ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROPUESTA DE UNA SOLUCIÓN IP-RAN PARA LA AMPLIACIÓN DE LA RED DE TRANSMISIÓN DE CUARTA GENERACIÓN PARA MEJORAR EL SERVICIO DE DATOS MÓVILES DE UNA OPERADORA DE TELEFONÍA CELULAR EN LA CIUDAD DE RIOBAMBA

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

RICHARD XAVIER JÁCOME GUANOLUISA
richard.jacome@epn.edu.ec

DIRECTOR: ING. ANDRÉS FERNANDO REYES CASTRO, MSc.
andres.reyes@epn.edu.ec

CODIRECTOR: ING. CARLOS ALFONSO HERRERA MUÑOZ, MSc.
carlos.herrera@epn.edu.ec

Quito, enero 2019

AVAL

Certificamos que el presente trabajo fue desarrollado por Richard Xavier Jácome Guanoluisa bajo nuestra supervisión.

ING. ANDRÉS REYES, MSc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

ING. CARLOS HERRERA, MSc.
CODIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo Richard Xavier Jácome Guanoluisa declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

RICHARD XAVIER JÁCOME GUANOLUISA

DEDICATORIA

Este trabajo lo dedico principalmente a Dios, quién siempre ha sido mi apoyo y fortaleza en todo momento.

A mis padres Nancy y Guido, quiénes me enseñaron que con esfuerzo y sacrificio todo se puede lograr.

A mis abuelitos Delia y Lizardo, por quererme como si fuera su hijo.

A mi tía Evelin, quién siempre me ha apoyado con sus palabras y comprensión.

A mis hermanos Cristian y Danny, por estar siempre unidos.

A mis amigas y amigos, por ser mi segunda familia.

AGRADECIMIENTO

Al terminar esta etapa de mi vida quiero agradecer a Dios por ser el apoyo y fortaleza en momentos de dificultad y debilidad, sin él esto no habría sido posible.

Gracias mami y papi, por ustedes tuve la fortuna de estudiar, por su dedicación y esfuerzo. Ustedes son las personas más fuertes que conozco, lo que han demostrado me ha servido de ejemplo para ser un hombre que no claudica y va siempre hacia adelante sin olvidar como fue el camino.

Un inmenso agradecimiento para mis abuelitos, quiénes hicieron que el amor de padre y madre siempre estén presentes, que dicha es verlos reír y hablar con nostalgia de sus recuerdos.

Evelin te agradezco por ser la hermana que nunca tuve, siempre apoyándome, gracias por enseñarme que todo en la vida tiene su lado bueno.

Gracias Cristian y Danny hacen que la palabra familia tenga significado.

Por ayudarme y guiarme en este trabajo, le agradezco al MSc. Andrés Reyes, quién puso interés y dedicación para que yo pueda lograr culminar este proceso.

Finalmente, pero no menos importante agradezco al resto de mi familia, amigas y amigos, quiénes me brindaron su apoyo. Sin ustedes no pude haber logrado esto.

ÍNDICE DE CONTENIDO

RESUMEN

En este Trabajo de Titulación inicialmente se realiza el estudio de la situación actual del servicio de datos móviles, de acuerdo con las operadoras y tecnologías desplegadas en el país mediante esta información, la cantidad de usuarios LTE en el país y en la ciudad de Riobamba se estima la capacidad que deberá soportar la IP-RAN.

Para obtener una solución IP-RAN adecuada se analizan requerimientos técnicos como capacidad de los puertos, capacidad de procesamiento, protocolos y tipos de medio de transmisión, mediante el cumplimiento de estos requerimientos se elige al fabricante de los equipos IP-RAN.

La IP-RAN diseñada consta de 26 *routers* dispuestos en una topología HRT (*Hierarchical Ring Tree*), en la cual 21 *enodeB* están enlazados con *routers* del nivel de acceso, estos *routers* se conectan a un anillo de agregación IP-RAN formado por 4 *routers* del nivel de agregación y un *router* del nivel de borde que permite la integración de la IP-RAN con una red de transporte MPLS.

Los *enodeB* alcanzan la red troncal LTE y el sitio de gestión IP-RAN mediante servicios L3VPN (*Level 3 Virtual Private Network)* implementados en los *routers* de la nube MPLS y *routers* del anillo de agregación IP-RAN. Este entorno de red es simulado y comprobado en el software GNS3.

Finalmente, se realiza una revisión de los sitios donde se podrán desplegar los equipos y se plantea un esquema básico de instalación para los tres tipos de *routers* de la IP-RAN.

PALABRAS CLAVE: transporte, IP-RAN, LTE, L3VPN, *routers.*

ABSTRACT

This final career project presents the design of an IP-RAN solution that will allow communication between the enodeBs and the backbone of a LTE network in the city of Riobamba.

In the theoretical framework, the fundamentals of LTE (Long Term Evolution), IP-RAN (Internet Protocol - Radio Access Network), MPLS (Multi-Protocol Label Switching) and Routing Protocols are described to understand of the transport information.

Before choosing IP-RAN equipment, in order to approximate the capacity requirement that must be supported by the IP-RAN, a traffic analysis is performed according to the LTE users in Riobamba, and technical requirements are established for the IP-RAN adaptation to current and future services. Based on these requirements a comparison between two manufacturers is made and then one is chosen for the network.

The physical IP-RAN design consists on the geographical location of the equipment in the city of Riobamba, including node distribution according to the network hierarchy, establishment of identification nomenclature according to the site and definition of links between the IP-RAN routers.

The logical IP-RAN design considers the IP addressing and routing criteria to provide L3VPN (Level 3 Virtual Private Network) services in the LTE network. Then a simulation of the proposed network is executed, and the network operation is verified.

According with the actual status of the sites for the deployment of IP-RAN equipment, a basic installation proposal is made.

Finally, conclusions and recommendations are presented.

KEYWORDS: transport, IP-RAN, LTE, L3VPN, routers.

1. INTRODUCCIÓN

La demanda creciente del servicio de datos móviles ha creado la necesidad de mejorar la capacidad y cobertura que las operadoras de telefonía celular ofrecen mediante tecnologías como: GSM (*Global System for Mobile Communications*), UMTS (*Universal Mobile Telecommunications System*), HSPA+ (*High Speed Packet Access*) y LTE (*Long Term Evolution*) [1]. Para lograr satisfacer la capacidad requerida por las tecnologías móviles, se han propuesto las soluciones IP-RAN (*Internet Protocol – Radio Access Network*) que permiten el acceso a los servicios móviles.

En este capítulo se presenta el marco teórico que describirá de manera general el sistema LTE, la arquitectura IP-RAN, los protocolos de enrutamiento y la arquitectura MPLS (*Multi-Protocol Label Switching*), estos conceptos permitirán la comprensión del funcionamiento de la red IP-RAN, la cual brindará acceso a los servicios de la red de *Core*.

1.1 Objetivos

El objetivo general de este Proyecto Técnico consiste en:

- Proponer una solución IP-RAN para la ampliación de la red de transmisión de cuarta generación para mejorar el servicio de datos móviles para una operadora de telefonía celular móvil en la ciudad de Riobamba.

Los objetivos específicos de este Proyecto Técnico son:

- Describir conceptos teóricos acerca del funcionamiento de LTE, redes IP-RAN, MPLS, Protocolos de Enrutamiento.
- Analizar la situación actual del servicio de datos móviles en Riobamba.
- Definir los equipos de red a utilizar en la solución IP-RAN y sus requerimientos técnicos.
- Diseñar y simular la topología de la red IP-RAN en la ciudad de Riobamba.
- Determinar la ubicación geográfica y física de los equipos con los implementos necesarios para su instalación.

1.2 Alcance

Se analizará el tipo de equipos (*routers*) que la red de acceso necesitará para disponer de enlaces con suficiente capacidad para abastecer del servicio de datos según los requerimientos que las tecnologías como: UMTS, HSPA+ y LTE demandan. Realizando un análisis de la capacidad que cada tecnología requiere se logrará obtener el tipo de

puertos que deberán disponer los *routers*. Con la información de las especificaciones técnicas de los equipos de los diferentes fabricantes se procederá a hacer una diferenciación entre ellos y se propondrá uno para realizar el diseño de la red IP-RAN.

De acuerdo con los equipos escogidos se realizará el diseño físico, en el cual se indicará la ubicación geográfica de los equipos haciendo uso de *Google Earth* que permitirá diferenciar los sitios, el número de equipos siguiendo una topología jerárquica, la nomenclatura de los equipos según su ubicación, los medios de transmisión a usar. También se realizará un diseño lógico, en el cual se hará el direccionamiento IP y la asignación de puertos de los equipos para las transmisiones según sea el caso.

Por medio de un software de simulación, se evaluarán los escenarios de despliegue y la topología de conexión de los equipos que será HRT (*Hierarchical Ring Tree*), debido a que las soluciones IP-RAN se basan en dicha topología, ya que brinda altas prestaciones en capacidad, disponibilidad y desempeño. Según los requerimientos técnicos de los equipos que se escogerán los protocolos necesarios para obtener conectividad en la red.

Finalmente, se revisarán los sitios en los cuales se instalarán los equipos, se realizará un análisis del espacio físico para proceder a la ubicación de los equipos en las correspondientes unidades de rack según sea el caso, ya que pueden ser ubicados en *Mini-Shelters* (ambientes *OUTDOOR*) o Racks ubicados en cuartos de equipos (ambientes *INDOOR*).

1.3 Marco Teórico

1.3.1 Sistema LTE

LTE marca el punto de inicio hacia 4G, ya que es una tecnología que permite el transporte de datos con el soporte del protocolo IP. El desarrollo de LTE permite obtener mejoras como: el aumento de la velocidad de transmisión (100 Mbps en *downlink* y 50 Mbps en *uplink*) y la reducción del retardo. Además, la característica de interoperabilidad que posee LTE, admite que sistemas 3GPP y sistemas no 3GPP accedan a sus servicios [2].

3GPP usó el término SAE (*System Architecture Evolution*) para referirse a la red troncal denominada EPC (*Evolved Packet Core*) o *Evolved 3GPP Packet Switched Domain* que en conjunto con la red de acceso E-UTRAN forman la arquitectura EPS (*Evolved Packet System*), todos estos componentes de LTE soportan mecanismos de conmutación de paquetes, mediante despliegue del protocolo IP. LTE tiene su primera especificación incluida en el *Release 8* del 3GPP, la cual mejora a UMTS [2].

LTE ofrece transferencia de paquetes IP, entre el equipo de usuario y una red externa, mediante el servicio portador EPS (*EPS Bearer Service*) que soporta calidad de servicio (*Quality of Service* QoS), así se pueden adaptar los parámetros de transmisión para brindar mejor servicio a los usuarios [2].

La distribución de los elementos de la arquitectura LTE permiten verificar la diferenciación entre la red de acceso (E-UTRAN), que permite que los clientes puedan alcanzar los servicios ofertados por LTE, y la red de *Core* (EPC), que mediante interfaces permite la interconexión entre sistemas 3GPP y sistemas no 3GPP [2], como se muestra en la Figura 1.1.

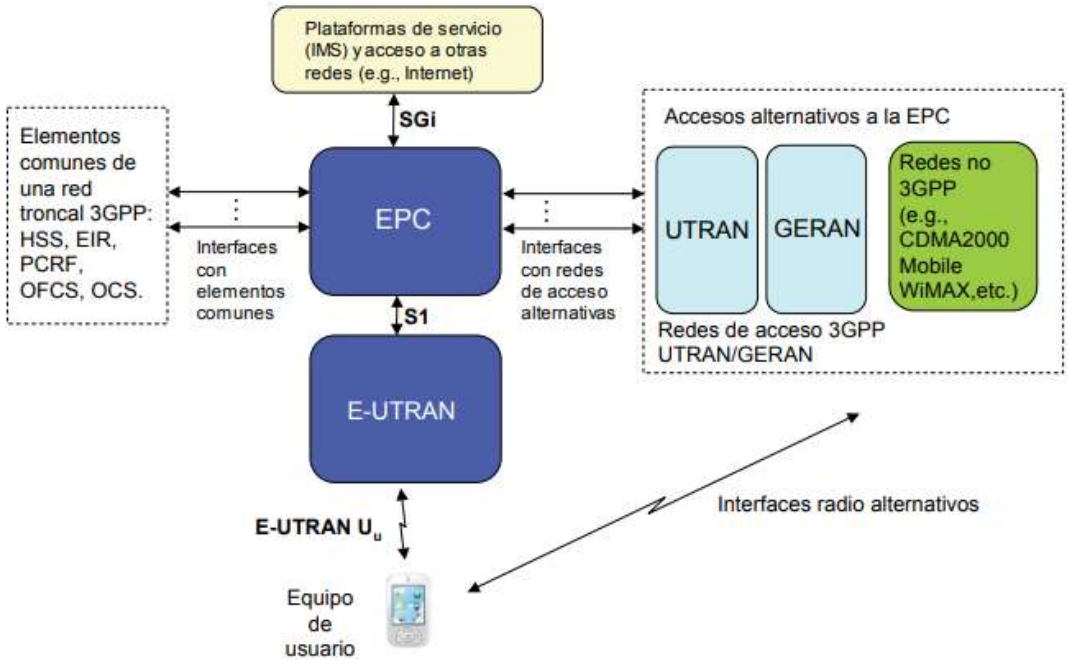

Figura 1.1. Estructura de la Arquitectura de un Sistema LTE [2].

La interconexión de los equipos físicos de la red troncal EPC como de la red de acceso E-UTRAN, se realiza mediante tecnologías de red basadas en IP. La red física que se utiliza para interconectar los diferentes equipos de una red LTE, se denomina comúnmente como red de transporte, que es una red IP convencional, la cual va a permitir la interconexión de otros equipos de capa 3 del modelo OSI (*Open System Interconnetion*) que implementan funciones diferentes del estándar 3GPP [2].

1.3.1.1 E-UTRAN (*EVOLVED UNIVERSAL TERRESTRIAL RADIO ACCESS NETWORK*)

La red E-UTRAN está compuesta por estaciones base, denominadas *Evolved Node B* (*eNB*). E-UTRAN establece una red de acceso, cuyo fin es brindar conectividad entre equipos de usuario (UE *User Equipment*) y la red troncal EPC, para lo cual se necesita

un sistema de comunicación conformado por tres interfaces[1]: E-UTRAN Uu, S1 y X2 [2], como se indica en la Figura 1.2.

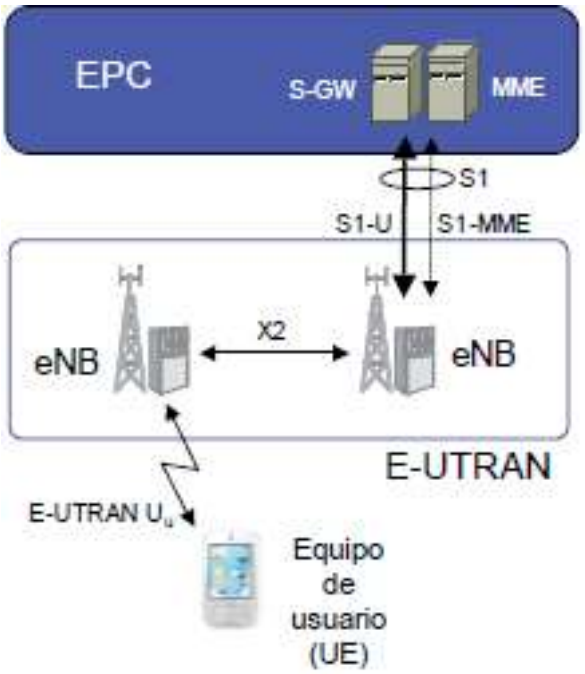

Figura 1.2. Interfaces de la E-UTRAN [2].

1.3.1.2 INTERFACES E-UTRAN

1.3.1.2.1 **INTERFAZ DE RADIO (Uu):** Esta interfaz también se la conoce como LTE Uu o simplemente interfaz de radio LTE, la cual permite la transmisión de información por el canal de comunicaciones es de tres tipos: señalización de control, paquetes IP e información de control entre el equipo de usuario (UE) y el eNB. La interfaz de radio utiliza el acceso múltiple por división de frecuencia ortogonal (OFDMA) en *downlink*, mientras que en *uplink* utiliza acceso múltiple por división de frecuencia con portadora simple (SC-FDMA), en la capa física presenta esquemas de modulación como: QPSK, 16 QAM y 64 QAM [2].

Los parámetros utilizados por OFDMA en LTE permiten que tenga flexibilidad en el ancho de banda desde 1.4 MHz hasta 20 MHz, siendo la separación entre subportadoras de 15 KHz para *donwlink* y *uplink* [2].

1.3.1.2.2 **Interfaz S1**: Mediante esta interfaz se realiza la conexión entre el eNB y la red troncal EPC, para que el eNB se conecte con dos nodos diferentes

[1] Interfaz: Permite la interconexión y el envío de tráfico y señalización entre el terminal móvil y las estaciones base [2].

de la EPC. La interfaz S1 se divide en dos subinterfaces, esta separación ayuda a realizar un mejor dimensionamiento de los recursos que se utilizan en la transmisión de información [2].

Subinterfaz S1-U: Esta subinterfaz es utilizada en el plano de usuario, cuyos protocolos se usan para enviar información de usuario entre la E-UTRAN y la EPC. La entidad de red que procesa el plano de usuario se denomina: *Serving Gateway*, S-GW [2].

Subinterfaz S1-MME: La funcionalidad de esta subinterfaz se basa en el plano de control, que mediante su conjunto de protocolos permite gestionar la operación de la interfaz o entidad de red correspondiente (*Mobility Management Entity*, MME) [2].

1.3.1.2.3 **Interfaz X2:** Esta interfaz es usada para la conexión entre eNB, en la cual las interferencias sean pocas. La interfaz X2 permite gestionar: el uso de los recursos de radio, el proceso de *handover* de manera eficiente, esta gestión se lleva a cabo mediante el intercambio de mensajes de señalización [2].

1.3.1.3 eNB (*Evolved NodeB*)

La principal función que un eNB realiza es la gestión de los recursos de radio, ya que cumple con el control de admisión de servicios portadores de radio, control de movilidad, asignación dinámica de recursos de radio, control de interferencias entre eNB, control de medidas de los equipos de usuario. Además, el eNB puede seleccionar dinámicamente la entidad MME que se encuentra en la EPC [2].

Mediante el servicio portador de radio (*Radio Bearer*, RB) el eNB transmite información formando paquetes IP desde o hacia los equipos de usuario, mientras que para controlar la operación de la interfaz radio se hace uso de mensajes de señalización [2].

1.3.1.4 EPC (*EVOLVED PACKET CORE*)

Esta arquitectura de red está diseñada para soportar conectividad IP, no solo permite integrar la red de acceso E-UTRAN y ofrecer mayor capacidad que otras tecnologías, sino que además admite el acceso a otras redes tanto 3GPP (UTRAN y GERAN) como no 3GPP (Mobile WiMAX, CDMA2000, etc) [2].

La red troncal EPC es conformada por tres entidades de red: MME (*Mobility Management Entity*), S-GW (*Serving Gateway*) y P-GW (*Packet Data Network Gateway*), y la base de datos HSS (*Home Subscriber Server*) [2].

1.3.1.4.1 MME: Este elemento de red controla los equipos de usuario, ya que puede acceder a la información de los usuarios autorizados para conectarse a la E-UTRAN, a través de la HSS, la MME también cumple funciones como señalización, seguridad en NAS (*Non Stratum Access*) entre la red de *Core* y el terminal de usuario, selección de entidades S-GW y P-GW, gestión de movilidad cuando el usuario está en modo idle, autenticación de usuarios mediante los registros que dependen de la ubicación geográfica del equipo de usuario, gestiona la localización de los usuarios registrados en la red [2].

1.3.1.4.2 P-GW: Esta entidad de red se encarga de conectar redes externas o plataformas de servicio (IMS) con la EPC, es decir, la interconexión de la EPC con redes externas. Además, P-GW realiza el direccionamiento IP de los equipos de usuario, usa mecanismos para controlar los parámetros de calidad de servicio de las conexiones de red establecidas, filtra paquetes, realiza una conexión interna con el S-GW cuando ambas entidades pertenecen al mismo operador, proporciona servicio de *roaming* cuando la S-GW se encuentra en otra red [2].

1.3.1.4.3 S-GW: Este *gateway* permite el encaminamiento de los paquetes IP, gestiona la calidad del servicio en el transporte de la información, sirve de punto de anclaje cuando el equipo de usuario está en movimiento. El equipo de usuario debe estar asociado a solo un S-GW [2].

1.3.1.4.4 HSS: Este servidor contiene la base de datos de suscripción del usuario, puede ser consultada y modificada por elementos de red que brindan servicios de conectividad, como es el caso de la entidad MME que accede a la HSS para la gestión de usuarios. La información contenida en el HSS permite: gestionar la movilidad en redes diferentes a LTE, autenticación y autorización para el acceso de los usuarios a través de credenciales. La información que posee la HSS también es necesaria para la provisión de los servicios según acuerdos establecidos en contratos [2].

1.3.1.4.5 PCRF (*Policy and Charging Rules Function*): Para autorizar los servicios portadores ofrecidos por LTE es necesaria la entidad PCRF, que gestiona la calidad de servicio y toma políticas para controlar el tráfico. PCRF controla la facturación por flujo de datos a través de las entidades OFCS (*Offline Charging System*) y OCS (*Online Charging System*) que se conectan al P-GW [2].

En la Figura 1.3. se muestra la arquitectura del sistema EPC, cuyos elementos proveen conectividad IP entre los equipos de usuario, que acceden por la E-UTRAN, y las redes externas. Se puede realizar una diferenciación en la EPC, ya que el plano de usuario basa su funcionamiento en el P-GW y el S-GW, mientras que el plano de control se centraliza en la base de datos MME [2].

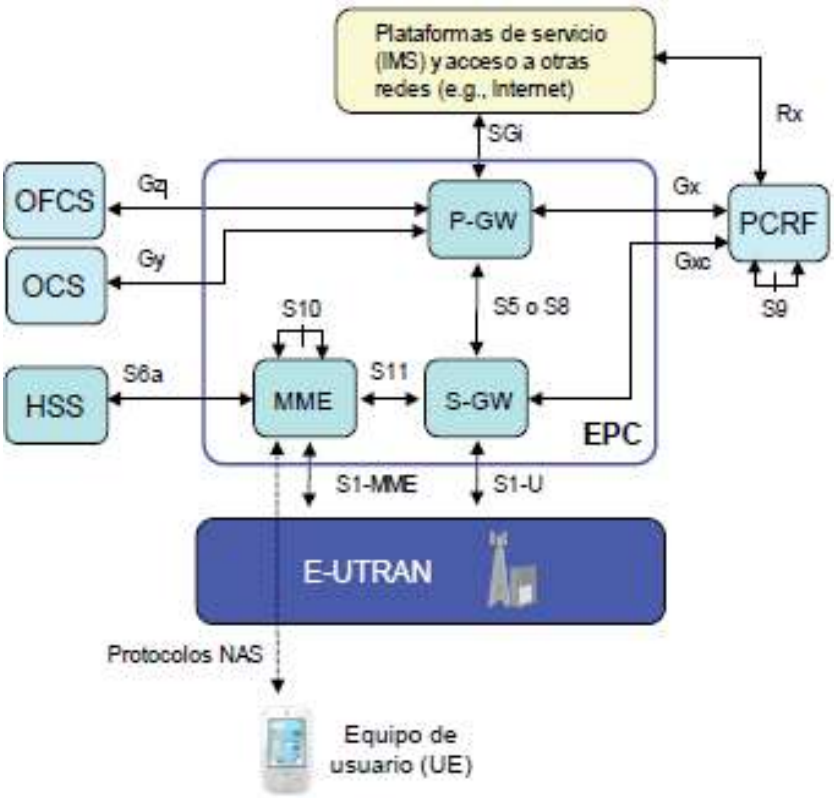

Figura 1.3. Distribución de la Red de *Core* EPC [2].

1.3.1.5 Equipo de Usuario (UE)

El equipo de usuario (UE) permite que los usuarios accedan a los servicios ofertados por las operadoras móviles, siendo la interfaz de radio el medio que utiliza el equipo de usuario para conectarse a la red LTE. El equipo está formado por: el módulo de subscripción del usuario (SIM/USIM) y el equipo móvil (*Mobile Equipment* ME) conformado por dos entidades funcionales como son el terminal móvil (*Mobile Terminal*, MT) y el equipo terminal (*Terminal Equipment* TE) [2], como se puede apreciar en la Figura 1.4. y, además, se encuentra que un equipo de usuario puede permitir al cliente acceder a servicios brindados por tecnologías GSM, UMTS y/o LTE.

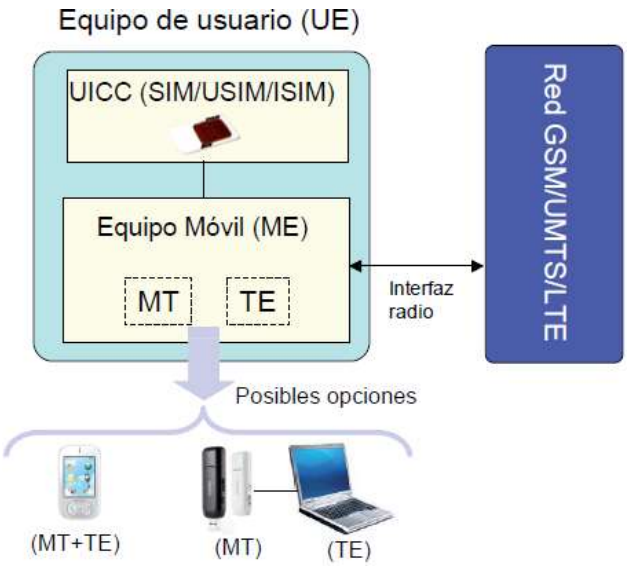

Figura 1.4. Estructura del Equipo de Usuario (UE) [2].

1.3.2 Arquitectura IP-RAN

Para brindar conectividad con la posibilidad de expansión a nuevos clientes en una red celular, se debe proponer una solución que permita cubrir la demanda de servicios móviles, tanto para datos como para control, por lo que una Red de Radio Acceso (RAN) es una buena solución, ya que permite cubrir los requerimientos de ancho de banda que los operadores de servicios móviles deben ofrecer a los usuarios [3].

Una variación de la RAN es la IP-RAN, cuya tecnología permite que redes de datos basadas en el protocolo IP puedan acceder a transmisiones de radiofrecuencia [3].

La IP-RAN se destina a la administración de la movilidad de los usuarios en tiempo y espacio. Esta red es dirigida por un operador, el cual puede proponer distintas políticas de funcionamiento ya sean de seguridad, calidad de servicio, entre otras; estos criterios de red deben ser dados tanto a nivel físico como lógico [4].

La interconexión de los dispositivos de la red IP-RAN no depende de la tecnología de radio, lo cual facilita la implementación de esta solución. La red de acceso IP-RAN debe permitir el acceso terrestre, inalámbrico o celular mediante estaciones base con soporte para tecnologías como 2G, 3G y 4G. Además, una IP-RAN presenta flexibilidad para bridar acceso a nuevas tecnologías, sin que el rendimiento de las tecnologías existentes sea afectado [4].

Entre los principales beneficios que una red IP-RAN ofrece se tiene: reducción del costo operacional al utilizar una infraestructura de transporte existente, permite la interoperabilidad de tecnologías 2G, 3G y 4G, ya que la IP-RAN puede brindar servicios

a través de cualquier red de acceso, posibilita la escalabilidad de la red, se pueden manejar velocidades de 1Gbps, por lo cual LTE y otras tecnologías son capaces de funcionar en la misma red, servicios de movilidad de usuario, seguridad, cifrado, sincronización, localización y calidad de servicio y enrutamiento de llamadas [5].

1.3.2.1 Capas, Etapas o Niveles de una IP-RAN

El sistema jerárquico de una red de acceso IP-RAN se divide en 3 capas:

1.3.2.1.1 ***Low*** **RAN Acceso:** Este nivel está constituido por equipos CSG (*Cell Site Gateway*), los cuales posibilitan que las estaciones base como *NodoB* o eNB se conecten con la red de *backhaul* y entre ellas, para realizar estas conexiones se pueden utilizar varios tipos de enlaces físicos como: microondas, cobre o fibra óptica. En esta capa se realiza la encapsulación de la información en paquetes que serán transportados por VPNs (*Virtual Private Networks*) de Capa 3 hacia el *Core* IP-RAN [6].

1.3.2.1.2 ***Mid*** **RAN Agregación:** Este nivel conformado por equipos ASG (*Agregation Site Gateway*) que permiten realizar la agregación de todo tipo de tráfico, especialmente de aquel proveniente del nivel de acceso, por lo que en esta etapa se deben diferenciar los servicios. Al igual que la capa de acceso los equipos ASG también pueden realizar el proceso de encapsulación de la información que será transportada por VPNs al nivel *High* RAN [6].

1.3.2.1.3 ***High*** **RAN *Core*:** Este nivel agrupa a equipos RSG (*Radio Site Gateway*), los cuales se encargan de concentrar el tráfico proveniente del nivel de agregación y lo encaminan hacia la red de *Core*, por lo que es la etapa más importante. Además, en esta capa se debe realizar la clasificación del tráfico, ya que la información se dirige a los distintos servidores de la red troncal. Los equipos de esta capa trabajan como *routers* de borde, ya que dirigen el tráfico hacia la red de *Core*, por lo que deben estar ubicados cerca de la EPC [6].

