DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

TEMA: "ARQUITECTURA DE RED BASADA EN SEAMLESS MPLS PARA EL BACKHAUL DE TRANSMISIÓN IP-RAN DE UNA OPERADORA MÓVIL PARA INTERCONECTAR LA RED MÓVIL 4G LTE EN LA CIUDAD DE CUENCA"

AUTOR: MORÁN ORTIZ, ALEX ANTONIO

DIRECTOR: ING. AGUILAR SALAZAR, DARWIN LEONIDAS Mgs

SANGOLQUÍ

2020

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"ARQUITECTURA DE RED BASADA EN SEAMLESS MPLS PARA EL BACKHAUL DE TRANSMISIÓN IP-RAN DE UNA OPERADORA MÓVIL PARA INTERCONECTAR LA RED MÓVIL 4G LTE EN LA CIUDAD DE CUENCA"*** fue realizado por el señor ***Morán Ortiz, Alex Antonio*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 21 de Enero de 2020

.....

Ing. Darwin Leonidas Aguilar S. Mgs
DIRECTOR
C.C.: 1103036826

DEPARTAMENTO DE ELÊCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, ***Morán Ortiz, Alex Antonio***, declaro que el contenido, ideas y criterios del trabajo de titulación: ***"ARQUITECTURA DE RED BASADA EN SEAMLESS MPLS PARA EL BACKHAUL DE TRANSMISIÓN IP-RAN DE UNA OPERADORA MÓVIL PARA INTERCONECTAR LA RED MÓVIL 4G LTE EN LA CIUDAD DE CUENCA"*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 21 de Enero de 2020

.....

Alex Antonio Morán Ortiz

C.C.: 1720877735

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

*Yo, **Morán Ortiz, Alex Antonio** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"ARQUITECTURA DE RED BASADA EN SEAMLESS MPLS PARA EL BACKHAUL DE TRANSMISIÓN IP-RAN DE UNA OPERADORA MÓVIL PARA INTERCONECTAR LA RED MÓVIL 4G LTE EN LA CIUDAD DE CUENCA"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.*

Sangolquí, 21 de Enero de 2020

.....

Alex Antonio Morán Ortiz

C.C.: 1720877735

DEDICATORIA

Dedico esta tesis a:

Primero a Dios, ya que la fe y su amparo me ha dado la fortaleza para culminar esta ardua lucha.

A mi madre que siempre se ha mantenido a mi lado, con sus consejos y regaños, siendo el apoyo incondicional, brindándome el cariño y los recursos para convertirme en un profesional.

A Fernando que sin ser mi padre me apoyo cada día para alcanzar mi meta.

A mi abuelita por ser la persona que con su cariño apacigua mis días.

A mi hermano y primo Darwin por su paciencia y comprensión.

No podría olvidarme de mis maestros y compañeros con los cuales he compartido estos años de estudiante, algunos de los cuales tengo el placer de compartir aún en el ambiente laboral.

Gracias a todos porque de una u otra forma fueron los que me impulsaron para seguir adelante.

Sin su ayuda no hubiese podido llegar a este momento.

Gracias a todos.

Alex Antonio.

AGRADECIMIENTO

A la vida que me dio la oportunidad de alcanzar esta meta tan importante.

Agradezco también a mi madre, que me brindo su apoyo incondicional en todos los ámbitos a poder recorrer el camino que marque para llegar a culminar mis estudios.

A mi abuelita que nunca me dejo solo y me ayudo desde el inicio de mi educación hasta el día de hoy.

A Fernando y a mi primo Darwin les agradezco por todo el respaldo y la ayuda hacia mí, por ese cariño y la confianza que nos une como familia a pesar de cualquier diferencia.

A Cinthy, le agradezco por ser esa persona que me dio ánimos para continuar y hacerme entender el valor de una persona se demuestra con hechos más que con palabras.

A mi tutor y director de carrera, Ing. Darwin Aguilar, por confiar ciegamente en mí y en la idea del proyecto a realizar, gracias el apoyo incondicional en todas las circunstancias que se han presentado hasta llegar a este punto.

Agradezco a mis compañeros de trabajo que mediante su sabiduría y conocimiento fueron un faro que ha iluminado mi camino a lo largo del desarrollo del proyecto.

Alex Antonio Morán Ortiz

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

A nivel global existe un creciente requerimiento de servicios de banda ancha móvil, originados por la alta penetración de redes celulares, y la creciente demanda de acceso a datos, contenido multimedia y servicios. Las redes tradicionales 2G y 3G se han visto sobrepasadas en su capacidad, sin lograr atender esta demanda, sufriendo de congestión, con impacto en la calidad de servicio al usuario. La tecnología LTE, Long Term Evolution, surge como respuesta a estas necesidades, presentando una arquitectura de comunicación diseñada para brindar un acceso de banda ancha a través de una red móvil (Jaramillo, 2015).

El despliegue actual de la tecnología LTE desde el año 2015 en el Ecuador muestra un crecimiento exponencial del uso de redes de nueva generación esto puede representar un problema haciendo que las redes de transporte o backhaul queden obsoletas. Debido al incremento masivo de servicios y suscriptores en la red el MPLS tradicional esto complicará en exceso la escalabilidad y administración de la red. Al tener MPLS solo en el borde el despliegue jerárquico requiere una mayor cooperación entre las diferentes capas, dificultando la expansión de la red y el servicio debido a que los servicios no son End to End.

A partir de un dimensionamiento del posible número de usuarios LTE y el throughput que estos puedan generar para el año 2023, se propone diseñar una arquitectura de red basada en Seamless MPLS la cual permitirá extender la región de MPLS a la capa de acceso y no solo en el borde como tradicionalmente se lo maneja, para de esta manera tener una comunicación End to End facilitando la administración y escalabilidad de la red.

Seamless MPLS ofrece la ventaja de establecer una ruta de conmutación de etiquetas de extremo a extremo (E2E LSP) a través de las capas de acceso, agregación y borde es decir todos los servicios pueden encapsularse utilizando MPLS en la capa de acceso y transmitirse a través de las tres capas, esto gracias a que se establece un LSP entre dos nodos cualquiera para implementar servicios.

El presente proyecto se enfoca en proponer un diseño el cual involucre a la tecnología Seamless MPLS a fin de poder tener una arquitectura que garantice la escalabilidad e interoperabilidad de la red móvil 4G LTE para la ciudad de Cuenca. Este diseño involucra la parte de equipamiento, arquitectura de red, protocolos y presupuesto final para los routers de acceso, agregación y borde de la red IP-RAN.

PALABRAS CLAVE:

- **TECNOLOGÍA LTE (LONG TERM EVOLUTION)**
- **IP-RAN**
- **SEAMLESS MPLS**
- **THROUGHPUT**
- **MOBILE BACKHAUL (IP RAN)**
- **E2E LSP**

ABSTRACT

Globally there is a growing requirement for mobile broadband services, caused by the high penetration of cellular networks, and the growing demand for access to data, multimedia content and services. Traditional 2G and 3G networks have been exceeded in their capacity, without meeting this demand, suffering from congestion, with an impact on the quality of service to the user. The LTE technology, Long Term Evolution, arises as a response to these needs, presenting a

communication architecture designed to provide broadband access through a mobile network. (Jaramillo, 2015) .

The current deployment of LTE technology since 2015 in Ecuador shows an exponential growth in the use of new generation networks, this can be a problem making transport or backhaul networks obsolete. Due to the massive increase in services and subscribers in the network, traditional MPLS will complicate network scalability and administration in excess. Having MPLS only in the borde hierarchical deployment requires greater cooperation between the different layers, making it difficult to expand the network and the service because the services are not End to End.

Based on a sizing of the possible number of LTE users and the throughput that they can generate by 2023, it is proposed to design a network architecture based on Seamless MPLS which will allow the MPLS region to be extended to the access layer and not only in the borde as it is traditionally handled, in order to have an End to End communication facilitating the administration and scalability of the network.

Seamless MPLS offers the advantage of establishing an end-to-end label switching path (E2E LSP) through the access, aggregation and borde layers, that is, all services can be encapsulated using MPLS in the access layer and transmitted through of the three layers, this thanks to the fact that an LSP is established between any two nodes to implement services.

The present project focuses on proposing a design which involves Seamless MPLS technology in order to have an architecture that guarantees the scalability and interoperability of the 4G LTE mobile network for the city of Cuenca. This design involves the equipment part, network architecture, protocols and final budget for the access, aggregation and borde routers of the IP-RAN network.

KEYWORDS:

- **SEAMLESS MPLS**
- **THROUGHPUT**
- **MOBILE BACKHAUL (IP RAN)**
- **LTE (LONG TERM EVOLUTION)**
- **E2E LSP**

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Antecedentes

En la sociedad moderna el empleo de la tecnología está en constante demanda, su amplio uso ha ido cambiando nuestra vida diaria y nuestras necesidades, cada día las tecnologías de la información y comunicación (TIC) adquieren mayor relevancia, sin embargo, debe existir una evolución a la par entre las tecnologías y las redes que permiten el uso de estas, con el fin de asegurar las demandas del mercado y garantizar una escalabilidad sostenible en el tiempo.

De manera particular, el sector de las comunicaciones móviles en los últimos años ha tenido un cambio trascendental debido al gran incremento en el número de usuarios y el uso de dispositivos móviles cada vez más sofisticados. El desarrollo de tecnologías, servicios y aplicaciones basadas en el consumo de datos hacen que el empleo de los dispositivos móviles no solo se limite al uso del servicio de voz, mínimos servicios web o mensajes cortos (SMS) como tradicionalmente lo hacían. De acuerdo con Jiménez (2013) el servicio de voz tradicional está quedando en segundo plano frente al consumo de datos móviles, siendo necesarios anchos de banda mayores para servicios multimedia que históricamente solo eran disponibles a través de redes fijas. (Jiménez, 2013)

En esta última década la llegada de tecnologías de nueva generación como 4G LTE y en un futuro próximo 5G, exigen la evolución a la par en las tecnologías empleadas en el transporte móvil y el manejo de tráfico de datos, con el fin de que adaptándose a nuevos protocolos y arquitecturas permitan un transporte rentable y escalable para todas las tecnologías móviles (GPRS, GSM,

EDGE, UMTS, HSPA, HSPA+, LTE, LTE-A) además las arquitecturas deben estar en plena consonancia con la evolución e interoperabilidad futura de tecnologías móviles.

Actualmente las redes de transporte están basadas en IP, lo que permite seguir usando la misma infraestructura de la red de transporte tradicional, pero manejando la demanda de tráfico de datos de una manera más adecuada, reduciendo el costo asociado al ancho de banda. Con la llegada del 4G en los últimos años la red de transporte sufrió un cambio generacional, cambiando el backhaul móvil a tecnologías basadas en la conmutación de etiquetas, sin embargo, este esquema solo se maneja en el core de la red impidiendo tener una escalabilidad sostenible debido a la cantidad de conexiones que deben agregar los equipos de core, por lo que los proveedores de servicio buscan nuevas soluciones que permitan reducir los gastos OPEX y CAPEX que garanticen la escalabilidad de la red a la vez que se introducen nuevos servicios.

1.2. Justificación e importancia

El consumo de datos IP por dispositivos móviles está aumentando. Los usuarios acceden desde redes móviles a la misma variedad de servicios de banda ancha que se experimentan en redes fijas, causando un alto volumen de tráfico y problemas de escalabilidad (Sobanski, 2018). Actualmente las telecomunicaciones en el Ecuador atraviesan un proceso de cambios basados en el despliegue de la banda ancha inalámbrica; estos cambios se presentan como desafíos para los operadores móviles, desde el año 2015 en Ecuador existió un crecimiento exponencial de los servicios de LTE, para marzo del 2019 el número de suscriptores de esta tecnología había crecido un 82% respecto al año 2017, el uso masivo de terminales móviles más robustos y sofisticados hace que los usuarios demanden más servicios, llevando a que muchas de las redes de transporte(backhaul) queden obsoletas. El incremento de suscriptores y la cantidad de tráfico de datos hace trascendental migrar

la red de transporte a una que permita cubrir las expectativas de velocidad de los usuarios y de las operadoras móviles.

Con el fin de adaptarse al futuro internet para las demandas de tráfico anticipadas, las tecnologías deben ser escalables independientemente del tipo de servicio, es en donde Seamless MPLS ofrece la ventaja de que todos los servicios pueden ser encapsulados en la capa de acceso y transmitirse a lo largo del LSP E2E hacia las otras capas.

1.3. Alcance del proyecto

Con el proyecto de investigación a realizarse, se espera obtener un diseño de red que permita facilitar la comunicación y garantizar la interoperabilidad entre las capas de acceso, agregación y core de una red seamless MPLS para los componentes de una red móvil 4G. Este proyecto permitirá a futuras investigaciones analizar la escalabilidad de un esquema de red basado en seamless MPLS añadiendo más servicios al Mobile Backhaul (IP-RAN).

1.4. Objetivos

1.4.1. Objetivo General

- Proponer una arquitectura física (Network Región) y lógica de la red basada en Seamless MPLS para la implementación de un Mobile Backhaul (IP-RAN) de nueva generación en la ciudad de Cuenca.

1.4.2. Objetivos Específicos

- Determinar y reconocer los conceptos que conforman un sistema LTE, arquitectura IP-RAN, protocolos de enrutamiento y Seamless MPLS.

- Dimensionar los equipos(routers) IP de acuerdo con un estudio de la situación actual del servicio de datos móviles, cantidad de usuarios y throughput que estos generan en la ciudad de Cuenca.
- Definir la segmentación de la red de acuerdo con las múltiples regiones (acceso, agregación y borde) basado en un dominio IGP independiente para cada región.
- Simular la arquitectura IP-RAN propuesta basada en un entorno seamless MPLS garantizando una óptima conectividad y enrutamiento.
- Describir los detalles técnicos necesarios para la correcta instalación de los routers usados a nivel de acceso, agregación y borde.
- Realizar un presupuesto del costo de la solución para el backhaul de transmisión IP-RAN de una operadora móvil en la ciudad de Cuenca.

1.5. Descripción General del Proyecto

Primero, se presenta de modo general la explicación del trabajo de titulación, así como la justificación e importancia, los objetivos y el alcance.

En la segunda sección, se expone el Estado del Arte de los asuntos involucrados en el proyecto, se detalla los componentes de una arquitectura LTE, la jerarquía en IP-RAN y los protocolos de enrutamiento necesarios para armar seamless MPLS.

Para una tercera sección, se hace un estudio de la situación actual del Ecuador y la ciudad de Cuenca, se realiza el diseño físico, lógico y una simulación de la red en base a una arquitectura seamless MPLS. Finalmente, se analiza el funcionamiento de la red.

CAPÍTULO II

2. ESTADO DEL ARTE.

2.1. Tecnología LTE o Mobile Network

LTE ó Long Term Evolution es un estándar de alta velocidad para comunicaciones inalámbricas destinada a terminales de datos y teléfonos móviles. La tecnología LTE es la sucesora del sistema universal de telecomunicaciones móviles (UMTS) que a su vez evoluciono del sistema global para comunicaciones móviles (GSM) (yateBTS, s.f.).

LTE utiliza dúplex por división de tiempo (TDD) y dúplex por división de frecuencia (FDD). Un enlace descendente o ascendente con TDD usa intervalos de tiempo en la misma frecuencia, mientras que FDD usa bandas separadas para transmitir datos de enlace descendente y ascendente. Los esquemas de modulación en LTE son:

- Enlace Descendente: QPSK, 256-QAM, 64-QAM, 16-QAM.
- Enlace Ascendente: QPSK, 64-QAM, 16-QAM (yateBTS, s.f.).

Un QAM más alto brinda mejores tasas de velocidad y un QAM más bajo mejor robustez contra la interferencia y el ruido. Respecto a tecnologías de comunicaciones anteriores LTE tiene una eficiencia espectral dos a cuatro veces mayor. Los elementos principales en la arquitectura de red LTE son:

- Núcleo de paquete evolucionado (EPC).
- UMTS evolucionada (E-UTRAN).
- Equipo de usuario (UE) (yateBTS, s.f.).

2.1.1. EPC

EPC es la red central de LTE, se comunica con redes que manejan paquetes de datos. EPC usa componentes que cumplen las funciones de; autenticación, enrutamiento de carga, descarga de paquetes IP, asignación de direcciones IP, gestión de movilidad calidad y servicio. EPC está formado por:

- **Entidad de gestión de movilidad (MME):** Es la entidad que se encarga de la señalización entre EPC-NodeB y EPC-UE. Non access stratum (NAS) es el protocolo utilizado para realizar la señalización. MME realiza autenticación conectándose a la interfaz del eNodeB, para lo cual solicita al HSS información del usuario que intenta conectarse a la red, existe un intercambio de información entre HSS-UE. MME posibilita la movilidad del usuario dentro de la propia red o diferentes redes y también es el responsable de fijar un router de puerta de enlace a internet.
- **Servicio de puerta de enlace S-GW:** Se utiliza para realizar handover o traspaso del servicio entre estaciones vecinas eNodeB. En caso de intercepción ilegal, S-GW realiza replicación del tráfico de usuarios.
- **Paquete de datos Gateway (P-GW):** Es la entidad que garantiza la conectividad del UE hacia redes externas. Es el nodo de conexión entre redes externas y el UE, siendo el punto de entrada y salida del tráfico de datos.
- **Servicio de abonado domestico (HSS):** Es la base de datos que contiene información de usuario-suscripción que permite el establecimiento de sesiones y llamadas. Es un componente heredado de GSM y UMTS (yateBTS, s.f.).

La interfaz entre S-GW y P-GW es llamada S8 si los dispositivos están en redes diferentes o S5 si se encuentran en la misma red, los componentes de EPC descritos se ilustran en la Figura 1.

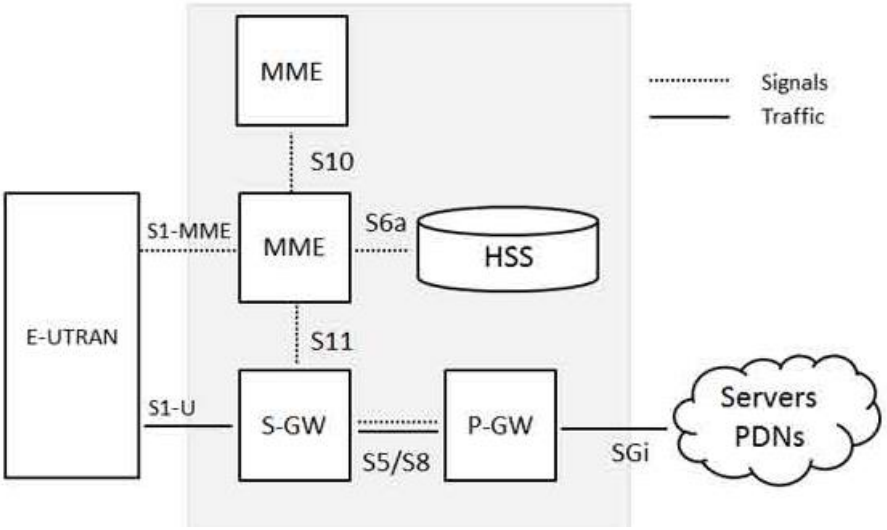

Figura 1. Componentes EPC
Modificado de: (yateBTS, s.f.)

2.1.2. E-UTRAN

Es el encargado de conducir las comunicaciones entre el EPC y el UE, solo tiene un componente llamado eNodeB el cual es una estación. eNodeB provee todos los UE recepción y transmisión de radio mediante el procesamiento de señales digitales y analógicas (yateBTS, s.f.).

E-ULTRAN envía mensajes de señalización a todos los UE. La interfaz S1 es usada para la conexión entre EPC-eNodeB. La interfaz X2 se utiliza para la conexión entre eNodeB cercanas y sirve para reenviar paquetes y señalización. La arquitectura de la red de acceso de radio terrestre UMTS evolucionada (E-UTRAN) se ilustra en la Figura 2 (yateBTS, s.f.).

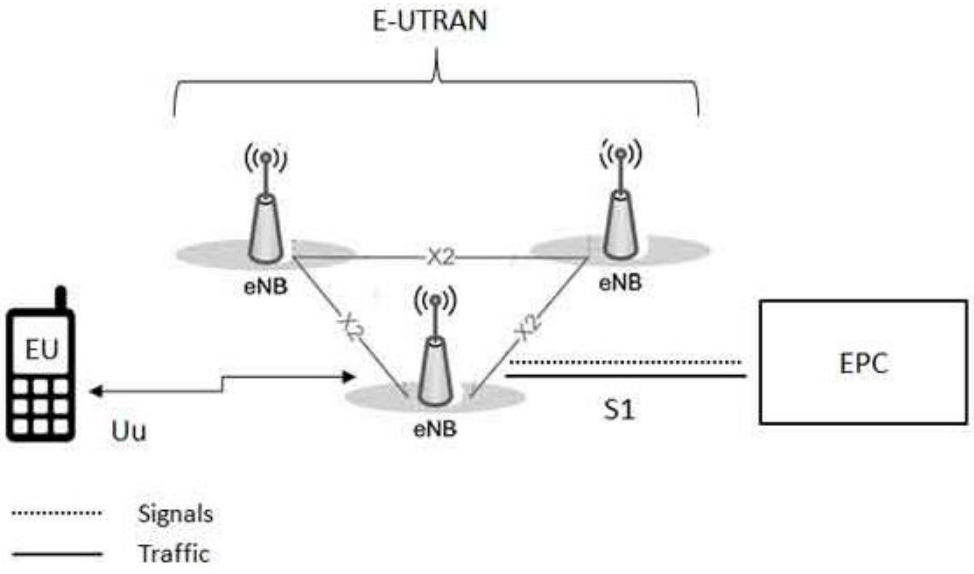

Figura 2. Arquitectura E-ULTRAN
Modificado de: (yateBTS, s.f.)

2.1.3. UE

UE es un dispositivo del usuario final. Los dispositivos pueden ser computadoras equipadas con un adaptador de banda ancha móvil, un teléfono portátil o cualquier equipo usado para la comunicación o conexión con el eNodeB (yateBTS, s.f.).

Todas las llamadas inician y terminan en el UE. Las tareas realizadas por el UE hacia el EPC son:

- Control de llamadas.
- Gestión de la movilidad.
- Gestión de la sesión.
- Gestión de la identidad.

UE posee una tarjeta de circuito integrado universal (UICC) conocida como SIM la cual almacena información del usuario y claves de seguridad identificadas por su operador móvil para conocer su número, plan o servicios (yateBTS, s.f.).

2.2. Mobile Backhaul (IP-RAN)

El termino IP-RAN(IP Radio Access Network) es usado para describir una red de acceso por radio (2G, 3G o 4G) la cual usa IP en su capa de trasporte, IP-RAN remplaza a tecnologías basadas en TDM y con ello permite que el proveedor de servicios se beneficie de la reducción del gasto operativo(OPEX) (MPIRICAL, s.f.).

El término “Mobile Backhaul” se refiere a la red de transporte existente entre el core de la red móvil y las radio bases (Paredes, 2016). La función principal de un Mobile Backhaul es brindar óptima conectividad entre los diferentes componentes que conforman un Mobile Network sean estas arquitecturas de 2G, 3G o 4G, como se observa a alto nivel en la Figura 3 (Fujitsu Network Communications, 2017).

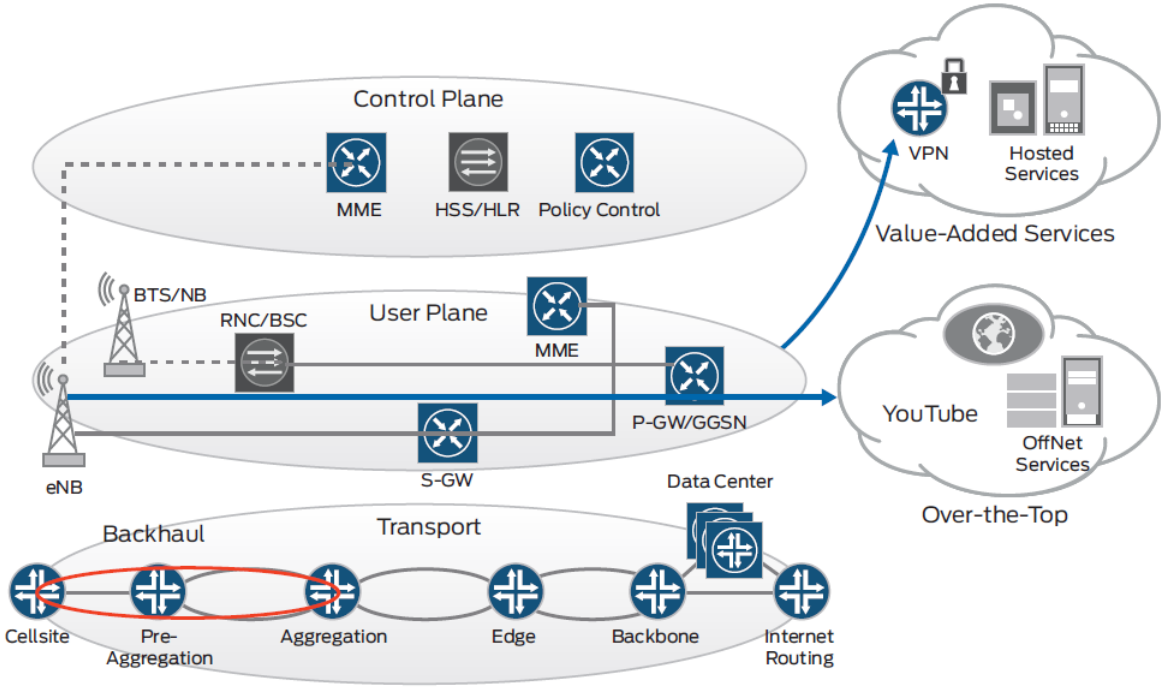

Figura 3. Componentes del Mobile Backhaul (IP RAN).
Modificado de: (Fujitsu Network Communications, 2017)

Los componentes de la Mobile Network para 4G tienen requerimientos de conectividad como se observa en la Tabla 1 (Fujitsu Network Communications, 2017).

Tabla 1
Requerimientos de conectividad Mobile Networks 4G

Mobile Network (Generación)	**Componentes Principales**	**Interface de Conexión**	**Mobile Network Requerimiento**	**Topología del Servicio**
4G	eNB, SGW, MME, PGW	eNB to eNB (X2) eNB to EPC (S1)	Ethernet/IP	Partially Mesh, Full Mesh & Hub-Spoke

Los recursos a nivel de tiempos de convergencia y capacidad transporte en caso de fallas para 4G se describen en la Tabla 2 (Fujitsu Network Communications, 2017).

Tabla 2
Requerimientos de capacidad Mobile Networks 4G.

Mobile Network (Generación)	**Componentes Principales**	**Interface de Conexión**	**Mobile Network Requerimiento**
4G	S1-U	150 Mbps	200 ms
	S1-MME	10 Mbps	200 ms
	X2-C	10 Mbps	200 ms
	X2-U	10 Mbps	200 ms

Una implementación IP-RAN presenta también beneficios a nivel de OPEX debido a que se utiliza el mismo Mobile Backhaul existente en la red reduciendo el costo operacional y además garantiza la interoperabilidad de los diferentes componentes de las tecnologías dentro del Mobile Network (Fujitsu Network Communications, 2017).

La red IP-RAN está formada por routers de conmutación de paquetes los cuales proporcionan alta confiabilidad, bajo retraso, gran ancho de banda y E2E QoS (quality of service). IP-RAN se ha convertido en una solución convencional para el transporte de los diferentes servicios para el Mobile Backhaul. Los servicios que transporta la red IP-RAN garantizan cumplir la amplia gama de multiservicios requeridos, cubriendo las necesidades de acceso a las estaciones base 2G, 3G y LTE/LTE-A independientemente del tipo de servicio, desde servicios de voz móviles hasta multiservicios de banda ancha (Baoya, 2016).

El avance hacia una red IP-RAN trae consigo tecnologías que permiten tener una convergencia más rápida que las redes de conmutación de paquetes tradicionales. El uso de protocolos de convergencia de rápida o protecciones de túnel ofrecen confiabilidad en la red y una respuesta a nivel de milisegundos. Para evolucionar hacia una red IP-RAN se necesitan routers de gran capacidad y confiabilidad, medidores de desempeño del rendimiento de alta precisión y sincronización de reloj (Baoya, 2016).

A medida que las redes de radio evolucionan 2G, 3G, LTE y 5G el despliegue de las estaciones ocurre más densamente. El salto generacional demanda mayores prestaciones para los equipos. En la era 4G(LTE) la velocidad máxima es de 100 Mbps, para LTE-A la velocidad máxima es de 1 Gbps y se espera que para la era 5G la tasa pueda llegar hasta los 20 Gbps, con ello los requerimientos de ancho de banda que deben manejar los routers son cada vez mayores. Los routers de core deben tener prestaciones que varían desde los cientos de Gbps a decenas de Tbps, para cumplir con los requisitos de ancho de banda de 4G y hasta 5G en el que el router de core se debe manejar capacidades de 100GE, 200GE o 400GE por slot y 10GE/40GE/100GE por tarjeta (Baoya, 2016).

