UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA DE GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“DISEÑO DE UNA RED 4G-LTE PARA SERVICIOS MOVILES DE LA POLICIA NACIONAL DEL PERU (PNP), CON SEDE EN SAN ISIDRO, LIMA”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

VILLASANTE ANTÓN, VÍCTOR JOEL

Villa El Salvador

2016

DEDICATORIA

A mis padres Víctor y María, por ser siempre el ejemplo de vida y por demostrarme siempre su cariño y apoyo incondicional.

A mis hermanas, primos y tía Violeta por los grandes momentos en mi vida, los cuales me sirvieron de inspiración.

AGRADECIMIENTO

Gracias a Dios, a mis padres que fueron los grandes pilares en mi vida, tanto en mi carrera como a lo largo de mi vida, por su sacrificio y apoyo constante. A mis profesores, que me apoyaron en el transcurso de mi carrera profesional. A mis compañeros, por el apoyo, respeto y amistad.

Índice

CAPÍTULO III: DISEÑO/ DESCRIPCIÓN DE LA HERRAMIENTA/ MODELO/SISTEMA

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCION

El presente trabajo de investigación lleva por título “Diseño de una Red 4G-LTE para servicios móviles de la Policía Nacional del Perú”, para optar el título de “Ingeniero Electrónico y de Telecomunicaciones”, presentado por el alumno Villasante Antón, Víctor Joel.

En estos últimos años se ha presentado una cantidad considerable de evolución en el estudio y aplicación de técnicas que diseñan sistemas las cuales permitan la comunicación a larga distancia a través de la transmisión y recepción de señales.

Actualmente se cuenta con diversos sistemas de transmisión y recepción de la comunicación a distancia, el presente trabajo define el sistema en tecnología móvil de última generación alcanzado en nuestro país para lo que es el servicio de comunicación.

La estructura que se ha seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al diseño del proyecto.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCION DE LA REALIDAD PROBLEMÁTICA

En el país se tiene un avance hacia servicios informáticos los cuales nos ayuda en cualquier ámbito de nuestra vida. Si una persona desea tener acceso hacia una Red Publica esto sería fácil de realizar mediante diferentes equipos de Transmisión (Computadora de mesa, Laptop, Smartphone, etc.).

Desafortunadamente no hay un control en la Red el cual limite al usuario a ingresar en diferentes páginas web u otros accesos que se puedan realizar con una Red el cual permita realizar todas las funciones en la Web, en la actualidad no se plantean proyectos o trabajos de los cuales se pueda apoyar y/o incentivar un mejor manejo de control hacia diferentes salidas que se tiene en la Web, si ello se realizara esto conllevaría a una mejora ascendente acerca de las políticas de privacidad que se tiene.

En la actualidad los patrulleros de la Policía Nacional Del Perú cuentan con un sistema en el cual se pueden comunicar con una central y también les permite tener comunicación entre ellos mediante políticas de Red específicas. Han venido utilizando el sistema de Red Móvil que cuenta con tecnología 3G, debido a la constante evolución que se tiene en base a la tecnología de comunicación se está realizando las gestiones para que este sistema cambie a uno de mayor evolución.

La implementación de una Red Banda Ancha en Tecnología Red Móvil 4G (LTE) que tenga control de accesos hacia un grupo reducido de IPs Publicas se viene a dar a consecuencia de tener internet de alta velocidad y un control por parte de los responsables del servicio de la Policía Nacional del Perú, esto se da debido a consecuencia de un acuerdo entre la empresa y el mayor proveedor de servicios móviles que se tiene en el país. En el departamento de Lima, la implementación de estos sistemas se viene dando actualmente pero con tecnología de Red en 3G, en estos últimos meses se está dando a empresas un control de sus accesos ya implementando Tecnología de alta velocidad LTE, los cuales van a ser de gran utilidad para los responsables de acceso de las empresas ya que va a haber un mayor control hacia la Red. Este proyecto tiene la finalidad de desplegar una red de Transporte hacia los usuarios finales para que tengan acceso hacia los servicios de Red propios de la empresa.

Actualmente el diseño y la implementación de una Red Banda Ancha en Tecnología Red Móvil 4G (LTE) es realizado mediante una conexión de Red Móvil y una Red MPLS, esto es lo que permite realizar la comunicación de los dispositivos finales con la Red de control de la empresa, de este modo se tendrá un mejor control del servicio el cual va a facilitar los accesos que se tengan en el punto ya sea un Smartphone, Tablet, Laptop, etc.

Una problemática que se tendría en este punto seria tener un control en las diferentes área de Red por la cual se va a transportar la información de la señal hacia los usuarios finales, ya que conlleva a una cantidad de áreas involucradas todas ellas deben tener el alcance de las configuraciones o cambios que se van a realizar en la Red, si esto se da de la manera correcta se garantizara un correcto funcionamiento del servicio.

1.2 JUSTIFICACION DEL PROYECTO

El presente proyecto en referencia hacia los servicios móviles que van a tener los patrulleros de la Policía Nacional del Perú se está realizando con el

fin de tener una comunicación entre los diferentes usuarios así como la central que se tendrá para el control del servicio.

Este tipo de servicio de una red usando tecnología 4G en comparación con el que se tiene actualmente 3G va a tener las siguientes diferencias en cuanto a mejora del servicio:

- Velocidad de subida/Velocidad de bajada a una alta tasa de transmisión.
- Usuarios solo tengan acceso a ciertas IPs Publicas Especificas.
- Se tendrá acceso en el departamento de Lima (Donde se tenga alcance de cobertura del operador móvil).

Actualmente los sistemas de Banda Ancha en Tecnología Red Móvil 4G son basados en equipos que trabajan en formato digital, los cuales ejercen de una manera completa un área determinada para el acceso a los usuarios finales, se tratan de sistemas que han alcanzado una mejor transmisión del servicio a largas distancias(Mayor velocidad en la transmisión).

1.3 DELIMITACION DEL PROYECTO

1.3.1 TEORICA

Este trabajo se basa en las teorías de las tecnologías de Red 3G, 4G y MPLS.

1.3.2 ESPACIAL

El trabajo se realizara en el Departamento de Lima teniendo la Sede Principal en San Isidro

1.3.3 TEMPORAL

El periodo de tiempo está comprendido entre las fechas 01/07/2016 hasta 08/08/2016.

1.4 FORMULACION DEL PROBLEMA

¿Cómo diseñar una Red 4G-LTE para los servicios móviles de la Policita Nacional del Perú?

1.5 OBJETIVO GENERAL

Diseñar un sistema mediante tecnología 4G (LTE) el cual permita la comunicación de los dispositivos finales hacia la salida de accesos públicos controlados sin necesidad de utilizar medios de transmisión alámbricos para dicha conexión.

1.5.1 OBJETIVOS ESPECIFICOS

- Buscar una forma de comunicación la cual sea de fácil acceso para los dispositivos móviles.
- Tener un mayor control en la comunicación que se va a tener para un mejor aprovechamiento de los recursos.
- Generar una nueva forma de comunicación para los dispositivos móviles.

CAPITULO II
MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACION

Existen trabajos similares al mío del cual puedo mencionar los siguientes:

DISEÑO DE UNA RED 4G-LTE INDOOR PARA EL CENTRO COMERCIAL REAL PLAZA SANTA CLARA, elaborado por Michael Eduardo Chancasana Cueto quien concluyo lo siguiente “Las redes indoor mejoran la cobertura dentro de edificaciones, además, descongestionan las redes outdoor. Un correcto despliegue de redes indoor en lugares con gran afluencia de usuarios hace que las redes outdoor se liberen y reduzcan su radio de cobertura emitiendo menores niveles de potencia. Los usuarios deben entender que el aumento de estaciones base y redes indoor en vez de generar mayor radiación y niveles de potencia las disminuye”.

DISEÑO DE UNA RED LTE PARA EL DISTRITO DEL CALLAO, elaborado por José Alejandro Milla Cazana quien concluyo lo siguiente “El despliegue de una red LTE en el distrito del Callao no presenta mayores problemas en lo que respecta a la red de transporte, ya que al tratarse de un distrito costeño, se cuenta con una demografía ideal para el despliegue de redes móviles, tal como se muestra en la FIGURA 4-5 y en el ANEXO 1. Es por ello que es importante indicar que este modelo aplica generalmente para zonas costeñas con bajo relieve demográfico. Para localidades de la sierra o selva sería distinto ya que es muy probable que se necesite emplear repetidores, mayor cantidad de amplificadores, femtoceldas o picoceldas.”

ANÁLISIS Y DISEÑO DE UNA RED 3GPP LTE EN EL DEPARTAMENTO DE CUSCO, elaborado por Christopher Wong Matos quien concluyo lo siguiente “El despliegue de una red LTE en la ciudad del Cusco presenta una serie de dificultades en cuanto a la ubicación de las estaciones base, sobre todo en los lugares turísticos como Machupicchu, pero ese problema también se presenta en las redes actuales. El gran desafío está en la red de transporte ya que el uso de microondas a mediano plazo será ineficiente y la fibra óptica se hace imprescindible para poder soportar las grandes capacidades de transmisión.”

2.2 BASES TEORICAS

2.2.1 LTE (Long Term Evolution)

En la actualidad cuando se lee todo tipo de artículos relacionados con redes celulares, es imposible no toparse con las siglas LTE. Long Term Evolution es el nombre detrás de estas siglas y se trata de lo último en lo que respecta a tecnologías móviles. Junto con WIMAX son las que están llamadas a revolucionar el mundo de las telecomunicaciones. Esto por una sencilla razón, LTE permitirá tener velocidades de transmisión de datos muy altas con una latencia de paquetes mucho menor que las otras tecnologías, lo cual es un creciente requerimiento en los servicios hoy en día.

Esto se logra gracias a que LTE emplea una técnica de acceso múltiple en la capa física, llamada OFDMA (del inglés Orthogonal Frequency Division Multiplexing Access) en el Dowlink (descarga de datos), en la que divide el canal en un conjunto de subportadoras que se reparten en grupos en función de la necesidad de cada uno de los usuarios. Mientras que para el Uplink (carga de datos) utiliza la técnica SC-FDMA (del inglés Single Carrier Frequency Division Multiplexing Access) que es una variante de OFDMA con la diferencia de que esta presenta un PARP (del inglés Peak to Average Power Ratio) reducido, lo cual evitará que tengamos picos muy grandes en la señal.

Además lo que repotencia el esquema de LTE es el uso de antenas MIMO (del inglés Multiple-Input and Multiple-Output). MIMO hace posible el contar con múltiples antenas tanto en el transmisor como en el receptor, para de esta forma mejorar la calidad de la comunicación.

2.2.2 Breve Historia de LTE

LTE significa hasta el día de hoy el pico de la evolución para 3GPP (del inglés 3G Partnership Project). Sin embargo, es importante recordar el proceso de evolución por las que pasaron las tecnologías de 3GPP para llegar a LTE.

El Release 99 fue publicado en diciembre de 1999 y contenía los aspectos básicos de WCDMA (del inglés Wideband Code Division Multiple Access). A partir del año 2001 el 3GPP dejó de nombrar los Releases por el año de publicación e inició una nueva nomenclatura a partir del Release 4 el cual fue terminado en marzo 2001 y contenía la versión TDD (del inglés Time Division Multiplexing), TD-SCDMA (del inglés Time Division Synchronous Code Division Multiple Access) para baja capacidad. El Release 5 se concluyó en marzo de 2002 y estaba dedicado a HSDPA (del inglés High Speed Downlink Packet Access), mientras que el Release 6 se publicó en diciembre de 2004 y se refería a HSUPA (del inglés High Speed Uplink Packet Access) para WCDMA. El Release 7 se terminó en junio de 2007 y presentaba ciertas mejoras tanto en HSDPA como en HSUPA.

Actualmente se ha terminado el Release 8 con mejoras en HSDPA/HSUPA, denominado HSPA (del inglés High Speed Packet Access) y también contiene las primeras especificaciones de LTE, el Release 8 fue terminado en diciembre de 2008.

Por su parte el Release 9 se refiere a LTE y se desarrolló en paralelo con el Release 10 que define la tecnología 4G que cumplía con las especificaciones de IMT –Advanced (del inglés International Mobile Telecommunication Advanced) de la ITU (International Telecommunication Unit). Precisamente en el año 2010 esta organización la aprobó junto a WiMAX como las elegidas para llevar el rótulo de tecnología 4G. En la FIGURA 2 se muestra esta evolución a través del tiempo.

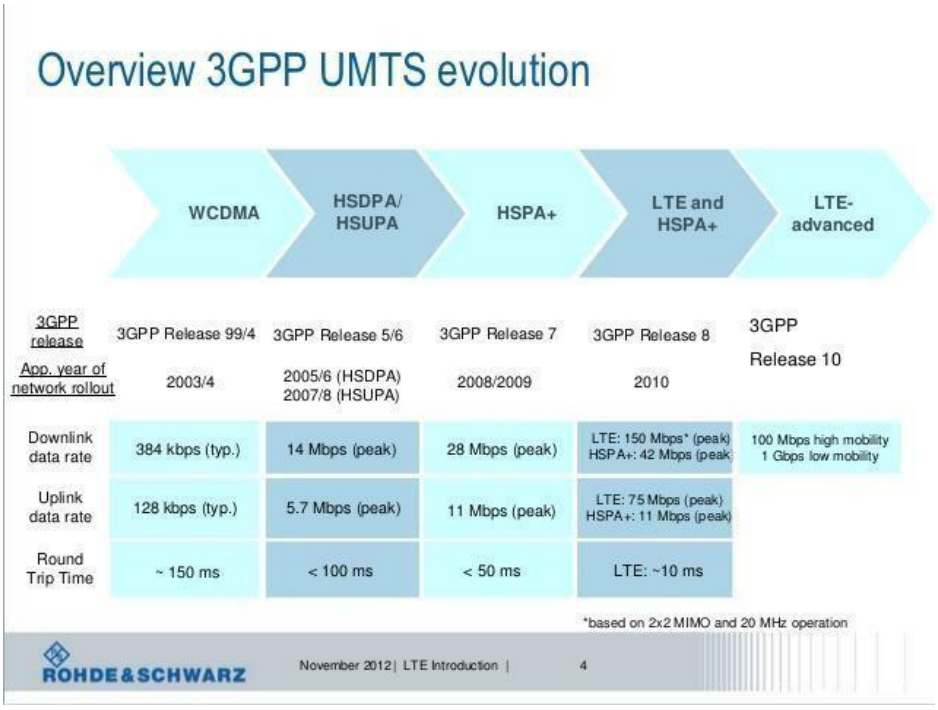


Figura 1: *Evolución a Travez del tiempo de la tecnología móvil*
Fuente: *http://www.slideshare.net/RohdeSchwarzNA/lte-eutran-rsanov2012day1*

2.2.3 Arquitectura de red LTE

La arquitectura LTE abarca un equipo de usuario (User Equipment (UE)) y de una infraestructura de red que se divide de forma lógica en una infraestructura de red troncal (Core Network (CN)) y una de red de acceso (Access Network (AN)).

- Equipo de Usuario (UE): es el equipo que permite al usuario conectar a la red LTE. El equipo de usuario contiene dos elementos básicos: un módulo de suscripción de usuario (SIN/USIM) y el terminal móvil (celular, Tablet, etc.).

- Red de Acceso (AN): E-UTRAN es la interfaz aérea de ruta de actualización de 3GPP-LTE para redes móviles. Esta es la interfaz que comunica los equipos de usuario y la red troncal EPC. Todas las funciones y protocolos que se necesitan para realizar él envió de datos y controlar la interfaz se implementan en la entidad de Red eNB (Nodo B Evolucionado). Un eNB se comunica con el resto de elementos del sistema mediante tres interfaces: E-UTRAN Uu, S1 y X2.

- Red Troncal (CN): En la interfaz EPC o Red Troncal de Paquetes Evolucionada se encuentra:

- MME (Mobility Mnagenment Entity): Contiene datos del suscriptor a través de la información almacenada en el HSS (Home Subscriber Server). El MME autentifica, autoriza y selecciona el PDN (Packet Data Networks) apropiado para establecer el enlace entre E-UTRAN a las redes o ejercicios externos.

- SGW (Serving Gateway): Puente del plano del usuario entre E-UTRAN y la troncal EPC. El S-GW también es un punto de monitoreo de las políticas de conexión y servicio en el PCRF (Policy and Charging Rules Funtion)

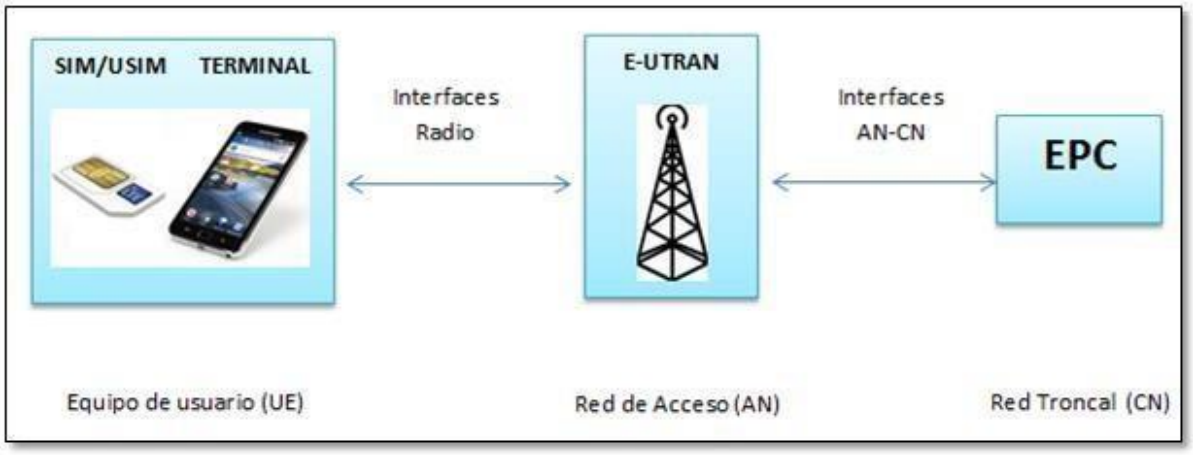


Figura 2: *Arquitectura de Red LTE*
Fuente: *http://inalambricas-lte4g.blogspot.pe/2014/08/arquitectura-lte-la-arquitectura-lte.html*

2.2.4 Componentes e Interfaces en EPC

- MME (Mobility Management Entity): El MME obtiene datos del subscriptor a través de la información almacenada en el HSS. El MME autentica, autoriza y selecciona el PDN (Packet Data Network) apropiado para establecer el enlace entre el E-UTRAN a las redes o servicios externos. MME también realiza funciones de administración de movilidad y recolecta información de cobro. El MME proporciona conectividad entre el eNodoB y la red LTE existente a través del S-GW (Serving Gateway).

