PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
ESCUELA DE POSGRADO

Diseño de una Red de Proveedor de Servicios de Telecomunicaciones basado en Arquitectura SR-MPLS

TESIS PARA OPTAR EL GRADO DE MAGÍSTER EN INGENIERÍA DE LAS TELECOMUNICACIONES

AUTOR
Ing. Luis Henry Paredes Malpartida

ASESOR
Dr. Merino Acuña, Henry William

Marzo, 2021

RESUMEN

La presente tesis describe y explica mediante simulaciones el funcionamiento de las arquitecturas Seamless-MPLS y Segment Routing-MPLS (SR-MPLS), así como los principios de diseño para la implementación en una red de transporte de un proveedor de servicios de telecomunicaciones, incluyendo las pautas de migración hacia una arquitectura basada en Segment Routing Best Effort (SR-BE) y Segment Routing Traffic Engineering (SR-TE). Arquitecturas las cuales son requeridas para una transición hacia SDN, base para la implementación de 5G. El documento pretende otorgar una guía descriptiva para el desarrollo, configuración e implementación de la solución.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE SIGLAS Y ACRÓNIMOS

- **ADJ-SID** Adjacency Segment ID
- **ARP** Address Resolution Protocol
- **BGP** Border Gateway Protocol
- **DSCP** Differentiated Services Code Point
- **DWDM** Dense Wavelength Division Multiplexing
- **ECMP** Equal Cost Multipath
- **EGP** Exterior Gateway Protocol
- **FIB** Forwarding Information Base
- **GSM** Global System for Mobile
- **GUI** Graphical User Interface
- **ICMP** Internet Control Message Protocol
- **IETF** Internet Engineering Task Force
- **IGP** Interior Gateway Protocol
- **IP** Internet Protocol
- **ISIS** Intermediate System-to-Intermediate System
- **LDP** Label Distribution Protocol
- **LFIB** Label Forwarding Information Base
- **LIB** Label Information Base
- **LSA** Link State Advertisement
- **LSP** Label Switched Path
- **LSR** Label Switching Router
- **LTE** Long Term Evolution
- **MPLS** Multiprotocol Label Switching
- **MW** Microwave
- **NGN** New Generation Netwok
- **NODE-SID** Node Segment ID
- **OSPF** Open Shortest Path First
- **PCEP** Path Computation Element Protocol
- **PHP** Penultimate Hop Popping
- **QoE** Quality of Experience
- **QoS** Quality of Service
- **RAN** Radio Access Network
- **RTT** Round-Trip Time
- **SDH** Syncronous Digital Hierarchy
- **SDN** Software Defined Networking
- **SRGB** Segment Routing Global Block
- **SID** Segment Identifier
- **SLA** Service Level Agreement

- **SPF** Shortest Path First
- **SR** Segment Routing
- **TCP** Transmission Control Protocol
- **UDP** User Datagram Protocol
- **UMTS** Universal Mobile Telecommunications System
- **VLAN** Virtual Local Area Network
- **VPN** Virtual Private Network

CAPÍTULO I
INTRODUCCIÓN

En redes de proveedores de servicios móviles, la implementación de una red IP NGN considera la agregación a nivel de Ethernet de la red de acceso RAN (GSM, UMTS, LTE y 5G), servicios empresariales y terceros, servicios de valor agregado, el Core de Paquetes y el Core de Voz. La implementación de una red de altas prestaciones y capacidad, que ofrezca tiempos de respuesta óptimos y rápida convergencia ante eventos de fallas, es esencial para un proveedor de servicios de telecomunicaciones. En la actualidad, los indicadores de aceptación de usuario (KQI – *Key Quality Indicator*) respecto a un servicio están más relacionados a lo que se denomina *Calidad de la Experiencia* (QoE: Quality of Experience, por sus siglas en inglés) y son mucho más importantes ya que permiten observar el comportamiento de la red y su influencia sobre los servicios que por tal cursan.

El diseño de una red del tipo IP/MPLS no está guiado estrictamente por estándares o protocolos de diseño. Necesita más de conocimiento y experiencia en saber qué protocolos y parámetros se necesitan configurar de acuerdo a los requerimientos del proveedor de servicio. Por tanto, mediante la presente tesis, se sustentan los principios de funcionamiento de la arquitectura MPLS-SR. Tener claros los conocimientos de los

protocolos involucrados permitirán al Ingeniero elaborar un diseño acorde a lo que requiere el proveedor, cumpliendo los siguientes principios básicos: baja latencia , escalabilidad y alta disponibilidad.

Las redes de transporte de datos tienen componentes que pueden diferenciarse según la capa en que trabajan, por ejemplo, utilizando el modelo TCP/IP se puede separar en: elementos en la capa física (DWDM, MW, SDH, etc.) los cuales se encargan de la transmisión física de la señal por distintos medios según sea la naturaleza del enlace, y elementos en la capa de Internet (routers, switches) que se encargan de encaminar un paquete por el camino más óptimo. En principio, se consideraba la red de transporte con únicamente protocolos de Capa 2, actualmente, por las claras ventajas que MPLS ofrece, se trata de acercar MPLS lo más cercano al nodo. Es así que la arquitectura de Seamless-MPLS permite llegar a los elementos de acceso, segmentando el protocolo de IGP pero permitiendo establecer un LSP extremo a extremo. De esta manera, se pueden instalar equipos con menores prestaciones en cada radio-base o estación final.

Sin embargo, esta arquitectura tiene algunos puntos en contra cuando se piensa en desplegar 5G. No es una arquitectura amigable para una transición hacia SDN, el balanceo de carga del tipo ECMP debe ser manual, utilizando otros protocolos auxiliares; y finalmente, el aprovisionamiento requiere de la configuración de diversos puntos de la red.

La red de transporte debe ser **“simple”**, esto es, cumplir con las siguientes características: rápido aprovisionamiento, automatización, alta disponibilidad, evitar la subutilización de enlaces y facilidad de análisis ante fallas. Es por eso que Segment Routing MPLS se presenta como una arquitectura que soluciona las falencias presentadas en Seamless-MPLS.

Otras investigaciones relacionadas hacen referencia exclusivamente a la arquitectura Segment Routing [1] [2], su interacción con orquestadores de red [3], elementos para cómputo de caminos en la red [4], automatización e implementación de escenarios de Ingeniería de Tráfico [5].

El presente estudio complementa otras investigaciones en cuanto a una explicación comparativa con la arquitectura tradicional (actualmente utilizada por diversos operadores en el país) y la propuesta, así como detallar los lineamientos y recomendaciones para un proveedor de servicios móviles, distribuido en cinco capítulos, se presenta el desarrollo teórico de los protocolos más importantes, los principios de diseño, configuraciones recomendadas, simulaciones y, por último, se brindan recomendaciones orientadas a las proyecciones de crecimiento.

Esta red deberá tener la capacidad de brindar diversos servicios sobre una misma infraestructura, utilizando al máximo los recursos de ancho de banda.

1.1. Objetivos

1.1.1. Objetivo Principal

- Análisis y descripción del proceso de implementación y migración de una arquitectura Seamless-MPLS hacia Segment-Routing MPLS.

1.1.2. Objetivos Específicos

- Identificar escenario de simulación en base a una topología típica de una red de un proveedor de servicios de Internet.
- Verificar el funcionamiento de los protocolos involucrados en el estudio, a través de simulaciones por software.
- Realizar simulaciones en software sobre el funcionamiento de una red basada en Segment Routing.
- Proponer lineamientos y recomendaciones para la migración de arquitectura Seamless-MPLS a SR aplicable a un proveedor de servicios de internet

CAPÍTULO II
MARCO TEÓRICO

2.1. Protocolos de enrutamiento dinámico

Todos los protocolos de enrutamiento dinámico están construidos sobre un algoritmo. El algoritmo especifica el procedimiento paso a paso para resolver un problema. Un algoritmo de enrutamiento debe especificar como mínimo: el procedimiento de cómo compartir información de rutas alcanzables a otros dispositivos, el procedimiento de qué hacer con la información que proviene de otros routers, el procedimiento para determinar la mejor ruta óptima y el procedimiento para reaccionar frente a cambios de topología d de la red. [6]

Como se puede observar en la figura 2.1, el router puede seleccionar entre diversas opciones el camino más apropiado a través de la red, acorde a la dirección destino (inscrita en el encabezado del paquete), y lo envía al siguiente salto, el cual puede ser otro router o, finalmente, el dispositivo destino. El router construye una tabla de enrutamiento que le permite listar todos los segmentos destino. Cada entrada de la tabla de enrutamiento indica el segmento destino, protocolo, distancia administrativa del

protocolo, costo hasta el destino desde el punto de vista del router, la IP del siguiente salto y la interfaz de salida.

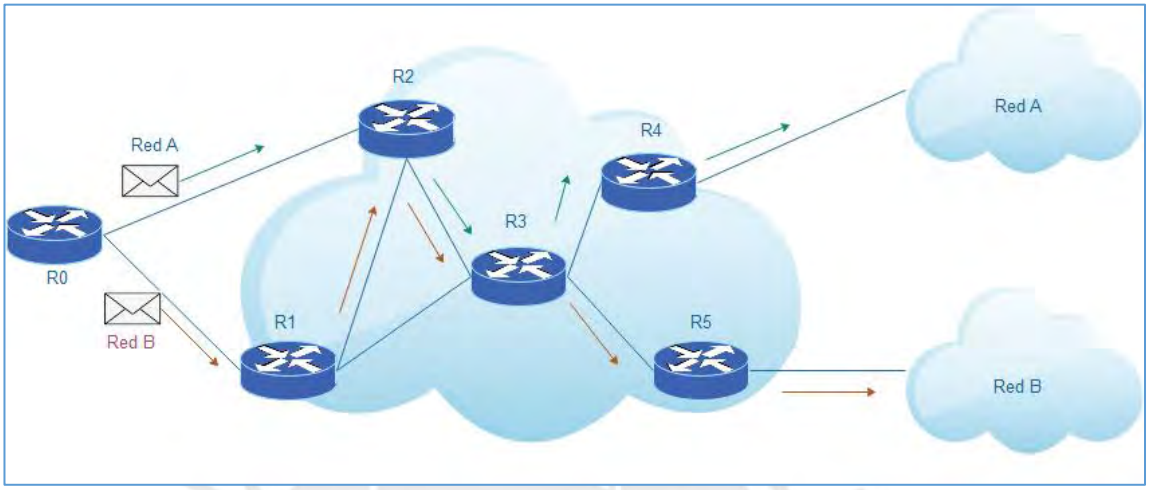

Fig. 2.1 Enrutamiento de paquetes

Los protocolos de enrutamiento pueden clasificarse de acuerdo al área de trabajo, los cuales pueden ser Internos (IGP) o Externos (EGP), desde el punto de vista del Sistema Autónomo (AS). Se define el AS como un grupo de routers que se encuentran bajo una administración en común. Dentro de un AS, se pueden utilizar múltiples protocolos de enrutamiento [6].

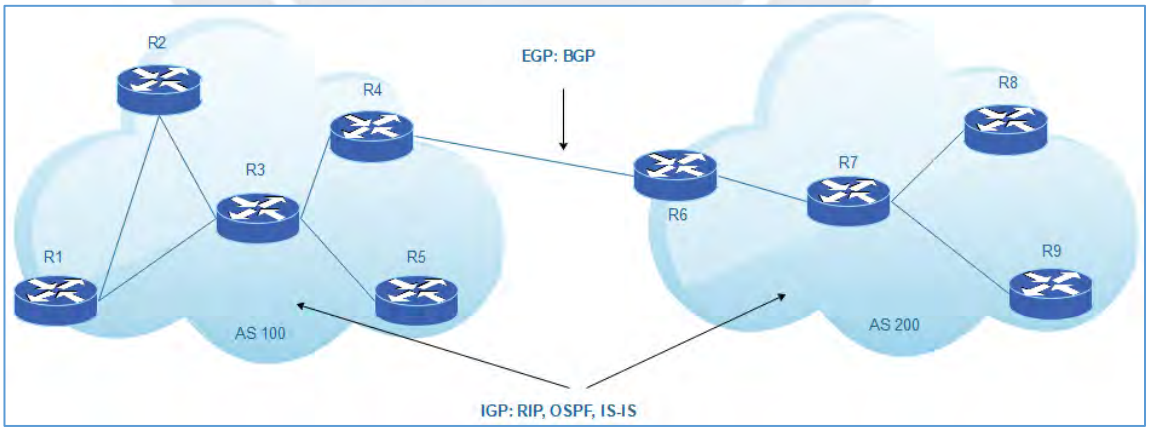

Fig. 2.2 Clasificación por área de trabajo: IGP y EGP

Otra forma de clasificación de los protocolos de enrutamiento como se muestra en la tabla 2.1. es de acuerdo al algoritmo de ruteo, los cuales pueden ser del tipo Vector-Distancia y de Estado de Enlace. Se define un protocolo vector distancia el cual considera como métrica/costo únicamente el número de saltos intermedios para llegar al destino. Los protocolos del tipo de Estado Enlace consideran diferentes parámetros para el cálculo de la métrica (ancho de banda de la interfaz, carga, latencia, confiabilidad.

Tabla 2.1 Vector-distancia y Estado de enlace.

Algoritmo de Vector Distancia	Algoritmo de estado enlace
RIP	OSPF
IGRP	IS-IS

El protocolo de enrutamiento RIP es un protocolo obsoleto, únicamente utilizado en redes muy pequeñas (con menos de 15 saltos intermedios). En redes de mayor envergadura, es recomendable el uso de OSPF o IS-IS, los cuales pueden proveer una mejor performance por su rápida convergencia y soporte de mejores características de red.

Adicionalmente, en la actualidad, BGP es el único protocolo de enrutamiento que permite el intercambio de información entre diferentes sistemas autónomos. BGP se caracteriza más por su estabilidad (es basado en TCP) que por su tiempo de convergencia ante fallas en la red.

2.2. Protocolo OSPF

2.2.1 Descripción de protocolo

El protocolo Open Shortest Path First (OSPF) se define por el IETF en la RFC 2328 como un Protocolo de gateway interior que se usa para distribuir información de enrutamiento dentro de un sistema autónomo. OSPF es un protocolo del tipo de “estado-enlace”. El estado del enlace describe detalladamente las redes que participan en el

proceso OSPF, indicando el origen de la red, métricas entre otros parámetros que permiten identificar cada enlace. OSPF utiliza el concepto de áreas para establecer jerarquías y segmentación de la red que mejoran tiempos de convergencia. Los equipos que forman parte del proceso OSPF, conocen la información de toda la topología OSPF asociada al área la cual pertenecen, y utilizan el algoritmo de Dijikstra para computar un camino sin bucles, y menor costo para cada router en el área. [7]

2.2.2 Funcionamiento de protocolo OSPF

Los anuncios de estado de enlace, o LSAs, son mensajes que utilizan los routers para distribuir información de las redes que se involucran en el proceso OSPF. Cada router que pertenece a un proceso OSPF, genera LSAs de diversos tipos, cada uno depende del origen del segmento de red. Se pueden clasificar en seis tipos [7], los cuales se detallan en la Tabla 2.2.

Tabla 2.2 Tipos de LSAs en OSPF

Tipo LSA	Descripción del anuncio LSA
1	Son generados por cada router para cada área a la que pertenece y describen las redes directamente conectadas al router, sólo son distribuidos dentro de un área determinada.
2	Son generados por routers DR/BDR. Describen el conjunto de routers conectados a una red determinada. Son distribuidos dentro del área que contiene la red.
3 ó 4	Son generados por los routers de borde de área (ABR). Describen los enlaces que provienen de otras áreas. El tipo 4 describe las rutas a ASBR.
5	Originados por ASBR. Describen rutas hacia los destinos externos al AS. Son distribuidos en su totalidad excepto bajo configuraciones específicas.
10	Los LSAs tipo 10 (Opaque) tienen significado dentro del área a donde pertenecen. Se utiliza para extender capacidades de OSPF (como Segment Routing o Ingeniería de Tráfico)

2.3. BGP

2.3.1. Descripción de Protocolo

Border Gateway Protocol (BGP) es un protocolo de enrutamiento dinámico usado entre sistemas autónomos . BGP es ampliamente usado por los proveedores de servicio de internet. Actualmente es utilizada la versión BGP-4, la cual posee las siguientes características [3]:

- Al contrario de los protocolos IGP, como OSPF o IS-IS, BGP es del tipo EGP, el cual se enfoca en controlar y seleccionar las mejores rutas entre ASs, mas no en el descubrimiento o convergencia de la red.
- BGP utiliza TCP como protocolo de capa de transporte, lo que mejora la confiabilidad de BGP.
- Vecinos BGP deben estar lógicamente conectados a través de TCP, utilizando el puerto destino 179.
- BGP soporta CIDR.
- Cuando existe un cambio en la red o actualización de la ruta, BGP transmite únicamente las rutas actualizadas, lo cual reduce el consumo de ancho de banda durante la distribución de rutas, por tanto, BGP es aplicable al intercambio de rutas de Internet, donde un gran número de rutas son transmitidas.