2.2.1. Jerarquía IP-RAN

La red IP-RAN debe ser capaz de priorizar y diferenciar entre los diferentes servicios y aplicaciones de la red; cada elemento en la red de transporte debe asegurar una buena experiencia al usuario final (Vega, 2016). Existen tres etapas o jerarquías dentro de una red de transporte IP-RAN en la que cada una cumple funciones específicas dentro del backhaul, siendo el objetivo general de esta división aislar los errores a una única región, mejorando la convergencia e incrementando la escalabilidad de la red; estas etapas se detallan a continuación:

2.2.1.1. Low RAN

Low RAN también conocida como etapa de acceso constituye todos los routers que se encuentran en los eNodeB, llamados también routers de celda. La función principal dentro del backhaul es transportar todo el tráfico de la celda hasta el nodo de Mid RAN. El medio de transporte de esta información dependerá de los diferentes medios físicos (fibra óptica o microondas) del proveedor del servicio. Los routers en esta etapa son llamados equipos cell site Gateway (CSG) (Ayala, 2011).

2.2.1.2. Mid RAN:

Mid RAN también conocida como etapa de agregación debido a que los equipos dentro de esta etapa agregan todo el tráfico de los equipos de acceso y los convergen hacia la siguiente etapa del IP-RAN (High RAN). La cantidad de tráfico que estos equipos manejen dependerá del número de routers de celda que agreguen dentro de la topología de la red. Los routers en esta etapa son llamados equipos de agregación (AGG). (Ayala, 2011)

2.2.1.3. High RAN:

High RAN también conocida como etapa de borde, se encarga de recoger y concentrar el tráfico de los agregadores que pertenezcan a su topología y direccionarlo hacia el core de la red MPLS. Los routers en esta etapa son llamados equipos de borde (BO). (Ayala, 2011)

2.3. Protocolos de Enrutamiento

Los componentes de un protocolo de enrutamiento son; estructuras de datos (tablas de enrutamiento), algoritmos y mensajes de protocolo. Un protocolo de enrutamiento facilita el intercambio de datos entre dispositivos definiéndose como la agrupación de algoritmos, mensajes y procesos usados para transmitir información (Cisco, 2009).

Un algoritmo de enrutamiento, como menciona Tanenbaum (2012) “Es un proceso por el cual la red decide qué ruta tomar”, sirve para escoger el mejor camino por donde un paquete entrante se transmitirá hacia su destino en base a ciertos criterios de la red. Dentro de este proceso el enrutamiento IP se puede dividir en dos grandes categorías; enrutamiento estático y enrutamiento dinámico ambas permiten enrutar y construir las tablas de enrutamiento (RIB) y las tablas de reenvió (FIB) (Douglas, 2009).

2.3.1. Enrutamiento Estático

Las rutas estáticas son definidas administrativamente y representan una ruta especifica por la cual los paquetes deberán llegar a su destino. Tiene varios usos, entre ellos están:

- Enrutamiento desde y hacia redes de conexión única.
- En redes formadas por pocos routers y que su red no tenga previsto crecer con el tiempo.
- En redes donde se requiera configurar una ruta predeterminada (Cisco, 2009).

La configuración de enrutamiento estático acarrea un mínimo procesamiento del CPU de los routers, sin embargo, la configuración en cada router requiere intervención de un administrador que conozca toda la red para la correcta implementación, derivando en mantenimientos más prolongados en caso de que la red crezca o existan cambios en esta (Cisco, 2009).

2.3.2. Enrutamiento Dinámico

El enrutamiento dinámico permite que los routers puedan conocer la topología de red de manera automática, la tabla de enrutamiento de cada router guarda la información y dependiendo de la distancia administrativa o la métrica desde el destino se escoge el camino más eficiente, esta ruta es guardada en la tabla de reenvío, en caso de que la distancia administrativa y la métrica sean iguales se reparte el tráfico entre las rutas (Tanenbaum, 2012). Es decir, el enrutamiento dinámico tiene dos procesos principales; obtener información actual de la topología y calcular la mejor manera de reenviar la información en base a la información de la topología (Douglas, 2009).

Cada router comparte información con otros sobre las redes que conoce, las rutas se propagan y permiten conocer los posibles destinos a los que pueden llegar otros routers, el enrutamiento dinámico permite aprender rutas automáticamente sobre estas redes a partir de otros routers, de esta manera la información de las tablas RIB y FIB se mantiene actualizada periódicamente (Douglas, 2009).

2.3.3. Autonomous System (AS)

Autonomous System hace referencia a un grupo de dispositivos bajo una sola administración técnica común, el grupo de dispositivos que conforman el AS usan un único protocolo de puerta de enlace (IGP) y métricas para difundir la información. Los distintos AS son identificados por un número asignado por la Network Información Center (NIC) (Juniper Networks, 2019).

El tamaño de un sistema autónomo puede variar dependiendo de razones técnicas, económicas o administrativas. Se debe considerar que el tráfico de enrutamiento puede crecer como el cuadrado del número de enrutadores, entonces dependiendo del tamaño del sistema autónomo la capacidad de procesamiento de los routers a escogerse variara (Douglas, 2009).

Existen AS públicos y privados, el número del sistema autónomo es de 16 bits es decir se tiene 65535 números para elegir, los números privados del sistema autónomo están en el rango 64512 – 65535 y para números globalmente únicos en el rango 1 – 64511 (Juniper Networks, 2019).

2.3.4. Tipos de Protocolos de Enrutamiento

La arquitectura de internet distingue entre dos categorías en protocolos de enrutamiento descritos a continuación:

- Protocolo de gateway interior (IGP).
- Protocolo de gateway exterior (EGP) (Gross, 1992).

2.3.4.1. Interior Gateway Protocol (IGP)

Los IGP son protocolos de enrutamiento usados en todos los dispositivos bajo un mismo dominio administrativo conocido como sistema autónomo. Existen múltiples protocolos IGP estandarizados para la arquitectura de internet, es razonable utilizar un IGP estándar dentro de un AS mientras se usa un segundo protocolo IGP dentro de un segundo AS (Gross, 1992).

De acuerdo con Douglas (2009), "un IGP puede limitar el tamaño y la complejidad de enrutamiento dentro del sistema autónomo". Los IGPs utilizan métricas de enrutamiento para escoger el camino más optimo hacia el destino. Las métricas pueden estar definidas por; el número de saltos entre los routers o el estado del enlace basado en el throughput, delay, o Jitter. Existen IGPs que escogen el camino más optimo basado en un conjunto de parámetros (Douglas, 2009).

2.3.4.2. Protocolo de gateway exterior (EGP)

El protocolo EGP es usado para intercambiar información de enrutamiento entre distintos sistemas autónomos. El protocolo tiene mecanismos de monitoreo para conocer la accesibilidad de los vecinos y descubrir si existen solicitudes de actualización, está basado en el intercambio de mensajes Hello/I-Heard-You (IHU) a manera de encuestas periódicas. EGP permite anunciar únicamente redes de destino accesible dentro del AS. Solamente el protocolo de gateway fronterizo (BGP) es usado para configurar un EGP (Mills, 1984).

La instalación y configuración de un EGP es más complicada que la de un IGP, pero ofrece más flexibilidad y una cabecera más pequeña que tiene impacto en un menor tráfico. EGP usa políticas de restricción mediante las cuales un administrador elige exactamente qué información se desea divulgar (Douglas, 2009).

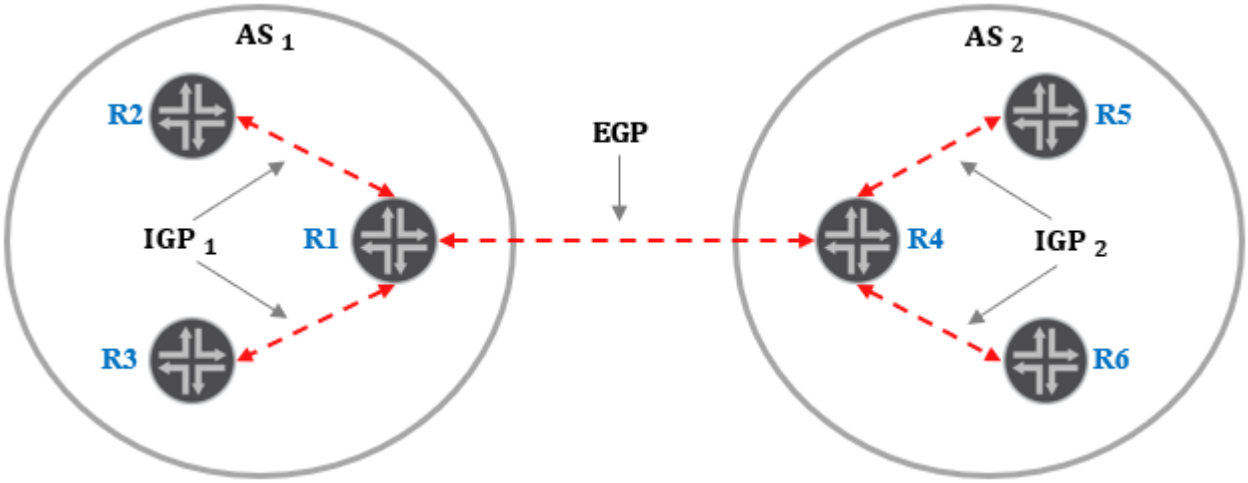

Figura 4. Comunicación EGP/IGP entre sistemas autónomos
Modificado de: (Molenaar, 2017a)

La Figura 4 ilustra la comunicación de routers en sistemas autónomos (AS_1, AS_2), cada sistema autónomo es libre de usar un tipo de IGP, el sistema autónomo 1(AS_1) se comunica internamente con los routers(R_2, R_3) usando IGP_1 y el sistema autónomo 2(AS_2) se comunica internamente con

los routers(R_5, R_6) usando IGP_2. La comunicación entre los sistemas autónomos se da entre los routers R_1 y R_4 que usan EGP para comunicarse, R_1 envía un resumen sobre la información de su AS_1 hacia R_4 por su parte R_4 propaga la información hacia los routers (R_5, R_6) dentro de su sistema autónomo (AS_2), el mismo proceso se da desde R_4 hacia R_1. (Molenaar, 2017a)

2.3.5. Intermediate System to Intermediate System (IS-IS)

Es un protocolo IGP de estado de enlace el cual forma adyacencias vecinas con routers que estén en su mismo nivel para intercambiar información de estado de enlace, formando una base de datos y ejecutando un algoritmo que le ayuda a elegir la mejor ruta. El algoritmo usado por IS-IS es Dijkstra ó Shortest Path First (SPF), este algoritmo determina el camino más optimo en base a la información de la base de datos. (Molenaar, 2017a)

Se conoce como adyacencias vecinas o vecindad al sistema por el cual se mantiene la comunicación de enrutamiento entre dos routers, IS-IS usa dos niveles de jerarquía, el uso de jerarquías en la topología IS-IS permite trabajar con grandes dominios. Un dominio de enrutamiento puede ser dividido en subdominios conocidos como áreas esto permite que IS-IS soporte grandes topologías (Cisco, 2020).

Todo router es parte de un nivel de IS-IS y puede tener tres distintos roles:

- **Router de nivel 1:** Es un router intra-area, conoce solo los prefijos de su propia área en base a ellos forma una base de datos del estado de enlace de nivel 1 y crea un árbol SPF para su área. El nivel de IS-IS manejado por los routers es llamado L1.
- **Router de nivel 2:** Es un router backbone o de red troncal, conoce todas las rutas dentro y fuera del área, forma una base de datos de estado de enlace de nivel 2 y crea un árbol SPF de backbone. El nivel de IS-IS manejado por los routers es llamado L2.

- **Router de nivel 1-2:** Es un router que maneja roles de nivel 1 y nivel 2, forma bases de datos de estado de enlace diferentes una para cada nivel y compone dos árboles SPF para cada base de datos. Los niveles de IS-IS manejados al mismo tiempo por los routers es llamado L1/L2 (Juniper Networks, 2018).

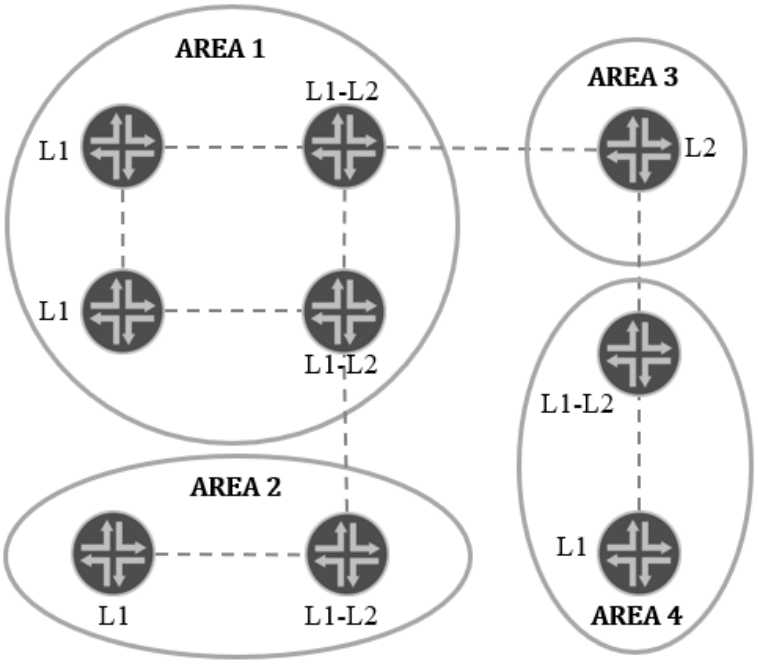

Figura 5. Topología basada en IS-IS.
Modificado de: (Molenaar, 2017a)

El enrutamiento interno dentro del área es enrutamiento de nivel 1 y el enrutamiento entre las distintas áreas es enrutamiento de nivel 2. Una topología de red basada en IS-IS, como la observada en la Figura 5, usa los dos niveles de IS-IS y los tres tipos de roles de un router. se observan tres hechos relevantes:

- El área 3 corresponde a un router backbone, en esta área no existen routers de nivel 1 por lo tanto no necesitan un router de nivel 1-2.
- El área 1 tiene dos routers de nivel 1-2, estos routers forman dos adyacencias de distintos niveles entre sí.

- Los routers de nivel 2 forman una cadena continua de routers de red troncal, como se observa en la Figura 6. (Molenaar, 2017a)

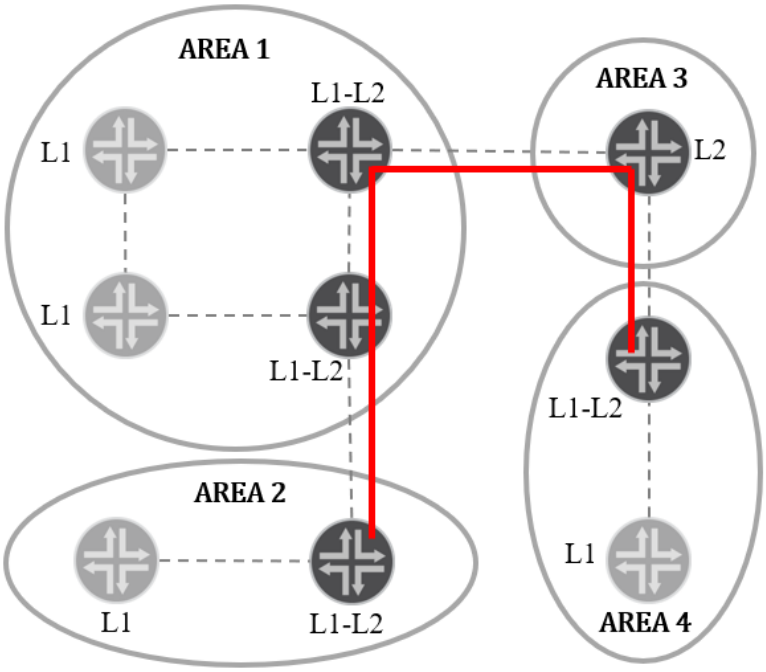

Figura 6. Topología basada en IS-IS, cadena continua de routers de nivel 2.
Modificado de: (Molenaar, 2017a)

Las adyacencias vecinas se forman al intercambiar paquetes hello entre routers del mismo nivel, formada la adyacencia los routers inundan al área con paquetes de estado de enlace (LSPs) de manera que todos conozcan su LSP en el área, cada router que haya formado una adyacencia vecina añade el LSP recibido y lo agrega su base de datos, ejecuta SPF y descubre la ruta más corta a cada destino. Cada router en IS-IS crea un único LSP para cada nivel, los LSP llevan múltiples prefijos (Molenaar, 2017a).

La base de datos para un router nivel 1-2 está formada por la agrupación de la base de datos de nivel 1 y la base de datos de nivel 2, ambas bases de datos están separadas, la base de datos de nivel 1 tiene el LSP del propio router y los LSPs de routers adyacentes de nivel 1, mientras que la base de datos de nivel 2 tiene tres elementos: el LSP del propio router, los LSPs de routers adyacentes

de nivel 2 y los nuevos prefijos copiados desde la base de datos de nivel 1 hacia la base de datos de nivel 2, es decir los routers troncales de nivel 2 conocen todos los prefijos que existen (Molenaar, 2017a).

La base de datos para los routers de nivel 1 y nivel 2 está formada por la agrupación del LSP del propio router junto con los LSPs aprendidos de routers de adyacencia vecina del mismo nivel. No existe intercambio de LSPs entre routers que tengan diferentes niveles, nunca un router de nivel 1 podrá aprender prefijos de otras áreas. Todos los routers deben haber formado una adyacencia vecina del mismo nivel antes de intercambiar LSPs (Molenaar, 2017a).

IS-IS prefiere prefijos que se encuentren en bases de datos de nivel 1 sobre prefijos que se encuentren en bases de datos nivel 2, sí existe el mismo prefijo en ambas bases de datos se elige el existente en la base de datos de nivel 1. Las bases de datos están sincronizadas y existe un paquete de número de secuencia (SNP) que se modifica cuando existe un cambio en un LSP, existen dos tipos de SNP (Cisco, 2020):

- **Paquete de número de secuencia parcial (PSNP):** Usado como acuse de recibo de una solicitud especifica de uno o más LSPs. También se usa para solicitar uno o más LSPs.
- **Paquete de número de secuencia completo (CSNP):** Usado para informar a otros routers que tienen información obsoleta o faltante, contiene una lista de todos los LSPs de la base de datos actual. (Cisco, 2020):

2.3.5.1. Sistema intermedio designado (DIS)

El mecanismo DIS se creó para solventar dos problemas relacionados a la inundación de LSPs en IS-IS, estos problemas son:

- Cuando un router envía un LSP, los routers receptores no informan al remitente que han recibido su LSP.
- La base de datos de estado de enlace crece exponencialmente con respecto al número de enrutadores en el sistema (Molenaar, 2017b).

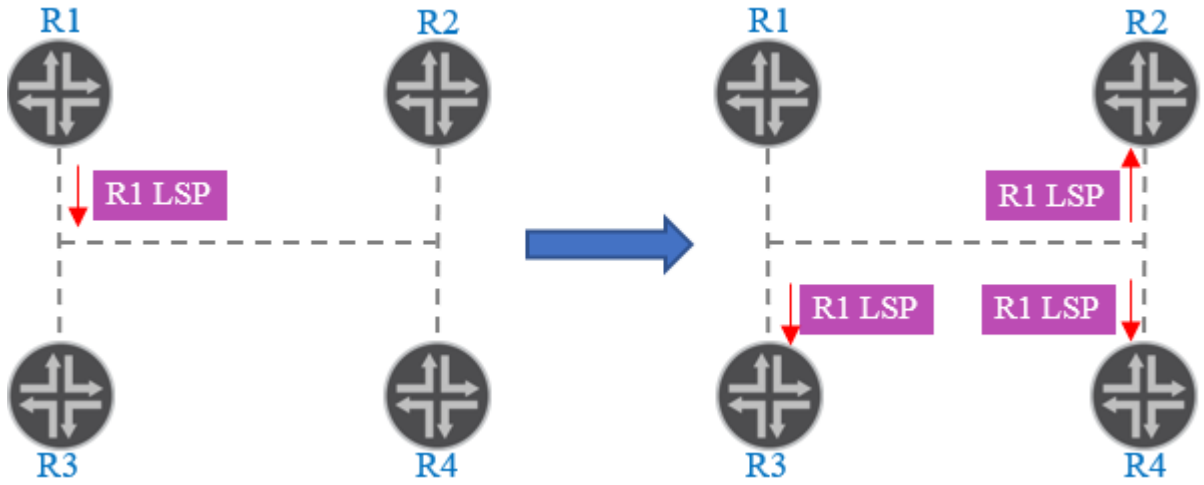

Figura 7. Difusión de un LSP en routers conectados a un segmento LAN
Modificado de: (Molenaar, 2017a)

El problema en el que los routers receptores no informan al remitente que han recibido su LSP se observa en la Figura 4. El router R1 envía su LSP, pero desconoce si los routers R2, R3 y R4 con quien formo adyacencias vecinas tienen su LSP, esto hace que R1 vuelva a inundar la red con su LSP (Molenaar, 2017b).

DIS soluciona el problema al escoger a uno de los routers dentro del área para que cree y actualice un pseudonodo o nodo virtual, el cual creara un CSNP e informará y actualizará los enlaces hacia todos los vecinos. El router DIS se selecciona basándose en la prioridad de la interfaz o en la dirección Mac. Un router se convierte en DIS sí su MAC es la más elevada de toda el área (Molenaar, 2017b).

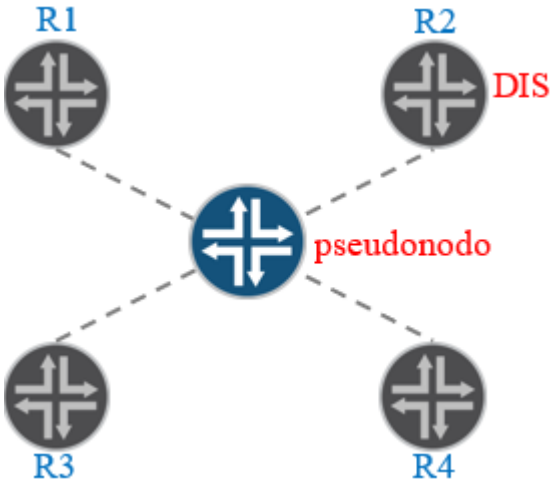

Figura 8. Pseudonodo creado por el router 2(R2)
Modificado de: (Molenaar, 2017a)

El pseudonodo observado en la Figura 8 fue creado por el router R2 que en este caso se seleccionó como DIS. El pseudonodo enviará un pseudo LSP que contiene una lista de todos los vecinos a los que está conectado con una métrica 0. Este comportamiento convierte la red acceso múltiple en una red de topología punto a punto, al simplificarse la topología del estado de enlace solo existen 4 adyacencias:

- **R1-**Pseudonodo
- **R2-**Pseudonodo
- **R3-**Pseudonodo
- **R4-**Pseudonodo

Solucionando el problema del crecimiento exponencial de la base de datos de estado de enlace (Molenaar, 2017b).

Además, existe el problema ocasionado por la falta de información de los routers receptores al remitente que han recibido su LSP, que, para solucionarlo, el pseudonodo envía un CSNP como se observa en la Figura 9.

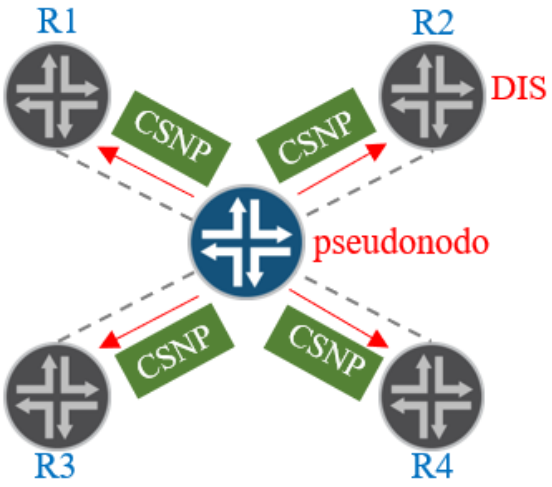

Figura 9. Pseudonodo envío de CSNPs
Modificado de: (Molenaar, 2017a)

Cada router verifica en el CSNP recibido su LSP con el que inundó la red, de esta manera el CSNP actúa como acuse de recibo, en caso de algún router no encontrar su LSP este router inundará la red nuevamente hasta recibir un acuse de recibo con su LSP. (Molenaar, 2017b).

Cuando un router reconoce su LSP en el CSNP, sin embargo, el número de secuencia es mayor que el de su propia base de datos, el router envía un PSNP solicitando la información más reciente, este PSNP es recibido por todos los routers que tengan la adyacencia vecina no obstante sólo DIS responderá este mensaje. Los CSNP se envían desde el pseudonodo cada 10 segundos de manera que cada router verifica si LSP es reconocida en el área y si su información está actualizada. Existe un router DIS para cada nivel de ISIS (Molenaar, 2017b).

2.3.5.2. Título de entidad de red (NET)

El identificador único para cada enrutador en IS-IS es llamado NET. El título de entidad de red es equivalente al ID del sistema o como en otros protocolos la dirección IP más alta del router. NET se basa en una dirección de servicio de red de punto de acceso (NSAP). Conforme a los requisitos de la red las NET pueden variar en hexadecimales de entre 8 a 20 octetos de longitud, la

dirección es configurada manualmente, con el formato que se observa en la Figura 10 (Molenaar, 2017a).

Figura 10. Formato título de entidad de red (NET)
Fuente: (Molenaar, 2017a)

En general, el formato de la NET puede ser dividido en parte del dominio inicial (IDP) y parte específica del dominio (DSP). IDP es usado para identificar a que dominio de enrutamiento pertenece y está formado por dos secciones (Molenaar, 2017a):

- **Identificador de autoridad y formato (AFI):** Es una codificación administrada por ISO, identifica una autoridad administrativa responsable de asignarle el direccionamiento.
- **Identificador de dominio inicial (IDI):** El IDI depende de la autoridad, por lo general utilizarán un valor diferente para cada cliente que se refiere a un número de (sub) dominio, en el formato más simple el IDI es omitido (Juniper Networks, 2018).

En redes privadas el AFI es 49 y el uso de IDI es opcional. La segunda parte de NET es DSP que son configuraciones locales, consta de tres partes:

- **High Order DSP:** Es el identificador de dominio de área puede ser de 0 a 12 bytes.
- **Sistem ID:** Es el identificador del sistema consta de 6 bytes únicos en todo el dominio puede ser una agrupación de la dirección MAC o una dirección IP expresados en formato decimal codificado en binario (BCD).
- **NSEL:** Es un selector y siempre tiene un valor de 0 (Juniper Networks, 2018).

2.3.6. Border Gateway Protocol (BGP)

BGP es el único EGP y admite dos tipos de intercambios de información, como se observa en la Figura 11. Cuando se intercambian rutas entre diferentes AS es llamado BGP externo (eBGP) y cuando se intercambian rutas dentro de un mismo AS es llamado BGP interno (iBGP) (Juniper Networks, 2019).

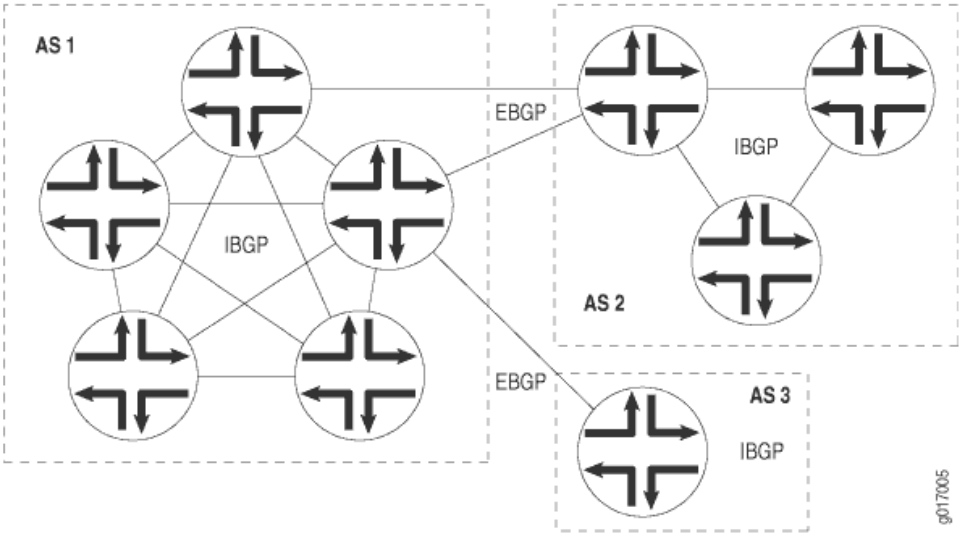

Figura 11. eBGP e iBGP en distintos AS
Fuente: *(Juniper Networks, 2019)*

Cada sistema autónomo es libre de elegir el IGP con el que desea trabajar, cada IGP usa una métrica de enrutamiento, por este motivo EGP no puede realizar comparaciones significativas entre las métricas usadas por cada IGP y definir que ruta tiene el menor costo o cual es la más optima entre múltiples sistemas autónomos, no hay manera de convertir saltos en throughput, esto quiere decir que BGP no usa métricas como los IGP. EGP reporta la existencia de rutas mas no su costo y elegirá la ruta en función a políticas de la red o reglas que usen atributos de ruta BGP (Douglas, 2009).

Los sistemas BGP se organizan en grupos. En un grupo eBGP hay pares de grupo llamados pares externos, los pares externos están en diferentes AS y comúnmente la subred es compartida.

En un grupo iBGP hay pares de grupo llamados pares internos, los cuales están en un mismo AS y no tienen que estar conectados directamente (Juniper Networks, 2019).

BGP en base de información de accesibilidad hacia cada sistema autónomo, construye un gráfico de conectividad AS, esto permite tomar decisiones de políticas a nivel de AS. El enrutamiento apoyado en políticas permite controlar la redistribución de información y elegir entre diferentes rutas a un destino (Juniper Networks, 2019).