  MME trabaja con las siguientes interfaces:

S1-MME: Es el punto de referencia para el plano de control entre el EUTRAN y el MME.

S11: Punto de referencia para la conexión entre MME y SGW.

S6a: Permite la transferencia de información de los suscriptores y su autenticación/autorización al EPS (Evolved Packet System).

SGs: se utiliza para la gestión de la movilidad y de los procedimientos de localización entre EPS y dominio CS (Circuit Switched).

- S-GW (Serving Gateway): El S-GW es un equipo de plano de usuario que es controlado por el MME. El S-GW también es un punto de monitoreo de las políticas de conexión y servicio establecidas en el PCRF (Policy and Charging Rules Function).

  S-GW trabaja con las siguientes interfaces:

S1-U: Punto de referencia entre EUTRAN y el SGW.

S11: Punto de referencia para la conexión entre MME y SGW.

S5: Interconecta el S-GW con el P-GW y además hace tunelizacion de los datos del plano de usuario entre estas dos interfaces. También es usada en la relocalización de S-GWs dada la movilidad del UE.

- P-GW (PDN Gateway): El P-GW puede ser comparado con las funciones realizadas por el GGSN pero además tiene un importante rol en el control de la movilidad. El P-GW asigna la dirección IP al UE.

  P-GW trabaja con las siguientes interfaces:

S5: Interconecta el S-GW con el P-GW.

SGi: Es el punto de referencia entre el PGW y la PDN.

- HSS (Home Subscriber Server): El HSS almacena y administra todo lo relativo a los datos de suscripción de los usuarios.

HSS trabaja con la siguiente interfaz:

S6a: Permite la transferencia de información de los suscriptores y su autenticación/autorización al EPS.

- MSC (Mobile Switching Centre, o Centro de Conmutación de Servicios Móviles): es un elemento que tiene como función interconectar usuarios de la red fija con la red móvil, o usuarios de la red móvil entre sí. Al mismo

tiempo mantiene las bases de datos para tratar las peticiones de llamada de los clientes.

MSC trabaja con la siguiente interfaz:

SGs: se utiliza para la gestión de la movilidad y de los procedimientos de localización entre EPS y dominio CS (Circuit Switched).

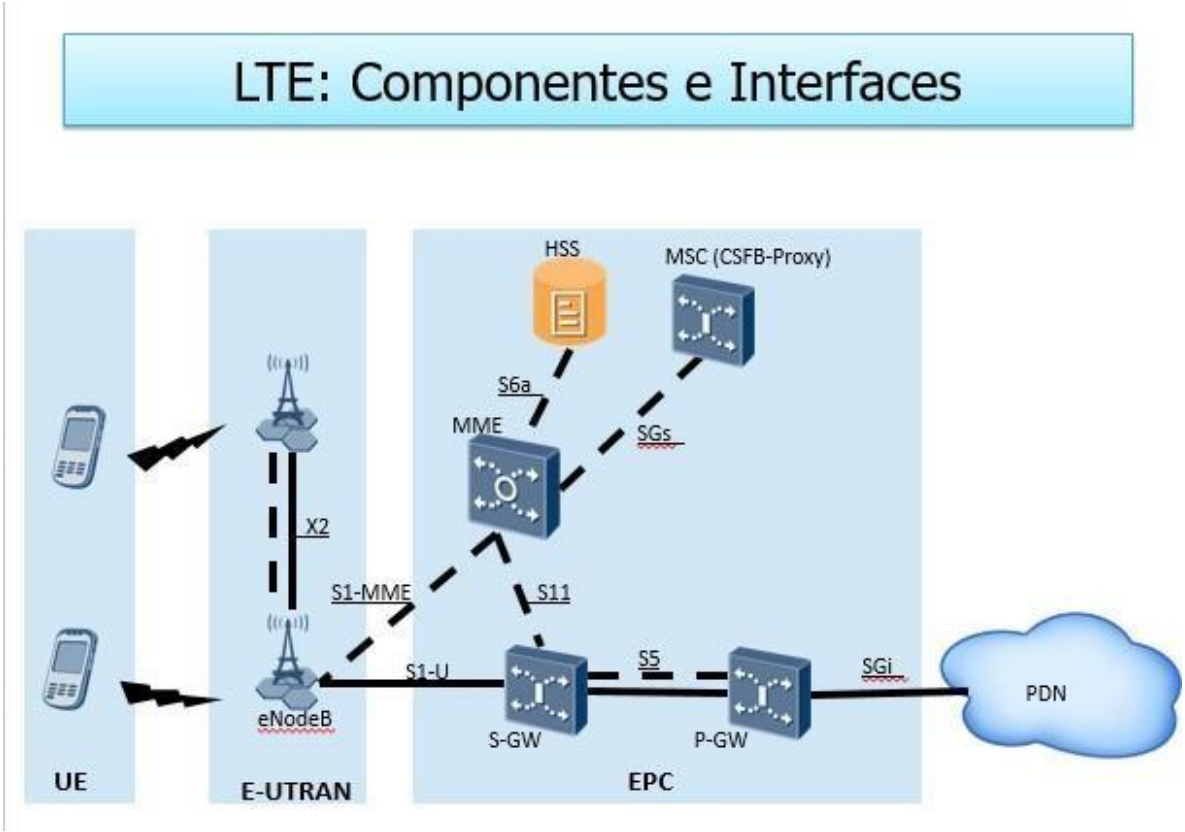


Figura 3: *Red LTE – Componentes e Interfaces del EPC*
Fuente: *Realización Propia*

2.2.5 Orthogonal Frequency Division Multiple Access (OFDMA)

OFDM es una técnica de multicanalización basada en el uso de varias subportadoras.

Estas subportadoras son elegidas de tal manera que ninguno de sus espectros interfiera con la frecuencia central de las otras subportadoras. El estándar IEE 802.16e tiene dos capas físicas basadas en OFDM: una que usa OFDM como tal, y otra que usa una variante de esta OFDMA, donde varios usuarios comparten un símbolo ODFM.

La técnica OFDM es similar a FDM. La diferencia se basa en que mientras FDM debe dejar una banda de guarda entre canales, OFDM por su parte trata de acercar los canales lo más posible hasta superponerlos.

Esto se logra escogiendo frecuencias que sean ortogonales, lo cual significa que estas son perpendiculares en el sentido matemático; permitiendo así que sus espectros se superpongan sin interferir.

Esto significará un ahorro de ancho de banda, a continuación se muestra la Figura 4 para las ilustraciones del caso:

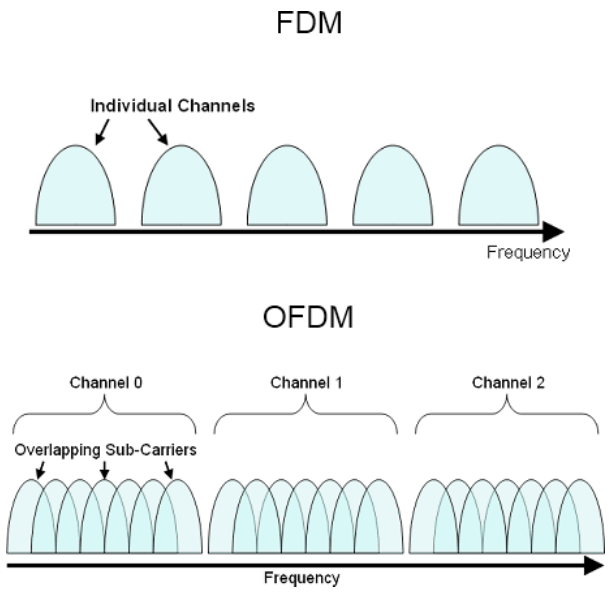


Figura 4: *Comparación entre FDM y OFDM*
Fuente: *https://www.eeweb.com/electronics-forum/ofdm*

Como se aprecia en la Figura 4, OFDM puede ser considerada como una técnica de modulación y también una técnica de acceso múltiple. Si se da el caso en que las subportadoras se comparten entre varios usuarios finales, entonces se hablará de una técnica de acceso múltiple, es decir OFDMA.

ODFM ha sido principalmente empleada en 3G, ahora con 4G OFDMA ha sido la técnica más empleada, ambas para el Downlink.

OFDM presenta dos desventajas claras. En primer lugar, el hecho de tener un PAPR elevado, lo cual genera limitaciones para los dispositivos electrónicos de los sistemas, en particular a los amplificadores. Y en segundo lugar, el hecho de ser muy sensible a cambios en la frecuencia de las subportadoras. Sin embargo, presenta grandes ventajas como el reducir la

Interferencia Intersimbólica, el presentar Robustez ante los multitrayectos, contar con una alta eficiencia espectral y el hecho de que su implementación sea sencilla.

2.2.5.1 Simple Carrier Frequency Division Multiple Access (SC-FDMA)

Como se mencionó en líneas anteriores, SC-FDMA es una variante de OFDMA. Es por ello que tiene las mismas características de esta como el hecho de presentar robustez ante los multitrayectos, el tener una alta eficiencia espectral, reducir la Interferencia Intersimbólica y el hecho de que su implementación sea sencilla. Además, muestra otras ventajas que OFDMA no nos daba, como el caso del PAPR, con SC-FDMA el PAPR será reducido al igual que el consumo de potencia. Sin embargo, en SC-FDMA tendremos un receptor muy complejo, pero esto se soluciona utilizando SC-FDMA para el Uplink, con lo cual tendremos que el receptor en la unidad móvil debe ser sencilla y económica mientras que la complejidad del receptor y los altos costos que se pudiesen generar se dejan a la Estación Base, la cual tiene más recursos.

En resumen, en OFDMA se comparte el ancho de banda, cada símbolo de datos (dependiendo de la modulación) se usa para modular una subportadora, las cuales son ortogonales entre sí, de aquí es de donde nace la característica multiportadora de OFDMA. Además los “M” símbolos que se transmiten lo harán en paralelo y repartiéndose en todo el ancho de banda disponible. Esto implicará que se superpongan varios símbolos de datos en

forma simultánea, es decir varias sinusoides con amplitudes y fases distintas, las cuales en determinado instante pueden estar algunas de ellas en fase y producir un PAPR elevado.

Por el contrario, en SC-FDMA se emplea una combinación lineal, donde varios símbolos de datos se usan para modular varias subportadoras ortogonales; es decir que cada símbolo de los “M” que se transmitan lo harán ocupando todo el ancho de banda disponible y con una duración igual a una parte del tiempo del símbolo SCFDMA. Esto quiere decir, que en el ancho de banda que se dispone, solo se envía información de varios símbolos de datos dependiendo de la modulación que se elija.

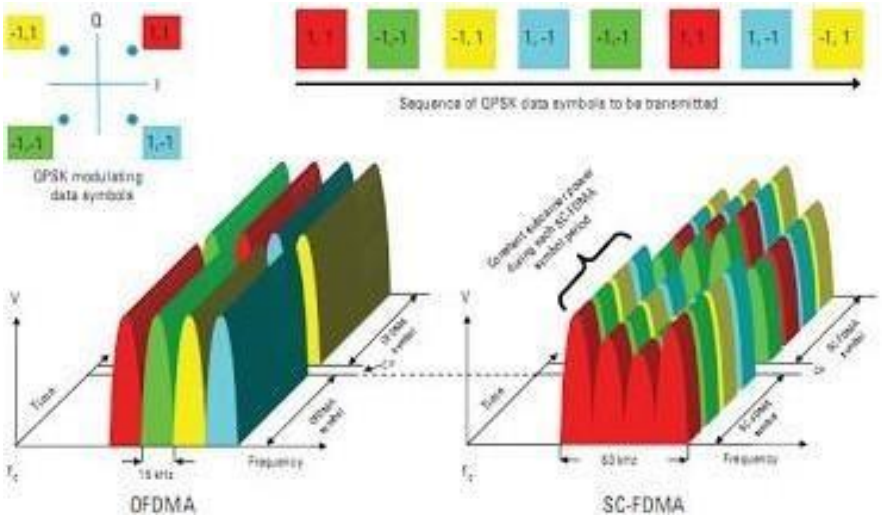


Figura 5: *OFDMA vs SC-FDMA*

Fuente: *http://gsmcommunications.blogspot.pe/2011/01/using-sc-fdma-in-lte.html*

2.2.6 Ventajas de LTE

Todo lo anteriormente explicado, coopera para que se pueda especificar las ventajas que significaría el hecho de emplear LTE.

- Con LTE será posible llegar a velocidades de hasta 200 Mbps.

- La latencia, es decir el retardo en la respuesta desde la red, será menor en comparación con otras tecnologías.

- Se contará con una arquitectura de red basada únicamente en el protocolo IP que permitirá a los operadores reducir el costo de los servicios que ofrecen, y a su vez permitirá a los usuarios contar con nuevas posibilidades de servicios multimedia interactivos. Con ello, tendremos que el costo de esta tecnología se reducirá notablemente.

Se generará una alta eficiencia en lo que respecta a los costos de operación de las redes, lo cual permitirá reducir el impacto ambiental en la zona donde esta se implemente.

2.2.7 Servicios en LTE

LTE podría ofrecer servicios tales como:

- Push to talk Over Cellular (PoC): se trata básicamente de los servicios de comunicación punto-punto o punto-multipunto que se ofrecen en las redes móviles.

- Presence: servicio que hace posible que los usuarios compartan información de sus actividades, ubicación actual, zona horaria donde se encuentran, etc.
- Multimedia Broadcast y Multicast Service (MBMS): son aquellos servicios como:
  - ✓ Transmisión de audio y/o video: publicidad, suscripción ciertos servicios o Descarga de audio y/o video
  - ✓ Descarga de archivos: actualización de aplicaciones
- Telefonía Multimedia :
  - ✓ VoIP: servicio de transmisión y recepción de voz a través de IP.
  - ✓ Video Telefonía: servicio de telefonía con la particularidad de un video multimedia de la persona en tiempo real durante la llamada.

2.2.8 MPLS

Conmutación Multi Protocol Label (MPLS) es una tecnología de conmutación que regula el tráfico de datos y el reenvío de paquetes en una red compleja. Una metodología orientada a la conexión que atraviesa los paquetes desde el origen al nodo de destino a través de redes es lo que hace para la transmisión rápida de paquetes. Tiene la característica de que abarca los paquetes en los diferentes protocolos de red.

En el enrutamiento IP tradicional, los paquetes se someten a análisis en cada salto, seguido de reenvío de decisión de acuerdo con el análisis de

cabecera de red y luego las operaciones de búsqueda en la tabla de enrutamiento. En una red MPLS, los paquetes que transportan datos se asignan con etiquetas en cada nodo y la decisión de envío está totalmente basada en estos encabezados de la etiqueta. Esto es diferente del mecanismo de enrutamiento convencional. La cabecera del paquete se analiza solamente una vez, mientras que entran en la nube MPLS a partir de entonces la decisión de envío es ' label-based (basado en etiqueta)' que asegura la transmisión rápida de paquetes entre nodos locales-locales y locales a distancia.

Esto asegura circuitos de extremo a extremo a través de cualquier tipo de medio de transporte utilizando cualquier protocolo de capa de red. En vista del hecho de que MPLS soporta Protocolo Internet(IPv4 e IPv6), IPX, AppleTalk en Capa 3; Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), Frame Relay y PPP (protocolo punto a punto) en la capa 2, que se conoce como "Capa de protocolo 2.5".

Con esta tecnología se intenta eliminar los protocolos que dependen de las tecnologías específicas de capa de enlace de datos, tales como ATM, Frame Relay, Ethernet y de red óptica síncrona (SONET). Ya que esto evita la necesidad de capas múltiples 2 para diferentes tipos de tráfico. Con esto se proporciona un servicio de portadora de datos unificada para los clientes, esto basado en sistemas de conmutación en circuitos para transmisión de paquetes.

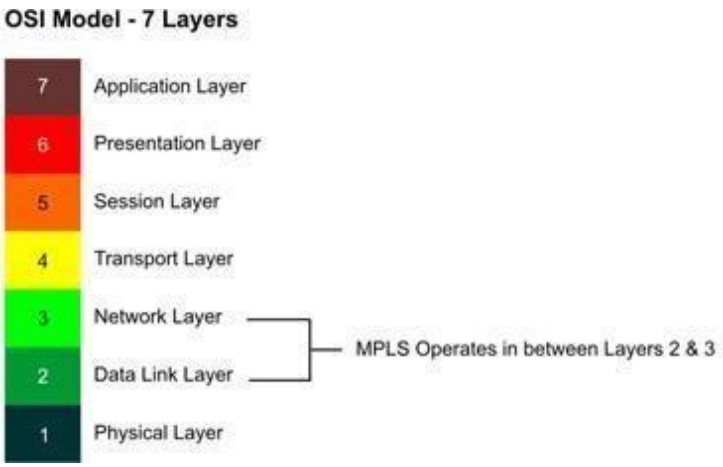


Figura 6: *MPLS – Capas del Modelo OSI*
Fuente: *http://mplsinfo.org/*

El estándar MPLS viene por la necesidad de dotar las redes IP de nuevas capacidades, permitiendo mejoras y nuevas funcionalidades, destacando:

- Ingeniería de tráfico.
- Mecanismos de protección y recuperación frente a fallos.
- Redes privadas virtuales.
- Soporte de QoS y CoS para servicios que requieren flujos de datos de tiempo real.
- Integración de las redes IP con distintas tecnologías de nivel 2.