2.3.2. Modos de Operación de BGP

En la Figura 2.3, se presentan las dos modalidades de trabajo del protocolo BGP de acuerdo a la función en el Sistema Autónomo: iBGP cuando es utilizado dentro del AS, y eBGP cuando se utiliza entre ASs.

Fig. 2.3 Despliegue de IBGP vs EBGP

2.3.3. Atributos BGP

Los atributos BGP son un conjunto de parámetros que caracterizan una ruta BGP. Mediante estos atributos, se puede aplicar filtros y selección de rutas. Estos atributos pueden clasificarse de la siguiente manera [8]:

- Well-known mandatory: Este tipo de atributos pueden ser identificados por todos los routers, y deben ser incluidos en los mensajes update.
- Well-known discretionary: este tipo de atributos pueden ser identificados por todos los routers, pero puede ser opcionalmente incluidos en los mensajes update.
- Optional transitive: Estos mensajes se intercambian entre sistemas autónomos. Un router BGP podría o no reconocer este atributo, pero lo acepta y lo reenvía hacia otros vecinos.
- Optional non-transitive: si el router BGP no reconoce este tipo de atributo, no lo advierte hacia otros vecinos.

Los atributos más conocidos son:

- AS_Path: este atributo almacena ordenadamente todos los ASs por los cuales ha pasado determinada ruta.
- MED: este atributo es transmitido únicamente entre 2 ASs conectados. El AS que recibe una ruta con MED no lo advierte a un tercero. Es utilizado para influenciar el tráfico de entrada desde un AS vecino.
- Local_Pref: este atributo indica la prioridad que posee una ruta BGP, y está disponible dentro de una red iBGP, no siendo anunciada a otros ASs. Es utilizado para influenciar el tráfico de salida de un AS.

También existen atributos privados (por ejemplo, pref_val, weight) que son definidos por cada proveedor.

2.3.4. Route-Reflector

BGP utiliza TCP para el establecimiento de sesiones. En una red iBGP, requiere que todos los elementos establezcan sesiones entre todos los elementos. De existir un número n de routers, son necesarias n*(n-1) /2 sesiones establecidas. Este escenario hace que la escalabilidad de la red se vea afectada, pues cada elemento nuevo que ingrese a la red, necesitará obligatoriamente establecer sesiones con cada uno de los elementos ya desplegados como se muestra en la Figura 2.4, donde en una red con cuatro elementos, se tiene 6 sesiones iBGP establecidas.

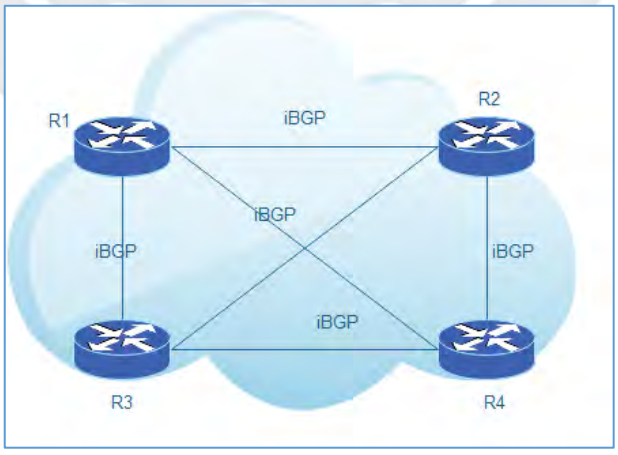

Fig. 2.4 Despliegue de iBGP full-mesh

La utilización de la técnica de Route-Reflectors puede resolver el inconveniente, tal como se puede observar en la Figura 2.5. Dentro de un AS, un router funciona como Route-Reflector [9] (RR) y otro funciona como cliente. Los clientes establecen conexiones iBGP con los RRs y el RR refleja las rutas hacia los clientes, por lo que no es necesario establecer conexiones iBGP entre clientes. También se permite las sesiones contra elementos no-clientes.

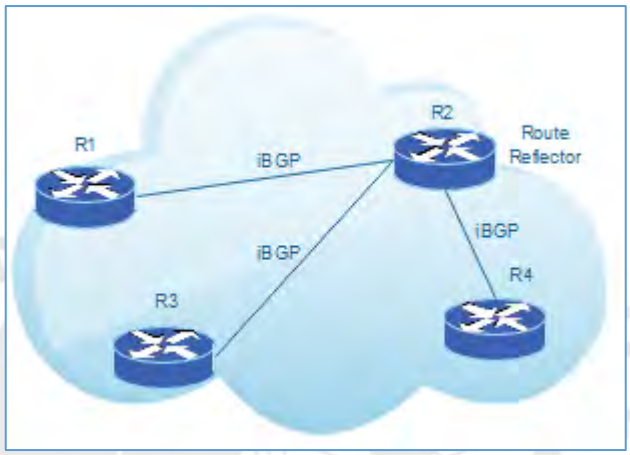

Fig. 2.5 Despliegue de iBGP con Route-Reflector

2.4. MPLS

2.4.1. Descripción

MPLS es un estándar IP de conmutación de paquetes del IETF [10], que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (Forward Equivalence Class), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio. Cuando MPLS está implementado como una solución IP pura o de nivel 3, que es la más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete. Los campos de la cabecera MPLS de 4 bytes, ilustrados en la Figura 2.6, son los siguientes:

- Label (20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.
- CoS (3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.
- Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que, al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa. [10] [11]

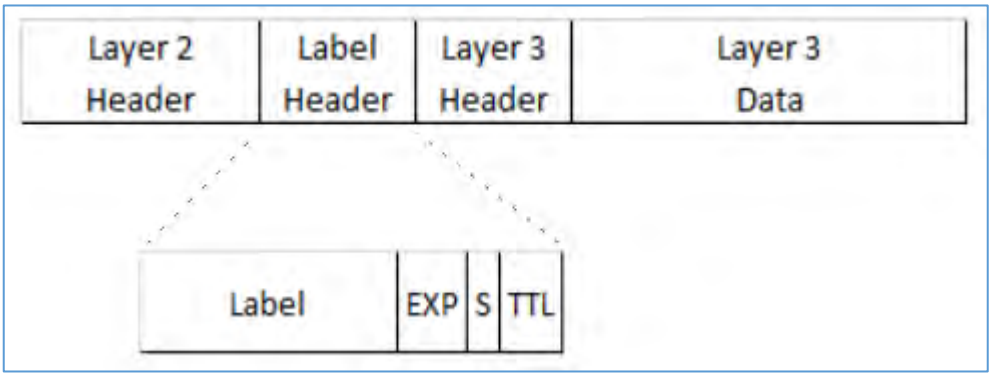

Fig. 2.6 Encabezado de paquete MPLS

2.4.2 Elementos de una red MPLS

En MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol – Traffic Engineering) o CR-LDP (Constraint-based Routing – Label Distribution Protocol); siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos. [10] [11]

Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers), tal y como se muestra en el ejemplo de la Figura 2.7. Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los "routers" IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP

destinatarias. Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento.

Los LERs están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un "router" IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias. [11]

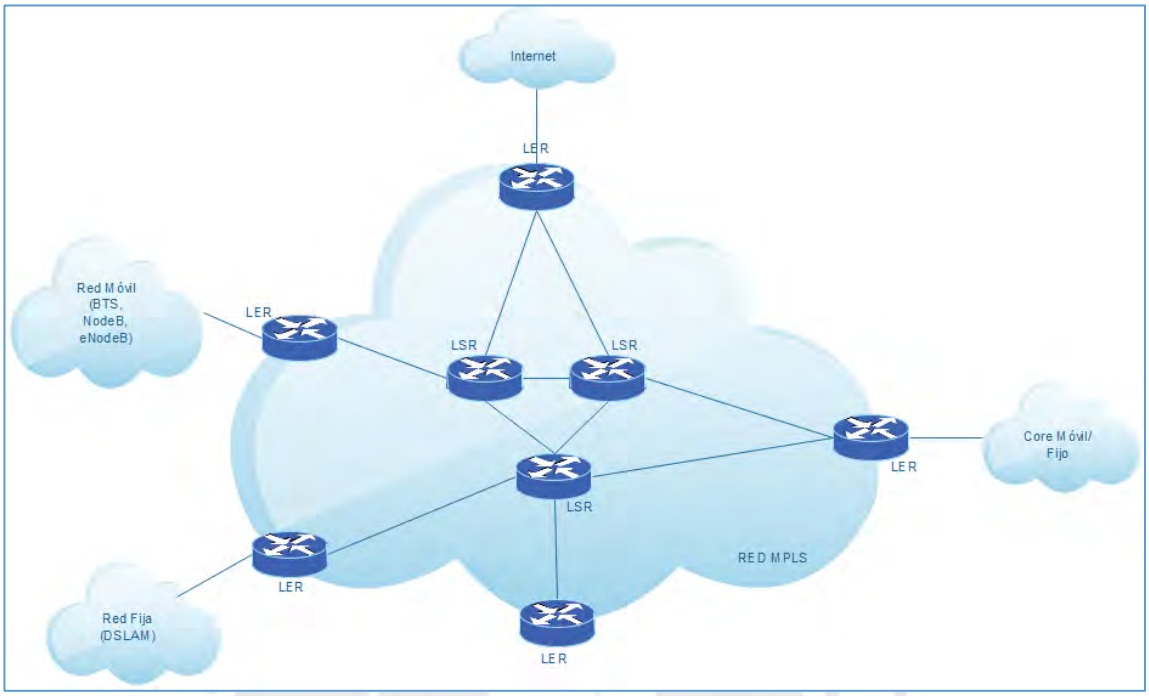

Fig. 2.7 Arquitectura MPLS

2.4.3. Funcionamiento de una red MPLS

Cada LSR (P) tiene una tabla FEC que contiene la interfaz de salida y la etiqueta de salida con la cual se tomarán las decisiones para el envío de los paquetes por el camino establecido. La conmutación de paquetes se basa en la lectura de las etiquetas. Dependiendo de la configuración de los elementos, cada elemento de red puede asignar una etiqueta por prefijo existente en la red. Esto es, cada elemento mantiene una tabla de FEC/Etiqueta independiente de los otros elementos. Para que se establezca la comunicación entre dos LER a través de una red MPLS, es necesario que los elementos puedan interpretar las etiquetas ya sea mediante el intercambio de etiquetas o por medio de instrucciones o segmentos. [11] [12]

2.4.4. Protocolo LDP

LDP se basa en la RFC 5036. Todo LSR que soporte el protocolo LDP debe mantener sesiones LDP con otros LSR o LER que hagan lo mismo. Durante una sesión LDP se

generan diversos tipos de mensajes con la finalidad de dar a conocer a otros enrutadores que el enrutador está vivo, mantener vivo dicho conocimiento, anunciar prefijos nuevos y notificar eliminación de otros, solicitar etiquetas, entre otras funciones. En resumen, el protocolo LDP mantiene el dominio MPLS en coherencia, dado que una de sus funciones principales es la de ser el encargado de realizar el intercambio de etiquetas entre todos los elementos de red. [12]

LDP utiliza el protocolo TCP y requiere establecer una sesión con el vecino (o la dirección destino configurada manualmente). Si se da el caso, se establece la conexión y se inicia una sesión LDP entre los LSR interesados. [12]

2.4.5. MP-BGP y BGP/MPLS

La versión convencional de BGP-4 administra solo rutas del tipo IPv4 Unicast, y el intercambio de información de paquetes IPv6 y multicast es limitado. Para soportar múltiples protocolos de la capa de red, la IETF extendió las capacidades de BGP-4 a Multiprotol Extensions para BGP-4 (MP-BGP). Esto conlleva a la extensión de los siguientes atributos opcionales no transitivos: MP_REACH_NLRI y MP_UNREACH_NLRI. [13] [14]

2.5. Seamless MPLS

2.5.1. Descripción

Seamless MPLS es una técnica que extiende las características de MPLS a la red de acceso, estableciendo un LSP extremo a extremo, a través de la red de acceso, agregación y core. MPLS es una tecnología madura y ampliamente desplegada por los proveedores de servicio, e integra múltiples redes basadas en Ethernet a nivel de la agregación y core. La evolución de las redes móviles y las ventajas de MPLS sobre otros protocolos (MPLS, protocolos de capa 2), exigen que MPLS sea extendido extremo a extremo, bajo una arquitectura de red más plana, por lo que Seamless MPLS utiliza los protocolos existentes (BGP, IGP, MPLS) permitiendo que el tráfico extremo a extremo sea encapsulado y enviado utilizando MPLS [15].

2.5.2. Beneficios

Seamless MPLS ofrece los siguientes beneficios [15]

- Integra las capas de acceso, agregación y Core en una única red MPLS, encapsulando todos los servicios utilizando MPLS, y transmita estos servicios a lo largo de un LSP extremo a extremo. Seamless MPLS simplifica el aprovisionamiento, operación y mantenimiento de la red.
- Provee facilidad de despliegue y gran escalabilidad. En una red seamless MPLS, un LSP puede ser establecido entre 2 nodos extremos para desplegar un servicio, sin necesidad de configuración en la capa de Core.

2.6. Segment Routing

2.6.1. Descripción

Segment Routing (SR) es un protocolo diseñado para la conmutación de paquetes utilizando el modelo de ruteo basado en origen. SR-MPLS es implementado utilizando el plano de datos de MPLS, donde SR divide un camino a lo largo de una red en diversos segmentos y asigna identificadores (SID) a cada segmento y elemento de red. Los segmentos y los nodos son posteriormente ordenados para formar un conjunto de instrucciones que definirán el camino a lo largo de la red MPLS Segment Routing (SR) es un protocolo diseñado para la conmutación de paquetes utilizando el modelo de ruteo basado en origen. SR-MPLS es implementado utilizando el plano de datos de MPLS, donde SR divide un camino a lo largo de una red en diversos segmentos y asigna identificadores (SID) a cada segmento y elemento de red. Los segmentos y los nodos son posteriormente ordenados en listas de segmentos para formar un conjunto de instrucciones que definirán el camino a lo largo de la red MPLS. Esta solución permite la habilitación de servicios con mayor control, por ejemplo, permitiendo definir parámetros de calidad para un flujo específico (bajo jitter, baja latencia, alto ancho de banda, etc.) o realizando balanceo de tráfico automáticamente entre dos caminos disponibles.

SR tiene las siguientes características:

- Utiliza extensiones de protocolos existentes (IGP) para facilitar la evolución de la red.
- Facilita el proceso de evolución de la red hacia SDN.
- Para MPLS-TE, se requiere que todos los elementos de tránsito manejen la información del camino establecido. Utilizando SR-TE, no se requiere dicha información en todos los elementos de red. Por tanto, la cantidad de etiquetas disminuye considerablemente al depender de la cantidad de elementos en la red y no de la cantidad de túneles o servicios que cursan por la red. [16]

2.6.2. Definición y Tipos de Segmentos

Como se detalló anteriormente, un segmento es una instrucción, y se puede clasificar en tres tipos:

- Segmento de Prefijo, es manualmente configurado, identifica el prefijo de una dirección destino (16001, 16002, 16003)
- Segmento de Adyacencia, es asignado dinámicamente o puede ser manualmente configurado. Identifica el enlace por donde transita un paquete y es de significado local. Los valores asignados están fuera del bloque SRGB. (1001, 1002, 1003)
- Segmento del Nodo, es manualmente configurado, identifica un elemento de red específico. (101, 102, 103). Luego de que se distribuya en la red el SID, todos los elementos conocerán los valores de SID de un determinado elemento de red, posteriormente se ejecuta el algoritmo SPF para calcular la mejor ruta hacia el destino. Si existen dos rutas con costos iguales, se realiza balanceo de carga, caso contrario, se establece un camino de redundancia.

