UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

DISEÑO Y SIMULACIÓN DE UNA RED BACKHAUL BASADA EN IP/MPLS DE ALTA DISPONIBILIDAD UTILIZANDO TÉCNICAS DE INGENIERÍA DE TRÁFICO Y CALIDAD DE SERVICIO

AUTOR:

Ing. Leonidas Alberto Moran Carreño

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

Ing. Ilen Rivero Pouymiro. Msc

Guayaquil, a los 7 días del mes de junio del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por LEONIDAS ALBERTO MORAN CARREÑO como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

MSc. Ilen Rivero Pouymiro

DIRECTOR DEL PROGRAMA

MSc. Manuel Romero Paz

Guayaquil, a los 7 días del mes de junio del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, LEONIDAS ALBERTO MORAN CARREÑO

DECLARO QUE:

El trabajo de Titulación **"DISEÑO Y SIMULACIÓN DE UNA RED BACKHAUL BASADA EN IP/MPLS DE ALTA DISPONIBILIDAD UTILIZANDO TÉCNICAS DE INGENIERÍA DE TRÁFICO Y CALIDAD DE SERVICIO"** previa a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 7 días del mes de junio del año 2021

EL AUTOR

_____
LEONIDAS ALBERTO MORAN CARREÑO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, LEONIDAS ALBERTO MORAN CARREÑO

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación, **"DISEÑO Y SIMULACIÓN DE UNA RED BACKHAUL BASADA EN IP/MPLS DE ALTA DISPONIBILIDAD UTILIZANDO TÉCNICAS DE INGENIERÍA DE TRÁFICO Y CALIDAD DE SERVICIO"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

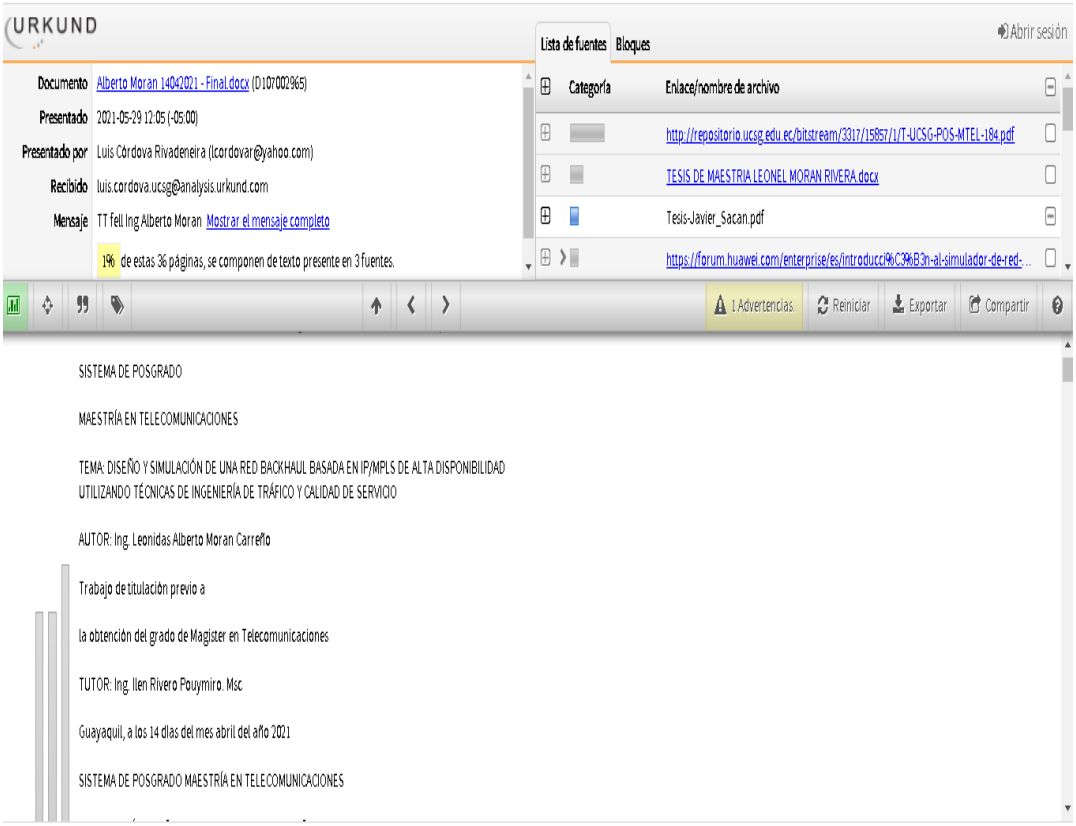
Guayaquil, a los 7 días del mes de junio del año 2021

EL AUTOR

_____

LEONIDAS ALBERTO MORAN CARREÑO

REPORTE URKUND



Dedicatoria

Dedicatoria a Dios por haber guiado de mis pasos en mi vida, tanto personal como profesional, y por permitir culminar esta nueva etapa de mi formación profesional, nada de esto hubiera sido posible sin el acompañamiento y guía de él.

A mis padres y hermanas, por confiar en mí y apoyarme en todas mis decisiones, y a su vez brindándome ese apoyo incondicional para seguir avanzando y no declinar en tiempos complejos.

A mis amigos de infancia, y a los amigos que en el transcurso de la vida educativa y profesional he realizado, los cuales de alguna manera formaron parte de esto, dándome ánimos a seguir, que todo sacrificio tiene su recompensa.

Morán Carreño, Leonidas Alberto

Agradecimientos

Agradecimiento infinito a DIOS, por oportunidades y bendiciones que me brinda a diario.

Allcompu Manta, empresa que me vio crecer como persona y como profesional, a todo el personal técnico y administrativo, que, con sus experiencias y conocimientos adquirí destrezas y habilidades las cuales me desarrollaron como profesional, y me permitió empezar y concluir este estudio de postgrado.

A la Universidad Católica Santiago de Guayaquil, Escuela de Postrado, y a todos los docentes que compartieron sus conocimientos y experiencias profesionales para así poder finalizar y alcanzar nuestros estudios de cuarto nivel.

A MSc. Ilen Pouymiro, por ser mi directora de tesis, y apoyarme en todo este proceso, que con su experiencia y dedicación pudo hacer posible que finalice este trabajo de titulación de una manera exitosa.

Morán Carreño, Leonidas Alberto

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Ilen Rivero Pouymiro
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

_____

MSc. Edgar Quezada Calle
REVISOR

RESUMEN

Debido a que los proveedores de servicios (SP, Services Providers) crecen día a día, esto representa consumo de recursos de red como ancho de banda, por lo cual, la demanda de tráfico crece exponencialmente debido a la gran cantidad de tráfico que atraviesa por la red. Para satisfacer la demanda de tráfico de red en los proveedores de servicios de Internet, es oportuno y necesario establecer mecanismos que manipulación de tráfico con el objetivo de minimizar la congestión, perdida de paquetes y el encolamiento de tráfico. Para minimizar el retardo, las redes de los SP deben implementar mecanismos que aporten con este objetivo, MPLS aporta de manera significativa el poder minimizar el retardo y, a su vez, brinda características importantes para el despliegue de tecnologías como L3VPN y MPLS TE. La disponibilidad y la tolerancia a fallos es crucial en un entorno de proveedores de servicios. Por tal razón, se deben desarrollar estrategias de ingeniería de tráfico contribuyan a minimizar y prevenir eventos como perdida de paquetes, latencia y cuellos de botella. La calidad de servicios en entornos donde la demanda de tráfico es constante y de gran tamaño, resulta de vital importancia establecer mecanismos de calidad de servicio que controlen el tráfico de red y minimicen la congestión, el retardo y fluctuación de retardo.

Palabras clave: MPLS, MPLS-TE, QOS, ANCHO DE BANDA, JITTER, CONGESTIÓN, RECURSOS.

ABSTRACT

As service providers (SP, Services Providers) grow day by day, this represents consumption of network resources such as bandwidth, therefore, the demand for traffic grows exponentially due to the large amount of traffic that passes through network. To satisfy the demand for network traffic in Internet service providers, it is timely and necessary to establish mechanisms that manipulate traffic in order to minimize congestion, packet loss and traffic queuing. To minimize delay, SP networks must implement mechanisms that contribute to this objective, MPLS significantly contributes to being able to minimize delay and, in turn, provides important characteristics for the deployment of technologies such as L3VPN and MPLS TE. Availability and fault tolerance is crucial in a service provider environment. For this reason, traffic engineering strategies must be developed to help minimize and prevent events such as packet loss, latency, and bottlenecks. The quality of services in environments where the demand for traffic is constant and large, it is vitally important to establish quality of service mechanisms that control network traffic and minimize congestion, delay and jitter.

Keywords: MPLS, MPLS-TE, QOS, BANDWIDTH, JITTER, CONGESTION, RESOURCES.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO 1 . DISEÑO DE LA INVESTIGACIÓN

En el capítulo 1 se describirá los elementos fundamentales de la investigación, la cual está dividida en: Introducción, antecedentes, definición del problema, justificación, objetivos, hipótesis y la metodología a utilizar.