Además tiene una serie de características fundamentales:

- Multiprotocolo: Es aplicable a cualquier protocolo de capa de red, e independiente de la capa de enlace utilizada.

- Conmutación por etiquetas. El reenvío (fordwarding) de los paquetes se realiza basándose en etiquetas con las que estos son marcados. Las etiquetas contienen información de encaminamiento y atributos de servicio.

- Se desacopla la función de reenvío con la de encaminamiento (routing).

- Tiene dos niveles funcionales en la red: frontera (edge) y núcleo (core).

2.2.8.1 Historia de MPLS

El Grupo de Trabajo de Ingeniería de Internet (IETF) se formó en 1997 y el primer MPLS RFC tuvo su lanzamiento en 2001. RFC 3031 especifica la arquitectura MPLS y RFC 3032 especifica su codificación de sistema basado en etiquetas. La conmutación de etiquetas permite a un dispositivo realizar las mismas operaciones del router con el rendimiento del conmutador ATM. Con ello las búsquedas de las etiquetas sea un sistema más rápido que un enrutamiento IP convencional. Con el avance de la conmutación de paquetes, MPLS supera los contratiempos ATM con los servicios, también genera

menos gastos generales, esto debido a la conexión de tramas con longitud variable. Esto también proporciona la ventaja de mantener la ingeniería de tráfico y de control fuera de banda. De este modo Frame Relay y ATM son menos necesitados para la instalación de redes a gran escala, el rendimiento de MPLS es muy superior a los anteriores.

En medio de estas ventajas, hay algunas desventajas para esta conmutación de etiqueta de la tecnología. En primer lugar, la gestión de MPLS es complicado, ya que depende de los protocolos de enrutamiento para la transferencia de datos. En este instante, cualquier desperfecto en la red puede perturbar todo el transporte y la reorientación de los paquetes de datos. Inicialmente, la estructura de la etiqueta permite que los routers puedan decidir el encaminamiento de paquetes IP. Esto se basa en el contenido de la etiqueta en lugar de un mecanismo de búsqueda de rutas difíciles según la dirección IP. Con el progreso técnico, conmutadores de nivel 3 (routers basados en ASIC) llevan a cabo consultas de rutas a una velocidad suficiente para soportar tipos de interfaz.

2.2.8.2 Arquitectura de red MPLS

Una red MPLS consta fundamentalmente de los siguientes elementos:

- LSR (Label Switching Router): encargado de conmutar las etiquetas de los paquetes e intercambiar información con otros LSR de la red para establecer las asociaciones entre flujos y etiquetas.
- LER (Label Edge Router): Constituye el elemento de entrada y salida de la red MPLS, y se encuentra en la frontera de la misma. Se suele distinguir entre el equipo de entrada (ingress) y el de salida (egress).

A la entrada de la red se realiza la función de procesar los paquetes, seleccionarlos y aplicar la etiqueta que les corresponda.

En la salida de la red se encarga de suprimir las etiquetas y reenviar los paquetes hacia el destino utilizando el reenvío de la capa 3.

- FEC (Forwarding Equivalent Class). Conjunto de paquetes que son tratados de la misma forma en el proceso de reenvío, siguiendo la misma ruta con independencia de los destinos finales.
- LSP (Label Switched Path). Camino que se establece dentro de la red MPLS para todo tráfico de una misma FEC. Todos los paquetes identificados por esa FEC tendrán el mismo encaminamiento a través de la red. El LSP define un camino unidireccional, por lo que para el envío de tráfico bidireccional será necesario establecer dos LSP, uno para cada sentido de la comunicación. Esta ruta está definida antes de que comience la transmisión de datos.

- LIB. Forma parte del Plano de control cuya base de datos es usada por el LDP para distribución de etiquetas. Cuando esto ocurre los prefijos IP son asociados con sus entradas de etiquetas locales y el próximo salto con la información aprendida anteriormente.

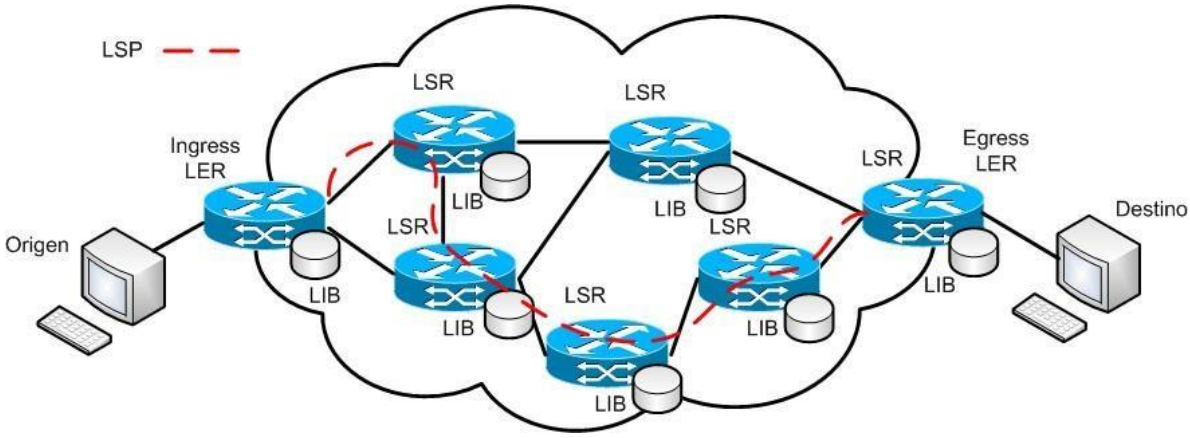


Figura 7: *Arquitectura MPLS*
Fuente: *http://mplsinfo.org/*

Como en toda nueva tecnología, los elementos que definen la arquitectura de la misma deben ser estudiados intensamente ya que cumplen ciertas funciones y roles dentro de un dominio nuevo como es el caso de MPLS.

Elementos como LSRs y LERs son los principales dispositivos que ocupan una parte muy importante al momento de definir la arquitectura MPLS. Estos dispositivos cumplen con la función de intercambiar etiquetas dentro de una red MPLS. Los LSRs y LER en su estructura interna constan de dos componentes que requieren de profundo entendimiento como lo son: El Plano de Control y el Plano de Datos o de Envío.

Plano de Control de conmutación de etiquetas

En el Plano de Control en un LSR y un LER se encuentran los protocolos de encaminamiento y las tablas de encaminamiento.

El protocolo de encaminamiento se encarga de mantener la información de las actualizaciones de rutas entre los LSRs que se encuentra dentro de la red MPLS. Los protocolos de encaminamiento crean la tabla de enrutamiento IP que es usada para construir la base de información de envío (LIB). Esta tabla de enrutamiento IP en el plano de control es empleada para determinar el intercambio de etiquetas, donde los nodos adyacentes las intercambian para todas las subredes que están contenidas dentro de su tabla. Este intercambio realizado por el protocolo de distribución de etiquetas (LDP) crea la base de información de etiquetas (LIB).

Plano de Datos o Plano de Envío de Etiquetas

A diferencia del Plano de Control, el Plano de Envío en los LSRs y LERs difiere un poco ya que en el LER se extienden las funcionalidades debido a que no solo cuenta con la tabla de envío de etiquetas sino que también trabaja con una tabla de envío IP.

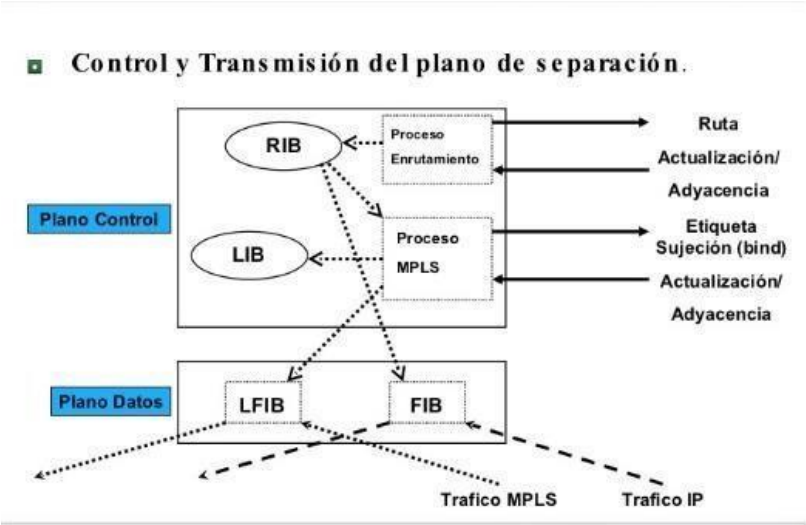


Figura 8: *Plano de Control y Datos en MPLS*
Fuente: http://mplsinfo.org/

Por esta diferencia se describe separadamente las funcionalidades del Plano de Envío para el LSR y el LER.

LSR: En el proceso de enrutamiento IP-MPLS se utilizan las etiquetas que se intercambian entre LSRs adyacentes que ayudan a la creación de la tabla de envío de etiquetas en el Plano de Datos para enviar los paquetes etiquetados a través de una red MPLS.

LER: La tabla de envío IP estándar es construida en base a tabla de enrutamiento IP y es extendida con información de etiquetas. Esta extensión de componentes en el Plano de Datos se debe a que los paquetes IP entrantes a un LER pueden ser enviados como paquetes IP natos a un nodo no MPLS o pueden ser etiquetados y enviados a otros nodos MPLS. Además si los

paquetes entrantes vienen etiquetados pueden ser enviados a otros nodos MPLS, o si su destino es un dominio no MPLS, su etiqueta puede ser removida y el chequeo de capa de red es realizado (envío IP) para encontrar el destino no MPLS.

En general, y para ambos casos, al crearse la tabla de envío de etiquetas cada entrada de la tabla contendrá una etiqueta de entrada y una etiqueta de salida, que corresponden a cada interfaz de entrada a un nodo MPLS. En la Figura 9 se ilustra el funcionamiento de un LSR del núcleo MPLS. En este caso un paquete que llega a un LSR por la interfaz 3 y con etiqueta 45, se le remueve esa etiqueta y se le asigna la etiqueta 22 que le indica que el paquete debe salir por la interfaz 4 hacia el siguiente LSR, de acuerdo con la información de la tabla.

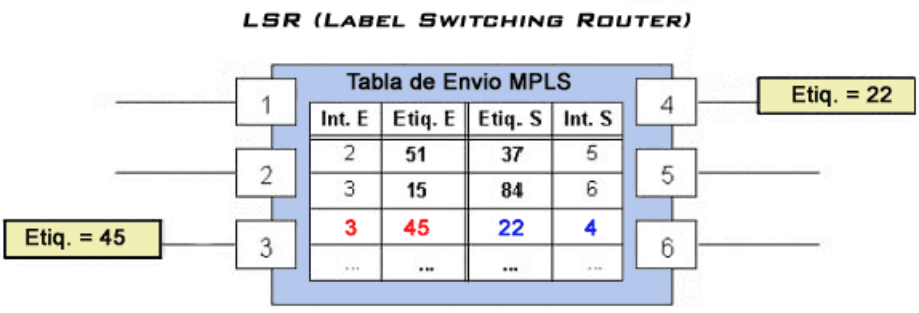


Figura 9: *Diagrama de Envió en MPLS*

Fuente: http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm

La etiqueta MPLS es un identificador dentro de la cabecera de los paquetes que permite clasificar un paquete con respecto a la FEC a la que pertenece. Esta asociación FEC-etiqueta puede no ser unívoca, y puede utilizarse la misma etiqueta para diferentes FECs (por ejemplo para darle el mismo tratamiento a diferentes FEC dentro de un segmento de la red), o pueden asociarse varias para la misma FEC (para realizar reparto de carga, por ejemplo).

MPLS añade una sobrecarga adicional para la comunicación entre routers adyacentes, sumada a la propagación de los prefijos de enrutamiento se agregan las funcionalidades de mantenimiento de las LIB y LFIB junto con las tablas de adyacencia, generado un consumo de recursos extra. CEF, LDP y otros procesos contribuyen también al aumento de consumo de dichos recursos.

La distribución de etiquetas se lleva a cabo a través de un protocolo de distribución de etiquetas, como LDP particularmente MPLS LDP.

Hay que tener en cuenta que la arquitectura de MPLS permite dos formas de propagar la información necesaria:

1. Extender la funcionalidad de los protocolos existentes.
2. Crear nuevos protocolos dedicados a la tarea de intercambios de etiquetas.

Extender la funcionalidad de un protocolo existente requiere bastante tiempo y esfuerzo, especialmente en BGP y OSPF.

En una arquitectura MPLS la decisión de asignar una etiqueta en particular a un FEC es propiedad del LSR en cada host a lo largo del camino. El LSR anterior informa al siguiente LSR sobre etiquetas decididas para esa FEC, esto implica esencialmente que las etiquetas se asignan en sentido ascendente hacia el destino.

El flujo del tráfico es un factor importante teniendo en cuenta que ocurre en un sentido bidireccional, es decir, que las etiquetas serán propagadas en ambas direcciones. Split Horizon hace que las etiquetas sean distribuidas en sentido descendente evitando que se propaguen hacia el vecino que propago la etiqueta. La FIB está sujeta a las normas de horizonte dividido por defecto desde el punto de vista del enrutamiento, por lo tanto la LIB y la LFIB también lo están.

La distribución de etiquetas puede ocurrir de dos formas:

- Unsolicited downstream
- Downstream-ondemand

Cualquiera de los dos casos ocurre ante un evento de convergencia, un vecino MPLS puede enviar (Unsolicited downstream) p solicitar que le envíen alguna actualización (Downstream-ondemand). Un ejemplo es cuando una etiqueta no está asociada a un FEC determinado.

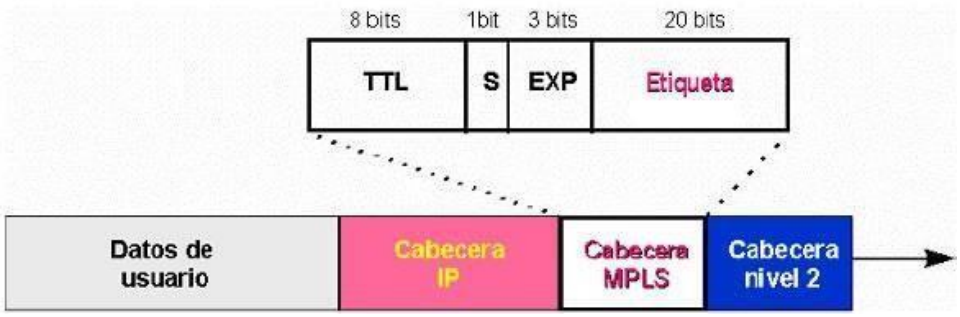


Figura 10: *Diagrama de Paquetes en MPLS*
Fuente: *http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm*

En la figura 10 se representa el esquema de los campos de la cabecera genérica MPLS. Los 32 bits de la cabecera MPLS se reparten en:

- 20 bits para la etiqueta MPLS.
- 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS).
- 1 bit de pila (stack) para poder apilar etiquetas de forma jerárquica.
- 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP.

LDP

LDP (Label Dsitribution Protocol) constituye un protocolo de control para distribuir la asociación de etiquetas a los LSRs. Se emplea para mapear las FECs a las etiquetas, a partir de las cuales se establecen los LSPs.

Las sesiones LDP se establecen siempre entre las parejas LSRs, conocidas como LDP Peers, no necesariamente adyacentes. Para el

establecimiento de sesiones utiliza TCP, e incluye mecanismos para el descubrimiento de LDP Peers potenciales.

Es un protocolo escalable, de forma que la distribución de etiquetas es incremental. Cuando hay pocas etiquetas utiliza asignación basada en downstream-on-demand y métodos de retención conservativos. Por el contrario cuando hay muchas etiquetas la asignación es unsolicited-downstream y la retención liberal.

Se definen cuatro tipos de mensajes LDP:

- Descubrimiento (Discovery messages). Utilizados para señalizar la presencia de LSRs en la red. Los mensajes se envían por difusión sobre UDP.
- Sesión (Session messages). Empleados para el establecimiento, mantenimiento y liberación de sesiones LDP (sesiones entre LDP Peers). Los mensajes se envía sobre TCP.
- Anuncio (Advertisement messages). Para crear, cambiar o borrar las asociaciones FEC-etiqueta.
- Notificación (Notification messages). Proporcionan información de avisos y señalización de errores.

2.2.8.3 Operación MPLS

Para transportar los paquetes de datos a través de una red MPLS es necesario llevar a cabo una serie de pasos:

- Descubrimiento de la topología de la red.
- Creación y distribución de etiquetas.
- Creación de los LSPs a partir del intercambio de etiquetas.
- Reenvío de paquetes.
- Eliminación de etiquetas a la salida de la red.

Descubrimiento de la topología.

El descubrimiento de la topología de la red se hace utilizando la propia información encaminamiento que manejan los protocolos estándar como OSPF, RIP, BGP, etc.

A partir de la información proporcionada por estos protocolos se construyen las tablas de encaminamiento en los LSRs.

Creación y distribución de etiquetas.

Los LSRs establecen las asociaciones FEC-etiqueta y construyen sus tablas (LIBs) antes de que comience el envío de tráfico. Para ello intercambian información de las asociaciones e información de las características de tráfico o capacidades MPLS mediante protocolos de distribución de etiquetas como LDP.

El contenido de las tablas establece el mapeo entre una etiqueta y un FEC, de forma que en función del interfaz y la etiqueta de entrada se puede obtener el interfaz, la etiqueta de salida y el siguiente salto. Las entradas de la tabla son actualizadas cada vez que se establece una nueva asociación FEC-etiqueta.