La información intercambiada entre dos routers que maneja BGP incluye la ruta total hacia cada destino (ruta AS) e información adicional hacia la ruta, con esta información se conoce la topología y BGP puede:

- Detectar bucles de enrutamiento y eliminarlos.
- Tomar decisiones de políticas de enrutamiento y hacer cumplir preferencias administrativas a grupos de rutas específicos (Juniper Networks, 2019).

La ruta AS tiene una lista de todos los sistemas autónomos por los que pasa la ruta hasta llegar al destino. El primer número en esa lista corresponde al último sistema autónomo de la ruta antes de llegar al destino y el último número de la lista corresponde al primer sistema autónomo o generalmente el origen de la ruta. La información adicional hacia la ruta incluye los atributos de ruta usados en la política de enrutamiento (Juniper Networks, 2019).

Se usan mensajes de actualización para anunciar rutas, los mensajes de actualización se dan entre pares BGP. Las rutas se almacenan en la tabla de enrutamiento(inet.0). La información almacenada en inet.0 es la siguiente:

- Información de enrutamiento local.
- Información de enrutamiento adquirida de mensajes de actualización, recibida de pares.

- Información que BGP anuncia en mensajes de actualización (Juniper Networks, 2019).

La información de enrutamiento local es la que BGP aplica a las rutas en base a políticas locales. Se llama ruta activa a la ruta seleccionada como la mejor. De acuerdo con que router BGP anuncia una ruta se asignan valores para identificar su origen, siempre se prefiere el valor de origen más bajo, los valores posibles son:

- 0: La ruta fue aprendida mediante un IGP.
- 1: La ruta fue aprendida mediante un EGP.
- 2: Se desconoce el origen de la ruta aprendida (Juniper Networks, 2019).

2.4. MPLS

MPLS o conmutación de etiquetas multiprotocolo, es una tecnología de transporte de datos, en el modelo OSI este mecanismo esta entre la capa de red y la capa de enlace de datos, es llamado protocolo de capa 2.5, el encabezado MPLS se agrega entre el encabezado Ethernet e IP como se observa en la Figura 13 (Ghein, 2007).

Multiprotocolo debido a que se puede componer túneles para distintos tipos de tráfico como IP, Ethernet, frame-relay, etc. Su funcionamiento no se basa en la búsqueda del destino en la tabla de enrutamiento, sino en un reenvió en función de etiquetas.

MPLS admite dos soluciones de red:

- MPLS sin interrupciones intra-AS: Las etapas de low RAN, mid RAN y high RAN están dentro de un mismo AS. Este esquema es aplicable a redes de portadores móviles.
- MPLS sin interrupciones entre-AS: Las etapas de low RAN y mid RAN están dentro de un mismo AS mientras que la etapa de high RAN está en otro AS. Este esquema es aplicable a redes de servicios empresariales (Ghein, 2007).

Los campos en una cabecera MPLS se distribuyen a manera de un conjunto de bits, como se observa en la Figura 12.

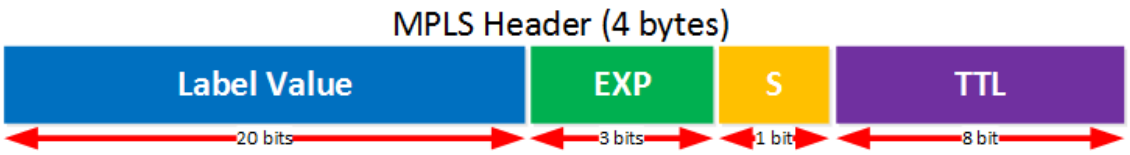

Figura 12. Cabecera MPLS
Fuente: (Molenaar, 2015)

- **Label Value:** Campo de 20 bits, contiene el valor de la etiqueta.
- **EXP:** Campo de tres bits, del inglés experimental, se usa para segmentar en base a calidad y servicio (QoS) cada etiqueta.
- **S:** Campo de un bit, del inglés stack, establece su valor en uno si el encabezado actual corresponde al último o establece su valor en cero si quedan más encabezados MPLS por venir.
- **TTL:** Campo de 8 bits, del inglés Time-to-live, representa el tiempo de vida de la cabecera, decrementa su valor al pasar por un router, cuando llega a cero el paquete es descartado (Ghein, 2007).

El encabezado MPLS se encuentra entre el encabezado de capa 2 y capa 3, como se observa en la Figura 13:

Figura 13. Encabezado MPLS entre el encabezado Ethernet (capa 2) e IP (capa 3).
Fuente: (Molenaar, 2015)

2.4.1. Equipos en una red MPLS:

Los equipos más comunes dentro de la red MPLS son el equipo del cliente conocido como Cliente Edge (CE), los equipos que conforman un esquema general de un proveedor de servicios

de internet ISP son; el equipo de borde de proveedor (PE) y el equipo de core del proveedor (P), como se observa en la Figura 14.

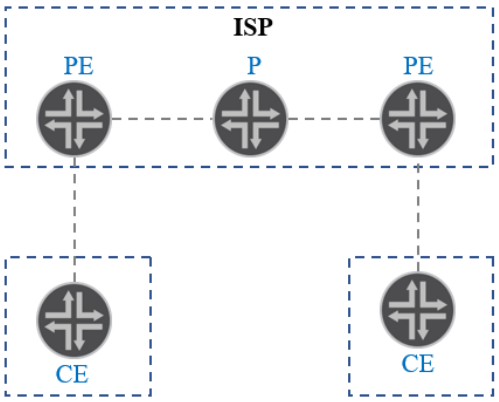

Figura 14. Esquema cliente-ISP dentro de una red MPLS
Modificado de: (Molenaar, 2015)

Los tres equipos presentados en la Figura 14 son descritos a continuación:

- **CE:** Último equipo de la red del cliente no usa MPLS y puede ser de capa 2 o capa 3.
- **PE:** Es el equipo borde en la red del ISP, recibe los paquetes IP del CE y les agrega una etiqueta MPLS para enviarlos al P. Este equipo es conocido como label edge router (LER).
- **P:** Es el equipo de core e interconecta los PE, pueden existir varios equipos P que interconecten dos PE. El equipo P intercambia paquetes de acuerdo con sus etiquetas. Este equipo es conocido como label switch router (LSR) (Molenaar, 2015).

Los equipos de una red MPLS pueden realizar tres acciones con etiquetas:

- **Push:** Acción de añadir una etiqueta a un paquete.
- **Pop:** Acción de remplazar una etiqueta con otro valor
- **Swap:** Acción de remover la etiqueta. (Molenaar, 2015)

El envío de un paquete IP en una red MPLS, como se observa en la Figura 15, realiza todas las acciones (push, pop, swap) con etiquetas descritas.

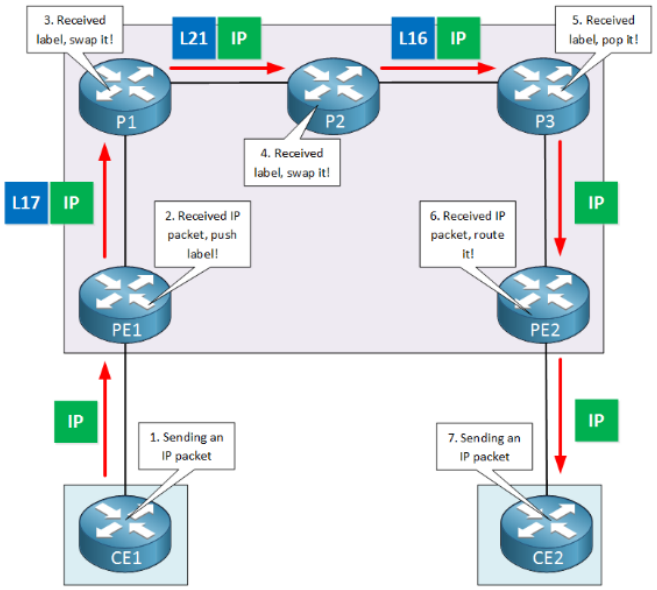

Figura 15. Envío de paquete IP usando MPLS
Fuente: (Molenaar, 2015)

El proceso presentado en la Figura 15 tiene como finalidad llevar el paquete IP entre equipos de los clientes desde CE1 hasta CE2, el desarrollo se describe a continuación:

- CE1 envía el paquete IP hacia PE1.
- PE1 recibe el paquete IP de CE1, realiza push y lo envía al core del ISP.
- P1 recibe el paquete etiquetado de PE1, realiza swap y lo envía a P2.
- P2 recibe el paquete etiquetado de P1, realiza swap y lo envía a P3.
- P3 recibe el paquete etiquetado de P2, realiza pop y lo envía a PE2.
- PE2 recibe el paquete IP de P3 y lo envía a CE2 (Molenaar, 2015).

Los routers CE1 y CE2 solo trabajan con paquetes IP, no tienen conocimiento de MPLS. Los router P1 y P2 realizan swap cada uno debido a que las etiquetas son significativas solo localmente.

El router P3 realiza pop para que PE2 reciba y envié solo un paquete IP. El último P del core siempre realizará pop.

Los routers CE1 y CE2 solo trabajan con paquetes IP, no tienen conocimiento de MPLS. Los router P1 y P2 realizan swap cada uno debido a que las etiquetas son significativas solo localmente. El router P3 realiza pop para que PE2 reciba y envíe solo un paquete IP. El último P del core siempre realizará pop.

La arquitectura MPLS usa los siguientes términos para referirse al tráfico y rutas que están bajo una etiqueta:

- **Label switched path (LSP):** Toda ruta MPLS bajo una etiqueta entre dos extremos es llamada LSP.
- **Forwarding Equivalence Class (FEC):** Todo tráfico bajo una etiqueta recibe el nombre de FEC (Ghein, 2007).

2.4.2. Protocolo de distribución de etiquetas (LDP)

LDP es un protocolo usado en MPLS para intercambiar información y generar automáticamente etiquetas. Las etiquetas se generan en cada router en función de los prefijos aprendidos y son intercambiadas con otros routers después de formar una adyacencia LDP (Molenaar, 2015).

La adyacencia LPD se forma utilizando multidifusión y el protocolo de datagramas de usuario (UDP), se envían paquetes hello entre las interfaces de los routers para de esta manera descubrir vecinos, cada paquete hello contiene una dirección IP. Dos router vecinos que hayan establecido adyacencias usan el protocolo de control de transmisión (TCP) para establecer una conexión e intercambiar etiquetas. La conexión TCP se usa comúnmente con la interfaz Loopback (LO), como se observa en la Figura 16. (Molenaar, 2015)

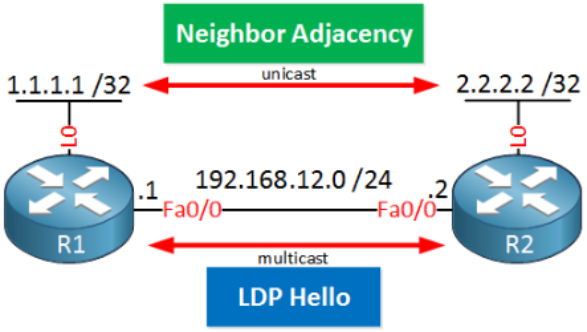

Figura 16. Adyacencia LDP utilizando la interfaz loopback.
Fuente: (Molenaar, 2015)

Cada prefijo excepto los BGP tiene asociada una etiqueta que se almacena en la base de información de enrutamiento (RIB). Los prefijos BGP se guardan en la base de datos de información de etiquetas (LIB). La base de datos LIB se usa para crear la base de información de reenvió de etiquetas (LFIB), como se observa en la Figura 17. La base de información LFIB es usada para tomar las decisiones de reenvió de etiquetas (Molenaar, 2015).

La información intercambiada en routers con adyacencia vecina LDP está presente en la base de datos LIB de cada router. Todos los prefijos conocidos por R1 asociados a una etiqueta serán conocidos por R2 y viceversa. Cada router que ejecute LDP conocerá el valor de la etiqueta al intercambiar un paquete MPLS. (Molenaar, 2015)

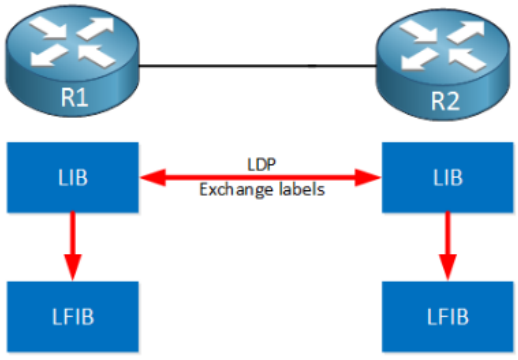

Figura 17. Adyacencia LDP utilizando la interfaz loopback.
Fuente: (Molenaar, 2015)

2.4.3. MPLS L3VPN

MPLS Virtual Private Networks o MPLS VPN provee escalabilidad, divide la red en pequeñas redes lo cual es útil en redes empresariales grandes, en donde la infraestructura de TI debe ofrecer redes aisladas a departamentos individuales (Ghein, 2007).

Una VPN es una red que emula una red privada sobre una infraestructura común, un ISP provee una infraestructura común para los clientes. VPN facilita la comunicación entre la capa 3 o 2 del modelo OSI. Una red privada requiere que todos los sitios de los clientes puedan interconectarse pero que las VPN estén totalmente separadas, sin embargo, de ser necesario diferentes VPN pueden interconectarse si se desea. MPLS VPN se ejecuta en el backbone y facilita la separación del plano de control y el plano de datos, esta separación no existe a nivel de IP. Los routers PE son los únicos que ejecutan VPN MPLS, como se observa en la Figura 18 (Ghein, 2007).

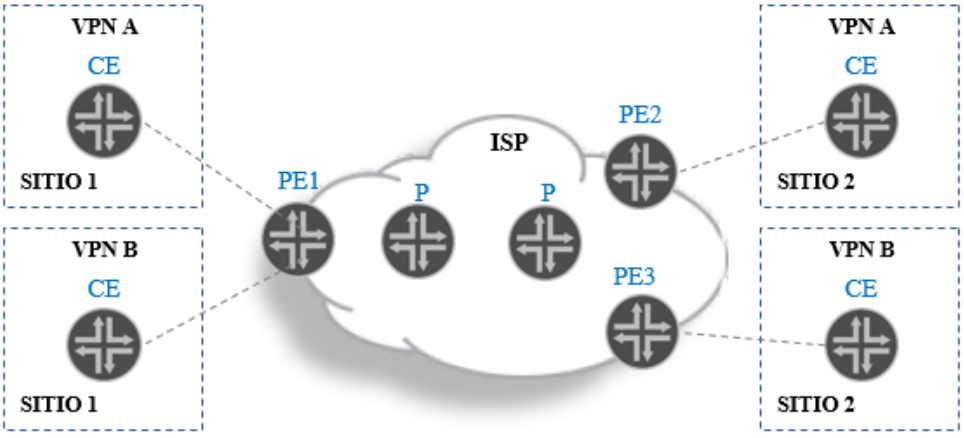

Figura 18. Service Provider corriendo MPLS VPN
Fuente: (Ghein, 2007)

Los routers en cada VPN tienen su propio esquema de direccionamiento, los equipos de distintas VPN pueden tener el mismo direccionamiento IP, sin embargo, es necesario usar route distinguisher y route targets que permitan que todos los prefijos aprendidos sean únicos (Ghein, 2007).

2.4.3.1. Virtual routing forwarding (VRF)

De acuerdo con Ghein (2007), un enrutamiento/reenvió virtual (VRF) es una instancia de reenvió y enrutamiento VPN. Cada router PE tiene una instancia VRF para cada VPN, como se observa en la Figura 19. PE1 tienen la tabla de enrutamiento IP global y también tablas de enrutamiento VRF una para cada VPN.

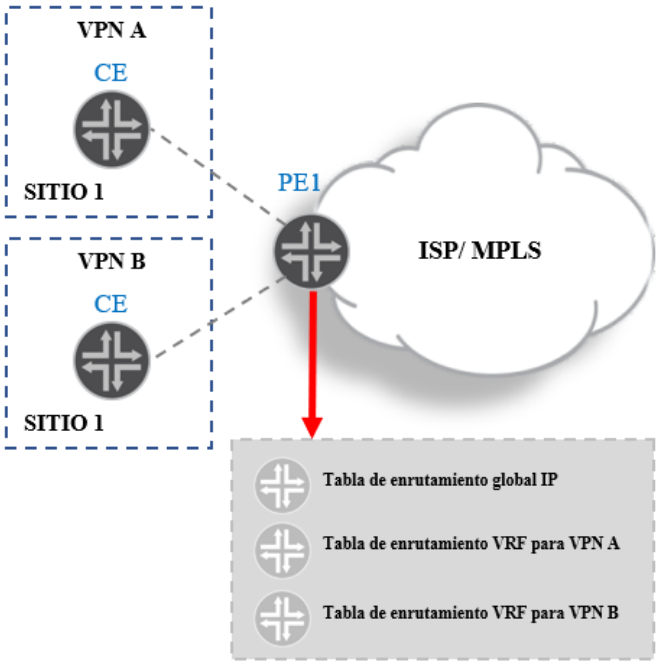

Figura 19. VRFs en un router PE
Fuente: *(Ghein, 2007)*

Existe una tabla de enrutamiento VRF para cada VPN, de esta manera el enrutamiento para cada cliente (VPN) es privado y separado en el router PE. Todos los paquetes IP recibidos en la interfaz VRF se identifican inequívocamente como pertenecientes a ese VRF. Se puede asignar una o varias interfaces al mismo VRF (Ghein, 2007).

2.4.3.2. Multi protocolo BGP (MP-BGP)

Una extensión del protocolo BGP es MP-BGP. El protocolo BGP solo admite prefijos unicast IPV4, sin embargo, MP-BGP admire diferentes direcciones unicast y multicast para IPV4 e IPV6.

MP-BGP es usado en MPLS para intercambiar etiquetas VPN. Los routers bajo MP-BGP pueden usar direcciones IPV6 para formar una adyacencia vecina e intercambiar prefijos IPV4 o viceversa (Molenaar, 2015).

BGP en MPLS permite que los routers PE compartan información de las VRF. En caso de que dos clientes de diferentes VPN usen direcciones IP superpuestas, se hace necesario tener prefijos únicos debido a que cuando los PE intercambien información, el PE de final de ruta no tendrá idea de a qué cliente pertenece el prefijo, es aquí en donde se ve necesario usar un identificador de ruta llamado route distinguisher (Ghein, 2007).

2.4.3.3. Route distinguisher (RD)

Un route distinguisher es un identificador único para cada prefijo VRF, la combinación del RD y el prefijo IPv4 recibe el nombre de VPNv4. La información intercambiada mediante MP-BGP entre los router PE son estos prefijos vpnv4 (Ghein, 2007).

El campo route distinguisher es de 64 bits, como se observa en la Figura 20. RD admite dos formatos, uno basado en el número del sistema autónomo (ASN: NN) y otro basado en el número IP (IP-address: NN). NN es el número que el proveedor de servicios asigna de forma exclusiva al VRF. El route distinguer se usa para que las rutas VPN sean identificadas de manera única, se pueden diferenciar entre los prefijos de los clientes en caso de que las rutas IPV4 de un cliente y otro se superpongan (Molenaar, 2015).

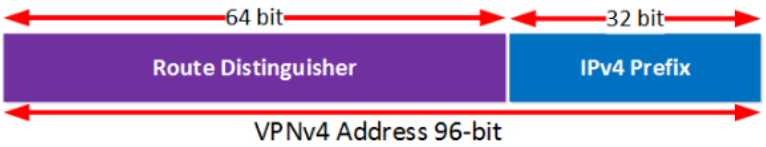

Figura 20. Formato de una ruta VPNv4
Fuente: (Molenaar, 2015)

2.4.3.4. Route target (RT)

Mediante route target se determina en que VRF se exportan o importan rutas VPNv4. Un RT es una comunidad extendida BGP. Un RT exportado denota que la ruta VPNv4 exportada recibe una comunidad extendida BGP, mientras que un RT importado denota que la ruta VPNv4 recibida de MP-BGP será colocada en la tabla de enrutamiento VRF, pero siempre después de una comprobación con una comunidad extendida coincidente, en caso de que no exista coincidencia se rechaza el prefijo (Molenaar, 2015).

Un RT usa el mismo formato y tiene el mismo campo de 64 bits que el RD (AS: NN), un RT se anuncia entre routers PE y usa un valor de comunidad extendida BGP que indica que RT se quiere exportar e importar para cada VRF. (Molenaar, 2015)

El proceso de exportación e importación de un RT llevado en una red MPLS se puede apreciar en la Figura 21.

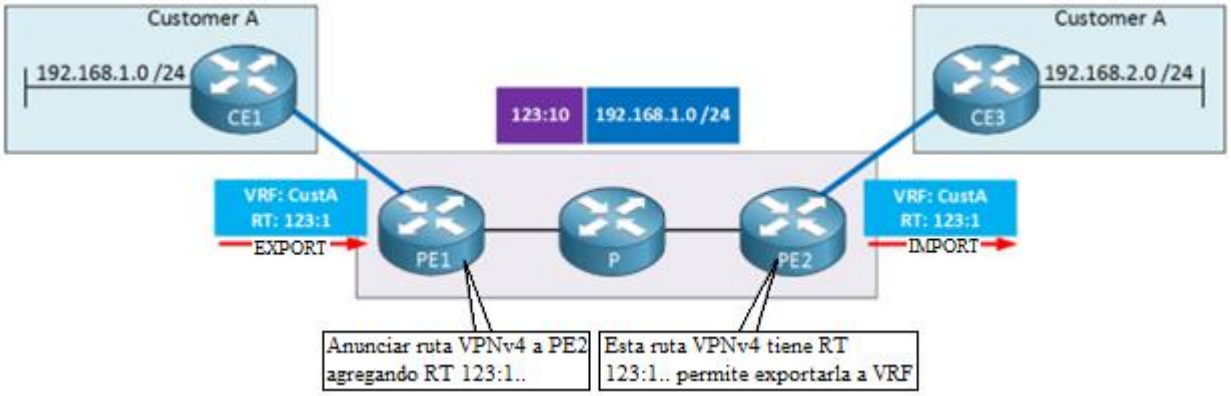

Figura 21. Exportación e importación de un RT
Fuente: (Molenaar, 2015)

El procedimiento para llevar un prefijo de CE1 a CE3, como se observa en la Figura 21 es el siguiente:

- La VRF configurada para el cliente A en PE1 y PE2 es llamada CustA.

- CE1 anuncia el prefijo 192.168.1.0/24 hacia PE1.
- PE1 recibe un prefijo del router CE1 y para crear una ruta VPNv4 única creando un RD (123:10).
- PE1 agrega un RT (123:1), PE1 está configurado para que a todas las rutas VPNv4 del VRF CustA se le agregue ese RT.
- PE1 informa de la ruta VPNv4 a PE2.
- PE2 exporta la ruta VPNv4 en la VRF CustA, PE2 está configurado para exportar todas las rutas que usen el RT (123:1) en la VRF CustA.
- PE2 redistribuye la ruta VPNv4 hacia CE3.
- CE3 aprende el prefijo 192.168.1.0/24 que anuncio CE1.

Un RT permite controlar las rutas VPNv4 para que mediante la importación y exportación de ciertos RT, el uso de RT permite también añadir más clientes o dar acceso a clientes en otras redes con mayor facilidad (Molenaar, 2015).

2.4.4. Seamless MPLS

Seamless MPLS es la arquitectura de red en donde el transporte de los servicios se extiende a una ruta conmutada de etiqueta de extremo a extremo (E2E) a través de las diferentes etapas del IP-RAN esto impacta directamente en las funcionalidades y escalabilidad disponibles para cada servicio. Todos los servicios se encapsulan en MPLS transmitiéndose a lo largo del E2E a través de las etapas de low RAN, mid RAN y high RAN (Huawei, 2019).

Seamless MPLS utiliza protocolos confiables como BGP, IGP y MPLS para establecer un E2E LSP entre las tres etapas del IP-RAN de esta manera simplifica el aprovisionando, el mantenimiento y las operaciones de la red debido a que los servicios se encapsulan y transmiten a

lo largo de un E2E LSP, para desplegar servicios se puede establecer un LSP entre dos nodos garantizando una alta flexibilidad de escalabilidad e implementación (Huawei, 2019).

2.4.4.1. Network Region

Es el conjunto de nodos o dispositivos bajo un mismo dominio IGP, el uso de regiones o etapas dentro de una red es un concepto importante en la arquitectura seamless MPLS, esta segmentación se destina a solventar problemas inherentes a redes planas que no tienen jerarquía lógica (Huawei, 2019).

Segmentar la red en etapas reduce el número de LSP o LDP en la red, con ello el número de entradas en las tablas de enrutamiento RIB y FIB se ve disminuido, mejorando la convergencia y simplificando el throubleshooting ya que los problemas no se propagan en la red, estos se aíslan a una sola región. El crecimiento de la red también se ve simplificada debido a que la integración de nuevas regiones no requiere compatibilidad de IGP/LDP entre regiones, simplemente se necesita compatibilidad a nivel de BGP-LU, protocolo que posibilita el enrutamiento E2E (Huawei, 2019).

2.4.4.2. BGP-LU

BGP label unicast o BGP LU es una característica que posibilita distribuir una etiqueta MPLS en el mismo mensaje de actualización BGP usado para distribuir rutas. Las etiquetas son asignadas por el LSR y se identifican por el valor del atributo next hop de la ruta (Rosen, 2001).

Se usa BGP LU en redes que usen múltiples regiones. Un equipo que hable BGP usa BGP-LU para adjuntar una etiqueta MPLS a un prefijo IGP anunciado y distribuir la etiqueta MPLS a sus pares. BGP-LU proporciona conectividad entre regiones mejorando la capacidad de escalabilidad y tiempos de convergencia debido a que las fallas en una región se aíslan en la misma y las tablas de reenvió son más pequeñas (Noction, 2018).

CAPÍTULO III

3. METODOLOGÍA

3.1. Análisis del servicio móvil avanzado en el Ecuador.

3.1.1. Líneas activas por tecnología

Existe un total de 15.968.846 líneas activas. Las líneas activas constituyen servicios de tecnologías como: GSM, UMTS, HSPA+ y LTE. Tecnologías que se encuentran desplegadas por tres diferentes prestadoras, la cantidad de clientes por prestadora es el siguiente: CONECEL S.A. (CLARO) 8.355.627 usuarios, OTECEL S.A. (MOVISTAR Y TUENTI) 4.540.063 usuarios y CNT EP 3.073.156 usuarios. (ARCOTEL, 2019)

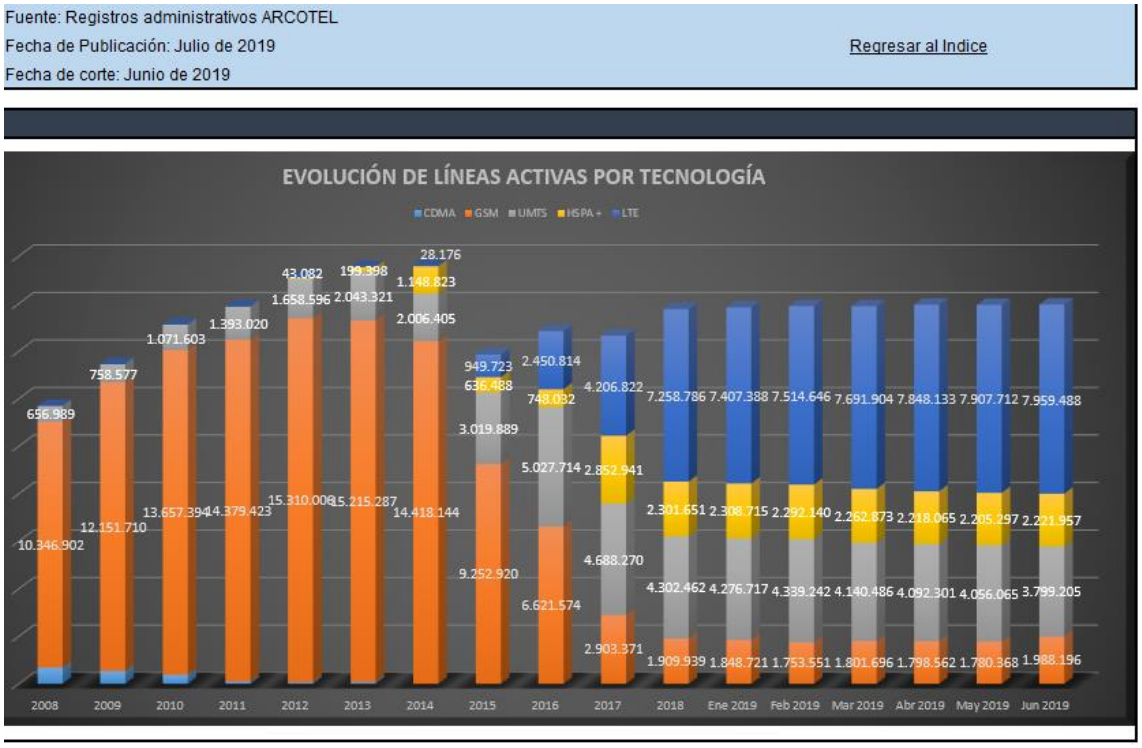

Figura 22. Cantidad de líneas activas por tecnología
Fuente: *(ARCOTEL, 2019)*

En el año 2014 la mayor cantidad de líneas activas correspondían exclusivamente al servicio de voz, sin embargo, para el 2019 la mayoría de las líneas pertenecen a líneas de voz y datos, se

evidencia que actualmente LTE es la tecnología con mayores líneas activas ocupando un 49,84% de las líneas activas por tecnología. (ARCOTEL, 2019).