1.3.3 Protocolos de Enrutamiento

El proceso para enrutar, dirigir o enviar la información a una red destino por una línea de salida, se conoce como: enrutamiento. Los protocolos de enrutamiento se componen de un conjunto de reglas para que equipos de red como *routers* puedan intercambiar información de enrutamiento [7].

Enrutamiento Estático: Las rutas para alcanzar al destino deben ser configuradas manualmente por un administrador que además debe realizar el mantenimiento de las tablas de enrutamiento en cada cambio de topología, ya que en este tipo de enrutamiento no existen decisiones en base a mediciones del tráfico y topología actual [7].

Enrutamiento Dinámico: En este tipo de enrutamiento las mejores rutas son elegidas para llevar la información, las decisiones de enrutamiento se realizan automáticamente de acuerdo con los cambios de topología o tráfico de información [7].

Los protocolos de enrutamiento se encargan de crear y mantener las tablas de enrutamiento, las cuales contienen información de redes conocidas y puertos que se asocian a ellas. Para llevar a cabo este objetivo los protocolos de enrutamiento se clasifican en [7]:

1.3.3.1 Protocolos de Gateway Interior (IGP: *Interior Gateway Protocol*)

Estos protocolos distribuyen la información de enrutamiento entre los dispositivos de red, *routers*, dentro de un Sistema Autónomo (AS). Este tipo de protocolos presentan flexibilidad, ya que no necesita ser implementado fuera del sistema [8].

Sistema Autónomo: Es el conjunto de redes y *routers* bajo una misma administración que intercambian información haciendo uso de un mismo protocolo de enrutamiento, donde cada AS cuenta con su propio conjunto de reglas, políticas y un número de AS de 16 bits que los hace únicos, la asignación de estos números está dada por la IANA (*Internet Assigned Numbers Authority*) cuyos rangos son [8]:

- 0 ➔ Reservado
- 1-48127 ➔ Asignado
- 48128-54271 ➔ No Asignado
- 54272-64511 ➔ Reservado por la IANA
- 64512-65534 ➔ Libre para uso Interno
- 65535 ➔ Reservado

Los IGP se componen por 2 tipos de algoritmos de enrutamiento que son:

1.3.3.2.1 Algoritmo de Enrutamiento por Vector Distancia: También conocido como Algoritmo de Enrutamiento Bellman-Ford, este algoritmo proporciona la mejor dirección y distancia (vector) conocida al destino.

Para las tablas de enrutamiento los *routers* comparten periódicamente información con sus vecinos, por lo que los equipos de red, *routers*, no poseen la información completa de la topología de red. Entre los protocolos más representativos se tienen RIP v1/2 (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*) y EIGRP (*Enhanced Interior Gateway Routing Protocol*) [8].

1.3.3.2.2 Algoritmo de Enrutamiento por Estado de Enlace: El algoritmo de Dijkstra o SPF (*Shortest Path First*) es utilizado para encontrar los mejores caminos a todos los posibles destinos, en este tipo de algoritmo los *routers* conocen la información completa de la topología de red, por lo que este tipo de enrutamiento es el más usado. Entre los protocolos de enrutamiento por estado de enlace más representativos están: ISIS (*Intermediate System to Intermediate System*) y OSPF (*Open Shortest Path First*) [8].

ISIS: En este protocolo de enrutamiento la información se propaga para construir un mapa de conectividad de red completa en cada *router*, cuya información es usada para calcular la mejor ruta al destino. ISIS es multiprotocolo ya que soporta IPv4 e IPv6, lo cual permite que la red sea escalable [9].

El protocolo ISIS tiene algunos beneficios, ya que es el mayormente usado en ISPs (*Internet Service Providers*), por lo que es optimizado frecuentemente, también puede transportar información de varios protocolos de capa de red simultáneamente [9].

ISIS divide un dominio de enrutamiento [2] en uno o más subdominios, en el que cada subdominio se toma como un área y se le asigna una dirección de área. Un *router* es conocido como un Sistema Intermedio (IS *Intermediate System*) según terminología de OSI (*Open System Interconnection*). De acuerdo con el criterio de áreas se tienen diferentes niveles donde un IS (*router*) opera [9]. En la Figura 1.5. se pueden apreciar los tres niveles que tiene una Red implementada con IS-IS.

[2] Dominio de Enrutamiento: Es un conjunto de *routers* que se encuentran bajo una administración común, donde la información es intercambiada a través de un mismo protocolo de enrutamiento [8].

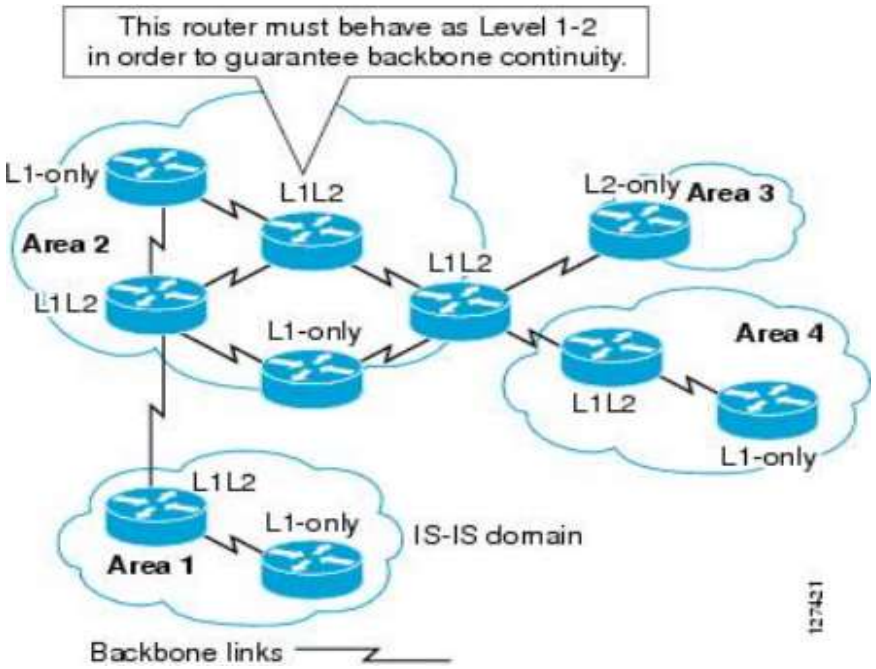

Figura 1.5. Dispositivos de red en un ambiente IS-IS [9].

1. **IS nivel 1(L1):** El *router* intercambia información de enrutamiento con otros *routers* de nivel 1 en una misma área [9].
2. **IS nivel 2 (L2):** El *router* intercambia información de enrutamiento con otros *routers* de nivel 2 que pueden estar en diferentes áreas nivel 1, siendo el conjunto de *routers* nivel 2 un Subdominio Nivel 2, el cual no debe ser dividido para trabajar en óptimas condiciones [9].
3. **IS nivel 1-2(L1L2):** El *router* intercambia información de enrutamiento hacia fuera y dentro de un área [9].

ISIS opera mediante 3 bases de datos las cuales son: la base de datos de vecinos llamada: LSP *Database* (LSPDB), la base de datos de topología y la tabla de enrutamiento (*Forwarding*) [9].

1.3.3.2 Protocolos de *Gateway* Exterior (EGP: *Exterior Gateway Protocol*)

Los protocolos de *Gateway* exterior sirven para realizar interconexión entre redes de más de un sistema autónomo (AS), esto mediante la compartición de información de enrutamiento entre los dispositivos de red de diferentes sistemas autónomos. Un EGP no conoce los detalles de la ruta hacia el AS destino, por lo que maneja menos información que un IGP. El protocolo EGP más usado es el BGP (*Border Gateway Protocol)*, detallado a continuación [7]:

1.3.3.2.1 BGP: Este protocolo es un tipo de protocolo de vector distancia, utilizado para interconectar redes, especialmente redes mediante dispositivos de aplicable con la arquitectura TCP/IP por lo que es ampliamente usado en Internet e ISPs [7].

BGP es multiprotocolo, ya que puede soportar IPv4 e IPv6. BGP permite el enrutamiento de paquetes IP entre diferentes AS que pueden utilizar diferente IGP, por lo que utiliza sesiones BGP inter-AS sobre conexiones TCP, donde se intercambian prefijos de rutas [7].

El algoritmo *Path*-Vector es utilizado por BGP para escoger las mejores rutas al destino almacenadas en tablas de enrutamiento, estas rutas están conformadas por una secuencia de números o identificadores de sistemas autónomos, donde el último número es el AS donde se encuentra el destino. Al guardar todos los identificadores de los sistemas autónomos por los que la información debe cruzar para llegar al destino se pueden detectar y evitar lazos de enrutamiento [7].

Sesión BGP: En una sesión BGP se lleva a cabo el proceso llamado *peering*, en el cual un AS comparte la información a otro AS de las redes que pueden ser alcanzadas. En una sesión BGP dos *routers* (*peers*) intercambian información de enrutamiento, donde un *router* puede estableces múltiples sesiones BGP [10].

Para propagar rutas entre sistemas autónomos se utilizan dos variantes del protocolo BGP los cuales son:

a) **iBGP (BGP interno):** Este tipo de protocolo es intradominio, ya que puede interconectar *routers* de borde en un mismo AS, ya que necesitan conocer las mismas rutas externas e internas [10].

b) **eBGP (BGP externo):** Esta variante de BGP es interdominio, porque permite el intercambio de información de enrutamiento entre *routers* de borde de distintos AS [10].

En la Figura 1.6. se puede apreciar cómo se diferencia eBGP con iBGP en una topología diseñada con BGP, donde si BGP se ejecuta entre dos AS diferentes es llamado BGP externo, mientras que cuando BGP se ejecuta entre *routers* de un mismo AS se denomina BGP interno [11].

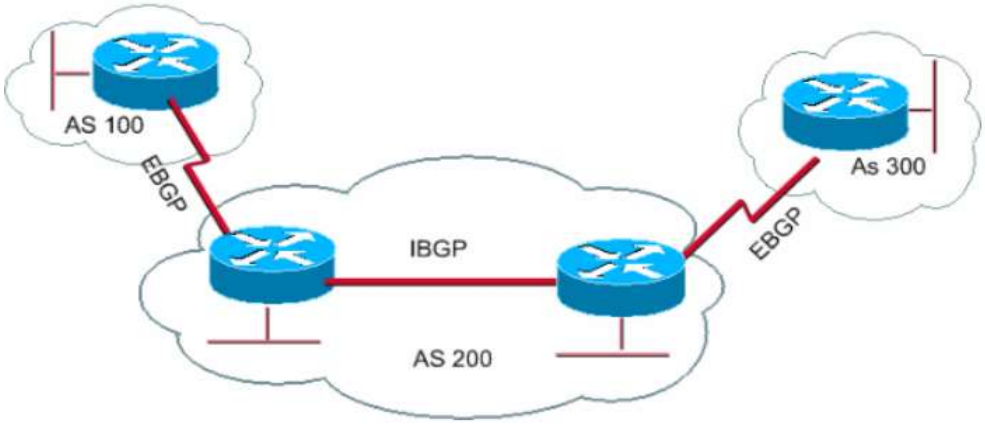

Figura 1.6. Dispositivos de Red en un ambiente BGP [11].

1.3.4 MPLS (*Multi-Protocol Label Switching*)

MPLS es una arquitectura de red que permite el transporte eficiente de la información, mediante la diferenciación y priorización del tráfico en una red de conmutación de paquetes [12].

Características:

- *Escalabilidad de Enrutamiento:* Mediante el uso de etiquetas se realiza la agregación de información de reenvío, con lo cual se pueden implementar VPNs (*Virtual Private Networks*) de capa 3 [12].
- *Flexibilidad al brindar servicios de enrutamiento:* El uso de etiquetas permite identificar el tráfico, dando la posibilidad de soportar calidad de servicio (QoS) [12].
- *Mejora el Rendimiento:* Con el uso de la ingeniería de tráfico se evita la congestión en la red [12].
- *Simplifica la integración de routers con otras tecnologías:* MPLS es una arquitectura independiente de capa 2 y 3 del modelo OSI, por lo que es multiprotocolo [12].

1.3.4.1 Componentes de MPLS

LER (*Label Edge Router*): *Routers* también conocidos como *routers* PE (*Provider Edge*) son *routers* ubicados en el borde de la nube MPLS que envían el tráfico que ingresa a la red MPLS, mediante un protocolo de señalización de etiquetas como LDP (*Label Distribution Protocol*) y distribuye el tráfico que sale de la nube MPLS a las distintas redes. Los paquetes de información en la nube MPLS se conmutan mediante

FEC (*Forwarding Equivalence Class*). Estos *routers* también se encargan de la asignación y retiro de etiquetas en la entrada o salida de la nube MPLS [12].

LSR (*Label Switched Router*): *Routers* también denominados como *routers* P (*Provider*) son *routers* que se distribuyen en el *Core* de la red MPLS, donde se encargan de la conmutación de los paquetes según su etiqueta, ya que los *routers* intercambian las etiquetas en cada salto de LSR, por lo que tienen características de gran velocidad [12].

FEC (*Forwarding Equivalence Class*): Este concepto trata de un grupo de paquetes pertenecientes a un mismo flujo de datos que comparten atributos como: el destino, la VPN y/o el servicio. Los paquetes que ingresan a la red son asignados a una FEC que se representa por una etiqueta en cada LSP (*Label Switched Path*) [13].

LSP (*Label Switched Path*): Es un camino unidireccional formado por una malla de túneles que son formados entre LERs. Una nube MPLS permite transmitir información en trayectorias mediante la conmutación de etiquetas en cada *router* [12].

1.3.4.2 Formato de la Cabecera MPLS

La cabecera MPLS tiene un valor fijo de 4 bytes, los cuales están compuestos por 4 componentes como se indica en la Figura 1.7.

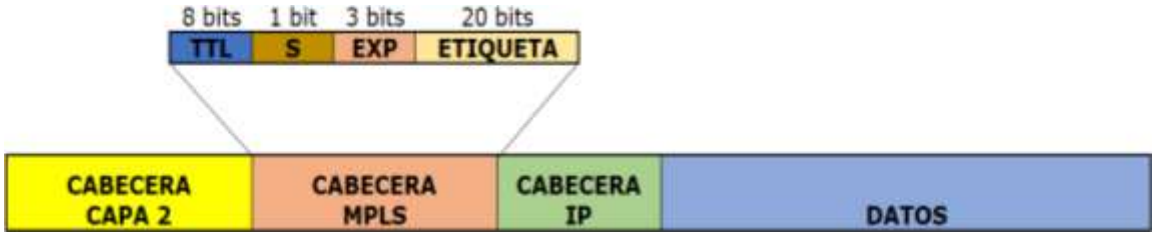

Figura 1.7. Estructura de la Cabecera MPLS

Etiqueta: Con una longitud de 20 bits que identifican una FEC, lo cual es válido en un par de *routers* ya que tiene validez local y se reemplaza en cada salto.

EXP: Con una longitud de 3 bits conocidos como “bits Experimentales” son utilizados para identificar la clase de servicio.

S (*Bottom of Stack*): Con una longitud de 1 bit que indica una pila de etiquetas que permite la implementación de VPN e Ingeniería de Tráfico.

TTL (*Time to Live*): Con una longitud de 1 byte, su valor decrementa en cada nodo para evitar lazos, si el valor de TTL es igual a 0 el paquete se excluye [13].

1.3.4.3 Funcionamiento de MPLS

Para revisar cómo se realiza la asignación e intercambio de etiquetas, se tienen en cuenta las funciones que los *routers* pueden desempeñar, las cuales son:

1. *Insertar (push):* Al ingreso a la red un LER agina e inserta una etiqueta en el paquete entrante mediante el proceso de enrutamiento IP [13].
2. *Intercambiar (swap):* La etiqueta de un paquete en la nube MPLS es intercambiada por otra en cada *router* LSR, este intercambio se basa según la información de la LFIB (*Label Forwarding Information Base*) [13].
3. *Remover (pop):* La etiqueta es removida del paquete a la salida de la nube MPLS o un salto antes. Además, se realiza la revisión del enrutamiento para encaminar el paquete al destino [13].

MPLS para implementación se divide en dos componentes que son:

1. *Componente de Control:* Este plano permite el intercambio de información de enrutamiento y etiquetas, ya que esta componente genera la base de datos de enrutamiento (RIB *Routing Information Base*) y la base de datos de etiquetas (LIB *Label Information Base*) [13].
2. *Componente de Envío:* Este plano realiza la conmutación de los paquetes que ingresan a la nube MPLS mediante las bases de datos generadas por la componente de control, para llevar a cabo esta función hace uso de dos tablas de información: FIB (*Forwarding Information Base*) utilizada para indicar la interfaz por la cual se reenvía el paquete y LFIB (*Label Forwarding Information Base)* usada para la conmutación de etiquetas [13].

1.3.4.4 Protocolos de Distribución de Etiquetas

La arquitectura MPLS no hace uso de un protocolo específico para la distribución de etiquetas, por lo que se tienen los siguientes como opciones: LDP (*Label Distribution Protocol*), CR-LDP (*Constrained-Based Routing* LDP), RSVP-TE (*Resource Reservation Protocol Traffic Engineering*) o extensión de BGP (*Border Gateway Protocol*) [13].

1.3.4.4.1 LDP (*Label Distribution Protocol*): Este protocolo es un conjunto de procedimientos y mensajes mediante los cuales se establece un LSP para las FECs que representan una dirección IPv4 o IPv6, esto se lleva a cabo basándose en información proporcionada por el IGP. LDP opera entre dos *routers*, ya que se distribuyen las etiquetas a sus pares LDP

(LDP *peers*) o vecinos. Toda información intercambiada en LDP es codificada por TLV [3][13].

1.3.4.4.2 CR-LDP (*Constrained-Based Routing* LDP): Este es un protocolo mediante enrutamiento explicito permite establecer un LSP denominado CR-LSP. El LSP se genera con criterios de Calidad de Servicio e información que generan los algoritmos de enrutamiento [13].

Los CR-LSP pueden ser utilizados para crear túneles MPLS, cuyas rutas se basan en la calidad de servicio que se le da al tráfico. También un CR-LSP puede ser usado para realizar balanceo de carga [13].

1.3.4.4.3 RSVP-TE (*Resource Rerservation Protocolo – Traffic Engineering*): El protocolo RSVP tiene una extensión la cual permite la creación y mantenimiento de LSP, además de crear reservas de ancho de banda. El camino de un LSP señalizado por RSVP no sigue necesariamente la trayectoria dada por el IGP, ya que RSVP-TE en el ingreso del *router* puede indicar la ruta que el LSP debe seguir. En MPLS este protocolo es importante en la Ingeniería de Tráfico porque RSVP permite administrar la ruta que sigue el flujo de información, con lo que se puede solucionar problemas de red como es la congestión, además de que RSVP dar a los LSPs soporte a CoS (Clase de Servicio) [12].

1.3.4.4.4 BGP *Label Distribution*: Esta extensión del protocolo de enrutamiento BGP, también llamado: MP-BGP (*Multi-Protocol* BGP) soporta a múltiples familias de direcciones, que permite que la información se manejada de mejor manera, ya que se puede anunciar el prefijo de red y una o más etiquetas asociadas al prefijo, lo cual permite a BGP desenvolverse con el contexto de inter-AS MPLS/VPNs al establecer LSPs que cruzan los límites de los AS [12].

Este protocolo permite que la red sea escalable al soportar un gran número de rutas de clientes y al usar VPN MPLS permite un transporte directo de rutas de clientes entre *routers* PE [13].

Para evitar que existan direcciones IP duplicadas de los clientes, el protocolo MP-BGP realiza una expansión de prefijos IP para obtener

[3] TLV (Type-Length-Value): Es un esquema utilizado para representar la información transportada en los mensajes LDP [13].

direcciones IP únicas, esto se logra mediante RD (*Router Distinguishers*) que es un prefijo de 64 bits que se añaden a la dirección IP del cliente, formando una dirección única denominada VPNv4 o VPN IPv4 de 96 bits. El RD tiene un significado global por lo que es configurado en el *router* PE, requiriendo un RD por cliente [13].

Mediante RT (*Route Target*) que añade 64 bits a las direcciones VPNv4, se logra la identificación de un sitio que participa en más de una VPN, especificando la comunidad que se agregará a la dirección IPv4, mediante la opción *export* y especificando las comunidades ingresan a la tabla de enrutamiento virtual (*VRF Virtual Routing Forwarding*) que provee privacidad al cliente, mediante la opción *import*. Los RT se distinguen en dos tipos: el RT de exportación que identifica un conjunto de VPNs, cuyos sitios pertenecen a una tabla de enrutamiento virtual, mientras que el RT de importación permite que los *routers* PE puedan seleccionar las rutas para ingresar su VRF [13].

1.3.4.5 Modelo VPN-MPLS

Una VPN es una red privada utilizada para proveer redes dedicadas a clientes que se encuentran en diferentes ubicaciones, cuya transferencia de información dispone del soporte de calidad de servicio (QoS). Una VPN asegura que la información sea desconocida para otros clientes externos [14].

En el modelo VPN/MPLS los *routers* PE tienen participación en el enrutamiento del cliente, ya que se brinda un transporte separado de rutas por cada cliente que tiene asignado una tabla de enrutamiento virtual (VRF) [13]. Según los servicios brindados, basándose en el modelo OSI se tienen los siguientes tipos de VPN:

1.3.4.5.1 L2VPN-VPWS (*Virtual Private Wire Service*): Desarrollado para servicios capa 2 del modelo OSI sobre MPLS, los cuales establecen conexiones punto-punto entre los sitios del cliente mediante VPNs [15].

VPWS se presenta como una alternativa a líneas dedicadas, circuitos virtuales ATM o *Frame Relay*. VPWS permite la inclusión de servicios IP o L2VPN en la red de *Core* de un proveedor, lo cual reduce los costos en infraestructura [15].

El mecanismo usado por VPWS es mediante la creación de pseudo líneas que simulan un circuito capa 2, este servicio puede ser creado en topologías malladas o *hub & spoke* [15].

1.3.4.5.2 L2VPN-VPLS (*Virtual Private LAN Service*): También conocido como TLS (*Transparent LAN Services*) desarrolla VPNs capa 2 multipunto sobre MPLS, lo cual permite establecer conexiones con múltiples sitios de un único dominio IP/MPLS. VPLS permite emular al cliente una única LAN en la cual los múltiples sitios se interconectan independientemente de la ubicación [15].

VPLS brinda un mecanismo en el cual los *routers* PE indican el inicio y fin de la VPN, ya que en estos se deben establecer los túneles para interconectar los *routers* PE vecinos, este proceso se realiza mediante puentes conocidos como VB (*Virtual Bridge*) por cada instancia VPLS. El tipo de conexión necesaria para VPLS es una topología mallada, ya que los *routers* PE crean conexiones entre PW (*Pseudowires*) conocidos como túneles Martini utilizados para señalización punto a punto [15].

En las VPNs capa 2 los datos, como tramas *Ethernet*, son transmitidos de forma transparente a través de la nube MPLS, ya que se considera como una red conmutada, la cual permite establecer conexiones nivel 2 para redes dedicadas entre diferentes locaciones [11], como se muestra en la Figura 1.8.

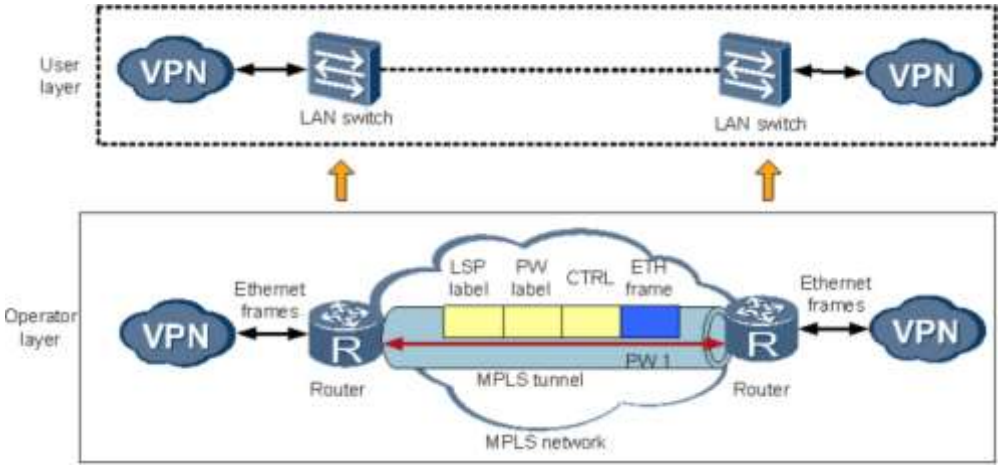

Figura 1.8. L2VPN MPLS [11].

1.3.4.5.3 MPLS L3VPN: Este tipo de VPNs tienen soporte para paquetes IP sobre MPLS, ya que opera en la capa 3 del modelo OSI, en este contexto de VPN se puede tomar la nube MPLS como un conmutador, ya que va a permitir al

cliente tener conexiones IP entre los diferentes sitios mediante líneas dedicadas virtuales [14].

Para la configuración de los servicios L3VPN se debe tomar en cuenta que los *routers* PE deben almacenar y procesar las rutas del cliente, por lo que se necesitan configuraciones extras en el lado del proveedor de servicios [15].

El mecanismo usado por L3VPN basado en el RFC 4364 permite que los proveedores de servicios puedan usar su red de *backbone* para implementar las L3VPNs para sus clientes. Este tipo de servicios está relacionado con el protocolo MP-BGP, ya que con este protocolo permite la distribución de la información de las VPNs, a través del *backbone* del proveedor, mientras que para enviar el tráfico VPN, a través del *backbone* a los sitios de los clientes se utiliza MPLS. La privacidad que los servicios L3VPN brindan permite que los clientes puedan usar direcciones públicas o privadas, ya que se utilizan prefijos para la identificación de las VPNs, además cada VPN tiene una tabla de enrutamiento VPN específica [15].

Las VPNs capa 3 admiten el uso de paquetes IP que son transmitidos en base a la dirección de destino a través de la nube MPLS, la cual se considera como una red conmutadora de paquetes, que permite establecer conexiones IP para redes dedicadas de diferente ubicación [11], como se ilustra en la Figura 1.9.

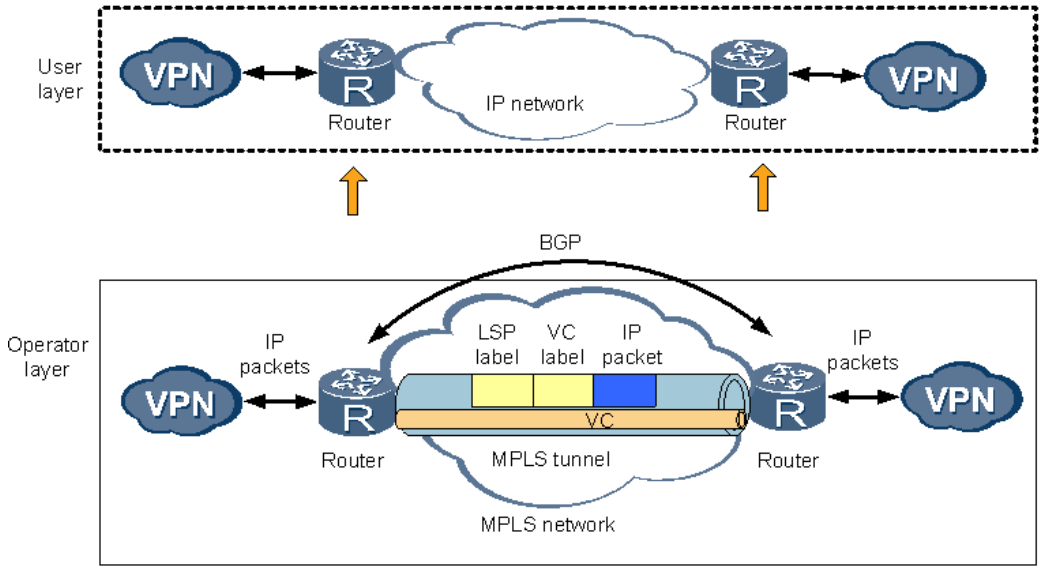

Figura 1.9. L3VPN MPLS [14].

2. METODOLOGÍA

2.1 Estudio de la situación actual del servicio de datos móviles en Ecuador

En el país el SMA (Servicio Móvil Avanzado) se encuentra desplegado por tres prestadoras: CONECEL S.A. (Consorcio Ecuatoriano de Telecomunicaciones Sociedad Anónima), conocida como CLARO, OTECEL S. A. (Operadora de Telefonía Celular Sociedad Anónima.), conocida como MOVISTAR/TUENTI y CNT E.P. (Corporación Nacional de Telecomunicaciones Empresa Pública) [16].

En la Figura 2.1, se presenta el porcentaje de líneas activas de las prestadoras del SMA, encontrando que CONECEL S.A es la empresa con la mayor cantidad de líneas activas y abonados en el país [16].