Creación de los LSPs

Los LSPs son creados en dirección inversa a la creación de entradas LIBs. El LER de entrada a la red MPLS utiliza la información de las tablas para encontrar cual es el próximo salto y con ello la etiqueta asociada a un determinado FEC.

La obtención de dicha asociación dependerá del método de distribución de etiquetas utilizando:

- Con downstream on demand el LER solicitará al siguiente salto la información de la etiqueta asociada a la FEC.
- Con unsolicited downstream puede disponer y de dicha información de los anuncios de asociación FEC-etiqueta recibidos de otros LSRs.

En los saltos siguientes si el LSR no tuviera información de la etiqueta de salida asociada a un FEC la solicitaría al LSR del siguiente salto, y así sucesivamente hasta llegar al LER de salida de la red MPLS.

Reenvío de paquetes

Cuando un paquete entra en la red el LER de entrada podría no tener ninguna etiqueta para ese paquete. En ese caso tendrá que crear un LSP para el FEC al que corresponde el paquete, siguiendo el procedimiento indicado en el punto de creación de LSPs.

Se dispone de la etiqueta el LER de entrada la inserta en el paquete y la reenvía al LSR del primer salto. A partir de ese punto cada LSR examina la etiqueta del paquete recibido, la sustituye por la etiqueta de salida y la reenvía hacia el LSR del siguiente salto por el interfaz de salida especificado en la LIB.

Eliminación de etiquetas a la salida

Una vez que el paquete llega al LER de salida este elimina la etiqueta ya que el paquete está saliendo de la red MPLS, y lo entrega al destino.

2.2.8.4 PROTOCOLOS DE ENRUTAMIENTO DINAMICO PARA MPLS

MPLS al igual que las tecnologías actuales de TCP/IP, utiliza los protocolos de enrutamiento dinámico tales como: protocolos de Gateway Interior y Exterior IGPs y EGPs respectivamente.

A continuación se detalla los protocolos de enrutamiento OSPF y BGP.

2.2.8.4.1 PROTOCOLO BGP

BGP (Border Gateway Protocol) es un protocolo de enrutamiento moderno diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables ente las organizaciones. BGP soporta VLSM, CIDR y sumarización.

BGP es un protocolo de enrutamiento extremadamente completo, usado entre organizaciones multinacionales y en internet. El principal propósito de BGP es conectar grandes redes o sistemas autónomos. Las grandes organizaciones utilizan BGP como el vínculo entre diferentes divisiones empresariales. BGP se utiliza en Internet para conectar diferentes organizaciones entre sí.

Es el único protocolo que actualmente soporta enrutamiento entre dominios, los dispositivos equipos y redes por una organización son llamados sistemas autónomos, AS. Esto significa independencia, es decir que cada organización es independiente de elegir la forma de conducir el tráfico y no se los puede forzar a cambiar dicho mecanismo. Por lo tanto BGP comunica los AS con independencia de los sistemas que utilice cada organización.

Funcionamiento Básico de BGP

BGP asocia redes con sistemas autónomos de tal manera que otros router envían tráfico hacia el destino a través de un sistema autónomo. Cuando el tráfico llega a los routers frontera de BGP, es trabajo de los routers del IGP encontrar el mejor camino interno.

BGP es un protocolo path-vector, aunque mantiene muchas características comunes con los de vector-distancia. Las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando y los bucles son enviados rechazando aquellas rutas que tienen el mismo número de sistema autónomo al cual están llegando.

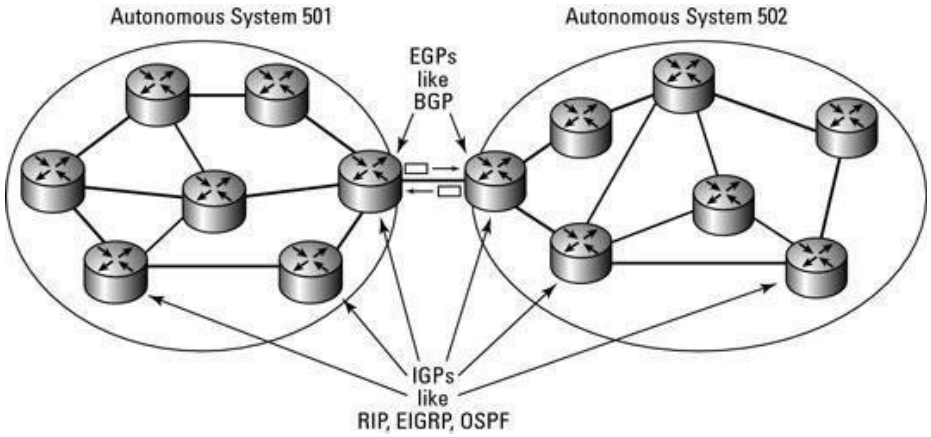


Figura 11: *Red con Protocolo BGP*
Fuente: *http://www.dummies.com/how-to/content/border-gateway-protocol-bgp-routing-protocol-overv.html*

Los vecinos BGP son llamados peers, estos no son automáticamente descubiertos sino que deben estar predefinidos. Existen cuatro tipos de mensajes en BGP para que la relación sea construida y posteriormente mantenida:

- Open
- Keeplive
- Update

- Notificaction

Cuando el proceso de BGP comienza se crean y mantienen las conexiones entre los peers utilizando el puerto TCP 179 a través de mensajes **BGP open,** posteriormente las sesiones son mantenidas enviando constantemente mensajes **keepalive** y la información de peer se mantiene en una tabla de vecinos separada. Si un peer es reseteado, este envía un mensaje de **notification** para indicar la finalización de la relación. Cuando se establece por primera vez la relación de vecindad, los routers BGP intercambian sus tablas de enrutamiento por completo utilizando mensajes **update**. Finalmente solo se enviaran actualizaciones incrementales cuando existan cambios en la red.

Jerarquías BGP

Otros protocolos de enrutamiento han sido creados de tal manera que soporten sumarizaciones y para que se pueda organizar la red de manera jerárquica. Las organización no están distribuidas jerárquicamente, por lo tanto BGP debe trabajar con cualquier topología que le sea dada. BGP se beneficia de la sumarización de la misma manera que los demás protocolos de enrutamiento, es decir, menos consumo de recursos de memoria y CPU, y tablas de enrutamiento más pequeñas.

Una red BGP optimizada será altamente sumarizada pero no necesariamente de manera jerárquica. BGP por naturaleza proporciona un resumen de las rutas claves identificando los posibles caminos entre sistemas autónomos. Debido a que los AS no están bien organizados, las redes BGP reflejan esa falta de organización. BGP puede ser implementado entre redes o dentro de una red. BGP detecta los bucles mirando las rutas de las AS-path.

Tablas de BGP

El enrutamiento a través de BGP involucra tres tipos de tablas:

- Tabla de vecinos
- Tabla de BGP
- Tabla de enrutamiento IP

Las rutas de BGP son mantenidas en una tabla de BGP separada y las mejores rutas son pasadas a la tabla de enrutamiento. A diferencia de los protocolos detallados en los capítulos anteriores, BGP no utiliza una métrica. En su lugar BGP emplea un proceso de 10 pasos para seleccionar las rutas dependiendo de una serie de propiedades.

BGP soporta herramientas como route-maps y listas de distribución que permiten al administrador cambiar el flujo de tráfico basado en los atributos de este protocolo.

MP – BGP (BGPv4)

Anteriormente BGPv4 era capaz de llevar solamente información para trafico IPv4. Sin embargo como se define en el RFC 2283, ya existen extensiones que permiten que BGPv4 lleve información de enrutamiento para múltiples protocolos de capa de red (IPv6 lPX, etc…). Las extensiones son compatibles con versiones anteriores, es decir, un ruteador que soporte las extensiones puede operar con otro ruteador que no soporte las extensiones.

Esta extensión del protocolo BGPv4 existente se utiliza para anunciar rutas VPN cliente entre los routers de tipo PE que se aprendieron de los routers de tipo CPE conectados. Estas rutas de los clientes pueden ser aprendidas a través de las rutas normalizadas de BGPv4, RIPv2, estáticas u OSPF.

MP-BGP solo se requiere dentro de la columna vertebral del proveedor de servicios. Por lo tanto, todas las sesiones de MP-BGP son sesiones internas de BGP, interna porque la sesión se da entre dos routers que pertenecen al mismo sistema autónomo.

MP-iBGP se requiere dentro de la arquitectura MPLS-VPN por que la actualización BGP necesita llevar más información que solo una dirección IPv4 como por ejemplo: dirección VPN-IPv4, información de etiquetas MPLS, comunidades BGP extendidas y comunidades posiblemente estándar BGP.

2.2.8.4.2 PROTOCOLO OSPF

El protocolo de “solamente la ruta más corta primero” (OSPF), es un protocolo de estado de enlace. Se conoce que los protocolos de estado de enlace mantienen una base de datos de información de topología. El algoritmo de enrutamiento de estado de enlace mantiene información compleja sobre ruteadores lejanos y su interconexión. Los protocolos de estado de enlace generan una inundación (flooding) de información de ruta, que da a cada ruteador una visión completa de la topología de red. El método de actualización desencadenada por eventos permite el uso eficiente de un ancho de banda y una convergencia rápida. Los cambios de estado de un enlace se envían a todos los ruteadores en la red tan pronto como se produce.

El protocolo OSPF es uno de los protocolos de estado de enlace más importantes, y se basa en las normas de código abierto (Open Source), lo que significa que muchos fabricantes lo pueden desarrollar y mejorar. Es un protocolo complejo que se describe en varios estándares del IETF cuya implementación en redes más amplias presenta un verdadero desafío. Este es un protocolo de enrutamiento de Gateway Interior (IGP) que es preferido por todos ya que presenta soluciones de escalabilidad. OSPF puede ser usado tanto en redes pequeñas como en redes grandes, en una sola área o en varias áreas.

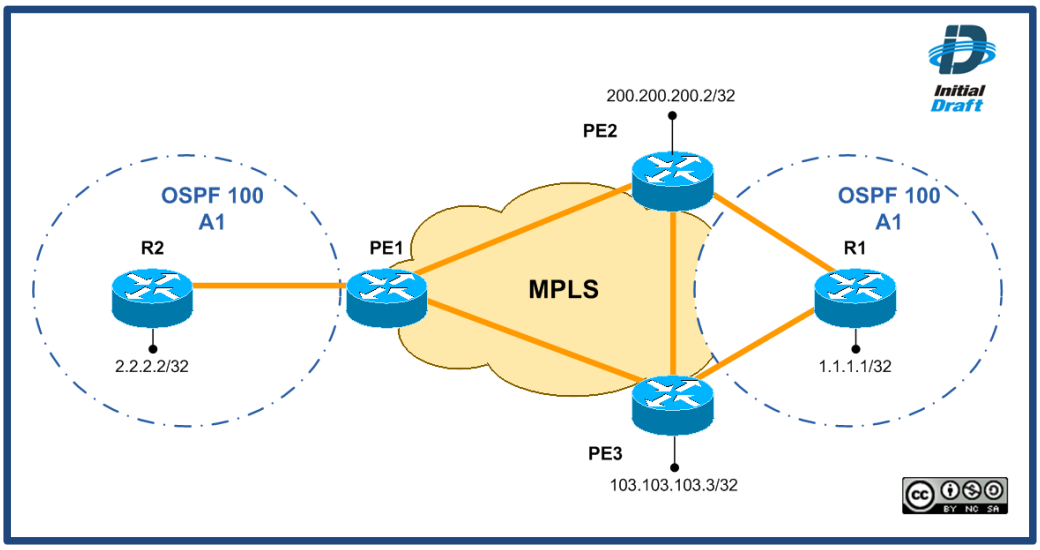


Figura 12: *Red con Protocolo OSPF*
Fuente: *https://blog.initialdraft.com/archives/2558/*

Las grandes redes OSPF utilizan diseño jerárquico, dado que varias áreas se conectan a un área de distribución o a una área cero, conocida como backbone. El enfoque del diseño para redes OSPF permite el control extenso de las actualizaciones de enrutamiento. La definición de área acelera la convergencia, limita la inestabilidad de la red y mejora el rendimiento.

OSPF utiliza un algoritmo de ruta más corta desarrollado por Dijkstra, un especialista holandés en informática en 1959. Este algoritmo considera la red como un conjunto de nodos conectados con enlaces punto a punto. Cada enlace tiene un costo, un nombre y cuenta además con una base compleja de todos los enlaces y por lo tanto se conoce la información sobre la topología física en su totalidad. Todas las bases de datos del estado de enlace, dentro de una determinada área, son idénticas. El algoritmo de ruta más corta calcula

entonces la topología sin bucles con el nodo como punto de partida y examinando a su vez la información que posee sobre nodos adyacentes.

Para que los ruteadores OSPF puedan compartir la información de enrutamiento se requiere una relación de vecinos y se tiende a esto cuando un ruteador es adyacente con por lo menos uno en cada red IP a la cual está conectado. Los ruteadores OSPF determinan con que otros pueden intentar formar adyacencias tomando como base el tipo de red a las cuales están conectados, es decir, unos trataran de hacerse adyacentes con respecto a todos los ruteadores vecinos y otros tratan de hacerse adyacentes con respecto a solo uno de los ruteadores vecinos. Una vez formada la adyacencia, se intercambia la información del estado de enlace.

Los equipos de enrutamiento con interfaces OSPF se reconocen tres tipos de redes:

a) Multiacceso de Broadcast (ej. Ethernet)
b) Redes Punto a Punto
c) Multiacceso sin Broadcast (ej. Frame Relay)

Cuando un ruteador inicia un proceso de enrutamiento OSPF en una interfaz, envía paquetes de descubrimiento (HELLOs) a intervalos regulares. En la capa de red los paquetes de descubrimiento se direccionan hacia la dirección Multicast 224.0.0.5 que equivale a todos los ruteadores OSPF, los mismos que utilizan estos paquetes para iniciar nuevas adyacencias y

asegurarse que entre los vecinos se mantenga el funcionamiento. Los mensajes de descubrimiento (HELLOs) se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes como Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un ruteador designado (DR) el cual se hace adyacente a todos los ruteadores del segmento broadcast y presenta un único punto de falla ya que todos los ruteadores del segmento envían el estado de enlace a este ruteador designado. Además de ello se elige un ruteador designado de respaldo (BDR).

El paquete de descubrimiento transmite información para la cual, todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

Los ruteadores adyacentes pasan por una secuencia de estados, y deben estar en su estado completo antes de crear las tablas de enrutamiento y direccionar el tráfico. Cada elemento de actualización del estado de enlace (LSU). Esos LSAs describen todos los enlaces de los ruteadores quienes al recibirlas de sus vecinos las registran en la base de datos del estado de enlace.

Una vez completas las bases cada ruteador utiliza el algoritmo SPF para calcular la ruta con menor costo hacia un destino desconocido, luego la información de enrutamiento mantenida y cuando existe un cambio en el

estado del enlace se produce la inundación notificándose así el cambio en la red.

2.2.9 VPN

Una Red Privada Virtual (VPN) es una red de información privada que usa una infraestructura pública de telecomunicaciones. Conecta diferentes segmentos de red o usuarios a una red principal, manteniendo la privacidad.

Es virtual porque al momento del establecimiento de la conexión el cliente virtualmente extiende la red de la empresa hasta donde él este, esto lo hace trabajar lógicamente dentro de la misma empresa.

Es privada ya que pertenece a una organización, pero que utiliza un canal compartido o público con estándares de seguridad y confiabilidad similares a los de un enlace privado gracias a la codificación de la información que transita entre los puntos de comunicación.

Es una red porque las VPNs son capaces de interconectar, extender y comunicar redes o segmentos de redes.

Una Red Privada Virtual se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalente a las que se obtienen con una red privada.

2.2.9.1 VPN de Capa 3

En las VPNs de capa 3, los proveedores de servicio entregan una conexión de línea arrendada entre un cliente y el POP (punto de presencia) más cercano en la red del proveedor de servicio. Actualmente las tecnologías VPN mas desplegadas, basadas en IP, son las VPN basadas en MPLS BGP (Border Gateway Protocol). Estas tecnologías pueden acomodar intranet, extranet y aplicaciones de acceso a internet, satisfaciendo la necesidad de las empresas de interconectar sitias dispersos geográficamente de manera segura y privada

Las VPNs basadas en IP permiten a las empresas tomar ventaja de la flexibilidad y ubicuidad de Internet y de las backbone basados en proveedores de servicio IP, para una comunicación segura, de un sitio a otro, de manera más eficiente. Las imperfecciones más importantes de VPNs basadas en IP son que soportan solamente IP y requieren una infraestructura de capa 3.

Propiedades:

- Encapsulación: Las VPNs encapsulan datos privados con un encabezado que les permite atravesar la red pública.
- Cifrado de datos: Esta propiedad permite convertir texto legible en un texto ilegible, logrando de esta manera que solo la persona a la que se le envía lo convierta en un texto legible.

Existen varias técnicas de cifrado de datos que funcionan en distintos niveles del modelo OSI, de esta manera se puede encontrar algoritmos de cifrado de enlace de datos y algoritmos de cifrado a nivel de red.

Beneficios: los beneficios de una Red Privada Virtual son solo un término general, que se utiliza para describir todas las utilidades potenciales cuando se implementa la tecnología VPN, entre estos podemos señalar: Seguridad, transparencia, flexibilidad, facilidad de instalación y uso, cobertura, ahorro de costos.

2.2.9.2 Redes VPN-MPLS

El estándar más extendido para proporcionar soluciones de VPN sobre MPLS es el definido por el IETF en la RFC 2547bis. Se conoce también como BGP/MPLS ya que utiliza BGP para distribuir la información de routing de la VPN a través del Backbone del proveedor de servicios, y MPLS para en reenvío del tráfico entre emplazamiento de la VPN.

El modelo de VPN definido por la RFC 2457bits consta de varios elementos:

- CE (Customer Edge Router). Es el router de cliente que proporciona acceso a la red del proveedor sobre un enlace de datos que se establece con uno o varios routers del proveedor. Una de las características más importantes es que puede utilizarse cualquier tecnología de acceso a

cualquier protocolo de encaminamiento entre el equipo del cliente y el del proveedor.