1.1 Introducción

Actualmente, las empresas de Tecnologías de la Información (TI) y los proveedores de servicios de Internet, telefonía móvil o fija e incluso empresas de servicios de video on demand, enfrentan grandes retos para satisfacer la demanda de tráfico de miles de clientes. Cada cliente desea tener ancho de banda dedicado y disfrutar del servicio de llamadas, conexión a Internet o simplemente disfrutar jugando en línea o viendo una película online en alta definición.

Para que los proveedores de servicios puedan satisfacer esta demanda de tráfico y al mismo tiempo ser competitivos en el mercado, necesitan herramientas que les permitan diferenciar y manejar adecuadamente los distintos tipos de tráfico o servicios que atraviesan su red. Esto con el objetivo de optimizar sus recursos de red, principalmente el ancho de banda y la capacidad de procesamiento de los equipos de red.

El protocolo de enrutamiento IS-IS *(Intermediate System – Intermediate System)* es un protocolo de tipo IGP *(Interior Gateway Protocol)* de tipo de estado de enlace, el cual ofrece alta disponibilidad, escalabilidad, tiempos de convergencia mínimos y un rendimiento óptimo para los proveedores de servicios para manejar una red *IP Backhaul* amplia, esto con el fin de desplegar los múltiples servicios como voz, datos y video.

Una de las funcionalidades que ofrece la conmutación de etiquetas multiprotocolo o MPLS (Multiprotocol Label Switching) es la utilización de técnicas ingeniería de tráfico o TE *(Traffic Engineering)*, las cuales permiten la manipulación de rutas para el transporte de datos de acuerdo con los criterios que el administrador de la red considere. Esto ofrece varios

beneficios, como crear túneles específicos de acuerdo con los servicios que ofrece el proveedor y poder mover tráfico de red por algún túnel menos congestionado. De manera que, apoya a ofrecer un servicio de calidad.

La calidad de servicio o QoS *(Quality of Service)* es fundamental para su correcta prestación y el cumplimiento de los niveles de acuerdos de estos, lo que permitirá que siempre esté disponible y con la mejor calidad ofrecida.

1.2 Antecedentes

A diferencia de crisis pasadas, el Covid-19 ha impactado prácticamente a la totalidad de individuos y organizaciones a nivel mundial, generando procesos de adaptación y reinvención que se evidencian en acciones centradas en la transparencia, la ética, solidaridad y uso efectivo de recursos pensando más allá del corto plazo e impulsando la digitalización en términos de uso y transacciones en línea, superando el temor a nuevos canales de venta, transacción, servicio y comunicación. Entre 2019 y 2020 se ha multiplicado la cantidad de usuarios que realizan transacciones online, del 2% al 10%, demostrando el potencial de mercado y oportunidad para marcas que todavía no integran su oferta a plataformas digitales eficientes. Siendo importante aclarar que una transacción digital no es una compra en línea, es una operación realizada a través de terminales digitales (Ponce, 2021).

El tráfico transportado por Internet aumenta rápidamente en conjunto con imponentes requisitos de confiabilidad, calidad de servicio y manejabilidad. Esta tendencia obliga a la tecnología de redes a venir con nuevos enfoques y soluciones. MPLS ha surgido como una tecnología que puede proporcionar muchas de las funcionalidades asociadas con ATM (*Asycronous Transfer Mode)*. En MPLS, los paquetes se encapsulan, al ingresar puntos, con etiquetas que luego se utilizan para reenviar los paquetes a lo largo de los caminos conmutados por etiquetas o LSP (*Label Switched Paths)* (Li, 1999).

Los protocolos *IS-IS* y OSPF (*Open Shortest Path First)* fueron diseñados para admitir enrutamiento en capa de red con servicio de

datagramas. *OSPF* fue diseñado para el Protocolo de Internet (IP), que es una red protocolo de en la suite TCP/IP. IS-IS fue diseñado originalmente para el Protocolo de Capa de Red Sin Conexión o CLNP (Connectionless Network Layer Protocol, por sus siglas en inglés), el protocolo de capa de red de datagramas en la suite de la ISO (*Intemational Organization for Standardizatio).* Sin embargo, puede soportar la capa de red del Protocolo *IP*, así como la capa de red *IS0* (Mijeong Yang, 2003).

Las redes de gran escala siguen siendo un gran desafío para la gestión y garantizar un buen nivel de Calidad de Servicio por sus términos en inglés *Quality of Service* (QoS) y sobre todo optimizar (uso racional de los recursos de la red). MPLS es utilizado principalmente en la columna vertebral de los proveedores de servicios de Internet, debe cumplir con uno de los desafíos principales. SDN (*Software-Defined Network*), es un paradigma que permite, a través del principio de orquestación y abstracción de capas, gestionar redes de gran escala mediante protocolos específicos (Bahnasse et al., 2018).

Los *Request for Comments* (RFC), son una serie de publicaciones del grupo de trabajo de ingeniería de Internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. Y comentarios e ideas sobre estos (RFC Editor).

1.3 Definición del problema

El incremento del uso de las redes de telecomunicaciones debido a la demanda de tráfico hacia Internet eleva el consumo de recursos de procesamiento en las redes actuales, por lo que se generan malas experiencias en los usuarios debido a la falta de calidad de servicio y de mecanismos que aporten al transporte de datos eficiencia y agilidad.

1.4 Planteamiento del problema

Las redes de comunicaciones están basadas de manera predeterminada en el mejor esfuerzo, toman decisiones de enviar tráfico de red basados en las rutas proporcionadas por los protocolos de enrutamiento, sin establecer mecanismos de calidad de servicio.

Por tal motivo, a mayor demanda de transporte de datos, los caminos proporcionados por los protocolos de enrutamientos serán saturados, mientras otros caminos no son utilizados por la naturaleza de los protocolos, lo que genera mala experiencia de usuario y una inadecuada gestión de los recursos de la red.

1.5 Justificación del problema

Debido a la pandemia actual se evidencia una disminución de velocidad de banda ancha fija en Ecuador (-19,6%), combinando esto con un incremento de la latencia en la misma tecnología de 11,8% según cifras de Ookla/Speedtest (DATTA, 2020).

Para satisfacer la demanda de tráfico, se deben desarrollar estrategias efectivas de ingeniería de tráfico a fin de prevenir posibles cuellos de botella, minimizar latencia, pérdida de paquetes por saturación de ancho de banda y establecer bases para garantizar la correcta entrega de los servicios con una excelente experiencia de usuario. A su vez aplicar técnicas y herramientas de MPLS-TE para garantizar la implementación y mecanismos de TE en redes basadas en IP/MPLS por donde pasarán múltiples servicios como voz, datos, video y servicios de conectividad corporativa a través de *L2VPN (Layer 2 Virtual Private Network)* o *L3VPN (Layer 3 Virtual Private Network).*

Por tales impulsos, el trabajo va a consistir en tener un enfoque práctico explicativo, donde se pretende demostrar la efectividad de utilizar mecanismos o técnicas de ingeniería de tráfico y calidad de servicio en las redes de los ISP. A su vez, permitirá adquirir habilidades y destrezas para para tener visibilidad completa de las redes, y poder manipular tráfico basado en mejores prácticas para minimizar el consumo de recursos de procesamiento y tener mejor control sobre los dispositivos de red.

1.6 Objetivos de la investigación

En esta sección se indicarán los objetivos específicos que permitirán alcanzar el objetivo general de la investigación a realizar.

1.6.1 Objetivo general

Diseñar y simular una red *Backhaul* basada en IP/MPLS de alta disponibilidad utilizando técnicas de ingeniería de tráfico y calidad de servicio.

1.6.2 Objetivos específicos

- Analizar los fundamentos teóricos y técnicos relacionados con el protocolo de enrutamiento IS-IS así como la arquitectura MPLS, y en conjunto las herramientas de ingeniería de tráfico para la creación de tuneles para transportar datos aplicando calidad de servicio.
- Diseñar una red IP Backhaul de alta disponibilidad basada en IP/MPLS con MPLS-TE y QoS
- Simular el diseño de la red mediante el software EVE-NG y eNSP con dispositivos de Huawei.
- Evaluar los resultados de la red Backhaul IP/MPLS con ingeniería de tráfico y calidad de servicio diseñada.

1.7 Hipótesis

Utilizar una red Backhaul IP/MPLS con técnicas de ingeniería de tráfico y calidad de servicio, aportará para mejorar sustancialmente el rendimiento y aprovechamiento de los recursos de red disponibles; y, la reducción de latencia, pérdida de paquetes y saturación de tráfico en los enlaces, lo que permitirá una correcta gestión de los recursos de la red y una buena experiencia de usuario.

1.8 Metodología de investigación

El tipo de investigación a desarrollar es exploratoria, descriptiva y explicativo-experimental.

Metodología exploratoria por la recolección de información previa sobre redes de transporte con ingeniería de tráfico y mecanismos de QoS.