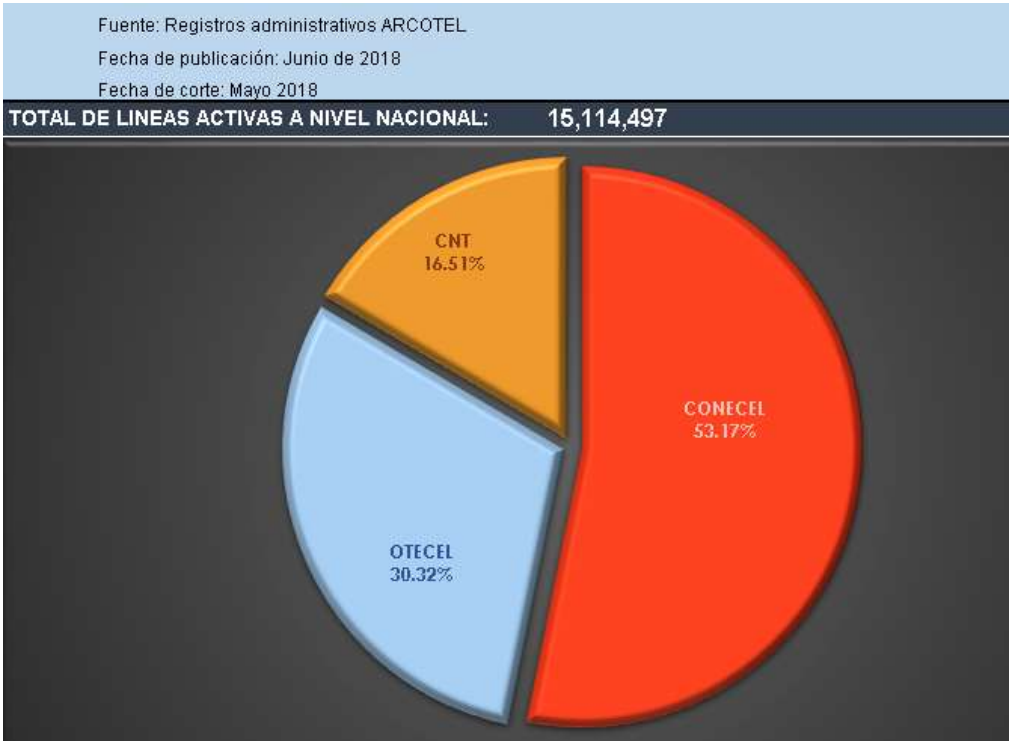

Figura 2.1. Participación de las Prestadoras del SMA en Ecuador [16]

En la Figura 2.2, se observa que las tecnologías utilizadas por las operadoras para brindar el SMA son: GSM (*Global System for Mobile Communications*), UMTS (*Universal Mobile Telecommunications System*), HSPA+ (*High Speed Packet Access*) y LTE, además, se evidencia que el uso de la tecnología GSM ha ido disminuyendo [17].

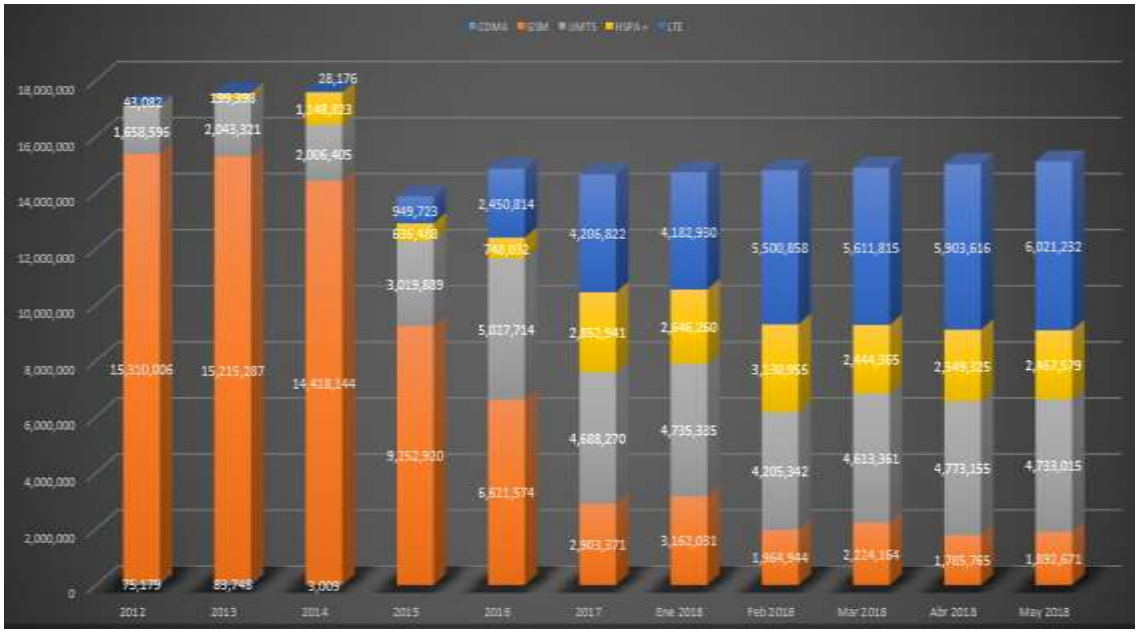

Figura 2.2. Evolución de Líneas activas por tecnología desde el 2012 al 2018 [17]

Ecuador registra que hasta mayo del 2018 alrededor de 15 millones de líneas tuvieron acceso al servicio de datos móviles, de las cuales el 12.52% corresponden a tecnología 2G, 47.64% a 3G y 39.84% a 4G [17].

Los datos obtenidos por la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) muestran que existen 8.58 millones abonados al servicio de voz y datos, esto implica que del total de pobladores en Ecuador un 51% utiliza dicho servicio, esto se encuentra influenciado al uso de teléfonos inteligentes conectados a la red, tomando en cuenta que en Ecuador existe la depuración de bases de datos propias de las operadoras, lo que evita un incremento irreal de abonados [18].

2.2 Estudio de la situación actual del servicio de datos móviles en la ciudad de Riobamba

2.2.1 Situación Geográfica de Riobamba

La ciudad de Riobamba constituye la capital de la Provincia del Chimborazo, esta ciudad es la principal generadora de bienes y servicios para el cantón y provincia, debido a su condición de capital provincial y sede regional y zonal de varias instituciones [19].

Los límites territoriales de Riobamba son: al norte con los cantones de Guano y Penipe, al Sur la parroquia de Cacha, al Este con el cantón Chambo y al Oeste la parroquia de Licán, como se puede observar en la Figura 2.3.

Figura 2.3. Ubicación Geográfica de Riobamba [20]

2.2.2 Análisis del servicio de datos móviles en Riobamba

Según datos de la ARCOTEL, la proyección poblacional del cantón Riobamba en el 2018 es de 258.597 habitantes [21], de los cuales el 69.426% corresponden a la ciudad de Riobamba [22], es decir, 179.534 habitantes.

Actualmente existen problemas en las redes de acceso, ya que en ciertos casos las estaciones base se encuentran en proceso despliegue, por lo que no cuentan con equipos de red, en otros casos hay *routers* de acceso que presentan interfaces *Fast Ethernet* (100 Mbps), las cuales están descontinuadas, esto indica que la red necesita una actualización, debido la continua evolución de la tecnología. Estos problemas sugieren al operador de servicios móviles proponer una solución de red mediante la cual se logre alcanzar mayor velocidad de conexión y permita la operación de las tecnologías celulares.

Para solucionar los problemas mencionados anteriormente, se propone una IP-RAN que es una arquitectura de red basada en IP que permite la conectividad de las estaciones base al *Core* de Servicios, en el caso de LTE permite que los *enodeB* accedan a la red troncal EPC. Mediante el despliegue de una IP-RAN se logrará escalabilidad en la red, se reducirán los costos de despliegue, ya que la IP-RAN puede utilizar un mecanismo

de transporte existente, además la IP-RAN permitirá la integración de varias tecnologías celulares como: GMS, UMTS, HSPA+, LTE, entre otras.

2.2.2.1 Análisis de Tráfico LTE

Para dimensionar la cantidad de usuarios que cursarán por la red LTE en la ciudad de Riobamba para una operadora, se tienen los siguientes datos:

- **H:** *Habitantes de la ciudad de Riobamba:* 179.534 [21], [22]
- **A:** *Porcentaje de Abonados de Voz y Datos:* 51% [18]
- **B:** *Porcentaje de utilización de LTE:* 38,84% [17]
- **C:** *Participación por Operadoras en el mercado:* 53,17% CONECEL, 30,32 % OTECEL y 16,51% CNT, para el presente estudio se tomará el porcentaje de CNT [16].
- **U:** número de usuarios LTE

Los parámetros descritos anteriormente permiten obtener el número de usuarios que utilizan servicios LTE, para lo cual se utiliza la Ecuación 2.1.

$$U = H\ x\ A\ x\ B\ x\ C$$

$$U = 179534\ x\ 0{,}51\ x\ 0{,}3884\ x\ 0{,}1651 = 5871.42 = 5872\ usuarios$$

Ecuación 2.1. Número de Usuarios LTE [23]

Dimensionamiento del Tráfico LTE en la ciudad de Riobamba para una operadora

Para estimar el tráfico de la red a la hora pico, se utilizará un modelo de tráfico y servicio que permitirá obtener el *throughput* total.

En la Tabla 2.1 se muestra el modelo de servicio utilizado para el dimensionamiento de la cantidad de información a intercambiarse durante una sesión [24].

Tabla 2.1 Modelo de Servicio [24]

Traffic Parameters	UL				DL			
	Bearer Rate (Kbps)	PPP Session Time (s)	PPP Session Duty Ratio	BLER	Bearer Rate (Kbps)	PPP Session Time (s)	PPP Session Duty Ratio	BLER
VoIP	26.90	80	0.4	1%	26.90	80	0.4	1%
Video Phone	62.53	70	1	1%	62.53	70	1	1%
Video Conference	62.53	1800	1	1%	62.53	1800	1	1%
Real Time Gaming	31.26	1800	0.2	1%	125.06	1800	0.4	1%
Streaming Media	31.26	3600	0.05	1%	250.11	3600	0.95	1%
IMS Signalling	15.63	7	0.2	1%	15.63	7	0.2	1%
Web Browsing	62.53	1800	0.05	1%	250.11	1800	0.05	1%
File Transfer	140.69	600	1	1%	750.34	600	1	1%
Email	140.69	50	1	1%	750.34	15	1	1%
P2P file sharing	250.11	1200	1	1%	750.34	1200	1	1%

Con la información de la Tabla 2.1 se calcula el volumen de tráfico intercambiado durante la prestación de un determinado servicio a un solo usuario [24], para llevar a cabo dicho cálculo se utilizará la Ecuación 2.2.

$$Throughput_S = \frac{BearerRate\ x\ PPPSessionsTime\ x\ \ PPPSessionsDutyRatio}{1 - BLER}$$

Ecuación 2.2. *Throughput* por Sesión [24]

Donde:

Throughput$_s$: Volumen de información por sesión.

Bearer Rate: Velocidad de transferencia de datos para el funcionamiento de un servicio.

PPP Sessions Time: Tiempo en el cual una sesión permanece activa.

PPP Sessions Duty Ratio: Porcentaje por sesión para la utilización del canal de transmisión.

BLER: Tasa de Error de Bloque [24].

En la Tabla 2.2 se muestran los resultados del cálculo del volumen de tráfico por sesión.

Tabla 2.2 Volumen de tráfico por sesión [24]

Tipo de Tráfico	UL	DL
	Volumen por Sesión (Kbit)	Volumen por Sesión (Kbit)
VoIP	869	869
Video Phone	4421	4421
Video Conference	113687	113687
Real Time Gaming	11369	90950
Streaming Media	5684	864023
IMS Signalling	22	22
Web Browsing	5684	22737
File Transfer	85265	454749
Email	7105	11369
P2P File Sharing	303166	909498

En la Tabla 2.3 se muestran los parámetros del modelo de tráfico, los cuáles describen el comportamiento del UE en un ambiente urbano denso [24], estos datos servirán para calcular el *throughput* por usuario.

Tabla 2.3 Modelo de Tráfico [24]

User Behavior	Dense Urban	
	Traffic Penetration Ratio	BHSA
VoIP	100.00%	1.4
Video Phone	20.00%	0.2
Video Conference	20.00%	0.2
Real Time Gaming	30.00%	0.2
Streaming Media	15.00%	0.2
IMS Signalling	40.00%	5
Web Browsing	100.00%	0.6
File Transfer	20.00%	0.3
Email	10.00%	0.4
P2P file sharing	20.00%	0.2

Mediante la Ecuación 2.3 se obtiene el *throughput* por usuario basado en el modelo de tráfico y servicio:

$$Throughput_u = \sum_K [Throughput_{S_K} \; x \; BHSA_K \; x \; TPR_K \;] \; x \; \frac{(1 \; + \; PAR)}{3600[kbps]}$$

Ecuación 2.3. *Throughput* por Usuario [24]

Donde:

Throughput$_u$: Velocidad de transferencia de datos por usuario.

BHSA: *Busy Hour Session Attemps*.

Traffic Penetration Ratio (TPR): Porcentaje de la demanda del servicio, 40% en ambientes urbanos densos.

Peak to Average Ratio (PAR): Desviación Estándar.

K: Tipo de Servicio [24].

Con la información de la Tabla 2.2 y Tabla 2.3, se realizan los cálculos para obtener el *throughput* para un usuario en *uplink* y *downlink*, cuyos resultados se muestran en la Tabla 2.4.

Tabla 2.4 *Throughput* según el modelo de servicio y tráfico [24]

User Behavior	Dense Urban			
	Traffic Penetration Ratio	BHSA	Busy Hour Throughput Per User (bps)	
			UL	DL
VoIP	100.00%	1.4	338	338
Video Phone	20.00%	0.2	49	49
Video Conference	20.00%	0.2	1263	1263
Real Time Gaming	30.00%	0.2	189	1516
Streaming Media	15.00%	0.2	47	7200
IMS Signalling	40.00%	5	12	12
Web Browsing	100.00%	0.6	947	3790
File Transfer	20.00%	0.3	1421	7579
Email	10.00%	0.4	79	126
P2P file sharing	20.00%	0.2	3369	10106
Total	-	-	10802	44771

En el dimensionamiento del tráfico generado por un usuario, se añade el *overhead* causado por procesos de control y señalización al *throughput* por usuario, por lo general se considera un 25% de *overload* en relación con el *throughput* [23]. Entonces el tráfico que un usuario genera se calcula mediante la Ecuación 2.4.

$$Tráfico\ por\ usuario = Throughput_u\ x\ Porcentaje\ de\ Overload$$

DOWNLINK

$$Tráfico\ por\ usuario = 44771\ x\ 1{,}25 = \ 55{,}96\ [Kbps]$$

UPLINK

$$Tráfico\ por\ usuario = 10802\ x\ 1{,}25 = 13{,}50\ [Kbps]$$

Ecuación 2.4. Tráfico por Usuario [23]

Para calcular el tráfico a cursar por la red LTE, se considera que el 60 % de los usuarios LTE [25] en la ciudad Riobamba se conectarán simultáneamente. Entonces el tráfico LTE se calcula mediante la Ecuación 2.5.

$$Tráfico\ LTE = 0{,}6\ x\ U\ x\ Tráfico\ por\ usuario$$

DOWNLINK

$$Tráfico\ LTE = 0{,}6\ x\ 5872\ x\ 55{,}96\ = 197{,}17\ [Mbps]$$

UPLINK

$$Tráfico\ LTE = 0{,}6\ x\ 5872\ x\ 13{,}50 = 47{,}57\ [Mbps]$$

Ecuación 2.5. Tráfico de Usuarios LTE al 60 % de ocupación

De acuerdo con los datos de la Figura 2.4 el crecimiento de usuarios LTE en el país tiene una tendencia exponencial [23], esta información es utilizada para realizar una proyección de usuarios LTE para el año 2022, la cual indica un crecimiento del 123% con respecto al año 2018, es decir, que en el año 2022 el número de usuarios LTE sería de 13,3979 millones.

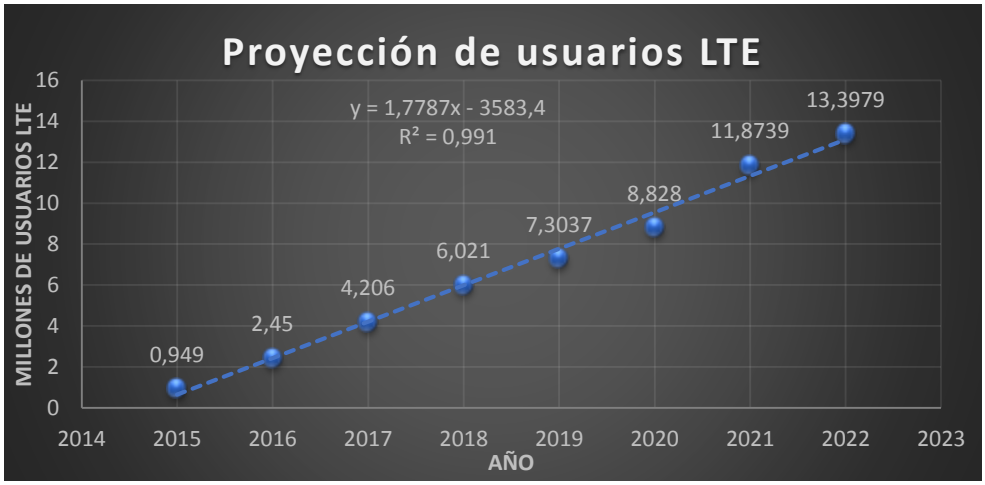

Figura 2.4. Proyección de usuarios LTE en Ecuador para el 2022

Entonces tomando en cuenta el factor de crecimiento de 123% de usuarios LTE, para obtener el tráfico proyectado a 4 años que el sistema LTE en Riobamba debe soportar se utiliza la Ecuación 2.6.

$$Tráfico\ LTE\ \ Proyectado = Tráfico\ LTE\ x\ (2{,}23)^4$$

DOWNLINK

$$\boldsymbol{Tráfico\ LTE\ \ Proyectado = 4{,}876[Gbps]}$$

UPLINK

$$\boldsymbol{Tráfico\ LTE\ \ Proyectado = 1{,}176[Gbps]}$$

Ecuación 2.6. Tráfico LTE Proyectado a 4 años [23]

Dimensionamiento del Tráfico LTE en Ecuador para una operadora

Para dimensionar el tráfico LTE en Ecuador, se tiene la información del *throughput* por usuario, la tasa de crecimiento, el número de usuarios LTE de la operadora CNT E.P. (2'131.494 de usuarios) [17] y mediante la Ecuación 2.6 se obtiene el tráfico LTE proyectado a 4 años.

$$Tráfico\ LTE\ Proyectado = (0{,}6\ x\ U\ x\ Tráfico\ por\ usuario\ )\ x\ (2{,}23)^4$$

DOWNLINK

$$\boldsymbol{Tráfico\ LTE\ \ Proyectado = 1769{,}952\ [Gbps]}$$

UPLINK

$$\boldsymbol{Tráfico\ LTE\ \ Proyectado = 427{,}040\ [Gbps]}$$

El tráfico de 1,77 [Tbps] debe ser soportado por el *router* RSG, ya que este dirigirá la información hacia la red troncal EPC.

2.3 Equipamiento

Para el despliegue de la red IP-RAN al ser una arquitectura jerárquica, deberá disponer de *routers* de acceso, agregación y borde, cuyas características garanticen la disponibilidad de los servicios móviles, en la ciudad de Riobamba.

En la solución IP-RAN a proponer se dispondrá en una topología HRT, cuya propuesta combina la topología en anillo y en árbol [26], por lo que los *routers* de acceso se conectarán al *router* de agregación más cercano, los *routers* de agregación formarán un anillo de agregación con el *router* de borde, cuya capacidad se considerará de 10

Gbps, ya que actualmente las operadoras como CNT E.P. poseen redes de transporte como IP/MPLS y DWDM, cuyas capacidades alcanzan de hasta 10 Gbps [27]. Finalmente se tiene que el *router* de borde se conecta a la nube MPLS para llegar al *Core* de LTE, tal como se muestra en la Figura 2.5. Aprovechando la ubicación geográfica de la ciudad de Riobamba se propone utilizar el *router* de borde para dirigir el tráfico nacional hacia la red troncal EPC.

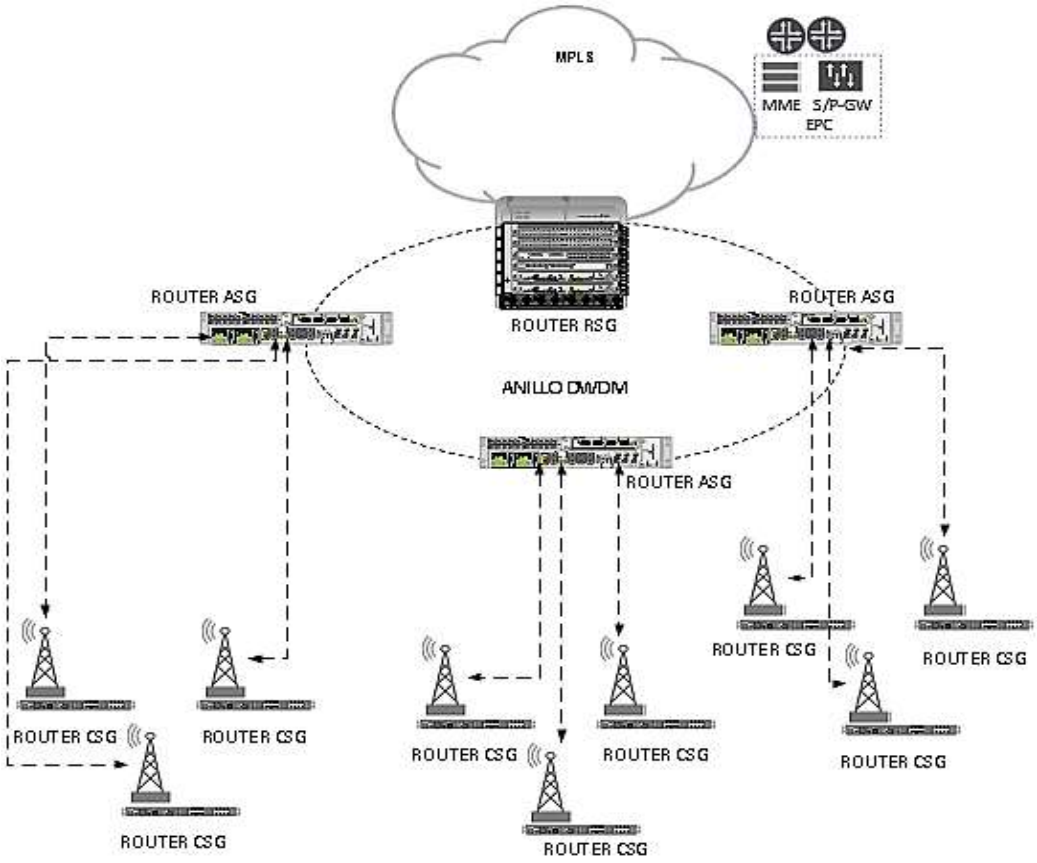

Figura 2.5. Topología HRT de la IP-RAN

2.3.1 Requerimientos a Nivel de Puertos

Actualmente en Ecuador según datos de la ARCOTEL, las estaciones base utilizadas para brindar cobertura móvil a los usuarios permiten el despliegue de servicios 2G, 3G y 4G [17].

El requerimiento en puertos en el nivel de acceso debe tomar en cuenta el ancho de banda requerido por cada tecnología (GSM, UMTS, HSPA+ y LTE) para establecer los enlaces entre los *routers* IP-RAN, siendo 100 Mbps de LTE [2] la capacidad teórica máxima a satisfacer actualmente, sin embargo, la IP-RAN al tener la característica de interoperabilidad deberá brindar servicios a otras tecnologías como *LTE-Advanced*, cuya capacidad máxima teórica es de 1 Gbps [2].

Entonces para satisfacer el requerimiento de puertos del *router* de acceso por tecnología móvil, se proponen puertos *Gigabit Ethernet*, ya que estos puertos brindan capacidades de hasta 1Gbps, lo cual satisface el requerimiento de LTE-*Advanced*.

Según datos de la ARCOTEL, se tiene que hasta mayo del 2018 en Riobamba se han instalado un promedio de 21 radiobases por operadora para LTE en la banda de 1700 MHz [28]. Debido a que los *routers* de acceso se ubicarán en los sitios donde se encuentran los *enodeB* se tomará esta cantidad (21) para el número de *routers* CSG.

En la Tabla 2.5 se puede apreciar el requerimiento de puertos tomando en cuenta un factor de escalabilidad del 20% en la red, además se propone que en el nivel de Borde se pueda agregar a *routers* de acceso, ya que pueden existir casos en los cuales la distancia entre el *router* de acceso y un *router* agregador sea muy grande.

Tabla 2.5. Requerimiento de los Puertos de los *Routers*

Tipos de *Routers*	**Tipo de Puerto según el Servicio**	**Tipo de Puerto según la Capacidad**
CSG	Acceso a 2G	GE
	Acceso a 3G	GE
	Acceso a 4G	GE
	Acceso a 4.5G	GE
	Conexión al *router* ASG	GE
	Total	**5 x 1.2 = 6 puertos GE**
ASG	Acceso a 5 *routers* CSG	5 x GE
	Total	**5 x 1.2 = 6 puertos GE**
	Conexión para el Anillo	2 x 10 GE
	Total	**2 x 1.2 = 3 puertos 10 GE**
RSG	Posible Acceso a *routers* CSG	5 x GE
	Total	**5 x 1.2 = 6 puertos GE**
	Conexión para el Anillo	2 x 10 GE
	Enlace para el *Router* PE	2 x 10 GE
	Total	**4 x 1.2 = 5 puertos 10 GE**

2.3.2 Requerimientos en Capacidad de Procesamiento

A partir de lo revisado en las secciones 2.2.2.1 y 2.3.1 se obtiene la Tabla 2.6 que enlista la capacidad requerida por *router* según el nivel en la IP-RAN, teniendo que el *router* RSG deberá soportar 1,77 Tbps, ya que este *router* se encargará de dirigir la información del tráfico nacional hacia el *Core* de servicios LTE, asumiendo que el tráfico se genera por igual en los *enodeB,* se tiene que los *routers* CSG deberán procesar al menos 232,19 Mbps, mientras que los *routers* ASG deberán procesar el tráfico LTE de la ciudad de Riobamba, adicionalmente se tendrá en cuenta que cada *router* ASG podrá agregar información de otra ciudad, por lo que la capacidad de los routers ASG será al menos de 4 veces el tráfico LTE en Riobamba, es decir, 19,50 Gbps.

Tabla 2.6. Requerimiento de Capacidad de Procesamiento de los *Routers* IP-RAN

Tipo de *Router*	**Capacidad**
RSG	1,77 [Tbps]
ASG	19,50 [Gbps]
CSG	232,19 [Mbps]

2.3.3 Requerimientos de Protocolos y Configuraciones

En la Tabla 2.7 se enlistan los requerimientos a nivel lógico (protocolos y políticas de red) que los *routers* de la IP-RAN deberán soportar para realizar la interconexión de los *enodeB* con la red troncal EPC.

Tabla 2.7. Requerimientos de Protocolos y Configuraciones

Requerimiento	**Descripción**
ISIS	IGP para la interconexión de *routers* de la IP-RAN.
BGP	Configuración del protocolo de enrutamiento para el establecimiento de adyacencias y la configuración de la extensión MP-BGP para trabajar con L3VPN.
MPLS	Habilitación de MPLS en las interfaces de los *routers*, para mejorar la conmutación de paquetes.
LDP	Protocolo para utilizado para la distribución de etiquetas.
L3VPN	Transporte de los diferentes servicios de la red.
Políticas de QoS	Clasificación y Priorización del Tráfico.

2.3.4 Requerimientos del Medio de Transmisión

Para realizar las conexiones de los nodos IP-RAN se utilizarán medios de transmisión alámbricos, debido a que las estaciones se ubican en la ciudad y por lo tanto, no son necesarios los medios de transmisión inalámbricos como las microondas.

Para el presente estudio, se considerará el uso de la fibra óptica, ya que en comparación con el par trenzado de cobre (UTP), la fibra óptica brinda los siguientes beneficios:

- Mayor capacidad de transmisión.
- Evita las interferencias electromagnéticas y estáticas.
- Amplio rango de variación de temperatura.
- Más pequeñas y livianas.
- Baja atenuación.
- Resistencia a la corrosión.
- Los sistemas de fibra óptica son los más utilizados a nivel mundial [29].

Se propone la utilización de la fibra óptica monomodo[4], ya que en comparación con la fibra óptica multimodo presenta mejores características de ancho de banda, no presentan dispersión modal, es más barata, tiene baja atenuación y es recomendada para redes de acceso [29].

En las Tablas 2.8 y 2.9 se muestran las recomendaciones más importantes que hacen referencia a la utilización de la fibra óptica, estas recomendaciones son establecidas por la Unión Internacional de Telecomunicaciones (UIT).

[4] Fibra Óptica Monomodo: Este tipo de fibra óptica permite la propagación de un solo rayo de luz en línea recta en el interior de la fibra, el diámetro del núcleo está en el orden de 4 a 10 micrones, a tal punto que éste actúa como guía de onda [29].

Tabla 2.8. Comparación de Normas de la UIT para la utilización de fibra óptica Parte 1 [30], [31], [32]

Tipo de Fibra	**Principales Características**
G.652	• Presenta dispersión de longitud de onda nula cerca de 1310 nm. • Operación recomendada en regiones de 1310 nm y 1550 nm. • Atenuación entre 0.2 a 0.5 dB/km.
G.653	• Presenta Dispersión de longitud de onda Desplazada. • Operación recomendada en la región de 1550nm y regiones cercanas a 1310 nm. • Atenuación entre 0.2 dB/km a 0.5 dB/km.
G.654	• Presenta dispersión de longitud de onda nula cerca de 1300 nm. • Operación recomendada en regiones entre 1530 y 1625 nm. • Atenuación entre 0.15 dB/km a 0.25 dB/km.