- PE (Provider Edge Routers). Es el router de entrada a la red del proveedor de servicios, al que se conectan los router de cliente, con los que intercambia información de encaminamiento pudiendo proporcionar el servicio de VPN a múltiples cliente, el PE mantiene las tablas de enrutamiento específicas de las VPN y a nivel MPLS actúa como LER y tiene capacidad para conmutar etiquetas.
- P (Provider Routers). Son los routers internos de la red del proveedor, que se comunican con los PE y con otros P pero no están conectados directamente a los routers de cliente. No necesitan mantener información específica de las rutas de la VPN y a nivel MPLS funcionan como LSRs conmutando etiquetas. La comunicación para el establecimiento de rutas entre Pes y Ps se realiza mediante el protocolo MP-BGP (Multiprotocol BGP).
- VRF (VPN Routing and Forwarding Table). Tabla de rutas única que se crea en el PE para cada VPN conectada al mismo, de forma que el PE se comporta como su hubiera varios routers virtuales, uno por cada VPN con su propia tabla de enrutamiento y retransmisión.

Este es el método utilizado para proporcionar seguridad, aislando el tráfico entre distintas VPNs. Cuando el PE recibe un paquete del CE se utiliza la tabla

de encaminamiento VRF que está asignada a ese emplazamiento para determinar el enrutado de los datos.

La asociación con el VRF establece a nivel de puerto, de forma que si el PE tiene varias conexiones (varios enlaces en distintos puertos) con el mismo emplazamiento todas ellas se pueden asociar con el mismo VRF.

Por otro lado dos interfaces solo pueden mapearse con el mismo VRF a menos que se pretenda que compartan información de rutas, y la dirección de destino de los paquetes para un VRF se determina en función del interfaz de entrada.

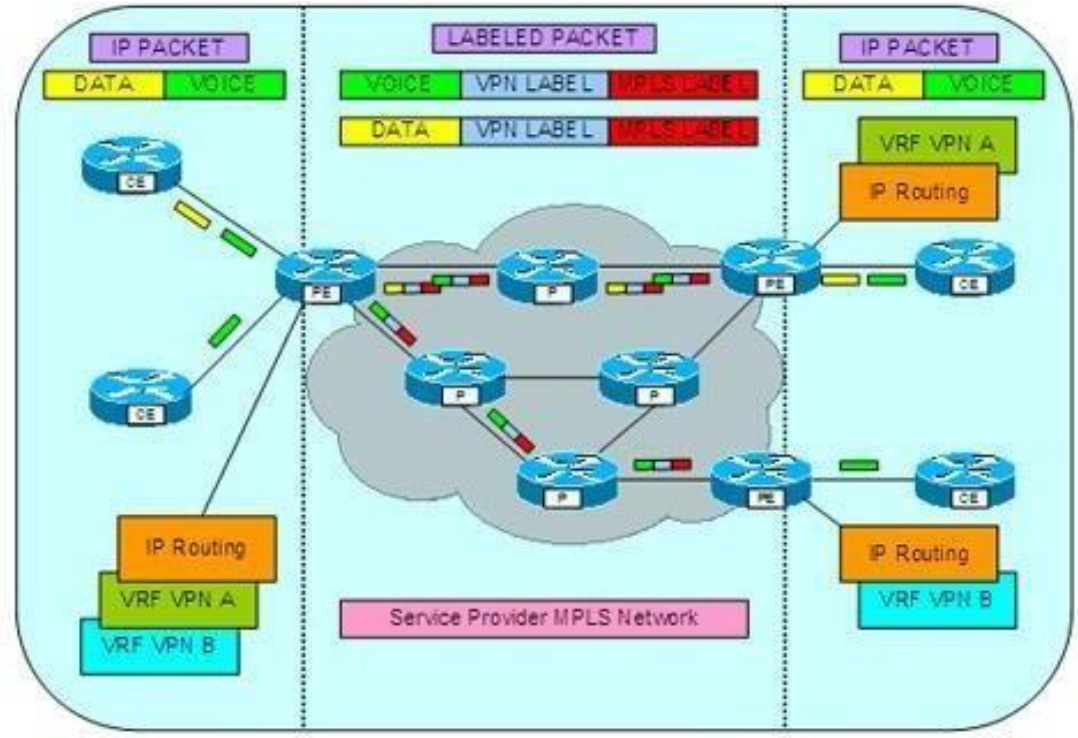


Figura 13: *Diagrama de MPLS-VPN*
Fuente: *http://www.tatateleservices.com/tata-enterprise-mpls-vpn-services.aspx?print=yes*

Este modelo es altamente escalable, a la vez que sencillo de configurar y administrar, ya que la información de encaminamiento de la VPN solo es necesario almacenarla en los PE que dan acceso a los distintos emplazamiento de una organización y, por otro lado, para añadir una nueva sede solo es necesario configurar el CE y el PE al que esté conectada.

Dentro de esta arquitectura se establecen dos tipos de topología para la comunicación entre las sedes de un VPN, organizando la red en subconjuntos de sedes conocidos como CERC (CE Routing Communities). Las dos topologías más comunes son hub-and-sopke y full-mesh.

Es la topología hub-and-spoke hay uno o varios CEs que actúan como hubs, y el resto de los CEs se comunican a través de estos en lugar de hacerlo directamente. Esta topología puede resultar útil cuando tenemos carios Ces ubicados dentro de la misma sede, o hay varias sedes interconectadas a través de otra red, o cuando se quiere reducir la información de enrutamiento que han de manejar los PEs y el número de LSPs dentro de la red MPLS.

La topología full-mesh es en la que todos los CEs se pueden comunicar directamente entre ellos.

Ventajas

Las redes VPN-MPLS presentan numerosas ventajas tanto desde el punto de vista del operador como del cliente:

- Utilización de la red de núcleo del operador. Desde el punto de vista del operador la tecnología MPLS ya está desplegada en el núcleo de la red IP, dando servicio a múltiples clientes, lo que permite ofrecer el servicio sin tener que hacer inversiones adicionales en el backbone y aun coste competitivo para el cliente.

- Desde el punto de vista del cliente el utilizar el backbone del operador supone un elevado ahorro de costes frente a la solución basada en el establecimiento de enlaces punto a punto. La construcción de enlaces se reduce el establecimiento del enlace entre la sede del cliente y el punto de entrada a la red MPLS del operador, lo que facilita y abarata la incorporación de nuevas sedes.

- Escalabilidad. La solución VPN-MPLS proporciona una alta escalabilidad a la red del cliente. Incluir una nueva sede solo requiere montar el enlace entre la sede y el PE de acceso a la red MPLS y configurar este PE. La capacidad de autodescubrimiento de los PE y la ausencia de información de routing de la VPN en los routers P hacen que no sea necesario modificar la configuración de todos los equipos de la red, evitando además el riesgo asociado a las reconfiguraciones. Este modelo de provisión se conoce como Point-to-Cloud.

- Accesibilidad. La VPN-MPLS permite utilizar cualquier tecnología de acceso para interconectar las sedes con la red del operador, lo que también proporciona una gran flexibilidad.

Por un lado permite al operador seleccionar la tecnología de acceso según el despliegue de red que tenga en cada zona, pudiendo proporcionar una mayor cobertura geográfica, y abaratar los costes de establecimiento del enlace para el cliente.

- Flexibilidad. La VPN-MPLS proporciona la interconexión de todas las sedes entre si lo que permite adaptarse a la topología requerida por las aplicaciones del cliente, pudiendo configurar fácilmente estructuras Full Mesh, Hub&Spoke, mixtas, etc. según las necesidades del cliente.

Por otra parte la tecnología permite el solapamiento de espacios de direcciones entre distintos cliente, con lo que el cliente puede utilizar su propio espacio de direcciones, público o privado, adaptándose completamiento a sus necesidades y minimizando la configuración de su red interna.

- QoS. La utilización de la red MPLS ofrece la posibilidad de definir clases de servicio dentro de cada VPN que se adapten a las diferentes aplicaciones que pueda necesitar el cliente, proporcionando distintos mecanismos que garanticen la calidad de servicio.

- Administración. Desde la perspectiva del cliente toda la administración y gestión del backbone la realiza el operador lo que simplifica todas las tareas asociadas al mantenimiento de su propia red.

Los routers de cliente de cada sede no tienen que intercambiar información de enrutamiento con otros routers de la VPN, por lo que todos los problemas de enrutamiento dentro del backbone son responsabilidad del operador, y el cliente tampoco tiene que gestionar los accesos a los routers PE o P.

En el lado del operador la misma red de backbone puede proporcionar servicio a las VPNs de múltiples clientes sin necesidad de administrar cada una de ellas por separado.

- Seguridad. La VPN proporciona la separación de flujos de tráfico entre los distintos clientes que utilizan el backbone del operador ofreciendo niveles de seguridad equivalentes a los de los circuitos virtuales ATM o Frame Relay sin necesidad de implementar técnicas de encriptado adicional.

Aun así en caso de ser necesarias medidas de protección adicionales se puede recurrir a soluciones combinadas como la utilización de IPsec sobre VPN-MPLS

- Disponibilidad. La red de backbone del proveedor de servicios generalmente ofrece unos niveles de redundancia y alta disponibilidad que es aprovechado por el cliente al utilizar esta red como punto de unión entre todas las sedes.

Conseguir los mismos niveles de disponibilidad con otro tipo de tecnologías supondría una solución muy compleja y costosa para el cliente. Con la VPN-MPLS el cliente se beneficia de la alta disponibilidad sin añadir complejidad a su red, de forma transparente, y aun coste reducido.

Por otra parte la red VPN-MPLS permite conectar todas las redes en una topología totalmente mallada entre las diferentes sedes, lo que supone que ante la caída de una de las sedes el resto permanecen comunicadas entre sí.

2.3 MARCO CONCEPTUAL

A continuación se detalla el tipo de conexión que se va a realizar para el diseño de la Red:

Para lo que es la conexión de la Red Móvil se empleara para los servicios móviles de la Policía Nacional del Perú los siguientes términos:

- MME (Mobility Management Entity): La MME es el control-nodo clave para el acceso de LTE hacia la red. Es responsable de realizar el procedimiento de etiquetado que incluye transmisiones y retransmisiones en el UE (Equipo de Usuario). Está implicado en el proceso de activación portador / desactivación y también es responsable de la elección de la S-GW para un UE en adjuntar la inicial y en el momento de intra-LTE de traspaso que implica la Red Central (CN) la nueva ubicación del nodo.

- S-GW: El S-GW es un equipo de plano de usuario que es controlado por el MME. El S-GW también es un punto de monitoreo de las políticas de conexión y servicio establecidas en el PCRF (Policy and Charging Rules Function).

- P-GW: El P-GW puede ser comparado con las funciones realizadas por el GGSN pero además tiene un importante rol en el control de la movilidad. El P-GW asigna la dirección IP al UE.

Para la red MPLS se va a usar MPLS VPN (Virtual Private Network MPLS). MPLS VPN proporciona direccionamientos privados e independientes entre sí. Por ejemplo supongamos que un proveedor de servicios de internet tiene diferentes clientes, los clientes de una entidad en concreto no desearon que direccionamiento sea conocido por otro cliente del proveedor. Con MPLS VPN cada cliente es totalmente anónimo y privado para otro y su enrutamiento

desconocido. Sería lo que podríamos decir entornos de routing independientes. MPLS VPN consigue las diferentes tablas de routing mediante las llamadas VRF (Virtual routing and forwarding). Cada cliente tendría asignado su VRF y por otro lado su propia tabla de enrutamiento. Al tratarse de tablas de routing independientes y privadas podemos duplicar IPs mientras estas no se encuentren dentro de la misma VRF. Este hecho es una gran ventaja si lo comparamos con otro tipo de redes.

Para la conexión en el MPLS se utiliza tres términos para describir el rol de los equipos que forman parte de una red MPLS:

- CPE (Customer Premises Equipment): dispositivo que se encuentra fuera de la red MPLS y por lo tanto no utiliza sistema de etiquetado (Generalmente es el cliente de un ISP).
- PE (Provider Edge): Equipo que comparte al menos un enlace con un CPE y otro dentro de la red MPLS. Se encarga de introducir las VRFs y realizar las funciones de PUSH y POP
- P (Provider): Router que estaría totalmente dentro de la red MPLS. No tendría ningún enlace conectado directamente a un CPE.

Entre los dispositivos del tipo P y PE se realiza el MPLS unicast y básicamente utilizaremos el protocolo de routing BGP para asociar etiquetas con IPs.

Por otra parte el PE debe aprender las rutas del CPE. Estas rutas aprendidas por el PE se deben transmitir hacia el P. Para ello se utiliza el protocolo de routing BGP. BGP nos permite establecer vecinos sin que estos estén directamente conectados e intercambiar las diferentes rutas (siempre y cuando un vecino BGP sepa cómo llegar hasta otro).

A continuación se muestra la figura 13 para describir la topología de Red que se va a utilizar en este Diseño:

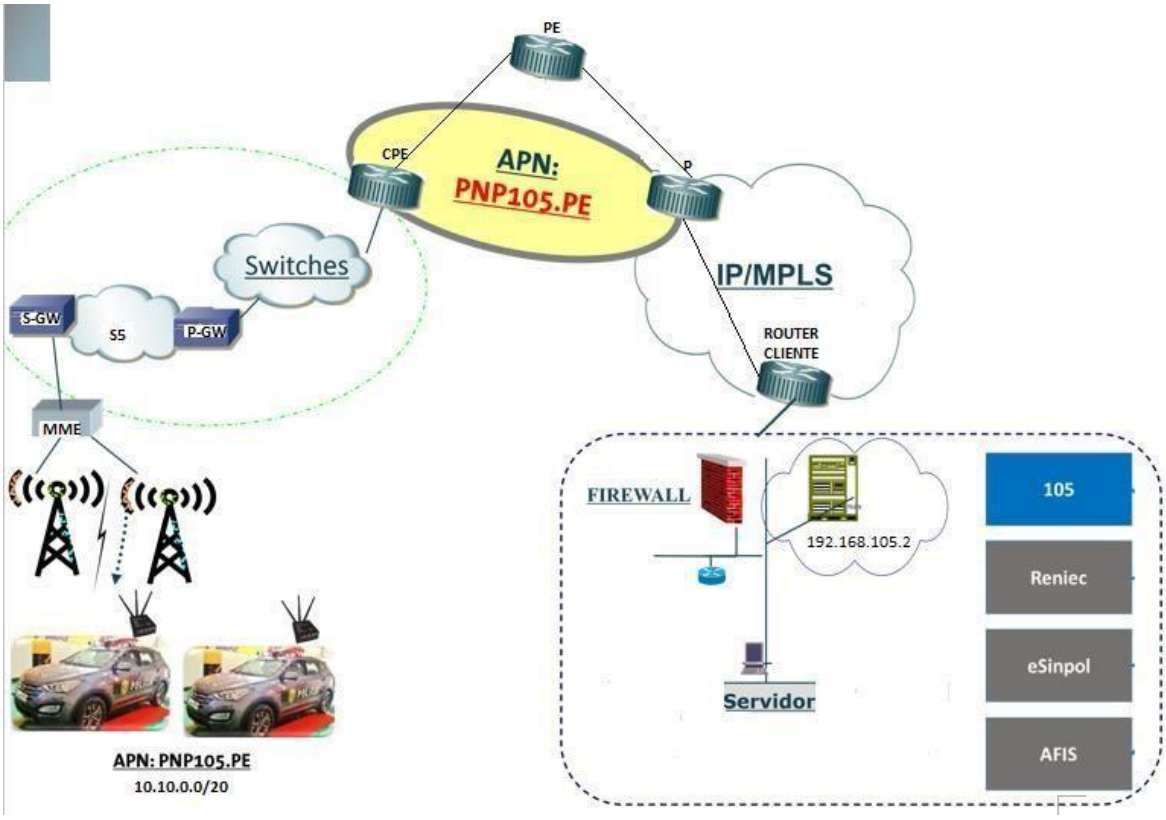


Figura 14. *Topología de Red para la PNP*
Fuente: *Realización Propia*

CAPITULO III

3.1 ANÁLISIS DEL SISTEMA

Este proyecto está enfocado básicamente en la interconexión que van a tener la sede principal y los patrulleros de la Policía Nacional del Perú, aprovechando la red pública de un Proveedor de Servicios.

Para la solución a la problemática actual que se presenta se implementa una red bajo una plataforma que está constituido en la unión de la Red Móvil con la red VPN-MPLS con la cual integraremos sus servicios e interconectaremos a los usuarios con la Sede Principal, aprovechando las bondades de la Red Móvil 4G LTE que permite una transmisión a una alta velocidad a diferencia de las demás tecnologías y también la red MPLS presenta un modelo acoplado e inteligente, ya que MPLS reconoce la existencia de VPNs (Redes Privadas Virtuales), se minimizará la complejidad

de los túneles, fácil provisión de servicios ya que cada conexión afecta a un solo router, mayor escalabilidad, garantías para QoS(Calidad del Servicio), ingeniería de tráfico entre otros, de esta forma se disminuirá los costos.

En la siguiente gráfica (Ver Figura 15) se puede ver la interconexión centralizada que va a existir entre los usuarios (Patrulleros de la Policía) y la sede principal, esta comunicación se implementará mediante o a través de la red Móvil y la red MPLS de un proveedor de servicios, esta red es transparente para el Cliente final “Policía Nacional Del Perú”, ya que va a actuar como si fuese una conexión punto a punto.

Las conexiones punto a punto (Sede Principal → Usuarios) se va a realizar mediante una VRF (Virtual Routing Forwarding) que se crea en la Nube Móvil y MPLS específicamente en los routers y otros equipos de transmisión, la cual garantiza una conexión segura y libre de tráfico que no corresponde a la Data del cliente.

