol ppp
#
```

```
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.30 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.5.1 255.255.255.255
#
bgp 100
 router-id 10.0.5.1
 peer 10.0.4.1 as-number 100
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.6.1 as-number 100
 peer 10.0.6.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.4.1 enable
  peer 10.0.6.1 enable
#
ospf 1 router-id 10.0.5.1
 area 0.0.0.0
  network 10.0.0.24 0.0.0.3
  network 10.0.0.28 0.0.0.3
  network 10.0.5.1 0.0.0.0
  network 192.168.2.0 0.0.0.255
```

```
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.6. Router 6

```
   #
sysname router6
#
mpls lsr-id 10.0.6.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher M-T$US_Fu-ani^>"qh^;"[\#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.29 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
```

```
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.42 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.6.1 255.255.255.255
#
bgp 100
 router-id 10.0.6.1
 peer 10.0.4.1 as-number 100
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.5.1 as-number 100
 peer 10.0.5.1 connect-interface LoopBack1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.4.1 enable
  peer 10.0.5.1 enable
  peer 10.0.10.1 enable
#
ospf 1 router-id 10.0.6.1
 area 0.0.0.0
  network 10.0.0.20 0.0.0.3
  network 10.0.0.28 0.0.0.3
  network 10.0.6.1 0.0.0.0
  network 10.0.0.40 0.0.0.3
#
user-interface con 0
user-interface vty 0 4
```

```
user-interface vty 16 20
#
return
```

A.7. Router 9

```
   #
sysname P1
#
mpls lsr-id 10.0.9.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher '^Ho"}OGID:z9:%F'[a=f[i#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.18 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.34 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
```

```
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.13 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.9.1 255.255.255.255
#
bgp 100
 router-id 10.0.9.1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.3.1 as-number 100
 peer 10.0.3.1 connect-interface LoopBack1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.2.1 enable
  peer 10.0.3.1 enable
  peer 10.0.10.1 enable
#
ospf 1 router-id 10.0.9.1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 10.0.9.1 0.0.0.0
  network 10.0.0.16 0.0.0.3
  network 10.0.0.32 0.0.0.3
#
```

```
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

A.8. Router 10

```
  #
sysname P2
#
mpls lsr-id 10.0.10.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher :DQ*;H'^uHECB7Ie7'/)P[W#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.14 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.38 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
```

```
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.41 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.10.1 255.255.255.255
#
bgp 100
 router-id 10.0.10.1
 peer 10.0.4.1 as-number 100
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.6.1 as-number 100
 peer 10.0.6.1 connect-interface LoopBack1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.4.1 enable
  peer 10.0.6.1 enable
  peer 10.0.9.1 enable
#
ospf 1 router-id 10.0.10.1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 10.0.10.1 0.0.0.0
  network 10.0.0.40 0.0.0.3
```

```
  network 10.0.0.36 0.0.0.3
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

Anexo B. Configuración routers Simulación 2

B.1. Router 1

```
   #
sysname router1
#
mpls lsr-id 10.0.1.1
mpls
#
mpls ldp
#
#
acl number 2001
 rule 5 permit source 10.0.2.1 0
 rule 10 permit source 10.0.3.1 0
 rule 15 permit source 10.0.9.1 0
 rule 20 permit source 10.0.10.1 0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher vM)O,XrBAA+/Y@:Y>Lw(tM^#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 10.0.0.1 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.1
 mpls
```

```
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.5 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.1
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.80.2 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.1.1 255.255.255.255
#
bgp 100
 router-id 10.0.1.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 10.0.1.1 255.255.255.255 route-policy 1
  network 192.168.1.0 route-policy 1
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
```

```
#
ospf 1 router-id 10.0.1.1
 filter-policy 2001 import
 area 0.0.0.1
  network 10.0.1.1 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.0.0.4 0.0.0.3
#
route-policy 1 permit node 1
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.2. Router 2

```
#
sysname router2
#
mpls lsr-id 10.0.2.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher vM)O,XrBAAani^>"qh^;tM_#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.1
 mpls
 mpls ldp
#
```

```
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.33 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.2.1 255.255.255.255
#
bgp 100
 router-id 10.0.2.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.2.1
 area 0.0.0.0
```

```
  network 10.0.0.32 0.0.0.3
 area 0.0.0.1
  network 10.0.2.1 0.0.0.0
  network 10.0.0.0 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.3. Router 3

```
   #
sysname router3
#
mpls lsr-id 10.0.3.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher zW#6~cNJPUjKUGU-KkpB)Mo#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
 ip address 10.0.0.17 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
```

```
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.6 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.1
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.3.1 255.255.255.255
#
bgp 100
 router-id 10.0.3.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.3.1
 area 0.0.0.0
  network 10.0.0.16 0.0.0.3
 area 0.0.0.1
  network 10.0.0.4 0.0.0.3
```

```
  network 10.0.3.1 0.0.0.0
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.4. Router 4