Descriptiva debido a que se estudiarán conceptos de ingeniería de tráfico y calidad de servicio sobre una red *Backhaul* IP/MPLS.

Explicativo-experimental, ya que se someterá a simulación los conceptos revisados y las técnicas aplicadas, para esto nos basaremos en el emulador EVE-NG y eNSP para simular dispositivos de red del fabricante Huawei.

Adicionalmente será inductivo – deductivo para la selección y caracterización de datos, analítico – sintético debido a que el objetivo general se dilatará en objetivos específicos, para al concluir recolectando toda esta información y por medio de la síntesis encontrar la solución a la problemática, y con un enfoque cuantitativo el cual permitirá medir las funcionalidades implementadas en el diseño propuesto.

CAPITULO 2 . MARCO TEÓRICO

En el presente capítulo se abordará la fundamentación teórica como base fundamental para la realización de la investigación.

2.1 Redes de telecomunicaciones

Las redes de telecomunicaciones son sistemas compuestos por infraestructuras alámbricas e inalámbricas. Cual objetivo fundamental es transportar datos desde un punto inicial como referencia hacia un destino en particular, garantizando la integridad de estos durante todo el camino.

Las redes se definen como un conjunto de nodos en los cuales se resuelve o procesa los datos, y un conjunto de enlaces o canales que proporcionan conexión de los nodos entre sí, los cuales permiten el transporte de información de un origen a un destino.

A su vez, las redes de telecomunicaciones actualmente tratarán de garantizar la correcta entrega de datos entre un origen y destino, cumpliendo con los principios fundamentales de disponibilidad, integridad y confidencialidad.

2.2 IP Backhaul

La principal función de una red *IP Backhaul* es transportar datos que son originados desde el núcleo hacia la red de acceso o incluso desde la capa de acceso hacia la misma como se muestra en la Figura 2-1.

Figura 2-1: IP Backhaul

Fuente: Elaborado por el autor

Las redes *IP Backhaul* están basadas en el modelo *TCP/IP*, por tal motivo funcionan sobre protocolos *Ipv4* o *Ipv6*. Además, poseen elementos o funcionalidades ubicadas en cada capa del modelo *TCP/IP*; en la capa de acceso al medio se encuentran medios de transmisión alámbricos como

cobre y fibra óptica, e inalámbricos cuya representación son las microondas.

2.2.1 Arquitectura de red IP Backhaul, Interconexión regional

En su mayoría, el despliegue de redes *IP Backhaul* por parte de los proveedores de servicio de Internet es muy amplia, ya que puede estar instalada a nivel cantonal, provincial y a nivel país.

Para la interconexión de las diferentes redes *IP Backhaul* se utiliza una red troncal que, por lo general está desplegada por fibra óptica de gran capacitad, y con tecnología de fibra óptica WDM (*Wavelength Division Multiplexing*, multiplexación por división de longitud de onda*)* o DWDM *(Dense Wavelength Division Multiplexing,* multiplexado denso por división en longitudes de onda*)* (Ming Xia, 2010*).*

2.2.2 Arquitectura Backhaul Móvil

La arquitectura Backhaul en una red móvil, a nivel general, es una red IP Backhaul que interconecta una Red de Acceso Radio o RAN (*Radio Access Network)* con el núcleo de la red.

La arquitectura en redes móviles está compuesta por redes como UMTS *(Universal Mobile Telecommunications*, Sistema universal de telecomunicaciones móviles*),* LTE *(Long Term Evolution*, evolución a largo plazo) o LTE+ *(Long Term Evolution Advance*, evolución a largo plazo avanzado*).* Dichas redes son denominadas como RAN con la cual hay una interconexión con el núcleo de la red, que permitirá el tránsito de los datos partiendo de la conjunción de diferentes tecnologías (Ayala Abarca Ana Cristina, 2019).

2.2.3 IP Backhaul en Telefonía Móvil

En las redes de telefonía móvil, las redes IP Backhaul, se comportan como una red de tránsito. Permiten comunicar varios elementos de la red entre sí.

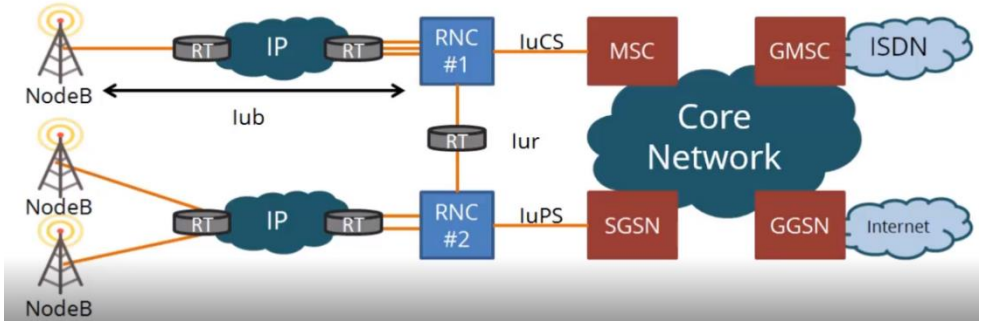


Figura 2-2:IP Backhaul en Telefonía Móvil
Fuente: Telecapp, IP Backhaul

Como se muestra en Figura 2-2 los *NodeB* son los que proporcionan conexión a los dispositivos finales, los elementos *NodeB* se conectan con elementos de controlador de red radio o RNC (*Radio Network Controller*), a través de una interfaz lógica llamada *Iub;* cuya interfaz es una ruta compuesta por varios routers que forman parte de la red IP Backhaul. Lo mismo sucede cuando se comunican elementos entre sí. Para comunicar dos elementos RNC entre sí, se hace a través de una interfaz lógica llamada Iur. Para la comunicación con el núcleo de la red, esto es posible mediante las interfaces lógicas IuCS o IuPS dependiendo si los datos son conmutados por circuitos o por paquetes respectivamente.

2.3 Protocolos de enrutamiento

Son utilizados para facilitar el intercambio de información o prefijos de enrutamiento entre dispositivos de capa 3. Estos protocolos permiten a los *routers* o *switches* de capa 3 compartir información de manera dinámica sobre redes remotas y a su vez, agregar la información automáticamente en sus tablas de enrutamiento (Brad Edgeworth, 2020). Entre de los protocolos que se verá está IS-IS y OSPF.

2.3.1 Protocolos de tipo vector distancia

En este tipo de protocolos, las rutas son publicadas como vectores de distancia y de dirección. La distancia se puede definir en términos de una métrica como el conteo de saltos, y la dirección, hace referencia del siguiente *router* por el cual el tráfico alcanzará el destino o por la interfaz de salida que conmutarán los datos. Normalmente estos protocolos utilizan

algoritmos de Bellman Ford para determinar el mejor camino hacia una red de destino.

Algunos de los protocolos de tipo vector distancia son:

- RIP
- EIGRP

2.3.2 Protocolos de tipo estado de enlace

Los protocolos de enrutamiento de tipo Estado-Enlace, le permiten a los *routers* construir y tener noción de la topología completa de la red, al reunir información proveniente de todos los demás *routers* vecinos. Se les llama protocolos de tipo estado enlace, porque al usarlos, los *routers* normalmente se encuentran monitoreando el estado de los enlaces con sus vecinos, de tal manera de que cuando ocurra un cambio en la red, la información y las tablas de enrutamiento se actualizan.

Algunos protocolos de enrutamiento de tipo estado-enlace son:

- OSPF
- IS-IS

2.3.3 IS-IS (Intermediate System – Intermediate System)

IS-IS es un protocolo de enrutamiento dinámico diseñado inicialmente por la Organización Internacional de Normalización (ISO) para su Protocolo de red sin conexión (CLNP).

Para admitir el enrutamiento IP, el Grupo de trabajo de ingeniería de Internet (IETF*, Internet Engineering Task Force*) amplía y modifica IS-IS en los estándares relevantes, lo que permite que IS-IS se aplique tanto a entornos TCP / IP como de interconexión de sistemas abiertos (OSI). Este tipo de IS-IS se denomina IS-IS integrado o IS-IS dual (Callon, 1990).

En IS-IS, se utiliza una terminología diferente, en donde los Hosts son considerados como ES (*End System*) y los *routers* o equipos intermedios de capa 3, se consideran como IS (*Intermediate System*).

Características de IS-IS:

- Es un protocolo de tipo IGP Estado-Enlace.
- Su métrica es el costo.
- Permite trabajar con esquemas de direccionamiento de máscara variable (VLSM, *Variable Length Subnet Mask*).

- Al igual que OSPF, utiliza el algoritmo SPF de Dijkstra (AfNOG, 2013).
- Distancia Administrativa: 115.
- Utiliza la nomenclatura NET basada en direcciones NSAP.
- Referenciado bajo RFC 1142

2.3.3.1 Funcionamiento de IS-IS

IS-IS segmenta la red en tres tipos de áreas, por lo que se tendrán los siguientes niveles:

- **Nivel 1:** Intra-Área
- **Nivel 2:** Inter-Área
- **Nivel 1-2:** Los *routers* de este tipo realizan funciones de nivel 1 y 2 de manera simultánea.