3.1.2. Densidad y participación de mercado

La densidad nacional de líneas activas y la participación de mercado para el servicio móvil avanzado para el mes de junio del 2019 se presentan en la Tabla 3 y Figura 23 respectivamente (ARCOTEL, 2019).

Tabla 3
Densidad nacional de líneas activas

Mes/Año	Líneas Activas	Población Nacional	Densidad Nacional de Líneas Activas
Junio 2019	15.968.846	17.145.697	93,14%

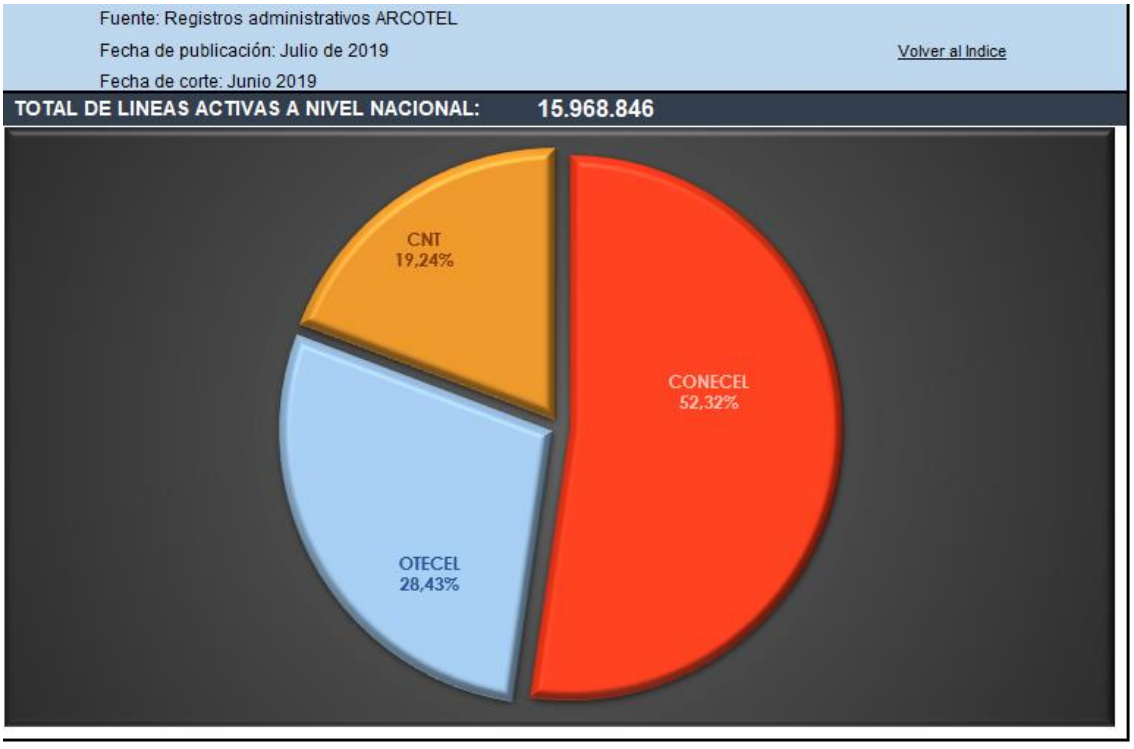

Figura 23. Participación de mercado, servicio móvil avanzado
Fuente: *(ARCOTEL, 2019)*

De acuerdo con los datos publicados por ARCOTEL en el Ecuador el 52,5% de habitantes usan el servicio de voz y datos esto equivale a un total de 9.000.411 de abonados al servicio de voz y datos.

3.1.3. Cobertura de servicio móvil avanzado

Para prestar el servicio móvil avanzado se ha desplegado para junio del 2019 un total de 17.142 Radio bases (RBS) para las diferentes tecnologías 2G (CDMA, GSM), 3G (UMTS) y 4G (LTE) de las cuales el 54,86% corresponden al operador CONECEL S.A., el 29,44% OTECEL S.A. y el 15,69% CNT E.P. (ARCOTEL, 2019).

El despliegue de la tecnología LTE ya se encuentra disponible en varias provincias del país sin embargo en algunas aún se encuentra en fase de implementación, la Figura 24 presenta el número total de radio bases por tecnología y proveedor a nivel nacional (ARCOTEL, 2019).

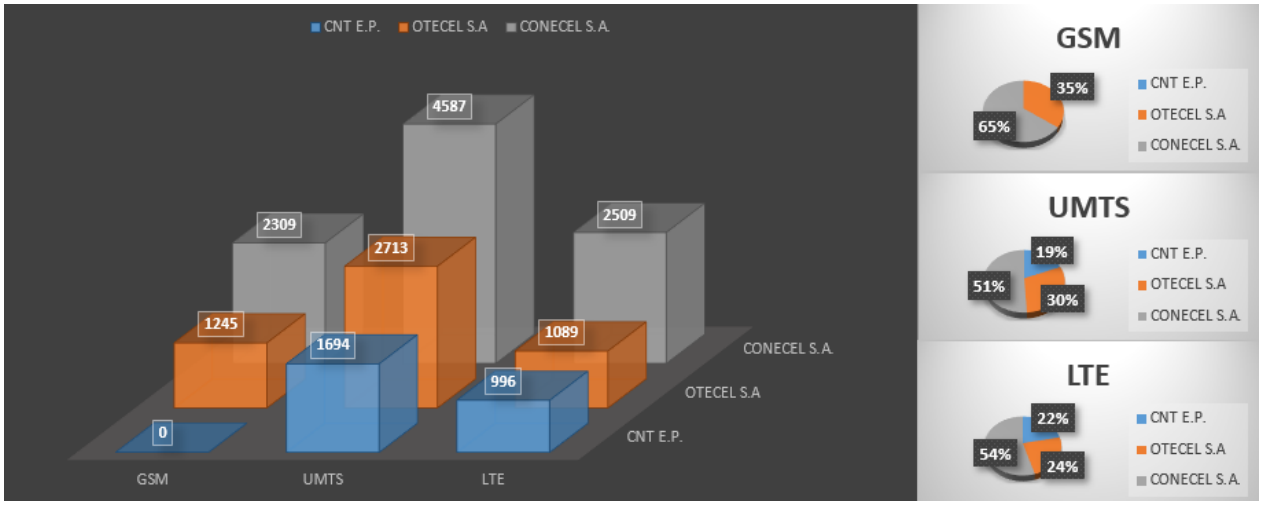

Figura 24. Cantidad de Radio bases por tecnología y proveedor en el Ecuador.

3.2. Análisis del servicio móvil avanzado en la ciudad de Cuenca

3.2.1. Datos generales de la ciudad de Cuenca

Cuenca, oficialmente Santa Ana de los Ríos de Cuenca es una ciudad ecuatoriana, capital de la provincia de Azuay tiene una proyección poblacional para el año 2019 de 625.775 habitantes, lo cual la convierte en la tercera ciudad más poblada del país después de Quito y Guayaquil (INEC, 2019).

Figura 25. Ubicación geográfica de Cuenca.

3.2.2. Cobertura de servicio móvil avanzado en la ciudad de Cuenca

El servicio móvil avanzado para la ciudad de Cuenca cuenta para junio del 2019 con un total de 607 RBS para las diferentes tecnologías 2G, 3G y 4G de las cuales el 43,49% corresponden al operador CONECEL S.A., el 42% OTECEL S.A. y el 14,49% CNT E.P. (ARCOTEL, 2019).

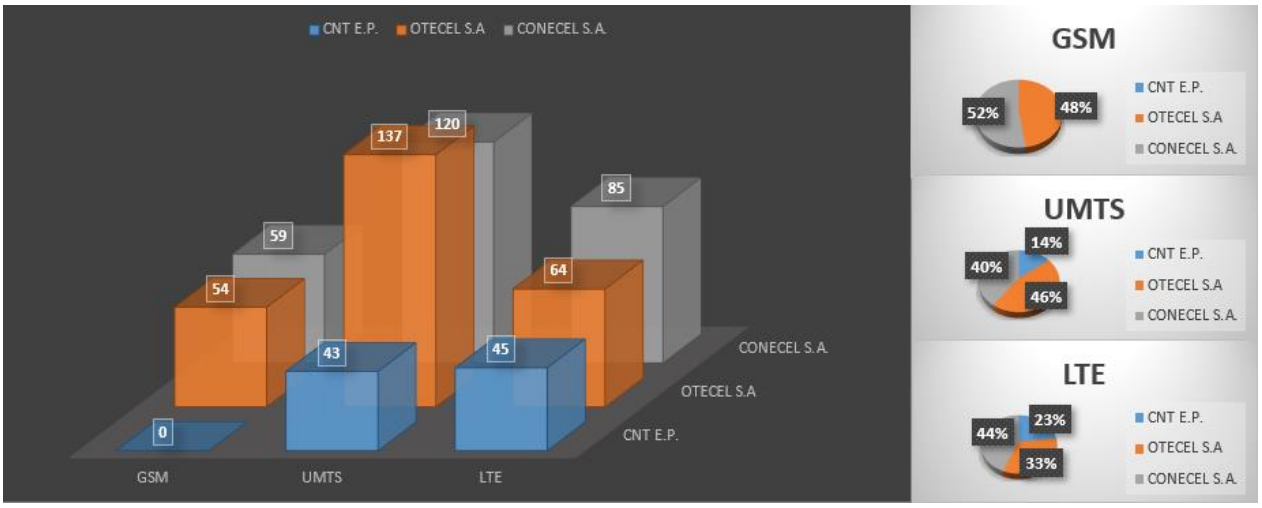

Figura 26. Cantidad de Radio bases por tecnología y proveedor en Cuenca.

El número total de radio bases con tecnología LTE entre las tres operadoras en la ciudad de Cuenca es de 194 lo cual representa apenas un 11,99% las radio bases LTE existentes en Quito, considerando que Cuenca es la tercera ciudad más poblada del Ecuador se estima que el número de radio bases para LTE se duplique en los próximos años. (ARCOTEL, 2019).

La Figura 26 evidencia una necesidad de desplegar infraestructura LTE, en el caso de los operadores CONECEL S.A. y OTECEL S.A el estado actual respecto a infraestructura 3G en uno de los casos duplica a la infraestructura 4G, esto impacta directamente en la calidad de servicio que perciben los usuarios, experimentando latencias altas y bajas tasas de velocidad.

Centrándose en la cantidad de radio bases LTE se evidencia el proveedor CNT E.P. es el que menos radio bases posee, resulta trascendental que, en los próximos años debida a la creciente demanda de acceso a datos, CNT E.P. logre atender la demanda de esta tecnología en la ciudad de Cuenca. En las siguientes secciones se presenta un dimensionamiento que permita a las redes de transporte (backhaul) actuales cubrir las expectativas de tráfico que se puedan generar los usuarios para el año 2023. (ARCOTEL, 2019).

3.3. Proyección del tráfico LTE para el año 2023

La cantidad de usuarios que acceden al servicio LTE tiene un crecimiento exponencial, desde el año 2015 a junio 2019 la cantidad de usuarios ha crecido en un 738%, el número de suscriptores es siete veces mayor, en la Figura 27 se presenta el número de usuarios proyectados para el año 2023 *(ARCOTEL, 2019).*

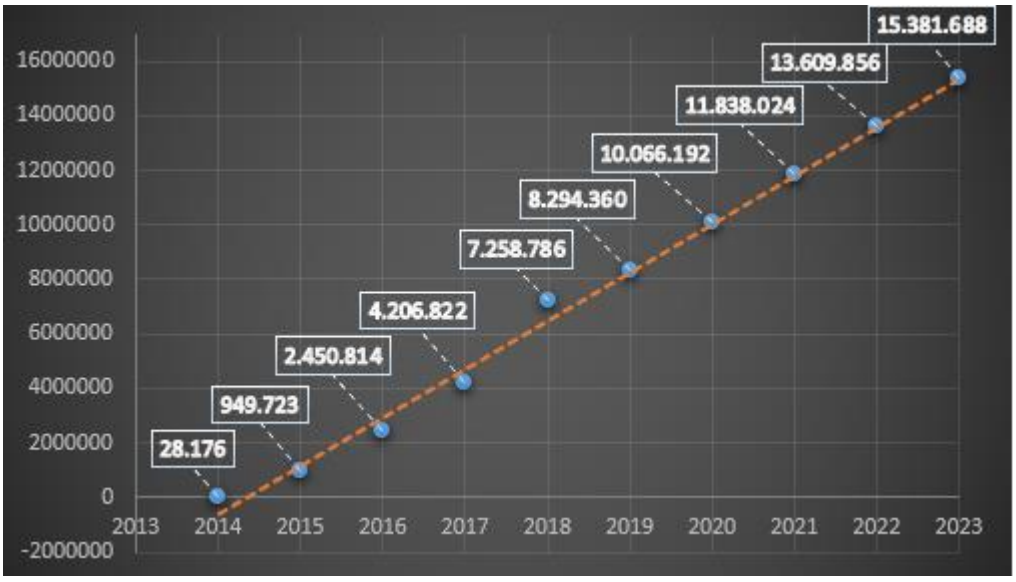

Figura 27. Proyección de usuarios LTE en Ecuador a 2023.

3.3.1. Número de usuarios LTE en la ciudad de Cuenca

Mediante la Ecuación 1 se conocerá el throughput total que deben soportar los equipos de borde dentro de cuatro años, para lo cual se necesita conocer la cantidad de usuarios LTE en la Ciudad de Cuenca y el throughput actual, los datos requeridos para el cálculo de la cantidad de usuarios LTE para el año 2023 son presentados en la Tabla 4, mismos que fueron descritos en la sección 3.1 y 3.2.

Tabla 4
Parámetros a considerar para calcular la cantidad de usuarios LTE en el 2023.

H: Cantidad de Habitantes en Cuenca	625 775
A: Porcentaje de abonados de voz y datos	52,5%
L: Porcentaje de usuarios LTE	49,84%
P: Porcentaje de participación en el mercado del operador	19,24%

$$N_{2019} = H \times A \times L \times P \quad (1)$$

$$N_{2019} = 625\,775 \times 0{,}525 \times 0{,}4984 \times 0{,}1924$$

$$N_{2019} = 31\,504\ usuarios\ LTE$$

Asumiendo que todos los usuarios se encuentran en ambientes urbanos con la Ecuación 2 se encuentra el número de usuarios LTE dentro de 4 años, para lo cual es necesario el factor de crecimiento de usuarios, de acuerdo con la Figura 27 el factor de crecimiento estimado es del 85,45% del 2019 al 2023.

$$N_n = N_0(1 + gf)^n \quad (2)$$

Donde:

- N_n: Cantidad de usuarios LTE proyectados
- N_0: Cantidad de usuarios LTE actuales
- gf: Factor de crecimiento
- n: Años de proyección

$$N_{2023} = 31\,504\,(1 + 0{,}8545)^4$$

$$N_{2023} = 372\,626\ usuarios\ LTE$$

3.3.2. Throughput LTE real en la ciudad de Cuenca equipo de borde.

La capacidad de tráfico manejado por un equipo de borde en la ciudad de Cuenca se ilustra en la Figura 28, el throughput real en el equipo de borde de Cuenca corresponde al mes de junio del 2019, se destaca que el pico más alto para tráfico LTE desde el equipo de borde hacia los clientes (downlink) es 5.88 [Gbps] y del equipo de borde hacia el core (uplink) es 999,23 [Mbps].

Figura 28. Throughput real en el equipo de borde para usuarios LTE en Cuenca, junio 2019.

Al throughput total de usuarios LTE se recomienda añadir un 25% de utilización para procesos de sincronización, señalización y control (Castillo, 2017). Los nuevos valores de throughput se presentan en la Tabla 5.

Tabla 5
Throughput LTE equipo borde de Cuenca.

Throughput downlink	7,35 [Gbps]
Throughput uplink	1, 25 [Gbps]

El factor de crecimiento obtenido de la proyección de usuarios en la Figura 27 es de 85,45% desde junio de 2019 hasta el 2023. Usando la Ecuación 3 se obtiene el throughput LTE para el año 2023.

$$T_p = T_a\ (1 + gf)^n \quad (3)$$

Donde:

- T_p: Throughput proyectado
- T_a: Throughput actual
- gf: Factor de crecimiento
- n: Años de proyección

DOWNLINK:

$$T_{p_{downlink}} = T_a\ (1 + gf)^n$$

$$T_{p_{downlink}} = 7{,}35\ (1 + 0{,}8545)^4$$

$$T_{p_{downlink}} = 86{,}94\ [Gbps]$$

UPLINK:

$$T_{p_{uplink}} = 0{,}99\ (1 + 0{,}8545)^4$$

$$T_{p_{uplink}} = 14{,}77\ [Gbps]$$

Considerando que el equipo debe garantizar la misma capacidad tanto para el tráfico de entrada como para el de salida, el router deberá manejar una capacidad de dos veces el throughput máximo proyectado, así se garantiza que no exista pérdida de paquetes en caso de trabajar a capacidad completa, este valor es 173,87 [Gbps].

Se debe considerar un 20% de sobredimensionamiento para garantizar que el equipo también tenga vida útil sobre los cuatro años proyectados, con ello el router deberá tener al menos una capacidad de 208,64 [Gbps], como se observa en la Figura 29.

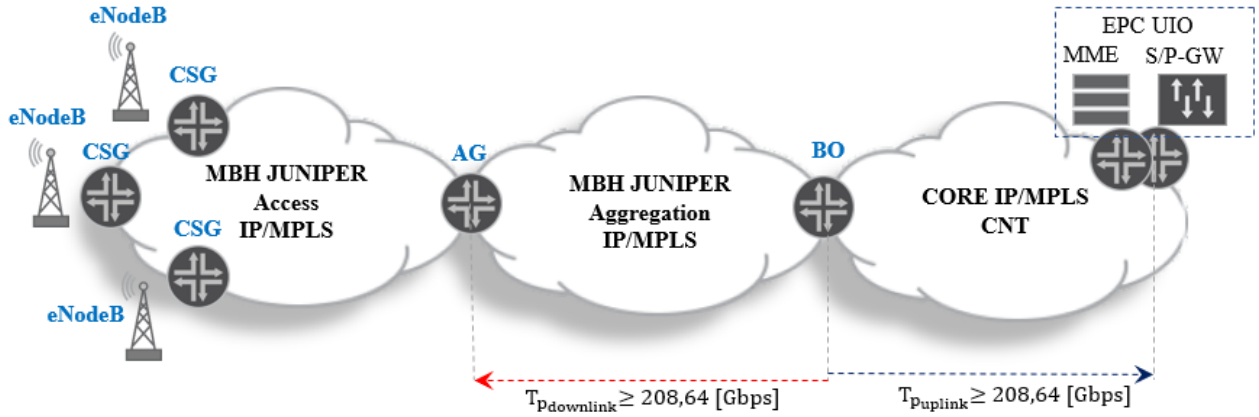

Figura 29. Throughput LTE proyectado a 2023 equipo de borde en la Red Nacional IP/MPLS.

3.3.3. Throughput LTE real en la ciudad de Cuenca equipo de acceso.

La capacidad de tráfico manejado por un equipo de acceso en la ciudad de Cuenca se ilustra en la Figura 30, el throughput real en el equipo de acceso de Cuenca corresponde al mes de junio del 2019, se destaca que el pico más alto para tráfico LTE desde el equipo de borde hacia el equipo acceso (downlink) es 34,91 [Mbps] y del equipo de acceso hacia el borde (uplink) es 7,64 [Mbps].

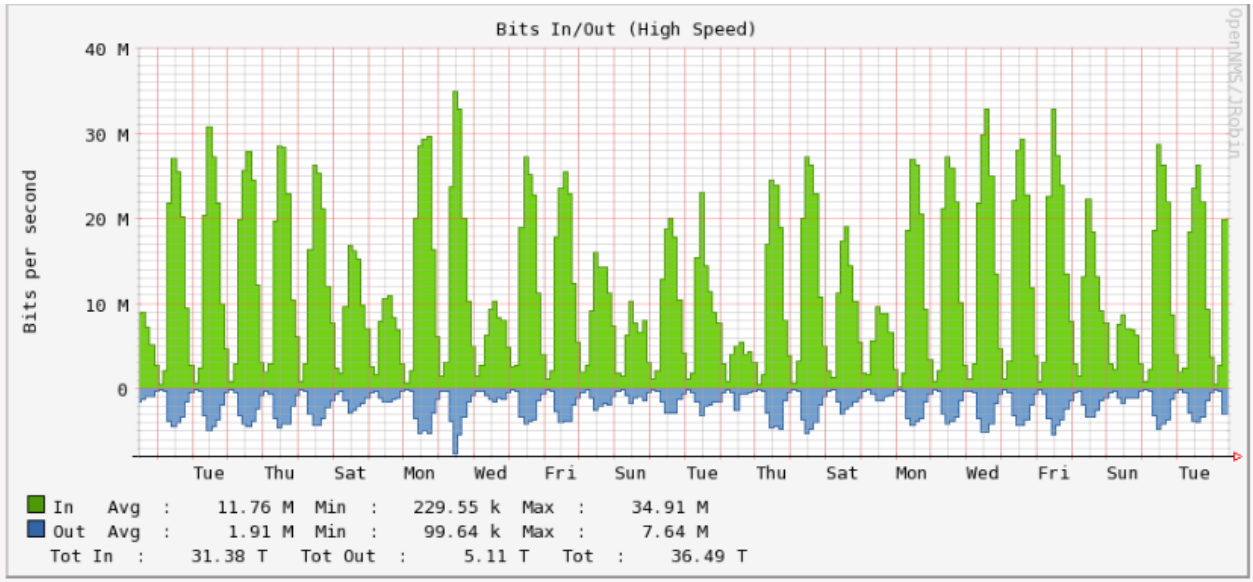

Figura 30. Throughput real en el equipo de acceso para usuarios LTE en Cuenca, junio 2019.

Al igual que para el equipo de borde al throughput total en este caso para el equipo de acceso se recomienda añadir un 25% de utilización para procesos de sincronización, señalización y control (Castillo, 2017). Los nuevos valores de throughput se presentan en la Tabla 6.

Tabla 6
Throughput LTE equipo de acceso en Cuenca.

Throughput downlink	43,63 [Mbps]
Throughput uplink	9,55 [Mbps]

Como se observa en la Tabla 5 y Tabla 6 el throughput de downlink es mayor, esto debido a que los suscriptores o el UE tienen mayores cantidades de descargas que de cargas. Se calcula el throughput de uplink y downlink usando la ecuación (3).

DOWNLINK:

$$T_{p_{downlink}} = T_a\,(1+gf)^n$$

$$T_{p_{downlink}} = 43{,}63\,(1+0{,}8545)^4$$

$$T_{p_{downlink}} = 516{,}14\,[Mbps]$$

UPLINK:

$$T_{p_{uplink}} = 9{,}55\ (1 + 0{,}8545)^4$$

$$T_{p_{uplink}} = 112{,}95\ [Mbps]$$

Considerando que el equipo debe garantizar la misma capacidad tanto para el tráfico de entrada como para el de salida, el router deberá tener una capacidad de al menos dos veces el throughput de downlink es decir al menos 1,03 [Gbps] para que no exista una pérdida de paquetes en caso de trabajar a capacidad completa. Los equipos de acceso comerciales manejan un throughput mínimo de 60 [Gbps] full duplex, su función no va ligada directamente a las capacidades de throughput que estos pueden manejar como si lo hacen los equipos de borde, si no, al uso de seamless MPLS en la capa de acceso.

3.4. Equipamiento

El constante desarrollo de nuevas tecnologías y/o aplicaciones, la demanda cada vez mayor de acceso a internet y la inminente evolución a la nueva era del internet de las cosas (IoT) requiere que los proveedores de servicios estén en constante evolución y a la vanguardia con arquitecturas y dispositivos de red de nueva generación que permitan desplegar nuevas características, aplicaciones y servicios de manera eficiente maximizando los objetivos de negocio.

El diseño respecto al equipamiento contempla routers de acceso, agregación y borde para la red IP-RAN, con el objetivo de superar y satisfacer los requerimientos de equipamiento de última generación se propone definir como parte de la arquitectura de red IP RAN los equipos presentados en la Tabla 7, los cuales son dispositivos de nueva generación y alto desempeño.

Tabla 7
Equipamiento red IP-RAN

Capa red IP-RAN	Juniper Networks
Acceso	Juniper ACX2200
Agregación	Juniper MX104
Borde	Juniper MX480

3.4.1. Juniper MX480 (BO)

El equipo Juniper MX480 es un dispositivo de alto desempeño, confiabilidad y escalabilidad ideal para implementaciones a gran escala en proveedores de servicio y data centers, ya que soporta una gran cantidad de interfaces de 10G, 40G y 100G.

El dispositivo Juniper MX480 es ideal para implementaciones que requieren estabilidad, alto desempeño y un comportamiento previsible en caso de fallas ya que tiene una arquitectura modular y redundante en cada uno de sus componentes como se describe en la Tabla 8.

Tabla 8
Características equipo Juniper MX480

Especificaciones	Juniper MX480
Capacidad máxima de conmutación del sistema (Full duplex)	2,88 [Tbps]
Unidades de rack (RU)	8
Slots fijos para linecards	6
Puertos 1GE (Max)	240
Puertos 10GE (Max)	240
Puertos 40GE (Max)	72

CONTINÚA

Puertos 100GE (Max)	24
Redundancia del sistema	Routing Engine (2) Fabric (2) Power (2) Fan (2)

De acuerdo con los cálculos realizados para el equipo de borde, el dispositivo MX480 debería garantizar una capacidad de reenvió full duplex de al menos 416 [Gbps], como se observa en la Figura 29. Se considerarán usar dos linecards MPC3E-3D-NG, cada linecard garantiza al menos 200 [Gbps] por slot, como se observa en la Figura 31.

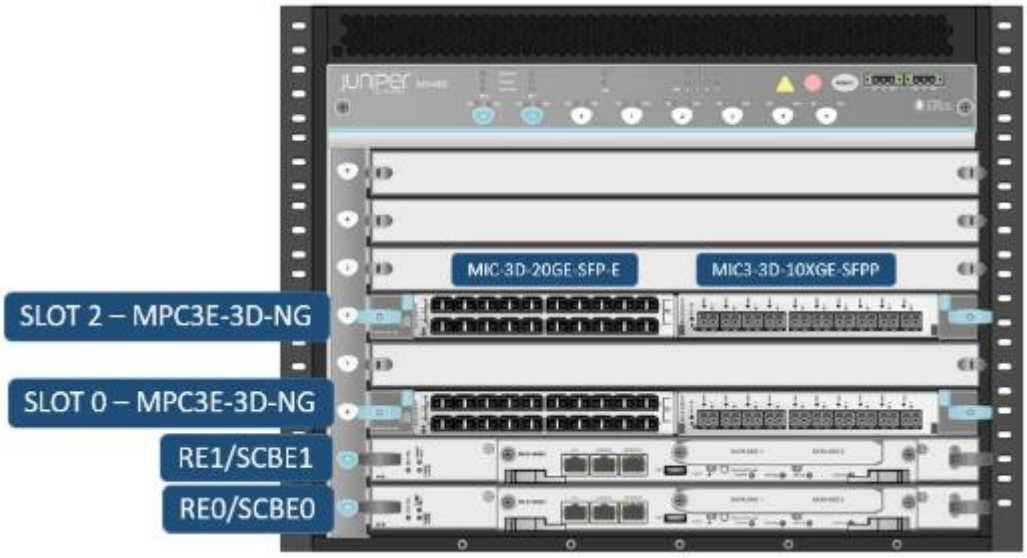

Figura 31. Linecards consideradas en Juniper MX480

Cada linecard tiene dos mics, estas garantizan 480 [Gbps] de capacidad de reenvió full duplex. Las mics usadas para el diseño son:

- **MIC-3D-20GE-SFP-E:** Permite usar en su tarjeta 20 SFP (small form-factor pluggable transceptor) ópticos o eléctricos de capacidad de 1 [Gb] cada uno.

- **MIC-3D-10XGE-SFPP:** Permite usar en su tarjeta 10 SFP ópticos de capacidad de 10 [Gb] cada uno.

3.4.1.1. Routing engine (RE)

El dispositivo Juniper MX480 cuenta con dos slots en su chasis para instalar tarjetas del tipo Routing Engine para implementaciones en alta disponibilidad. Esta tarjeta es la encargada de administrar todos los procesos de software relacionados a los protocolos de enrutamiento (Control Plane), administración de los componentes del chasis y el acceso de usuarios.

3.4.1.2. Switch control board (SCBE2)

El Switch Fabric del sistema está integrado directamente en esta tarjeta, como se ilustra en la cual es la encargada de proveer una arquitectura Non-Blocking que permite conectar todos los componentes dentro del chasis para el envío de tráfico. El dispositivo Juniper MX480 tiene una arquitectura modular que le permiten garantizar una capacidad de procesamiento de 480Gbps en un esquema de redundancia 2+0 (es decir con las dos SCBE2 activas a la vez).

Figura 32. Switch Control Board (SCBE2) - Juniper MX480

Adicionalmente esta tarjeta es la encargada de administrar todas las funciones inherentes al chasis como monitorear, controlar, sincronizar, resetear o apagar todos los componentes del sistema como son las tarjetas, los Fans, la distribución de energía.

3.4.1.3. Power system

El dispositivo Juniper MX480 puede funcionar con fuentes de poder con entrada AC o DC, tiene una arquitectura de zonas para la distribución de energía compuesta por un máximo de 4 fuentes, cada fuente tiene una función específica en cuanto al componente a energizar como se describe en la Tabla 9.