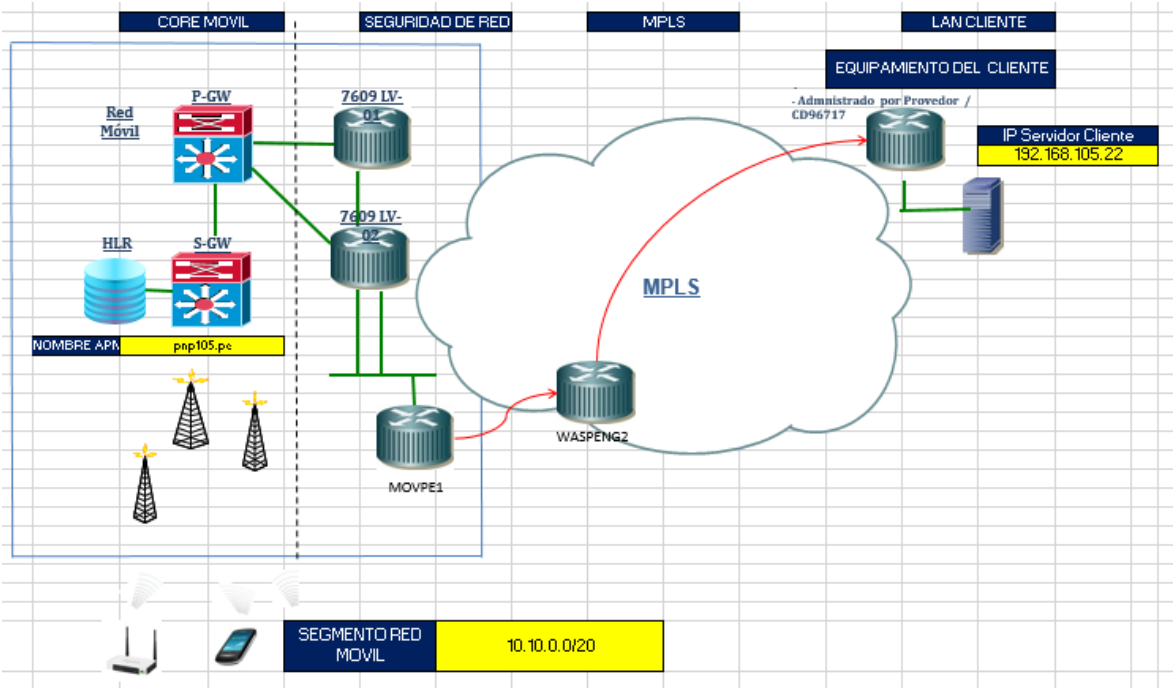


Figura 15. *Diseño de Red para la PNP*

Fuente: *Realización Propia*

Como se puede observar se han adicionado diferentes servicios de manera didáctica, por lo que al usar la Red Móvil y la Nube MPLS del proveedor de servicios se pueden transmitir todo tipo de información ya sea Data (Correos, Internet, transacciones que manejará la empresa, etc.).

3.2 DISEÑO DE LA TOPOLOGIA DE RED PARA LA COMUNICACIÓN DE LOS MOVILES DE LA POLICIA NACIONAL DEL PERU

Cuando se trata de diseñar una red, se deben considerar aspectos importantes ya que al momento de implementar es necesario asegurarse que el diseño escogido fue la topología más adecuada con los equipos de buen

desempeño que puedan ofrecer confiabilidad, Las consideraciones de diseño para la red presente se han establecido de la siguiente forma:

Para la Red Móvil: está formado por la Red 4G LTE que tiene los siguientes equipos para la transmisión de Datos, HSS este equipo sirve para el registro de los usuarios en la red móvil, USN este equipo sirve para la creación de contexto de la línea en la Red de Datos Móviles y UGW sirve para la salida a la transmisión de Datos hacia otras Redes.

Para la Red MPLS: está formado por una red mallada completa (Full mesh), construida con equipos de la plataforma Cisco, de tal forma que un proveedor con un diseño full mesh en su núcleo de red pueda ofrecer garantías de envío de información y que además cuente con caminos adicionales y redundantes según se dé el caso de que falle algún nodo en el núcleo de la nube.

En el caso de la red para la Policía Nacional del Perú, para enviar información a través de la Red móvil y la nube MPLS se debe ofrecer una topología lógica de tal manera que haga parecer que se cuenta con enlaces dedicados desde un sitio matriz (Sede Principal) hacia cada una de los usuarios finales (Patrulleros). Una red diseñada que será utilizada para el envío de información debe ser transparente para la empresa (Cliente) dado que, al contar con una topología definida se puede alcanzar los destinos por diferentes caminos y así hacer del transporte de la información algo confiable. La siguiente

figura da una referencia de cómo se conectan la Sede Central con la Sede 105 así como también con los usuarios finales(Patrulleros) con su matriz para ser servidor de las distintas aplicaciones que van a utilizarse tales como: acceso al 105, Reniec, transferencia de archivos, eSinpol, AFIS, etc.

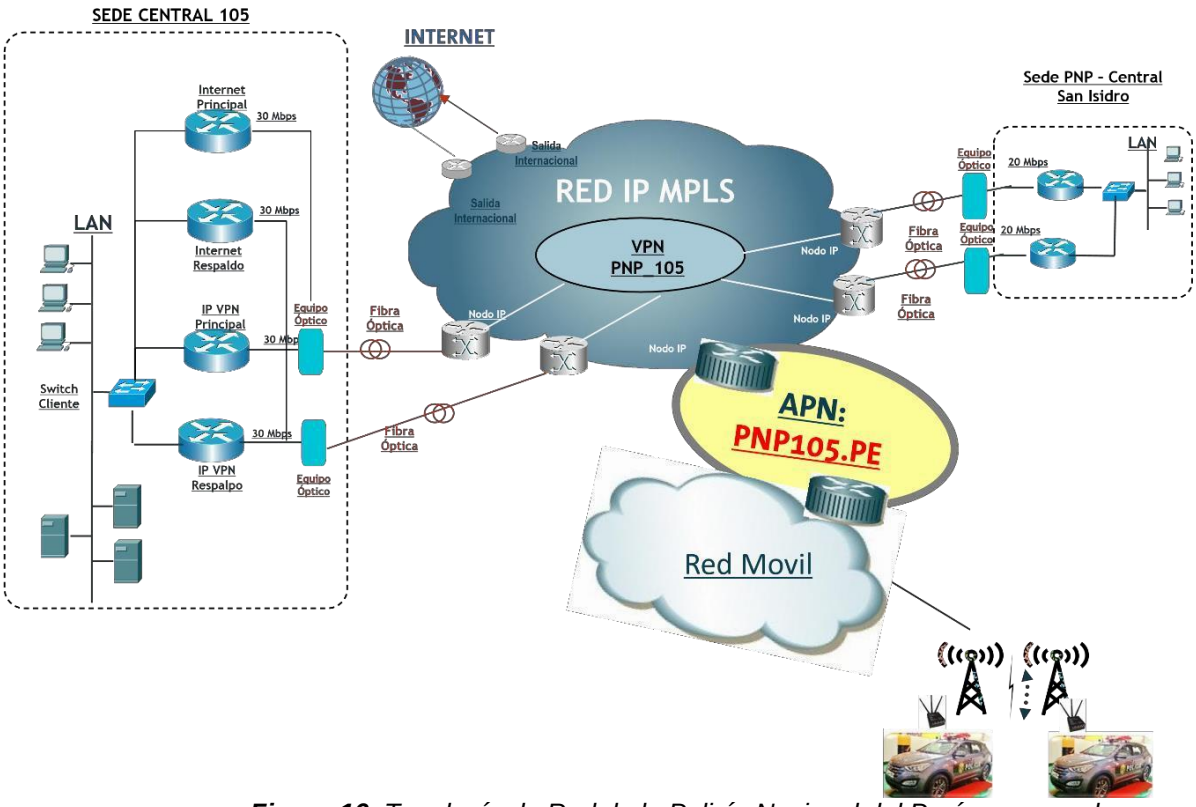


Figura 16. *Topología de Red de la Policía Nacional del Perú en general*
Fuente: *Realización Propia*

3.2.1 Herramientas representativas en el diseño de la Red Móvil

Como se menciona en capítulos anteriores, una red Móvil de Datos está formado por el MME, S-GW y P-GW; los siguientes equipos son los que se van a utilizar para la transmisión de Datos, HSS9860 (MME), USN9810 (S-GW) y UGW9811 (P-GW).

3.2.2 Herramientas representativas en el diseño de la Red MPLS

Como se menciona en capítulos anteriores, una red MPLS está constituida por elemento de núcleo (P – Routers o LSRs) y elementos de frontera (PE – Routers o LERs). En lo correspondiente, tanto a la frontera como al núcleo MPLS se toma en cuenta el uso de ruteadores de la serie Cisco 2900, con un sistema operativo IOS C2921/K9 para uso de proveedores de servicio, el mismo que cuenta con las funcionalidades necesarias, cualidades de procesamiento y gestión de recursos adecuadas a usarse en una red MPLS.

3.2.3 Configuración de los protocolos a usar en la Red de la Policía Nacional Del Perú en el emulador.

Para un mayor conocimiento y validación de la topología elegida como modelo de la red es necesario el uso de herramientas de aplicación que simulen el comportamiento de la red de tal manera que se pueda estudiar el comportamiento del tráfico que circulara por la Red. Las características que deben presentar las herramientas de simulación, deben acoplarse a los requerimientos que demande una Red, para que de esa forma las condiciones y problemas que se presenten, se tomen en cuenta en ambientes de implementación con equipamiento real. Las herramientas que se utilizan para este diseño de red son muy poderosas y se destacan por ser:

a) Configurable: De tal manera que se pueden alterar parámetros de red y de tráfico que circula a través de ella.
b) Rigurosa: Ya que muestra estabilidad.
c) Analizable: porque los resultados revelan el comportamiento de la red y los posibles problemas que puedan surgir.
d) Portable: dado que es código abierto y fácil de ejecutar en varios sistemas operativos.

3.2.4 Configuración que se va a realizar para la simulación de la Red Móvil

Para la siguiente simulación de la Red se ha empleado una línea de prueba la cual va a servir para verificar la configuración por parte del área de la Red Móvil en los diferentes equipos de transmisión. La línea de prueba es 996666709 con ella vamos a identificar como se desplaza la configuración en los diferentes puntos de la Red Móvil, más adelante se mostrara la configuración de la Red MPLS.

3.2.4.1 Configuración en el MME

Primero se verifica en el equipo HSS9860 (MME) que la línea ha sido registrada para la comunicación del servicio de Datos, en la Figura 17 se verifica que se crea registro a nivel de GSM y GPRS.

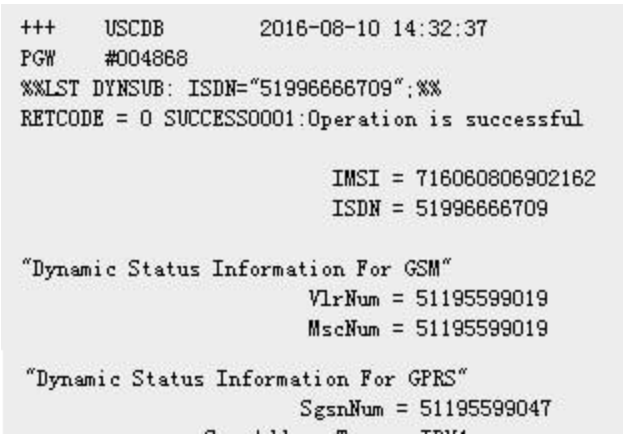


Figura 17. *Registro en MME*
Fuente: *Realización Propia*

Luego hay que verificar que la línea tenga el APN impactado en la plataforma, en este caso el APN pnp105.pe tiene el Template 219, trabaja con IP Estática el cual se le ha asignado la IP 10.10.15.250 para entablar la comunicación.

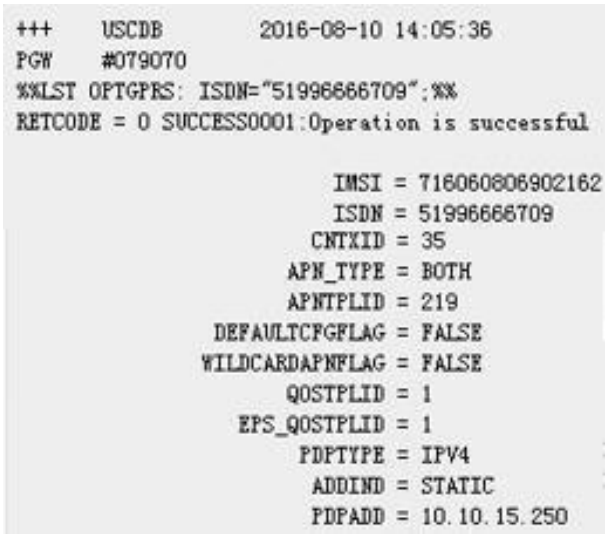


Figura 18. *Registro del APN en MME*
Fuente: *Realización Propia*

3.2.4.2 Configuración en el S-GW

Luego de haber verificado el registro se tiene que observar que la línea se ha atachado a la Red de Datos, esto se realiza mediante la comunicación que se da en el S-GW, en la Figura 19 se verifica que la línea se atacha a la Red de Datos, esto implica que ha generado un contexto el cual va a permitir la comunicación con el P-GW.

Figura 19. *Registro en S-GW*
Fuente: *Realización Propia*

Luego de verificar que esta atachado a la Red de Datos hay que observar en que Estación Base (eNodoB) se a atachado esta configuración se verifica en la plataforma, luego hay que realizar la conversión para observar el CI de la Estación a la cual se ha conectado.

```
                Tracking area list  =  716060898
E-UTRAN cell global identity  =  716060050401
            Global eNodeB ID  =  7160600504
```

4G SECTOR (Global e-Node ID)	CELDA 4G (ENVIAR A ACCESO)
7160600504	1284

Figura 20. *Registro para ubicar Estación Base conectada en el S-GW*
Fuente: *Realización Propia*

Después se verifica en la Tabla adjunta a que estación se ha conectado la línea de prueba.

CI-4G	1284
Dirección :	Av. San Felipe 1100-1144
Region	LIMA
Departamento:	LIMA
Provincia:	LIMA
Distrito:	SURQUILLO
Estación Base :	FELIPE
Sector:	MACRO-CELDA
Latitud:	-12.108797
Longitud:	-77.015696
Amplitud:	65
Azimut:	329
Hora:	
Fabricante:	NOKIA
Tecnologia:	LTE
Controlador:	NA
Tipo de equipo:	LTE
Frecuencia:	2100
TRX:	0
Tipo de Transmision:	FIBRA OPTICA
Grupo Responsable:	RADIO

Tabla 1. Verificación de la Estación a la cual se conectó a la Red de Datos

Por último se observa en plano la ubicación que se tiene con referencia hacia la Estación Base en el cual se ha conectado la línea de prueba, para este caso presenta parámetros correctos de ubicación.

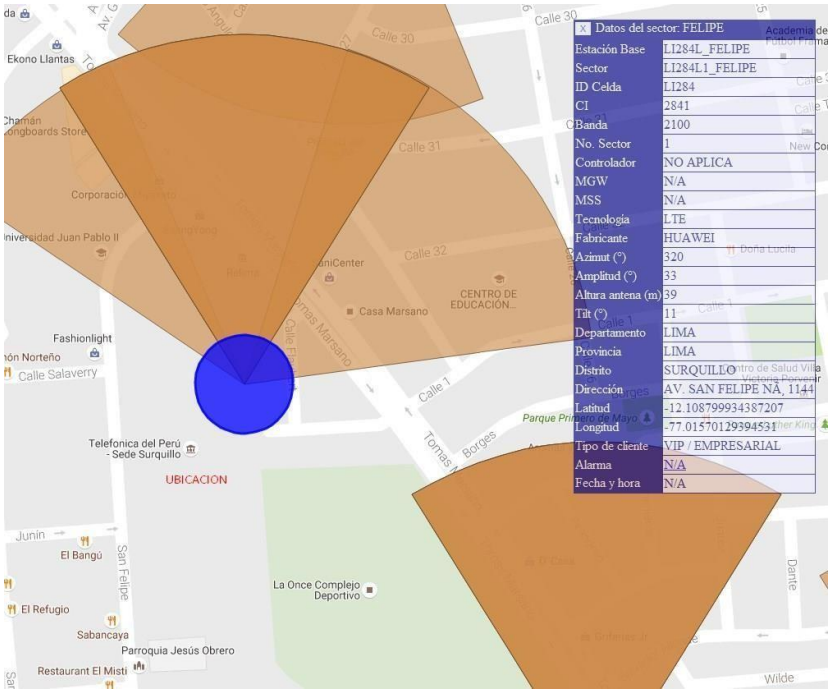


Figura 21. *Ubicación de Estación Base conectada en el S-GW*

Fuente: *Realización Propia*

3.2.4.3 Configuración en el P-GW

Luego de haber verificado que la línea se atacho a la Red se tiene que observar que la línea se encuentre en la base de Datos del P-GW para obtener la transmisión de Datos hacia el exterior (Envió y Recepción de paquetes), esto se realiza mediante la comunicación que se da en el S-GW, en la Figura

22 se verifica que la línea está registrada en la plataforma, esto implica que ya va a haber comunicación hacia la nube MPLS.

```
<UGWLV01>display pdpcontext msisdn 51996666709
The PDP context on board 11
--------------------------------
                          IMSI  =  716060806902162
                          IMEI  =  867820023326730
                      UGW Role  =  PGW
                  EPS Bearer ID  =  6
                Default Bearer  =  Yes
                      PDP type  =  IPv4
             IPv4 Address type  =  STATIC ADDRESS
              IPv4 PDP address  =  10.10.15.250
                        MSISDN  =  51996666709
                      APN name  =  pnp105.pe
```

Figura 22. *Registro en P-GW*
Fuente: *Realización Propia*

3.2.5 Configuración que se va a realizar para la simulación de la Red MPLS

Para la configuración de la Red MPLS se va a emplear las siguientes configuraciones en los router de acceso que se va a tener.