Un dispositivo de nivel 1-2 mantiene dos LSDB: un LSDB de nivel 1 y un LSDB de nivel 2. El LSDB de nivel 1 se usa para el enrutamiento dentro del área, mientras que el LSDB de nivel 2 se usa para el enrutamiento entre áreas.

2.3.3.2 Tipos de paquetes de IS-IS

En la siguiente tabla, se detallan los tipos de paquetes o mensajes que son enviados para establecer y mantener adyacencias IS-IS.

Tabla 2-1: Tipos de paquetes de IS-IS

HELLO	Se utiliza para formar adyacencias entre los IS
LSP (Link State Packet)	Son utilizados por los IS para el intercambio de paquetes y el estado de los enlaces con los vecinos
SNP (Sequence Number Packet)	Se utilizan para el control de los paquetes LSP y la sincronización de la base de datos.

Fuente: Elaborado por el autor

2.3.3.3 Estructura de direcciones de IS-IS

En el modelo OSI, el NSAP se utiliza para localizar recursos. La ISO adopta la estructura de direcciones que se muestra en la Figura 2-3.

Un NSAP se compone de la IDP (Initial Domain Part, Parte de dominio inicial) y la DSP (Domain Specific Part, Parte específica de dominio). IDP es la contraparte del ID de red en una dirección IP y DSP es la contraparte del número de subred y la dirección de host en una dirección IP (RFC 1195, 1990).

Según lo define la ISO, el IDP consiste en el Identificador de formato y autoridad (AFI) y el Identificador de dominio inicial (IDI). AFI especifica el mecanismo de asignación de direcciones y el formato de la dirección; la IDI identifica un dominio.

El DSP de orden superior (HODSP), la identificación del sistema y el selector de NSAP (SEL). La parte específica del dominio de orden superior se utiliza para dividir áreas; el ID del sistema identifica un host; el SEL indica el tipo de servicio. Las longitudes de IDP y DSP son variables. La longitud del NSAP varía de 8 a 20 bytes (RFC 1195, 1990).

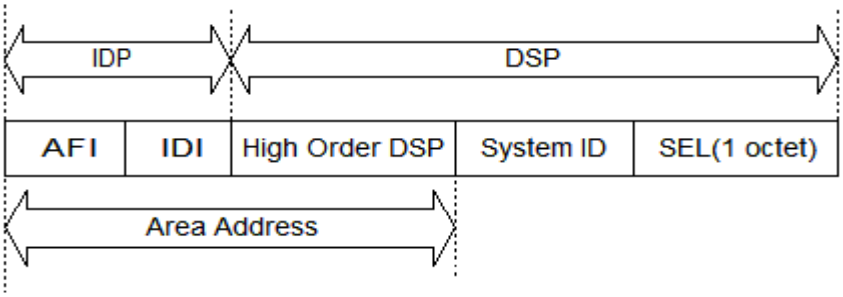


Figura 2-3: Estructura de direcciones IS-IS

Fuente: (Huawei Technologies Co., Ltd., 2018)

Las direcciones que identifican a los *routers* en IS-IS son del siguiente formato:

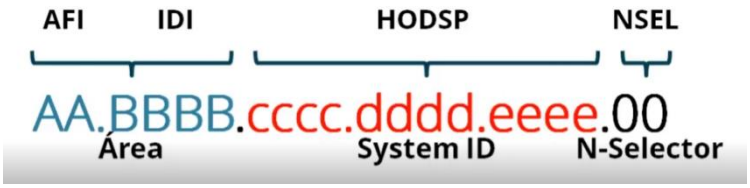


Figura 2-4: Dirección NSAP

Fuente: Elaborado por el autor

- **AFI (*Authority and Format Identifier*):** Compuesto de 1 byte, su función es especificar el formato de la dirección.

- **IDI (*Initial Domain Identifier*):** Especifica el área al que pertenece el router, se compone de 2 bytes.
- **HODSP (*High Order Domain Specific Part*):** Se compone de 6 bytes que sirven para identificar al dispositivo.
- **NSEL (*NSAP Selector*):** Compuesto por 1 byte, sirve para identificar puertos, normalmente en IS-IS siempre se coloca 00.

2.3.3.4 Tipos de redes en IS-IS

IS-IS admite los siguientes tipos de redes:

- *Broadcast network*
- *Point-to-point* (P2P) *network*

2.4 Fundamentos de MPLS

MPLS fue desarrollado por la *IETF* y su arquitectura está definida bajo la *RFC 3031*. La tecnología MPLS, lleva ya unos cuantos años funcionando en las redes de hoy en día.

De hecho, han aportado muchas de las funcionalidades y han creado una gran revolución en las redes aportando soluciones a problemas que antes eran difíciles de solventar con la conmutación de redes puramente IP (Alvarado Rocafuerte, 2020).

Mediante el uso de las etiquetas en los paquetes IP, el objetivo de esta tecnología, es permitir que los *routers* puedan construir un mapa topológico de la red mucho más eficiente. Los *routers* reenviarán entonces los paquetes IP mediante las etiquetas que los paquetes poseen, sin necesidad de ver la dirección IP de destino.

2.4.1 Funcionamiento de MPLS

Es una tecnología creada para el transporte unificado de datos mediante conmutación de etiquetas que sirve tanto para las redes basadas en circuitos como para las redes basadas en paquetes. Dada su naturaleza, permite la transmisión simultánea de voz, datos y video.

Los principales beneficios de MPLS

- Permite la utilización de infraestructuras de red unificadas.

- Mejora la integración de tecnologías como ATM sobre redes IP.
- Permite la utilización dinámica y controlada de múltiples VPN Site-To-Site.
- Trabaja muy bien con protocolos de enrutamiento como BGP.
- Óptimo control de flujo.
- Mejora la capacidad de enviar paquetes de voz, datos y video a través de la red.

2.4.2 Cabecera MPLS

En la Figura 2-5, se muestra la estructura de la cabecera MPLS, está compuesta de 4 octetos, que conforman 32 bits, a su vez la cabecera cuenta con cuatro campos:

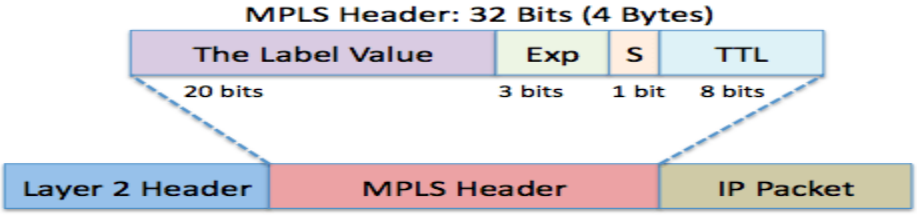


Figura 2-5: Cabecera MPLS

Fuente: Elaborado por el autor

- Label: este campo representa la etiqueta MPLS.
- EXP: Bits experimentales, utilizados para QoS.
- BoS (Bottom of Stack): es 0 a menos que sea la etiqueta inferior de la pila, en cuyo caso es 1.
- TTL: valor que decrece en 1 por cada salto que de el paquete.

2.4.3 Arquitectura de MPLS

En MPLS los *routers* tiene un nombre específico, se denominan LSR (*Label Switch Router*). En MPLS los *routers* conmutan los paquetes mediante la utilización de etiquetas, es por eso, por lo que cada *router* en MPLS se conoce como LSR. Dependiendo de su posición dentro de la red, cada *router* tendrá una función específica, hay tres tipos de *router* LSR, y estos son:

- **Ingress-LSR (In-LSR):** los I-LSR, son los *routers* de entrada de la red MPLS. Reciben un paquete (Inicialmente sin ninguna etiqueta), y le colocan una primera etiqueta para reenviarlo hacia otro router del backbone MPLS.
- **Intermediate LSR:** son los *routers* MPLS que se encuentran en el medio de la red, reciben un paquete con una o más etiquetas a través de una interfaz de entrada y proceden a reenviar hacia su destino a través de una interfaz de salida.
- **Egress-LSR (E-LSR):** es el router final, su función es retirar las etiquetas del paquete IP, y entregarlo así a su destino final.

El proceso de conmutación de etiquetas de MPLS se apoya en dos componentes fundamentes: el plano de control estará el proceso de ruteo de las etiquetas, y en el plano de datos *forwarding* o conmutación. La manera en que MPLS hace todo el proceso de conmutación de etiquetas está basado en por unas operaciones propiamente de los *routers* que conocen de MPLS. Los *routers* LSR realizan las siguientes operaciones:

- **PUSH:** agrega una o más etiquetas en el stack de etiquetas del paquete.
- **SWAP:** cuando un LSR recibe un paquete etiquetado y cambia la etiqueta del tope del stack por una nueva.
- **POP:** remover una o más etiquetas en el topo del stack de etiquetas del paquete IP.