Tabla 2.9. Comparación de Normas de la UIT para la utilización de fibra óptica Parte 2 [33], [34], [35]

Tipo de Fibra	**Principales Características**
G.655	• Reduce los efectos no lineales. • Operación recomendada en regiones entre 1530 a 1565 nm, puede ser utilizada para longitudes de onda de hasta 1625nm y longitudes de onda debajo de 1460 nm. • Atenuación entre 0.2 dB/km a 0.35 dB/km.
G.656	• Reduce los efectos no lineales. • Operación recomendada en regiones entre 1530 a 1565 nm y entre 1460 a 1625 nm. • Atenuación entre 0.2 dB/km a 0.4 dB/km.
G.657	• Mejor rendimiento que fibras con recomendación G.652. • Operación recomendada en regiones entre 1260 a 1625 nm. • Atenuación entre 0.3 dB/km a 0.4 dB/km.

La red IP-RAN utilizará una red de transporte ya establecida, por lo que se pone el ejemplo de CNT-EP que posee equipos de transmisión que soportan fibras G.652, G.653, G.654 y G.655 [36].

Con lo descrito en las Tablas 2.8 y 2.9 se propone la utilización de fibra monomodo G.652 D para la interconexión de la IP-RAN, debido a que su uso es adecuado para DWDM [30] y el costo de este tipo de fibra es económico.

Para realizar conexiones en la IP-RAN, los equipos de red deben soportar la incorporación de dispositivos SFP (*small form-factor pluggable transceptor*) que son módulos que permiten la operación de la fibra óptica en *routers*, *switches*, etc [37].

2.3.5 Elección del Fabricante de los *Routers*

Para el despliegue de la red IP-RAN se necesitarán *routers* de 3 tipos, según el nivel jerárquico, para lo cual existen diferentes fabricantes que pueden ofertar equipos, los cuales deben cumplir con los requerimientos mencionados en las secciones 2.3.1, 2.3.2, 2.3.3 y 2.3.4. Para la comparación de equipos, se toman en cuenta los fabricantes Huawei Technologies y Cisco Sytems.

2.3.5.1 *Routers* de Acceso CSG

En la Tabla 2.10 se presenta la comparación de las características técnicas entre un *router* Cisco ASR 1001-HX y un *router* Huawei ATN 910B-A. Los *routers* de las dos marcas cumplen con los requisitos de la IP-RAN, sin embargo, el *router* de la marca Cisco presenta mayor número de puertos GE y 10 GE lo que permite ofrecer más servicios, además si en el futuro se necesita brindar acceso a servicios que requieran más de 1 Gbps se pueden utilizar los puertos de 10 GE, lo que no sucede en el router Huawei, ya que solo posee 2 puertos 10 GE.

Tabla 2.10. Comparación para el *Router* de Acceso [38], [39]

Especificaciones	**CISCO ASR 1001-HX**	**HUAWEI ATN 910 B-A**
Descripción	El equipo Cisco ASR 1001-HX es un *route*r de servicios compactos para sucursales empresariales de alta gama, ya que presenta una solución de alto rendimiento, ya que pertenece a las series ASR 1000 que presentan disponibilidad de hasta cinco 9.	Los *routers* de la serie ATN 910 B ocupan pequeños espacios, atienden a múltiples servicios, son aplicables en el borde de una red. Este equipo presenta una gran flexibilidad de implementación por lo que se sugiere en una red de acceso.
Redundancia de Fuente	Sí	Sí
RU (*Rack Unit*)	1 RU	1 RU
Slots	Equipo Integrado	Equipo Integrado
Puertos	8 puertos 1 GE 4 puertos 10 GE 4 puertos configurables para 10 GE y 1 GE	2 puertos 10 GE 8 puertos GE/FE 16 E1
Soporte SFP	Sí	Sí
Capacidad Total	44 - 60 Gbps	44 – 64 Gbps
Protocolos y Servicios	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, HSRP, RSVP, EIGRP, L3VPN, L2VPN, PTP, CEF, Ipv4 e IPv6.	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, RSVP, L3VPN, L2VPN, PTP, Ipv4 e IPv6.
Características Ambientales	Temperatura de Operación: 0 a 40 °C Humedad de Operación: 5 a 95%	Temperatura de Operación: -40 a 65 °C Humedad de Operación: 5 a 95 %

2.3.5.2 *Routers* de Agregación ASG

En la Tabla 2.11 se presenta la comparación de las características técnicas de un *router* Cisco ASR 9001 y un *router* Huawei ATN 950B. Los routers de las dos marcas cumplen con los requerimientos de la IP-RAN, sin embargo, el *router* Cisco presenta mayor capacidad de procesamiento, esta característica puede ser aprovechada en caso de crecimiento del tráfico LTE, para agregar tráfico LTE de otras ciudades o para brindar otros servicios.

Tabla 2.11. Comparación para el *Router* de Agregación [40], [41]

Especificaciones	**CISCO ASR 9001**	**HUAWEI ATN-950B**
Descripción	El *router* Cisco ASR 9001 pertenece a la familia ASR 9000, cuyos equipos permiten escalabilidad en la red y soportan al *backhaul* de una RAN mediante su infraestructura de sincronización integrada.	El *router* ATN 950B está diseñado para la integración de servicios, este equipo cumple funciones multi-servicio, permite la sincronización con alta precisión, su tamaño economiza el gasto del operador.
Redundancia de Fuente	Sí	Sí
RU (*Rack Unit*)	2 RU	2 RU
Slots	Arreglo de 4 puertos 10 y 2 MPA (*Modular Port Adapters*)	2 slots para CXP y 6 slots para tarjetas de interfaces de servicio,
Puertos	Puertos Integrados: 4 puertos 10 GE Puertos Modulares: 20 puertos 1 GE 2 puertos 10 GE 1 puerto 40 GE.	Las tarjetas de interfaz de servicio cuentan con los siguientes arreglos de puertos 4 puertos GE por slot 8 puertos GE por slot 1 puerto 10 GE por slot 2 puerto 10 GE por slot
Soporte SFP	Sí	Sí
Capacidad Total	240 Gbps	66 – 84 Gbps
Protocolos y Servicios	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, HSRP, RSVP, EIGRP, L3VPN, L2VPN, PTP, CEF, Ipv4 e IPv6.	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, RSVP, L3VPN, L2VPN, PTP, Ipv4 e IPv6.
Características Ambientales	Temperatura de Operación: 0 a 40 °C Humedad de Operación: 5 a 95%	Temperatura de Operación: -40 a 65 °C Humedad de Operación: 5 a 95 %

2.3.5.3 *Router de Borde RSG*

En la Tabla 2.12 se presenta la comparación de las características técnicas entre un *router* Cisco ASR 9006 y un *router* Huawei NE40-X2-M8. Los *routers* de las dos marcas presentan las características mínimas para formar parte de la red IP-RAN, sin embargo, se nota un ahorro de espacio físico con el *router* Huawei debido a que ocupa 5 RU, mientras que el *router* Cisco ocupa 10 RU, además se puede notar que el *router* Cisco puede llegar a tener puertos de mayor capacidad que los puertos del *router* Huawei.

Tabla 2.12. Comparación para el *Router* de Borde [42], [43]

Especificaciones	**CISCO ASR 9006**	**HUAWEI NE40-X2-M8**
Descripción	El *router* Cisco ASR 9006 perteneciente a la familia de la serie 9000, permiten enrutamiento de extremo y núcleo, con gran escalabilidad y confiabilidad de clase portadora.	Los *routers* NE40-X2-M8 es un *router* compacto que permite implementar soluciones IP/*Ethernet* de alta gama para proveedores de servicio, *backhaul* móvil y enrutamiento de borde
Redundancia de Fuente	Sí	Sí
RU (*Rack Unit*)	10 RU	5 RU
Slots	Slots Horizontales: 4 tarjetas de línea y 2 RSP	2 para NPUs, 2 para MPUs y 8 para PICs.
Puertos	Las Tarjetas de Línea tienen diferentes arreglos de puertos con capacidades de 1GE, 10 GE, 40 GE y 100 GE, como ejemplo: tarjetas con arreglos de: 48 puertos 10 GE/1GE 2 puertos 100 GE 2 puertos 40 GE 1 tarjeta RSP dispone de 2 puertos 10 GE	1 NPU: 2 puertos 10 GE 1 MPU: 1 Puerto GE/FE 1 PIC tiene diferentes arreglos de puertos como: 4 puertos 10 GE 1 puerto 10 GE + 8 Puertos GE/FE 8 puertos GE/FE
Capacidad Total	7 Tbps	2.54 Tbps
Soporte SFP	Sí	Sí
Protocolos y Servicios	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, HSRP, RSVP, EIGRP, L3VPN, L2VPN, PTP, CEF, Ipv4 e IPv6.	BFD, BGP, ISIS, MPLS-TE, IS-IS, OSPF, LDP, RSVP, L3VPN, L2VPN, PTP, Ipv4 e IPv6.
Características Ambientales	Temperatura de Operación: 0 a 40 °C Humedad de Operación: 5 a 95%	Temperatura de Operación: -40 a 65 °C Humedad de Operación: 5 a 95 %

Tomando en cuenta lo detallado en las Tablas 2.10, 2.11 y 2.12, se concluye que se pueden utilizar equipos de cualquiera de las dos marcas, ya que cumplen con los requerimientos mínimos planteados, sin embargo, se verifica que los *routers* de la marca Cisco presentan mejores características, tales como la cantidad de puertos y la capacidad de procesamiento, estas características pueden ser aprovechadas para mantener la correcta operación de los servicios LTE en caso de crecimiento del tráfico o para brindar otros servicios de red.

A partir de lo detallado anteriormente y por motivos de operabilidad entre equipos se escoge la marca Cisco como la mejor opción en este caso de estudio, ya que operadoras en el país tienen su red de transporte desplegada con tecnología Cisco [27], además estos equipos brindan alta confiabilidad.

Para obtener más información técnica acerca de los *routers* CSG, ASG y RSG, se pueden revisar los ANEXOS I, II Y III, respectivamente.

2.4 Diseño Físico de la red IP-RAN para Riobamba

Como se detalló en la sección 2.3.1 el diseño de la IP-RAN para la ciudad de Riobamba tomará en cuenta 21 *enodeB*, los cuales se conectarán con los *routers* de acceso CSG que dirigirán la información hacia un anillo de agregación IP-RAN formado por 4 *routers* ASG y un *router* RSG, el *router* RSG será el punto de conexión a la red de transporte MPLS que permitirá interconectar los *enodeB* con el *Core* LTE (EPC). Los *enodeB* cubren la ciudad de Riobamba cuya superficie se muestra en la Figura 2.6.

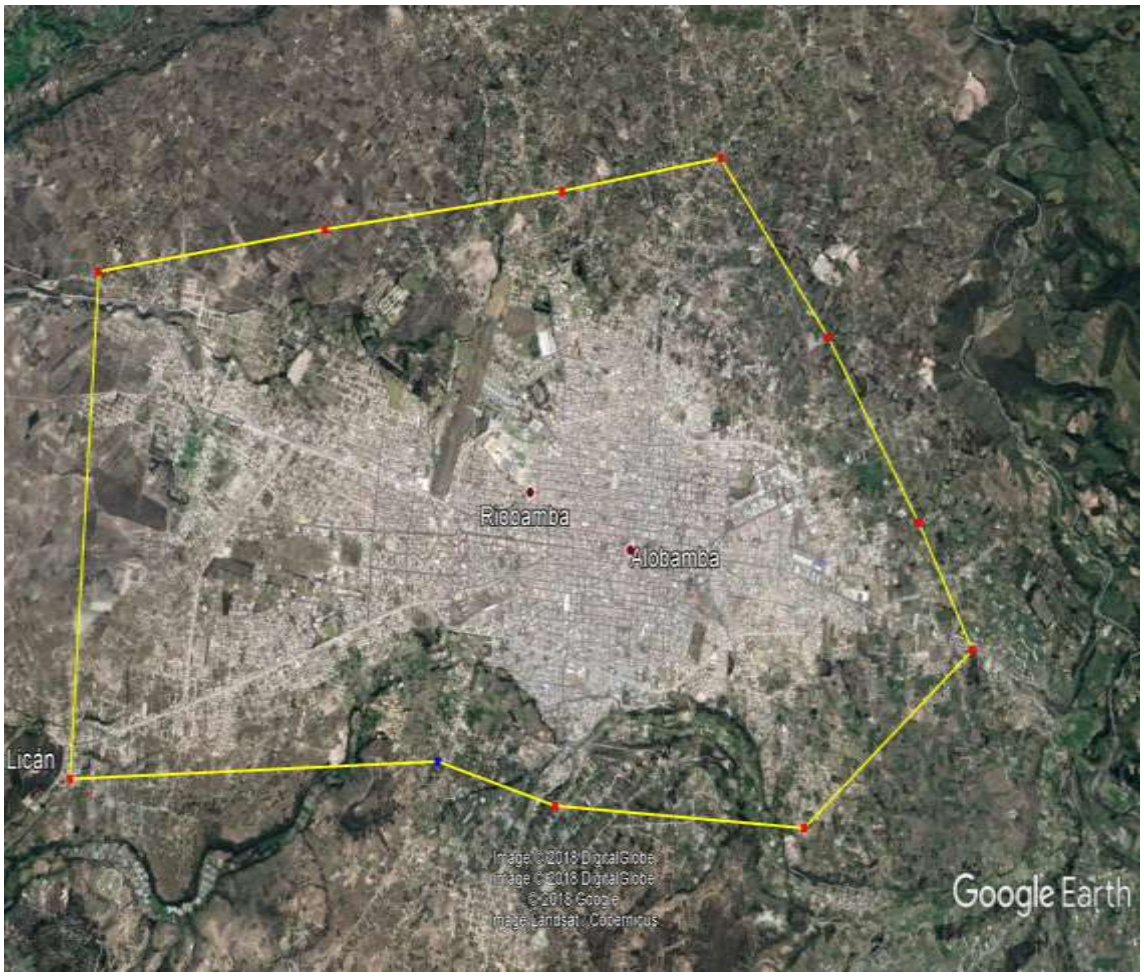

Figura 2.6. Área a cubierta por los *enodeB* en la ciudad de Riobamba [20]

2.4.1 Distribución Geográfica de los nodos IP-RAN.

En la Figura 2.7 se muestra que la mayor concentración poblacional de la ciudad de Riobamba se localiza en el centro y sur, esto se debe tomar en cuenta en la distribución y ubicación de los *enodeB*.

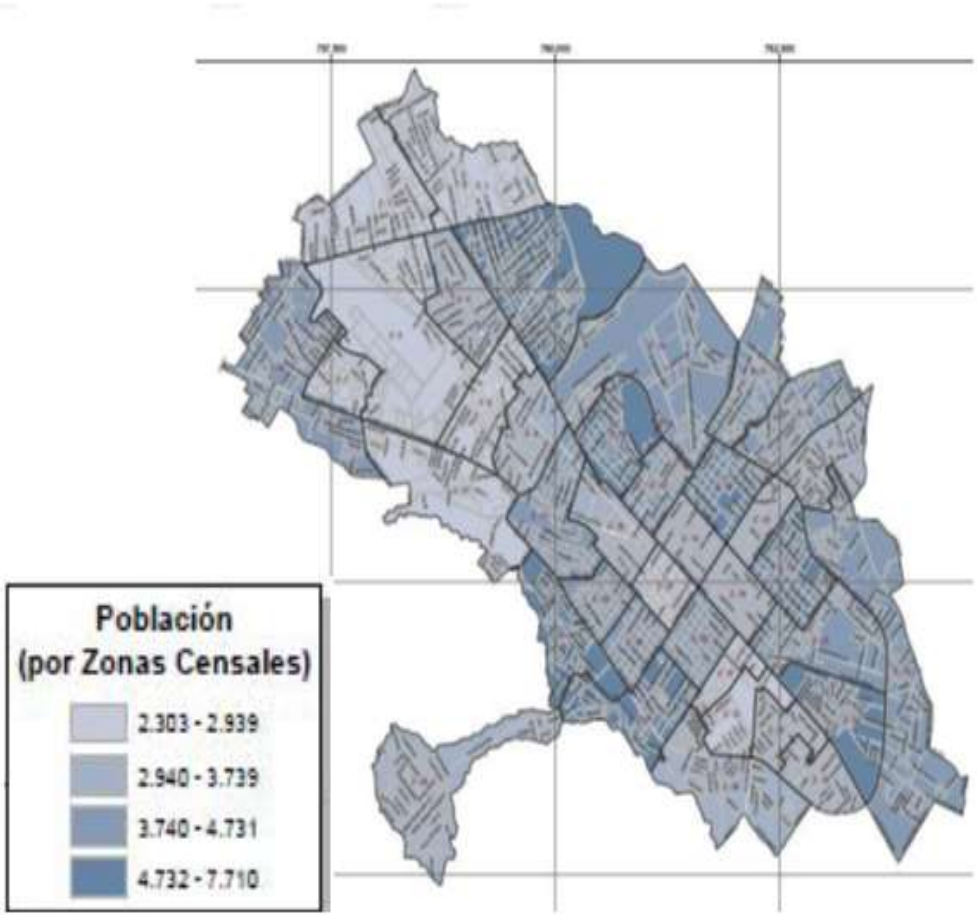

Figura 2.7. Distribución Poblacional de Riobamba según el censo 2010 [19]

Para la identificación de los *routers* IP-RAN en los nodos, se usa el siguiente identificador:

AAABBBCCCDEE

- ***AAA:*** *Acrónimo de la provincia ➔ Chimborazo (CHI)*
- ***BBB:*** *Acrónimo de la ciudad ➔ Riobamba (RIO)*
- ***CCC:*** *Nombre del sitio ➔ Ejemplo: RIO_CSG_CROACIA (CRO)*
- ***D:*** *Jerarquía del Router: Acceso ➔ C, Agregación ➔ A y Borde ➔ R*
- ***EE:*** *Número del equipo dentro del sitio.* [44]

Ejemplo: RIO_CSG_CROACIA ➔ CHIRIOCROC01

En las Tablas 2.13 y 2.114 se detalla la ubicación geográfica de los sitios, donde los *routers* de la IP-RAN se deberán desplegar, teniendo en total 21 *routers* CSG para el acceso, 4 *routers* ASG para la agregación y 1 *router* RSG para el borde.

Tabla 2.13. Ubicación Geográfica de los Nodos e Identificación de equipos IP-RAN Parte 1

TIPO DE NODO	NOMBRE DEL SITIO	ID. *ROUTERS*	COORDENADAS GEOGRÁFICAS	
			LATITUD	LONGITUD
CSG	RIO_CSG_BONILLA	CHIRIOBONC01	1°40'26.44"S	78°39'31.80"O
CSG	RIO_CSG_CEMENTERIO	CHIRIOCEMC01	1°40'43.79"S	78°39'28.44"O
CSG	RIO_CSG_LEONIDAS	CHIRIOLEOC01	1°41'0.46"S	78°39'0.40"O
CSG	RIO_CSG_LOMA	CHIRIOLOMC01	1°39'54.62"S	78°39'0.89"O
CSG	RIO_CSG_MALDONADO	CHIRIOMLDC01	1°40'6.06"S	78°39'19.40"O
CSG	RIO_CSG_ESTADIO	CHIRIOESTC01	1°39'48.60"S	78°39'36.70"O
CSG	RIO_CSG_CISNEROS	CHIRIOCISC01	1°40'31.26"S	78°38'0.17"O
CSG	RIO_CSG_PINOS	CHIRIOPINC01	1°39'38.52"S	78°39'27.47"O
CSG	RIO_CSG_UNIDO	CHIRIOUNIC01	1°40'8.26"S	78°38'17.74"O
CSG	RIO_CSG_UCHIMBORAZO	CHIRIOUCHC01	1°40'58.98"S	78°38'17.45"O
CSG	RIO_CSG_24ABRIL	CHIRIOABRC01	1°39'38.34"S	78°38'40.88"O
CSG	RIO_CSG_CEMENTO	CHIRIOCMTC01	1°39'16.99"S	78°40'1.38"O
CSG	RIO_CSG_POLITECNICA	CHIRIOPOLC01	1°39'23.36"S	78°40'49.30"O
CSG	RIO_CSG_UNACH	CHIRIOUNAC01	1°39'4.03"S	78°38'32.50"O
CSG	RIO_CSG_SANMIGUEL	CHIRIOSMIC01	1°38'32.86"S	78°40'22.55"O
CSG	RIO_CSG_AMBATO	CHIRIOAMBC01	1°38'16.01"S	78°40'48.68"O
CSG	RIO_CSG_CENTRO	CHIRIOCTRC01	1°40'24.13"S	78°38'51.25"O
CSG	RIO_CSG_CROACIA	CHIRIOCROC01	1°41'24.54"S	78°38'29.98"O

Tabla 2.14. Ubicación Geográfica de los Nodos e Identificación de equipos IP-RAN Parte 2

TIPO DE NODO	NOMBRE DEL SITIO	ID. *ROUTERS*	COORDENADAS GEOGRÁFICAS	
			LATITUD	LONGITUD
CSG	RIO_CSG_MORGAN	CHIRIOMORC01	1°39'13.41"S	78°41'35.22"O
CSG	RIO_CSG_ESPEJO	CHIRIOESPC01	1°39'57.00"S	78°38'37.72"O
CSG	RIO_CSG_SANTAFAZ	CHIRIOSTFC01	1°40'40.83"S	78°39'6.83"O
ASG	RIO_ASG_ORIENTAL	CHIRIOORIA01	1°39'36.00"S	78°39'45.00"O
ASG	RIO_ASG_NORTE	CHIRIONORA01	1°38'45.40"S	78°40'45.60"O
ASG	RIO_ASG_OCCIDENTAL	CHIRIOOCCA01	1°40'43.79"S	78°39'28.44"O
ASG	RIO_ASG_SUR	CHIRIOSURA01	1°41'21.64"S	78°38'4.72"O
RSG	RIO_RSG_CENTRO	CHIRIOCTRR01	1°40'24.13"S	78°38'51.25"O

Mediante el uso del software *Google Earth* se realiza la ubicación de los sitios de la IP-RAN en la ciudad de Riobamba.

En la Figura 2.8 se puede apreciar que los apuntadores amarillos señalan el lugar donde se ubicarán los *routers* CSG, los apuntadores azules indican la ubicación de los *routers* ASG, mientras que el *router* RSG se identifica con el apuntador rojo. En la imagen se debe considerar que debido a la cercanía los sitios RIO_CSG_CENTRO y RIO_RSG_CENTRO se encuentran sobrepuestos, el mismo caso ocurre con RIO_CSG_CEMENTERIO y RIO_ASG_OCCIDENTAL.

Figura 2.8. Distribución de los nodos IP-RAN en la ciudad de Riobamba [20]

2.4.2 Definición de los Enlaces de la IP-RAN

Como se describió en la sección 2.3.4, la IP-RAN hará uso de fibra óptica G.652.D para la interconexión de los equipos, en la Tablas 2.15 y 2.16 se indica cómo se realizarán los enlaces entre los nodos, cuyas longitudes se aproximan haciendo uso de *Google Earth*. Además, se indica que un *router* de acceso se conectará a *router* de borde, esto se debe a que se encuentran en la misma ubicación.

Tabla 2.15. Enlaces de la IP-RAN Parte 1

Enlace	Nodo Origen	Nodo Destino	Medio de Transmisión	Distancia [m]
1	RIO_CSG_LEONIDAS	RIO_ASG_SUR	Fibra Monomodo G.652 D	1840
2	RIO_CSG_UCHIMBORAZO	RIO_ASG_SUR	Fibra Monomodo G.652 D	800
3	RIO_CSG_CROACIA	RIO_ASG_SUR	Fibra Monomodo G.652 D	794
4	RIO_CSG_CISNEROS	RIO_ASG_SUR	Fibra Monomodo G.652 D	1550
5	RIO_CSG_UNIDO	RIO_ASG_SUR	Fibra Monomodo G.652 D	2282
6	RIO_CSG_BONILLA	RIO_ASG_OCCIDENTAL	Fibra Monomodo G.652 D	537

Tabla 2.16. Enlaces de la IP-RAN Parte 2

Enlace	Nodo Origen	Nodo Destino	Medio de Transmisión	Distancia [m]
7	RIO_CSG_CEMENTERIO	RIO_ASG_OCCIDENTAL	Fibra Monomodo G.652 D	30
8	RIO_CSG_SANTAFAZ	RIO_ASG_OCCIDENTAL	Fibra Monomodo G.652 D	680
9	RIO_CSG_MALDONADO	RIO_ASG_OCCIDENTAL	Fibra Monomodo G.652 D	1180
10	RIO_CSG_ESPEJO	RIO_ASG_OCCIDENTAL	Fibra Monomodo G.652 D	2130
11	RIO_CSG_ESTADIO	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	455
12	RIO_CSG_PINOS	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	544
13	RIO_CSG_LOMA	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	1472
14	RIO_CSG_24ABRIL	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	1983
15	RIO_CSG_UNACH	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	2430
16	RIO_CSG_CEMENTO	RIO_ASG_NORTE	Fibra Monomodo G.652 D	1682
17	RIO_CSG_SANMIGUEL	RIO_ASG_NORTE	Fibra Monomodo G.652 D	796
18	RIO_CSG_AMBATO	RIO_ASG_NORTE	Fibra Monomodo G.652 D	902
19	RIO_CSG_POLITECNICA	RIO_ASG_NORTE	Fibra Monomodo G.652 D	1179
20	RIO_CSG_MORGAN	RIO_ASG_NORTE	Fibra Monomodo G.652 D	1764
21	RIO_CSG_CENTRO	RIO_RSG_CENTRO	Fibra Monomodo G.652 D	40
22	RIO_ASG_OCCIDENTAL	RIO_ASG_NORTE	Fibra Monomodo G.652 D	4346
23	RIO_ASG_OCCIDENTAL	RIO_RSG_SUR	Fibra Monomodo G.652 D	2850
24	RIO_ASG_NORTE	RIO_ASG_ORIENTAL	Fibra Monomodo G.652 D	2444
25	RIO_ASG_ORIENTAL	RIO_RSG_CENTRO	Fibra Monomodo G.652 D	2213
26	RIO_ASG_SUR	RIO_RSG_CENTRO	Fibra Monomodo G.652 D	2280

En la Figura 2.9 se muestran los enlaces que se establecerán en la IP-RAN, donde los enlaces de color rojo indican la conexión de los *routers* de acceso con el anillo de agregación IP-RAN representado por los enlaces de color azul.

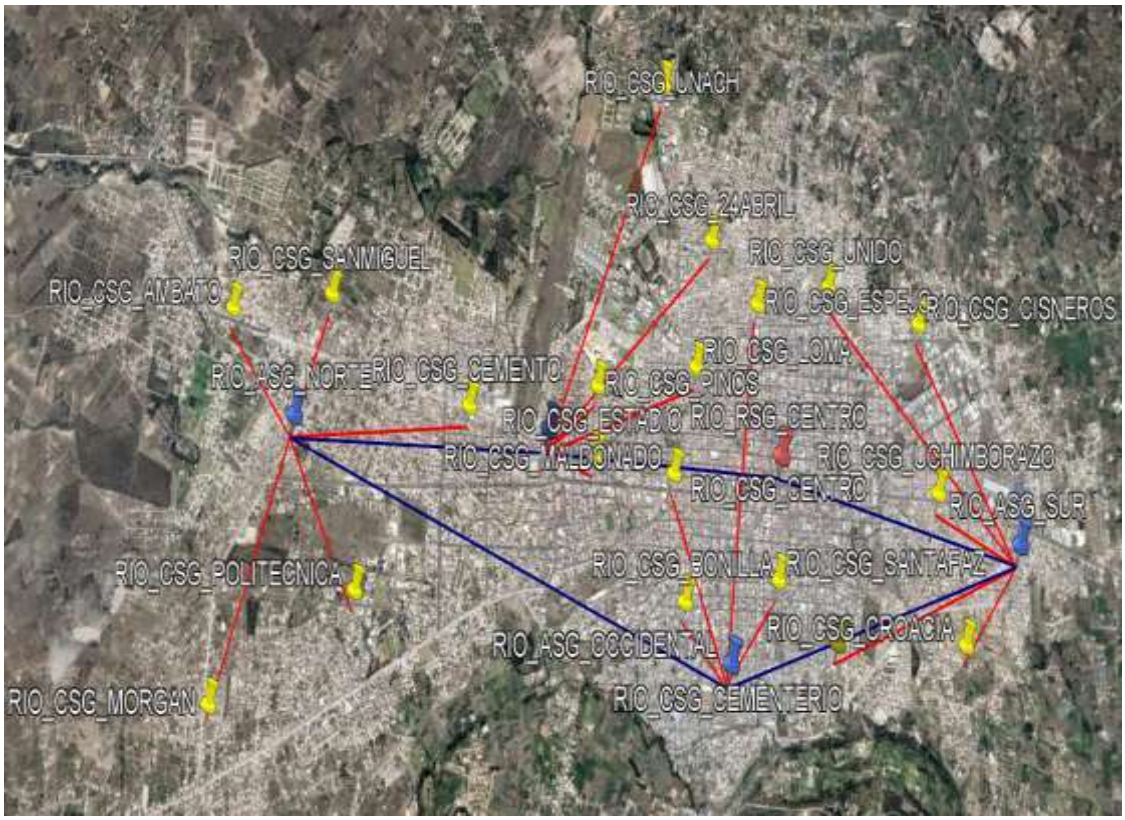

Figura 2.9. Enlaces IP-RAN en la ciudad de Riobamba [20]

También se debe tomar en cuenta que la IP-RAN se conecta con una red de transporte MPLS, la cual permite alcanzar la red troncal EPC, para lo cual se decide poner 2 enlaces desde el *router* de borde a dos *routers* PE de la nube MPLS, de tal manera que se obtiene redundancia.