3.2.5.1 Configuración del MPLS en el router Cisco

Es necesario habilitar las funcionalidades multiprotocolo las cuales permitan que a los paquetes IP se les añada etiquetas para el envío MPLS.

Mediante la Tabla 2 se indican los comandos para la configuración de MPLS en un ruteador Cisco.

COMANDOS	Funcionalidad
Router(config)# ip cef	Habilita de manera global una funcionalidad de envió y conmutación propietaria de Cisco
Router(config)# mpls ip	Habilita el envió MPLS de paquetes de longitud IPv4, normalmente caminos enrutados por la plataforma
Router(config)# interface <type> <slot/port>	Permite ingreso al modo de configuración de Interfaz

Tabla 2. *Configuración de MPLS*

3.2.5.2 Configuración de Intercambio de Etiquetas – LDP (Label Distribution Protocol)

Para la distribución de etiquetas en las interfaces es necesario especificar el protocolo que se utilizara y que de esa manera los dispositivos vecinos realicen el intercambio correspondiente y la negociación para luego crear las respectivas tablas que indican las etiquetas correspondientes a los paquetes entrantes. El comando presentado (Tabla 3) detalla la sencilla configuración para la distribución de etiquetas en una interfaz.

Comandos	Propósito
Router(config - if)# **mpls label protocol** <ldp | tdp | both>	Configura el protocolo de distribución de etiquetas en una interfaz

Tabla 3. *Configuración de señalización LDP*

3.2.5.3 Configuración del Protocolo BGP

El protocolo de Gateway de frontera BGP, permite la comunicación entre dominios por lo que su implementación debe ser únicamente en las fronteras de una Red. Para la conexión de sitios locales con sitios remotos mediante VPNs, este protocolo es muy usual ya que además permite ser trabajado como protocolo de interiores y se utiliza para la comunicación específica entre dispositivos de frontera. Su implementación debe referirse al uso de sistemas autónomos y dado que en esta implementación se utiliza como BGP interior, el sistema autónomo será único y servirá para identificar a la nube MPLS como sistemas bajo una administración común. La Tabla 4 muestra en detalle los pasos a seguir a la hora de implementar la comunicación BGP entre dispositivos de frontera que pertenecen a un mismo sistema autónomo.

Comandos	Propósito
Router(config)# **router bgp** <*AS número*>	Configura el proceso de enrutamiento IBGP con el número de sistema autónomo que será pasado a otros vecinos IBGP
Router(config-router)# **neighbor** <ip-address | peer-group-name> **remote-as** <AS-number>	Especifica la dirección IP de un vecino con el cual se establecerá en enrutamiento BGP identificando el sistema autónomo al que pertenece.
Router(config-router)# **neighbor** <ip-address | peer-group-name> **update-source** <loopback-interface>	Configura a BGP para que utiliza cualquier interface operacional en conexiones TCP
Router(config-router)# **neighbor** <ip-address | peer-group-name> **activate**	Establece el emparejamiento con un vecino especificado.

Tabla 4. *Configuración de Enrutamiento BGP*

3.2.5.4 Configuración de la VPN

La creación y configuración de VPNs en MPLS es muy sencilla con el uso de BGP y se deben tener en cuenta pasos como: definición de VPNs configuración de iBGP entre dispositivos de frontera, y configuración de enrutamiento hacia cliente en los ruteadores de frontera (Tablas 5,6 y 7).

Definición de VPNs de capa de red	
Comando	**Propósito**
Router(config)# **ip vrf** <vrf-name>	Define la instancia de enrutamiento virtual con su nombre
Router(config-vrf)# **rd** <route-distinguisher>	Crea tablas de enrutamiento y envío
Router(config-vrf)# **route-target import** <route-target-ext-community>	Crea una lista de importacion de comunidades extendidas de ruta objetivo para la VRF especificada
Router(config-vrf)# **route-target export** <route-target-ext-community>	Crea una lista de exportación de comunidades extendidas de ruta objetivo para la VRF especificada
Router(config-vrf)# **interface** <type> <slot/port>	Ingresa al modo de configuración de interfaz
Router(config-if)# **ip vrf forwading** <vrf-name>	Asocia una VRF con una interfaz

Tabla 5. *Creación y definición de VPNs de capa 3*

Configuración de MP - IBGP entre sesiones PE – PE	
Comando	**Propósito**
Router(config)# **router bgp** *<AS número>*	Ingresa al proceso de enrutamiento IBGP con el número de sistema autónomo que está configurado
Router(config-router)# **address-family vpnv4**	Ingresa al modo para configuración de MP - IBGP para VPNv4
Router(config-router-af)# **neighbor** <ip-address | peer-group-name> **activate**	Establece el emparejamiento con un vecino especificado.
Router(config-router-af)# **neighbor** <ip-address | peer-group-name> **send-community both**	Los vecinos renegocian sus capacidades

Tabla 6. *Configuración de Multiprotocol BGP*

Configuración de MP-BGP entre sesiones PE -PE	
Comando	**Propósito**
Router(config)# **address-family ipv4 vrf** <name-vrf>	Configurar por VRF el enrutamiento por BGP
Router(config)# **neighbor** <ip-address> **remote-as** <AS-number>	Especifica la dirección ip del vecino que se establecerá el enrutamiento BGP
Router(config)# **neighbor** <ip-address> **activate**	Especifica la dirección ip del router vecino y la activa
Router(config)# **neighbor** <ip-address> **as-override**	Activa la función de cambio de AS de los router de origen por lo de destino.

Tabla 7. *Configuración del enrutamiento BGP sobre la VRF*

3.2.5.5 Configuración del Router final del Cliente en la Sede principal

Para la sede central del cliente se va a configurar el Router por medio de una red MPLS que les brinde seguridad al momento de transmitir información, es necesario conocer los diferentes dominios que se pueden presentar al momento de entablar las redes de datos.

En este caso el Router tiene la etiqueta CD96717, en la figura 23 se muestra la configuración que tiene para entablar la comunicación hacia la Red Móvil.

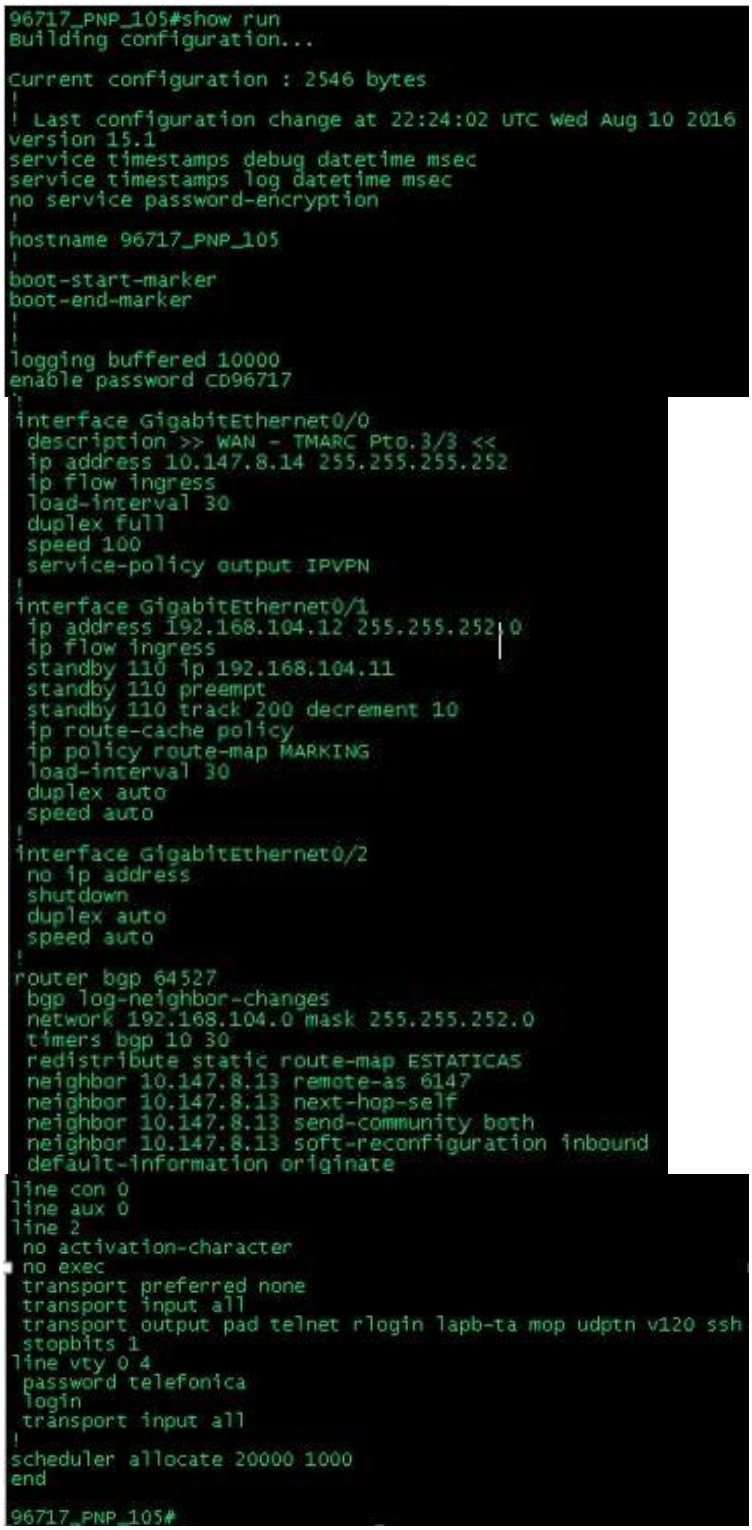


Figura 23. *Configuración en el Router del cliente*

Fuente: *Realización Propia*

3.3 Revisión y Consolidación de Resultados

Para la revisión del Trabajo de la Red se va a verificar la configuración que se tiene en los diferentes equipos así como también de las pruebas de conectividad que se tiene que realizar para verificar la conectividad del servicio.

Como resultado final tenemos la siguiente topología.

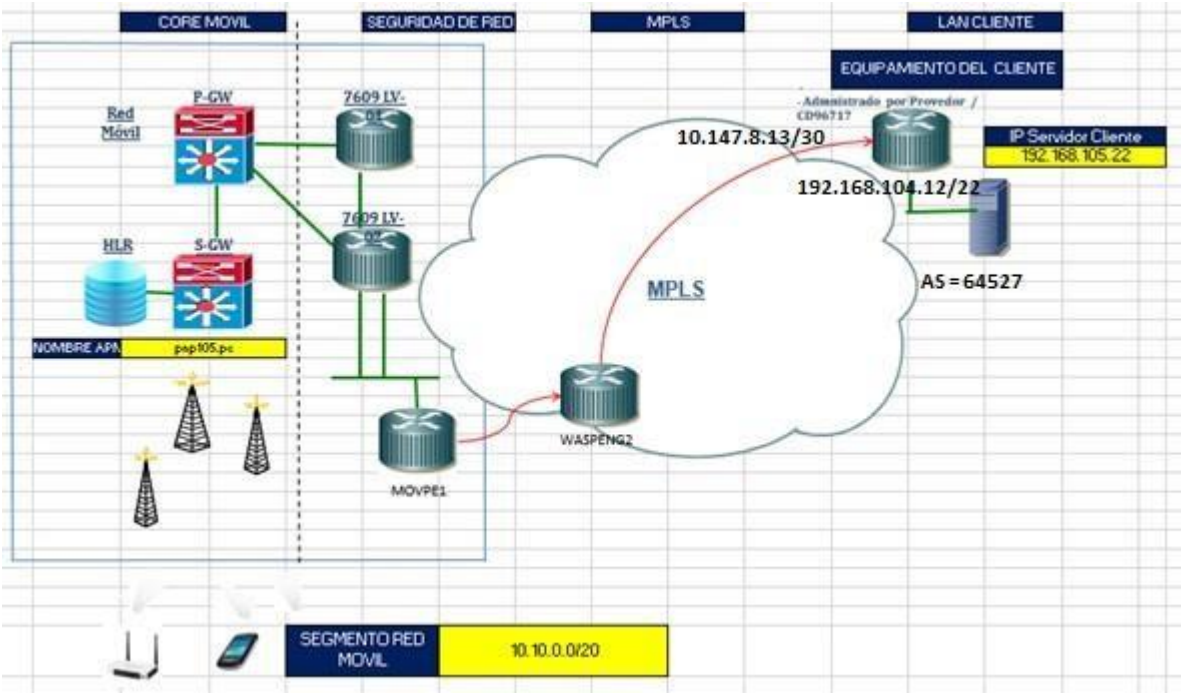


Figura 24. *Diseño Final de Red para los servicios Móviles de la Policía Nacional del Perú*

Fuente: *Realización Propia*

3.3.1 Revisión de la Configuración

Se va a identificar los parámetros de configuración en los equipos de comunicación que se tiene en la Red.

3.3.1.1 Configuración en el WASPENG2

Se verifica que la configuración en el WASPENG2 contiene los parámetros de Red para la comunicación.

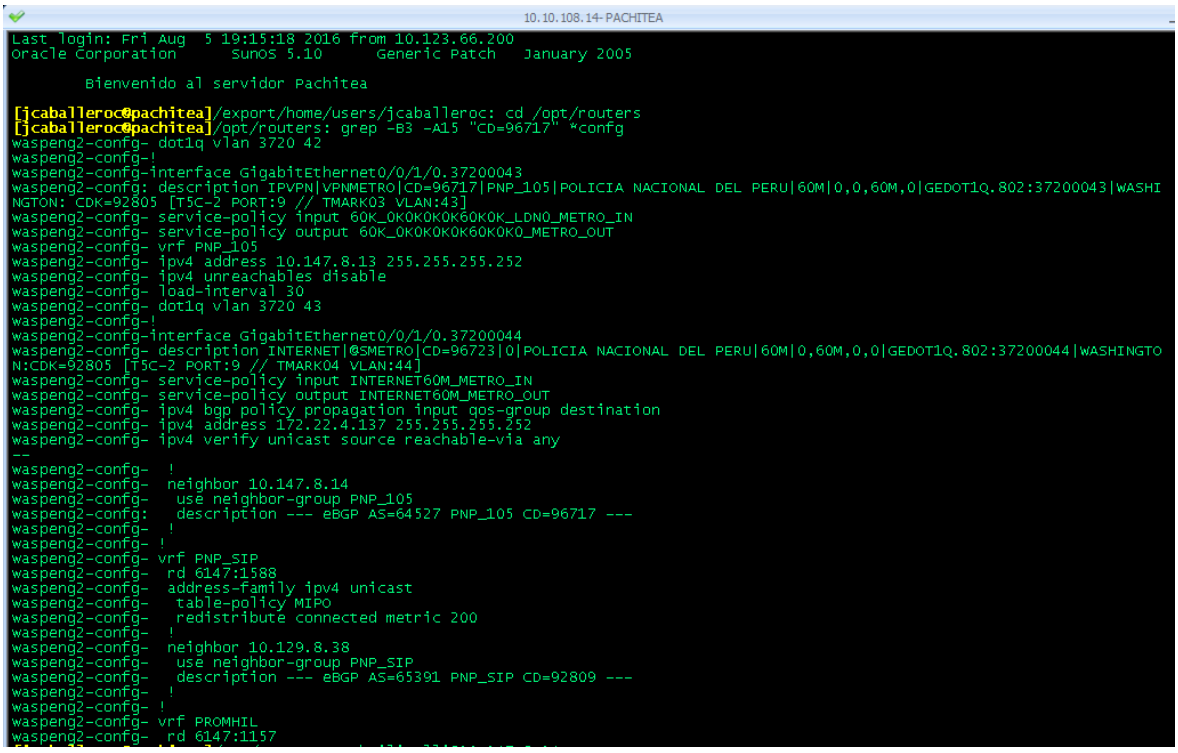


Figura 25. *Configuración en el WASPENG2*

Fuente: *Realización Propia*

3.3.1.2 Configuración en el Router del Cliente (CD9617)

A continuación se detalla la configuración de las Interfaces de la Red WAN y LAN respectivamente.

```
96717_PNP_105#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         10.147.8.14     YES NVRAM  up                    up
GigabitEthernet0/1         192.168.104.12  YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
96717_PNP_105#
```

Figura 26. *Configuración de Interfaz en el CD96717*
Fuente: *Realización Propia*

En la siguiente figura se nuestra la Tabla de Ruteo que se tiene en el CD96717 para lograr la conectividad a nivel de Capa 3 en el enlace de la Red hacia el segmento de los usuarios finales.

```
96717_PNP_105#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.104.14 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.104.14, GigabitEthernet0/1
      10.0.0.0/8 is variably subnetted, 20 subnets, 8 masks
B        10.10.0.0/20 [20/0] via 10.147.8.13, 1w6d
B        10.10.8.0/22 [20/0] via 10.147.8.13, 4w1d
```

Figura 27. *Configuración de Rutas en el CD96717*
Fuente: *Realización Propia*

3.3.2 Consolidación de Resultados

A continuación se va a detallar las pruebas de conectividad que se realizó para verificar el correcto funcionamiento de la red, para ello se realizaron las pruebas de PING y Telnet para verificar la conectividad entre un equipo y otro.

También se realizó un Tracer para verificar la correcta comunicación de los equipos.

3.3.2.1 Pruebas de Ping

En la Figura 28 se muestra la conectividad que hay entre el WASPENG2 y el enlace WAN del CD96717.

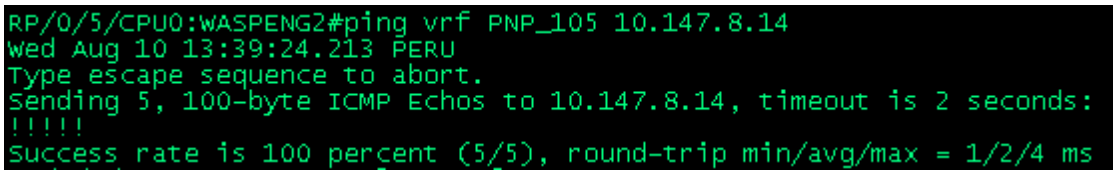


Figura 28. Conectividad mediante VRF entre el WASPENG2 y el enlace WAN del CD96717
Fuente: Realización Propia

En la Figura 29 se muestra la conectividad que hay desde el MOVPE1 hacia la línea de prueba, enviando un ping constante con una repetición de 1000.