2.4.4 Distribución de etiquetas en MPLS

En MPLS, las rutas son denominadas LSP, camino conmutado por etiquetas. Un LSP es una secuencia de LSRs que conmutan un paquete etiquetado a través de una red MPLS o parte de esta. Comúnmente, los proveedores de servicios y los diferentes fabricantes utilizan uno de los varios protocolos para la distribución de etiquetas MPLS sobre redes basadas en IP.

- ***Tag Distribution Protocol* (TDP)->Obsoleto:** Es un protocolo que se ejecuta sobre una capa de transporte orientada a la conexión con entrega secuencial garantizada.
- ***Label Distribution Protocol* (LDP)-> Formalizado por IETF:** Es una protocolo de conmutación de etiquetas, el cual tiene como soporte a los protocolos de enrutamiento para la distribución de las etiquetas asignadas a los prefijos de red
- ***Resource Reservaton Protocol* (RSVP)->MPLS TE:** Es un conjunto de reglas de comunicación que permite reservar canales o rutas en Internet para la transmisión de datos, que garantiza el mejor servicio, el servicio en tiempo real y el intercambio de enlaces controlado.

Para obtener o reenviar paquetes a través de un camino LSP en una red MPLS, todos los *routers* de la red IP (LSRs) deben tener habilitado el protocolo LDP, el cual tiene las siguientes funciones principales:

- Descubrir los *routers* LSR de la red.
- Establer y mantener las sesiones.
- Comunicar el mapeado utilzado para las etiquetas.
- Enviar mensajes de notificación cuando haya errores en la red.

2.4.5 Ventajas y desventajas de MPLS

Entre las principales ventajas que ofrece la tecnología MPLS se encuentra la separación de paquetes, y la capacidad de transportar diferentes tipos de tráficos de un origen a un destino, la reducción de latencia, pérdida de paquetes y disminuir tiempos de respuesta. Además, la escalabilidad que ofrece para el crecimiento de la red, y el mantenimiento y gestión de esta.

La principal desventaja de MPLS es el costo de ancho de banda. MPLS es un servicio que debe comprarse a un operador, lo que hace que sea mucho más costoso que enviar tráfico a través de Internet. Además, encontrar un proveedor de servicios MPLS que pueda ofrecer cobertura global es bastante complicado.

Por lo general, los proveedores de servicios combinan la cobertura global a través de asociaciones con otros proveedores de servicios, lo que hace que el servicio se encarezca aún más (Americas(ITLA), 2020).

2.5 Ingeniería de Tráfico

La ingeniería de tráfico consiste en un conjunto de técnicas y herramientas que permiten manipular el tráfico de un origen a un destino, dependiendo de la demanda de tráfico y ajustar los recursos de la red, donde su principal ventaja es minimizar la congestión (Johnson, 2017).

En las redes de los proveedores de servicios de Internet, telefonía móvil o fija, se transportan múltiples cantidades de servicios que convergen entre toda la red. Como principio, se entiende que las redes, en su mayoría, están basadas en el mejor esfuerzo, no discriminan la prioridad de los servicios que se transportan a través de esta.

Debido al comportamiento de las redes basadas en el mejor esfuerzo se lo puede atribuir a:

- El modelo TCP/IP está orientado a aque las PDU se entreguen bajo el esquema del mejor esfuerzo.
- La red de distribución puede estar constituida por diversas tecnologías simultáneas: (*IP /SONET/SDH / ATM / Metro-Ethernet / DWDM)*
- En principio en las redes TCP/IP, los protocolos de enrutamiento dinámico no tienen la capacidad de discriminar los diferentes tipos de servicios.

2.5.1 Calidad de servicio

Cuando nos referimos a *QoS*, nos referimos a la capacidad de entregar los diferentes servicios que se transportan por toda la infraestructura de la red de manera eficiente, sin degradar la experiencia de usuario (Bernardo A. Movsichoff, 2007).

Esto nos indica, que, aunque el tráfico que ingresa a la red llegue de manera desordenado al *router*, estos tipos de tráfico pueden ser clasificados y reordenados. Esto mediante técnicas y herramientas de

calidad de servicio para su posterior conmutación por los diferentes LSPs de la red, esto con el fin de transportar el tráfico cuyas prioridades sean mayores.

2.5.2 Demanda de tráfico

A la red de los proveedores de servicios, se conectarán usuarios, empresas e incluso conexiones entre proveedores de servicios. Cada uno de ellos generará una demanda de tráfico de voz, datos y video.

Si no se gestiona correctamente los recursos de la red, la demanda de tráfico podría exceder la disponibilidad de los recursos, y por ende podría presentar problemas de retardo, variaciones, degradaciones, pérdida de paquetes y ancho de banda mal utilizado. Es por ello por lo que se deben tener en cuenta consideraciones generales:

- Los recursos de la red de los proveedores son limitados.
- Los recursos deben gestionarse de manera adecuada para no degradar o efectar la disponibilidad del servicio.
- Los usuarios consumen simultáneamente diferente tipos de servicios como, voz, video y datos a la vez.
- Las horas “pico” en la red, son aquellas donde la demanda de tráfico alcanza su valor máximo en comparación con el ancho de banda disponible en los enlaces de la red.

2.5.3 Congestión

Unos de los conceptos más importantes de ingeniería de tráfico es la congestión. Se refiere a congestión cuando la demanda de tráfico es igual o superior al ancho de banda disponible en los enlaces de la red.

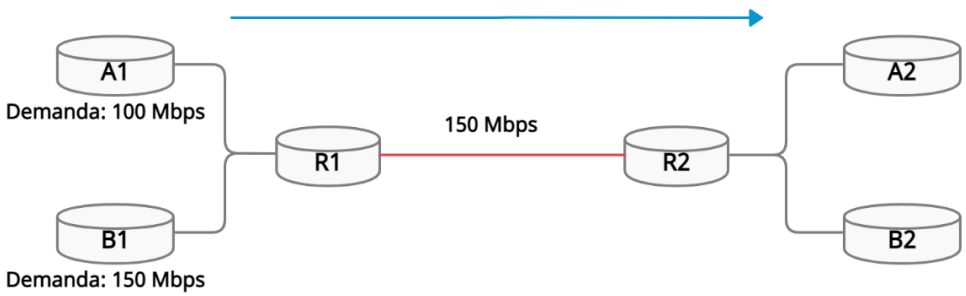


Figura 2-6: Congestión

Fuente: Elaborado por el autor

En la Figura 2-6, se puede observar que el *router* A1 tiene una demanda de 100 Mbps; y el *router* B1 genera una demanda de 150 Mbps, por lo cual se está generando demanda de tráfico de dos fuentes distintas que deben atravesar un mismo tramo de la red para llegar a su destino final.

El tramo es el que se muestra entre R1 y R2, cuya capacidad del enlace es de 150 Mbps el cual es igual a la demanda de tráfico del *router* B1, de manera qué, se generará un cuello de botella que traerá una degradación muy importante en el servicio la cual se traduce a una mala experiencia del usuario.

2.5.4 Ingeniería de Tráfico

La ingeniería de tráfico o por su sigla en inglés TE (*Traffic Engineering)*, a nivel de telecomunicaciones, es un conjunto de herramientas y técnicas que consiste en manipular la demanda de tráfico para ajustarlo a los recursos de la infraestructura de red. El objetivo común es minimizar la congestión (Khan, 2012).

La ingeniería de tráfico se categoriza como: orientado al tráfico y recursos; orientado al tráfico consiste en mejorar los indicadores relacionados al transporte de la información, que incluye minimizar la pérdida de paquetes, el retardo, el *jitter* e incrementar el rendimiento de la red.

Y orientado a los recursos, en donde el objetivo es optimizar los recursos de la red para que puedan ser manejados de manera correcta y eficiente, en este punto está enfocado más al ancho de banda.

2.5.5 Funciones y requemientos de TE

La ingeniería de tráfico tiene las siguientes funciones principales:

- Crear caminos alternos de aquellos puntos de mayor congestión de la red (Cuellos de botella).
- Gestionar de manera eficiente el ancho de banda disponible.
- Maximizar la eficiencia operacional.
- Mejorar el rendimiento del tráfico cursante a través de la red.

- Reducir latencia, minimizar la congestión y pérdida de paquetes.

Para poder realizar una estrategia eficiente de ingeniería de tráfico sobre una red de telecomunicaciones, se necesita considerar los siguientes aspectos:

- Manejar un protocolo de tipo IGP eficiente.
- Utilizar MPLS.
- MPLS TE (Funcionalidad de MPLS relacionada a ingeniería de tráfico).
- Reservar ancho de banda para ciertos enlaces.
- Implementar enlaces con ancho de banda suficientes como para soportar la demanda de tráfico.
- Protocolos de señalización como LDP y RSVP

2.6 Herramienta de ingeniería de tráfico sobre MPLS

MPLS TE es una de las herramientas que proporciona beneficios a una red IP/MPLS. Esto es, usar de modo eficiente los recursos de ancho de banda de la red, proporcionar protección de tráfico ante fallos; y combinar con QoS, para mejorar las SLAs (*Service Level Agreement*, acuerdo de nivel de servicio).