SR utiliza la estructura de conmutación de paquetes como lo hace MPLS. El elemento origen crea el listado de etiquetas, y la etiqueta externa se eliminará conforme transita por la red. [16]

Esta solución permite la habilitación de servicios con mayor control, por ejemplo, permitiendo definir parámetros de calidad para un flujo específico (bajo jitter, baja

latencia, alto ancho de banda, etc.) o realizando balanceo de tráfico automáticamente entre dos caminos disponibles. [16]

En la Figura 2.8 se muestran los tipos de segmentos de acuerdo a lo descrito anteriormente:

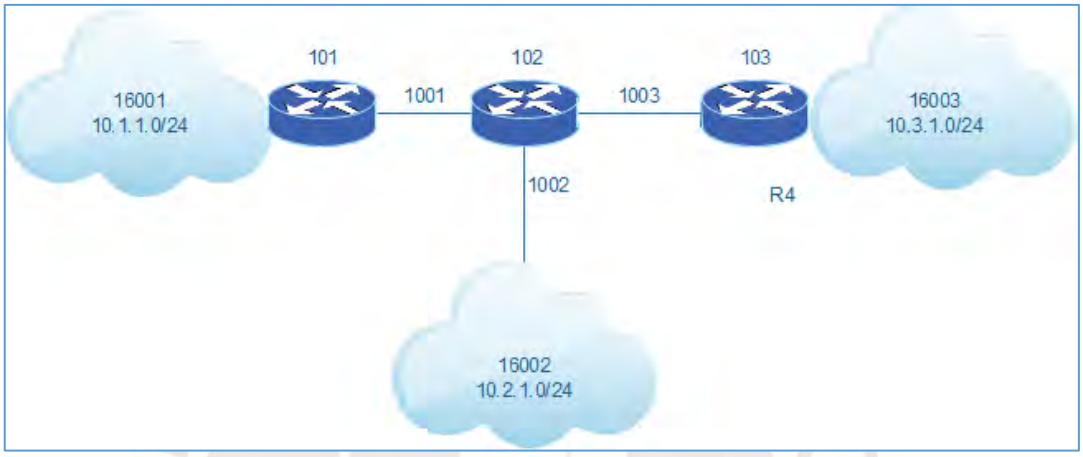

Fig. 2.8 Tipos de Segmentos

2.6.3. OSPF en SR-MPLS

Segment Routing utiliza un IGP para advertir la información de la topología, prefijos, SRGB e información de las etiquetas. Para cumplir estas tareas, el IGP requiere de extender sus capacidades. OSPF hace uso del LSA Tipo 10 (Opaque) para cumplir los requerimientos de SR. Estas extensiones son conocidas como TLVs y Sub-TLVs, que definen las capacidades necesarias para intercambio de información de segmentos [17].

Los TLVs se clasifican de la siguiente manera:

- TLV de Algoritmo SR, se utiliza para anunciar que se utilizará determinado algoritmo.
- TLV de Rango de Etiquetas/SID, se utiliza para anunciar el SR-MPLS SID o el SRGB.
- TLV de preferencia SRMS, anuncia la prioridad de un concentrador de funciones SR.

Los Sub-TLVs se clasifican de la siguiente manera:

- SID/Label Sub-TLV, anuncia losSIDs o etiquetas MPLS.

- Prefix SID Sub-TLV, anuncia los prefijos de la red SR-MPLS.
- Adj-SID Sub-TLV, anuncia los SIDs de adyacencia en una red tipo P2P.
- LAN Adj-SID Sub-TLV, anuncia los SIDs de adyacencia en una red tipo LAN.

La Figura 2.9 muestra como ejemplo de una estructura de un TLV del tipo SID/Label Range, con un sub-TLV del tipo Adj-SID, presente en un LSA Update en una red OSPF del tipo P2P:

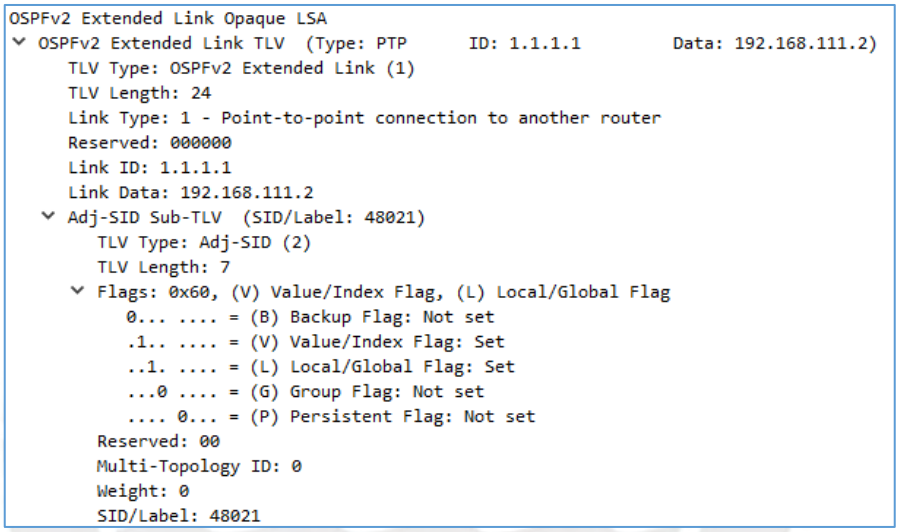

Fig. 2.9 Estructura de TLVs en OSPF LSA Tipo 10

2.7. Calidad de Servicio

2.7.1. Descripción

Calidad de Servicio se refiere a aplicación de mecanismos de clasificación, marcado, encolamiento, policing y shaping en el core de tal manera que el trato recibido por un paquete corresponde con los requisitos a nivel de servicio. No todas las aplicaciones que usan los servicios de transporte del Core van a requerir el mismo nivel de servicio. Al introducir mecanismos de Calidad de Servicio es posible que el core MPLS provea el rendimiento requerido por el tráfico más riguroso usando el core MPLS de una manera más económica que simplemente sobredimensionar la red entera, es así que es posible lograr un determinado SLA provisionando menor ancho de banda. Dicho esto, solo es

posible continuar enviando tráfico de mayor prioridad a expenses del tráfico de menor prioridad que va tener bufferizado y en último caso descartado para poder preservar el tráfico marcado como prioridad. Por lo tanto, cualquier implementación de Calidad de Servicio no puede ser vista como un método de reducción de ancho de banda entre dispositivos sino como un método de preservar el ancho de banda de tráfico de mayor prioridad y de baja tolerancia de latencia como el tráfico de voz durante periodos de congestión inesperada. Se recomienda utilizar una arquitectura de MPLS / DiffServ para ofrecer un servicio diferenciado basado en los bits de MPLS EXP. Para asegurar los niveles de retardo, jitter y pérdida de paquetes es necesario asegurar que el ancho de banda disponible para el flujo es mayor que el nivel de transmisión actual de ese flujo. [18]

2.7.2. Modelo Diffserv

Esta sección pretende ser una introducción al modelo de referencia Differentiated Services (DiffServ). DiffServ es un modelo en el que el tráfico es tratado por sistemas intermedios con prioridades relativas basadas en el campo de Type of Services (ToS) o Differentiated Services Code Point (DSCP). Definido en los RFCs 2474 y 2475, el estándar DiffServ reemplaza la especificación original de definición de prioridad de paquetes del RFC 791. El nuevo estándar DiffServ propone una nueva manera de interpretar el campo que siempre ha sido parte de un paquete IP. En el estándar DiffServ, el campo de ToS es renombrado como Differentiated Services Code Point (DSCP) y tiene un nuevo significado. El estándar DiffServ propone el incremento de los niveles de prioridad definibles mediante la reasignación de bits del paquete IP. El campo de ToS describe un byte entero (ocho bits) de un paquete IP. Precedence se refiere a los tres bits más significativos del campo de ToS: [XXX]XXXXX. Puede haber alguna confusión porque las personas ocasionalmente usan el termino ToS por los siguientes tres bits: XXX[XXX]XX. Para ser consistentes con la especificación del RFC 791, este documento usa el termino ToS para referirse a los ocho bits. Los tres bits más significativos del campo de ToS, los bits de Precedence, definen la prioridad del paquete IP en el RFC

791. En la figura 2.10 se ilustra el antiguo método para interpretar la porción de ocho bits del paquete IP. [18]

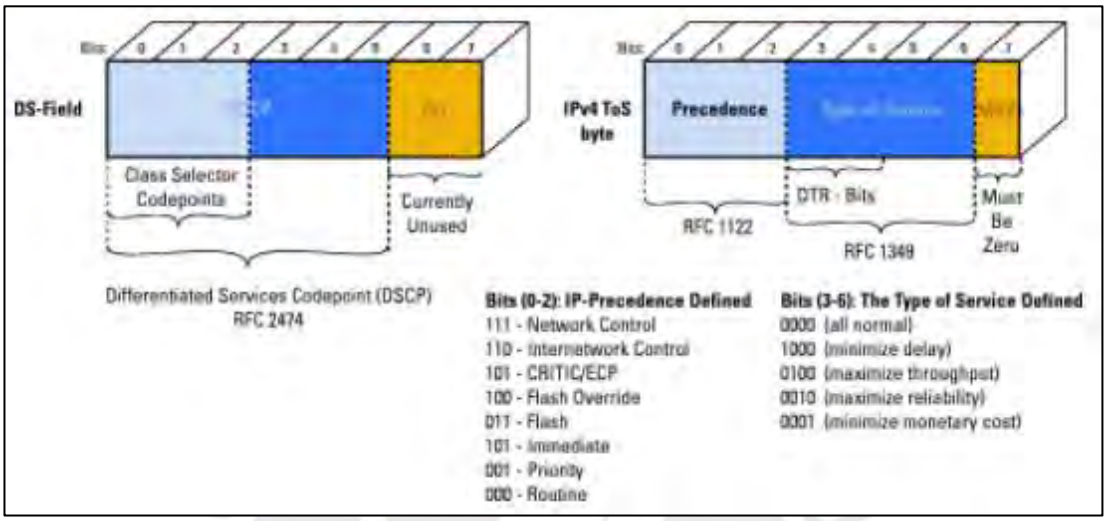

Fig. 2.10 DSCP y IP-Precedence

Este campo de ToS de un byte ha sido casi totalmente inutilizado desde que fue propuesto hace casi 20 años. Solamente en los últimos años las compañías empezaron a utilizar los bits de Precedence para establecer de decisiones de forwarding. El estándar de DiffServ sigue un esquema similar al RFC 791, pero utiliza más bits para establecer prioridad. El nuevo estándar mantiene compatibilidad con implementaciones con RFC 791, pero permite un uso más eficiente de los bits 3, 4 y 5. Los bits 6 y 7 están reservados para futuro uso. Con los tres bits adicionales, ahora hay un total de 63 clases en vez de las 7 clases previas. El RFC 2475 define Per Hop Behaviour (PHB) como el comportamiento de forwarding observable externamente aplicado en un nodo que cumple DiffServ a un DiffServ Behaviour Aggregate (BA). [18]

Con la habilidad del sistema de marcar paquetes de acuerdo a un esquema de DSCP, la colección y envío de paquetes con el mismo DSCP en una dirección particular, puede ser agrupados dentro de un BA. Paquetes de múltiples orígenes o aplicaciones pueden pertenecer a un mismo BA. En otras palabras, PHB se refiere a la programación de

paquetes, encolamiento, comportamiento de policing o shapings en un nodo en cualquier paquete perteneciente a un BA, configurado por un SLA o policy map. Las siguientes secciones describen los cuatro estándares disponibles de PHB [18]:

- Default PHB (definido en el RFC 2474)
- Class-Selector PHB (definido en el RFC 2474)
- Assured Forwarding (AFxy) PHB (definido en el RFC 2597)
- Expedited Forwarding (EF) PHB (definido en el RFC 2598)

2.7.3. Mecanismos para limitar tráfico

QoS ofrece dos tipos de mecanismo para el condicionamiento del tráfico, estos mecanismos son los denominados “policing” y “shaping”. Las políticas de tráfico pueden tener dos o tres clasificaciones/colores. Un “policing” de tráfico de dos colores da a entender dos posibles identificaciones de tráfico (conformed / exceeding). Un “policing” de tres colores identifica el tráfico de tres maneras (conformed / exceeding / violating). Por otro lado, un shaper típicamente contiene los paquetes excedidos agregando delay a los mismos, ya que realiza el buffering en memoria para no descartar. El concepto de “traffic shaping” y “policing” pueden trabajar en conjunto. Por ejemplo, un buen esquema de “traffic shaping” debería hacer más fácil la detección de anomalías de tráfico en la red. [19]

2.7.4. Mecanismos para evitar congestión

La técnica para evitar la congestión realiza un monitoreo de la carga de tráfico de manera proactiva, reaccionando en consecuencia para evitar posibles cuellos de botella. Esto es, se crean políticas de descarte de paquetes de manera aleatoria (de acuerdo a la criticidad definida en el paquete) para prevenir congestiones de enlace. Es necesario definir umbrales para el comportamiento correcto de las funciones de descarte, tratando de maximizar el throughput y la capacidad y minimizando la pérdida de paquetes y el delay. Weighted Tail Drop (WTD), Weighted Random Early Detect (WRED), y Distributed

WRED (DWRED) son ejemplos de mecanismos comúnmente soportados por los routers para el evitar la congestión. [19]

2.7.5. Mecanismo para manejo de congestión

Cuando tenemos una congestión en un enlace, se determinan mecanismos para manejar esta congestión. Una manera de que los elementos de red puedan manejar un overflow de tráfico utilizando una buena técnica de encolado para luego poder priorizarlos en la salida del link. Los algoritmos establecen que se procesen paquetes en base a la prioridad (definida por valores de [19]:

- Priority queueing (PQ)
- Low latency queueing (LLQ)
- Class-Based Weighted Fair Queueing (CBWFQ)

2.8. Gestión y Operación de Red

Esta sección contiene consideraciones específicas para una correcta gestión de la red a implementar.

2.8.1. Simple Network Management Protocol

La configuración SNMP es requerida para permitir a los sistemas de gestión monitorear el estado general de los elementos de la red. El Simple Network Management Protocol (SNMP) es utilizado para recabar estadísticas, contadores, y tablas almacenadas en un dispositivo de red. La información es utilizada por un sistema de Gestión para generar alertas en tiempo real, crear información estadística sobre el comportamiento de los elementos y sus interfaces, así como realizar configuraciones y revisiones ante fallas. El registro del SNMP envía notificaciones de cambios significativos en el estado del sistema a las estaciones de administración del SNMP. Se recomienda permitir los traps de SNMP para el registro del evento. [20]

2.8.2. Syslog

Para asistir y simplificar la solución de problemas y las investigaciones de seguridad, es necesario monitorear la información generada por el router. En su forma más simple, esto puede lograrse visualizando la información almacenada en la memoria buffer. Para hacer que el sistema de logging sea útil, el tamaño predeterminado del buffer debe aumentarse. Aunque simple, este método tiene algunas desventajas [21]:

- Es volátil. La información en el buffer no sobrevive si el sistema se reinicia.
- Tiene una capacidad limitada. El volumen de la información que puede ser retenida en el buffer está directamente relacionada con la cantidad de memoria de sistema y la porción de esta que se reserva para hacerlo.
- Configurar un buffer disminuye recursos a las funciones centrales del router.

Se recomienda que la estructura de logging esté basada en una infraestructura de syslog. Esto permite al dispositivo registrase físicamente y hasta geográficamente a un sistema separado utilizando syslog. Múltiples servidores syslog pueden ser configurados para la redundancia y distribución de la información. Cuando se configura un logging básico, deshabilitar el logging a consola es una buena práctica. El logging de consola puede ser habilitado cuando sea requerido [16].