Tabla 9
Zonas de energía – Juniper MX480

Chasis	Zona	Power supply (PEM)	Componentes que reciben energía
MX480 AC/DC	Zona 0	PEM 0 o PEM 2	Fan MPC slots 0 y 1 SCB/RE slots 0 y 1
	Zona 1	PEM 1 o PEM 3	Fan MPC slots 2 al 5

Por esta razón para proveer full capacidad al sistema se requiere de dos fuentes poder y para entregar full capacidad con un esquema de redundancia de 2+2 se requiere cuatro fuentes de poder. Las fuentes de poder se conectan directamente al Midplanle del dispositivo para distribuir energía a cada uno de los componentes, además son módulos que se remueven e insertan en caliente, cada fuente cuenta con su propio sistema de enfriamiento interno. La Figura 33 describe la ubicación de las fuentes de poder DC del dispositivo:

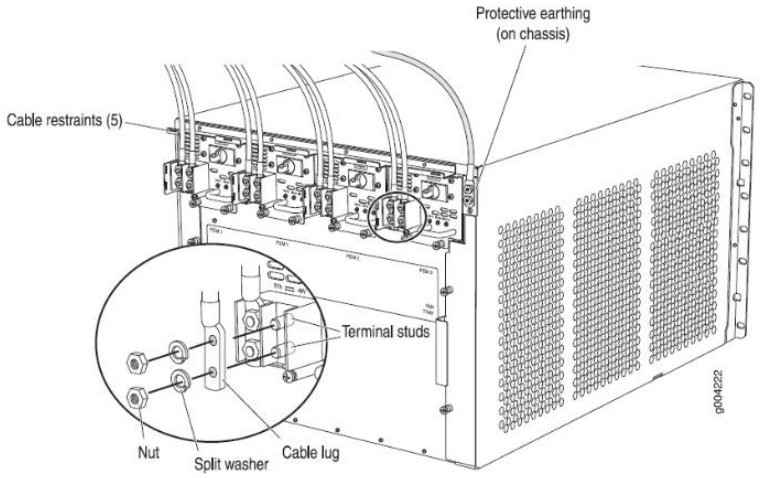

Figura 33. Power System DC - Juniper MX480

3.4.1.4. Cooling system

El sistema de enfriamiento del dispositivo Juniper MX480 consiste de un Fan Tray de 6 ventiladores y un filtro de aire ubicados en la parte lateral del dispositivo como se describe en la Figura 34, las cuales trabajan en conjunto para mantener todos los componentes del chasis dentro de los rangos de temperatura aceptables de operación.

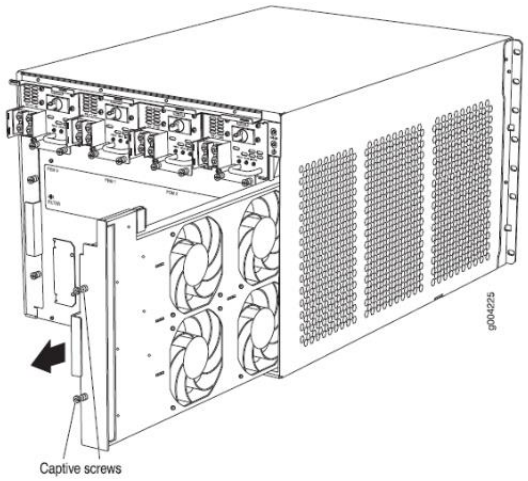

Figura 34. Bandeja de ventilador - Juniper MX480

El sistema de administración del dispositivo monitorea la temperatura de cada uno de los componentes del chasis, cuando el dispositivo opera normalmente los ventiladores trabajan a la

mitad de su capacidad y en caso de falla de unos de los ventiladores el sistema incrementa la velocidad de los otros ventiladores garantizando los suficientes niveles de enfriamiento para el dispositivo, el dispositivo Juniper MX480 puede operar normalmente con temperaturas en el rango de 0° a 40° C.

Adicionalmente el dispositivo tiene una entrada de aire localizada en la parte lateral del dispositivo, por donde el aire del sistema de enfriamiento del Data Center es empujado hacia cada uno de los componentes del chasis como se ilustra en la Figura 35.

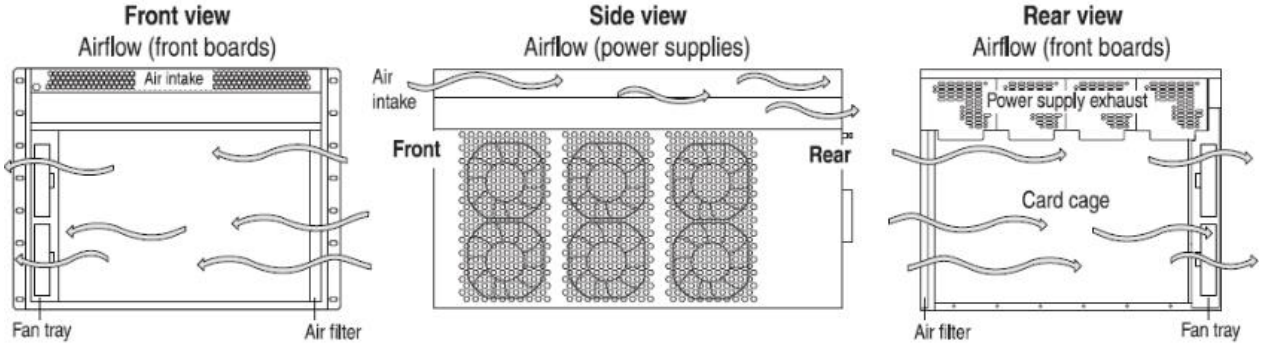

Figura 35. Flujo de aire - Juniper MX480

3.4.2. Juniper MX104 (AG)

Es un dispositivo modular, altamente redundante, de alto desempeño, confiabilidad y escalabilidad, el modelo Juniper MX104 se ilustra en la Figura 36.

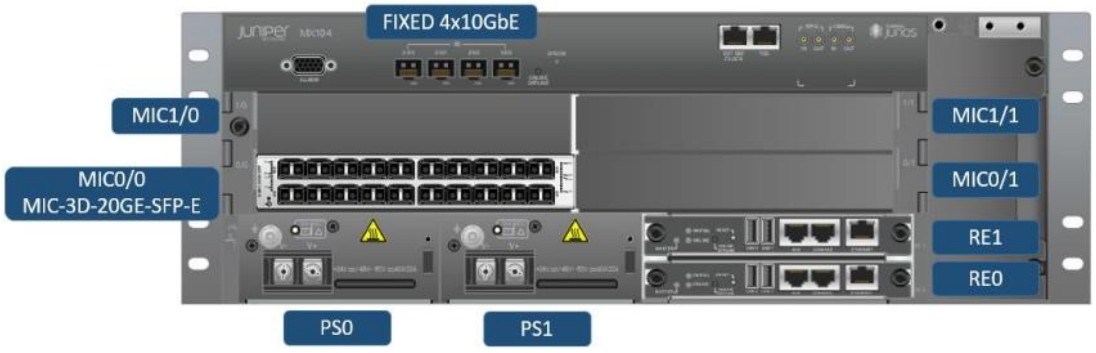

Figura 36. Juniper MX104

Este, comparte las mismas características avanzadas de Routing/Switching/Security que están disponibles en el resto de las plataformas de la serie MX, incluyendo el soporte de una gran variedad de servicios de L2VPN, L3VPN. La Tabla 10 describe las principales características de este dispositivo.

Tabla 10
Características equipo Juniper MX104

Especificaciones	**Juniper MX104**
Capacidad máxima de conmutación del sistema (Full duplex)	80 [Gbps]
Unidades de rack (RU)	3.5
Slots fijos para linecards	4 ranuras fijas de 10GbE + 4 MIC
Puertos 1GE (Max)	80
Puertos 10GE (Max)	8
Redundancia del sistema	Routing Engine (2) Power (2) Fan (2)

3.4.2.1. Power system

El dispositivo Juniper MX104 puede funcionar con dos fuentes de poder con entrada AC o DC. Las fuentes de poder están localizadas en la parte frontal del chasis como se describe en la Figura 36 y ofrecen un esquema de redundancia 1+1.

Cuando ambas fuentes de poder están presentes, ellas comparten la energía que brindan al chasis casi equitativamente. Si una fuente de poder en una configuración redundante falla o es removida, la otra fuente tiene la capacidad de asumir toda la carga eléctrica del chasis sin afectación alguna.

3.4.2.2. Cooling system

El sistema de enfriamiento del dispositivo Juniper MX104 consiste en un Fan Tray de 5 ventiladores y un filtro de aire que se encuentran en la parte lateral del dispositivo como se describe en la Figura 37.

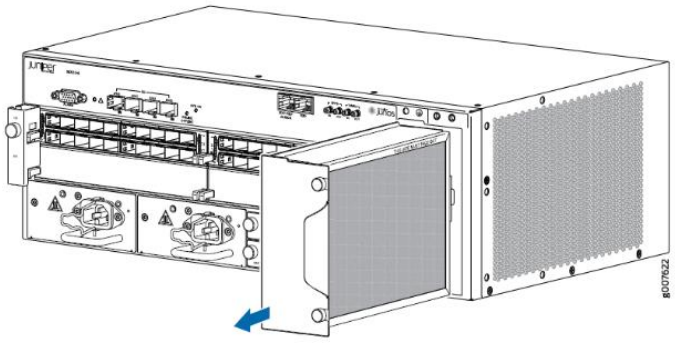

Figura 37. Bandeja de ventilador y filtro de aire - Juniper MX104

El sistema de administración del dispositivo monitorea la temperatura de cada uno de los componentes del chasis, cuando el dispositivo opera normalmente los ventiladores trabajan a la mitad de su capacidad y en caso de falla de unos de los ventiladores el sistema incrementa la velocidad de los otros ventiladores garantizando los suficientes niveles de enfriamiento para el dispositivo, el dispositivo Juniper MX104 puede operar normalmente con temperaturas en el rango de -40° a 65° C.

Adicionalmente el dispositivo cuenta con una entrada de aire para enfriar el chasis, está se encuentra localizada en la parte lateral derecha del dispositivo a lado del filtro de aire, la Figura 38 describe el flujo de aire de este dispositivo.

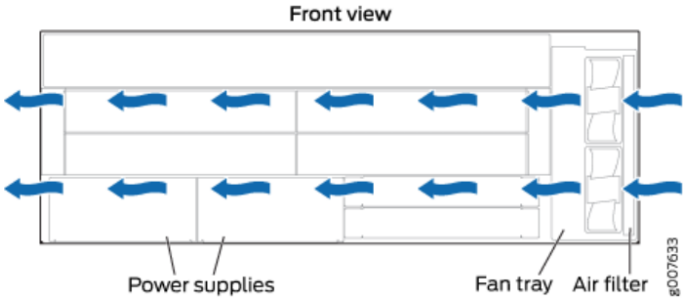

Figura 38. Flujo de aire - Juniper MX104

3.4.3. Juniper ACX-2200 (CSG)

Es un dispositivo de alto desempeño, confiabilidad y escalabilidad, ideal para la implementación de redes de acceso y agregación de soluciones de Mobile Backhaul 2G/3G/4G así como para la implementación de servicios Carrier Ethernet para empresas y acceso residencial, el equipo se ilustra en la Figura 39.

Figura 39. Juniper ACX2200

La Tabla 11 describe las principales características de este dispositivo:

Tabla 11
Características Juniper ACX2200

Especificaciones	**Juniper ACX2200**
Capacidad máxima de conmutación del sistema (Full duplex)	60 [Gbps]
Unidades de rack (RU)	1
Slots fijos para linecards	4xGbE de Cobre 4xGbE Combo (Cobre/Fibra) 2xGbE SFP 2x10GbE SFP+

El dispositivo Juniper ACX2200 es un Single-Board que garantiza Line Rate Full-Duplex en todos sus puertos, el cual cuenta con una RE encargada de brindar servicios de enrutamiento L3 y gestión de la red.

3.4.3.1. Power system

El dispositivo Juniper ACX2200 puede funcionar con dos fuentes de poder con entrada AC o DC. Las fuentes de poder están embebidas en el panel frontal izquierdo del chasis como se ilustra en la Figura 39. Cuando el dispositivo está operando normalmente y ambas fuentes de poder están encendidas, ocurre un balanceo de carga automáticamente entre ellas. Cuando una fuente falla o en su defecto es desconectada, la otra fuente inmediatamente asume toda la carga eléctrica del equipo.

3.4.3.2. Cooling system

El dispositivo Juniper ACX2200 no tiene ventiladores y es enfriado pasivamente por disipadores de calor como se muestra en la siguiente figura:

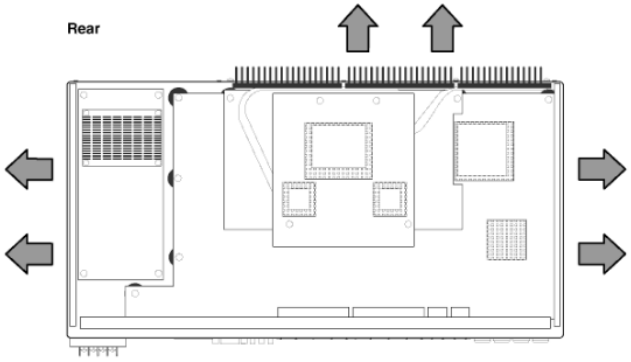

Figura 40. Disipadores de calor Juniper ACX2200

El objetivo principal es proveer un diseño que evite el mantenimiento lo cual se refleja directamente en un ahorro de OPEX del proveedor de servicios. Los sensores de temperatura en el chasis monitorean la temperatura, si esta sobrepasa el límite establecido, el dispositivo

automáticamente se apaga. El dispositivo Juniper ACX2200 puede operar normalmente con temperaturas en el rango de -40° a 65° C.

3.4.4. Software

La operatividad de todas las funcionalidades requeridas por los dispositivos Juniper MX480, Juniper MX104 y Juniper ACX2200 es brindada por el sistema operativo Junos, el cual es un software de nueva generación, modular, como se observa en Figura 41. Junos es flexible, con un alto nivel de consistencia que agiliza las operaciones de red, incrementa la disponibilidad y características de seguridad ya que fundamenta su diseño y desarrollo en los siguientes puntos:

- **Sistema operativo Universal:** Junos es el OS utilizado por todas las plataformas de Juniper Networks (Routing, Switching, Security y Datacenter).
- **Arquitectura modular:** Separación nativa del plano de Control del plano de Forwarding de manera que cada proceso corre de forma independiente en espacios blindados e independientes de memoria, lo que brinda la flexibilidad de efectuar cambios sin afectar los otros procesos y sobre todo sin afectar el tráfico de los usuarios.

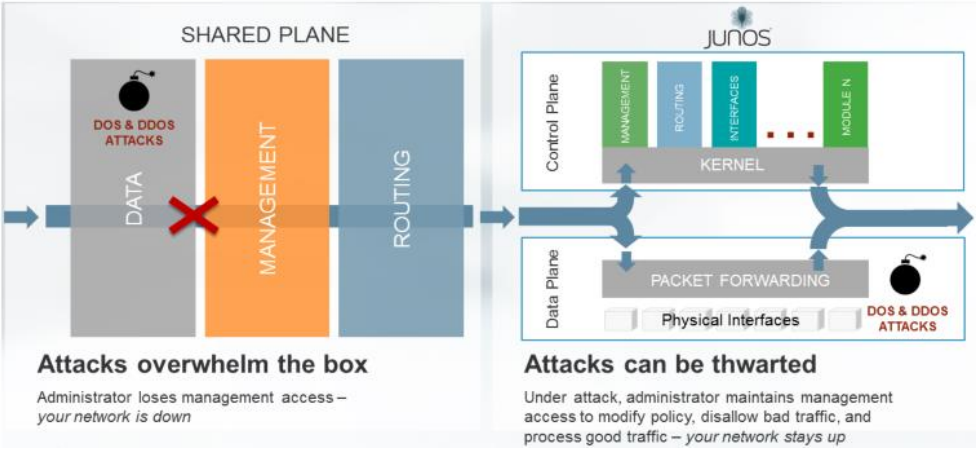

Figura 41. Arquitectura modular sistema operativo Junos

3.5. Arquitectura Física (Network Region)

Las regiones son un importante concepto en una arquitectura seamless MPLS, porque esta segmentación está destinada a solventar los problemas inherentes a las redes planas sin jerarquía lógica en cuanto a escalabilidad y tiempos de convergencia. Para la implementación del Mobile Backhaul se debe considerar hacer la agrupación o segmentación del network region de acuerdo con las siguientes consideraciones:

- Las regiones de acceso deben estar delimitadas a dispositivos con función de CSG y en caso de manejarse más de una provincia deben estar restringidas a la cobertura geográfica de esta.
- Las regiones de agregación deben estar delimitadas a dispositivos con función de AGG y en caso de ser manejadas por equipos LTE de distintos proveedores, deben ser restringidas geográficamente a las regiones de servicio con el proveedor, para este diseño se considerará un proveedor (Ericsson).

De acuerdo con las consideraciones nombradas anteriormente y en base a los eNodeB existentes en Cuenca del proveedor de telecomunicaciones, se elegirá el lugar apropiado y el número de routers de agregación basado en las restricciones geográficas. El número de eNodeB en la ciudad de Cuenca es 24 como se observa en la Figura 42.

Figura 42. Superficie cubierta por eNodeB en la ciudad de Cuenca

El número de eNodeB requiere que sean usados 3 agregadores distribuidos geográficamente cercanos a los equipos de acceso. El equipo de borde es crítico debido a que es el medio por el cual la red se comunica con el EPC, con el fin de garantizar un servicio continuo en caso de desastres se pretende usar dos equipos de borde para dar redundancia a la red. Los enlaces desde cada agregador hacia sus respectivos routers de acceso se observan en la Figura 43.

Figura 43. Superficie cubierta por equipos de acceso y agregación en la ciudad de Cuenca

La topología física de acuerdo con las consideraciones se ilustra en la Figura 44.

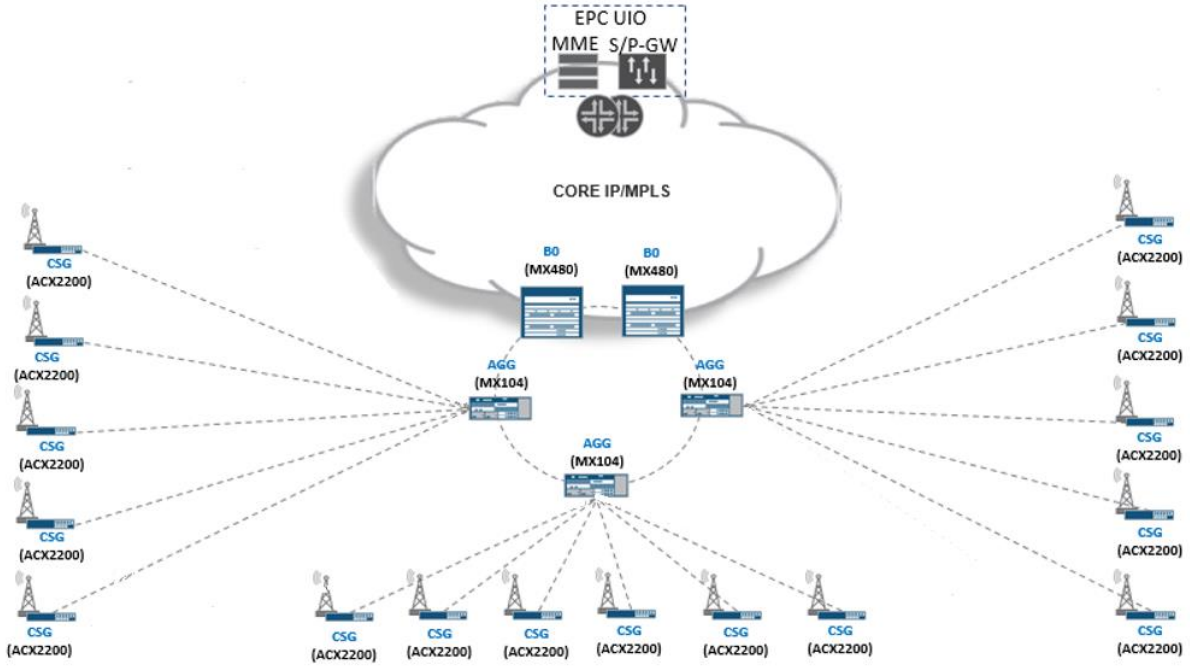

Figura 44. Topología de equipos - Mobile Backhaul

3.6. Arquitectura Lógica

Con el objetivo de mantener un diseño consistente en temas de administración de recursos como la asignación de direccionamiento, denominación de dispositivos, se define lo siguiente.

3.6.1. Direccionamiento

Para la implementación del Mobile Backhaul se asigna el segmento de red 10.33.X.100, donde x está determinado por las siguientes condiciones.

- **CSG:** 100-200.
- **AGG:** 11-100.
- **BO:** 1-10

Las condiciones de direccionamiento según el rol del equipo se observan en la Figura 45

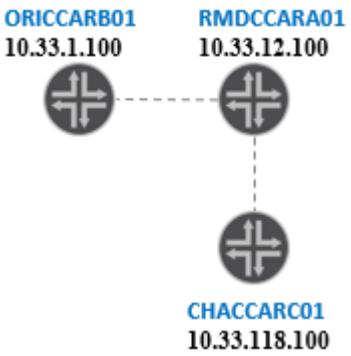

Figura 45. Esquema de direccionamiento enlace P2P

En caso de existir más regiones se debe asignar un segmento de red a cada provincia y considerar que el segundo octeto corresponde al ID de la provincia y que el segundo octeto corresponde al grupo de direcciones privadas conocidas como “Clase A”, que comienzan con el número 10.

El detalle de cada nemónico de los equipos se observa en la Tabla 12.

3.6.2. Nemónico de los equipos

El formato para el establecimiento de nombres en los equipos IP-RAN es AAABBBRF#.

- **AAA:** Define la localidad, la cual debe ser abreviada en 3 letras, por ejemplo, CCA para Cuenca.
- **BBB:** Permite identificar la capital de provincia en la cual se instala el equipo.
- **R:** Permite identificar a todo el conjunto de equipos que forman parte de la red IP-RAN; se utilizará la letra R la misma que viene de RAN.
- **F:** Permite identificar la función o rol que cumple el equipo en la red, existen 3 tipos:
    - **B:** Equipo de borde (B0) que permite interactuar directamente con la Red Nacional IP/MPLS.
    - **A:** Equipo de agregación (AGG) que permite interactuar directamente con las diferentes redes de acceso.
    - **C:** Permite identificar a los CSG, dispositivos encargados de interconectar los eNB.
- **#:** Permite identificar el número de equipo similar dentro de un mismo nodo, inicialmente debe ser 01

El detalle de cada nemónico de los equipos se observa en la Tabla 12.

Tabla 12
Loopback y hotname – Mobile backhaul

Equipo Juniper	Nombre	Hostname	Loopback
ACX2200	Altamira	ATMCCARC01	10.33.102.100
ACX2200	Giron	GRNCCARC01	10.33.106.100

CONTINÚA

ACX2200	Yunguilla	YNGCCARC01	10.33.107.100
ACX2200	Misicata	MSTCCARC01	10.33.112.100
ACX2200	Ponce Enríquez	PEZCCARC01	10.33.116.100
ACX2200	Ramírez Dávalos	RDVCCARC01	10.33.104.100
ACX2200	Cebollar	CEBCCARC01	10.33.105.100
ACX2200	Paucar	PAUCCARC01	10.33.108.100
ACX2200	Solca	SLCCCARC01	10.33.109.100
ACX2200	Baños	BNSCCARC01	10.33.114.100
ACX2200	Bellavista	BLLCCARC01	10.33.115.100
ACX2200	Espín	ESPCCARC01	10.33.101.100
ACX2200	Gualaceo	GUACCARC01	10.33.103.100
ACX2200	Estadio	ESTCCARC01	10.33.117.100
ACX2200	Chaullabamba	CHACCARC01	10.33.118.100
ACX2200	Ordoñez	ORDCCARC01	10.33.111.100
MX104	C. Ramada	RMDCCARA01	10.33.12.100
MX104	T. Terrestre	TRTCCARA01	10.33.11.100
MX104	R. Occidente	OCDCCARA01	10.33.13.100
MX480	Oriental	ORICCARB01	10.33.1.100
MX480	Occidente	OCDCCARB01	10.33.2.100

La arquitectura considerada para el direccionamiento y la distribución de interfaces se presenta en la Figura 46.

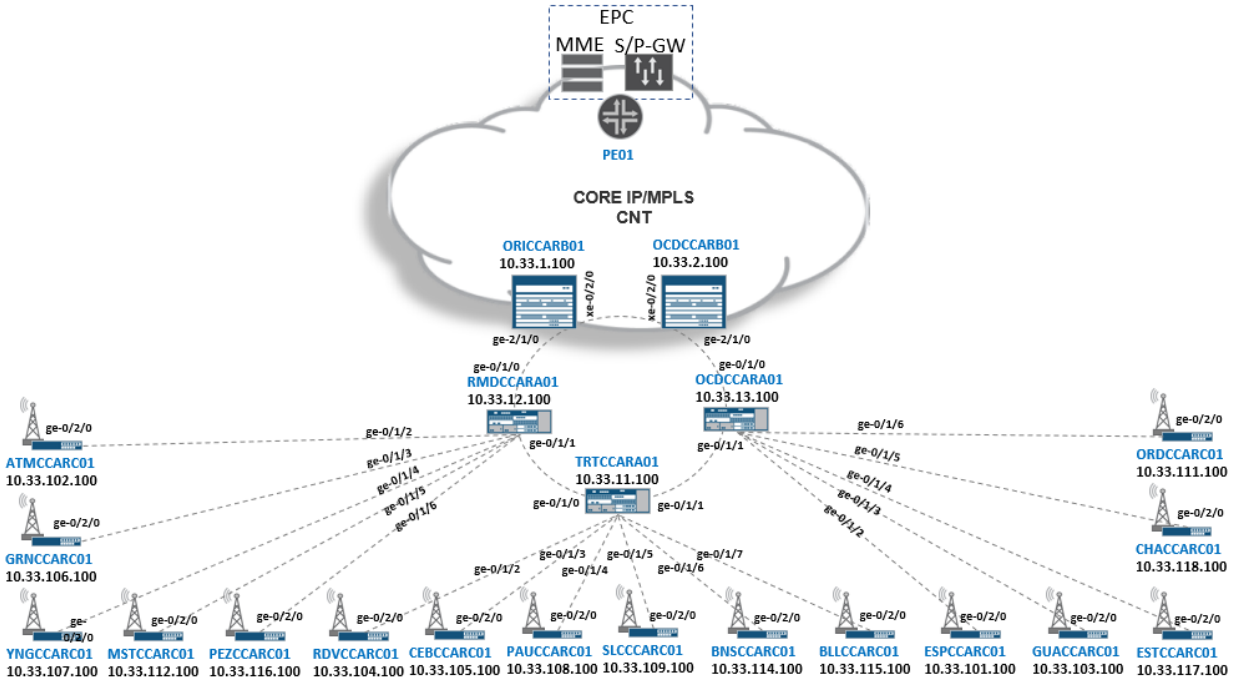

Figura 46. Topología Cuenca – Mobile Backhaul

La IPwan asociada a cada interfaz para los agregadores y para la arquitectura se presenta en la Tabla 13, Tabla 14 y Tabla 15.

Tabla 13
Información de conexión – RMDCCARA01

Interfaz	**Característica**	**Información**
ge-0/1/0	Equipo Destino	ORICCARB01
	IP WAN	10.33.1.6/30
ge-0/1/1	Equipo Destino	TRTCCARA01
	IP WAN	10.33.11.2/30
ge-0/1/2	Equipo Destino	ATMCCARC01

CONTINÚA

	IP WAN	10.33.12.1/30
ge-0/1/3	Equipo Destino	GRNCCARC01
	IP WAN	10.33.12.5/30
ge-0/1/4	Equipo Destino	YNGCCARC01
	IP WAN	10.33.12.9/30
ge-0/1/5	Equipo Destino	MSTCCARC01
	IP WAN	10.33.12.13/30
ge-0/1/6	Equipo Destino	PEZCCARC01
	IP WAN	10.33.12.17/30

Tabla 14

Información de conexión – TRTCCARA01

Interfaz	**Característica**	**Información**
ge-0/1/0	**Equipo Destino**	RMDCCARA01
	IP WAN	10.33.11.1/30
ge-0/1/1	**Equipo Destino**	OCDCCARA01
	IP WAN	10.33.11.5/30
ge-0/1/2	**Equipo Destino**	RDVCCARC01
	IP WAN	10.33.11.9/30
ge-0/1/3	**Equipo Destino**	CEBCCARC01
	IP WAN	10.33.11.13/30
ge-0/1/4	**Equipo Destino**	PAUCCARC01
	IP WAN	10.33.11.17/30
ge-0/1/5	**Equipo Destino**	SLCCCARC01

CONTINÚA

	IP WAN	10.33.11.21/30
ge-0/1/6	**Equipo Destino**	BNSCCARC01
	IP WAN	10.33.11.25/30
ge-0/1/7	**Equipo Destino**	BLLCCARC01
	IP WAN	10.33.11.29/30

Tabla 15

Información de conexión – OCDCCARA01

Interfaz	**Característica**	**Información**
ge-0/1/0	**Equipo Destino**	ORICCARB01
	IP WAN	10.33.13.1/30
ge-0/1/1	**Equipo Destino**	TRTCCARA01
	IP WAN	10.33.11.6/30
ge-0/1/2	**Equipo Destino**	ESPCCARC01
	IP WAN	10.33.13.5/30
ge-0/1/3	**Equipo Destino**	GUACCARC01
	IP WAN	10.33.13.9/30
ge-0/1/4	**Equipo Destino**	ESTCCARC01
	IP WAN	10.33.13.17/30
ge-0/1/5	**Equipo Destino**	CHACCARC01
	IP WAN	10.33.13.21/30
ge-0/1/6	**Equipo Destino**	ORDCCARC01
	IP WAN	10.33.13.13/30

Tabla 16
Información de conexión – ORICCARB01

Interfaz	Característica	Información
xe-0/2/0	**Equipo Destino**	OCDCCARB01
	IP WAN	10.33.1.1/30

Tabla 17
Información de conexión – OCDCCARB01

Interfaz	**Característica**	**Información**
xe-0/2/0	Equipo Destino	ORICCARB01
	IP WAN	10.33.1.2/30

3.6.3. Hardware para la simulación

Para la simulación presentada se usó un emulador de red llamado EVE-NG el cual corre sobre un sistema Ubuntu. El servidor que se utiliza tiene 31.8 [Gb] de memoria RAM y 8 vCPU, como se observa en la Figura 47. Los parámetros mínimos que el servidor debe cumplir para funcionar dependen del número de nodos que se desea simular y el software que estos nodos manejen.