2.6.1 Componentes de MPLS TE

MPLS TE ofrece cinco componentes para la correcta gestión y despliegue en la infraestructura de red.

- Traffic Tunnel
- Atributos de Traffic Tunnel
- Atributos de enlaces físicos
- *Constraint-Based Routing* (CBR)
- Protocolo de señalización de túnel.

2.6.2 Túneles MPLS TE

Los túneles de ingeniería de tráfico en una red MPLS están asociados a los LSP dentro del *backbone* de IP/MPLS, los cuales se construyen a lo largo de todo el camino de tránsito por la red hasta llegar el destino.

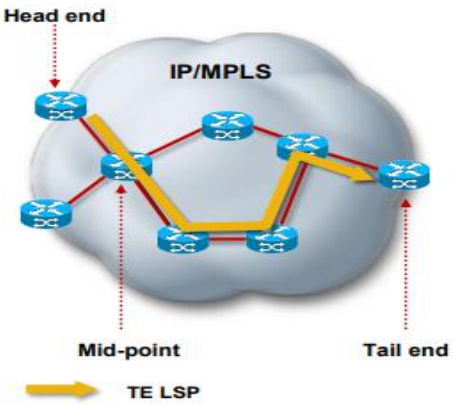


Figura 2-7: Túnel MPLS TE

Fuente: (Johnson, 2017)

En la Figura 2-7 se observa que un *router* I-LSR genera tráfico de red el cual va a hacer transportado por un túnel de ingeniería de tráfico LSP previamente establecido hasta alcanzar el destino.

2.6.3 Atributos de Túnel MPLS TE

Los túneles de TE implementan una interfaz de salida asociada con un camino definido internamente a la red. Se usan para poder enviar el tráfico a un camino predeterminado en la nube MPLS.

Los túneles de ingeniería de tráfico tienen los siguientes atributos que son:

- Unidireccional
- Destino: cola TE RID
- Prioridad / preferencia (configuración y

  Sostener)

- Atributos / Afinidad
- Ancho de banda / Loadshare
- Protección local

- Opciones de ruta (explícita / dinámica)

2.6.4 Distribución de información de enlace

En la Figura 2-8 se describe la posibilidad que la ingeniería de tráfico tiene la información necesaria y visible a todos los recursos de la red, y almacenar en su base de datos topológica, la cual incluye la siguiente información:

- Características adicionales del enlace
- Dirección de interfaz
- Dirección vecina
- Ancho de banda máximo reservable
- Ancho de banda sin reservas (en ocho prioridades)
- Métrica TE (peso administrativo)
- Banderas de atributos
- Información de enlace de inundación IS-IS o OSPF
- Todos los nodos de ingeniería de tráfico crean una base de datos topológica denominada TED (*Traffic Engineering Database*).
- No es necesario si se utiliza el cálculo de ruta fuera de línea

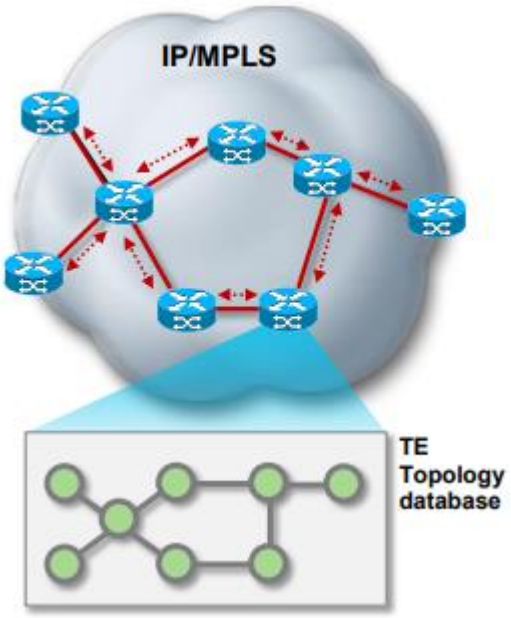


Figura 2-8: Distribución de información de enlace

Fuente: (Johnson, 2017)

2.6.5 Cálcuo de la ruta

Los nodos TE pueden realizar enrutamiento basado en restricciones, donde la cabecera del túnel es la responsable del cálculo de la ruta. Las restricciones y la base de datos topológica desde el punto de vista de RSVP son utilizados como entrada para el cálculo de la ruta, donde los enlaces que no cumplen con las restricciones no forman parte del algoritmo para el cálculo de ésta.

El túnel es establecido una vez que la señalización, basada en las restricciones donde encuentra un camino como se muestra en la Figura 2-9.

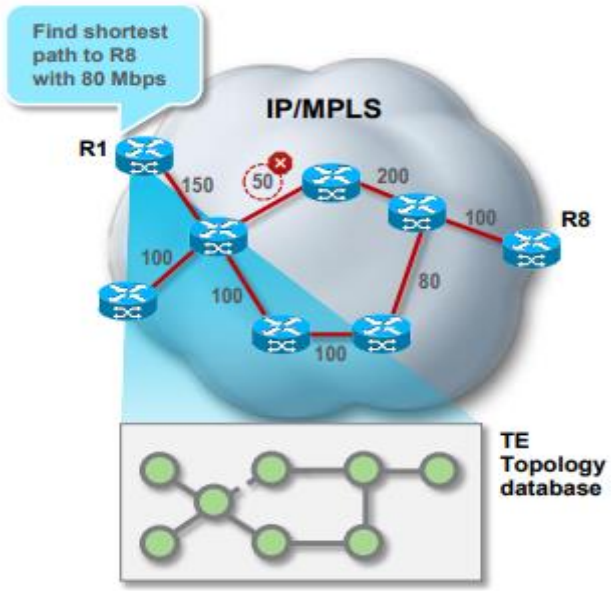


Figura 2-9: Cálculo de la ruta

Fuente: (Johnson, 2017)

2.6.6 Señalización de caminos para túneles de ingeniería de tráfico

El proceso de señalización para el establecimiento de túneles de ingeniería de tráfico se basa en las restricciones y la base de datos topológica proporcionada por protocolos de señalización y reservación de recursos. En la Figura 2-10, se ilustra cómo se realiza el proceso de señalización de etiquetas para los túneles TE, esta señalización va recolectando información como:

- Túnel señalizado con extensiones TE para RSVP
- Estado suave mantenido con downstream PATH messages

- Estado suave mantenido con upstream RESV messages
- Nuevos objetos RSVP
- *LABEL_REQUEST* (RUTA)
- *LABEL* (RESV)
- *EXPLICIT_ROUTE*
- *RECORD_ROUTE* (RUTA / RESV)
- *SESSION_ATTRIBUTE* (PATH)
- LFIB poblado con etiquetas RSVP asignadas por Mensajes RESV

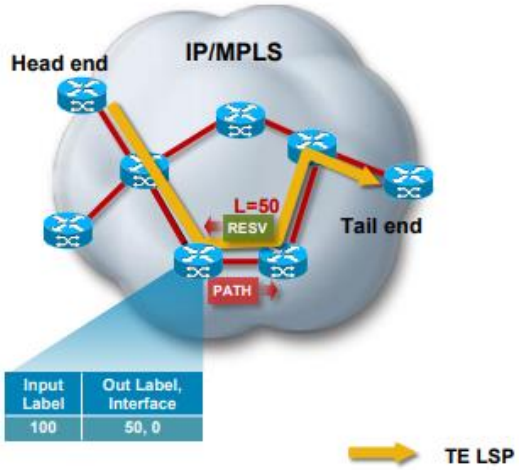


Figura 2-10: Señalización TE LSP

Fuente: (Johnson, 2017)

2.6.7 Confiabilidad de túneles de ingeniería de tráfico

MPLS TE posee un conjunto de herramientas que ayudan a proporcionar confiabilidad en caso de:

- Fallas o incidencias físicas.
- Fallas o incidencias lógicas.
- Modificaciones en la red.
- Saturación de ancho de banda en enlaces.

Make-before-break es un mecanismo de confiabilidad que aporta o sirve para prevenir la pérdida de tráfico durante una conmutación entre dos CR-LSP. *Make-before-break* puede incrementar o usar el ancho de banda de un enlace si lo considera necesario y solo si es posible.

Otro de los mecanismos de confiabilidad en MPLS con ingeniería de tráfico, es el CR-LSP, este mecanismo entra en juego cuando ocurre una falla en el CR-LSP Primario, por lo que el *Hot Standby* entra en funcionamiento y todo el tráfico pasa ahora por ese camino alterno o de respaldo.

TE FRR (*Fast Reroute*) proporciona protección de enlace y protección de nodo para túneles MPLS TE. Si un enlace o nodo falla, TE FRR cambia rápidamente el tráfico a una ruta de respaldo, lo que minimiza la pérdida de tráfico (Khan, 2012).

Cuando un CR-LSP primario falla, TE FRR proporciona un CR-LSP de respaldo de tipo momentáneo mientras se establece un nuevo camino CR-LSP para el reenvío de la información.