2.8.3. Authorization, Authentication y Accounting

El método recomendado para controlar el acceso al router es a través de la metodología “Authorization, Authentication and Accounting (AAA)”. Este brinda almacenamiento de cuentas de usuario en un servidor centralizado de manera segura, El método AAA brinda ventajas tales como una administración centralizada de manera segura, estableciendo perfiles para los usuarios de acuerdo al nivel de operación que requiere (monitoreo, mantenimiento, administración, etc.). Permite que todos los accesos al router sean registrados en el servidor. Inclusive es posible registrar todas las acciones realizadas en el router. En el caso que el servidor AAA no sea alcanzable por IP, entonces se puede

usar un nombre de usuario y contraseña local para acceder al router. Se recomienda que la consola sea autenticada utilizando un nombre se usuario y contraseña local [22].

2.8.4. Network Time Protocol

La necesidad de tiempo sincronizado es crítica para los entornos de red de hoy en día. Network Time Protocol (NTP) define las características para la sincronización de reloj en modo Cliente - Servidor. Cada aspecto de la administración, seguridad, planeamiento y troubleshooting de una red incluye determinar cuándo los eventos suceden. El tiempo es un elemento crítico que permite que un evento en un nodo de red sea mapeado a un evento correspondiente en otro [23].

2.8.5. Secure Shell

Se recomienda Secure Shell (SSH) como el método de gestión recomendado para administrar los dispositivos de red. Además, se recomienda limitar el acceso a la consola virtual y así evitar que usuarios no autorizados de accedan a los dispositivos de red [24].

CAPÍTULO III

DISEÑO DE ARQUITECTURA SEAMLESS MPLS

3.1 Introducción a Seamless MPLS

En este escenario, las capas de acceso, agregación y core pertenecen a un único sistema autónomo (AS). La topología se ilustra en la figura 3.1:

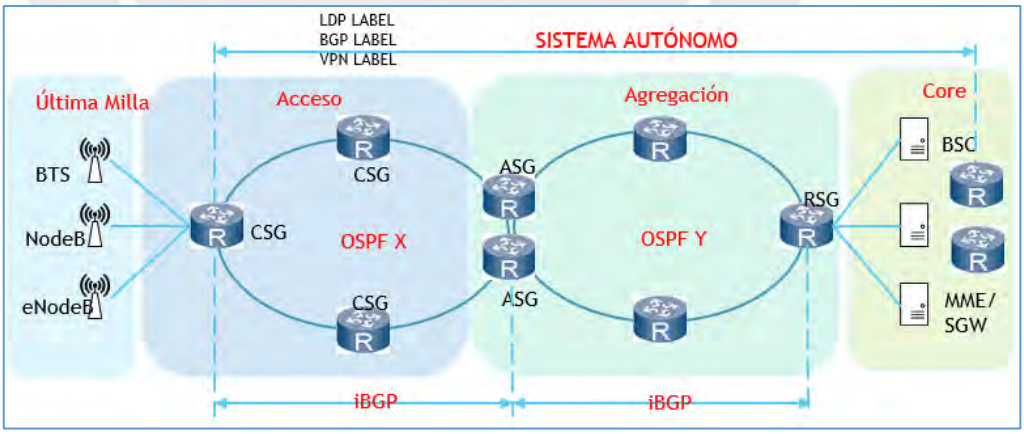

Fig. 3.1 Despliegue para Intra-AS seamless MPLS

Los protocolos de enrutamiento son desplegados de la siguiente manera:

- Un protocolo del tipo IGP (sea OSPF o IS-IS) es habilitado en cada uno de los elementos de las capas de acceso, agregación y core para implementar conectividad dentro del AS. No existe redistribución entre los protocolos IGP.
- El camino CSG → ASG → RSG es utilizado en el siguiente ejemplo: una sesión iBGP es establecida entre cada uno de los siguientes pares de elementos: CSG y ASG; ASG y RR. RSG y RR. Los RRs son los encargados de reflejar todas las rutas de la red.
- El ASG establece su loopback como IP del siguiente salto para las rutas anunciadas por BGP (next-hop self), con el fin de evitar el anuncio de redes mediante la redistribución a nivel de protocolo IGP. Al establecer el next-hop self adecuado, la ruta será válida.
- Un túnel es establecido utilizando LDP o RSVP-TE.
- Estos dispositivos son habilitados para anunciar rutas con etiqueta, y asignar etiquetas a rutas BGP que se especifican con una política de enrutamiento. Después de que los dispositivos intercambian rutas BGP con etiquetas, un LSP BGP E2E es establecido entre el CSG y RSG.

3.2 Estructura de simulación fase 1: Seamless-MPLS

El presente estudio realiza la simulación de una red, en su estructura básica, constituida por 8 Routers, semejante a la red de un proveedor de servicios de internet. Se utilizan los siguientes programas:

- eNSP con versión 1.3.00.100 V100R300C00SPC100,
- Wireshark con versión 3.2.6- g4f9257fb8ccc.
- SecureCRT con versión 8.7.2

Tenemos la siguiente estructura de ejecución para la simulación:

1. Configuración de IPs (interfaces físicas, lógicas)
2. Configuración de Protocolo IGP (OSPF para el presente caso de estudio)

3. Configuración de MPLS + LDP como protocolo de intercambio de etiquetas MPLS.
4. Configuración de Protocolo MP-BGP para intercambio de información de rutas VPNV4, donde el elemento P3 funcionará como RR de la red.
5. Habilitación de BGP+Label en todos los peers i-BGP, incluyendo red de Acceso.
6. Pruebas de conectividad desde el elemento **eNodeB** hasta el elemento **Core_NE**, tráfico que cursará a través de un servicio L3VPN construido sobre la red MPLS.

3.3 Implementación de prueba

En la Figura 3.2, se determina el primer escenario de prueba que se constituye de cinco elementos de core y agregación, un elemento de pre-agregación y dos elementos externos (e-NodeB y Core_NE) que emulan el comportamiento de "clientes", o dispositivos finales que requieren conectividad de extremo a extremo.

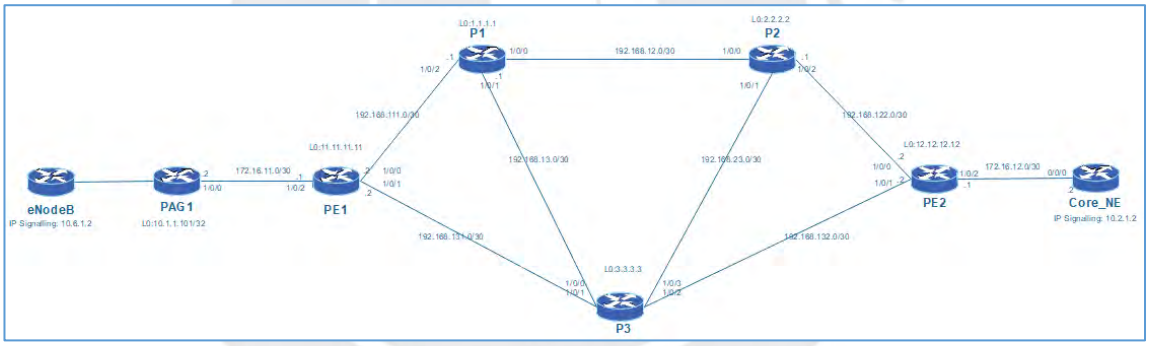

Fig. 3.2 Topología de Red de conexiones físicas y lógicas

En este esquema, se presenta una red MPLS, con arquitectura Seamless-MPLS, donde los elementos PE1, P1, P2, P3, PE2, constituyen el core/agregación de la red del proveedor de servicios. El elemento PE1 es considerado un ASBR, dado que tiene dos procesos OSPF en ejecución (proceso 1 hacia el Core y Proceso 100 hacia el pre-agregador, PAG1), ilustrado en la Figura 3.3. En este escenario el elemento PE1, posee 2 LSDB independientes de cada uno de los procesos a los que pertenece y no existe redistribución de rutas entre ambos procesos.

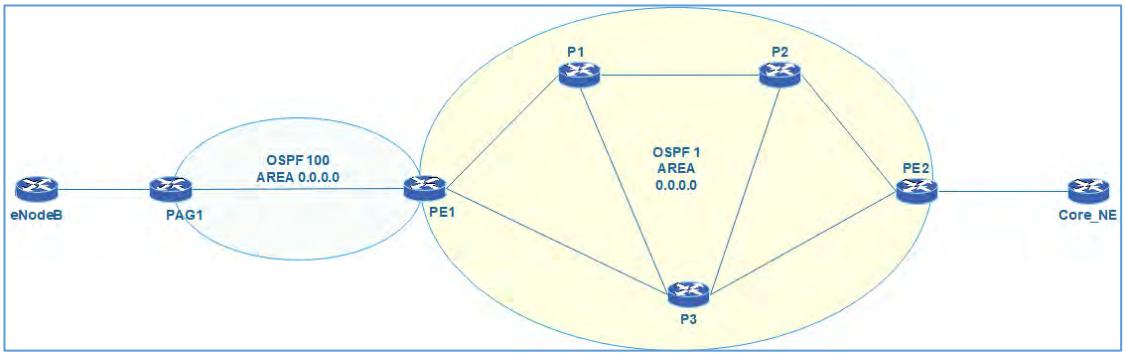

Fig. 3.3 Topología de diseño OSPF

La configuración del protocolo OSPF del elemento PE1 se muestra a continuación:

```
ospf 1 router-id 11.11.11.11
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
#
ospf 100
 import-route direct route-filter redistribute_loopback
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
#
xpl route-filter redistribute_loopback
 if ip route-destination in {11.11.11.11 32} then
  approve
 else
  refuse
 endif
 end-filter
#
```

Donde observamos que no se está realizando una redistribución entre ambos procesos, más sí la redistribución de la loopback 11.11.11.11, la cual corresponde al LSR-ID del elemento PE1. Esto para establecer la sesión MPLS-LDP entre los elementos PE1 y PAG1.

Es acá donde encontramos el primer punto en contra de la arquitectura Seamless-MPLS: la necesidad de un protocolo complementario (LDP) para la distribución de etiquetas MPLS entre todos los elementos de la red. LDP será el encargado de compartir la información de las etiquetas que se asignen por cada loopback o prefijo que exista en la red.

El elemento PE1 se encarga de dividir ambos procesos de IGP, para establecer la jerarquía Seamless-MPLS, comportándose como un Route-Reflector In-line de BGP. En este sentido, el pre-agregador PAG1 únicamente tiene una sesión i-BGP contra el RR-Inline (el router reflector del anillo), con quien intercambiará rutas. Cualquier elemento que sea integrado en el anillo de pre-agregación, levantará sesiones i-BGP únicamente con el RR-Inline (PE1). Los elementos de Core, tienen sesiones establecidas por i-BGP contra el elemento P3 que funciona como RR de Core (Route-Reflector de Jerarquía Nivel 1). El dispositivo P3 se encargará de distribuir las rutas entre todos los elementos del core. La relación de sesiones i-BGP se ilustran en la Figura 3.4:

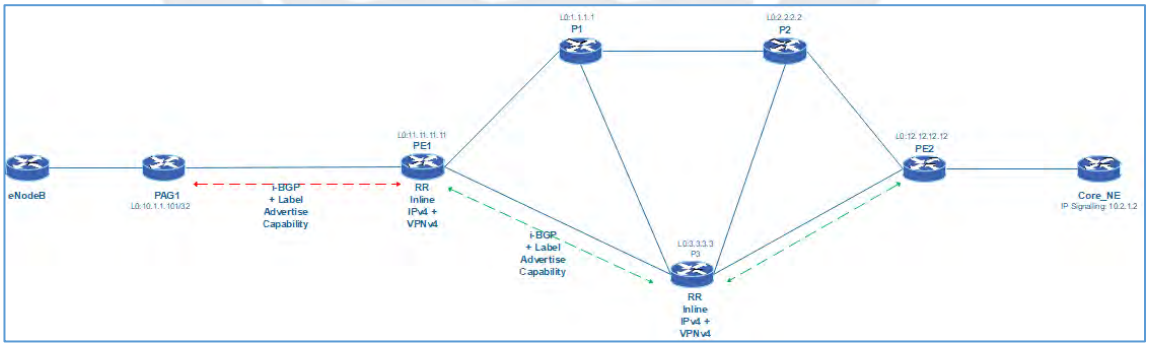

Fig. 3.4 Topología de diseño i-BGP

La arquitectura Seamless-MPLS requiere que el RR-Inline anuncie únicamente prefijos específicos, de segmento IP /32, que corresponden a las loopbacks de todos los

elementos del Core y que tienen una etiqueta MPLS. Esto para establecer las sesiones LSP extremo a extremo necesarias para la implementar la conectividad en elementos que se encuentran en dominios de IGP distintos. De esta manera, el elemento PAG1, conocerá únicamente las redes que son necesarias para él, mas no otras que no requiera establecer comunicación. Se utiliza BGP por la facilidad de establecer filtros de este tipo para el anuncio de rutas. En casos donde se encuentren dos agregadores, se deberá hacer uso de los atributos BGP, para establecer el camino preferido.

La conexión en los extremos (eNodeB – PAG1 y Core_NE – PE2) son conexiones establecidas únicamente a nivel de IP, se maneja enrutamiento estático por defecto para cada uno de los servicios emulados.

La configuración de BGP en el elemento PE1 se muestra a continuación:

```
bgp 65000
 router-id 11.11.11.11
 peer 3.3.3.3 as-number 65000
 peer 3.3.3.3 connect-interface LoopBack0
 peer 10.1.1.101 as-number 65000
 peer 10.1.1.101 connect-interface LoopBack100
 #
 ipv4-family unicast
  undo synchronization
  network 11.11.11.11 255.255.255.255
  peer 3.3.3.3 enable
  peer 3.3.3.3 route-filter seamless_RR export
  peer 3.3.3.3 next-hop-local
  peer 3.3.3.3 label-route-capability
  peer 3.3.3.3 advertise-community
  peer 10.1.1.101 enable
  peer 10.1.1.101 route-filter seamless_to_pag export
  peer 10.1.1.101 reflect-client
```

```
  peer 10.1.1.101 next-hop-local
  peer 10.1.1.101 label-route-capability
  peer 10.1.1.101 advertise-community
 #
 ipv4-family vpnv4
  undo policy vpn-target
  peer 3.3.3.3 enable
  peer 3.3.3.3 next-hop-local
  peer 3.3.3.3 advertise-community
  peer 10.1.1.101 enable
  peer 10.1.1.101 reflect-client
  peer 10.1.1.101 next-hop-local
  peer 10.1.1.101 advertise-community
#
xpl route-filter seamless_RR
 if ip route-destination in {11.11.11.11 32} then
  apply mpls-label
 elseif mpls-label exist then
  apply mpls-label
 else
  refuse
 endif
 end-filter
#
xpl route-filter seamless_to_pag
 if mpls-label exist then
  apply mpls-label
 else
  refuse
 endif
```

```
 end-filter
#
```

De esta manera, desde el punto de vista del PAG1, se establece una sesión LSP-BGP de extremo a extremo hasta el elemento PE2, como se muestra a continuación:

```
<PAG1>display mpls lsp
------------------------------------------------------------
LSP Information: LDP LSP
------------------------------------------------------------FEC
In/Out Label    In/Out IF                      Vrf Name
10.1.1.11/32       NULL/3          -/Eth1/0/0
10.1.1.11/32       48122/3         -/Eth1/0/0
10.1.1.101/32      3/NULL          -/-
11.11.11.11/32     NULL/3          -/Eth1/0/0
11.11.11.11/32     48123/3         -/Eth1/0/0
------------------------------------------------------------
                 LSP Information: BGP LSP
------------------------------------------------------------FEC
In/Out Label    In/Out IF                      Vrf Name
3.3.3.3/32         NULL/48006      -/-
10.1.1.101/32      48121/NULL      -/-
12.12.12.12/32     NULL/48007      -/-
10.6.1.0/30        48120/NULL      -/-            signaling
```