En la Figura 2.10 se muestra la topología IP-RAN que contiene todas las consideraciones propuestas anteriormente.

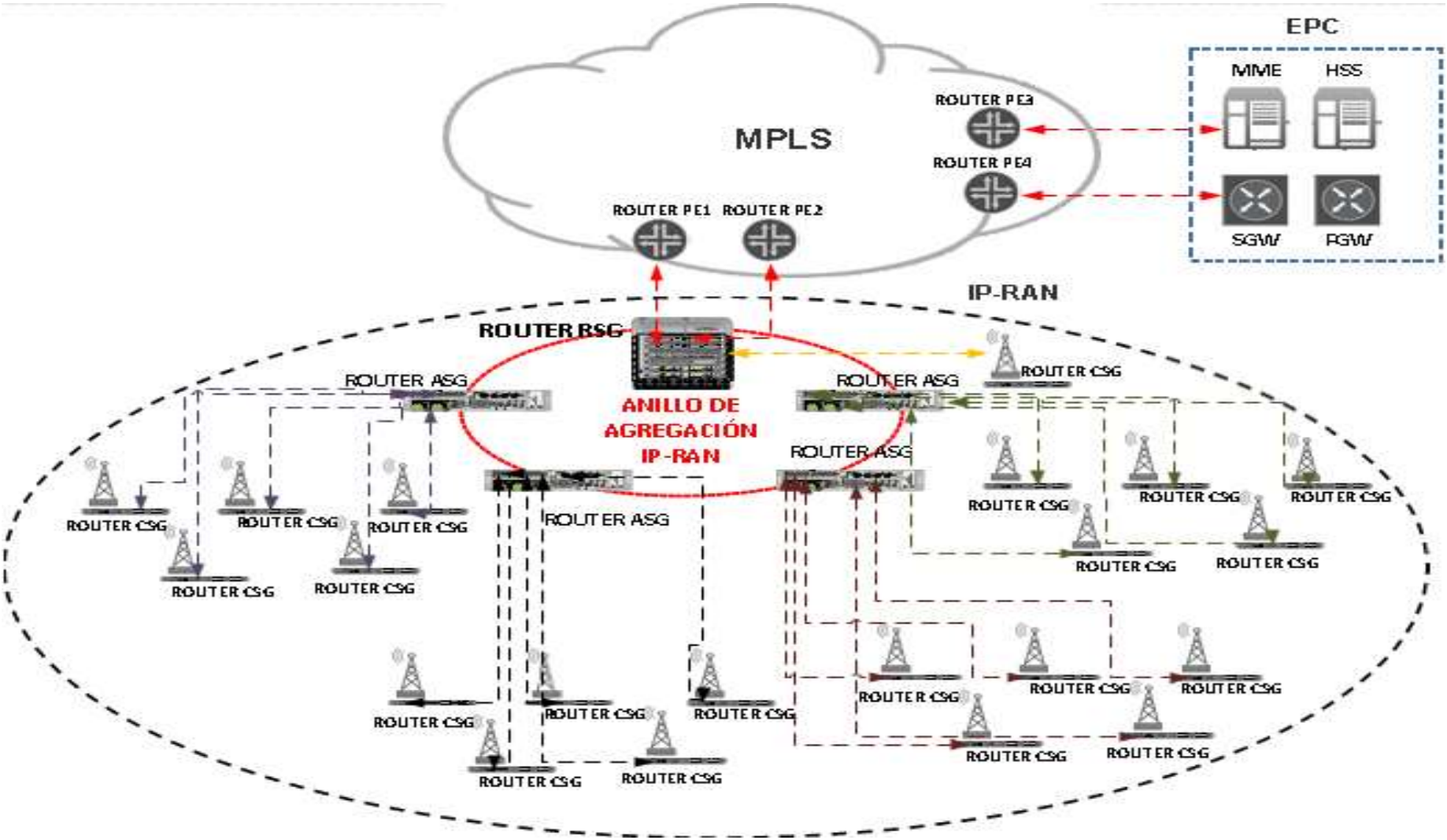

Figura 2.10. Enlaces IP-RAN con integración a la red troncal EPC

2.5 Diseño Lógico de la red IP-RAN

2.5.1 Consideraciones de Enrutamiento

ISIS: Para la conectividad en la IP-RAN se utilizará el protocolo de enrutamiento de estado de enlace IS-IS debido a que se ejecuta sobre la capa 2 del modelo OSI, lo que permite transportar información de varios protocolos de capa de red simultáneamente [9].

El diseño de la IP-RAN propone 26 *routers* y al no ser un alto número de equipos a interconectar, se define que los *routers* sean de ISIS nivel L2 en una misma área nivel 1, teniendo un límite de entre 800 a 1000 equipos en la misma área nivel 1[45].

La ventaja de implementar *routers* ISIS nivel 2 es que pueden intercambiar información de enrutamiento con otros *routers* de nivel 2 de diferente área nivel 1, esto facilita la conexión de los *routers* y permite que al operador administrar varios *routers* en un mismo AS [9].

Para la identificación de un *router* IS se define al identificador NET (*Network Entity Title*), de longitud variable entre 8 a 20 octetos y conformado por tres componentes [9], tal como se indica en la Figura 2.11.

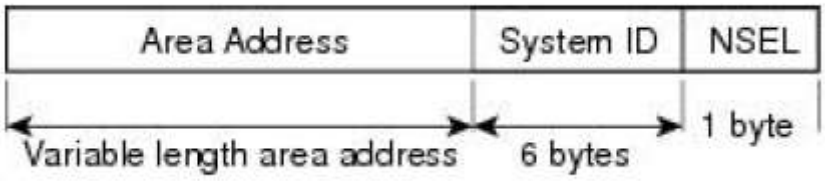

Figura 2.11. Formato NET [9]

- *Dirección de Área:* 49:0001, donde 49 indica que es una dirección privada y 0001 es el identificador del área nivel 1.
- *System ID:* 0000.0000.0001, estos 6 bytes identifican un área nivel 1.
- *NSEL:* 00, este campo no se altera [9].

Ejemplo: 49.0001.0000.0000.0001.00

En la Tabla 2.17 se muestran los identificadores NET que deberán ser configurados en los *routers* de la IP-RAN, utilizando un rango desde 49.0001.0000.0000.0001.00 hasta 49.0001.0000.0000.00ff.00 para los *routers* de acceso, un rango desde 49.0001.0000.0000.0100.00 hasta 49.0001.0000.0000.010f.00 para los *routers* de agregación y un rango desde 49.0001.0000.0000.0120.00 hasta 49.0001.0000.0000.0123.00 para el nivel de borde.

Tabla 2.17. Identificadores NET en la IP-RAN

NOMBRE DEL SITIO	HOSTNAME	NET
RIO_CSG_BONILLA	CHIRIOBONC01	49.01.0000.0000.0001.00
RIO_CSG_CEMENTERIO	CHIRIOCEMC01	49.01.0000.0000.0002.00
RIO_CSG_LEONIDAS	CHIRIOLEOC01	49.01.0000.0000.0003.00
RIO_CSG_LOMA	CHIRIOLOMC01	49.01.0000.0000.0004.00
RIO_CSG_MALDONADO	CHIRIOMLDC01	49.01.0000.0000.0005.00
RIO_CSG_ESTADIO	CHIRIOESTC01	49.01.0000.0000.0006.00
RIO_CSG_CISNEROS	CHIRIOCISC01	49.01.0000.0000.0007.00
RIO_CSG_PINOS	CHIRIOPINC01	49.01.0000.0000.0008.00
RIO_CSG_UNIDO	CHIRIOUNIC01	49.01.0000.0000.0009.00
RIO_CSG_UCHIMBORAZO	CHIRIOUCHC01	49.01.0000.0000.000a.00
RIO_CSG_24ABRIL	CHIRIOABRC01	49.01.0000.0000.000b.00
RIO_CSG_CEMENTO	CHIRIOCMTC01	49.01.0000.0000.000c.00
RIO_CSG_POLITECNICA	CHIRIOPOLC01	49.01.0000.0000.000d.00
RIO_CSG_UNACH	CHIRIOUNAC01	49.01.0000.0000.000e.00
RIO_CSG_SANMIGUEL	CHIRIOSMIC01	49.01.0000.0000.000f.00
RIO_CSG_AMBATO	CHIRIOAMBC01	49.01.0000.0000.0010.00
RIO_CSG_CENTRO	CHIRIOCTRC01	49.01.0000.0000.0011.00
RIO_CSG_CROACIA	CHIRIOCROC01	49.01.0000.0000.0012.00
RIO_CSG_MORGAN	CHIRIOMORC01	49.01.0000.0000.0013.00
RIO_CSG_ESPEJO	CHIRIOESPC01	49.01.0000.0000.0014.00
RIO_CSG_SANTAFAZ	CHIRIOSTFC01	49.01.0000.0000.0015.00
RIO_ASG_ORIENTAL	CHIRIOORIA01	49.01.0000.0000.0100.00
RIO_ASG_NORTE	CHIRIONORA01	49.01.0000.0000.0101.00
RIO_ASG_OCCIDENTE	CHIRIOOCCA01	49.01.0000.0000.0102.00
RIO_ASG_SUR	CHIRIOSURA01	49.01.0000.0000.0103.00
RIO_RSG_CENTRO	CHIRIOCTRB01	49.01.0000.0000.0120.00

Además, para mejorar los tiempos de convergencia del protocolo ISIS, se deberá implementar el protocolo BFD (*Bidirectional Forwarding Detection*), con el propósito de detectar fallas en las trayectorias de envió rápido para todo tipo de medio de transmisión, encapsulación, topología y protocolo de enrutamiento [9]. Este protocolo se debe habilitar en todas las interfaces de red, lo cual permite reducir el tiempo para anunciar cambios de topología en ISIS de 30 segundos a 300 milisegundos [44].

2.5.2 Habilitación de MPLS

Para reducir el procesamiento en los *routers* del anillo IP-RAN, se implementará MPLS, ya que permite la conmutación de paquetes, lo que evitará un re-cálculo de la ruta óptima al destino.

Esta implementación solo requiere la habilitación del protocolo en el *router* y en las interfaces requeridas, en el caso de la IP-RAN las interfaces que dispondrán MPLS son las que forman el anillo de agregación IP-RAN, donde se encuentran los *routers* ASG y RSG como se indica en la Figura 2.10.

Al disponer de equipos Cisco posibilita el uso CEF (*Cisco Express Forwarding*) que deberá ser activado en los *routers*, ya que permite reducir el uso de memoria dividiendo la información de la memoria caché de ruta en varias estructuras de datos, las cuales son: FIB y tablas de adyacencia, lo cual permite optimizar la búsqueda para el reenvío de paquetes [46].

Para realizar la distribución de etiquetas en la red MPLS se debe activar el protocolo LDP en los *routers* que conforman el anillo IP-RAN, para lo cual se utilizará la interfaz *loopback* 10. LDP construye los LSPs automáticamente mediante la información que el IGP le proporciona, por lo que ISIS debe ser implementado antes.

2.5.3 Servicios L3VPN

Para reducir el número de rutas en las tablas de enrutamiento y separar el tráfico, se dispondrán de 2 VRFs: vrf *TRAFICO-IPRAN-LTE* para aislar el tráfico de la interfaz X2 y el tráfico de la interfaz S1; y vrf *TRAFICO-GESTION-IPRAN* para la operación y mantenimiento.

Estas VRF deberán ser configuradas en los *routers* ASG, RSG y los *routers* PE conectados a la red troncal EPC, para que estos *routers* puedan intercambiar información de las VRF se deberá implementar el protocolo MP-BGP.

Para habilitar MP-BGP previamente se establecen sesiones I-BGP entre los *routers* ASG, RSG y los *routers* PE, por lo cual el anillo de agregación IP-RAN deberá establecerse en el mismo AS que la nube MPLS, mientras que los *routers* CSG se establecerán en un AS diferente como el sistema autónomo privado 65200, con lo cual establecerán sesiones e-BGP con los *routers* ASG y RSG, los cuales brindarán los servicios L3VPN a los *enodeB*.

Para realizar el intercambio de las rutas de las L3VPN se deben asociar los vecinos definidos en I-BGP (*routers* ASG, RSG y PE) a los vecinos de la familia VPNv4 definida en MP-BGP. Para el establecimiento de estas sesiones I-BGP y MP-BGP se utilizarán las interfaces *loopback* definidas en los *routers*.

Para la definición de los atributos de las VRF se utiliza el esquema: AS: XX, donde AS será el número del sistema autónomo de los *routers* CSG, mientras que XX será un número cualquiera. A continuación, se establecen los atributos de las VRF.

TRAFICO-IPRAN-LTE

- ***Route Distinguisher*:** 65200:1
- ***Route Target*:** L3VPN para el Tráfico X2 ➔ 65200:11
  L3VPN para el Tráfico S1 ➔ 65200:12

TRAFICO-GESTION-IPRAN

- ***Route Distinguisher*:** 65200:2
- ***Route Target*:** L3VPN de Mantenimiento ➔ 65200:21

En la Figura 2.12 se indica que la VRF TRAFICO-IPRAN-LTE se define en el anillo de agregación IP-RAN, es decir, en los *routers* ASG y RSG, ya que estos brindaran el servicio L3VPN que permitirá la comunicación entre los *enodeB* que se conectan a los *routers* CSG.

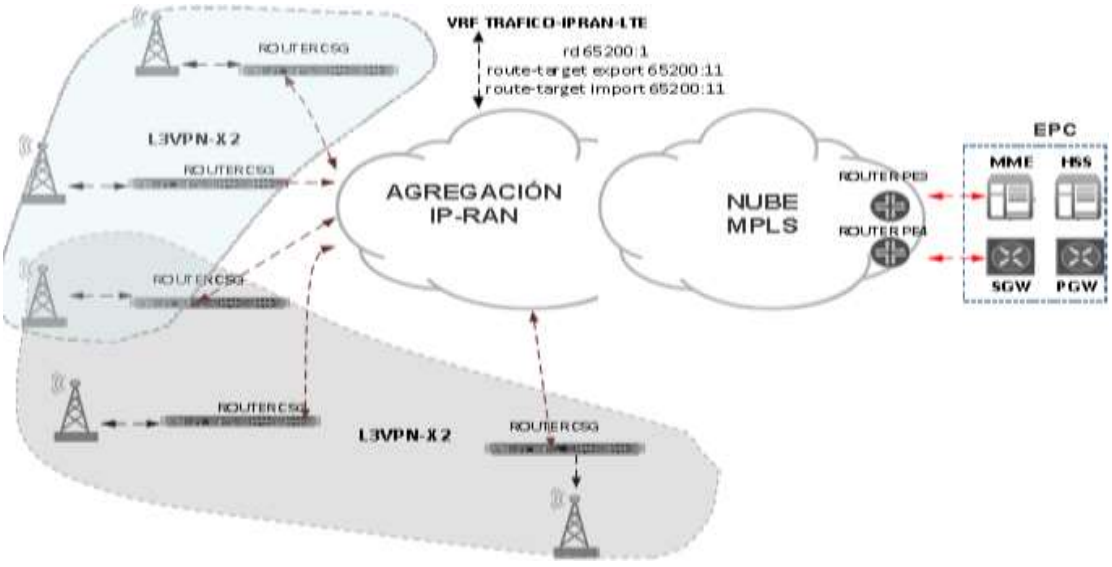

Figura 2.12. Servicio L3VPN-X2

En la Figura 2.13 se muestra que para servicio L3VPN para la interfaz S1, la VRF de tráfico LTE se define en los *routers* del anillo de agregación y en los *routers* PE que se conectan a la red troncal EPC, ya que la interfaz S1 permite que los *enodeB* se comuniquen con la entidad MME para intercambiar información de control y con la entidad S-GW para intercambiar información de datos.

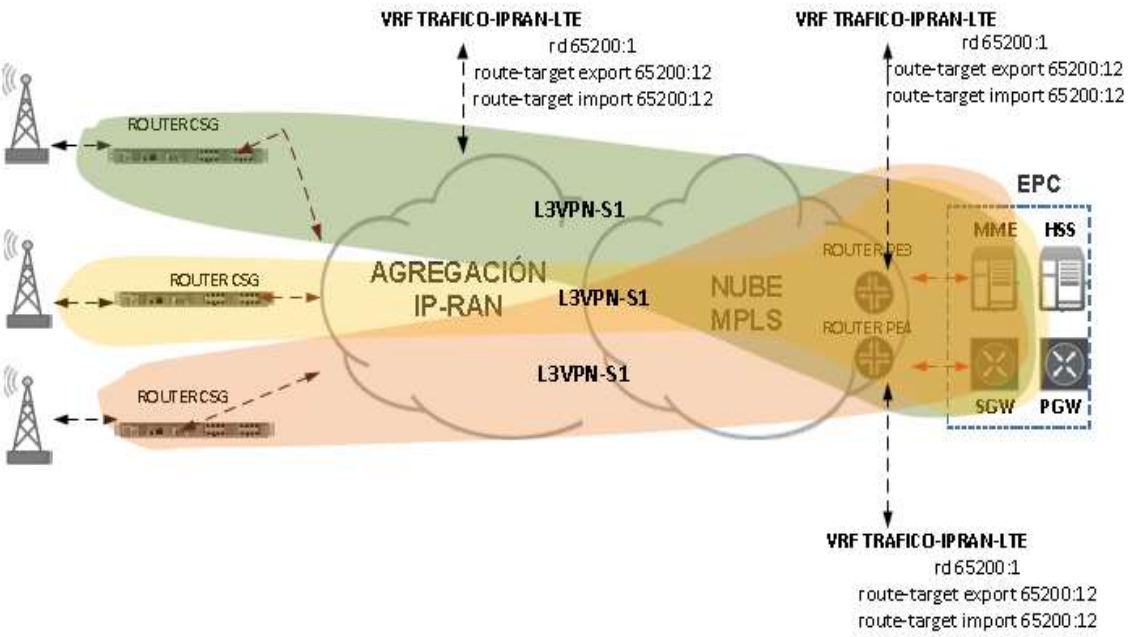

Figura 2.13. Servicio L3VPN-S1

En la Figura 2.14 se ilustra que de la VRF para gestión se deberá definir en los *routers* del anillo de agregación y en un *router* PE, ya que este brindará el servicio L3VPN a un sitio en el cual se realice el monitoreo y gestión de los *enodeB*.

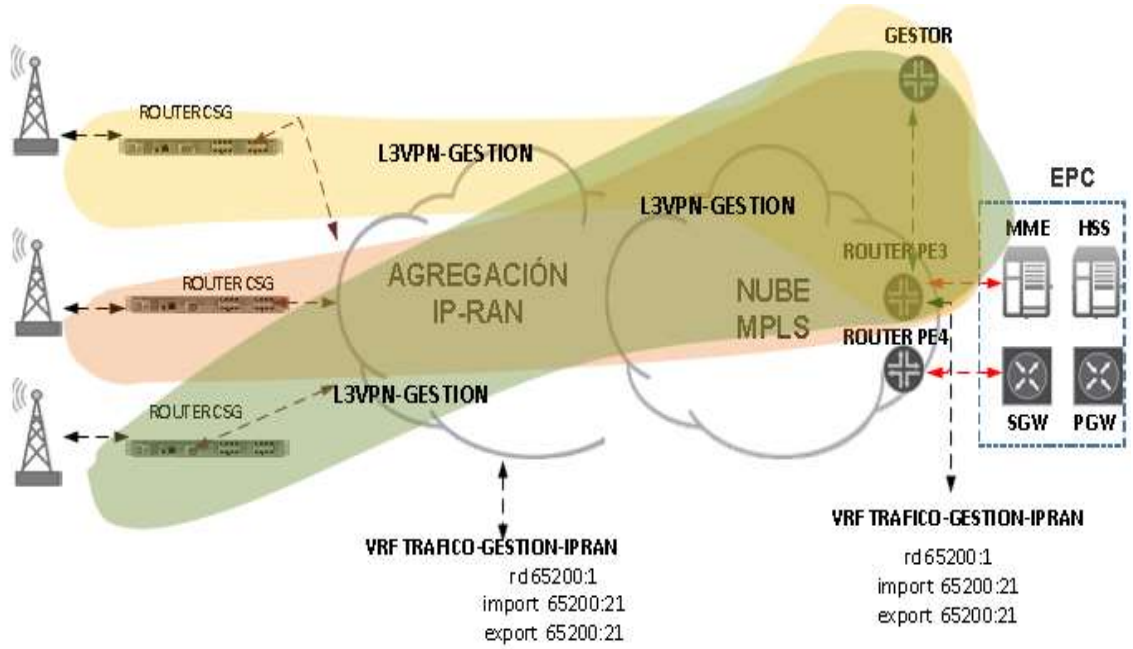

Figura 2.14. Servicio L3VPN para Gestión

2.5.4 Direccionamiento IP

Para realizar el direccionamiento de la IP-RAN se utilizarán direcciones IP privadas clase A, ya que están recomendadas para redes grandes.

La diferenciación de los *routers* dentro de la red a implementar se realiza mediante la implementación de una interfaz virtual, *loopback*, que representará la IP del sistema del *router*, esta interfaz tendrá una dirección IP con máscara /32, esta interfaz virtual podrá ser usada para los procesos BGP y MP-BGP.

En las Tablas 2.18 y 2.19 se muestra la identificación de cada *router* a implementar en la red IP-RAN para lo cual se utiliza la subred 10.1.0.0/16

Tabla 2.18. Identificación de nodos IP-RAN Parte 1

Nombre del Sitio	*Hostname*	Tipo	IP de *Loopback*	Máscara (/32)
RIO_CSG_BONILLA	CHIRIOBONC01	CSG	10.1.1.100	255.255.255.255
RIO_CSG_CEMENTERIO	CHIRIOCEMC01	CSG	10.1.2.100	255.255.255.255
RIO_CSG_LEONIDAS	CHIRIOLEOC01	CSG	10.1.3.100	255.255.255.255
RIO_CSG_LOMA	CHIRIOLOMC01	CSG	10.1.4.100	255.255.255.255
RIO_CSG_MALDONADO	CHIRIOMLDC01	CSG	10.1.5.100	255.255.255.255
RIO_CSG_ESTADIO	CHIRIOESTC01	CSG	10.1.6.100	255.255.255.255
RIO_CSG_CISNEROS	CHIRIOCISC01	CSG	10.1.7.100	255.255.255.255
RIO_CSG_PINOS	CHIRIOPINC01	CSG	10.1.8.100	255.255.255.255
RIO_CSG_UNIDO	CHIRIOUNIC01	CSG	10.1.9.100	255.255.255.255
RIO_CSG_UCHIMBORAZO	CHIRIOUCHC01	CSG	10.1.10.100	255.255.255.255
RIO_CSG_24ABRIL	CHIRIOABRC01	CSG	10.1.11.100	255.255.255.255
RIO_CSG_CEMENTO	CHIRIOCMTC01	CSG	10.1.12.100	255.255.255.255
RIO_CSG_POLITECNICA	CHIRIOPOLC01	CSG	10.1.13.100	255.255.255.255
RIO_CSG_UNACH	CHIRIOUNAC01	CSG	10.1.14.100	255.255.255.255
RIO_CSG_SANMIGUEL	CHIRIOSMIC01	CSG	10.1.15.100	255.255.255.255
RIO_CSG_AMBATO	CHIRIOAMBC01	CSG	10.1.16.100	255.255.255.255
RIO_CSG_CENTRO	CHIRIOCTRC01	CSG	10.1.17.100	255.255.255.255
RIO_CSG_CROACIA	CHIRIOCROC01	CSG	10.1.18.100	255.255.255.255
RIO_CSG_MORGAN	CHIRIOMORC01	CSG	10.1.19.100	255.255.255.255
RIO_CSG_ESPEJO	CHIRIOESPC01	CSG	10.1.20.100	255.255.255.255
RIO_CSG_SANTAFAZ	CHIRIOSTFC01	CSG	10.1.21.100	255.255.255.255

Tabla 2.19. Identificación de nodos IP-RAN Parte 2

Nombre del Sitio	*Hostname*	Tipo	IP de *Loopback*	Máscara (/32)
RIO_ASG_ORIENTAL	CHIRIOORIA01	ASG	10.1.100.100	255.255.255.255
RIO_ASG_NORTE	CHIRIONORA01	ASG	10.1.101.100	255.255.255.255
RIO_ASG_OCCIDENTE	CHIRIOOCCA01	ASG	10.1.102.100	255.255.255.255
RIO_ASG_SUR	CHIRIOSURA01	ASG	10.1.103.100	255.255.255.255
RIO_RSG_CENTRO	CHIRIOCTRB01	RSG	10.1.120.100	255.255.255.255

Las interfaces físicas que establecen los enlaces entre *routers* CSG y ASG o RSG, deben ser segmentadas en subinterfaces para poder diferenciar los servicios L3VPN, ya que se utilizarán 2 L3VPN para el tráfico generado en la red LTE y 1 L3VPN para el tráfico de gestión, estas interfaces utilizarán encapsulación dot1Q asignando la VLAN 10 para tráfico S1, VLAN 20 para el tráfico X2 y VLAN 30 para el tráfico de gestión.

En el ANEXO IV se indica que los enlaces entre los *routers* de acceso con el anillo de agregación IP-RAN para el tráfico S1 utilizarán la subred 10.1.130.0/24, para el tráfico X2 se usará la subred 10.1.131.0/24, para el tráfico de gestión se usará la subred 10.1.132.0/24. Se asignará la subred 10.10.10.0/24 para los enlaces del *router* RSG con la nube MPLS y la subred 10.10.20.0/24 se destinará para el enlace entre un *router* PE y el gestor de mantenimiento.

2.5.5 Políticas de Calidad de Servicio

El objetivo de aplicar calidad de servicio (QoS) en la red es asegurar que el tráfico de alta prioridad no sea descartado cuando exista congestión en la red [47].

Para el manejo de calidad de servicio, se propone el modelo de Servicio Diferenciado (*DiffServ*) mediante el cual se realiza la diferenciación de servicios definiendo comportamientos, denominados PHB (*Per Hop Behavior*), para cada tipo de tráfico que es identificado por el campo de DSCP (*Differentiated Services Code Point*) de IP [13].

Para realizar la clasificación del tráfico se tienen los siguientes tipos de servicio:

- **Servicio EF (*Expedited Forwarding*):** Brinda mayor garantía a los paquetes y equivale a una línea dedicada [13].
- **Servicio AF (*Assured Forwarding*):** Asegura un trato preferente a los paquetes de información, pero sin fijar garantías [13].
- **Servicio BE (*Best Effort)*:** No brinda garantías [13].

Los paquetes ya clasificados son enviados a colas para ser atendidos según la prioridad, estas colas son:

- **Cola PQ (*Priority Queuing*):** Los paquetes enviados a estas colas son atendidos con alta prioridad en caso de congestión [47].
- **Cola WFQ (*Weighted Fair Queuing*):** Esta cola asigna un peso a cada clase, esta cola es atendida después de que la cola PQ esté vacía [47].

En la Tabla 2.20 se muestran los requerimientos de QoS que se utilizan en una red LTE, con los cuales se debe efectuar la clasificación del tráfico y la correspondencia entre el campo DSCP de IP y el campo EXP de MPLS.

Tabla 2.20. Valores de DSCP y EXP para QoS en LTE [47]

Servicio	Sub-servicio	DSCP (CoS)	EXP	QoS
Wireless	Voz en Tiempo Real	46 (EF)	5	PQ
	Voz y video en tiempo real	26 (AF31)	3	PQ+WFQ
	Juegos en tiempo real	34 (AF41)	4	PQ+WFQ
	Datos en tiempo real	26 (AF31)	3	PQ+WFQ
	Señalización IMS	46 (EF)	6	PQ
	Video en tiempo no real	18 (AF21)	2	PQ+WFQ
	Voz, video y juegos en tiempo no real	18 (AF31)	2	PQ+WFQ
Control	-	46 (EF)	5	PQ
Operación y Mantenimiento	-	46 (EF)	5	PQ
	-	10(AF11)	1	PQ+WFQ

Para brindar calidad de servicio a la IP-RAN se deberá tener en cuenta los siguientes criterios:

- Los *enodeB* envían la información con tags de DSCP que la red troncal EPC espera recibir, por lo que la clasificación del tráfico se debe ejecutar en los *routers* CSG.
- La clasificación de tráfico para las interfaces que conectan el *router* CSG y el *enodeB* se basa en el campo DSCP.

- La clasificación de tráfico para las interfaces que conectan el *router* CSG y el anillo de agregación IP-RAN se basa en la correspondencia del campo DSCP con el campo EXP, ya que el anillo opera con MPLS.
- Aplicación de las políticas de tráfico entrante y saliente se realiza en las interfaces de acuerdo con la clasificación del tráfico comentada anteriormente, es decir, en las interfaces que conectan el *router* CSG con el *enodeB* se aplican políticas de clasificación de tráfico basadas en el campo DSCP, mientras que en las interfaces que conectan el *router* CSG con el anillo de agregación IP-RAN se deben aplicar las políticas de clasificación de tráfico basadas en el campo EXP.
- En los *routers* ASG y RSG solo se deben aplicar las políticas de calidad de servicio en las interfaces basándose en el campo EXP, ya que operan con MPLS [4].