2.7 Enrutamiento basado en restricciones

El algoritmo de enrutamiento basado en restricciones o *Constraint-Based Routing (*CBR), está basado en el algoritmo *Dijkstra* pero añadiendo algunas nuevas capacidades, como es el hecho de poder tener en cuenta el ancho de banda y características de cada una de las interfaces. Y, también tiene en cuenta las características que necesita el túnel MPLS TE para el establecimiento.

Al final con estos atributos puesto en el algoritmo CBR resultará una lista de LSP que debe ir cruzando el túnel. Luego, la lista es enviada al protocolo RSVP para que lo señalice y haga la reserva de ancho de banda y el túnel sea creado correctamente (Huertas).

2.8 Protocolo de reserva de recursos de red

RSVP es un estándar que está definido en el RFC 2205 y es el encargado de señalizar el túnel de ingeniería de tráfico. Es el que irá por cada uno de los *routers* que componen el LSP indicando la asignación de una etiqueta MPLS y ancho de banda necesarios para establecer el túnel, y, a su vez, notificará el modo de reservación de ancho de banda. (Khan, 2012).

En la Figura 2-11, se ilustra el flujo del proceso paso a paso que ocurre al momento de empezar el establecimiento de un túnel de ingeniería de

tráfico basado en las bases de datos del protocolo de enrutamiento, MPLS y RSVP para el cálculo de la mejor ruta.

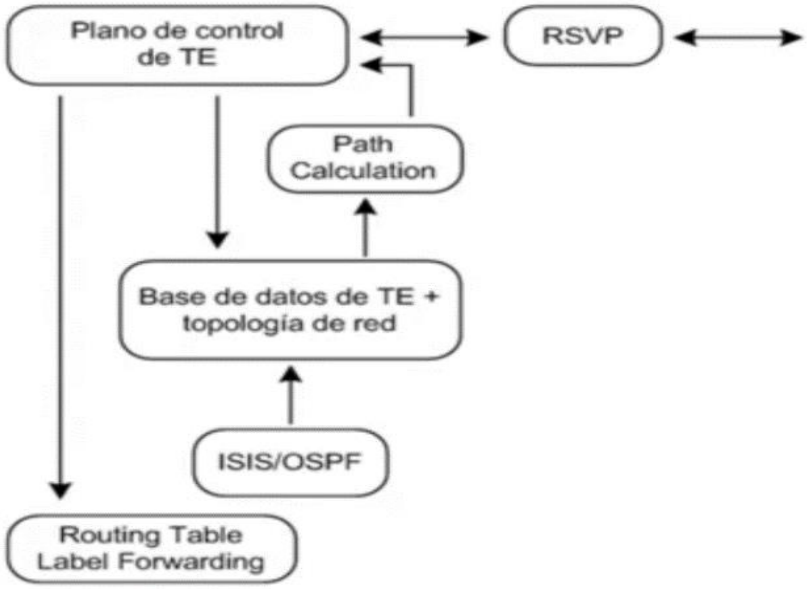


Figura 2-11: Flujo de RSVP

Fuente: (Huertas)

2.9 Calidad de Servicio

Calidad de Servicio es un conjunto integral de funcionalidades que le permiten a un *router* brindar prioridades a los paquetes y ordenar para asegurar la correcta entrega de los servicios (Dongli Zhang, 2007).

El objetivo de los proveedores de servicios es asegurar la correcta entrega de los servicios mientras se cumplen un conjunto de SLAs acordados con los clientes o incluso con otros proveedores de servicios.

2.9.1 Necesidad de QoS

Una empresa proveedora de servicios, básicamente, es un sistema autónomo que ofrece servicios de conectividad, Internet, voz y datos a los clientes o usuarios finales.

Para que el/los proveedores puedan ofrecer todos estos servicios se requiere de una infraestructura para la interconexión de todos los clientes.

Los recursos de la red del proveedor de servicios, hay que tener en cuenta que pueden ser finitos, es decir, ancho de banda limitado, pero, aun así, se deben cumplir con ciertos SLA con los clientes.

Adicionalmente, las redes convencionales están diseñadas bajo el esquema de mejor esfuerzo (*Best Effort*) con lo cual la información se envía en modalidad FIFO (*First In First Out*). Esto no es eficiente para el cumplimento de SLAs. Por lo que se requiere calidad de servicio.

2.9.2 Calidad de servicio sobre una redes IP/MPLS

Para transmitir servicios de voz, datos y video de manera simultánea con miles de usuarios normales o corporativos sobre la misma red de telecomunicaciones. Es necesaria la utilización de tecnologías como IP/MPLS QoS por varios motivos, entre los cuales se mencionan los siguiente:

- IP es el protocolo que más se utiliza a nivel mundial, especialmente en Internet.
- MPLS permite la conmutación de tramas mediante etiquetas, esto implica reducción importante de latencia.
- MPLS permite administrar los recursos de la red de manera eficiente gracias a la ingeniería de tráfico.
- QoS asegura las prioridades para la correcta entrega de los servicios y el cumplimiento de los SLAs.

2.9.3 Mecanismos de calidad de servicio sobre MPLS

Mediante MPLS QoS e ingeniería de tráfico, se garantiza que los clientes disfrutarán del servicio y tendrán una excelente experiencia de usuario (UX) ayudando a prevenir interrupciones molestas o caídas repentinas.

En la Figura 2-12, muestra los diferentes tipos de tráficos que se pueden generar en la red. Los mismo deben ser categorizados basados en el tipo de tráfico, y establecer mecanismos de prioridad y marcado, y de esa

manera brindar calidad de servicio a los datos de mayor sensibilidad para los usuarios.

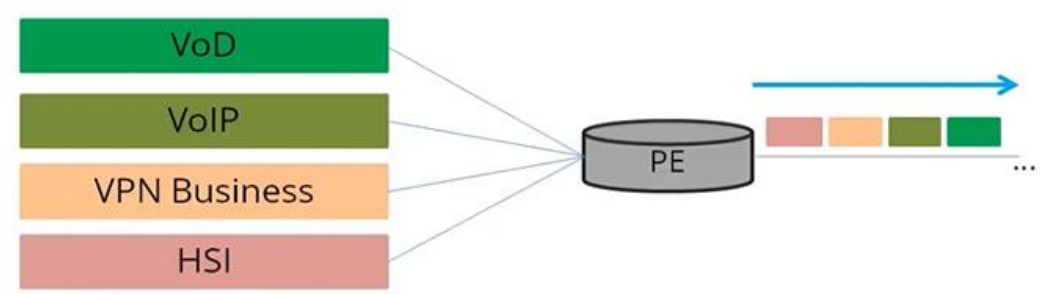


Figura 2-12: MPLS QoS

Fuente: Elaborado por el autor.

2.9.4 Aspectos que afectan a la red

Debido a que las redes tradicionales, de manera natural funcionan con el mejor esfuerzo para el reenvío de tráfico, por tal motivo existen aspectos que afectan a la red si no son tratados de una adecuada manera. A continuación, se mencionan varios aspectos:

- Rendimiento (*Throughput*).

  El rendimiento de la red se puede ver restringido o afectado por el ancho de banda y las tasas a las que pueden transmitir cada uno de los enlaces.

- Latencia (*Delay)*

  La latencia es una métrica definida en la RFC 2679 que sirve para medir el retardo unidireccional como la diferencia en el tiempo que se genera cuando un paquete cruza 2 puntos de referencia en la red.

- *Jitter*

  La RFC 3393 la define como un parámetro para medir la fluctuación unidireccional. Es la variación en el retardo de red experimentado por 2 datagramas consecutivos que cruzan un mismo segmento de la red.

- Pérdida de paquetes.

  La pérdida de paquetes está definida bajo las RFC 2680 y 3357 como una métrica para medir la pérdida de tráfico unidireccional. Existen diversos factores que pueden generar la pérdida de paquetes en la red.

  Algunos factores que pueden generar la pérdida de paquetes son:

  - Congestión.
  - Límite de velocidad del tráfico.
  - Errores de capa física.
  - Falla en elementos de red.

2.9.5 Modelos de QoS

Para garantizar la correcta interoperabilidad y convergencia de las redes, IEFT estandarizó dos modelos de QoS para redes basadas en IP/MPLS

- Servicios Integrados (*IntServ*)
- Servicios Diferenciados (*DiffServ*)

2.9.5.1 Modelo de servicios integrados.

El modelo de servicios integrados surgió en 1994 gracias al IETF como un esfuerzo para desarrollar una solución efectiva al modelo de mejor esfuerzo. Está definido bajo el RFC 1633.

Entre sus características se pueden mencionar las siguientes:

- Utilizar RSVP como protocolo de señalización.
- Reservar recursos de red para flujo de tráfico unidireccionales.
- Para flujos de tráfico bidireccionales, la señalización RSVP se realiza de manera independiente en cada dirección.
- Integrar con todos los servicios de manera controlada a través de los enlaces.
- Funciona tanto para comunicaciones unicast como multicast.