La etiqueta de salida con valor 3 (o implicit-Null) indica que se hará una operación POP sobre el FEC indicado. El paquete entre el elemento PAG-1 / PAG, tendrá una etiqueta que hace referencia al prefijo destino, **48011**, tal como se indica en la figura 3.5. La asignación de la etiqueta es de manera aleatoria, en un rango que puede ser configurable. Sin embargo, hay forma de poder asignar los valores de etiquetas manualmente, la cual sería una solución no escalable porque la cantidad de prefijos en la red puede estar en el orden de millones de entradas. En este caso, para una prueba

de conectividad extremo a extremo desde el eNodeB hacia el Core_NE (IP Origen: 10.6.1.2, IP Destino: 10.2.1.2) se determina lo siguiente:

```
<PAG1>disp ip routing vpn-instance signaling 10.2.1.2 ver
Route Flags: R - relay, D - download to fib, T - to vpn-instance,
B - black hole route
------------------------------------------------------------------------------
Routing Table : signaling
Summary Count : 1

Destination: 10.2.1.0/30
     Protocol: IBGP               Process ID: 0
   Preference: 255                      Cost: 0
      NextHop: 10.1.1.11          Neighbour: 10.1.1.11
        State: Active Adv Relied         Age: 00h47m46s
          Tag: 0                    Priority: low
        Label: 48011                QoSInfo: 0x0
   IndirectID: 0x1000080            Instance:
 RelayNextHop: 172.16.11.1         Interface: Ethernet1/0/0
     TunnelID: 0x0000000001004c4b42 Flags: RD
<PAG1>

Tunnel ID:       0x0000000001004c4b42
Type:            ldp
Name:            LDP LSP
Destination:     10.1.1.11
Instance ID:     0
MTU:             1500
Cost:            1
Status:          UP
```

```
Out Interface:    Ethernet1/0/0
  NextHop:        172.16.11.1
```

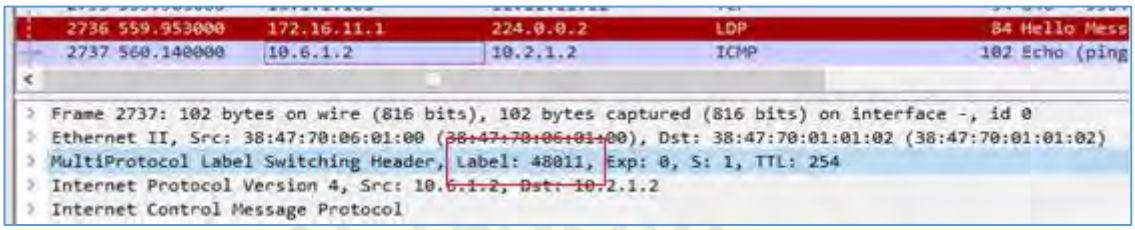

Fig. 3.5 Identificación de etiquetas en enlace PE1 – PAG1

En el elemento PE1, se observa que se tiene asignada una etiqueta de salida con valor 48002 para el destino 12.12.12.12, que se define como la etiqueta externa (LDP) y se realiza un SWAP de la etiqueta interna, esto es, para cada mensaje que ingrese con etiqueta 48011, se cambiará a 48006. Esto se confirma en la captura de paquetes entre PE1-P1 en la figura 3.6.

```
<PE1>disp mpls lsp
--------------------------------------------------------------
                 LSP Information: LDP LSP
--------------------------------------------------------------
FEC               In/Out Label    In/Out IF                    Vrf
Name
…
12.12.12.12/32      NULL/48002       -/Eth1/0/0
12.12.12.12/32      48002/48002      -/Eth1/0/0
--------------------------------------------------------------
                 LSP Information: BGP LSP
--------------------------------------------------------------
Name
10.2.1.0/30      48011/48006      -/-            ASBR LSP
```

```
...
<PE1>
```

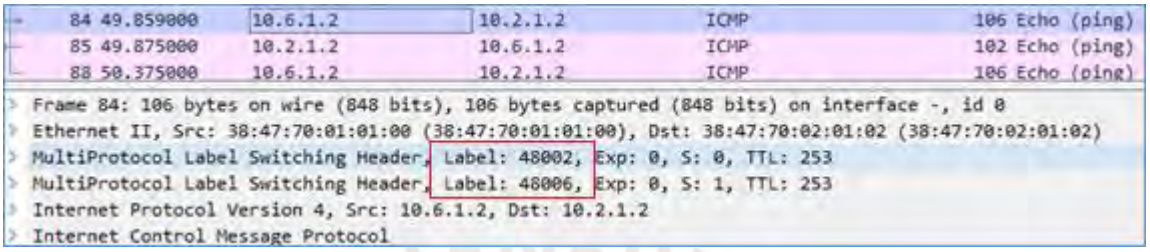

Fig. 3.6 Identificación de etiquetas en enlace PE1 – P1

En el elemento P1, se observa que se realiza una acción de SWAP de etiquetas MPLS, en este caso la etiqueta de entrada y de salida es la misma 48002, para el tráfico saliente por la interface Eth1/0/0. La información se valida en la captura de la figura 3.7:

```
<P1>disp mpls lsp
--------------------------------------------------------------
                 LSP Information: LDP LSP
--------------------------------------------------------------
FEC               In/Out Label    In/Out IF                    Vrf
Name
12.12.12.12/32      48002/48002      -/Eth1/0/0
12.12.12.12/32      NULL/48001       -/Eth1/0/1
12.12.12.12/32      48002/48001      -/Eth1/0/1
```

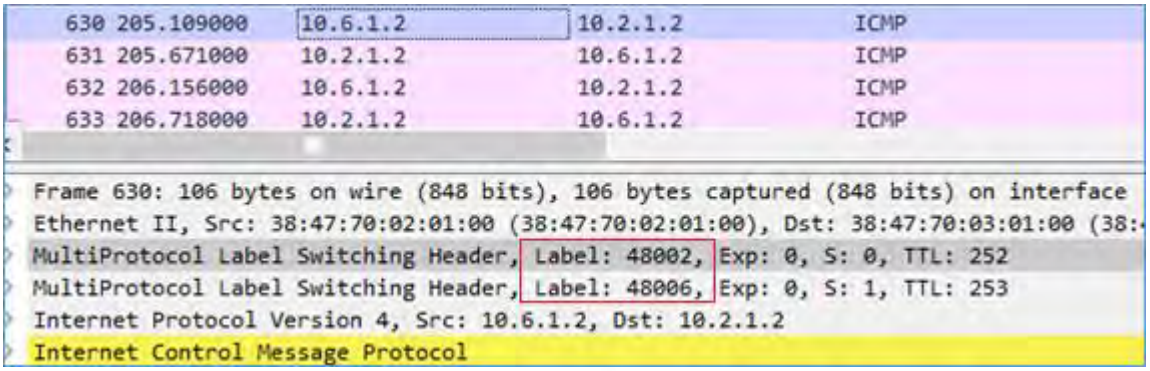

Fig. 3.7 MPLS SWAP P1

En el elemento P2, se ejecuta la acción de POP de la etiqueta externa, enviando hacia el elemento PE2 sin etiqueta LDP, se observa que a lo largo del tramo se mantiene la etiqueta interna **48006**, que identifica la VPN de SIGNALLING, tal como se muestra en la Figura 3.8:

```
<P2>disp mpls lsp
Flag after Out IF: (I) - RLFA Iterated LSP, (I*) - Normal and RLFA
Iterated LSP
Flag after LDP FRR: (L) - Logic FRR LSP
------------------------------------------------------------
                 LSP Information: LDP LSP
------------------------------------------------------------
FEC               In/Out Label    In/Out IF                    Vrf
Name
11.11.11.11/32     NULL/48000      -/Eth1/0/0
11.11.11.11/32     48001/48000     -/Eth1/0/0
12.12.12.12/32     NULL/3          -/Eth1/0/2
12.12.12.12/32     48002/3         -/Eth1/0/2
```

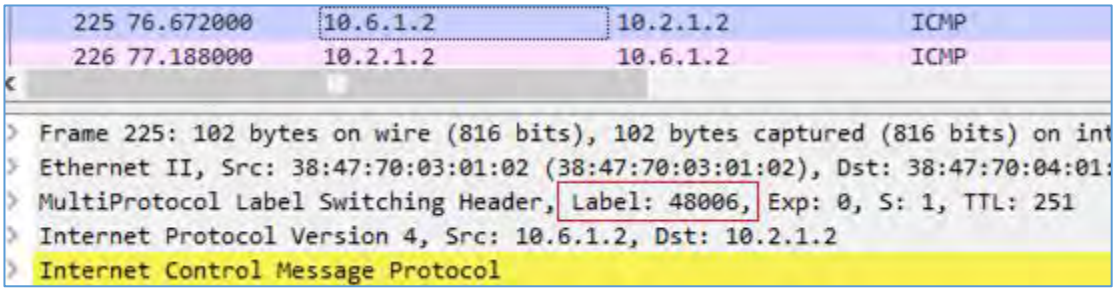

Fig. 3.8 Identificación de etiquetas en enlace P2 – PE2

La acción de SWAP se puede interpretar correctamente en el tráfico de regreso, donde el destino es la IP del elemento PE1, esto es, si recibe una etiqueta con valor 48001, la etiqueta de salida es la etiqueta 48000. En la Figura 3.9 se observa en una captura realizada entre el segmento P2-PE2, que el paquete viaja con una etiqueta 48001, y cambia a un valor de 48000 una vez ha pasado el paquete por el equipo PE2 hacia PE1 según se observa en la captura de la Figura 3.10

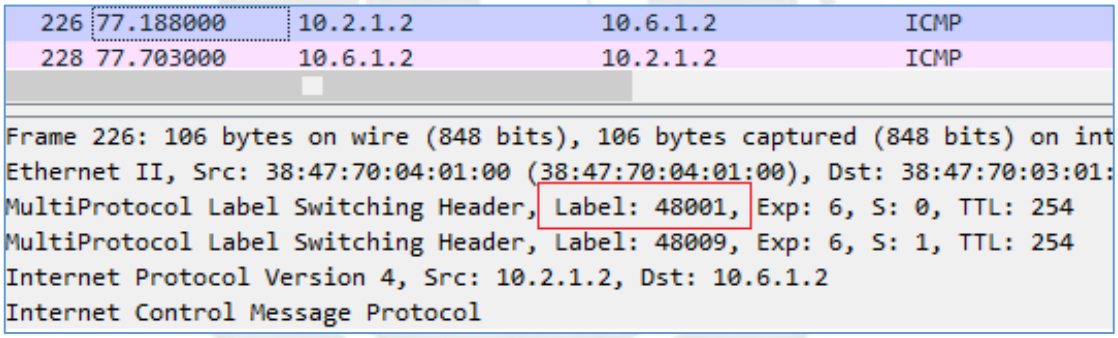

Fig. 3.9 Identificación de comportamiento SWAP en enlace P2 – PE2

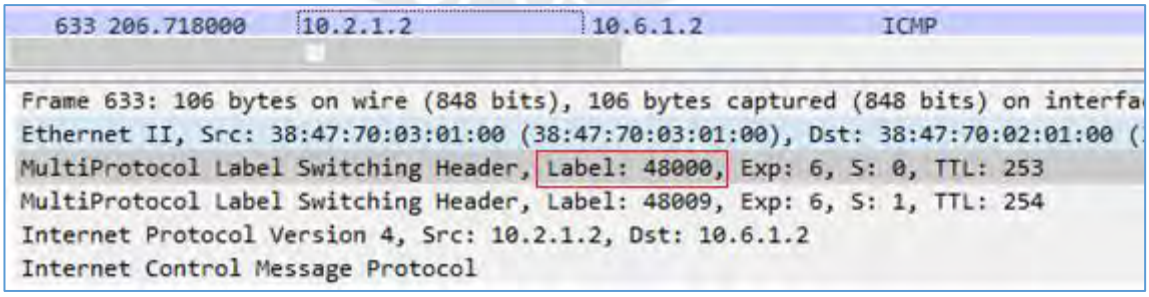

Fig. 3.10 Identificación de comportamiento SWAP en enlace P2 – P1

Para este escenario, con caminos con costos iguales, el balanceo de tráfico no es automático, dado que se escoge un único LSP (el más óptimo) para el envío de paquetes. Es necesario utilizar túneles de ingeniería de tráfico para la habilitación (mediante la utilización del protocolo RSVP-TE) para poder implementar el balanceo de carga. Los túneles tienen la naturaleza de ser uni-direccionales, por lo que se deberán crear por cada vpn o destino en específico. La solución tiende a ser no escalable en redes de gran envergadura.

3.4 Análisis de resultados de simulación Fase 1 Seamless-MPLS

El protocolo LDP es el encargado de realizar el intercambio de etiquetas entre todos los elementos de la red MPLS. Esto es, por cada FEC, o LSR-ID del elemento, se asignará una etiqueta, y mediante LDP, los elementos requieren compartir las etiquetas para construir los LSPs de extremo a extremo. La asignación de etiquetas e intercambio de etiquetas obedece a ciertas reglas específicas en la configuración del elemento. Si bien es posible la asignación manual de cada una de las etiquetas, esta es una solución poco escalable. Mientras que cuando se asignan etiquetas automáticamente y de manera aleatoria, es difícil de controlar y operar, debido a que el comportamiento puede variar en cada elemento. Así mismo, dado que el camino se establece utilizando el mejor costo indicado por el IGP, por defecto solo se puede escoger un único mejor camino, ocasionando una sub-utilización de enlaces. Se puede realizar el balanceo de tráfico mediante la implementación de ingeniería de tráfico (MPLS-TE), pero su aplicación es bastante compleja, donde hay que especificar los saltos intermedios para definir un camino explícito (existe la opción dinámica, pero ya deja de ser controlable totalmente). De igual manera, tiende a ser una solución no tan escalable cuando se trata de una red de proveedor de servicios, con una cantidad numerosa de equipos que constituyen la red MPLS. Concluimos que existen tres deficiencias en la arquitectura Seamless-MPLS:

1. Necesidad de un protocolo adicional (LDP, RSVP) para intercambio de etiquetas MPLS.

2. Asignación dinámica y aleatoria de etiquetas que complica la operación, mantenimiento y análisis de puntos de falla, dado que cada elemento puede manejar una distinta tabla de mapeo de etiquetas MPLS.
3. Subutilización de enlaces cuando se establecen LSPs mediante LDP, y dificultad de masificar la solución de MPLS-TE para balanceo de tráfico y optimización de recursos.

Ante este escenario, el despliegue de Segment Routing se presenta como una solución apropiada ante las deficiencias demostradas del protocolo LDP. El funcionamiento se presentará en el siguiente capítulo.

CAPÍTULO IV
DISEÑO DE ARQUITECTURA SEGMENT ROUTING

Las simulaciones realizadas en el presente capítulo tienen como base las configuraciones realizadas en el capítulo III, esto es, se parte de las configuraciones realizadas en los pasos anteriores y se procederá a describir la transición/migración de una red Seamless-MPLS hacia una red basada en Segment Routing.

4.1 Introducción a MPLS Segment Routing

Se define como “Segmento” a un conjunto de órdenes que se identifican para realizar la conmutación de un paquete. El enrutamiento en base a “segmentos” indica que la decisión de enviar un paquete por determinada interfaz física se realizará en base a la instrucción definida en el segmento. A diferencia de la arquitectura basada en Seamless, donde se necesita LDP para el intercambio de información de etiquetas, en MPLS-SR, los elementos intermedios tienen conocimiento de estos segmentos utilizando extensiones del protocolo IGP para intercambiar la información de los valores de los segmentos asignados. Para la Figura 4.1, se define el valor de segmento 17400 como el elemento destino del paquete, por lo que los elementos intermedios deberán tomar la decisión en base a cómo llegar al elemento con valor 17400.