```
   #
sysname router4
#
mpls lsr-id 10.0.4.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher +(V‘Q@‘WtCaniˆ>"qhˆ;vM,#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.37 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.25 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.2
 mpls
 mpls ldp
```

```
#
interface Ethernet0/0/1.1
#
interface Ethernet0/0/1.2
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.4.1 255.255.255.255
#
bgp 100
 router-id 10.0.4.1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.4.1
 area 0.0.0.0
  network 10.0.0.36 0.0.0.3
 area 0.0.0.2
```

```
  network 10.0.4.1 0.0.0.0
  network 10.0.0.24 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
snmp-agent
snmp-agent local-engineid 800007DB035489986E4379
snmp-agent sys-info version v3
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.5. Router 5

```
 #
    sysname router5
#
mpls lsr-id 10.0.5.1
mpls
#
mpls ldp
#
#
acl number 2002
 rule 5 permit source 10.0.4.1 0
 rule 10 permit source 10.0.6.1 0
 rule 15 permit source 10.0.10.1 0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher |o"(WuI;vVECB7Ie7'/)]Md#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.26 255.255.255.252
 ospf network-type p2p
```

```
 ospf enable 1 area 0.0.0.2
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.30 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.2
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.5.1 255.255.255.255
#
bgp 100
 router-id 10.0.5.1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 10.0.5.1 255.255.255.255 route-policy 1
```

```
  network 192.168.2.0 route-policy 1
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.5.1
 filter-policy 2002 import
 area 0.0.0.2
  network 10.0.5.1 0.0.0.0
  network 10.0.0.28 0.0.0.3
  network 10.0.0.24 0.0.0.3
#
route-policy 1 permit node 1
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.6. Router 6

```
    #
sysname router6
#
mpls lsr-id 10.0.6.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher jb5N4}}$IR]@l3D+mKgUTM+#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.29 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.2
```

```
 mpls
 mpls ldp
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.42 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.6.1 255.255.255.255
#
bgp 100
 router-id 10.0.6.1
 peer 10.0.4.1 as-number 100
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.5.1 as-number 100
 peer 10.0.5.1 connect-interface LoopBack1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
```

```
  undo synchronization
  peer 10.0.4.1 enable
  peer 10.0.4.1 route-policy 1 export
  peer 10.0.4.1 label-route-capability
  peer 10.0.5.1 enable
  peer 10.0.5.1 route-policy 1 export
  peer 10.0.5.1 label-route-capability
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.6.1
 area 0.0.0.0
  network 10.0.0.40 0.0.0.3
 area 0.0.0.2
  network 10.0.6.1 0.0.0.0
  network 10.0.0.28 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.7. Router 9

```
   #
sysname P1
#
mpls lsr-id 10.0.9.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher vM)O,XrBAA=H)H2[EInBˆM‘#
 local-user admin service-type http
#
```

```
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.18 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.34 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.13 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
```

```
 ip address 10.0.9.1 255.255.255.255
#
bgp 100
 router-id 10.0.9.1
 peer 10.0.1.1 as-number 100
 peer 10.0.1.1 connect-interface LoopBack1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.3.1 as-number 100
 peer 10.0.3.1 connect-interface LoopBack1
 peer 10.0.10.1 as-number 100
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.1.1 enable
  peer 10.0.1.1 route-policy 1 export
  peer 10.0.1.1 reflect-client
  peer 10.0.1.1 next-hop-local
  peer 10.0.1.1 label-route-capability
  peer 10.0.2.1 enable
  peer 10.0.2.1 route-policy 1 export
  peer 10.0.2.1 reflect-client
  peer 10.0.2.1 next-hop-local
  peer 10.0.2.1 label-route-capability
  peer 10.0.3.1 enable
  peer 10.0.3.1 route-policy 1 export
  peer 10.0.3.1 reflect-client
  peer 10.0.3.1 next-hop-local
  peer 10.0.3.1 label-route-capability
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 reflect-client
  peer 10.0.10.1 next-hop-local
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.9.1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 10.0.9.1 0.0.0.0
  network 10.0.0.16 0.0.0.3
  network 10.0.0.32 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
```

```
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

B.8. Router 10

```
   #
sysname P2
#
mpls lsr-id 10.0.10.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher zW#6~cNJPU939O4.‘(ZGiMg#
 local-user admin service-type http
#
isis 1
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.14 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.38 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
```