2.6 Simulación de la solución IP-RAN

Para la simulación de la red IP-RAN, se utilizó el software GNS3 (*Graphical Network Simulator*), ya que la red diseñada plantea el uso de tecnología Cisco y a diferencia del programa *Cisco Packet Tracer*, GNS3 permite la simulación de protocolos necesarios para la aplicación de la IP-RAN como BGP, MPLS, entre otros.

GNS3: Este software de simulación de libre acceso permite crear, diseñar y probar redes complejas en un entorno virtual libre de riesgos [48], tal como se puede apreciar en la Figura 2.15.

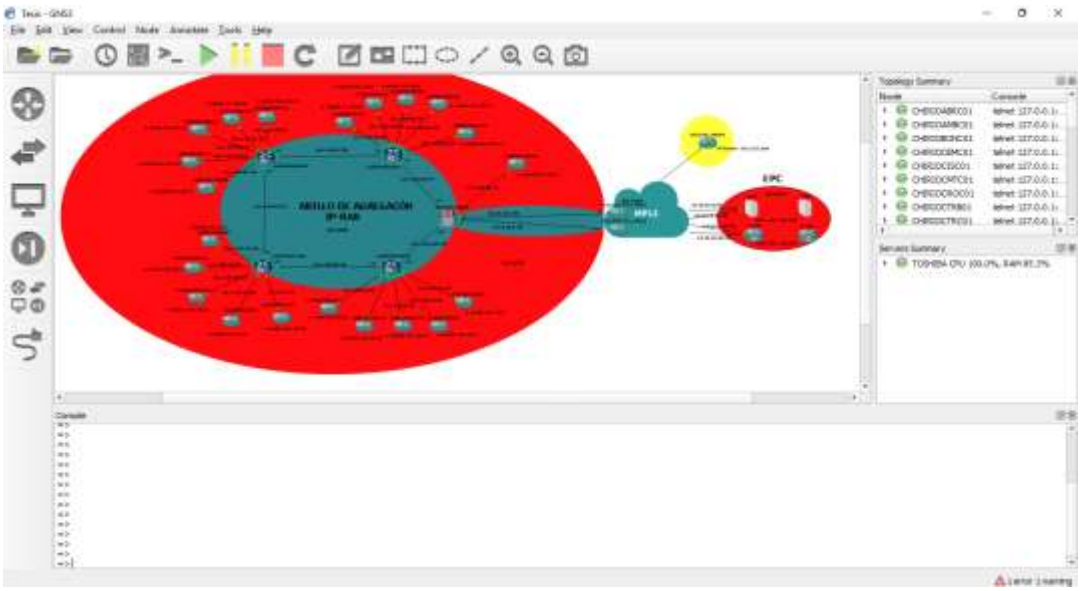

Figura 2.15. Interfaz Gráfica de GNS3 [Captura de Pantalla]

Mediante *Dynamips* [5] se proporcionan los Sistemas operativos de equipos de red de marcas como Cisco y Juniper, lo cual permite realizar configuraciones de manera similar que en los equipos físicos [48].

Para el diseño del entorno de red a simular se utilizará el IOS (*Internetwork Operating System*) Cisco del *router* c7200, tal como se puede ver en la Figura 2.16.

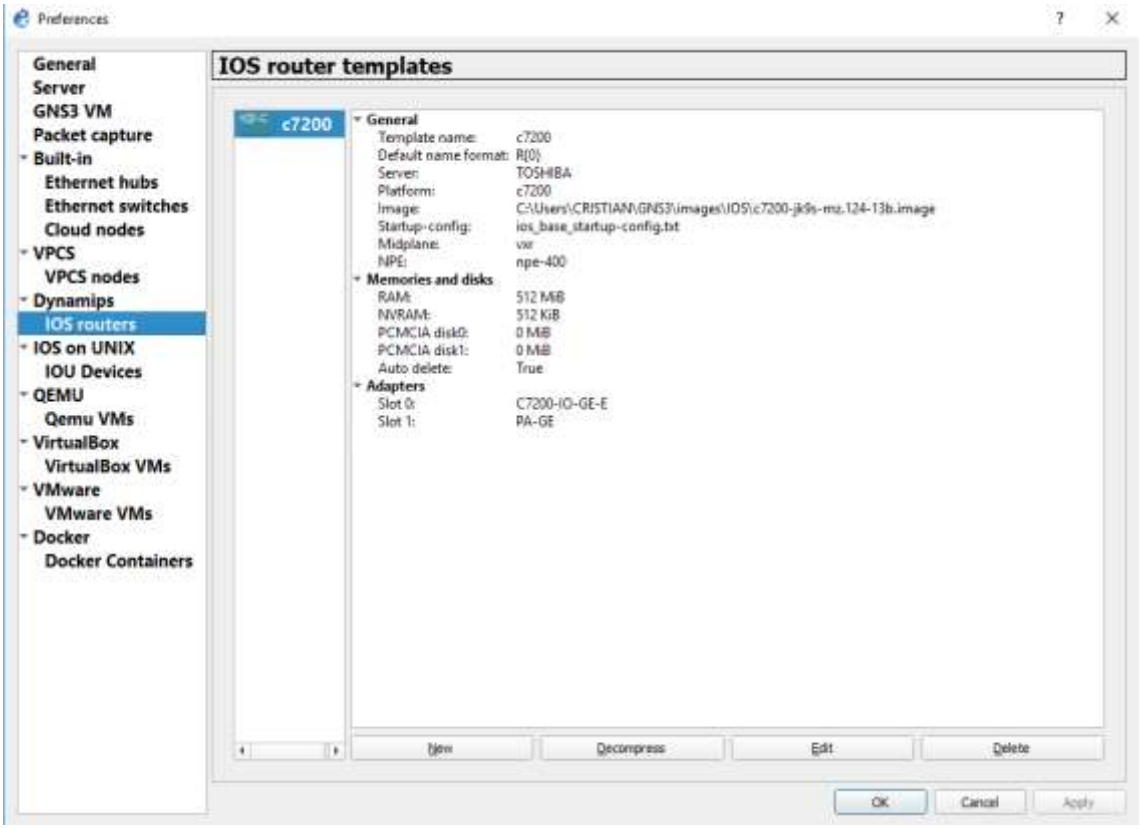

Figura 2.16. IOS Router Templates [Captura de Pantalla]

2.6.1 Criterios de simulación

El entorno de red a simular contiene la IP-RAN que permitirá la comunicación de los *enodeB* y las entidades MME y S-GW de la red troncal EPC a través de una red MPLS, la cual también permitirá que un sitio de gestión acceda a los *enodeB*; este ambiente de red se muestra en la Figura 2.17.

[5] *Dynamips*: Es un emulador que permite simular *hardware* de Cisco como *routers* y *switches,* este *software* permite la ejecución de las imágenes IOS directamente sin modificar [48].

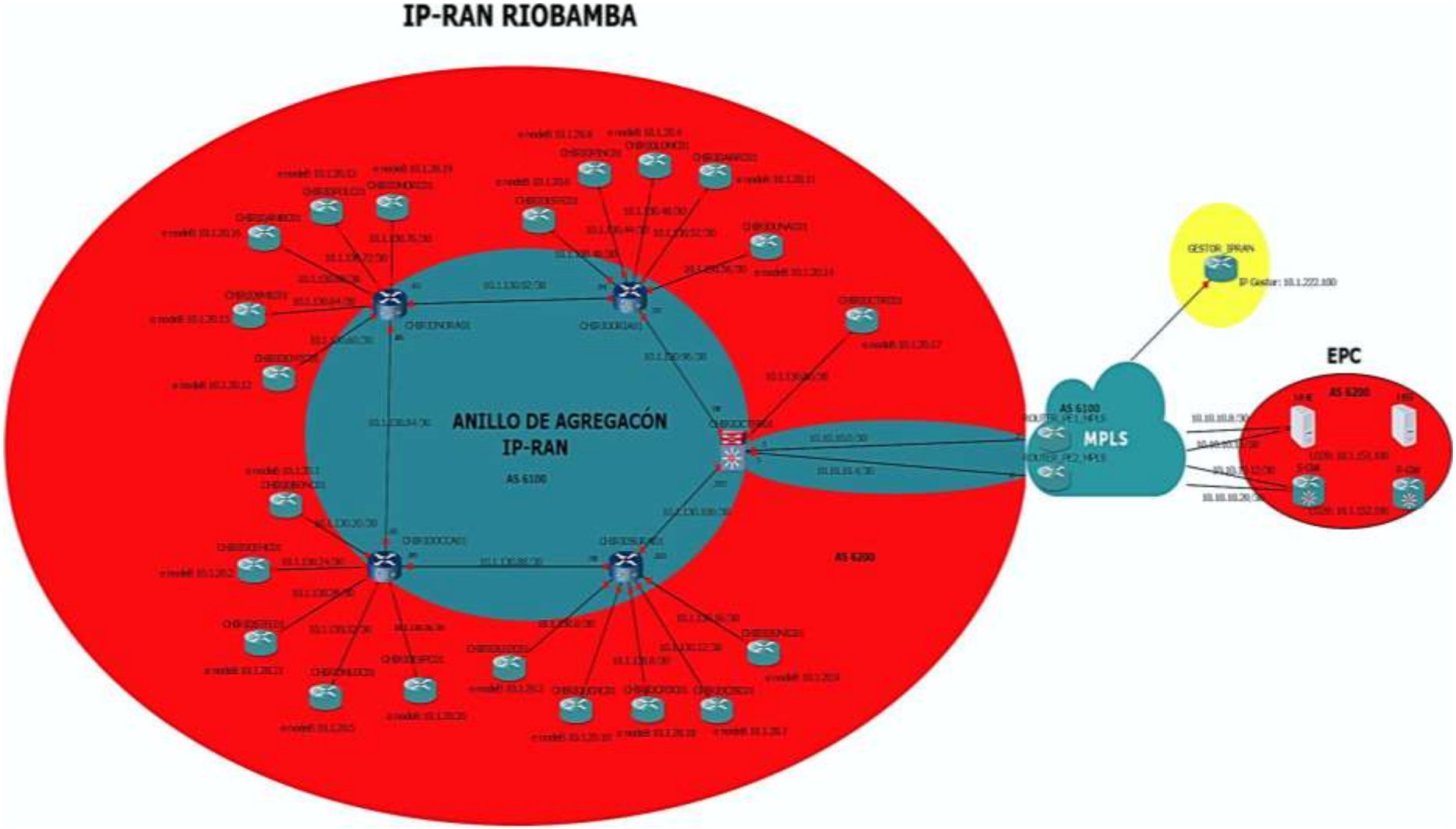

Figura 2.17. Arquitectura de la Red

. A continuación, se detallan los criterios que se utilizarán para realizar la simulación:

- ***enodeB*:** Los *routers* CSG simularán la conexión con los *enodeB* por medio de la interfaz *loopback* 20.
- **Red MPLS:** Esta red será representada por 2 *routers* PE que permitirán interconectar la IP-RAN con la red troncal EPC.
- **EPC:** 2 *routers* simularán a las entidades MME y S-GW mediante la interfaz *loopback* 20, estos *routers* se conectarán a los *routers* PE de la nube MPLS para poder alcanzar la IP-RAN.
- **Gestión IP-RAN:** 1 *router* permitirá que un sitio de gestión simulado por la interfaz *loopback* 20 pueda acceder a los *enodeB* de la IP-RAN.
- **Interfaces para Conexión:** Para la interconexión de los *routers* se utilizarán interfaces *GigabitEthernet*.
- **ISIS:** Se implementará ISIS nivel 2, estableciendo que los *routers* pertenecientes a la IP-RAN y la EPC utilizarán un área ISIS nivel 1 con identificador: 0001, mientras que los *routers* de la MPLS usarán un área ISIS nivel 1 con identificador: 0002.
- **MPLS y LDP:** Estos protocolos serán implementados en los *routers* ASG, RSG y PE.
- **BGP:** Los *routers* CSG, MME, S-GW y el GESTOR_IPRAN estarán en un AS 65200, mientras que los *routers* ASG, RSG Y PE estarán en un AS 65100.
- **Sesiones i-BGP:** Se establecerán adyacencias entre *routers* ASG, RSG y PE utilizando la interfaz *loopback* 10.
- **Sesiones e-BGP:** Se establecerán adyacencias entre los *routers* CSG y *routers* ASG o RSG mediante subinterfaces, según el servicio L3VPN.
- **Sesiones MP-BGP:** Estas sesiones se establecerán entre *routers* ASG, RSG y PE utilizando la interfaz *loopback* 10.
- **L3VPN:** Se utilizarán 2 VRFs para brindar servicios VPN, tal como se describe en la sección 2.5.3.

En la Tabla 2.21 se indica cómo se utilizarán las interfaces y subinterfaces de los *routers* de acceso de la IP-RAN.

Tabla 2.21. Asignación de Interfaces y Subinterfaces para *routers* CSG

Interfaz o Subinterfaz	Configuración de Protocolos	Destino	Subredes
loopback 10	-ISIS -Identificador BGP	-	10.1.1.100/32 - 10.1.21.100/32
loopback 20	-	MME, S-GW y GESTOR_IPRAN	10.1.20.1/32 - 10.1.20.21/32
Gi0/0.10	-Servicio L3VPN-S1 (VLAN 10)	*Router* ASG o RSG	10.1.130.0/30 - 10.1.130.80/30
Gi0/0.20	-Servicio L3VPN-S1 (VLAN 20)	*Router* ASG o RSG	10.1.131.0/30 - 10.1.131.80/30
Gi0/0.30	-ISIS -Servicio L3VPN-GESTION (VLAN 30)	*Router* ASG o RSG	10.1.132.0/30 - 10.1.132.80/30

En la Tabla 2.22 se indica cómo se utilizarán las interfaces y subinterfaces de los *routers* de agregación de la IP-RAN.

Tabla 2.22. Asignación de Interfaces y Subinterfaces para *routers* ASG

Interfaz o Subinterfaz	Configuración de Protocolos	Destino	Subredes
loopback 10	-ISIS -Identificador para BGP, MPLS, LDP y MP-BGP	-	10.1.100.100/32 - 10.1.103.100/32
Gi0/0	-ISIS -iBGP -MPLS	*Router* ASG o RSG	10.1.130.84/30 - 10.1.130.100/30
Gi1/0	-ISIS -iBGP -MPLS	*Router* ASG o RSG	10.1.130.84/30 - 10.1.130.100/30
Gi2/0.10 - Gi6/0.10	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Routers* CSG	10.1.130.0/30 - 10.1.130.76/30
Gi2/0.20 - Gi6/0.20	-ISIS -eBGP -Asignación de VRF para L3VPN-X2 (VLAN 20)	*Routers* CSG	10.1.131.0/30 - 10.1.131.76/30
Gi2/0.30 - Gi6/0.30	-ISIS -eBGP -Asignación de VRF para L3VPN-GESTION (VLAN 30)	*Routers* CSG	10.1.132.0/30 - 10.1.132.76/30

En la Tabla 2.23 se indica cómo se utilizarán las interfaces y subinterfaces del *router* de borde de la IP-RAN.

Tabla 2.23. Asignación de Interfaces y Subinterfaces para el *router* RSG

Interfaz o Subinterfaz	**Configuración de Protocolos**	**Destino**	**Subredes**
loopback 10	-ISIS -Identificador para BGP, MPLS, LDP y MP-BGP	-	10.1.120.100/32
Gi0/0	-ISIS -iBGP -MPLS	*Router* ASG	10.1.130.96/30
Gi1/0	-ISIS -iBGP -MPLS	*Router* ASG	10.1.130.100/30
Gi2/0.10	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Router* CSG	10.1.130.80/30
Gi2/0.20	-ISIS -eBGP -Asignación de VRF para L3VPN-X2 (VLAN 20)	*Router* CSG	10.1.131.80/30
Gi2/0.30	-ISIS -eBGP -Asignación de VRF para L3VPN-GESTION (VLAN 30)	*Router* CSG	10.1.132.80/30
Gi5/0	-ISIS -iBGP -MPLS	*Router* PE1	10.10.10.0/30
Gi6/0	-ISIS -iBGP -MPLS	*Router* PE2	10.10.10.4/30

En las Tabla 2.24 y 2.25 se muestran los criterios de funcionalidad que tendrán las interfaces de los *routers* de la EPC, la MPLS y el GESTOR_IPRAN.

Tabla 2.24. Asignación de interfaces de los *routers* de la MPLS, EPC y Gestión Parte 1

Tipo de *Router*	Interfaz	Configuración de Protocolos	Destino	Subredes
PE 1	*loopback* 10	-ISIS -Identificador para BGP, MPLS, LDP y MP-BGP	-	10.1.200.100/32
	Gi0/0	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Router* MME	10.10.10.8/30
	Gi1/0	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Router* S-GW	10.10.10.12/30
	Gi2/0	ISIS level 2, MPLS	*Router* RSG	10.10.10.0/30
	Gi3/0	-ISIS -eBGP -Asignación de VRF para L3VPN-GESTION (VLAN 30)	*Router* GESTION_IPRAN	10.10.20.0/30
PE 2	*loopback* 10	-ISIS -Identificador para BGP, MPLS, LDP y MP-BGP	-	10.1.201.100/32
	Gi0/0	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Router* S-GW	10.10.10.20/30
	Gi1/0	-ISIS -eBGP Asignación de VRF para L3VPN-S1 (VLAN 10)	*Router* MME	10.10.10.16/30
	Gi2/0	iBGP	*Router* RSG	10.10.10.4/30

Tabla 2.25. Asignación de Interfaces de los *routers* de la MPLS, EPC y Gestión Parte 2

Tipo de *Router*	Interfaz o Subinterfaz	Configuración de Protocolos	Destino	Subredes
MME	*loopback* 10	-ISIS -Identificador para BGP	-	10.1.151.100/32
	loopback 20	-	*enodeB*	10.1.20.151/32
	Gi0/0	eBGP	*Router* PE1	10.10.10.8/30
	Gi1/0	eBGP	*Router* PE2	10.10.10.16/30
S-GW	*loopback* 10	-ISIS -Identificador para BGP	-	10.1.152.100/32
	loopback 20	-	*enodeB*	10.1.20.152/32
	Gi0/0	-eBGP	*Router* PE2	10.10.10.20/30
	Gi1/0	-eBGP	*Router* PE1	10.10.10.12/30
GESTION-IPRAN	*loopback* 10	-ISIS -Identificador para BGP	-	10.1.155.100/32
	loopback 20	-	*enodeB*	10.1.222.100/32
	Gi0/0	-eBGP	*Router* PE1	10.10.20.0/30

2.6.2 Comandos para la Configuración de equipos IP-RAN

A partir de los criterios mencionados anteriormente se indicarán los comandos necesarios para configurar los *routers* del entorno de red a simular.

a) *ROUTER* CSG

Comandos para la configuración de interfaces *loopback* [49]:

interface loopback *instance*
 ipv4 address *ip-address*
 no shutdown

Comandos para la configuración de interfaces [49]:

interface gigabitEthernet *slot/port.number*
 ipv4 address *ip-address*
 no shutdown

Comandos para la configuración de subinterfaces [49]:

interface gigabitEthernet *slot/port.number*
 encapsulation dot1Q *vlan-id*
 ipv4 address *ip-address*
 no shutdown

Comandos para la activación de ISIS [9]: La activación de ISIS se realiza en el modo de configuración global y en la instancia ISIS se define el identificador net y el tipo de ISIS.

router isis
 net *network-entity-title*
 is-type level-2-only

La habilitación de ISIS también se debe efectuar en las interfaces y subinterfaces, para lo cual se debe aplicar lo siguiente:

interface loopback *10*
 ip router isis

interface gigabitEthernet *0/0.30*
 ip router isis

Comandos para la configuración de BGP [11]: La activación de BGP se realiza en el modo de configuración global y en la instancia BGP se define un identificador, para lo cual se utiliza la interfaz *loopback* 10.

router bgp *65200*
 bgp router-id *ip-address*

En la misma instancia BGP se establecen las adyacencias eBGP con cada una de las 3 subinterfaces de los *routers* ASG o RSG, una para cada servicio L3VPN brindado al *enodeB.* Además, se debe tener en cuenta que las redes provenientes de los vecinos eBGP y el *router* CSG pertenecen a un AS igual, por lo cual se debe ejecutar el comando *allowas-in* para cada adyacencia a establecer, tal como se muestra a continuación:

neighbor *ip-address* remote-as *65200*
neighbor *ip-address* allowas-in

En la instancia BGP se da a conocer los *enodeB,* es decir, se publica la red que contiene la interfaz *loopback* 20 a los *routers* ASG o RSG, para lo cual se debe ejecutar el siguiente comando:

network *network-number* [mask *network-mask*]

Cabe recalcar que los comandos descritos anteriormente también aplican para la configuración del *router* GESTOR_IPRAN.

b) *ROUTER* ASG y RSG

Comandos para la configuración de la interfaz *loopback e* interfaces [49]:

interface loopback *instance*
ipv4 address *ip-address*
no shutdown

interface gigabitEthernet *slot/port.number*
ipv4 address *ip-address*
no shutdown

Comandos para configuración de VRFs [50]: Antes de configurar las subinterfaces que interconectan los *routers* ASG y RSG con los CSG, se deben definir las VRF, ya que al asignar una VRF a una interfaz o subinterfaz la dirección IP se borra. La definición de las VRFs se realiza en el modo global y en la instancia VRF se definen los atributos rd (*route distinguisher*) y *route target*, tal como se muestra a continuación:

ip vrf *TRAFICO-IPRAN-LTE*
rd *65200:1*
route-target export *65200:11*
route-target import *65200:11*
route-target export *65200:12*
route-target import *65200:12*

ip vrf *TRAFICO-GESTION-IPRAN*
 rd *65200:2*
 route-target import *65200:21*
 route-target export *65200:21*

Comandos para la configuración de subinterfaces para distinción de L3VPNs [50]: En las subinterfaces se deben definir la VRF a utilizar según el caso, tal como se indica a continuación:

interface gigabitEthernet *slot/port.number*
 encapsulation dot1Q *10*
 ip vrf forwarding *TRAFICO-IPRAN-LTE*
 ipv4 address *ip-address*
 no shutdown

interface gigabitEthernet *slot/port.number*
 encapsulation dot1Q *20*
 ip vrf forwarding *TRAFICO-IPRAN-LTE*
 ipv4 address *ip-address*
 no shutdown

interface gigabitEthernet *slot/port.number*
 encapsulation dot1Q *30*
 ip vrf forwarding *TRAFICO-GESTION-IPRAN*
 ipv4 address *ip-address*
 no shutdown

Comandos para la activación y configuración de ISIS [9]: La configuración de ISIS en los *routers* ASG y RSG sigue los mismos pasos que en el *router* CSG.
router isis
 net *network-entity-title*
 is-type level-2-only

interface loopback *10*
 ip router isis

interface gigabitEthernet *slot/port.number*
ip router isis

Comandos para la habilitación de CEF, MPLS y LDP [50]: En el modo de configuración global se activan los protocolos CEF y MPLS, además se habilita LDP como protocolo de distribución tal como se muestra a continuación:

ip cef
mpls ip
mpls ldp router-id loopback *10*
mpls label protocol ldp

Comandos para la configuración de MPLS en las interfaces [50]:
interface gigabitEthernet *slot/port.number*
mpls ip

Comandos para la configuración de BGP [50]: La habilitación de BGP y definición de su identificador se realiza de la siguiente manera:

router bgp *65100*
bgp router-id *ip-address*

En esta instancia BGP las sesiones iBGP se establecen usando la interfaz *loopback* 10 de los *routers* ASG, RSG y PE, para lo cual se debe realizar la siguiente configuración para cada vecindad a establecer:

neighbor *ip-address* remote-as *65100*
neighbor *ip-address* update-source Loopback 10

Comandos para establecimiento de sesiones MP-BGP [50]: El establecimiento de sesiones MP-BGP se debe realizar en la instancia que especifica a la familia de direcciones VPNv4. Las adyacencias MP-BGP se establecen usando la interfaz *loopback* 10 de los vecinos (*routers* ASG, RSG y PE) con los cuales se requiere intercambiar prefijos VPNv4, para lo cual se deben aplicar las siguientes líneas de comandos para cada vecino:

router bgp *65100*
 address-family vpnv4 unicast
 neighbor *ip-address* activate
 neighbor *ip-address* send-community extended

Declaración de Vecindades eBGP para establecer conexión con los clientes (*routers CSG*) [50]: El establecimiento de estas adyacencias eBGP se realizan en la instancia que especifica a la familia de direcciones IP asignadas a una VRF. Estas adyacencias se establecen con las subinterfaces de los *routers* CSG, con lo cual se tendrán 3 vecindades por *router* CSG. Las siguientes líneas de comandos se deben aplicar para cada vecindad:

router bgp *65100*
 address-family ipv4 vrf *TRAFICO-IPRAN-LTE*
  neighbor *ip-address* remote-as *65200*
  neighbor *ip-address* activate

router bgp *65100*
 address-family ipv4 vrf *TRAFICO-GESTION-IPRAN*
  neighbor *ip-address* remote-as *65200*
  neighbor *ip-address* actívate

Cabe recalcar que los comandos descritos anteriormente también aplican para los *routers* ROUTER_PE1_MPLS y ROUTER_PE2_MPLS.

Las configuraciones completas de los *routers* de la EPC, MPLS, IP-RAN y GESTOR_IPRAN se incluyen en el ANEXO V.

3. RESULTADOS Y DISCUSIÓN

En este capítulo se presentan los resultados obtenidos de la simulación y la revisión de los 3 diferentes tipos de sitios para la instalación de los equipos de la IP-RAN.

3.1. Pruebas del entorno de red

Los escenarios de prueba de la IP-RAN son los siguientes:

- **Verificación de VRFs:** Se mostrarán las VRFs que se configuraron en los *routers* que brindan servicios L3VPN.
- **Rutas de las VRFs:** Se indicarán las redes contenidas en las 2 VRFs.
- **Despliegue del servicio L3VPN para tráfico X2:** Se comprobará que hay conectividad entre los *enodeB*.
- **Despliegue del servicio L3VPN para tráfico S1:** Se verificará que existe conectividad entre los *enodeB* y la EPC.
- **Despliegue del servicio L3VPN para tráfico de Gestión:** Se indicará que existe conectividad entre los *enodeB* y el sitio de gestión IP-RAN.

3.1.1 Verificación de VRFs

Para revisar la configuración de las VRFs en los *routers* ASG, RSG y PE, se debe ejecutar el comando **show ip vrf**.

En la Figura 3.1 se muestran las 2 VRFs que deben estar presentes en los *routers* ASG, RSG y PE, el ejemplo mostrado es del *router* "CHIRIOORIA01" cuya VRF: "TRAFICO-GESTION-IPRAN" contiene 5 subinterfaces con VLAN 30, ya que existen 5 *routers* CSG conectados para recibir el servicio L3VPN-GESTION, mientras que la VRF "TRAFICO-IPRAN-LTE" contiene 10 subinterfaces, mediante las cuales los *routers* CSG acceden a servicios L3VPN-S1 con VLAN 10 y L3VPN-X2 con VLAN 20.

```
CHIRIOORIA01#show ip vrf
  Name                             Default RD          Interfaces
  TRAFICO-GESTION-IPRAN            65200:2             Gi2/0.30
                                                       Gi3/0.30
                                                       Gi4/0.30
                                                       Gi5/0.30
                                                       Gi6/0.30
  TRAFICO-IPRAN-LTE                65200:1             Gi2/0.10
                                                       Gi2/0.20
                                                       Gi3/0.10
                                                       Gi3/0.20
                                                       Gi4/0.10
                                                       Gi4/0.20
                                                       Gi5/0.10
                                                       Gi5/0.20
                                                       Gi6/0.10
                                                       Gi6/0.20
```

Figura 3.1. VRFs para servicios L3VPN en *routers* ASG

Cabe recalcar que solo se indican los resultados de la ejecución del comando show ip vrf de un router ASG, ya que la información contenida es la misma en todos los routers ASG debido a que agregan el mismo número de routers CSG.

En la Figura 3.2 se aprecian las 2 VRFs configuradas en el *router* RSG, ya que un router CSG se conecta para recibir los servicios L3VPN para el tráfico S1, X2 y de Gestión.

```
CHIRIOCTRB01#show ip vrf
  Name                              Default RD          Interfaces
  TRAFICO-GESTION-IPRAN             65200:2             Gi2/0.30
  TRAFICO-IPRAN-LTE                 65200:1             Gi2/0.10
                                                        Gi2/0.20
```

Figura 3.2. VRFs para servicios L3VPN en el *router* RSG

En la Figura 3.3 se muestran las 2 VRFs que brindarán servicios L3VPN a los *routers* MME, S-GW y GESTOR_IPRAN.

```
ROUTER_PE1_MPLS#show ip vrf
  Name                              Default RD          Interfaces
  TRAFICO-GESTION-IPRAN             65200:2             Gi3/0
  TRAFICO-IPRAN-LTE                 65200:1             Gi0/0
                                                        Gi1/0
```

Figura 3.3. VRFs para servicios L3VPN en el Router_PE1_MPLS

En la Figura 3.4 se indica solamente la VRF “TRAFICO-IPRAN-LTE,” ya que el *router* PE2 no interviene en el servicio L3VPN para Gestión, por lo que solo tiene 2 interfaces asociadas al servicio L3VPN-S1 que permite conectar las entidades MME y S-GW con los *enodeB*.

```
ROUTER_PE2_MPLS#show ip vrf
  Name                              Default RD          Interfaces
  TRAFICO-IPRAN-LTE                 65200:1             Gi0/0
                                                        Gi1/0
```

Figura 3.4. VRF en el Router_PE2_MPLS

Se debe tener en cuenta que en los *routers* PE no se usan subinterfaces, ya que los *routers* cliente (MME, S-GW y GESTOR_IPRAN) solo acceden a 1 VPN, por lo que el uso de interfaces es suficiente.