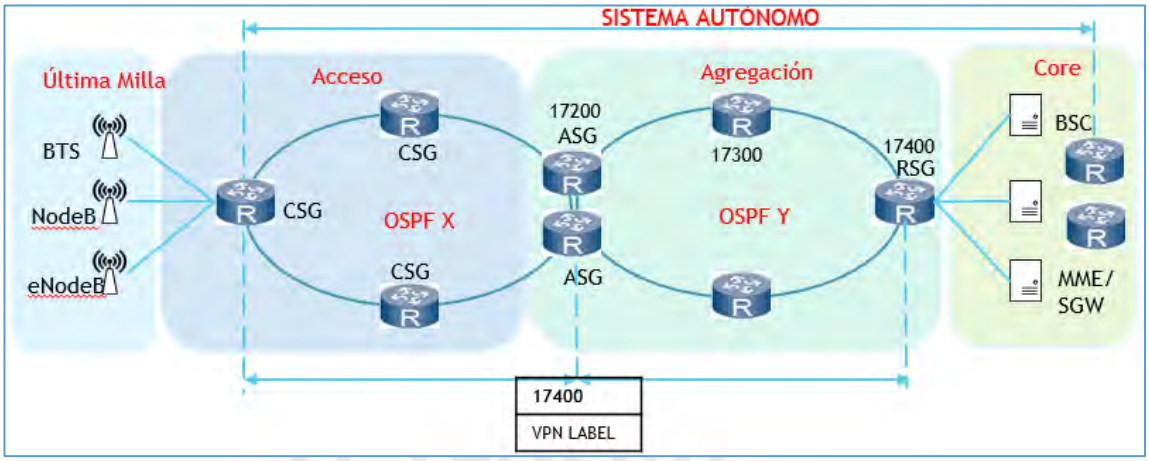

Fig. 4.1 Topología general de simulación SR

4.2 Evolución de OSPF-IGP

OSPF requiere utilizar LSAs tipo 10 para enviar la información mediante mensajes LSAu. En la Figura 4.2 se observa el mensaje del tipo LSAu entre los elementos PE1 y P1, al momento de asignarse el Segmento 16100 al elemento PE1.

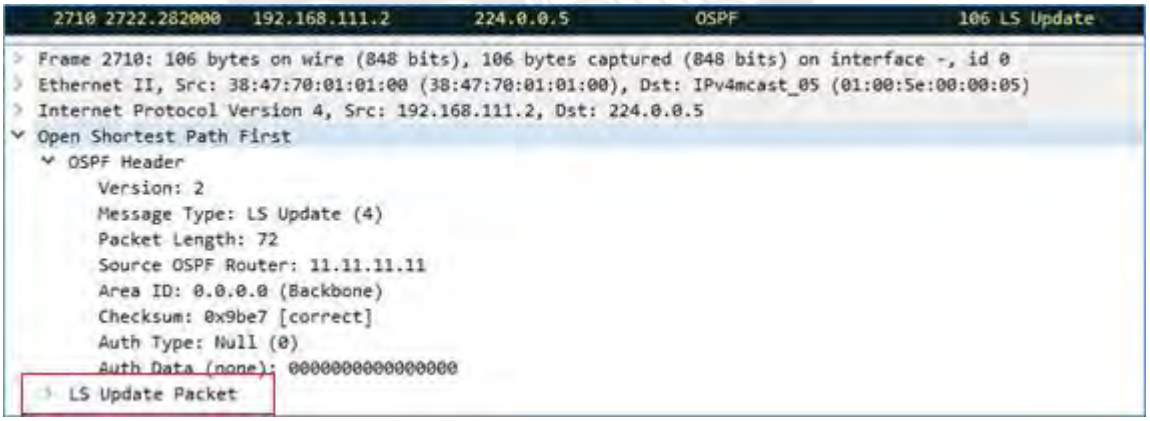

Fig. 4.2 Identificación de un LSAu entre PE1-P1

Es en este LSAu, que viaja la información de segment routing. Cuando se habilita Segment Routing en el elemento P1, se originan un paquete LSAu que lleva la información de tres LSAs tipo 10, como se observa en la Figura 4.3

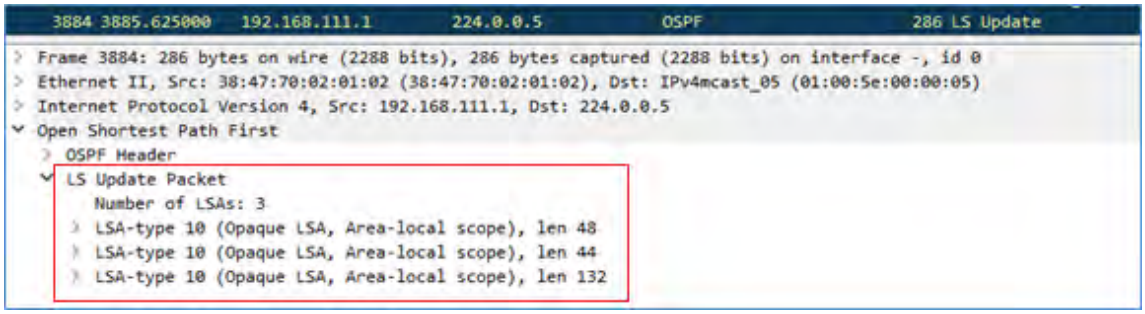

Fig. 4.3 Identificación de un LSAu entre PE1-P1

4.3 Estructura de simulación fase 2: MPLS-Segment Routing

Para esta fase, se hace el uso del mismo software que en el escenario del capítulo 3:

- eNSP con versión 1.3.00.100 V100R300C00SPC100,
- Wireshark con versión 3.2.6- g4f9257fb8ccc.
- SecureCRT con versión 8.7.2

Tenemos la siguiente estructura de ejecución para la simulación, considerando que las pruebas se realizan posterior a la configuración del capítulo anterior:

1. Habilitación de Segment Routing (SR) de manera Global
2. Habilitación de SR en el proceso OSPF y asignación del rango de prefijos (SGRB)
3. Habilitación de prefix-sid sobre la interface loopback
4. Verificación de información de prefijos compartidos por SR en la red.
5. Eliminación de protocolo LDP en la red y verificación de tráfico.
6. Establecer túneles de Ingeniería de Tráfico desde PE1 hasta PE2 y viceversa, y aplicarlo sobre un servicio de L3VPN.

7. Verificación de comportamiento de tráfico y comparación entre SR-TE y SR-BE.

4.4 Implementación de escenario de pruebas Fase 2 MPLS-SR

El primer LSA, identifica el Adj-SID Sub-TLV, que de acuerdo al elemento P1, se asigna el valor de 48022. El segundo LSA indica el Rango de SID (se establece el rango entre los valores 16000 y 25000, por tanto, se tiene un rango de 9001 SID que pueden ser asignados en la red. El tercer LSA identificado en la captura hace referencia a un LSA MPLS TE. Entre los elementos ya se tenía establecido MPLS-TE sobre OSPF previamente. El detalle se puede observar en la Figura 4.4

Fig. 4.4 Detalle de LSAs tipo 10 entre PE1-P1

Validando la información en el elemento P1:

```
   Segment Routing Adjacency MPLS Forwarding Information

Label  Interface NextHop       Type        MPLSMtu   Mtu
-------------------------------------------------------------48022
Eth1/0/2  192.168.111.2 OSPFv2      ---       1500

Total information(s): 1
#
ospf 1 router-id 1.1.1.1
```

```
 opaque-capability enable
 segment-routing mpls
 segment-routing global-block 16000 25000
 area 0.0.0.0
  mpls-te enable
#
```

Se debe asignar un valor de SID-Prefix a la loopback de elemento. Para este caso, se asigna el valor de 16001 a la loopback 0 del elemento P1, que actúa como identificador en la red MPLS-SR. La información viaja por un LSAu, enviado desde el elemento P1, como se observa en la Figura 4.5, donde se observa que para el prefijo 1.1.1.1 que actúa como Interfaz Loopback0 del elemento P1, se asigna SID de 1:

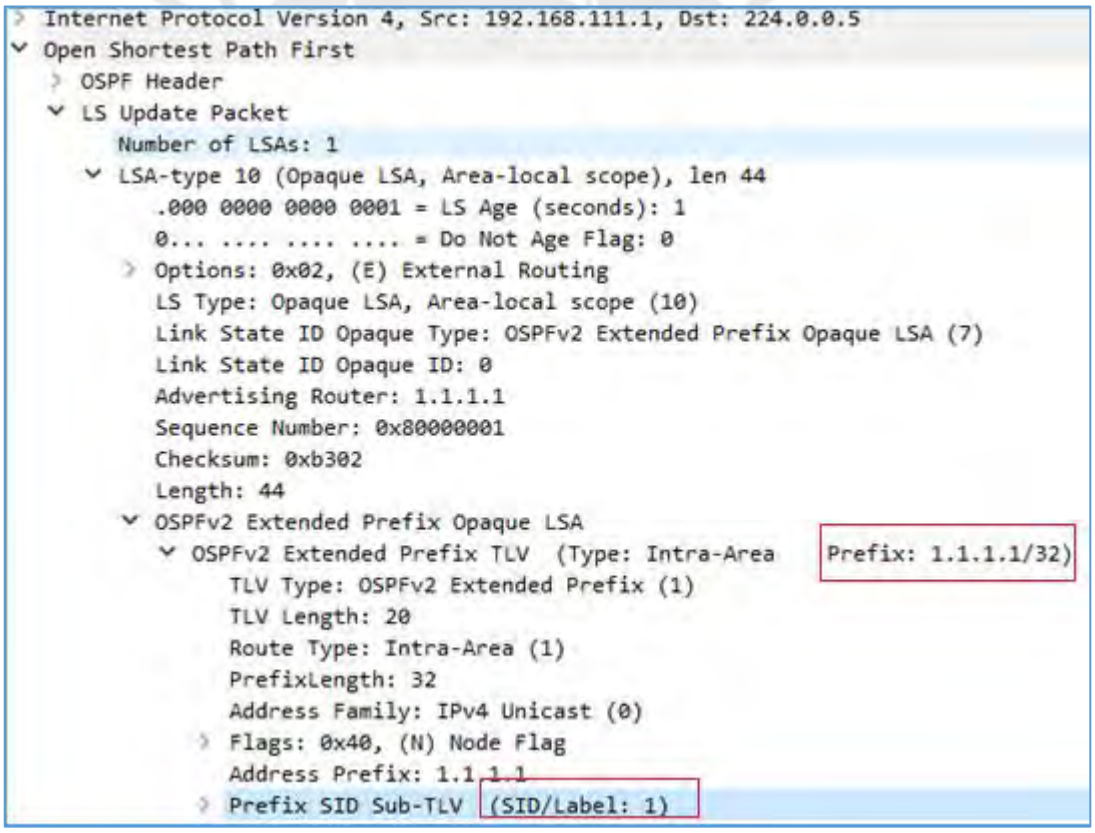

Fig. 4.5 Detalle de LSAs tipo 10 para un prefix-sid entre PE1-P1

Sin embargo, este valor es incremental, en relación al prefijo base (que es 16000), por tanto, su SID asignado es 16001:

```
      Segment Routing Prefix MPLS Forwarding Information
------------------------------------------------------------
Role : I-Ingress, T-Transit, E-Egress, I&T-Ingress And Transit

Prefix         Label  OutLabel  Interface NextHop     Role
MPLSMtu   Mtu     State
------------------------------------------------------------
1.1.1.1/32     16001   NULL     Loop0    127.0.0.1     E      --
-       1500    Active
11.11.11.11/32 16100   3        Eth1/0/2 192.168.111.2 I&T   ---
1500    Active

Total information(s): 2
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 ospf enable 1 area 0.0.0.0
 ospf prefix-sid absolute 16001
```

Se establecen los siguientes valores de SID-Prefix para los elementos de la red, detallado en la Tabla 4.1:

Elemento	IP Prefix	SID-Prefix
PE1	11.11.11.11	16100
P1	1.1.1.1	16001
P2	2.2.2.2	16002
P3	3.3.3.3	16003
PE2	12.12.12.12	16200

Tabla 4.1 Asignación de SIDs

Se valida los SID asignados:

```
    Segment Routing Prefix MPLS Forwarding Information
------------------------------------------------------------
Role : I-Ingress, T-Transit, E-Egress, I&T-Ingress And Transit

Prefix             Label      OutLabel   Interface
NextHop          Role  MPLSMtu   Mtu     State
------------------------------------------------------------------
-----------------------------------------------
1.1.1.1/32          16001      3          Eth1/0/0
192.168.12.1     I&T   ---       1500    Active
2.2.2.2/32          16002      NULL       Loop0
127.0.0.1        E     ---       1500    Active
3.3.3.3/32          16003      3          Eth1/0/1
192.168.23.2     I&T   ---       1500    Active
11.11.11.11/32      16100      16100      Eth1/0/0
192.168.12.1     I&T   ---       1500    Active
12.12.12.12/32      16200      3          Eth1/0/2
192.168.122.2    I&T   ---       1500    Active
```

4.5 Eliminación de LDP.

Una vez se tiene configurado SR en el core, y si al mismo tiempo se tiene LDP, LDP tiene mayor prioridad para la toma de decisiones de forwarding de paquetes. Esto es, se utilizará LDP para establecer el LSP extremo a extremo y enviar los paquetes a través de éste LDP.

Para nuestro escenario, estableciéndose conectividad entre los elementos eNodeB y Core_NE (con IPs 10.6.1.2 y 10.2.1.2 respectivamente), verificaremos rápidamente que aún configurado SR, se tiene la conmutación basado en señalización LDP.

```
<PE1>disp mpls lsp
Flag after Out IF: (I) - RLFA Iterated LSP, (I*) - Normal and
RLFA Iterated LSP
Flag after LDP FRR: (L) - Logic FRR LSP
------------------------------------------------------------
                 LSP Information: LDP LSP
------------------------------------------------------------
FEC                In/Out Label    In/Out IF
Vrf Name
…
12.12.12.12/32     NULL/48063      -/Eth1/0/0
12.12.12.12/32     48063/48063     -/Eth1/0/0
------------------------------------------------------------
                 LSP Information: BGP LSP
--------------------
FEC                In/Out Label    In/Out IF
Vrf Name
3.3.3.3/32         48069/48000     -/-
10.1.1.101/32      48068/48000     -/-
11.11.11.11/32     48071/NULL      -/-
12.12.12.12/32     48070/48003     -/-
------------------------------------------------------------
                 LSP Information: L3VPN LSP
------------------------------------------------------------
FEC                In/Out Label    In/Out IF
Vrf Name
10.2.1.0/30        48066/48004     -/-
ASBR LSP
10.6.1.0/30        48067/48001     -/-
ASBR LSP
```

```
<PE1>
```

Y se muestra en la captura de paquetes entre PE1 y P1, según la Figura 4.6

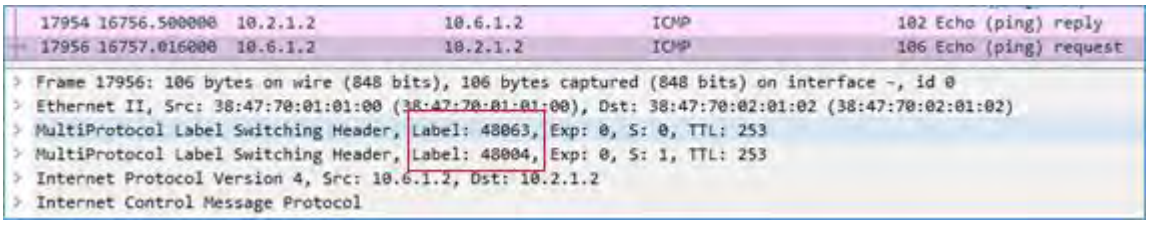

Fig. 4.6 Detalle de conmutación vía LDP

Procedemos a eliminar LDP de nuestros elementos de red, tomaremos como ejemplo P1. Todos los elementos de la red eliminarán LDP en las interfaces que comprenden al Core MPLS, y verificamos que no existe ningún LSP establecido en el elemento P1.

```
 interface ethernet1/0/0
  undo mpls ldp
  undo mpls te
 interface ethernet1/0/1
  undo mpls ldp
  undo mpls te
 interface ethernet1/0/2
  undo mpls ldp
  undo mpls te
#
<P1>disp mpls lsp
```

Verificamos que aún existe conectividad de extremo a extremo:

```
<eNodeB>ping -a 10.6.1.2 10.2.1.2
  PING 10.2.1.2: 56  data bytes, press CTRL_C to break
Reply from 10.2.1.2: bytes=56 Sequence=1 ttl=250 time=40 ms
<eNodeB>
```

Sobre la misma captura entre PE1 y P1, observamos que el comportamiento de los asignación de valores de las etiquetas ha variado, tal cual se muestra en la Figura 4.7:

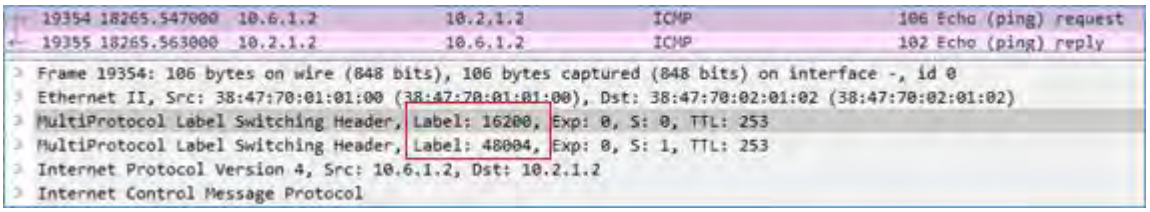

Fig. 4.7 Detalle de conmutación vía SR

Se mantiene el valor interno de la etiqueta en 48004 que hace referencia a la VRF, sin embargo, se utiliza la etiqueta 16200 como etiqueta externa. Esta etiqueta indica que se quiere alcanzar el elemento que tenía un SID-Prefix 16200, valor el cual según la Tabla 4.1 se asignó al elemento PE2. En caso de utilizar señalización por LDP, el elemento P1 deberá realizar un SWAP de las etiquetas para llegar a PE2, sin embargo, el valor se mantiene como vemos en la Figura 4.8, la cual representa una captura de paquetes entre los elementos P1 y P2.