Figura 47. Características generales del servidor usado para EVE-NG

Las condiciones de diseño para la arquitectura lógica con el fin de realizar la simulación se detallan a continuación.

3.6.4. Unidad máxima de transferencia MTU

Para un óptimo transporte del servicio 4G se debe garantizar un IP MTU de al menos de 1500 Bytes. La implementación de servicios en una red IP/MPLS basa su funcionamiento en el apilamiento de labels en el forwarding plane lo cual impacta directamente en el tamaño del paquete que se transporta como se observa en la siguiente Figura 48.

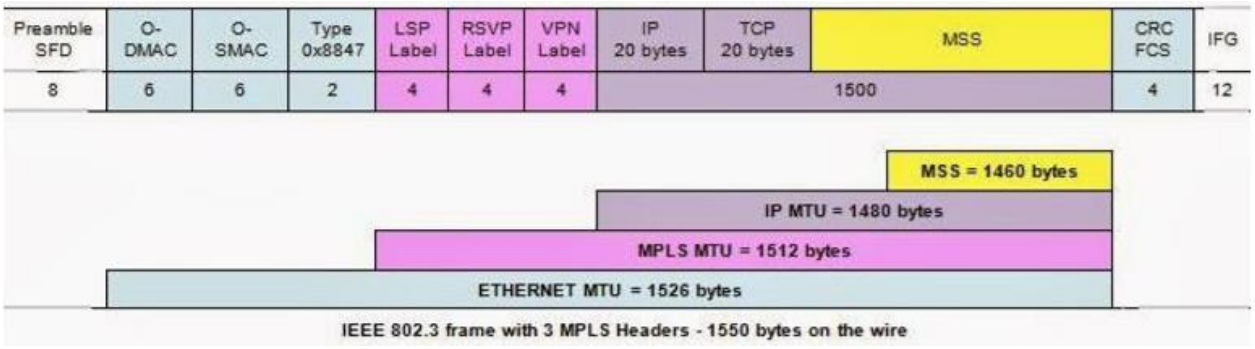

Figura 48. MPLS MTU

Por esta razón para transportar un paquete IP con un MTU de 1500 bytes, la red de IP/MPLS debe estar en la capacidad de transportar paquetes Ethernet de al menos 1550 bytes considerando que la implementación de un servicio en un entorno Seamless MPLS requiere de al menos 3 Labels. se configurará un MTU de 2026 bytes, es importante que la red de transmisión también garantice esta capacidad de transporte.

3.6.5. ISIS (Conectividad Intra-region)

En el diseño propuesto las etapas de acceso y agregación utilizaran un dominio IGP independiente para cada región, la cual estará basada en un nivel de ISIS. La Figura 49 describe el detalle de la implementación de este protocolo considerando un sistema autónomo con valor 28008 para el Mobile Backhaul.

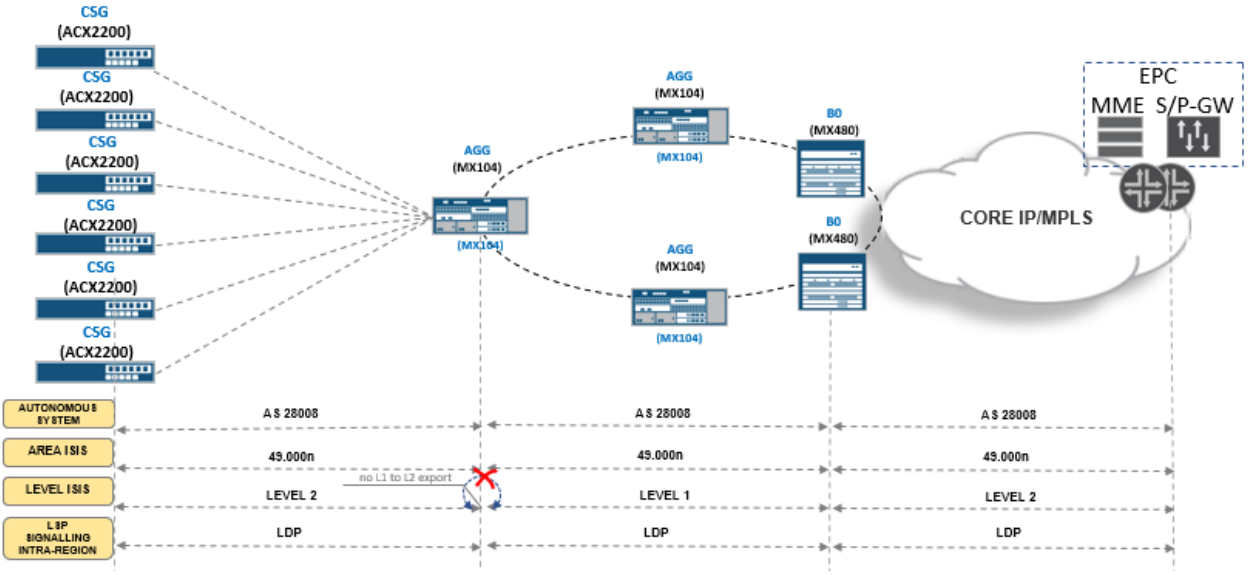

Figura 49. ISIS – Mobile backhaul

Cada región sea esta acceso o agregación debe formar parte de un nivel de IGP independiente en este caso ISIS sea este L1 o L2. Es decir, cada región tendrá un entorno de enrutamiento independiente basado en ISIS L2 lo cual garantiza un nivel de escalabilidad en el orden de miles de nodos en el acceso (fundamental para implementaciones basadas en LTE). En el caso de requerirse comunicación entre las redes de acceso de distintas provincias esta debe realizar mediante BGP-LU.

El comportamiento por default de ISIS es instalar las rutas L1 en la base de datos de los routers L2, por esta razón se debe configurar una política en los dispositivos L1/L2 que restrinja este comportamiento.

La detección de reenvío bidireccional (BFD) debe ser configurado en apoyo a ISIS como el mecanismo de detección de fallas en la red. BFD puede ser configurado para detección de fallas hasta en rangos de 10ms. Las interfaces de 1GbE deben ser configuradas con una métrica de 100,

mientras que las interfaces de 10GbE deben ser configuradas con una métrica de 10. BFD ayuda en la operación administración y mantenimiento.

ISIS utiliza como identificador para el intercambio de mensajes entre los dispositivos una dirección de red descrita por el ISO, cuyo el formato ya fue descrito en la sección 232.3.5.2. Se presenta los niveles de IS-IS asociados a cada equipo con su respectiva dirección NSAP en la Tabla 18. El estableció un identificador de área (High Order DSP) de 0008

Tabla 18
NSAP y niveles IS-IS – Mobile backhaul

Hostname	**NSAP**	**Nivel IS-IS**
ARPCCARC01	49.0008.0100.6110.1100.00	L2
LSLCCARC01	49.0008.0100.6110.2100.00	L2
BLLCCARC01	49.0008.0100.6110.3100.00	L2
SIGCCARC01	49.0008.0100.6110.4100.00	L2
MRFCCARC01	49.0008.0100.6110.5100.00	L2
RCRCCARC01	49.0008.0100.6110.6100.00	L2
MSTCCARC01	49.0008.0100.6110.7100.00	L2
YNGCCARC01	49.0008.0100.6110.8100.00	L2
SYUCCARC01	49.0008.0100.6111.9100.00	L2
RDVCCARC01	49.0008.0100.6111.0100.00	L2
GRNCCARC01	49.0008.0100.6111.1100.00	L2
AYRCCARC01	49.0008.0100.6111.2100.00	L2
BNSCCARC01	49.0008.0100.6111.3100.00	L2

CONTINÚA

ATMCCARC01	49.0008.0100.6111.4100.00	L2
SLCCCARC01	49.0008.0100.6111.5100.00	L2
PAUCCARC01	49.0008.0100.6111.6100.00	L2
CEBCCARC01	49.0008.0100.6111.7100.00	L2
ESPCCARC01	49.0008.0100.6111.8100.00	L2
ORDCCARC01	49.0008.0100.6111.9100.00	L2
CHACCARC01	49.0008.0100.6112.0100.00	L2
RCACCARC01	49.0008.0100.6112.1100.00	L2
PATCCARC01	49.0008.0100.6112.2100.00	L2
GUACCARC01	49.0008.0100.6112.3100.00	L2
ESTCCARC01	49.0008.0100.6112.4100.00	L2
RMDCCARA01	49.0008.0100.6101.1100.00	L1/L2
TRTCCARA01	49.0008.0100.6101.2100.00	L1/L2
OCDCCARA01	49.0008.0100.6101.3100.00	L1/L2
ORICCARB01	49.0008.0100.6100.1100.00	L1
OCDCCARB01	49.0008.0100.6100.2100.00	L1

3.6.6. Servicios L3VPN

El despliegue del servicio 4G está basado en servicios L3VPN, para el diseño se considera para todos los equipos de acceso ACX2200 usen la interface ge-0/0/0 para la conexión hacia el eNodeB y que el nombre de la VRF que tiene el servicio L3VPN sea llamada movlte, a nivel de la mobile

es la encargada del transporte del tráfico S1 y gestión hacia el EPC, como se observa en la *Figura 50*.

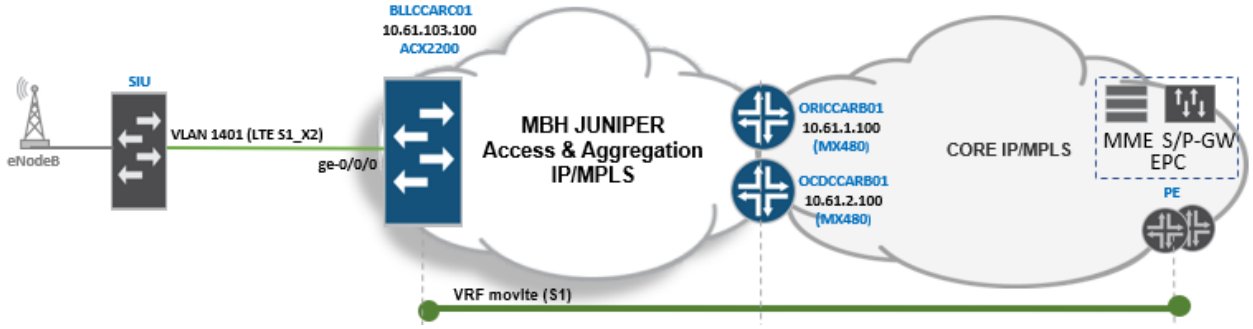

Figura 50. Servicio L3VPN – Nodo BLLCCARC01

Se tomará en cuenta los RT y RD asociados a la L3VPN para el nodo BLLCCARC01 para un sistema autónomo de valor 28008, los valores se presentan en la Tabla 19

Tabla 19
MPLS L3VPN servicios móviles 4G

VRF	**Movlte**
RD	28008:605003
RT Import	28008:605003
RT Export	28008:605003

Debido a que no existe una superposición de las Lo0 en el esquema propuesto, el valor de RT y RD serán iguales. Se considera que todos los servicios del EPC están saliendo por el mismo equipo PE con IP 10.64.44.67 por lo tanto cada VLAN será distinta para cada eNodeB y es presentada en la Tabla 20.

Tabla 20
VLAN – Equipo PE

Equipo Juniper	Nombre del sitio	Hostname	Interfaz Downlink	VLAN
ACX2200	Altamira	ATMCCARC01	ge-0/0/0	1401
ACX2200	Giron	GRNCCARC01	ge-0/0/0	1402
ACX2200	Yunguilla	YNGCCARC01	ge-0/0/0	1403
ACX2200	Misicata	MSTCCARC01	ge-0/0/0	1404
ACX2200	Ponce Enríquez	PEZCCARC01	ge-0/0/0	1405
ACX2200	Ramírez Dávalos	RDVCCARC01	ge-0/0/0	1406
ACX2200	Cebollar	CEBCCARC01	ge-0/0/0	1407
ACX2200	Paucar	PAUCCARC01	ge-0/0/0	1408
ACX2200	Solca	SLCCCARC01	ge-0/0/0	1409
ACX2200	Baños	BNSCCARC01	ge-0/0/0	1410
ACX2200	Bellavista	BLLCCARC01	ge-0/0/0	1411
ACX2200	Espín	ESPCCARC01	ge-0/0/0	1412
ACX2200	Gualaceo	GUACCARC01	ge-0/0/0	1413
ACX2200	Estadio	ESTCCARC01	ge-0/0/0	1414
ACX2200	Chaullabamba	CHACCARC01	ge-0/0/0	1415
ACX2200	Ordoñez	ORDCCARC01	ge-0/0/0	1416

3.7. Consideraciones técnicas para la instalación de equipos

3.7.1. Instalación para routers CSG: Router de acceso

Este tipo de routers necesitan conectarse con un enodeB, cuyas conexiones son generalmente outdoor. Los componentes de estos equipos se resumen en el siguiente párrafo:

Primero se necesita una unidad para distribuir corriente directa o DCDU, la cual entrega energía a estos equipos por medio de rectificadores que convierten 220 VAC a -48 VDC. La siguiente unidad se encarga de procesar la información a banda base por lo que se denomina Unidad de Banda Base o BBU y por último se encuentra la unidad de radio remoto o RRU que modula y demodula las señales tanto de banda base y radiofrecuencia, además de amplificar la señal en cuanto a su potencia y conectar con las antenas.

El router CSG se coloca dentro de un rack outdoor, como se observa en la Figura 51. El equipo se instalará según sea el caso en la unidad de rack disponible.

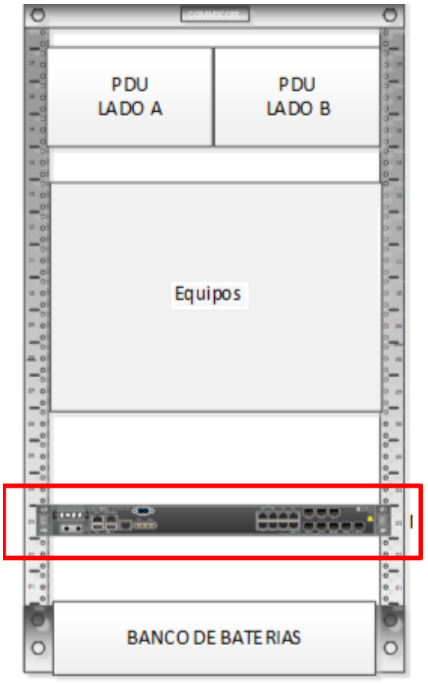

Figura 51. Diagrama de distribución de equipamiento ACX2200 en rack outdoor

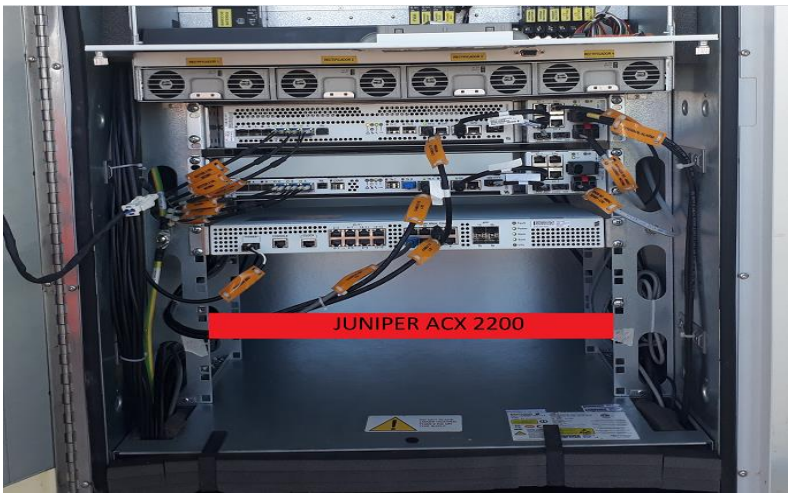

Figura 52. Posición del equipo ACX2200 en rack outdoor

Para que un router CSG reciba energía, sea AC o DC, necesita conectar por lo menos una fuente de poder de las dos existentes, sin embargo, en este escenario no existiría redundancia, por lo tanto, para que el suministro de energía tenga redundancia, se debe considerar instalar dos breakers de 6 amperios con sus circuitos eléctricos de -48 VDC desde el sistema de alimentación existente del rack de equipos hasta las entradas de las fuentes del router CSG.

Existirán dos fuentes de alimentación, la fuente 1 será energizada por el lado A mientras que la fuente 2 por el lado B lo cual da redundancia en la alimentación para el sistema, como se observa en la Figura 53. La posición de los breakers dependerá de los espacios disponibles del sistema de alimentación.

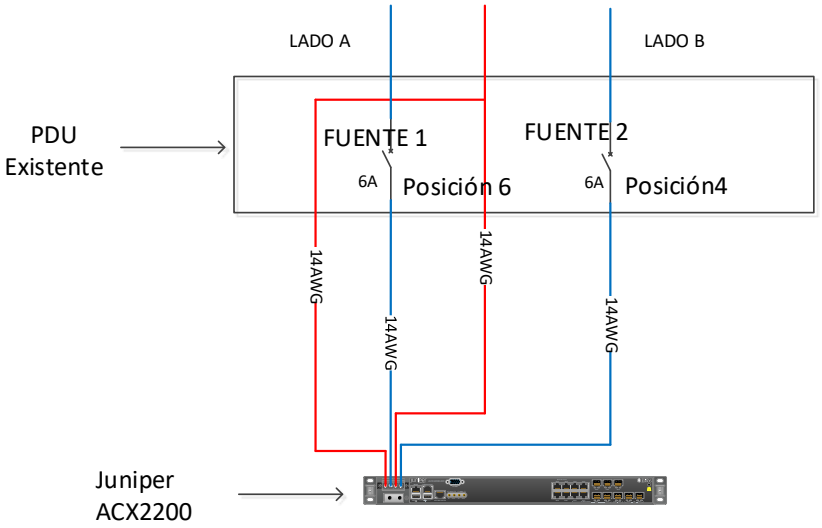

Figura 53. Diagrama de conexión eléctrica equipo ACX2200

El rack outdoor tiene un sistema de puesta a tierra al cual se conectará el chasis del equipo Juniper ACX2200, como se observa en la Figura 54.

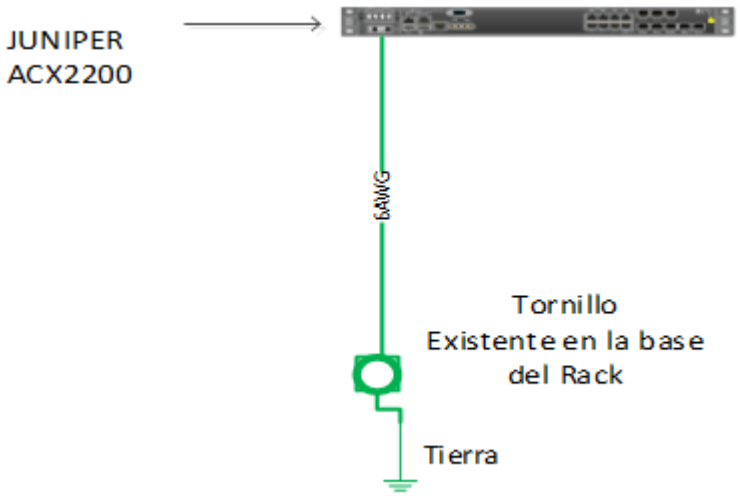

Figura 54. Diagrama de puesta a tierra equipo ACX2200

3.7.2. Instalación para routers ASG: Router de agregación

Este tipo de routers se hacen en instalaciones indoor, el equipo deberá instalarse en un rack que cuente con dos PDU independientes, así se garantiza redundancia en caso de desastres. Un posible diagrama de distribución del equipamiento se presenta la Figura 55.

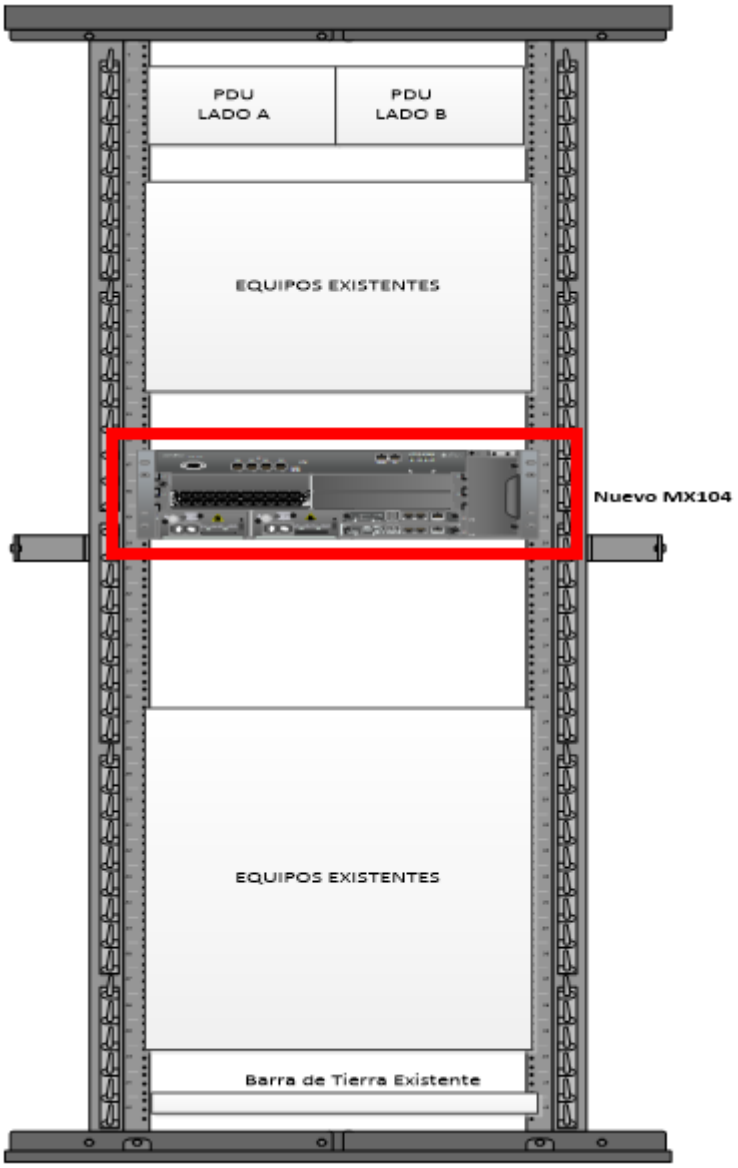

Figura 55. Diagrama de distribución de equipamiento equipo Juniper MX104

Figura 56. Posición del equipo MX104 en rack indoor existente

El router AGG se coloca dentro de un rack indoor, como se observa en la Figura 56 . El equipo se instalará según sea el caso en la unidad de rack disponible. La potencia consumida por este equipo es de 625 W con un voltaje de -48VDC. El suministro y la instalación de dos circuitos eléctricos de -48VDC desde el sistema de alimentación existente a las entradas de las fuentes del ASG se lo podría realizar con dos breakers de 32A, como se muestra en la Figura 57.

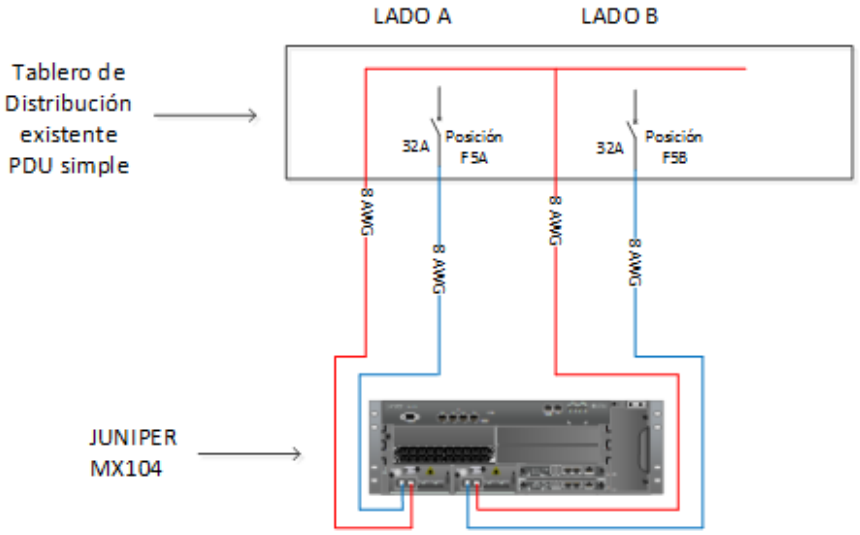

Figura 57. Diagrama de conexión eléctrica equipo MX104

El rack considerado para instalar este equipo deberá tener una barra de puesta a tierra horizontal, a la cual se conectará el chasis del equipo instalado, como se observa en la Figura 58.

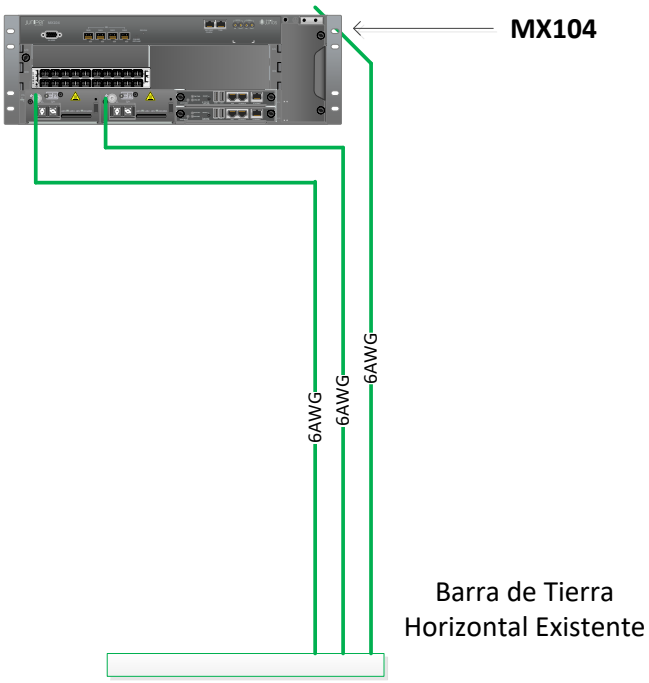

Figura 58. Diagrama de puesta a tierra equipo MX104

3.7.3. Instalación para routers BO: Router de borde

Este tipo de routers se hacen en instalaciones indoor, el cual deberá instalarse en un rack que tenga al menos 10 unidades de rack libres. Un posible diagrama de distribución del equipamiento se presenta en la Figura 59.

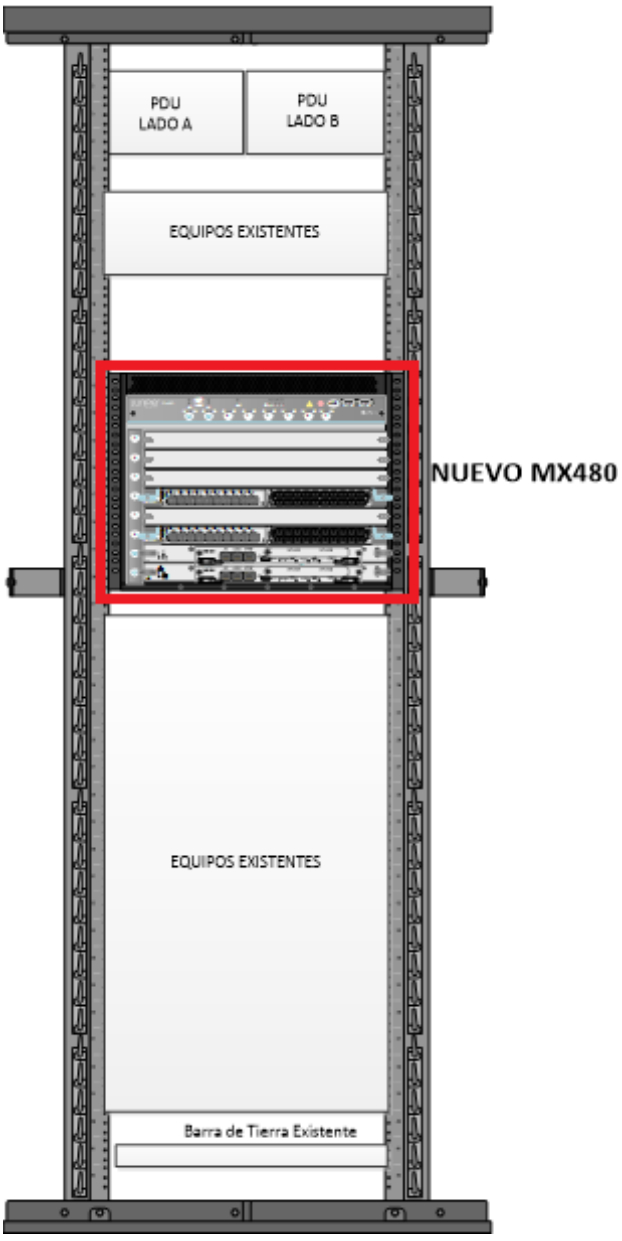

Figura 59. Diagrama de distribución de equipamiento equipo Juniper MX480

En el sistema de alimentación DC se usan cuatro breakers de 63 amperios. Desde este sistema se suministra e instala cuatro circuitos eléctricos de -48VDC hasta cada entrada de las fuentes del equipo. El lado A energizará las fuentes de alimentación PEM0 y PEM1, mientras que el lado B energizará las fuentes de alimentación PEM2 y PEM3, lo que da redundancia al sistema, como se observa en la Figura 60.