```
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.41 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.10.1 255.255.255.255
#
bgp 100
 router-id 10.0.10.1
 peer 10.0.4.1 as-number 100
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.5.1 as-number 100
 peer 10.0.5.1 connect-interface LoopBack1
 peer 10.0.6.1 as-number 100
 peer 10.0.6.1 connect-interface LoopBack1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.4.1 enable
  peer 10.0.4.1 route-policy 1 export
  peer 10.0.4.1 reflect-client
  peer 10.0.4.1 next-hop-local
  peer 10.0.4.1 label-route-capability
```

```
  peer 10.0.5.1 enable
  peer 10.0.5.1 route-policy 1 export
  peer 10.0.5.1 reflect-client
  peer 10.0.5.1 next-hop-local
  peer 10.0.5.1 label-route-capability
  peer 10.0.6.1 enable
  peer 10.0.6.1 route-policy 1 export
  peer 10.0.6.1 reflect-client
  peer 10.0.6.1 next-hop-local
  peer 10.0.6.1 label-route-capability
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 reflect-client
  peer 10.0.9.1 next-hop-local
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.10.1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 10.0.10.1 0.0.0.0
  network 10.0.0.36 0.0.0.3
  network 10.0.0.40 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

Anexo C. Configuración routers Simulación 3

C.1. Router 1

```
    #
sysname router1
#
mpls lsr-id 10.0.1.1
mpls
#
mpls ldp
#
#
aaa
```

```
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher vM)O,XrBAA3@9_G-B0Y2tEN#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
 ip address 10.0.0.1 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.5 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.80.2 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
```

```
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.1.1 255.255.255.255
#
bgp 100
 router-id 10.0.1.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 10.0.1.1 255.255.255.255
  network 192.168.1.0
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.0.0.4 0.0.0.3
  network 10.0.1.1 0.0.0.0
#
route-policy 1 permit node 1
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.2. Router 2

```
   #
sysname router2
#
mpls lsr-id 10.0.2.1
mpls
#
mpls ldp
#
#
aaa
```

```
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher |\37=#khc.ECB7Ie7'/)}D3#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.33 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
```

```
interface NULL0
#
interface LoopBack1
 ip address 10.0.2.1 255.255.255.255
#
bgp 100
 router-id 10.0.2.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.2.1
 area 0.0.0.0
  network 10.0.0.8 0.0.0.3
  network 10.0.0.0 0.0.0.3
  network 10.0.2.1 0.0.0.0
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.3. Router 3

```
   #
sysname router3
#
mpls lsr-id 10.0.3.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
```

```
 domain default_admin
 local-user admin password cipher DVMt+{JfDN]@l3D+mKgU+D+#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
 ip address 10.0.0.17 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.6 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.3.1 255.255.255.255
```

```
#
bgp 100
 router-id 10.0.3.1
 peer 10.0.9.1 as-number 100
 peer 10.0.9.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.9.1 enable
  peer 10.0.9.1 route-policy 1 export
  peer 10.0.9.1 label-route-capability
#
ospf 1 router-id 10.0.3.1
 area 0.0.0.0
  network 10.0.0.4 0.0.0.3
  network 10.0.0.8 0.0.0.3
  network 10.0.3.1 0.0.0.0
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.4. Router 4

```
    #
sysname router4
#
mpls lsr-id 10.0.4.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher =bKXOZWpp8;BH^68NhwO,DA#
 local-user admin service-type http
#
```

```
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.37 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.25 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1.1
#
interface Ethernet0/0/1.2
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.4.1 255.255.255.255
```

```
#
bgp 200
 router-id 10.0.4.1
 peer 10.0.10.1 as-number 200
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.4.1
 area 0.0.0.0
  network 10.0.0.20 0.0.0.3
  network 10.0.0.24 0.0.0.3
  network 10.0.4.1 0.0.0.0
  network 10.0.0.36 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
snmp-agent
snmp-agent local-engineid 800007DB035489986E4379
snmp-agent sys-info version v3
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.5. Router 5

```
   #
sysname router5
#
mpls lsr-id 10.0.5.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
```

```
 domain default
 domain default_admin
 local-user admin password cipher c^z()#9ivC:z9:%F‘[a=CDY#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.26 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.30 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
```

```
interface LoopBack1
 ip address 10.0.5.1 255.255.255.255
#
bgp 200
 router-id 10.0.5.1
 peer 10.0.10.1 as-number 200
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 10.0.5.1 255.255.255.255 route-policy 1
  network 192.168.2.0 route-policy 1
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.5.1
 area 0.0.0.0
  network 10.0.0.24 0.0.0.3
  network 10.0.0.28 0.0.0.3
  network 10.0.5.1 0.0.0.0
#
route-policy 1 permit node 1
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.6. Router 6

```
   #
sysname router6
#
mpls lsr-id 10.0.6.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
```