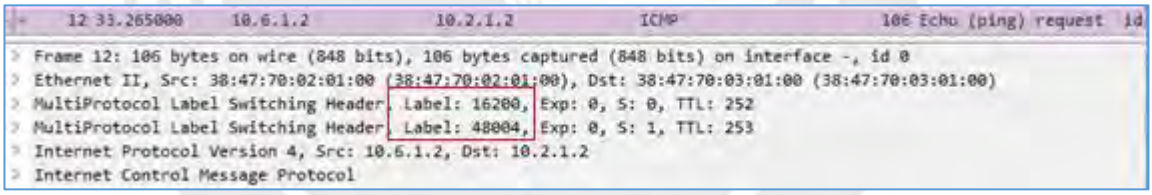

Fig. 4.8 Detalle de conmutación vía SR P1 – P2

En este punto observamos la primera ventaja de SR frente a LDP. La información necesaria para el envío de paquetes se ve reducida considerablemente. Es necesario únicamente que PE1 introduzca la etiqueta 16200 para que el resto de elementos pueda tomar las decisiones de re-envío de paquetes:

```
<PE1>disp segment-routing prefix mpls forwarding label 16200
verbose
Segment Routing Prefix MPLS Forwarding Information
------------------------------------------------------------
```

```
Role : I-Ingress, T-Transit, E-Egress, I&T-Ingress And Transit

Prefix             Label      OutLabel   Interface
NextHop          Role  MPLSMtu   Mtu     State
------------------------------------------------------------
12.12.12.12/32     16200      16200      Eth1/0/1
192.168.131.1    I&T   ---       1500    Active
Protocol : OSPF          SubProtocol : -             Process ID
: 1
Cost     : 2             Weight      : 0             UpdateTime
: 2020-10-18 15:30:30.711
BFD State: --
Label Stack (Top -> Bottom): { 16200 }
```

En el escenario donde todas las interfaces están en UP y los costos OSPF tienen el valor de 1 para cada una de las interfaces, el mejor camino para llegar a PE2 desde PE1 es a través de P3 (interfaz Eth1/0/1 en PE1), esto dado que el costo es de 2, frente a un costo de 3 en el camino PE1-P1-P2-PE2.

4.6 Balanceo de Tráfico

Sin embargo, una de las ventajas mencionadas anteriormente de la implementación de MPLS-SR era que el balanceo de carga en escenarios MECP, se dan automáticamente. Modificaremos manualmente los costos de las interfaces para demostrar este escenario. Los costos OSPF serán configurados manualmente en la interfaz y los valores se indican en la Figura 4.9. Ejemplo de configuración en PE1:

```
interface ether1/0/0
  ospf cost 10
 interface ether1/0/1
  ospf cost 15
```

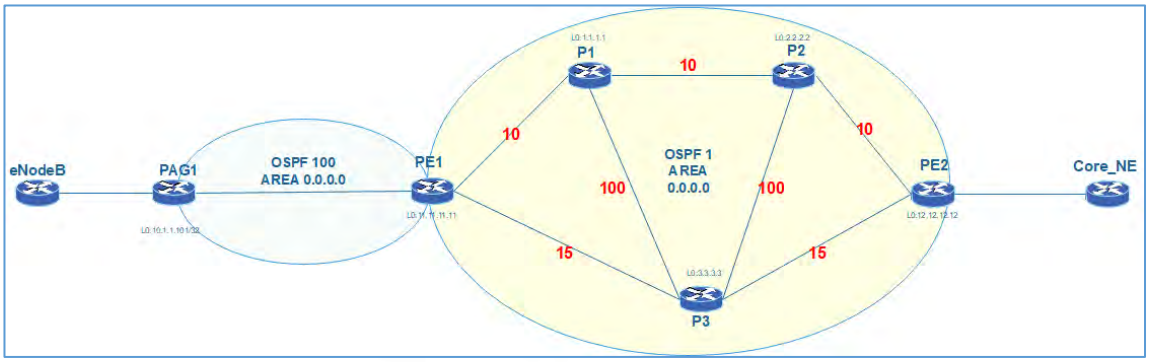

Fig. 4.9 Detalle de costos OSPF para ECMP PE1-PE2

Una vez modificados los valores de costos OSPF, verificamos la tabla de enrutamiento de PE1, donde observamos que existen dos caminos con el mismo costo (30) hasta PE2 (12.12.12.12) a través de dos interfaces Ethernet 1/0/0 y 1/0/1:

```
12.12.12.12/32  OSPF  10   30 D 192.168.131.1 Ethernet1/0/1
                OSPF  10   30 D 192.168.111.1 Ethernet1/0/0
```

En el escenario de LDP, aun existiendo dos caminos de mismo costo encontrados por el IGP, el LSP se establece únicamente por una de las interfaces. Para realizar balanceo de tráfico se requiere de la implementación de túneles de ingeniería de tráfico, los cuales deben ser especificados manualmente.

Para el caso de SR observamos que ahora se tienen dos formas de alcanzar el SID 16200, dado que SR utiliza el IGP (en este caso OSPF) para la elección de la mejor ruta, al encontrar dos rutas, utiliza las dos disponibles automáticamente:

```
Segment Routing Prefix MPLS Forwarding Information
------------------------------------------------------------
Role : I-Ingress, T-Transit, E-Egress, I&T-Ingress And Transit

Prefix            Label      OutLabel   Interface
NextHop          Role  MPLSMtu   Mtu     State
```

```
------------------------------------------------------------
12.12.12.12/32      16200      16200      Eth1/0/0
192.168.111.1     I&T    ---        1500     Active
Protocol : OSPF           SubProtocol : -             Process ID
: 1
Cost      : 30            Weight      : 0             UpdateTime
: 2020-10-18 15:41:32.002
BFD State: --
Label Stack (Top -> Bottom): { 16200 }

Prefix              Label      OutLabel   Interface
NextHop           Role  MPLSMtu   Mtu      State
------------------------------------------------------------
12.12.12.12/32      16200      16200      Eth1/0/1
192.168.131.1     I&T    ---        1500     Active
Protocol : OSPF           SubProtocol : -             Process ID
: 1
Cost      : 30            Weight      : 0             UpdateTime
: 2020-10-18 15:40:17.981
BFD State: --
Label Stack (Top -> Bottom): { 16200 }

Total information(s): 2
<PE1>
```

Realizando pruebas de conectividad desde el elemento eNodeB hacia el Core_NE, se envían cuatro paquetes ICMP, En la Figura 4.10 se valida por captura de paquetes el balanceo de carga por igual: dos paquetes entre los elementos PE1 y P1 y dos paquetes entre los elementos PE1 y P3

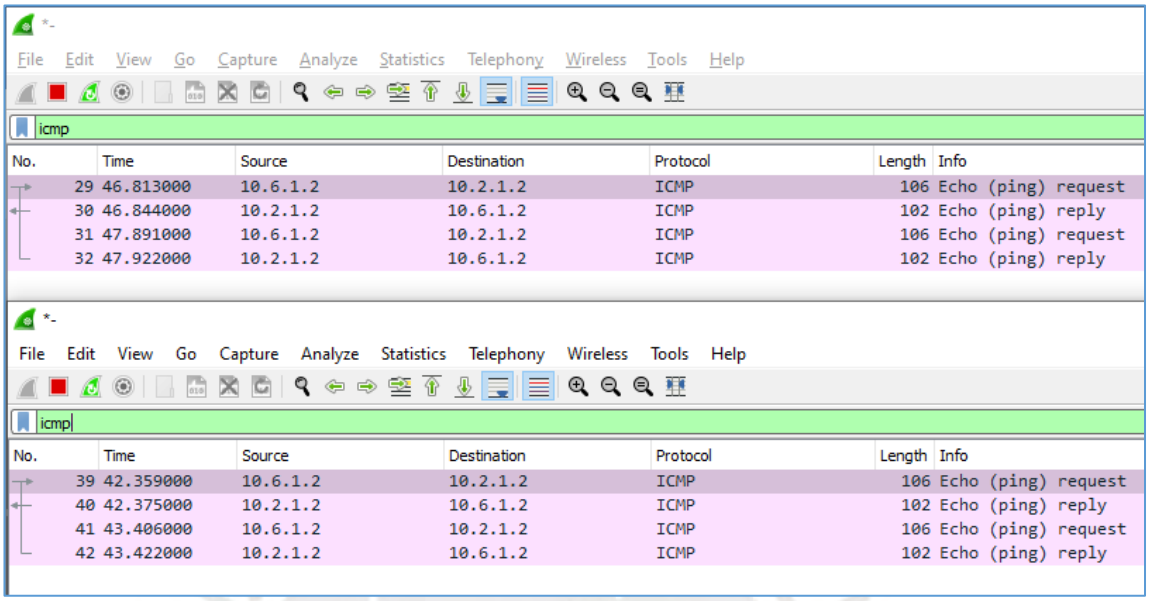

Fig. 4.10 Detalle de paquetes validando balanceo de carga.

4.7 Implementación de túneles de MPLS-SR TE

En nuestro escenario, todos los paquetes tendrán un comportamiento de balanceo de carga, independientemente del tipo de tráfico, tal cual se observa en la Figura 4.11.

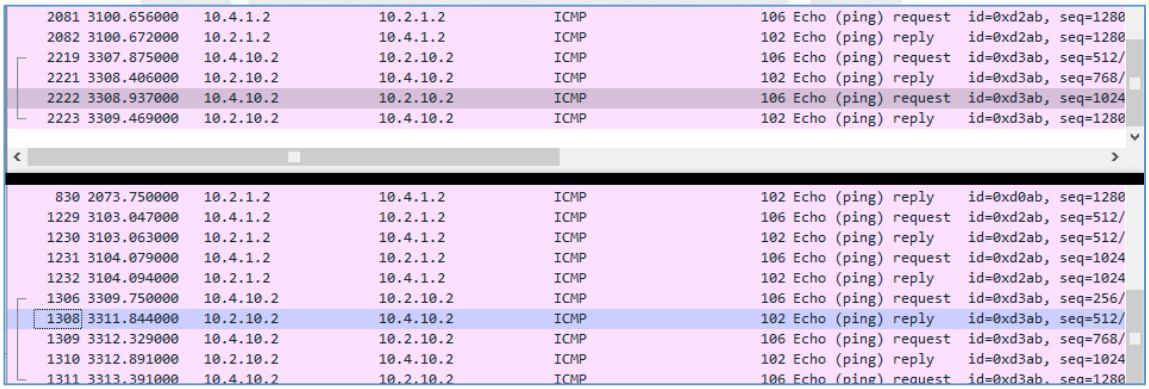

Fig. 4.11 Balanceo de tráfico entre PE1, P1 y P3.

Se requiere que el tráfico de señalización siga el camino PE1 – P1 – P2 – PE2, y que el tráfico de voz siga el camino balanceado. Para este objetivo, es necesario establecer

túneles de ingeniería de tráfico aplicado en la vpn de señalización. Hay que tomar en cuenta que los túneles son unidireccionales, por los cuales, para controlar el tráfico de ida y retorno, es necesario configurar dos túneles, uno en cada extremo.

Previo a la habilitación de los túneles, verificamos que el envío de paquetes se realiza a través de las interfaces físicas, desde el punto de vista de PE2:

```
[~PE2]disp ip routing-table vpn-instance signaling
Destination/Mask Proto Pre Cost Flags NextHop Interface
10.4.1.0/30  IBGP  255  0 RD  11.11.11.11     Ethernet1/0/0
             IBGP  255  0 RD  11.11.11.11     Ethernet1/0/1
```

Como ejemplo, se muestra la configuración de túneles de ingeniería de tráfico del elemento PE2 y la activación sobre la vpn de señalización.

```
explicit-path to_PE1_signaling
 next sid label 16002 type prefix
 next sid label 16001 type prefix
 next sid label 16100 type prefix
#
interface Tunnel1
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 11.11.11.11
 mpls te signal-protocol segment-routing
 mpls te tunnel-id 1
 mpls te path explicit-path to_PE1_signaling
#
tunnel-policy te_signaling
 tunnel select-seq sr-te load-balance-number 1
#
ip vpn-instance signaling
 tnl-policy te_signaling
```

Analizando la tabla de enrutamiento de ambas VPNs en el elemento PE2, observamos que para la vpn *signaling*, con destino 10.4.1.0, el tráfico es dirigido por la interfaz Tunnel1, sin embargo para el tráfico de la vpn *voice*, el tráfico se mantiene balanceado:

```
[~PE2]disp ip rout vpn signaling
Destination/Mask  Proto Pre Cost Flags NextHop   Interface

10.4.1.0/30       IBGP  255  0   RD  11.11.11.11  Tunnel1

[~PE2]disp ip rout vpn voice
Destination/Mask Proto Pre Cost Flags NextHop   Interface

10.4.10.0/30  IBGP    255  0  RD  11.11.11.11 Ethernet1/0/0
              IBGP    255  0  RD  11.11.11.11 Ethernet1/0/1
```

Veremos el detalle de la entrada 10.4.1.0 de la vpn de *signaling*:

```
[~PE2]disp ip rout vpn signaling 10.4.1.0 verbose
Destination: 10.4.1.0/30
     Protocol: IBGP               Process ID: 0
   Preference: 255                      Cost: 0
      NextHop: 11.11.11.11         Neighbour: 3.3.3.3
        State: Active Adv Relied         Age: 00h10m37s
          Tag: 0                    Priority: low
        Label: 48076                 QoSInfo: 0x0
   IndirectID: 0x1000080             Instance:
 RelayNextHop: 0.0.0.0              Interface: Tunnel1
     TunnelID: 0x00000000300000001 Flags: RD
[~PE2]disp tunnel-info tunnel-id 00000000300000001
 Tunnel ID:       0x00000000300000001
 Type:            sr-te
 Name:            Tunnel1
```

```
Destination:     11.11.11.11
Instance ID:     0
Cost:            0
Status:          UP
Out Interface:   Tunnel1
NextHop:        0.0.0.0
```

Se observa que la interfaz de salida para todo tráfico con destino 10.4.1.0 en la vpn de signaling, se enviará a la interfaz Tunnel1, el cual toma un camino establecido por SR-TE.