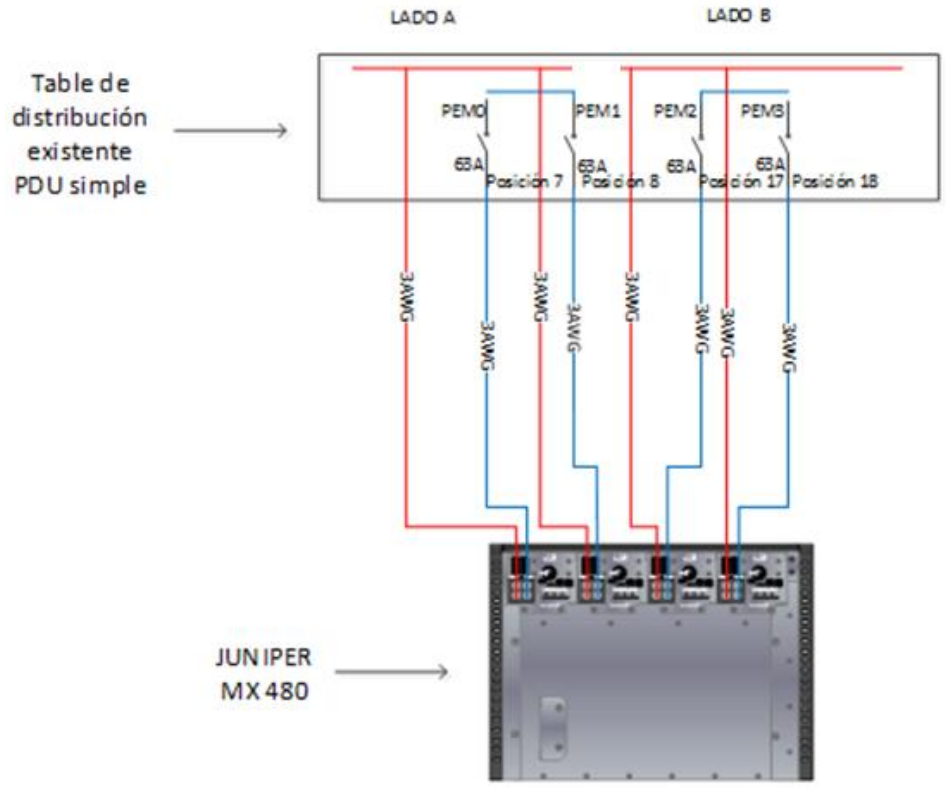

Figura 60. Diagrama de conexión eléctrica equipo MX480

El rack donde se instala el equipo debe tener una barra de tierra horizontal, al cual se conectará el chasis del equipo, como se muestra en la Figura 61.

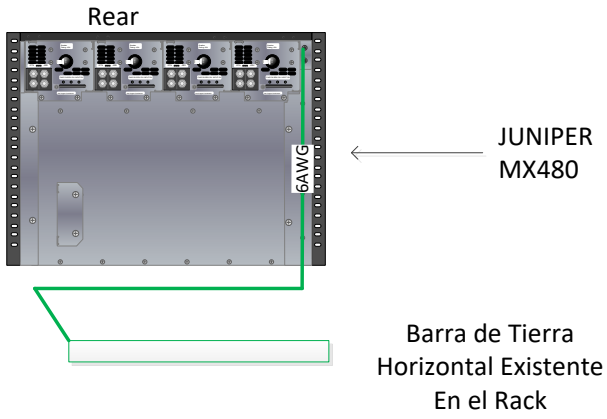

Figura 61. Diagrama de puesta a tierra equipo MX480

3.8. Presupuesto del costo final de la solución

El presupuesto detallado a continuación refleja el costo final de la solución a nivel de hardware Juniper. Las tarjetas necesarias para el equipo MX480 se observan en la Figura 31 y para el equipo MX104 en la Figura 36. De manera simplificada se puede decir que los equipos a utilizar serán los siguientes:

- 3 equipos MX104
- 2 equipos MX480
- 24 equipos ACX2200
- 4 MPC3E-3D-NG-R-B: Se necesitan dos linecards por cada equipo MX480, como se observa en Figura 31.
- 7 MIC-3D-20GE-SFP-E: Un equipo MX480 tiene dos MIC-3D-20GE-SFP-E y un equipo MX104 tiene una, como se observa en las Figura 31 y Figura 36.
- 4 MIC3-3D-10XGE-SFPP: Se necesitan dos por cada equipo MX480.
- 152 SFP-1GE-LX de los cuales 2 pertenecen a cada ACX2200, uno para la interfaz de uplink y otro para la interfaz de downlink. Los 24 adicionales corresponden a todos los

enlaces de downlink de los equipos MX104. Por último, cada equipo MX480 requiere 40 SFP-1GE-LX

- 48 SFPP-10GE-LR: Cada equipo MX480 necesita 20 SFPP-10GE-LR, como se observa en la Figura 31; otros 8 son necesarios para la interconexión del anillo entre agregadores y bordes como se indica en la Figura 44.

A continuación, se muestra en la Tabla 21 la cotización de los diferentes equipos usados en este proyecto, los cuales procederán de Estados Unidos, a través de único partner Juniper autorizado para Ecuador, el cual es Comgsp Ingeniería S.A., según la página oficial De JUNIPER NETWORKS.

Tabla 21
Presupuesto equipos Juniper

Item	Modelo	Cantidad (unidades)	Precio Total ($)
1	ACX2200-DC	24	-
2	MX104	3	-
3	MX480	2	-
4	MPC3E-3D-NG-R-B	4	-
5	MIC-3D-20GE-SFP-E	7	-
6	MIC3-3D-10XGE-SFPP	4	-
7	SFP-1GE-LX	152	-
8	SFPP-10GE-LR	48	-
Total			936.208,91

CAPÍTULO IV

4. DISEÑO Y RESULTADOS

4.1. Diseño en la arquitectura basada en el protocolo IS-IS

La configuración de la dirección NSAP e IP se ilustra en la Figura 62 conforme se definió para el nodo ATMCCARC01 en la Tabla 12 y Tabla 18.

```
    lo0 {
        unit 0 {
            description "### ROUTER ID ###";
            family inet {
                address 10.33.102.100/32;
            }
            family iso {
                address 49.0008.0100.3310.2100.00;
            }
        }
    }
}
```

Figura 62. Configuración NSAP - BLLCCARC01

Junos permite la creación de grupos con el objetivo de crear archivos de configuración simples y con una estructura lógica, que permitan un fácil entendimiento para los administradores de red. Para el protocolo ISIS se configuró un grupo que permita replicar masivamente en cada interfaz, el grupo creado es GR-ISIS, como se muestra Figura 63.

```
groups {
    GR-ISIS {
        protocols {
            isis {
                interface "<*[es]*>" {
                    level 2 {
                        hello-authentication-key "$9$BLXRyKwsg4JDdVP5TQCAEcye8XxNdY4ax7"; ## SECRET-DATA
                        hello-authentication-type md5;
                    }
                    level 1 {
                        hello-authentication-key "$9$kmQnRESyeWB1dbwsZGP5Q3Ctp0Bhylpu"; ## SECRET-DATA
                        hello-authentication-type md5;
                    }
                }
            }
        }
    }
}
```

Figura 63. Grupo GR-ISIS

Este grupo se aplica en la configuración del protocolo, como lo muestra la Figura 64 y será replicada a cada interfaz.

Figura 64. Aplicación del grupo GR-ISIS en el protocolo ISIS

De acuerdo con lo descrito en la Figura 49 el nivel de ISIS en el que se comunican los equipos de acceso debe ser de nivel 2. La configuración requerida para habilitar ISIS en los dispositivos CSG se describe en la Figura 65. La configuración presentada corresponde al nodo ATMCCARC01

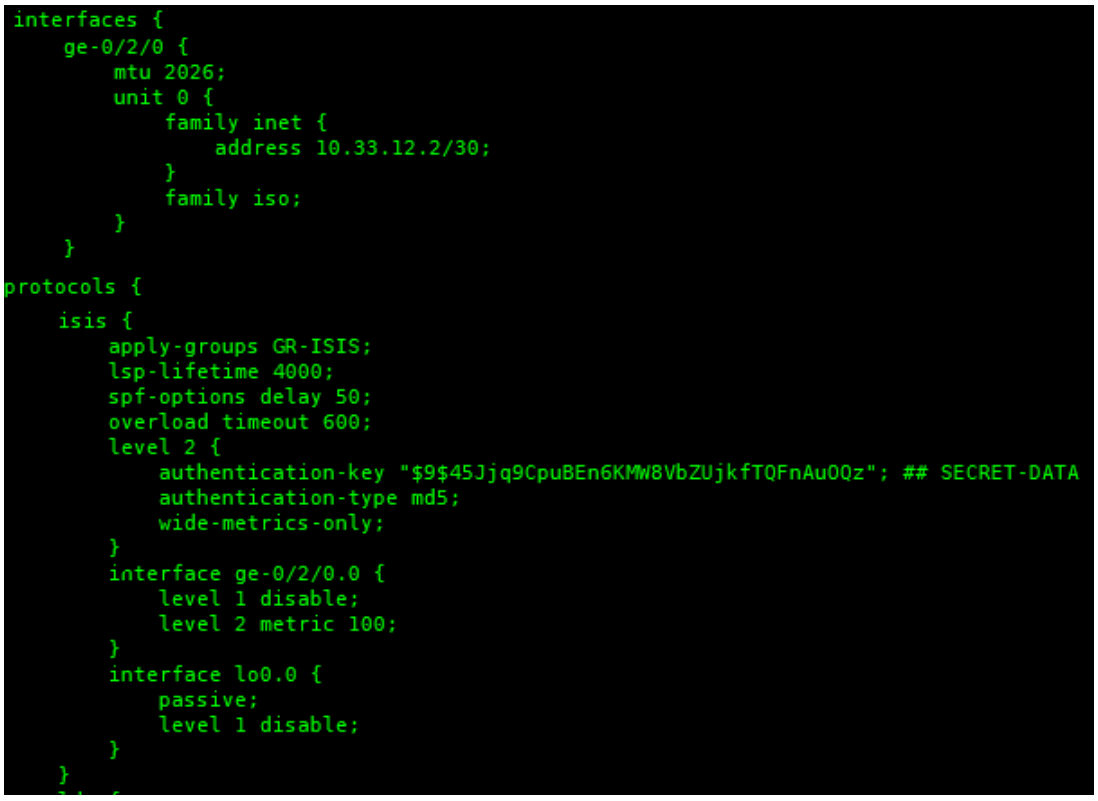

Figura 65. Nivel de ISIS en equipos CSG

De acuerdo con lo descrito en la Figura 49, el nivel 1 de ISIS corresponde a equipos de AGG y BO. La configuración de ISIS presentada en la Figura 66 corresponde al equipo de agregación RMDCCARA01.

Las interfaces entre agregadores deben trabajar en ISIS en nivel 1-2, debido a que los prefijos aprendidos por los agregadores de los CSG son ISIS nivel 2 y la comunicación entre el agregador y el borde es nivel 1. Todas las interfaces entre agregadores con el fin de conocer los prefijos de nivel 2 serán configuradas como ISIS nivel 1-2 y todas las interfaces entre agregador y borde serán configuradas como ISIS nivel 1, su configuración se observa en Figura 66. Las interfaces ge-0/1/1 y ge-0/1/1 corresponden a la interfaz hacia otro agregador y hacia el borde, como se aprecia en la Figura 46.

```
interfaces {
    ge-0/1/0 {
        mtu 2026;
        unit 0 {
            family inet {
                address 10.33.1.6/30;
            }
        }
    }
    ge-0/1/1 {
        mtu 2026;
        unit 0 {
            family inet {
                address 10.33.11.2/30;
            }
        }
    }
}
protocols {
    isis {
        apply-groups GR-ISIS;
        lsp-lifetime 4000;
        spf-options delay 50;
        }
        overload timeout 600;
        level 1 {
            authentication-key "$9$x.x-s4mPTQ39kqBIREKvdbsgZUDikfQFDj"; ## SECRET-DATA
            authentication-type md5;
            wide-metrics-only;
        }
        level 2 {
            authentication-key "$9$DhHPQOBRESepuxN-d4ok.PTn/9Ap1Ec9C"; ## SECRET-DATA
            authentication-type md5;
            wide-metrics-only;
        }
        interface ge-0/1/0.0 {
            level 2 disable;
            level 1 metric 100;
        }
        interface ge-0/1/1.0 {
            level 1 metric 100;
            level 2 metric 100;
        }
        interface lo0.0 {
            passive;
        }
    }
}
```

Figura 66. Nivel de ISIS - RMDCCARA01

Los niveles de ISIS entre todas las interfaces de la topología presentada en la Figura 46, se configuraron como se observa en la Figura 67.

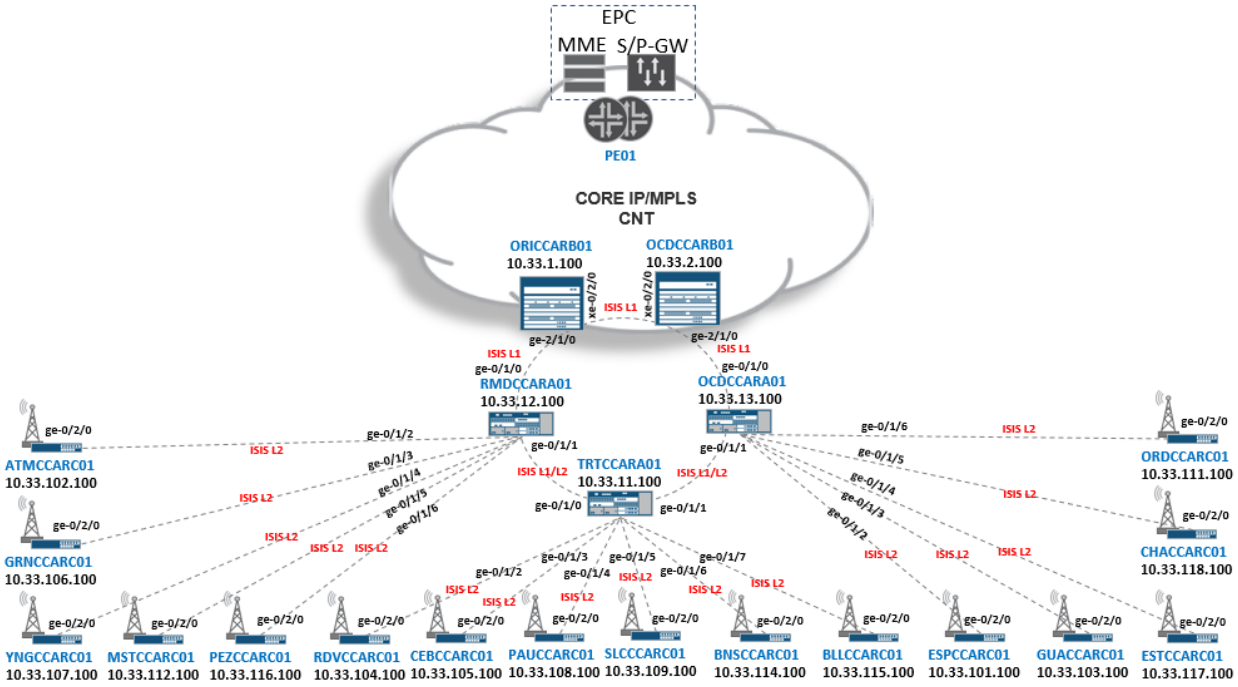

Figura 67. Nivel de ISIS por interfaz – Mobile Backhaul

Todos los LSPs intercambiados entre un equipo de agregación y de borde son de nivel 1. La base de datos de nivel 1 contendrá los nuevos prefijos aprendidos localmente desde routers CSG de nivel 2 y la información intercambiada desde routers de agregación de nivel 1. La configuración del equipo de borde ORICCARB01 a nivel de ISIS se muestra en la Figura 68.

```
interfaces {
    ge-2/1/0 {
        mtu 2026;
        unit 0 {
            family inet {
                address 10.33.1.5/30;
            }
            family iso;
                maximum-labels 5;
            }
        }
    }
    xe-2/2/0 {
        mtu 2026;
        unit 0 {
            family inet {
                address 10.83.4.18/30;
            }
            family iso;
        }
    }
 }
protocols {
    isis {
        apply-groups GR-ISIS;
        lsp-lifetime 4000;
        spf-options delay 50;
        }
        overload timeout 600;
        level 1 {
            authentication-key "$9$x.x-s4mPTQ39kqBIREKvdbsgZUDikfQFDj"; ## SECRET-DATA
            authentication-type md5;
            wide-metrics-only;
        }
        level 2 {
            authentication-key "$9$DhHPQOBRESepuxN-d4ok.PTn/9Ap1Ec9C"; ## SECRET-DATA
            authentication-type md5;
            wide-metrics-only;
        }
        interface ge-2/1/0.0 {
            level 2 disable;
            level 1 metric 100;
        }
        interface xe-0/2/0.0 {
            level 1 metric 100;
            level 2 disable;
        }
        interface lo0.0 {
            passive;
        }
    }
}
```

Figura 68. Nivel de ISIS – ORICCARB01

4.2. Diseño en la arquitectura basada en el protocolo LDP para el transporte MPLS

Para señalizar los LSP MPLS dentro de cada región se utilizará LDP, el cual es un protocolo de señalización simple y rápido para el establecimiento de LSPs en redes MPLS, la Figura 69 detalla la implementación de este protocolo para el Mobile Backhaul.

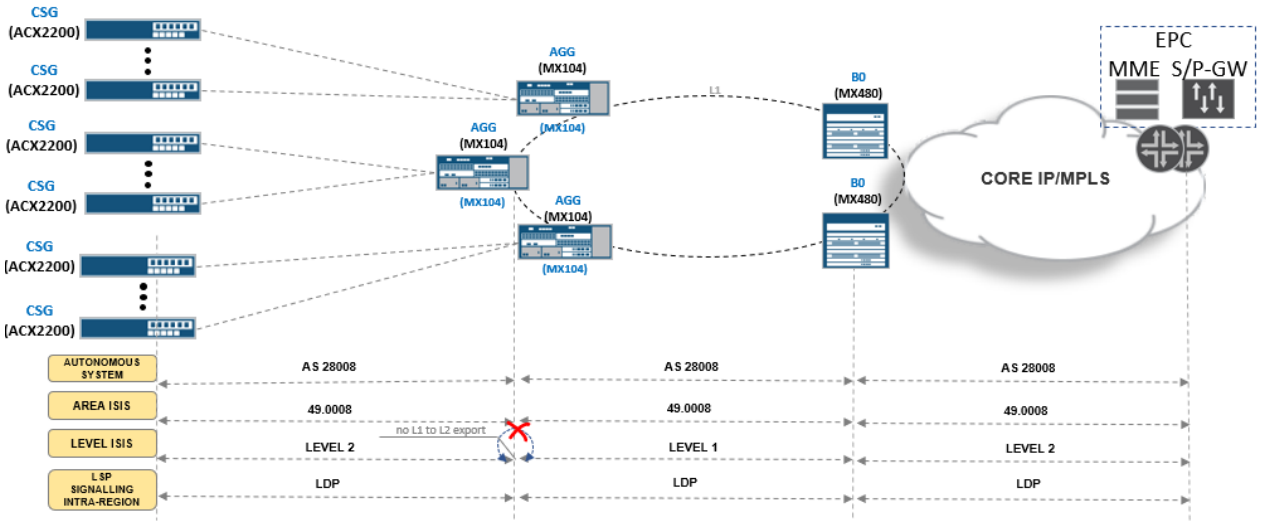

Figura 69. LDP - Mobile Backhaul

LDP es un protocolo que corre en el top de ciertos IGPs en este caso ISIS, por esta razón es fundamental que sea habilitado exclusivamente en las interfaces en las que el IGP se encuentra habilitado, se configuró en todas las interfaces descritas en la Tabla 13, Tabla 14, Tabla 15 y la interfaz ge-0/2/0 de cada CSG. La configuración presentada en la Figura 70 corresponde a las interfaces configuradas para el nodo de agregación TRTCCARA01.

```
protocols {
    ldp {
        interface ge-0/1/0.0;
        interface ge-0/1/1.0;
        interface ge-0/1/2.0;
        interface ge-0/1/3.0;
        interface ge-0/1/4.0;
        interface ge-0/1/5.0;
        interface ge-0/1/6.0;
        interface ge-0/1/7.0;
        interface ge-0/1/8.0;
        interface lo0.0;
    }
 }
```

Figura 70. LDP - TRTCCARA01

Las interfaces ge-0/1/0 y ge-0/1/1 de la Figura 70 corresponden a conexiones hacia agregadores y el resto de las interfaces conexiones hacia sus routers de acceso.

La implementación de LDP en Junos por defecto utiliza el router-id del dispositivo como transport-address para establecer la sesión TCP sobre la que funciona LDP, es importante que esta configuración sea definida acorde a la configuración realizada en la interfaz Lo0 como se describe a en la Figura 71 para el nodo RDVCCARC01.

```
lo0 {
    unit 0 {
        description "### ROUTER ID ###";
        family inet {
            address 10.33.104.100/32;
        }
        family iso {
            address 49.0008.0100.3310.4100.00;
        }
    }
}
```

Figura 71. LDP/router id – RDVCCARC01

Para que el establecimiento de los LSPs ocurra en Junos se debe habilitar la funcionalidad de MPLS en cada una de las interfaces asociadas a LDP. MPLS se configuró en todas las interfaces descritas en la Tabla 13, Tabla 14, Tabla 15 y la interfaz ge-0/2/0 de cada CSG. La configuración realizada en el equipo ESPCCARC01 se muestra en la Figura 72.

```
interfaces {
    ge-0/2/0 {
        mtu 2026;
        unit 0 {
            family inet {
                address 10.33.13.6/30;
            }
            family iso;
            family mpls;
        }
    }
}
protocols {
    mpls {
        interface ge-0/2/0.0;
    }
}
```

Figura 72. MPLS – ESPCCARC01

Adicionalmente se debe habilitar en todos los equipos a nivel del IGP (ISIS) la sincronización con LDP, como se observa en la Figura 73. El objetivo es que los LSP estén completamente establecidos antes de que el IGP envié tráfico, caso contrario se perdería tráfico.

```
GR-ISIS {
    protocols {
        isis {
            interface "<*[es]*>" {
                ldp-synchronization;
                level 2 {
                    hello-authentication-key "$9$H.T3IRcSlMOB-VbwJZmfTF9AtuOESrtp"; ## SECRET-DATA
                    hello-authentication-type md5;
                }
                level 1 {
                    hello-authentication-key "$9$MS.L-wiH.m5FUDtu0OSyX7-bgoaZUkmfaJ"; ## SECRET-DATA
                    hello-authentication-type md5;
                }
            }
        }
    }
}
```

Figura 73. Sincronización LDP en ISIS

4.3. Configuraciones generales

4.3.1. Alta disponibilidad

Los equipos de borde y agregación cuentan con dos tarjetas (RE) para manejar el control plane, estas tarjetas permiten la implementación de mecanismos basados en software y hardware para

incrementar la disponibilidad de los servicios que circulan por el dispositivo. Para garantizar la mínima disrupción durante la falla de una routing engine se debe;

- Sincronizar los archivos de configuración
- Habilitar Graceful RE Switchover (GRES)

4.3.1.1. Sincronizar los archivos de configuración

En Junos existen dos tipos de archivos de configuración estos son el archivo de configuración candidata y el archivo de configuración activa. El archivo de configuración candidata es un conjunto de comandos enviados desde el CLI sin guardar, un archivo de configuración candidata llega a ser un archivo de configuración activa cuando finalmente es guardado. El comando commit es el medio por el que un archivo de configuración de tipo candidata se vuelve de tipo activa. El comando commit es exitoso solo si la verificación de la sintaxis del archivo de configuración candidata es correcto.

En un dispositivo con dos routing engine (RE) como los MX104 y MX480, debe existir solamente una configuración y debe ser compartida por las dos tarjetas. La primera routing engine (RE0) cumple con la función de master, mientras que la segunda routing engine (RE1) la función de backup. En un evento inesperado en el falle la RE0 la RE1 cambia a ser master y la RE0 a backup.

El comando commit permite únicamente guardar el archivo de configuración candidata en la RE0 por lo cual resulta necesario habilitar en el sistema commit synchronize, como se observa en la Figura 74. El comando commit synchronize permite producir automáticamente la sincronización entre dos routing engine dentro del mismo chasis.

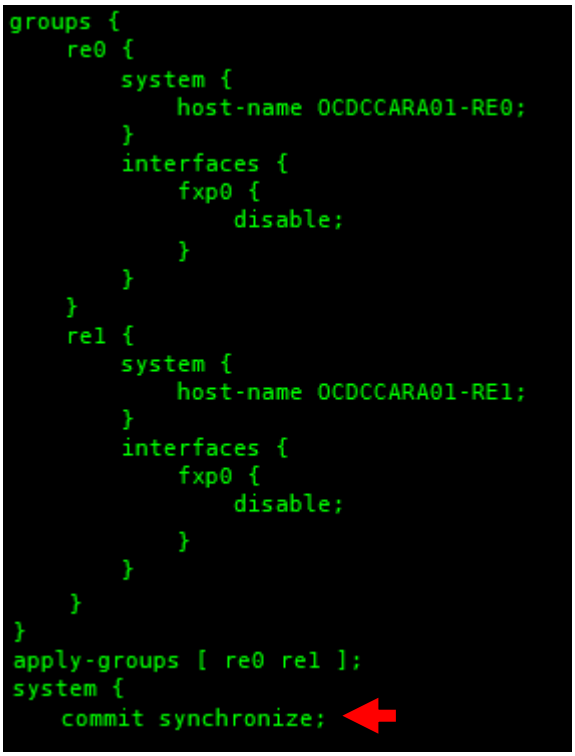

Figura 74. Habilitación de commit synchronize – OCDCCARA01

La interfaz fxp0 está destinada a ser un puerto de administración para el router. Existe una interfaz fxp0 por cada RE en todos los equipos.

Para que un chasis de la serie MX funcione correctamente, se debe configurar enhanced-ip, como se observa en la Figura 75, esto permite que los módulos MPC/MIC se enciendan con el chasis, caso contrarío deberán ser encendidas por comandos o manualmente, estas linecards/tarjetas se observan en la Figura 31.

```
chassis {
    dump-on-panic;
    redundancy {
        routing-engine 0 master;
        routing-engine 1 backup;
        failover {
            on-disk-failure;
        }
    }
    network-services enhanced-ip;
}
```

Figura 75. Condiciones de redundancia RE

Se pueden definir condiciones para la sincronización a nivel de hardware de las rounting engine, como se observa en la Figura 75.

4.3.1.2. Habilitar Graceful RE Switchover (GRES)

GRES posibilita que un router con routing engine redundantes continúen reenviando paquetes, incluso si falla uno de los RE. GRES conserva la interfaz y la información del núcleo. El tráfico no se interrumpe, la configuración de GRES se observa en la Figura 76.

```
chassis {
    redundancy {
        graceful-switchover;
    }
}
```

Figura 76. Graceful RE switchover

4.4. Resultados simulación plano de control

4.4.1. Resultados conectividad ISIS

Se verificará el nivel de ISIS en el que se conecta el equipo de agregación RMDCCARA01, el plano de control para el equipo de agregación se presenta en la Figura 77.