```
 local-user admin password cipher zLBCG.N/>2ani^>"qh^;oD=#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.29 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/0.1
#
interface Ethernet0/0/0.2
#
interface Ethernet0/0/1
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.42 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
```

```
#
interface LoopBack1
 ip address 10.0.6.1 255.255.255.255
#
bgp 200
 router-id 10.0.6.1
 peer 10.0.10.1 as-number 200
 peer 10.0.10.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.10.1 enable
  peer 10.0.10.1 route-policy 1 export
  peer 10.0.10.1 label-route-capability
#
ospf 1 router-id 10.0.6.1
 area 0.0.0.0
  network 10.0.0.20 0.0.0.3
  network 10.0.0.28 0.0.0.3
  network 10.0.6.1 0.0.0.0
  network 10.0.0.40 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

C.7. Router 9

```
   #
sysname P1
#
mpls lsr-id 10.0.9.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
```

```
 domain default_admin
 local-user admin password cipher \>Z5F/Vh'33IF$':[285{DX#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.18 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Ethernet0/0/1
 ip address 10.0.0.34 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.13 255.255.255.252
 mpls
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
```

```
interface LoopBack1
 ip address 10.0.9.1 255.255.255.255
#
bgp 100
 router-id 10.0.9.1
 peer 10.0.0.14 as-number 200
 peer 10.0.1.1 as-number 100
 peer 10.0.1.1 connect-interface LoopBack1
 peer 10.0.2.1 as-number 100
 peer 10.0.2.1 connect-interface LoopBack1
 peer 10.0.3.1 as-number 100
 peer 10.0.3.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.0.14 enable
  peer 10.0.0.14 route-policy 1 export
  peer 10.0.0.14 label-route-capability check-tunnel-reachable
  peer 10.0.1.1 enable
  peer 10.0.1.1 route-policy 1 export
  peer 10.0.1.1 reflect-client
  peer 10.0.1.1 next-hop-local
  peer 10.0.1.1 label-route-capability
  peer 10.0.2.1 enable
  peer 10.0.2.1 route-policy 1 export
  peer 10.0.2.1 reflect-client
  peer 10.0.2.1 next-hop-local
  peer 10.0.2.1 label-route-capability
  peer 10.0.3.1 enable
  peer 10.0.3.1 route-policy 1 export
  peer 10.0.3.1 reflect-client
  peer 10.0.3.1 next-hop-local
  peer 10.0.3.1 label-route-capability
#
ospf 1 router-id 10.0.9.1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 10.0.9.1 0.0.0.0
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
```

return

C.8. Router 10

```
   #
sysname P2
#
mpls lsr-id 10.0.10.1
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher -$[1(P>3t>+/Y@:Y>Lw(=E##
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 10.0.0.14 255.255.255.252
 mpls
#
interface Ethernet0/0/1
 ip address 10.0.0.38 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface Serial0/0/0
 link-protocol ppp
#
interface Serial0/0/1
 link-protocol ppp
#
interface Serial0/0/2
 link-protocol ppp
#
interface Serial0/0/3
 link-protocol ppp
#
```

```
interface GigabitEthernet0/0/0
 ip address 10.0.0.41 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
interface LoopBack1
 ip address 10.0.10.1 255.255.255.255
#
bgp 200
 router-id 10.0.10.1
 peer 10.0.0.13 as-number 100
 peer 10.0.4.1 as-number 200
 peer 10.0.4.1 connect-interface LoopBack1
 peer 10.0.5.1 as-number 200
 peer 10.0.5.1 connect-interface LoopBack1
 peer 10.0.6.1 as-number 200
 peer 10.0.6.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.0.13 enable
  peer 10.0.0.13 route-policy 1 export
  peer 10.0.0.13 label-route-capability check-tunnel-reachable
  peer 10.0.4.1 enable
  peer 10.0.4.1 route-policy 1 export
  peer 10.0.4.1 reflect-client
  peer 10.0.4.1 next-hop-local
  peer 10.0.4.1 label-route-capability
  peer 10.0.5.1 enable
  peer 10.0.5.1 route-policy 1 export
  peer 10.0.5.1 reflect-client
  peer 10.0.5.1 next-hop-local
  peer 10.0.5.1 label-route-capability
  peer 10.0.6.1 enable
  peer 10.0.6.1 route-policy 1 export
```

```
  peer 10.0.6.1 reflect-client
  peer 10.0.6.1 next-hop-local
  peer 10.0.6.1 label-route-capability
#
ospf 1 router-id 10.0.10.1
 area 0.0.0.0
  network 10.0.10.1 0.0.0.0
  network 10.0.0.36 0.0.0.3
  network 10.0.0.40 0.0.0.3
#
route-policy 1 permit node 1
 if-match mpls-label
 apply mpls-label
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```