3.1.2 Rutas de las VRFs

Para revisar las rutas que contienen las VRFs se usa el comando **show ip bgp vpnv4 vrf [Nombre de la VRF]**.

En la Figura 3.5 se muestran las redes contenidas en la VRF “TRAFICO-IPRAN-LTE,” cuyas rutas permiten la comunicación entre los *enodeB* y entre los *enodeB y* las entidades MME y S-GW, representadas por las direcciones 10.1.20.151/32 y 10.1.20.152/32 respectivamente. La columna “Next Hop” muestra los identificadores (interfaz *loopback* 10) de los *routers* ASG y RSG. De acuerdo con las redes alcanzadas por los *routers* ASG y RSG, se puede distinguir con 5 colores que los 4 *routers* ASG pueden alcanzar 5 *enodeB* cada uno, mientras que el *router* RSG alcanza 1 *enodeB*, tal como se detalló en el diseño.

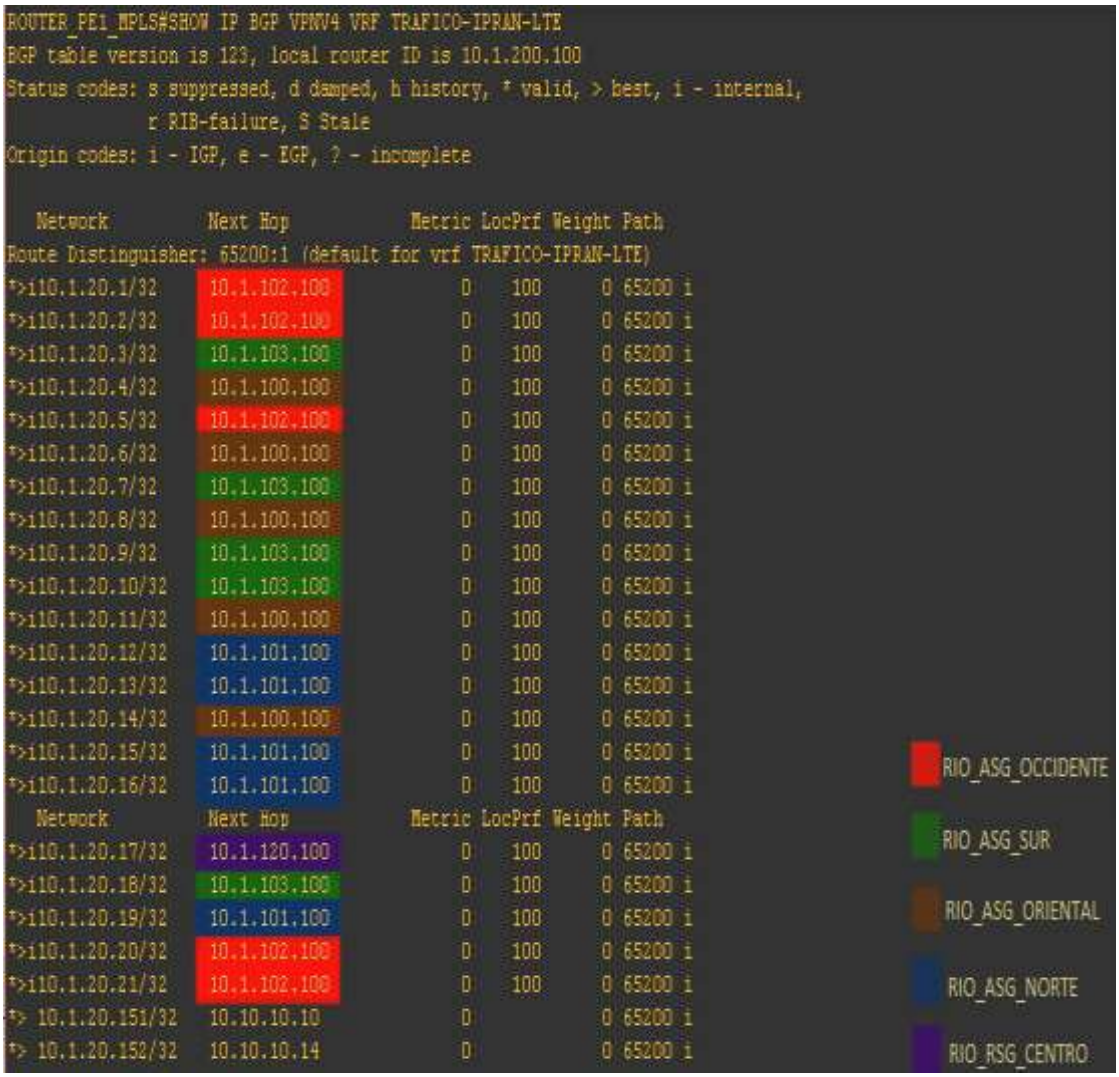

Figura 3.5. VRF para servicios L3VPN-S1 y L3VPN-X2

En la Figura 3.6 se detallan todas las redes que contiene la VRF “TRAFICO-GESTION-IPRAN,” cuyas rutas permiten que los 21 *enodeB* se puedan comunicar con el Gestor IP-RAN, representado por la dirección 10.1.222.100/32.

```
ROUTER_PE1_MPLS#show ip bgp vpnv4 vrf TRAFICO-GESTION-IPRAN
BGP table version is 178, local router ID is 10.1.200.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65200:2 (default for vrf TRAFICO-GESTION-IPRAN)
*>i10.1.20.1/32     10.1.102.100             0    100      0 65200 i
*>i10.1.20.2/32     10.1.102.100             0    100      0 65200 i
*>i10.1.20.3/32     10.1.103.100             0    100      0 65200 i
*>i10.1.20.4/32     10.1.100.100             0    100      0 65200 i
*>i10.1.20.5/32     10.1.102.100             0    100      0 65200 i
*>i10.1.20.6/32     10.1.100.100             0    100      0 65200 i
*>i10.1.20.7/32     10.1.103.100             0    100      0 65200 i
*>i10.1.20.8/32     10.1.100.100             0    100      0 65200 i
*>i10.1.20.9/32     10.1.103.100             0    100      0 65200 i
*>i10.1.20.10/32    10.1.103.100             0    100      0 65200 i
*>i10.1.20.11/32    10.1.100.100             0    100      0 65200 i
*>i10.1.20.12/32    10.1.101.100             0    100      0 65200 i
*>i10.1.20.13/32    10.1.101.100             0    100      0 65200 i
*>i10.1.20.14/32    10.1.100.100             0    100      0 65200 i
*>i10.1.20.15/32    10.1.101.100             0    100      0 65200 i
*>i10.1.20.16/32    10.1.101.100             0    100      0 65200 i
   Network          Next Hop            Metric LocPrf Weight Path
*>i10.1.20.17/32    10.1.120.100             0    100      0 65200 i
*>i10.1.20.18/32    10.1.103.100             0    100      0 65200 i
*>i10.1.20.19/32    10.1.101.100             0    100      0 65200 i
*>i10.1.20.20/32    10.1.102.100             0    100      0 65200 i
*>i10.1.20.21/32    10.1.102.100             0    100      0 65200 i
*> 10.1.222.100/32  10.10.20.2               0             0 65200 i
```

Figura 3.6. VRF para el servicio L3VPN-GESTION

Cabe recalcar que en esta sección solo se muestra el contenido de las VRFs en 1 solo *router*, ya que esta información es similar en todos los *routers* ASG, RSG y PE.

3.1.3 Escenario de Despliegue del Servicio L3VPN-X2

La L3VPN-X2 es identificada por el *route target* 65200:11 de la VRF “TRAFICO-IPRAN-LTE”. Esta VPN permitirá que los *enodeB* se interconecten entre sí, para lo cual se ingresará a uno de los *routers* CSG y se comprobará conectividad entre su *enodeB* representado por la interfaz *loopback* 20 y los 20 *enodeB* restantes, para lo cual se ejecutará el comando:

ping [dirección IP destino] source loopback 20

El comando mostrado anteriormente será utilizado en la comprobación del resto de escenarios de despliegue de servicios L3VPN.

Para la comprobación de conectividad entre los *enodeB*, en la Figura 3.7 se muestra un ejemplo en el cual se utilizó el *enodeB* conectado al *router* CSG “CHIRIOSTFC01” para realizar ping con otro *enodeB* identificado por la dirección 10.1.20.8.

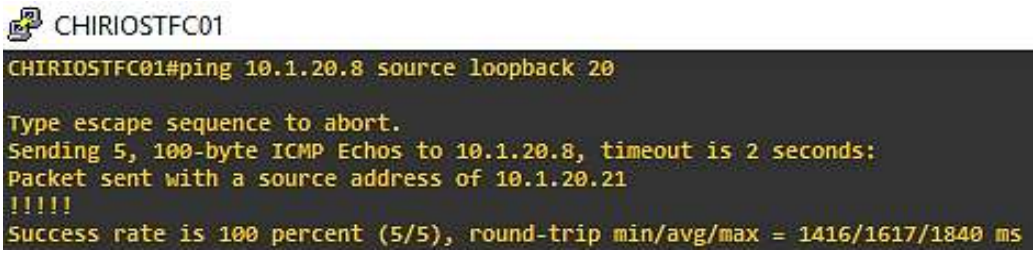

Figura 3.7. Ping entre 2 enodeB

Para verificar las rutas que sigue el tráfico de los *enodeB* para comunicarse entre sí se ejecutará el siguiente comando:

traceroute [dirección IP destino] source loopback 20

En la Figura 3.8 se indica un ejemplo del camino que deberá atravesar la información que genera el *enodeB* conectado al *router* CSG “CHIRIOSTFC01” para comunicarse con otro *enodeB. S*e puede notar que los saltos 2 y 3 identifican a MPLS, esto se debe a que los *routers* del anillo de agregación IP-RAN y los *routers* PE trabajan con este protocolo.

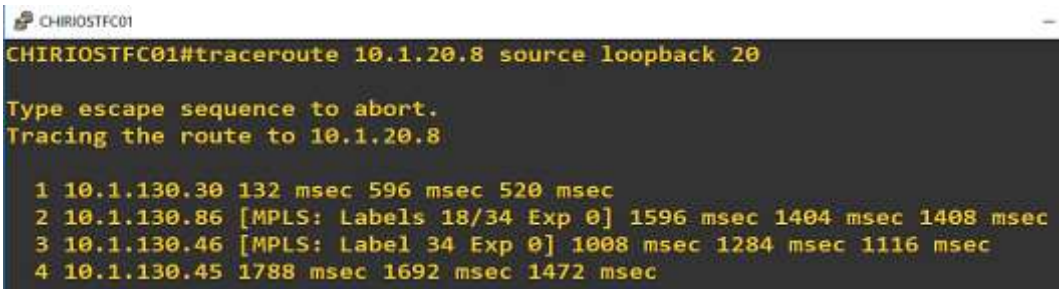

Figura 3.8. *Traceroute* entre 2 *enodeB*

En esta sección se mostró un ejemplo de conectividad con ping y traceroute entre 2 *enodeB* en el despliegue del servicio L3VPN-X2, la comprobación de conectividad para los 19 *enodeB* restantes se presenta en el ANEXO VI.

3.1.4 Escenario de Despliegue del Servicio L3VPN-S1

La L3VPN-S1 es identificada por el *route target* 65200:12 de la VRF "TRAFICO-IPRAN-LTE". Esta VPN permitirá que los *enodeB* se interconecten con las entidades MME y S-GW de la red troncal EPC.

En la Figura 3.9 se muestra un ejemplo de cómo se comprobó conectividad entre un *enodeB* y el MME, mientras que en la Figura 3.10 se demuestra que existe comunicación entre un *enodeB* y la entidad S-GW.

MME

```
MME#ping 10.1.20.9 source loopback 20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.9, timeout is 2 seconds:
Packet sent with a source address of 10.1.20.151
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1676/1869/1960 ms
```

Figura 3.9. *Ping* entre la MME y un *enodeB*

S-GW

```
S-GW#ping 10.1.20.9 source loopback 20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.9, timeout is 2 seconds:
Packet sent with a source address of 10.1.20.152
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1020/1504/1792 ms
```

Figura 3.10. *Ping* entre el S-GW y un *enodeB*

En la Figura 3.11 se indica un ejemplo de los saltos que deberá atravesar la información entre un *enodeB* y la entidad MME de la EPC, mientras que en la Figura 3.12 se muestra el camino que debe seguir el tráfico entre un *enodeB* y el S-GW.

MME

```
MME#traceroute 10.1.20.9 source loopback 20

Type escape sequence to abort.
Tracing the route to 10.1.20.9

  1 10.10.10.9 532 msec 472 msec 588 msec
  2 10.10.10.1 [MPLS: Labels 44/74 Exp 0] 1692 msec 1732 msec 1632 msec
  3 10.1.130.18 [MPLS: Label 74 Exp 0] 1296 msec 1280 msec 1340 msec
  4 10.1.130.17 1440 msec 2100 msec 1948 msec
```

Figura 3.11. *Traceroute* entre la MME y un *enodeB*

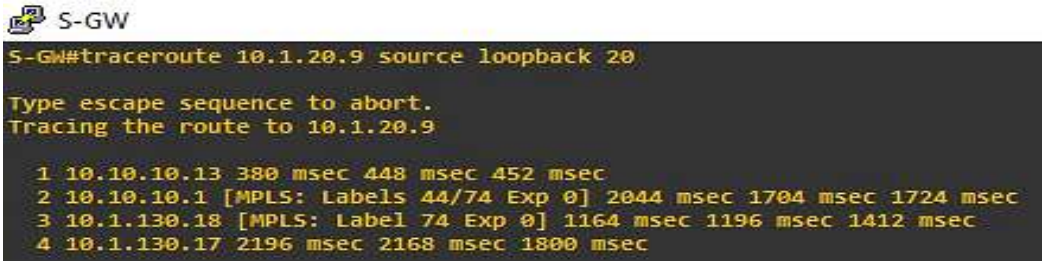

Figura 3.12. *Traceroute* entre el S-GW y un *enodeB*

En esta sección se mostró un ejemplo de conectividad mediante ping y traceroute entre un *enodeB* y la MME y un ejemplo de conectividad entre un *enodeB* y el S-GW en el despliegue del servicio L3VPN-S1, la comprobación para los 20 *enodeB* restantes se presenta en el ANEXO VII.

3.1.5 Escenario de Despliegue del Servicio L3VPN-GESTION

La L3VPN-GESTION es identificada por el *route target* 65200:2 de la VRF "TRAFICO-GESTION-IPRAN". Esta VPN permitirá la administración remota de los *enodeB*.

En la Figura 3.13 se muestra un ejemplo de cómo se comprobó conectividad entre un *enodeB* y el Gestor IP-RAN.

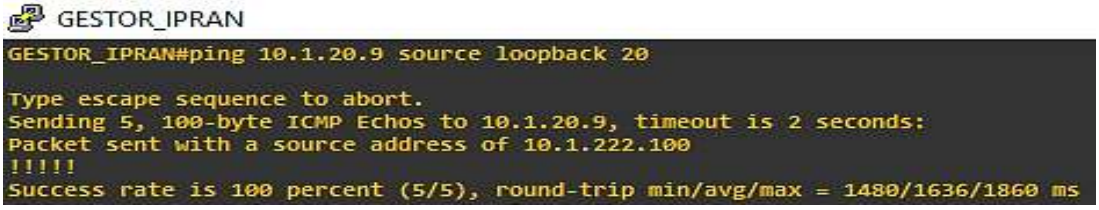

Figura 3.13. *Ping* entre un *enodeB* y el Gestor IP-RAN

En la Figura 3.14 se muestra un ejemplo del camino que deberá cruzar la información a intercambiada entre un *enodeB* y el Gestor IP-RAN.

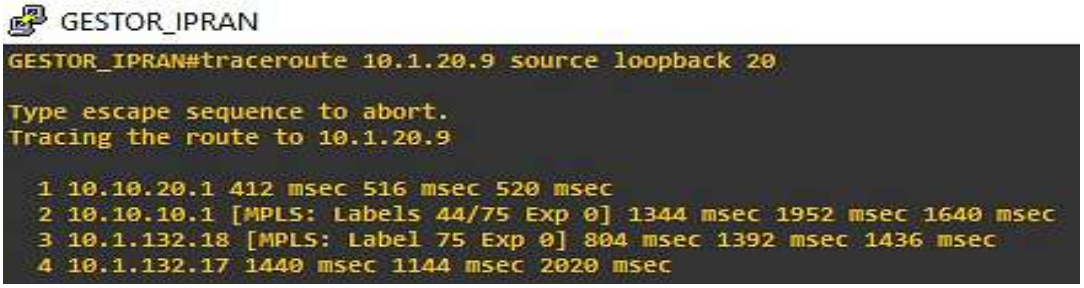

Figura 3.14. *Traceroute* entre un *enodeB* y el Gestor IP-RAN

En esta sección se mostró un ejemplo de conectividad mediante ping y traceroute entre un *enodeB* y el gestor IP-RAN en el despliegue del servicio L3VPN-GESTION, la comprobación para los 20 *enodeB* restantes se presenta en el ANEXO VIII.

3.2 Análisis para la instalación de los *routers* IP-RAN

En esta sección se realizará la revisión de los tipos de sitios, en los cuales se podrán instalar los equipos de la IP-RAN. Ya que la arquitectura IP-RAN se divide en niveles jerárquicos, se efectuará el análisis de instalación en 3 tipos de escenarios:

- Instalación para *routers* CSG
- Instalación para *routers* ASG
- Instalación para el *router* RSG

3.2.1 Instalación para *routers* CSG

Para la instalación de los *routers* CSG se toma en cuenta que estos se conectan con los *enodeB*. Los *enodeB* que se encuentran instalados en las estaciones corresponden al modelo RBS 6601 de marca Ericsson, cuyos componentes son los siguientes:

- **Unidad de distribución de Corriente Directa (DCDU):** Esta unidad de alimentación brinda energía a los equipos a través de rectificadores que transforman 220VAC en -48VDC [51].
- **Unidad de Banda Base (BBU):** Esta unidad procesa la información en banda base [51].
- **Unidad de Radio Remoto (RRU):** Estas unidades se conectan con las antenas y realizan funciones de modulación y demodulación de señales de banda base y radiofrecuencia, además la RRU permite amplificar la potencia de la señal [51].

La conexión de las unidades de los *enodeB* es en estrella [52], tal como se puede ver en la Figura 3.15.

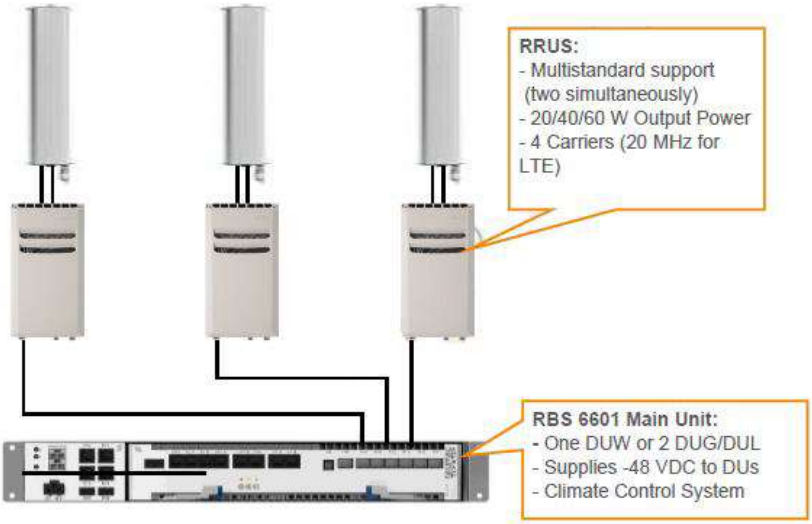

Figura 3.15. *enodeB* 6601 [52]

En las Figuras 3.16 y 3.17 se muestra la distribución de los elementos del *enodeB* en los sitios, donde las RRUs están cerca de las antenas, mientras que la DCDU y BBU se ubican dentro de un *Mini-Shelter*.

Figura 3.16. Estación Base

Figura 3.17. *Mini-Shelter* con los equipos de la estación base

La descripción de los componentes mostrados en la Figura 3.20 es la siguiente:

- **Antenas:** Tipo panel.
- **Tablero de Distribución de Energía (TDE):** Estos tableros de distribución suministran 220VAC [51].
- **Unidad de Radio Remoto (RRU)**
- **Mini-Shelter:** Es un mini rack para ambientes OUTDOOR, el cual brinda soporte y protección a los equipos [51]. En un mini-shelter generalmente se encuentra: BBU, DCDU, ODF (Optical Distribution Frames) y un banco de baterías. Dentro de una IP-RAN el *router* CSG se colocaría dentro del *mini-shelter.*

En la Figura 3.18 se puede apreciar que existe espacio suficiente para ubicar el *router* de acceso de la IP-RAN, que ocupa 1 unidad de rack [38], en el interior de un *mini-shelter.*

Figura 3.18. *Mini-Shelter*

La energización de los *routers* CSG requiere conectar uno de sus 2 alimentadores de poder, ya que el otro es redundante [38]. El tipo de corriente que utiliza este equipo puede ser AC o DC.

En la Figura 3.19 se muestra la ubicación física propuesta (cuarta unidad de rack) del *router* CSG en el *mini-shelter*. En la parte inferior se ubican los tomacorrientes de AC que permitirán energizar al *router.*

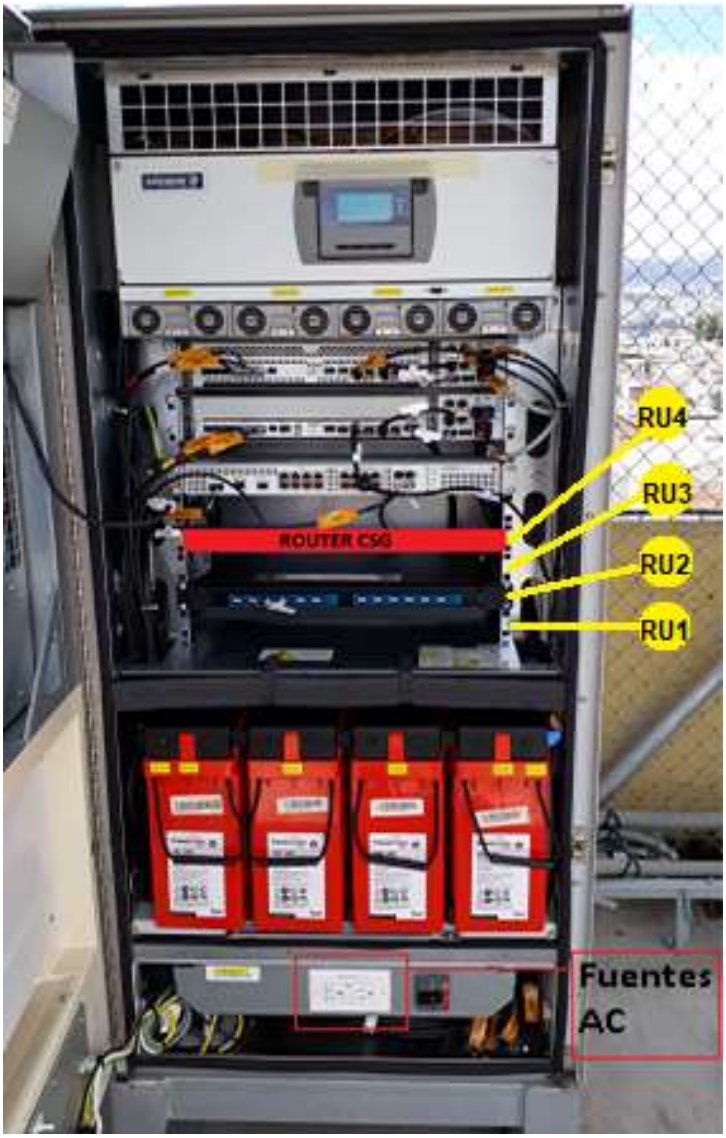

Figura 3.19. Ubicación del *router* CSG

En las Tablas 2.15 y 2.16 se obtiene que cada *router* CSG realiza una conexión con un *router ASG*, adicionalmente se debe tomar en cuenta la conexión entre el *enodeB y* el *router* CSG, tal como se muestra en la Figura 3.20.

Figura 3.20. Conexión entre el *enodeB* y el *router* CSG

Para contrarrestar el deterioro de los puertos de los *routers,* se utilizarán los ODFs que permitirán obtener reflejos de dichos puertos (estos reflejos permiten proteger las conexiones de fibra óptica contra daños).

En las Figuras 3.21 y Figura 3.22 se muestran los 2 tipos de ODF presentes en los sitios, los cuales cuentan con 12 puertos cada uno, lo que es suficiente para reflejar las 2 conexiones que deberá realizar el *router* CSG, sin embargo, se pueden instalar ODFs con más puertos de ser necesario.

Figura 3.21. ODF con terminales LC

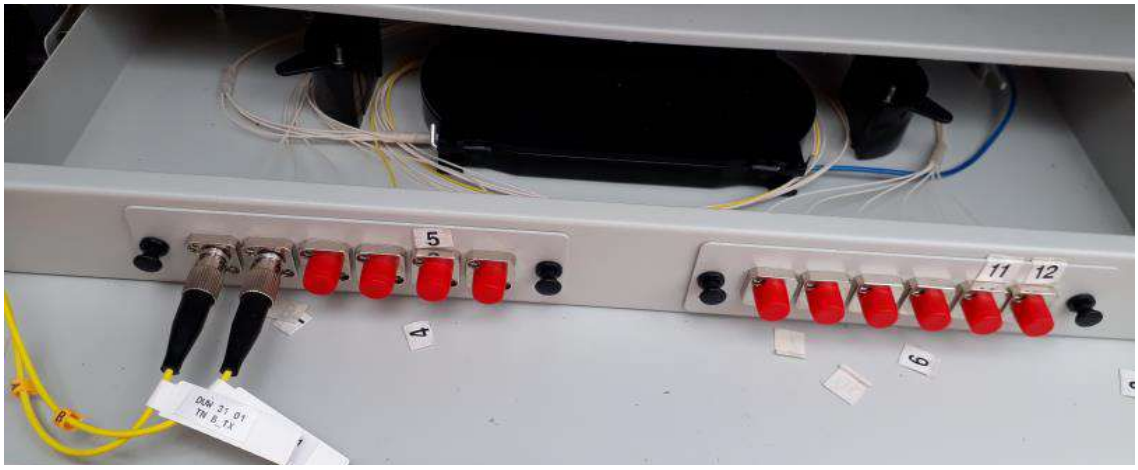

Figura 3.22. ODF con terminales FC

Debido a que generalmente los puertos ópticos o SFP de los *routers* soportan terminales LC, se utilizarán fibras G.652D LC/LC o LC/FC para reflejar los puertos utilizados para las conexiones de la IP-RAN al ODF, mientras que para la conexión entre el *enodeB* y el *router* CSG se deberán utilizar fibras G.652D LC/LC, ya que los puertos del *enodeB* soportan terminales tipo LC tal como se indicó en la Figura 3.20.

En la Tabla 3.1 se muestran las fibras adicionales, a las conexiones de la IP-RAN, el fin de estas fibras es reflejar los puertos del *router* CSG al ODF y conectar el *enodeB* con el *router* CSG.

Tabla 3.1. Fibras Adicionales para instalación de un *router* CSG

Uso de las fibras	**Cantidad de Fibras**	**Tipo**	**Longitud**
Reflejos para Transmisiones IP-RAN	1	Monomodo G.652 D	1 m
Conexión *enodeB-router* CSG	1	Monomodo G.652 D	1 m

3.2.2 Instalación para *routers* ASG

Debido a que este tipo *routers* serán parte del anillo de agregación IP-RAN estarán en ambientes *INDOOR*, es decir, en cuartos de equipos, por lo cual cada *router* ASG deberá ser instalado en un rack que tenga al menos 2 unidades de rack libres, ya que es el espacio que necesita un *router* de agregación [40].

Para energizar el equipo se necesitará al menos 1 fuente de poder AC o DC, ya que el equipo ASG tiene 2 alimentadores de poder, pero solo requiere alimentación de energía en una de sus fuentes de poder, ya que la otra es redundante [40].

Como se explicó en la anterior sección los puertos del *router* que se utilizan para transmisiones en la IP-RAN tendrán su correspondiente reflejo en los ODFs, por lo cual se pueden utilizar los ODFs existentes o instalar nuevos.

En la Figura 3.23 se muestran los requerimientos en espacio que necesitará un *router ASG* para su instalación en el rack, además se muestra la ubicación que podrá tener el ODF utilizado para obtener reflejos de los puertos del *router* y el equipamiento disponible para la energización.