Validando el comportamiento mediante captura de paquetes observamos que el tráfico generado sobre la vpn de señalización (Origen: 10.4.1.2 y destino 10.2.1.2) es enviado únicamente por el enlace entre PE1-P1-P2-PE2. La figura 4.12 muestra que los paquetes son enviados por el camino indicado (la parte superior es la captura entre PE1 y P1, y la captura inferior es entre PE1 y P3):

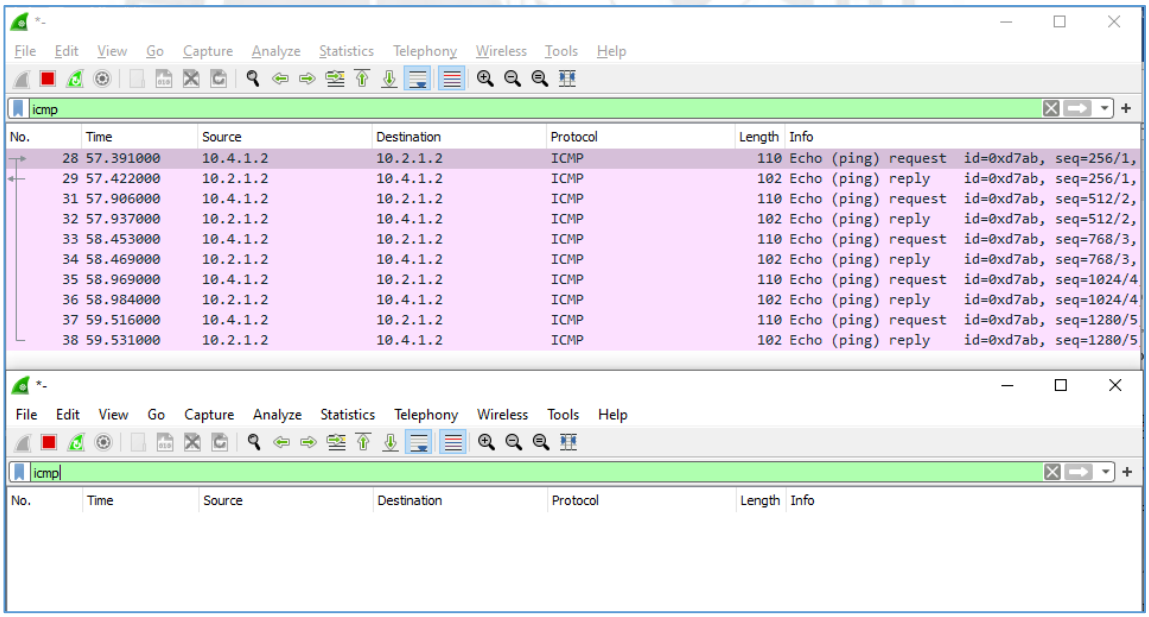

Fig. 4.12 Flujo de señalización por SR-TE

Una importante ventaja de utilizar SR-TE es que los elementos intermedios no requieren almacenar información del túnel, esto es, no asignan etiquetas para el tráfico. Adicionalmente, el primer elemento, en este caso PE1, aplica un stack de etiquetas (segmentos), el cual es el instructivo específico para que los siguientes elementos tomen la decisión al momento de enviar el paquete. El stack de etiquetas lo vemos con más detalle en la figura 4.13:

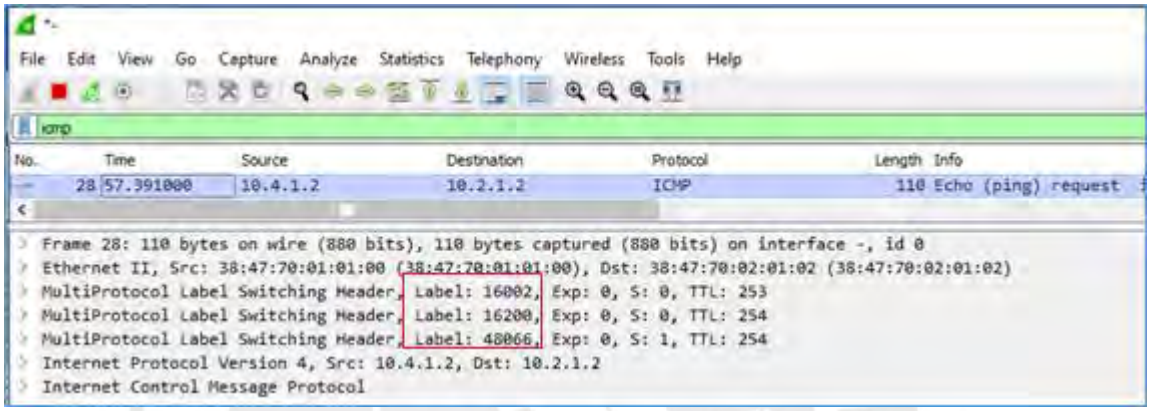

Fig. 4.13 Stack de etiquetas para SR-TE

El elemento PE1 asignó las instrucciones de acuerdo al camino especificado por configuración: P1 (16001) – P2 (16002) – PE2 (16200). En este caso no observamos la etiqueta 16001, puesto que la etiqueta de salida para ese destino es la etiqueta con valor 3 (implicit-null), esto es, se debe de retirar la etiqueta cuando el paquete sale del elemento PE1. De esta manera, el PE2 agiliza la decisión de envío de paquete:

```
   Segment Routing Prefix MPLS Forwarding Information
------------------------------------------------------------
Prefix              Label      OutLabel   Interface
NextHop           Role  MPLSMtu   Mtu     State
------------------------------------------------------------------------
-----------------------------------------------
1.1.1.1/32          16001      3          Eth1/0/0
...
```

4.8 Análisis de resultados de simulación Fase 2 SR-MPLS

Observamos que para redes con MPLS Segment Routing, se requiere una instrucción que contenga como mínimo un segmento (el destino), y los elementos intermedios podrán tomar la decisión basada en esa instrucción. Adicionalmente, MPLS-SR no requiere de un protocolo adicional para el intercambio de etiquetas, sino que utiliza a los protocolos de IGP para el intercambio de información (SIDs), para el presente caso en específico, OSPF utiliza LSAs tipo 10 por la cual anuncia información de los SIDs. De esta manera se reduce la complejidad al diseñar y desplegar una red MPLS. La asignación manual de los SIDs en cada uno de los elementos permite también que cada elemento de la red tenga un identificador único, permitiendo establecer caminos específicos de manera sencilla.

Así mismo, es posible y sin necesidad de aplicar nuevas configuraciones como establecer túneles de ingeniería de tráfico, el balanceo de tráfico a través de la red a por caminos que tengan el mismo costo (calculado por el IGP), permitiendo la mejor utilización de los recursos de la red.

Con la implementación básica de Segment Routing, hemos logrado solventar las tres deficiencias de la arquitectura Seamless-MPLS indicadas en el capítulo 3, inciso 3.4.

MPLS-SR es fundamental para la transición y migración a redes del tipo SDN por la forma de asignación de identificadores y funcionalidades. Mediante la conexión a un controlador, se pueden configurar servicios extremo-a-extremo, basado en parámetros de ancho de banda, latencia, jitter y packet loss. Adicionalmente, es posible el aprovisionamiento de servicios a través de una GUI, donde el operador solo debe determinar el camino que prefiera para establecer un servicio. Esto reduce el tiempo para la habilitación de un servicio comparado con arquitecturas tradicionales, relevante en la implementación de servicios de redes 5G.

4.9 Lineamientos para migración de Seamless-MPLS a MPLS-SR

La migración de una arquitectura Seamless-MPLS a Segment Routing no debe considerarse disruptiva, esto es, no debe interpretarse como un procedimiento en que ambas arquitecturas no puedan co-existir durante todo el proceso de migración. Esto permite que la transición hacia Segment-Routing tenga una afectación mínima desde el punto de vista del usuario final y que no requiera grandes cambios que pudieran afectar la continuidad del servicio.

En primer lugar, es necesario validar que los equipos involucrados soporten Segment-Routing. Caso contrario, se deben considerar escenarios híbridos (SR + LDP)

Resumiremos el proceso de implementación de una red basada en Seamless-MPLS:

1. Configuración de IPs (interfaces físicas, lógicas)
2. Configuración de Protocolo IGP (OSP, ISIS)
3. Configuración de MPLS + LDP como protocolo de intercambio de etiquetas MPLS.
4. Configuración de Protocolo MP-BGP para intercambio de información de rutas VPNV4, donde el elemento P3 funcionará como RR de la red.
5. Habilitación de BGP+Label en todos los vecinos i-BGP, desde la red de acceso, agregación y core.
6. De manera opcional, habilitación de MPLS RSVP-TE para establecimiento de túneles de ingeniería de tráfico.

Para la implementación de Segment-Routing, sobre una red ya establecida, podemos resumir en los siguientes pasos:

1. Habilitación de Segment Routing (SR) de manera Global
2. Habilitación de SR en el proceso OSPF/IS-IS y asignación del SGRB.
3. Habilitación de prefix-sid sobre la interface loopback por cada elemento de la red.
4. Verificación de información de prefijos compartidos por SR en la red.

En este punto, la red se encuentra distribuyendo SIDs de SR utilizando el protocolo IGP, pero los LSPs entre elementos LERs, se establecen aún por medio de LDP (o RSVP-

TE). La decisión de los equipos LSRs se basan en etiquetas distribuidas por protocolo LDP. El comportamiento de preferencia de LDP sobre SR es configurable. Una vez terminemos las verificaciones en donde todos los elementos conocen los SIDs de toda la red, podemos proceder a ejecutar los siguientes pasos:

1. Configurar manualmente en los elementos mayor preferencia de SR sobre LDP/RSVP-TE.
2. Eliminar LDP/RSVP-TE de la red.

Debido a las bajas prestaciones de los elementos en la red de acceso, pueden existir en la red equipos que no soporten SR como protocolo, esto requiere plantear un diseño de red híbrida, utilizando LDP en aquellos elementos que no soporten SR. Finalmente, el elemento de red interpreta y toma decisiones en base a etiquetas (mantiene la naturaleza de MPLS), sin embargo, algunas funcionalidades como conexión a un controlador y establecimiento de túneles SR-TE no podrán ser factibles en elementos que no soporten SR. A pesar de ello, no se verán afectados los servicios de aquellos elementos que no soporten SR. En un inicio, es recomendable que todos los elementos de los anillos de Core soporten SR.

Los esquemas de migración pueden basarse en función al rol que cumple el elemento de Red. Por ejemplo, se recomienda la habilitación primero en el Core, luego en los anillos de agregación y finalmente en los anillos de acceso.

CONCLUSIONES y RECOMENDACIONES

a. La presente tesis muestra mediante simulaciones en software, el comportamiento de una red basado en Arquitectura Seamless MPLS y una red basada en Arquitectura MPLS-Segment Routing.
b. En base a la identificación de escenarios típicos de una red de un proveedor, y tomando en consideración las limitantes de procesamiento del simulador, se establece una topología que permite analizar el comportamiento de los protocolos de una manera cercana a una red típica de un proveedor de servicios. La naturaleza del funcionamiento de los protocolos involucrados se mantiene aún cuando aumentan las cantidades de elementos que intervienen en la red.
c. Se detallaron los pasos recomendados para que planificar la migración de Seamless-MPLS a Segment Routing.
d. Se describieron los procesos de configuración para la habilitación de una Arquitectura basada en Seamless MPLS, con el fin de observar directamente las desventajas de la técnica tradicional: la necesidad de un protocolo adicional (LDP, RSVP) para intercambio de etiquetas MPLS; asignación dinámica y aleatoria de etiquetas que complica la operación, mantenimiento y análisis de puntos de falla, dado que cada elemento puede manejar una distinta tabla de mapeo de etiquetas MPLS; y, subutilización de enlaces cuando se establecen LSPs mediante LDP, por la dificultad de masificar la solución de MPLS-TE para balanceo de tráfico y optimización de recursos.
e. Se propone un proceso de configuración para la habilitación de una Arquitectura basada en MPLS - Segment Routing (SR-Best Effort y SR-Traffic Engineering), a través del cual se identifican los puntos fuertes de esta arquitectura: se extienden las capacidades del protocolo IGP (sea OSPF o IS-IS) para utilizarlo en la distribución de etiquetas; los segmentos del nodo son manualmente asignados, por tanto hay un mayor control del camino que tomará un paquete; el balanceo de carga para caminos

con múltiples opciones con costos iguales se hace de manera automática, utilizando de mejor manera los recursos de la red.

f. El capítulo IV parte de las configuraciones realizadas en el capítulo III, realizando la migración de una arquitectura Seamless - MPLS a una basada en SR-MPLS. Los resultados se contrastan entre las lecturas de indicadores observados en el elemento con capturas de paquetes realizadas en las interfaces de inter-conexión, identificándose el comportamiento de cada protocolo involucrado.

g. Las mejoras identificadas en la arquitectura SR-MPLS permite que la transición hacia una red del tipo SDN, sea de una manera más transparente, siendo SDN la plataforma de transporte recomendada para redes 5G.

TRABAJOS FUTUROS

La presente tesis ofrece diversas áreas para investigaciones futuras, como:

- Implementar un orquestador de Red para emular una red del tipo SDN, realizando aprovisionamiento de servicios mediante una GUI, aplicando protocolos del tipo PCEP (Path Computation Element Protocol), integrando a soluciones del tipo OpenFlow (mediante aplicaciones OpenDaylight) y Pathman.
- Realizar estudios de soluciones basadas Segment Routing para redes del tipo IPv6 como SRv6.

BIBLIOGRAFÍA

[1] Maila, Marius, Victor, “Segment Routing”, IEEE, 2017

[2] Castoldi, Giorgetti, Sgambelluri, “Segment Routing in Multi-Layer Networks”, IEEE, 2017

[3] Guedrez, Dugeon, “Demonstration of Segment Routing with SDN Based Label Stack Optimization”, IEEE, 2017

[4] Guedrez, Dugeon, “A New Method For Encoding MPLS Segment Routing TE Paths”, IEEE, 2017

[5] Castoldi, Giorgetti, Sgambelluri, “Segment Routing for Effective Recovery and Multi-domain Traffic Engineering”, IEEE, 2017

[6] J.Moy, IETF, RFC 2328, OSPF version 2, 1998

[7] Oran, IETF, RFC 1142, OSI IS-IS Intra-domain Routing Protocol, 1990

[8] Rekhter, Li, Hares , IETF, RFC 4271, A Border Gateway Protocol 4 (BGP-4), 2006

[9] Bates, Chandra, IETF, RFC 1966, BGP Route Reflection An alternative to full mesh IBGP, 1996

[10] Rosen, Viswanathan, Callon IETF, RFC 3031, Multiprotocol Label Switching Architecture, 2001

[11] Redes Definidas por Software, http://redessdn.blogspot.com/2016/12/mpls.html, 2016

[12] Anderson, Minei, Thomas, IETF, RFC 5036, LDP Specification, 2007

[13] Bates, Chandra, Katz, IETF, RFC 4760, Multiprotocol Extensions for BGP-4, 2007

[14] Rekhter, Rosen , IETF, RFC 3107, Carrying Label Information in BGP-4,

[15] Huawei Technologies CO. “Seamless MPLS Feature Description”, Agosto 2019

[16] Filsfils, Previdi, IETF, RFC 8402, Segment Routing Architecture, 2018

[17] Filsfils, Previdi, IETF, RFC 8665, OSPF Extensions for Segment Routing, 2019

[18]Babiarz, Chan, Baker, IETF, RFC 4594, Configuration Guidelines for DiffServ Service Classes, 2006

[19] Huawei Technologies CO. “Traffic Policing and Traffic Shaping Description”, Agosto 2020

[20] Levi, Meyer, IETF, RFC 3413, Simple Network Management Protocol (SNMP) Applications,

[21] Gerhards, IETF, RFC 5424, The Syslog Protocol, Marzo 2009

[22] Aboba, Wood, IETF, RFC 3539, Authentication, Authorization and Accounting (AAA) Transport Profile, Junio 2003

[23] Mills, Delaware, IETF, RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, Junio 2010

[24] Ylonen, Lonvick, IETF, RFC 4254, The Secure Shell (SSH) Connection Protocol, Enero 2006