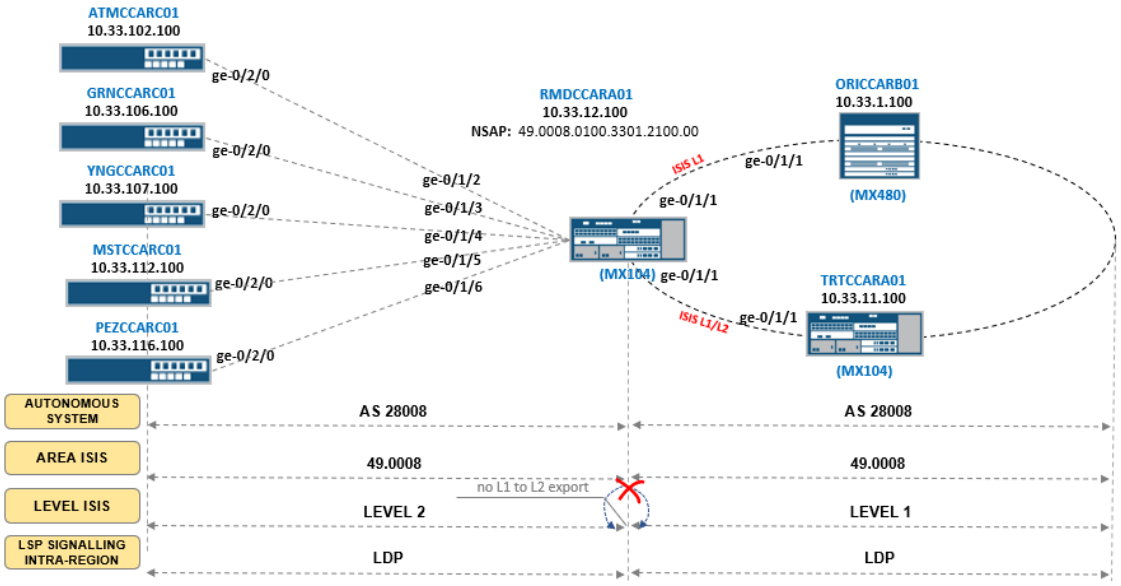

Figura 77. Plano de control - RMDCCARA01

Cada equipo de acceso se conecta con la región mediante ISIS nivel 2. La interfaz ge-0/1/1 se conecta al agregador mediante ISIS nivel 1 y la interfaz ge-0/1/1 se conecta con el agregador mediante ISIS nivel 1-2, como se observa en la Figura 78. El direccionamiento IP para RMDCCARA01 se presenta en la Tabla 13.

```
junos_space@RMDCCARA01> show isis adjacency detail
ORICCARB01
  Interface: ge-0/1/0.0, Level: 1, State: Up, Expires in 25 secs
  Priority: 0
  Circuit type: 1, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.1.5

TRTCCARA01
  Interface: ge-0/1/1.0, Level: 3, State: Up, Expires in 26 secs
  Priority: 0
  Circuit type: 3, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.11.1
ATMCCARC01
  Interface: ge-0/1/2.0, Level: 2, State: Up, Expires in 25 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.2

GRNCCARC01
  Interface: ge-0/1/3.0, Level: 2, State: Up, Expires in 26 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.6
YNGCCARC01
  Interface: ge-0/1/4.0, Level: 2, State: Up, Expires in 25 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.10

MSTCCARC01
  Interface: ge-0/1/5.0, Level: 2, State: Up, Expires in 21 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.14

RBBUNCHRC01
  Interface: ge-0/1/6.0, Level: 2, State: Up, Expires in 26 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.18
```

Figura 78. Adyacencia ISIS - RMDCCARA01

El nivel de ISIS en el que se conectan todos los equipos de acceso con su respectivo agregador es L2. El plano de control del equipo de acceso PEZCCARC01 con el equipo de agregación RMDCCARA01 se observa en la Figura 79.

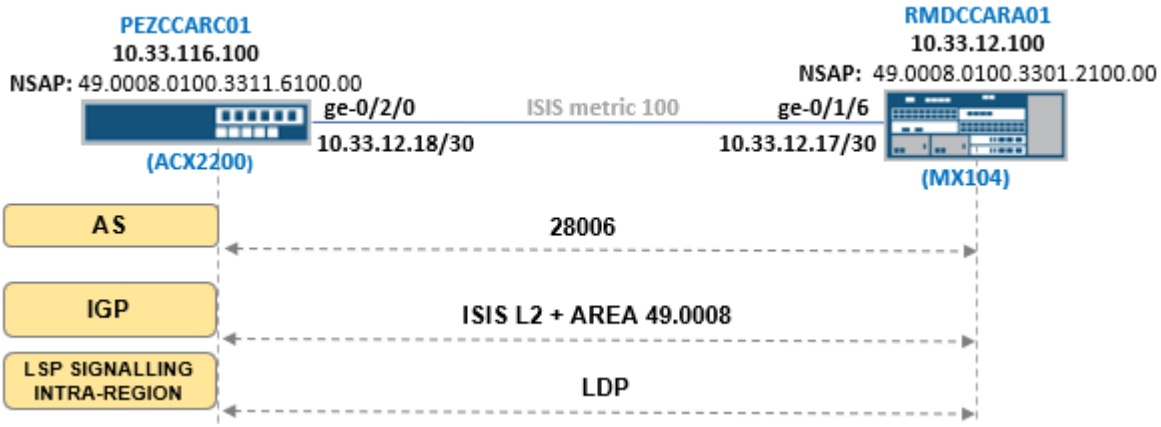

Figura 79. Plano de control - PEZCCARC01

Cada equipo de acceso se conecta con la región mediante ISIS nivel 2, como se observa en la Figura 80.

```
junos_space@PEZCCARC01> show isis adjacency detail
RMDCCARA01
  Interface: ge-0/2/0.0, Level: 2, State: Up, Expires in 21 secs
  Priority: 0
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 10.33.12.17
```

Figura 80. Adyacencia ISIS - PEZCCARC01

El protocolo ISIS permite a cada router aprender las loopback (Lo0) de Cuenca las cuales son guardadas en la tabla inet.0, esta tabla almacena las rutas unicast IPv4, estas rutas pueden ser aprendidas dinámicamente a través de protocolos de enrutamiento o definidas estáticamente, en este caso han sido aprendidas por ISIS, las Lo0 aprendidas por el equipo ESPCCARC01 son mostradas en la Figura 81.

```
junos_space@ESPCCARC01> show route table inet.0 protocol isis | match /32
10.33.11.100/32    *[IS-IS/18]   metric 200
10.33.12.100/32    *[IS-IS/18]   metric 300
10.33.13.100/32    *[IS-IS/18]   metric 100
10.33.102.100/32   *[IS-IS/18]   metric 400
10.33.103.100/32   *[IS-IS/18]   metric 200
10.33.104.100/32   *[IS-IS/18]   metric 300
10.33.105.100/32   *[IS-IS/18]   metric 300
10.33.106.100/32   *[IS-IS/18]   metric 400
10.33.107.100/32   *[IS-IS/18]   metric 400
10.33.108.100/32   *[IS-IS/18]   metric 300
10.33.109.100/32   *[IS-IS/18]   metric 300
10.33.111.100/32   *[IS-IS/18]   metric 200
10.33.112.100/32   *[IS-IS/18]   metric 400
10.33.114.100/32   *[IS-IS/18]   metric 300
10.33.115.100/32   *[IS-IS/18]   metric 300
10.33.116.100/32   *[IS-IS/18]   metric 400
10.33.117.100/32   *[IS-IS/18]   metric 200
10.33.118.100/32   *[IS-IS/18]   metric 200
```

Figura 81. Lo0 aprendidas mediante ISIS - ESPCCARC01

La tabla inet.0 muestra que la métrica es diferente para algunas Lo0, las rutas más bajas son las mejores, en este caso la Lo0 10.33.13.100 tiene la mejor métrica y corresponde al equipo de agregación con el que tiene una conexión directa.

4.4.2. Resultados del transporte con LDP

Una vez conocidas las Lo0 en una red seamless MPLS se necesita un LSP para llegar de un router a otro. El protocolo de transporte LDP es el encargado de crear los LSP asociados a cada IP. LDP permite la asignación de etiquetas, como lo muestra la Figura 82.

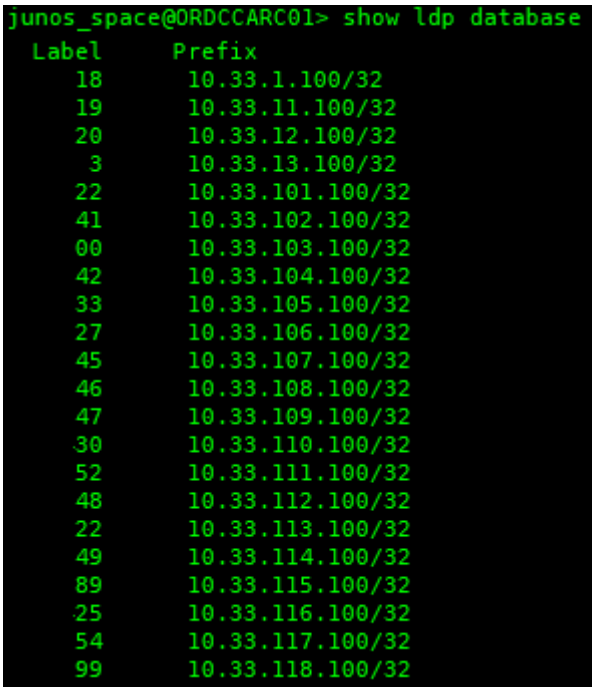

Figura 82. Base de datos LDP - ORDCCARC01

Existen una sesión LDP asociada a cada interfaz que se muestra en la Figura 46, de la siguiente manera:

- Existe una sesión LDP desde la interfaz del equipo de acceso hacía de su respectivo agregador
- El número de sesiones LDP en un agregador dependerá de la cantidad de interfaces que tengan configurado este protocolo.
- El número de sesiones LDP en el equipo de borde son dos una para la conexión hacia el otro agregador y otra para la conexión hacia el equipo de acceso.

Existe una sesión LDP asociada a cada interfaz que se muestra en la Figura 46, de la siguiente manera.

4.4.3. Resultados conectividad hacia el EPC

4.4.3.1. Servicio L3VPN – PEZCCARC01 hacia EPC

La información correspondiente al perfil de servicio 4G para el nodo PEZCCARC01 se muestra en la Figura 83. De acuerdo con la Tabla 20 el servicio está dentro de la VLAN 1405.

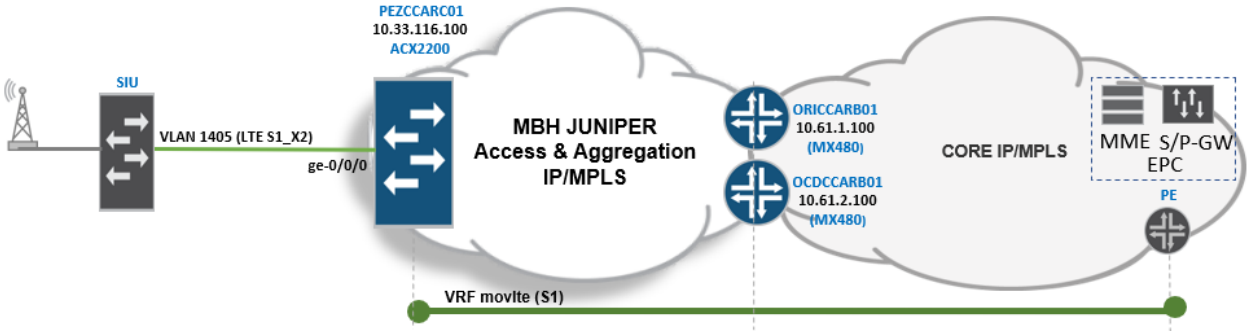

Figura 83. Diagrama de servicios - PEZCCARC01

El estado de la vrf con sus respectivos componentes RT, RD y VLAN para el equipo de acceso PEZCCARC01 están activos y permiten tener servicios L3VPN, como se observa en la Figura 84.

```
junos_space@PEZCCARC01> show route instance detail | find movlte
movlte:
  Type: vrf                  State: Active
  Interfaces:
    ge-0/1/0.1405
  Route-distinguisher: 28006:605003
  Vrf-import: [ __vrf-import-movlte-internal__ ]
  Vrf-export: [ __vrf-export-movlte-internal__ ]
  Vrf-import-target: [ target:28008:605003 ]
  Vrf-export-target: [ target:28008:605003 ]
  Tables:
    movlte.inet.0
```

Figura 84. Vrf movlte para servicios L3VPN - PEZCCARC01

La prueba de conectividad para el servicio L3VPN hacia el core de 4G se encuentra operativo no existen perdida de paquetes, como se observa en la Figura 85.

```
junos_space@PEZCCARC01> ping routing-instance movlte 10.64.44.67 size 1800
PING 10.64.44.67 (10.64.44.67): 1800 data bytes
1808 bytes from 10.64.44.67: icmp_seq=0 ttl=61 time=2.017 ms
1808 bytes from 10.64.44.67: icmp_seq=1 ttl=61 time=2.129 ms
1808 bytes from 10.64.44.67: icmp_seq=2 ttl=61 time=2.024 ms
1808 bytes from 10.64.44.67: icmp_seq=3 ttl=61 time=2.012 ms
1808 bytes from 10.64.44.67: icmp_seq=4 ttl=61 time=2.065 ms
^C
--- 10.64.44.67 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.012/2.049/2.129/0.044 ms
```

Figura 85. Ping hacia el EPC - PEZCCARC01

4.4.3.2. Servicio L3VPN – BNSCCARC01 hacia EPC

La información correspondiente al perfil de servicio 4G para el nodo BNSCCARC01 se muestra en la Figura 86. De acuerdo con la Tabla 20 el servicio está dentro de la VLAN 1410.

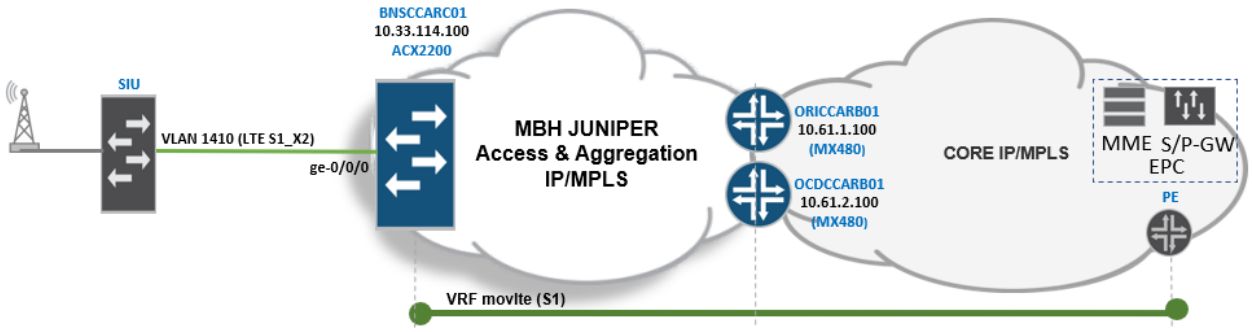

Figura 86. Diagrama de servicios - BNSCCARC01

El estado de la vrf con sus respectivos componentes RT, RD y VLAN para el equipo de acceso BNSCCARC01 están activos y permiten tener servicios L3VPN, como se observa en la Figura 87.

```
junos_space@BNSCCARC01> show route instance detail | find movlte
movlte:
  Type: vrf                  State: Active
  Interfaces:
    ge-0/0/0.1410
  Route-distinguisher: 28006:605003
  Vrf-import: [ __vrf-import-movlte-internal__ ]
  Vrf-export: [ __vrf-export-movlte-internal__ ]
  Vrf-import-target: [ target:28008:605003 ]
  Vrf-export-target: [ target:28008:605003 ]
  Tables:
    movlte.inet.0
```

Figura 87. Vrf movlte para servicios L3VPN - BNSCCARC01

La prueba de conectividad para el servicio L3VPN hacia el core de 4G se encuentra operativo y no existen perdida de paquetes, como se observa en la Figura 88.

```
junos_space@BNSCCARC01> ping routing-instance movlte 10.64.44.67 size 1900
PING 10.64.44.67 (10.64.44.67): 1900 data bytes
1908 bytes from 10.64.44.67: icmp_seq=0 ttl=61 time=2.134 ms
1908 bytes from 10.64.44.67: icmp_seq=1 ttl=61 time=1.962 ms
1908 bytes from 10.64.44.67: icmp_seq=2 ttl=61 time=1.966 ms
1908 bytes from 10.64.44.67: icmp_seq=3 ttl=61 time=2.075 ms
1908 bytes from 10.64.44.67: icmp_seq=4 ttl=61 time=1.966 ms
^C
--- 10.64.44.67 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.962/2.021/2.134/0.071 ms
```

Figura 88. Ping hacia el EPC - BNSCCARC01

4.4.3.3. Servicio L3VPN – BNSCCARC01 hacia EPC

La información correspondiente al perfil de servicio 4G para el nodo CHACCARC01 se muestra en la Figura 89. De acuerdo con la tabla Tabla 20 el servicio está dentro de la VLAN 1415.

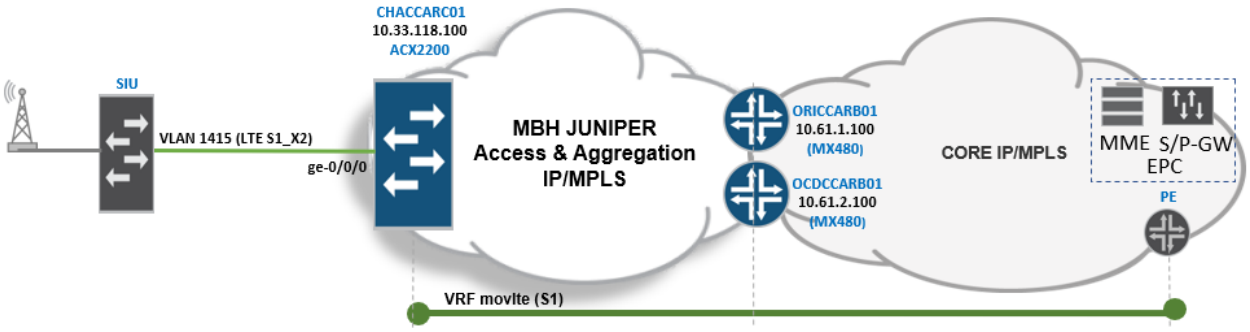

Figura 89. Diagrama de servicios - CHACCARC01

El estado de la vrf con sus respectivos componentes RT, RD y VLAN para el equipo de acceso CHACCARC01 están activos y permiten tener servicios L3VPN, como se observa en la Figura 90.

```
junos_space@CHACCARC01> ping routing-instance gesmov1 10.64.44.67
movlte:
  Type: vrf                State: Active
  Interfaces:
    ge-0/0/0.1415
  Route-distinguisher: 28006:605003
  Vrf-import: [ __vrf-import-movlte-internal__ ]
  Vrf-export: [ __vrf-export-movlte-internal__ ]
  Vrf-import-target: [ target:28008:605003 ]
  Vrf-export-target: [ target:28008:605003 ]
  Tables:
    movlte.inet.0
```

Figura 90. Vrf movlte para servicios L3VPN - CHACCARC01

El detalle de la conectividad para el servicio L3VPN hacia el core de 4G se encuentra operativo y no existen perdida de paquetes, como se observa en la Figura 91.

```
junos_space@CHACCARC01> ping routing-instance movlte 10.64.44.67 size 1600
PING 10.64.44.67 (10.64.44.67): 1600 data bytes
1608 bytes from 10.64.44.67: icmp_seq=0 ttl=61 time=2.005 ms
1608 bytes from 10.64.44.67: icmp_seq=1 ttl=61 time=1.973 ms
1608 bytes from 10.64.44.67: icmp_seq=2 ttl=61 time=2.011 ms
1608 bytes from 10.64.44.67: icmp_seq=3 ttl=61 time=1.998 ms
1608 bytes from 10.64.44.67: icmp_seq=4 ttl=61 time=2.019 ms
^C
--- 10.64.44.67 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.973/2.001/2.019/0.016 ms
```

Figura 91. Ping hacia el EPC - CHACCARC01

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

En base a los conceptos que conforman un sistema LTE y la arquitectura IP-RAN propuesta basada en seamless MPLS, se concluye que la prueba realizada de ping con carga para los datos hacia el core de 4G demuestran que, existe un óptimo transporte del servicio 4G ya que se está garantizando MTU mayores a 1500 bytes, lo cual es un requisito fundamental para trabajar con redes IP/MPLS y LTE.

El estudio realizado a la situación actual del servicio de datos móviles en el Ecuador permitió elaborar la arquitectura física y lógica de la red IP-RAN para la provincia de Cuenca. En la arquitectura física se detalla el dimensionamiento a nivel del throughput que los equipos de borde y acceso deberán manejar en el año 2023, además se consideró un 20% de sobredimensionamiento en todos los equipos para garantizar un mayor tiempo de vida útil de los mismos.

Se definió la segmentación de la red en regiones de acceso y agregación las cuales forman parte de un mismo sistema autónomo pero basado en un dominio IGP independiente, esto se logró mediante el uso de ISIS en distintos niveles para cada región. La región de acceso tiene un entorno de enrutamiento independiente basado en ISIS L2 lo cual garantiza un nivel de escalabilidad en el orden de miles de nodos en el acceso (fundamental para implementaciones basadas en LTE).

La simulación permitió demostrar una óptima conectividad al trabajar con protocolos ya existentes en la industria, pero bajo un esquema seamless MPLS. El uso de ISIS para el establecimiento de las sesiones, LDP como protocolo de distribución o transporte y bgp-lu para la comunicación con el core, todos bajo un esquema Seamless, permite incrementar la escalabilidad

de la red al limitar la interacción en condiciones normales y en caso de falla únicamente a cada región.

Los detalles técnicos necesarios para la instalación fueron descritos para cada equipo de la arquitectura IP-RAN, se expusieron diagramas de distribución del equipamiento diferenciando entre ambientes outdoor e indoor, además se facilitó diagramas de conexión eléctrica en base a un esquema de redundancia a nivel de fuentes de energía de cada equipo y especificando el número de conexiones a tierra necesarias dependiendo del tipo de chasis de cada equipo.

El presupuesto del costo de la solución abarcó costo de los equipos, linecards, dos diferentes tipos de tarjetas MIC y dos tipos de SFP de acuerdo a la cantidad de equipos y elementos necesarios para la implementación de la arquitectura propuesta.

El uso de seamless MPLS para la segmentación de la red en múltiples regiones permite reducir el número de entradas en las tablas de enrutamiento RIB y FIB. Reducir la cantidad de LSP LDP en la red. Simplificar el crecimiento de la red, ya que la integración de nuevas regiones no requiere compatibilidad a nivel de IGP/LDP entre las regiones. Las nuevas regiones únicamente requieren compatibilidad a nivel de BGP-LU esto simplifica el troubleshooting ya que los problemas son restringidos a una región y no son propagados a toda la red, de esta manera reduciendo considerablemente la cantidad de recursos a nivel de hardware requeridos por cada nodo o dispositivo, lo que impacta directamente en la escalabilidad de la red.

5.2. Recomendaciones

Es recomendable habilitar el protocolo RSVP en cada interfaz de tal forma que si futuras arquitecturas requieran señalizar LSP con consideraciones o restricciones como ancho de banda únicamente se debería configurar los LSP.

Previo a la puesta en producción y despliegue del diseño propuesto, se recomienda definir securing routing engine, así se establecen los protocolos que el proveedor de servicio considera confiables, con el objetivo de descartar tráfico malicioso buscando acceso a la red, actualizaciones no deseadas de protocolos de enrutamiento ó tráfico ilegitimo que excede un Ancho de Banda.

Para realizar balanceo de tráfico, con el objetivo de utilizar eficientemente la infraestructura de red, se recomienda habilitar el enrutamiento de múltiples rutas de igual costo (ECMP). Cuando existe ECMP permite instalar todas las rutas activas para alcanzar un destino en el packet forwarding engine (PFE) y balancear el tráfico por flujo.

En una implementación real con Junos por seguridad se recomienda usar el protocolo SSH para el acceso remoto a los dispositivos y para la transferencia de archivos se recomienda el uso del protocolo FTP. Ninguno de estos servicios está habilitado por defecto en los dispositivos razón por lo cual deben ser activados.

Cuando se presenta un problema en ambientes no controlados, se recomienda consultar los mensajes de Syslog, estos brindan información necesaria para el origen de los problemas. Para un mejor análisis Junos permite la definición de archivos personalizados sobre la información de Syslog que se desea recolectar, todos estos mensajes se guardan en /var/log. En caso de usar Syslog personalizados, en cada uno es recomendable definir una cantidad máxima de archivos y un peso máximo por archivo, esto evita saturar la memoria interna del dispositivo, que puede desembocar en la perdida a nivel de servicios y gestión remota. Se pueden usar un servidor externo para enviar la información una vez que sobrepase el número máximo de archivos.

Se recomienda configurar en todos los equipos Juniper la zona horaria del país al que pertenezcan y que además estén sincronizados con un servidor de NTP, así se mantiene una base

de tiempo consistente, la cual es muy útil para la depuración, seguimiento de eventos y análisis de mensajes de Syslog.

Para la implementación y despliegue de la topología se recomienda que todos los dispositivos del Mobile Bakchaul sean monitoreados a través de SNMP por otros sistemas de gestión, con el propósito de registrar configuraciones, logs, estado a nivel de CPU, temperatura y demás características críticas del sistema.

Para realizar un presupuesto más aproximado se recomienda tomar en cuenta valores de licenciamiento. El uso de licencias aplica únicamente en caso de existir un sistema de gestión o administración, su costo es por funcionalidades y por el número de puertos a monitorear. El uso de licencias no es necesario en caso de que no se utilicen sistemas de gestión o monitoreo.

BIBLIOGRAFÍA

ARCOTEL. (Junio de 2019). *Agencia de Regulación y Control de las Telecomunicaciones.* Obtenido de http://www.arcotel.gob.ec/servicio-movil-avanzado-sma_3/

Ayala, C. (2011). *Estudio y diseño de una red de transporte IP RAN para voz y datos para redes de telefonía celular de cuarta generación en el Ecuador.* ESPE.

Baoya, Z. (12 de 09 de 2016). *Key Technologies of IP RAN*. Obtenido de ZTE: https://www.zte.com.cn/global/about/magazine/zte-technologies/2016/5/en_709/460445.html

Castillo, C. (2017). *Dimensionamiento de un clúster de red LTE para brindad cobertura e la zona comercial de la ciudad de Loja.* Quito: Pontificia Universidad Católica del Ecuador.

Cisco. (2009). *CCNA 2 Exploration 4.0.* Universidad Nacional de Ingeniería.

Cisco. (2020). *IP Routing: ISIS Configuration Guide, Cisco IOS Release 15M&T.* San Jose: Cisco Systems.

Douglas, C. (2009). *Computer Networks and Internets.* New Jersey: Prentice Hall.

Fujitsu Network Communications. (2017). *4G Impacts to Mobile Backhaul.* Texas: Fujitsu.

Ghein, L. D. (2007). *MPLS Fundamentals.* Indianapolis: Cisco.

Gross, P. (1992). *RFC 1371.* Elmsford, NY: IESG.

Huawei. (2019). *Configuration Guide - MPLS.* Shenzhen: Huawei Tecnologies CO. LTD.

INEC. (2019). *Instituto Nacional de Estadistica y Censos.* Obtenido de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Poblacion_y_Demografia/Proyecciones_Poblacionales/proyeccion_cantonal_total_2010-2020.xlsx

Jaramillo, M. (2015). *Implementación de Red Móvil con Tecnología 4G LTE.* Guayaquil: ESPOL.

Jiménez, L. (2013). *Evolución de la red de transmisión de acceso móvil desde TDM a ALL-IP.* Universidad Politécnica de Valencia.

Juniper Networks. (10 de Junio de 2018). *IS-IS Overview*. Obtenido de Juniper Networks TechLibrary: https://www.juniper.net/documentation/en_US/junos/topics/concept/is-is-routing-overview.html

Juniper Networks. (06 de 03 de 2019). *Autonomous-System*. Obtenido de Juniper Networks TechLibrary: https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/autonomous-system-edit-routing-options.html

Juniper Networks. (25 de Diciembre de 2019). *BGP Overview*. Obtenido de https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-overview.html

Mills, D. (1984). *RFC 904.* IETF.

Molenaar, R. (13 de Agosto de 2015). *Introduction to MPLS*. Obtenido de Network Lessons: https://networklessons.com/mpls/

Molenaar, R. (11 de Mayo de 2017). *Introduction to IS-IS*. Obtenido de Network Lessons: https://networklessons.com/cisco/ccie-routing-switching-written/introduction-to-is-is

Molenaar, R. (22 de Mayo de 2017). *IS-IS DIS and Pseudonode*. Obtenido de Network Lessons: https://networklessons.com/cisco/ccie-routing-switching-written/is-is-dis-and-pseudonode/

MPIRICAL. (s.f.). *IPRAN - IP Radio Access Network*. Obtenido de MPIRICAL: https://www.mpirical.com/glossary/ipran-ip-radio-access-network

Noction. (17 de Octubre de 2018). *BGP Labeled Unicast (BGP-LU)*. Obtenido de Noction network intelligence: https://www.noction.com/blog/bgp-labeled-unicast-bgp-lu

Paredes, J. (2016). *Optimización de la red de acceso IP para interconectar nodos LTE (IP RAN) hacia el core de servicios de la plataforma de datos móviles.* PUCE.

Rosen, R. &. (2001). *RFC 3107.* IETF.

Sobanski, J. (19 de Abril de 2018). *LTE y más allá: la evolución de arquitecturas de red móvil IP jerárquicas a plana*. Obtenido de https://john.soban.ski/lte-and-beyond-the-evolution-to-a-flat-ip-architecture.html

Tanenbaum. (2012). *Redes de Computadoras.* PEARSON.

Vega, V. (2016). *Diseño de una red IP-RAN para el transporte de tráfico de datos de una red de telefonía celular de cuarta generación con tecnología LTE para un operador móvil, en la ciudad de Machala, provincia de El Oro, Ecuador*. Universidad Católica - Santiago de Chile.

Villegas, J., Villegas, O., & Gonzales, V. (2012). Semiología de los signos vitales: Una mirada novedosa a un problema vigente. *Archivos de Mecidina*, 221-240.

yateBTS. (s.f.). *LTE Architecture Concepts*. Obtenido de yateBTS: https://yatebts.com/documentation/concepts/lte-concepts/