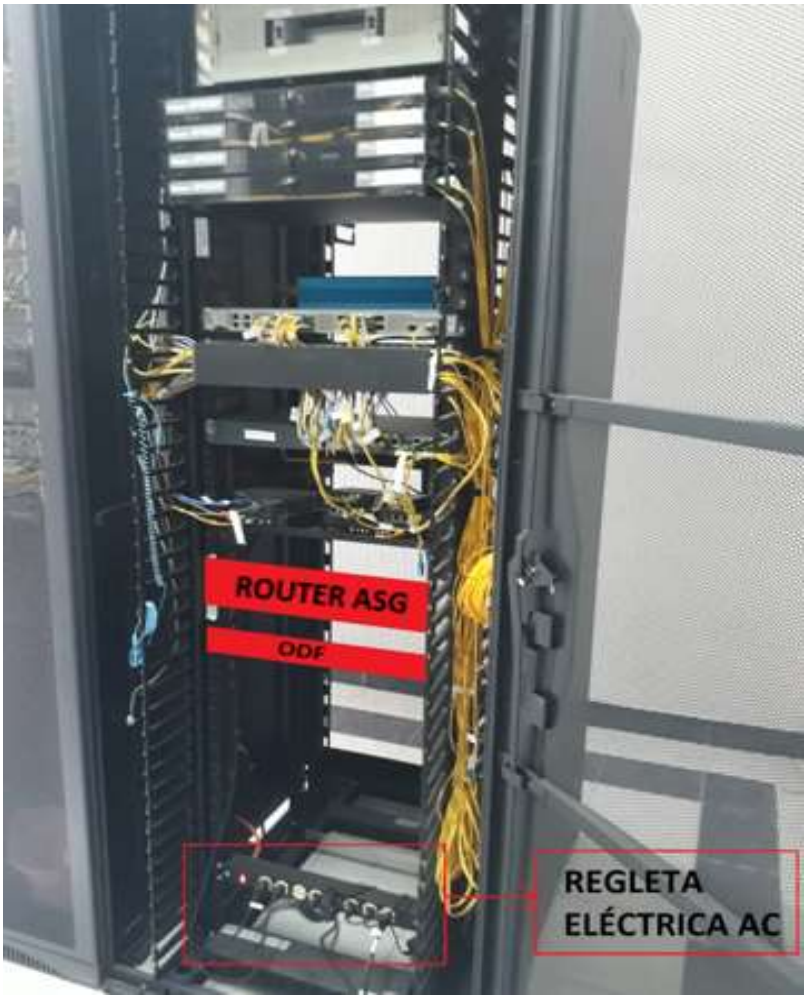

Figura 3.23. Ubicación del *router* ASG

En la Tabla 3.2 se muestran las fibras adicionales que se utilizarán para los reflejos de las transmisiones de cada *router* ASG, para lo cual se tomarán en cuenta los enlaces descritos en las Tablas 2.15 y 2.16.

Tabla 3.2. Fibras Adicionales para Instalación de un *router* ASG

Uso de las fibras	**Cantidad de Fibras**	**Tipo**	**Longitud**
Reflejos para Transmisiones IP-RAN	7	Monomodo G.652 D	1 m

Los ODFs de 12 puertos satisfacen el requerimiento para los reflejos, ya que se necesitarán 7 fibras por *router* ASG.

3.2.3 Instalación para el *router* RSG

Debido a que este tipo *router* será parte del anillo de agregación IP-RAN estará en un ambiente *INDOOR*, es decir, en un cuarto de equipos, por lo cual el *router* RSG se deberá instalar en un rack que tenga al menos 10 unidades de rack libres, ya que es el espacio que un *router* de borde necesita [42].

El equipo RSG tiene 4 fuentes de poder, pero solo requiere alimentación de energía en dos de sus fuentes, ya que las otras dos fuentes son de redundancia [42].

Como se explicó en la sección 3.2.1 los puertos del *router* que se utilizan para transmisiones en la IP-RAN y para transmisiones con la MPLS tendrán su correspondiente reflejo en los ODFs.

En la Figura 3.24. se muestran los requerimientos en espacio que necesitará un *router RSG* para su instalación en el rack, además se muestra la ubicación que podrá tener el ODF utilizado para obtener reflejos de los puertos del *router* y el equipamiento disponible para la energización.

Figura 3.24. Ubicación del *router* RSG

En la Tabla 3.3 se muestran las fibras adicionales que se utilizarán para los reflejos de las transmisiones del *router* RSG, para lo cual se tomarán en cuenta los enlaces descritos en las Tablas 2.15 y 2.16.

Tabla 3.3. Fibras Adicionales para Instalación de *routers* RSG

Uso de las fibras	Cantidad de Fibras	Tipo	Longitud
Reflejos para Transmisiones IP-RAN	3	Monomodo G.652 D	1 m
Reflejos para Transmisiones hacia la MPLS	2	Monomodo G.652 D	1 m

Los ODFs de 12 puertos satisfacen el requerimiento para los reflejos, ya que se necesitarán 5 fibras para el *router* ASG.

En la Tabla 3.4 se indica el espacio requerido (en unidades de rack) y el total de fibras requeridas por los *routers* de la IP-RAN, donde cada *router* CSG deberá contar con una fibra para la conexión hacia un *enodeB,* una fibra para la conexión hacia un *router* ASG y una fibra para el reflejo del puerto a ser utilizado para establecer conexión con el *router* ASG, mientras que cada *router* ASG deberá disponer con 5 fibras para las conexiones con *routers* CSG, 2 fibras para la conexión en el anillo de agregación IP-RAN y sus 7 reflejos correspondientes. Finalmente, el *router* RSG requerirá una fibra para la conexión con el *router* CSG, 2 fibras para la conexión en el anillo de agregación IP-RAN, 2 fibras para la conexión hacia la MPLS y 5 fibras para reflejar las conexiones detalladas anteriormente.

Tabla 3.4. Resumen de Fibras y Espacio Físico por los *routers* de la IP-RAN

Tipo de *Router*	Número de *routers*	Cantidad de Fibras por *router*	Unidades de *Rack*
CSG	21	3	1
ASG	4	14	2
RSG	1	10	10

4. CONCLUSIONES

- El estudio de la situación actual del servicio de datos móviles en la ciudad de Riobamba muestra un incremento en el número de usuarios, esto sugiere que se deben desarrollar mejoras en las redes que brindan acceso a este servicio, por lo que la propuesta de una IP-RAN se ve justificada ya que permite la expansión hacia nuevos clientes, proporciona el soporte IP requerido por tecnologías celulares como LTE y permite utilizar la infraestructura de transporte existente, reduciendo los costos de despliegue.

- En el caso del presente estudio se encontró que en el país existen redes de transporte desplegadas con tecnología Cisco, estas infraestructuras de red pueden ser utilizadas para integrarse con la IP-RAN, por lo que al momento de elegir el fabricante de los equipos se considera la marca Cisco, ya que al contar con *routers* del mismo fabricante se facilita la configuración, administración y gestión de la red.

- El resultado del análisis de tráfico para una operadora en la ciudad de Riobamba estima al 60% de ocupación de la red, por lo que la IP-RAN deberá soportar al menos 4,88 Gbps, mientras que la capacidad que el router de borde deberá soportar para procesar los datos de los usuarios del país es de al menos 1,77 Tbps. Esto se debe a que el *router* de borde RSG es el equipo que dirigirá la información de todos los *enodeBs* hacia la red de transporte MPLS que permite alcanzar la EPC.

- El número total de *routers* dispuestos en el diseño de la IP-RAN es de 26, de los cuales 21 *routers* se encuentran en el nivel de acceso, ya que estos equipos se deberán comunicar con 21 *enodeBs* en la ciudad de Riobamba, mientras que en el anillo de agregación IP-RAN se dispone de 4 *routers* ASG y un *router* RSG.

- El diseño IP-RAN planteado permite la integración de los *routers* del nivel de agregación y borde con la red de transporte MPLS, esto posibilita que los *routers* del anillo de agregación IP-RAN ofrezcan servicios L3VPN, ya que son configurados como *routers* PE, con lo que se logra el intercambio de información de las VRFs, cuyas rutas permiten la comunicación de entre los *enodeBs,* entre *enodeBs* y EPC, y entre el sitio de gestión y los *enodeBs.*

- La creación de 2 VRFs permite diferenciar el tráfico LTE y el tráfico de gestión. Para la VRF que maneja el tráfico LTE se tienen dos L3VPN, una L3VPN para la información de usuario, cuyo tráfico es intercambiado entre los *enodeB* y el S-GW, y otra L3VPN para la información de control, cuyo tráfico es intercambiado entre los *enodeB* y el MME. La VRF de gestión, permite el intercambio de información entre el sitio de gestión IP-RAN y los *enodeB.*

- El ambiente de red simulado con tecnología Cisco, se logra con el software GNS3, ya que a diferencia del simulador Packet Tracer, permite la implementación de protocolos avanzados como MPLS y MP-BGP. En GNS3 se pudo comprobar conectividad entre *enodeB,* EPC y el sitio de gestión mediante la creación L3VPN.

- Para establecer el esquema de instalación de los equipos IP-RAN primero se realizó una revisión del estado de los sitios, donde se logró diferenciar 3 tipos de instalación. Para la instalación de los *routers* CSG se encontró en todos los casos ambientes en exteriores donde la BBU del *enodeB* se encuentra en el interior de un *mini-shelter*, ya que los *mini-shelters* disponen más de una unidad de rack libre se decidió ubicar al *router* de acceso de la IP-RAN en su interior. La instalación de los *routers* ASG y RSG se deberá realizar en cuartos de equipos, para lo cual existen racks con suficiente espacio para la instalación, las diferencias de instalación de estos 2 tipos de *routers* son los requerimientos de espacio y las fuentes necesarias para alimentar los equipos ya que el *router* ASG necesita solo 1 fuente, mientras que el *router* RSG necesita 2 fuentes.

RECOMENDACIONES

- El diseño de la IP-RAN permite la integración de otros servicios, ya que existen puertos libres en los *routers*. Para dar acceso a nuevos servicios se deberá realizar un análisis de capacidad para evaluar si la capacidad procesamiento de los *routers* es el suficiente.

- El planteamiento del presente diseño se realiza para la ciudad Riobamba, sin embargo, puede ser expandida a nivel nacional, ya que la IP-RAN permite la integración de múltiples redes, por lo que se pueden proponer anillos de agregación que concentren la información de las principales ciudades para luego ser enviada hacia las redes de *Core*.

- Se sugiere profundizar el análisis de tráfico, ya que podrían variar ciertos factores que no se tomaron en cuenta en este Trabajo de Titulación, tales como el incremento del flujo de datos con respecto a los servicios brindados por LTE o la mejora en servicios que propone la tecnología LTE *Advanced*, la cual apenas está incursionando en el país.

- Para la protección de la red y de los usuarios, se recomienda el planteamiento de políticas de seguridad tanto a nivel físico como lógico, tales como la configuración de claves de acceso a los equipos, el control del acceso a la red por medio de ACLs (*Access Control Lists*), la inclusión de políticas de acceso por MAC en los puertos y la implementación de control biométrico para el acceso a los cuartos de equipos.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) "Internet: ARCOTEL: Estadísticas del Servicio Móvil Avanzado (SMA), " 2018.

[2] R. Agusti Comes, F. Bernardo Álvarez, F. Casadevall Palacio, R. Ferrús Ferre, J. Pérez Romero y O. Sallent Roig, "LTE: NUEVAS TENDENCIAS EN COMUNICACIONES MÓVILES," Fundación Vodafone España, 2010.

[3] F. Segales Pejovez, "Diseño y Simulación de red de transporte IPRAN, en la ciudad de Arequipa para una red LTE (4G)," Tesis de Ingeniería Electrónica, Universidad Nacional de San Agustín, Arequipa, 2014.

[4] A. Montilla Bravo, "Arquitectura de red de acceso móvil de cuarta generación: mobile-IP RAN," Tesis Doctoral en Ingeniería Telemática, Universidad Carlos III de Madrid, Leganés, España, 2009.

[5] H. Shahzad y N. Jain, "Internet Protocol Based Mobile Radio Access Network Architecture for Remote Service Areas," Tesis de Maestría en Ciencias, Kungliga Tekniska Högskolan (KTH), Estocolmo, 2007

[6] A. Ayala Abarca, "Estudio y Diseño de una Red de Transporte IP RAN para voz y datos para Redes de Telefonía Celular de Cuarta Generacion en el Ecuador," Tesis de Ingeniería en Electrónica y Telecomunicaciones, Escuela Politécnica del Ejército, Quito, 2011.

[7] A. Tanenbaum y D. Wetherall, "Redes de Computadoras," Quinta Edición, 2012

[8] W. Stallings, "Comunicaciones y Redes de Computadoras," Séptima Edición, 2004

[9] Cisco Systems, "IP Rounting: ISIS Configuration Guide, Cisco IOS Release 15M&T," 2015

[10] W. Crow, "Análisis de Calidad de Servicio en Transferencia de Voz y Video en una Red de Tecnología MPLS (Multi-Protocol Label Switching)," Tesis de Ingeniería en Electrónica y Telecomunicaciones y Redes, Escuela Superior Politécnica de Chimborazo, 2016.

[11] Cisco Systems, "BGP Case Studies," 2008

[12] I. Minei y J. Lucek, "MPLS-Enabled Aplications: Emerging Dvelopments and New Technologies," John Wiley & Sons, Ltd, 2005.

[13] P. Hidalgo, "Telemática II," Escuela Politécnica Nacional, 2016.

[14] L3VPN Features - RTN 980L V100R009C10 Feature Description 03- Huawei, 2018. Último acceso (2018,5) [Online]. Disponible en: http://support.huawei.com/enterprise/kr/doc/DOC1000133222?section=j00d

[15] Layer 2 VPNs and VPLS Feature Guide For Routing Devices, 2016. Último acceso (2018,5) [Online]. Disponible en: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpws-overview.html

[16] ARCOTEL - Densidad de líneas activas y participación de mercado. Último acceso (2018,5) [Online]. Disponible en: http://www.arcotel.gob.ec/servicio-movil-avanzado-sma/

[17] ARCOTEL - Densidad de líneas activas por tecnología. Último acceso (2018,5) [Online]. Disponible en: http://www.arcotel.gob.ec/servicio-movil-avanzado-sma/

[18] ARCOTEL - Boletín Estadístico: Regulación y Control de las Telecomunicaciones (junio 2018). Último acceso (2018,7) [Online]. Disponible en: http://www.arcotel.gob.ec/wp-content/uploads/2015/01/BOLETIN-ESTADISTICO-Junio-2018_f.pdf

[19] N. Cadena Oleas, "Plan de Desarrollo y Ordenamiento Territorial," Alcaldía de Riobamba, Febrero 2015.

[20] Google Earth Pro. Último acceso (2018,7) [Online]. Disponible en: https://www.google.com/earth/

[21] ARCOTEL – Proyección cantonal total 2010-2020. Último acceso (2018,5) [Online]. Disponible en: http://www.arcotel.gob.ec/poblacion-del-ecuador-2/

[22] INEC, Población y Demografía - Información Censal. Último acceso (2018,7) [Online]. Disponible en: http://www.ecuadorencifras.gob.ec/informacion-censal-cantonal/

[23] C, Castillo, “Dimensionamiento de un clúster de red LTE para brindar cobertura en la zona comercial de la ciudad de Loja,” Tesis de Maestría en Redes de Comunicaciones, Pontificia Universidad Católica del Ecuador, Quito, 2017.

[24] LTE Radio Network Capacity Dimensioning. Último acceso (2018,7) [Online]. Disponible en: http://www.academia.edu/30146860/LTE_Radio_Network_Capacity_Dimensioning

[25] Top Optimized Technologies, “Estudio sobre los requisitos técnicos que permitan caracterizar la cobertura con tecnología LTE necesaria para proporcionar determinados servicios de datos,” Estudio para la Dirección General de Telecomunicaciones y Tecnologías de la Información, España, 2014.

[26] A, Dziech and A. Czyżewski, "Multimedia Communications, Services and Security," 4th International Conference, MCSS, Krakow Poland, June 2-3, 2011

[27] Tecnología CNT, 2018. Último acceso (2018,7) [Online]. Disponible en: http://corporativo.cnt.gob.ec/tecnologia/

[28] ARCOTEL - Radiobases por prestador y tecnología. Último acceso (2018,5) [Online]. Disponible en: http://www.arcotel.gob.ec/servicio-movil-avanzado-sma/

[29] M. S. Jiménez, "Comunicaciones Ópticas," Escuela Politécnica Nacional, 2016.

[30] Recomendación G.652 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.652/es

[31] Recomendación G.653 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.653/es

[32] Recomendación G.654 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.654/es

[33] Recomendación G.655 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.655/es

[34] Recomendación G.656 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.656/es

[35] Recomendación G.657 I.T.U-d. Último acceso (2018,7) [Online]. Disponible en: https://www.itu.int/rec/T-REC-G.657/es

[36] J. Carrera, "Diseño de una red de transporte óptica basada en tecnología DWDM para la red SDH de CNT E.P. en Riobamba," Tesis de Ingeniería en Electrónica y Redes de Información, Escuela Politécnica Nacional, 2018

[37] Módulos SFP. Último acceso (2018,7) [Online]. Disponible en: http://optronics.com.mx/modulos/eCommerce/fotos/MduloSFP.pdf

[38] Cisco ASR 1001-HX Router and Cisco ASR 1002-HX Router. Último acceso (2018,7) [Online]. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/1001HX_1002HX/b_ASR1001HX-1002HX_HIG/b_ASR1001HX-1002HX_HIG_chapter_01.html

[39] Huawei ATN 910B-A Router. Último acceso (2018,7) [Online]. Disponible en: https://carrier.huawei.com/~/media/CNBG/Downloads/Product/Fixed%20Network/carrierip-router/ATN%20910B-English-version.pdf

[40] Cisco ASR 9001 Router. Último acceso (2018,7) [Online]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/routers/asr-9001-router/data_sheet_c78-685687.html

[41] Huawei ATN 950B Router. Último acceso (2018,7) [Online]. Disponible en: https://carrier.huawei.com/~/media/CNBG/Downloads/Product/Fixed%20Network/carrierip-router/ATN%20950B-English-version.pdf

[42] Cisco ASR 9006 Router. Último acceso (2018,7) [Online]. Disponible en: https://www.cisco.com/c/en/us/support/routers/asr-9006-router/model.html

[43] Huawei NE40E-X2-M5 Router. Último acceso (2018,7) [Online]. Disponible en: http://www1.huawei.com/ucmf/groups/public/documents/webasset/hw_413816.pdf

[44] V. Vega, "Diseño de una red IP-RAN para el trasnporte de tráfico de datos de una red de telefonía celular de cuarta generación con tecnología LTE par aun operador móvil, en la ciudad de Machala, provincia de El Oro, Ecuador," Tesis de Maestría en Telecomunicaciones, Universidad Católica de Santiago de Guayaquil, 2016

[45] IS-IS Deployment, Design Guidelines and New Features, Cisco Systems. Último acceso (2018,7) [Online]. Disponible en: https://www.nanog.org/meetings/nanog24/presentations/isis.ppt

[46] Comprensión de Cisco Express Forwarding (CEF). Último acceso (2018,8) [Online]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/routers/12000-series-routers/47321-ciscoef.pdf

[47] J. Paredes, "Optimización de la Red de Acceso IP para interconectar nodos LTE (IP RAN) hacia el *core* de servicios de la plataforma de datos móviles," Tesis de Maestría en Redes de Comunicaciones, Pontificia Universidad Católica del Ecuador, 2016

[48] GNS3. Último acceso (2018,8) [Online]. Disponible en: https://www.gns3.com

[49] Cisco Systems, "Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.X, Configuring Layer 3 Interfaces," 2018

[50] Cisco Systems, “MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T,” 2018.

[51] E. García, “Diseño e Instalación de un nodo B adicional en una zona de alto tráfico de la ciudad de El Coca provincia de Orellana para aumentar capacidad y cobertura de la red UMTS,” Tesis de Ingeniería en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, 2015.

[52] EnodeB Ericsson RBS 6601. Último acceso (2018,8) [Online]. Disponible en: https://www.launch3telecom.com/shared_media/datasheet/RBS%206601.pdf

6. ANEXOS

ANEXO I. Router CSG CISCO ASR 1001-HX (Anexo Digital)

ANEXO II. Router ASG CISCO ASR 9001 (Anexo Digital)

ANEXO III. Router RSG CISCO ASR 9006 (Anexo Digital)

ANEXO IV. Direccionamiento de los Enlaces IPRAN

ANEXO V. Configuración de Routers (Anexo Digital)

ANEXO VI. Conectividad en la Interfaz X2 (Anexo Digital)

ANEXO VII. Conectividad en la Interfaz S1 (Anexo Digital)

ANEXO VIII. Conectividad en la Interfaz de Gestión (Anexo Digital)

ANEXO IV

Nodo Origen	Dirección IP	Nodo Destino	Dirección IP	Máscara (/30)
TRÁFICO S1				
RIO_CSG_LEONIDAS	10.1.130.1	RIO_ASG_SUR	10.1.130.2	255.255.255.252
RIO_CSG_UCHIMBORAZO	10.1.130.5	RIO_ASG_SUR	10.1.130.6	255.255.255.252
RIO_CSG_CROACIA	10.1.130.9	RIO_ASG_SUR	10.1.130.10	255.255.255.252
RIO_CSG_CISNEROS	10.1.130.13	RIO_ASG_SUR	10.1.130.14	255.255.255.252
RIO_CSG_UNIDO	10.1.130.17	RIO_ASG_SUR	10.1.130.18	255.255.255.252
RIO_CSG_BONILLA	10.1.130.21	RIO_ASG_OCCIDENTAL	10.1.130.22	255.255.255.252
RIO_CSG_CEMENTERIO	10.1.130.25	RIO_ASG_OCCIDENTAL	10.1.130.26	255.255.255.252
RIO_CSG_SANTAFAZ	10.1.130.29	RIO_ASG_OCCIDENTAL	10.1.130.30	255.255.255.252
RIO_CSG_MALDONADO	10.1.130.33	RIO_ASG_OCCIDENTAL	10.1.130.34	255.255.255.252
RIO_CSG_ESPEJO	10.1.130.37	RIO_ASG_OCCIDENTAL	10.1.130.38	255.255.255.252
RIO_CSG_ESTADIO	10.1.130.41	RIO_ASG_ORIENTAL	10.1.130.42	255.255.255.252
RIO_CSG_PINOS	10.1.130.45	RIO_ASG_ORIENTAL	10.1.130.46	255.255.255.252
RIO_CSG_LOMA	10.1.130.49	RIO_ASG_ORIENTAL	10.1.130.50	255.255.255.252
RIO_CSG_24ABRIL	10.1.130.53	RIO_ASG_ORIENTAL	10.1.130.54	255.255.255.252
RIO_CSG_UNACH	10.1.130.57	RIO_ASG_ORIENTAL	10.1.130.58	255.255.255.252
RIO_CSG_CEMENTO	10.1.130.61	RIO_ASG_NORTE	10.1.130.62	255.255.255.252
RIO_CSG_SANMIGUEL	10.1.130.65	RIO_ASG_NORTE	10.1.130.66	255.255.255.252
RIO_CSG_AMBATO	10.1.130.69	RIO_ASG_NORTE	10.1.130.70	255.255.255.252
RIO_CSG_POLITECNICA	10.1.130.73	RIO_ASG_NORTE	10.1.130.74	255.255.255.252
RIO_CSG_MORGAN	10.1.130.77	RIO_ASG_NORTE	10.1.130.78	255.255.255.252
RIO_CSG_CENTRO	10.1.130.81	RIO_RSG_CENTRO	10.1.130.82	255.255.255.252
TRÁFICO X2				
RIO_CSG_LEONIDAS	10.1.131.1	RIO_ASG_SUR	10.1.131.2	255.255.255.252
RIO_CSG_UCHIMBORAZO	10.1.131.5	RIO_ASG_SUR	10.1.131.6	255.255.255.252

RIO_CSG_CROACIA	10.1.131.9	RIO_ASG_SUR	10.1.131.10	255.255.255.252
RIO_CSG_CISNEROS	10.1.131.13	RIO_ASG_SUR	10.1.131.14	255.255.255.252
RIO_CSG_UNIDO	10.1.131.17	RIO_ASG_SUR	10.1.131.18	255.255.255.252
RIO_CSG_BONILLA	10.1.131.21	RIO_ASG_OCCIDENTAL	10.1.131.22	255.255.255.252
RIO_CSG_CEMENTERIO	10.1.131.25	RIO_ASG_OCCIDENTAL	10.1.131.26	255.255.255.252
RIO_CSG_SANTAFAZ	10.1.131.29	RIO_ASG_OCCIDENTAL	10.1.131.30	255.255.255.252
RIO_CSG_MALDONADO	10.1.131.33	RIO_ASG_OCCIDENTAL	10.1.131.34	255.255.255.252
RIO_CSG_ESPEJO	10.1.131.37	RIO_ASG_OCCIDENTAL	10.1.131.38	255.255.255.252
RIO_CSG_ESTADIO	10.1.131.41	RIO_ASG_ORIENTAL	10.1.131.42	255.255.255.252
RIO_CSG_PINOS	10.1.131.45	RIO_ASG_ORIENTAL	10.1.131.46	255.255.255.252
RIO_CSG_LOMA	10.1.131.49	RIO_ASG_ORIENTAL	10.1.131.50	255.255.255.252
RIO_CSG_24ABRIL	10.1.131.53	RIO_ASG_ORIENTAL	10.1.131.54	255.255.255.252
RIO_CSG_UNACH	10.1.131.57	RIO_ASG_ORIENTAL	10.1.131.58	255.255.255.252
RIO_CSG_CEMENTO	10.1.131.61	RIO_ASG_NORTE	10.1.131.62	255.255.255.252
RIO_CSG_SANMIGUEL	10.1.131.65	RIO_ASG_NORTE	10.1.131.66	255.255.255.252
RIO_CSG_AMBATO	10.1.131.69	RIO_ASG_NORTE	10.1.131.70	255.255.255.252
RIO_CSG_POLITECNICA	10.1.131.73	RIO_ASG_NORTE	10.1.131.74	255.255.255.252
RIO_CSG_MORGAN	10.1.131.77	RIO_ASG_NORTE	10.1.131.78	255.255.255.252
RIO_CSG_CENTRO	10.1.131.81	RIO_RSG_CENTRO	10.1.131.82	255.255.255.252
TRÁFICO DE GESTIÓN				
RIO_CSG_LEONIDAS	10.1.132.1	RIO_ASG_SUR	10.1.132.2	255.255.255.252
RIO_CSG_UCHIMBORAZO	10.1.132.5	RIO_ASG_SUR	10.1.132.6	255.255.255.252
RIO_CSG_CROACIA	10.1.132.9	RIO_ASG_SUR	10.1.132.10	255.255.255.252
RIO_CSG_CISNEROS	10.1.132.13	RIO_ASG_SUR	10.1.132.14	255.255.255.252
RIO_CSG_UNIDO	10.1.132.17	RIO_ASG_SUR	10.1.132.18	255.255.255.252
RIO_CSG_BONILLA	10.1.132.21	RIO_ASG_OCCIDENTAL	10.1.132.22	255.255.255.252
RIO_CSG_CEMENTERIO	10.1.132.25	RIO_ASG_OCCIDENTAL	10.1.132.26	255.255.255.252

RIO_CSG_SANTAFAZ	10.1.132.29	RIO_ASG_OCCIDENTAL	10.1.132.30	255.255.255.252
RIO_CSG_MALDONADO	10.1.132.33	RIO_ASG_OCCIDENTAL	10.1.132.34	255.255.255.252
RIO_CSG_ESPEJO	10.1.132.37	RIO_ASG_OCCIDENTAL	10.1.132.38	255.255.255.252
RIO_CSG_ESTADIO	10.1.132.41	RIO_ASG_ORIENTAL	10.1.132.42	255.255.255.252
RIO_CSG_PINOS	10.1.132.45	RIO_ASG_ORIENTAL	10.1.132.46	255.255.255.252
RIO_CSG_LOMA	10.1.132.49	RIO_ASG_ORIENTAL	10.1.132.50	255.255.255.252
RIO_CSG_24ABRIL	10.1.132.53	RIO_ASG_ORIENTAL	10.1.132.54	255.255.255.252
RIO_CSG_UNACH	10.1.132.57	RIO_ASG_ORIENTAL	10.1.132.58	255.255.255.252
RIO_CSG_CEMENTO	10.1.132.61	RIO_ASG_NORTE	10.1.132.62	255.255.255.252
RIO_CSG_SANMIGUEL	10.1.132.65	RIO_ASG_NORTE	10.1.132.66	255.255.255.252
RIO_CSG_AMBATO	10.1.132.69	RIO_ASG_NORTE	10.1.132.70	255.255.255.252
RIO_CSG_POLITECNICA	10.1.132.73	RIO_ASG_NORTE	10.1.132.74	255.255.255.252
RIO_CSG_MORGAN	10.1.132.77	RIO_ASG_NORTE	10.1.132.78	255.255.255.252
RIO_CSG_CENTRO	10.1.132.81	RIO_RSG_CENTRO	10.1.132.82	255.255.255.252
Anillo de Agregación IP-RAN				
RIO_ASG_OCCIDENTAL	10.1.130.85	RIO_ASG_NORTE	10.1.130.86	255.255.255.252
RIO_ASG_OCCIDENTAL	10.1.130.89	RIO_RSG_SUR	10.1.130.90	255.255.255.252
RIO_ASG_NORTE	10.1.130.93	RIO_ASG_ORIENTAL	10.1.130.94	255.255.255.252
RIO_ASG_ORIENTAL	10.1.130.97	RIO_RSG_CENTRO	10.1.130.98	255.255.255.252
RIO_RSG_SUR	10.1.130.101	RIO_RSG_CENTRO	10.1.130.102	255.255.255.252
Enlace con nube MPLS				
RIO_RSG_CENTRO	10.10.10.1	ROUTER_PE1_MPLS	10.10.10.2	255.255.255.252
RIO_RSG_CENTRO	10.10.10.5	ROUTER_PE2_MPLS	10.10.10.6	255.255.255.252
Enlace para Mantenimiento IP-RAN				
ROUTER_PE1_MPLS	10.10.20.1	GESTOR_IPRAN	10.1.20.2	255.255.255.252

ORDEN DE EMPASTADO