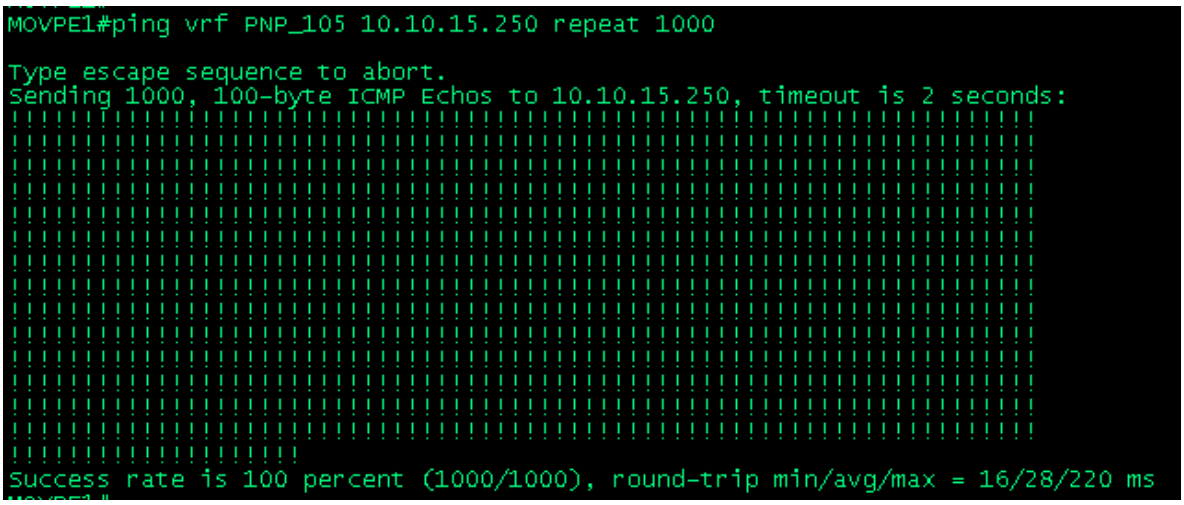


Figura 29. Conectividad mediante VRF entre el MOVPE1 y línea de prueba
Fuente: Realización Propia

En la Figura 30 se muestra la conectividad que hay desde el CD96717 hacia la línea de prueba, enviando un ping constante con una repetición de 1000.

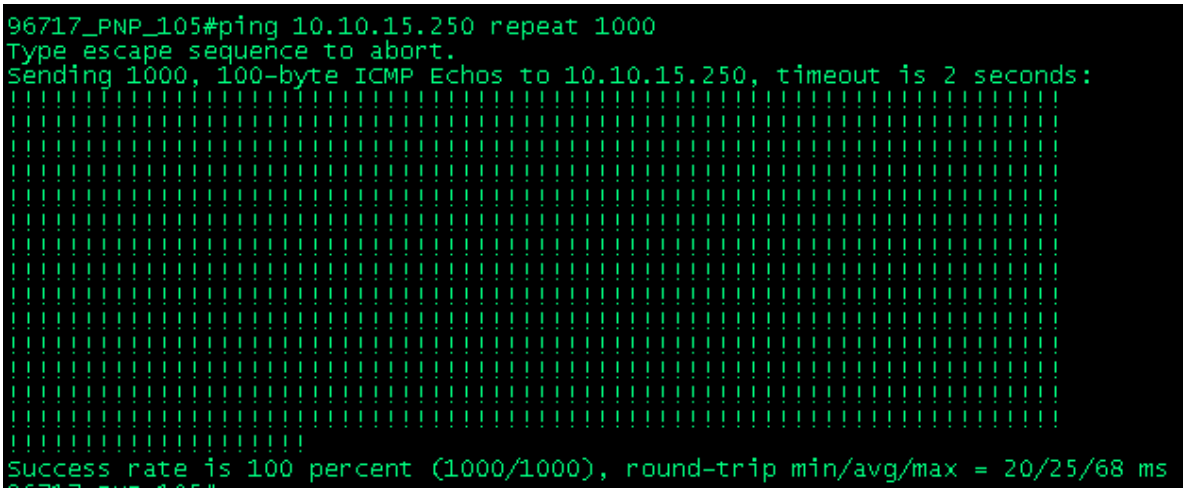


Figura 30. Conectividad entre el CD96717 y línea de prueba
Fuente: Realización Propia

3.3.2.2 Pruebas de Telnet

En la Figura 31 se muestra la prueba de Telnet que se realiza desde el WASPENG2 hacia el CD96717.

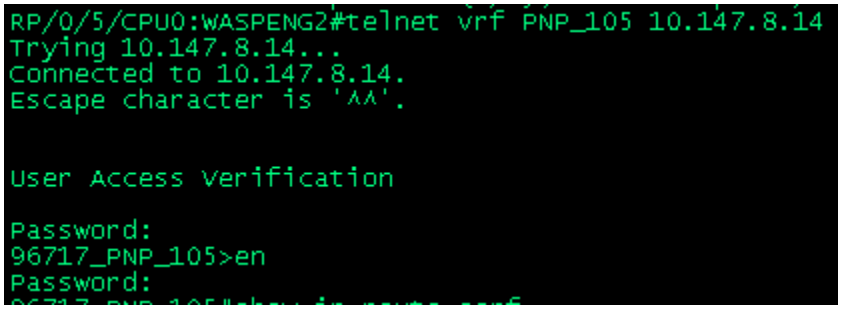


Figura 31. Telnet desde el WASPENG2 hacia el CD96717
Fuente: Realización Propia

3.3.2.3 Pruebas de Tracer

En la Figura 32 se muestra el encaminamiento que hay desde el MOVPE1 hacia la línea de prueba.

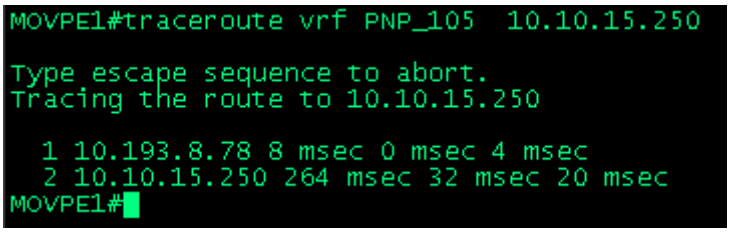


Figura 32. Verificación de los saltos desde el MOVPE1 hacia la línea de prueba
Fuente: Realización Propia

En la Figura 33 se muestra el encaminamiento que hay desde el CD96717 hacia la línea de prueba.

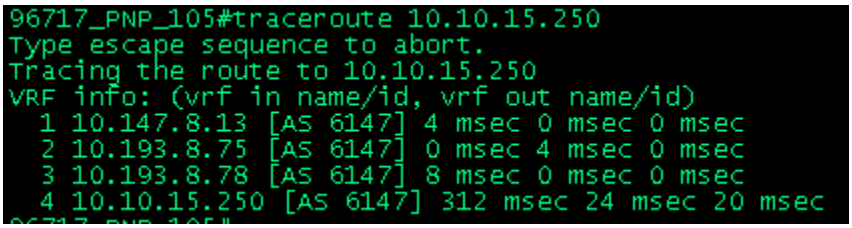


Figura 33. Verificación de los saltos desde el CD96717 hacia la línea de prueba
Fuente: Realización Propia

3.3.2.4 Envió y Recepción de Paquetes de la línea de Prueba

Se verifica el envió de los paquetes desde el P-GW de la línea de prueba en la Figura 34.

CRE TRC_USER:OP=MSISDN,MSISDN=51996666709',MT=GTPC-1&AAA-1&UP-1&DOWN-1&GY-1&PPP-1&L2TP-

Generation Time	Message Direction	Message Type	Message Length
2016-08-10 14:12:23...	PGW->SGW	Send Downlink Data	96
2016-08-10 14:12:23...	SGW->PGW	Receive Uplink Data	104
2016-08-10 14:12:23...	PGW->NET	Send Uplink Data	68
2016-08-10 14:12:23...	NET->PGW	Receive Downlink Data	108
2016-08-10 14:12:23...	PGW->SGW	Send Downlink Data	144
2016-08-10 14:12:23...	NET->PGW	Receive Downlink Data	83
2016-08-10 14:12:23...	PGW->SGW	Send Downlink Data	119
2016-08-10 14:12:23...	SGW->PGW	Receive Uplink Data	88
2016-08-10 14:12:23...	PGW->NET	Send Uplink Data	52
2016-08-10 14:12:23...	SGW->PGW	Receive Uplink Data	389
2016-08-10 14:12:23...	PGW->NET	Send Uplink Data	353
2016-08-10 14:12:23...	NET->PGW	Receive Downlink Data	52
2016-08-10 14:12:23...	PGW->SGW	Send Downlink Data	88
2016-08-10 14:12:23...	SGW->PGW	Receive Uplink Data	88
2016-08-10 14:12:23...	PGW->NET	Send Uplink Data	52
2016-08-10 14:12:28...	SGW->PGW	Receive Uplink Data	88
2016-08-10 14:12:28...	SGW->PGW	Receive Uplink Data	88
2016-08-10 14:12:28...	PGW->NET	Send Uplink Data	52
2016-08-10 14:12:28...	PGW->NET	Send Uplink Data	52
2016-08-10 14:12:30...	SGW->PGW	Receive Uplink Data	103
2016-08-10 14:12:30...	PGW->NET	Send Uplink Data	67
2016-08-10 14:12:30...	NET->PGW	Receive Downlink Data	118
2016-08-10 14:12:30...	PGW->SGW	Send Downlink Data	154
2016-08-10 14:12:30...	SGW->PGW	Receive Uplink Data	96
2016-08-10 14:12:30...	PGW->NET	Send Uplink Data	60
2016-08-10 14:12:31...	SGW->PGW	Receive Uplink Data	96
2016-08-10 14:12:31...	PGW->NET	Send Uplink Data	60
2016-08-10 14:12:33	SGW->PGW	Receive Uplink Data	96

Figura 34. *Verificación de los paquetes desde el P-GW de la línea de prueba*
Fuente: *Realización Propia*

CONCLUSIONES

- El diseño de la red y la topología ha sido realizada para que los servicios móviles de la Policía Nacional Del Perú puedan migrar y disfrutar de una red de altas prestaciones.

- Con la implementación de la VPN se logra permitir que los datos de la Policía Nacional Del Perú sean transmitidos a través de la red pública desde cada uno de los usuarios finales, proporcionando mayor rapidez, seguridad y confiabilidad.

- Al implementar servicio VPN en MPLS no es necesario contar con direccionamiento global o público para la información de la conexión punto a punto ya que este tipo de tecnologías, crea la VPN en base a instancias de enrutamiento y envío (VRF), por lo cual un cliente puede conservar su esquema de direccionamiento privado sin necesidad de realizar traducción de direcciones privadas a públicas.

- En cuanto a la Red Móvil se verifica una mayor rapidez en el enlace de Transmisión de Datos ya que esta tecnología es más avanzada que la empleada anteriormente por parte de la Policía Nacional del Perú.

RECOMENDACIONES

- Para el correcto funcionamiento de la Red se debe verificar que todos los elementos comprendidos en ella se encuentren en óptimas condiciones para la Transmisión de Datos.

- Se recomienda a la Policía Nacional Del Perú que el futuro Administrador de Red de la VPN, deber tener un plan de contingencia, que permita dar una breve solución a los diversos problemas que se puedan presentar en esta, en el caso de producirse desastres físicos o eléctricos.

- Para el servicio de la VPN MPLS se debe verificar en el enlace que las configuraciones estén correctamente provisionadas para no tener una mala comunicación por un problema lógico del enlace.

- Por último se recomienda tener en cuenta por parte de la Red Móvil el nivel de cobertura que se tiene en Lima para un correcto funcionamiento del servicio, ya que si un usuario se encuentra en un lugar fuera de cobertura de señal 4G la calidad del servicio se va a reducir considerablemente.

BIBLIOGRAFIA

1. Libro CCNA (Cisco Certified Network Associate)
2. Libro CCNP of route (Cisco Certified Network Professional)
3. CCNP a Fondo - Guía de Estudio (Cisco Certified Network Profesional)

Enlaces Webs:

- http://ohmyphone.orange.es/universo-orange/historia-de-la-red-movil-como-hemos-llegado-al-4g.html
- http://www.cusiglas.com/telecomunicaciones/ms/
- http://xius.com/es/4glte_network.php
- http://www.omicrono.com/2013/01/todo-sobre-el-4g-lte-que-es-para-que-sirve-y-cuando-llegara-a-espana/
- http://es.slideshare.net/fernandomendioroz/telefona-mvil-celular-0-a-4g-lteadvancedhttp://www.telecomhall.com/es/que-es-csfb-y-srvcc-en-lte.aspx
- http://www.telecomhall.com/es/que-es-csfb-y-srvcc-en-lte.aspx
- http://es.slideshare.net/ivandarklife/estudio-y-diseno-de-redes-uatf
- https://curiosoando.com/que-es-la-red-4g
- http://www.slideshare.net/RohdeSchwarzNA/lte-eutran-rsanov2012day1
- http://inalambricas-lte4g.blogspot.pe/2014/08/arquitectura-lte-la-arquitectura-lte.html
- https://www.eeweb.com/electronics-forum/ofdm
- http://gsmcommunications.blogspot.pe/2011/01/using-sc-fdma-in-lte.html
- http://mplsinfo.org/
- http://docplayer.es/1129857-Diseno-de-una-solucion-de-ip-trunking-sobre-red-vpn-entre-multiples-sedes-de-un-contact-centre.html
- http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm

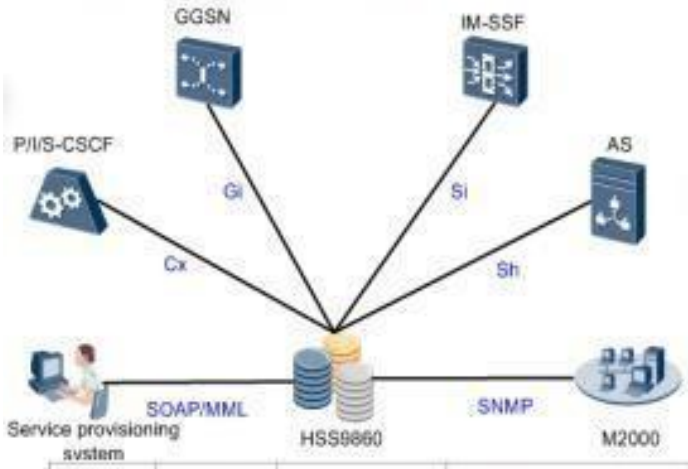
- http://www.tatateleservices.com/tata-enterprise-mpls-vpn-services.aspx?print=yes
- http://www.dummies.com/how-to/content/border-gateway-protocol-bgp-routing-protocol-overv.html
- https://blog.initialdraft.com/archives/2558/

ANEXOS

Anexo 1:

- **HSS9860**

Interfaces between the HSS9860 and other NEs when the HSS9860 serves as the IMS-HSS in IMS networks



Cx	• I-CSCF • S-CSCF	• Diameter/SCTP • Diameter/TCP	• Used by the HSS to send S-CSCF's capacity set at the I-CSCF's request for the I-CSCF to select an S-CSCF to serve the calling subscriber. • Used by the HSS to send backup data at the S-CSCF's request for the S-CSCF to implement redundancy networking.	• 3GPP TS 29.228 • 3GPP TS 29.229
Gi	GGSN	RADIUS/UDP	Used by the HSS to send Early IMS authentication data at the GGSN's request.	3GPP TS 33.978
Sh	AS	Diameter	Used by the HSS to send subscription data at AS' request.	• 3GPP TS 29.328 • 3GPP TS 29.329
Si	IM-SSF	MAP/SIGTRAN	Used by the HSS to send subscribers' CAMEL subscription information (CSI) at IM-SSF's request.	3GPP TS 23.278

Anexo 2:

- **USN9810**

PRODUCTS WE COVER

Evolved Packet Core

Huawei USN9810 / UGW9811
(8/16/2010)
| Client Access |

CURRENT ANALYSIS PRODUCT ASSESSMENTS

Product assessment reports provide a timely and in-depth evaluation on how leading products and services in a market measure up to their competition. Updated regularly by our industry-leading analysts, product assessment reports deliver an objective and un-biased look at a product's strengths and weaknesses, ratings on how well the product meets specific customer buying criteria, and relevant product metrics. Compare selected products with side-by-side listings of product metrics and other factors, with a focus on actionable intelligence. **Click here** to find out how you can get access to **Telecom Equipment Buyer**.

USN9810

Anexo 3:

- **UGW9811**

Este Gateway unificado de paquetes para redes móviles de conmutación de paquetes (PS) es un elemento central de los servicios de PS en redes GSM-R. Combina las funciones de múltiples Gateway en una sola plataforma y aun así puede ser administrado convenientemente como un Gateway único.

Para las redes GSM-R en particular, funciona como nodo de soporte (GGSN) del servicio general de radio por paquetes (GPRS) de Gateway. Asimismo, se puede utilizar como un Gateway para la evolución hacia los servicios de banda ancha eLTE.

UGW9811

Anexo 4:

- **CISCO ROUTER 2900**

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings The Integrated Services Routers Generation 2 platforms are future-enabled with multi-core CPUs, support for high capacity DSPs (Digital Signal Processors) for future enhanced video capabilities, high powered service modules with improved availability, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS® Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation which can quickly adapt to evolving network requirements. Overall, the Cisco 2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market leading security, unified communications, wireless, and application services.

Figure 1. Cisco 2900 Series Integrated Services Routers