2.9.5.2 Modelo de servicios diferenciados.

El modelo de Servicios Diferenciado está definido bajo la (RFC 2475, 1998). Bajo este modelo, el tráfico que ingresa se clasifica y posiblemente se condiciona en los límites de la red, y se asigna a diferentes agregados de comportamientos conocidos como *Bahavior Aggegates*(BA).

Los paquetes marcados por un punto de servicios diferenciados (DSCP, *Differentiated Services Code Point*) por los equipos clientes recibidos por *router* de borde del *DiffServ* quien los clasifica dentro de distintos BA. Luego en el núcleo de la red del SP, los paquetes se reenvían de acuerdo con el comportamiento definido por los *routers* de borde.

2.9.5.3 Elementos del DiffServ

Dentro de un DS *Domain* existen varios elementos importantes:

- BA: es el comportamiento de un agregado dentro de un DS Domain.
- DSCP: Es un valor definido en el campo de tipo de servicio (ToS, *Type of Service*) de la cabecera Ipv4. Este campo indica el comportamiento que el router de borde del DS debería asignarle.
- Comportamiento por salto (PHB, *Per-Hop Behavior*): es el tratamiento de QoS que el modelo DiffServ le aplica a una clase de tráfico en concreto cuando se mueve entre distintos nodos que forman parte de un mismo DS Domain.

2.9.5.4 Soporte de MPLS para DiffServ

Esta solución está documentada por la IETF bajo (RFC 3270, 2002). El objetivo es proporcionar un mecanismo para mapear a los BA del dominio *DiffServ* en rutas etiquetadas por los LSP, de manera tal que se cumplan los objetivos del proveedor de servicios.

Para el soporte de servicios diferenciados, la tecnología MPLS introduce 2 tipos de rutas por etiquetas LSP.

- E-LSP: un LSP en donde el PHB es determinado por el valor EXP de la cabecera MPLS de los paquetes.

- L-LSP: un LSP en donde el PHB es determinado tanto por el valor del EXP como por la etiqueta.

2.9.5.5 Tipos de PHB

El modelo *DiffServ* define cuatro tipos de PHB:

- Reenvío Acelerado (EF, *Expedited Forwarding*): Se usa para simular el reenvío de una línea arrendada virtual en el dominio, y proporcionar el servicio con una baja tasa de caída, bajo retardo y alto ancho de banda, como se muestra en la siguiente tabla.

Tabla 2-2: Reenvío Acelerado

PHB	DSCP	Destinado a	Encolamiento	RFC
EF	101110	Voz interactiva	Prioritario	3246

Fuente: Elaborado por el autor.

- Reenvío Asegurado (AF, *Assured Forwarding*): para aquellos paquetes que requieren un mínimo de ancho de banda para su entrega.

Tabla 2-3: Reenvio Asegurado

PHB	DSCP	Destinado a	Encolamiento	RFC
AF1	001010(AF11) 001100(AF12) 001110(AF13)	Transferencia de datos masivos, web y servicios generalizados	Basado en la tasa	2597
AF2	010010(AF21) 010100(AF22) 010110(AF23)	Acceso a base de datos, servicios transaccionales, tráfico interactivo o preferido.	Basado en la tasa	2597
AF3	011010(AF31) 011100(AF32) 011110(AF33)	Aplicaciones y servicios de datos importantes	Basado en la tasa	2597
AF4	100010(AF41) 100100(AF42) 100110(AF43)	Servicios de video interactivo.	Basado en la tasa	2597

Fuente: Elaborado por el autor

El objetivo de AF es asegurar el envío, por tanto, para este PHB la pérdida de paquetes es importante. Las subclases de AF se pueden representar como una matriz Afij.

Tabla 2-4: Matriz Afij

PHB	Baja Probabilidad de Descarte J = 1	Media Probabilidad de descarte J = 2	Alta Probabilidad de descarte J = 3
AF (i = 4)	100010	100100	100110
AF (i = 3)	011010	011100	011110
AF (i = 2)	010010	010100	010110
AF (i = 1)	001010	001100	001110

Fuente: Elaborado por el autor

- Selector de Clases (CS, Class Selector).

Tabla 2-5: Selector de Clases

PHB	DSCP	Destinado a	Encolamiento	RFC
CS7	11100	Mensajes de acceso a la red, Keepalive, etc.	Basado en la tasa	2474
CS6	11000	Protocolos de enrutamiento	Basado en la tasa	2474
CS4	100000	Streaming de video	Basado en la tasa	2474
CS3	011000	Señalización de telefonía y video (SIP, H.323)	Basado en la tasa	2474
CS2	010000	Gestión de la red (SNMP)	Basado en la tasa	2474
CS1	001000	Otros tipos de tráfico definido por el administrador de red	Basado en la tasa	2474

Fuente: Elaborado por el autor

El PHB CS5 generalmente es tratado igual que el PHB EF; y, el PHB CS0 Se considera como BE.

- BE (*Best Effort*): Envío tradicional basado en mejor esfuerzo.

Tabla 2-6: Mejor Esfuerzo

PHB	DSCP	Destinado a	Encolamiento	RFC
BE	000000	Tráfico sin especificar o sin ningún tipo de prioridad	Basado en la tasa, menor prioridad	2474

Fuente: Elaborado por el autor.

Si un *router* DS no consigue mapear el valor del DSCP a ningún PHB, considerará el paquete como BE.

2.9.5.6 Campo de Servicios Diferenciados.

Los servicios diferenciados agregan un campo en la trama de los protocolos. Estos protocolos interpretan ese campo de la cabecera a qué tipo de servicios diferenciados perteneces, y cuál es el comportamiento para tratar el tráfico al arribar a un dispositivo del dominio de *DiffServ*. A continuación, se menciona los campos de *DiffServ* en algunos protocolos:

- En la cabecera de Ipv4, se utiliza el campo ToS.
- En la cabecera de Ipv6, se utiliza el campo *Traffic Class* (TC)
- En ethernet se utiliza el campo 802.1p
- En la cabecera de MPLS se utiliza el campo EXPERIMENTAL(EXP).

Como sabemos que la tecnología MPLS permite la integración de diferentes tecnologías, el campo EXP es el que tendrá mayor importancia.

2.9.5.7 Campo ToS de IPv4

La cabecera del protocolo IPv4 consta de varios campos, uno de ellos es el tipo de servicio. Este campo permite determinar la prioridad con la cual va a ser tratado el tráfico de red. A continuación, se describirán los campos que tiene la cabera, como se muestra en la

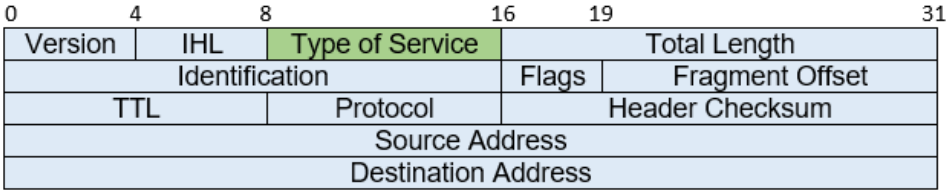


Figura 2-13: Campo ToS en IPv4

Fuente: Elaborado por el autor

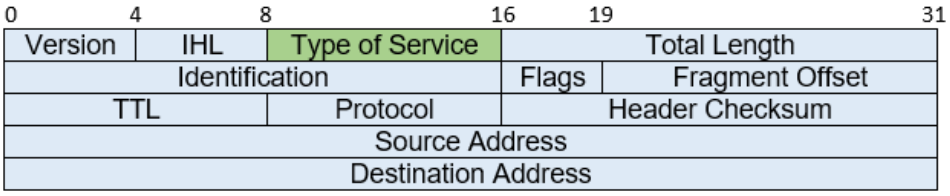


Figura 2-13

- Version (4 bits): Indica la versión del paquete Ipv4 o Ipv6.
- IHL (4 bits): Indica el tamaño de la cabecera del paquete IP.
- *Type of Service* (8 bits): Indica QoS deseada para el paquete.
- *Total Length* (16 bits): Indica el tamaño del paquete.
- *Identification* (16 bits): usuado para identificar los fragmentos de undatagrama original.
- *Flags* (3 bits): usado para información de los fragmentos.
- *Fragment Offset* (13 bits): indica la posición de la carga útil al comienzo del segmento de datos original no fragmentado.
- TTL (8 bits): indica el tiempo de vida del paquete. Decrementa en 1 con cada salto.
- *Protocol* (8 bits): indica el protocolo de capa superior utilizado.
- *Checksum* (16 bits): utilizado para verificar la correcta validez de la cabecera del paquete.
- *Source Address* (32 bits): dirección IP de origen.
- *Destination Address* (32 bits): dirección IP de destino.

Este campo de ToS está compuesto de 8 bits, los bits del 0 al 2 representan a un valor de precedencia, el bit 3 representa el *delay*, el bit 4 que constituye al *throughput* o rendimiento y el bit 5 representa la confiabilidad del paquete; los bits restantes no solo utilizados por tal motivo se completan con cero; y, a su vez la precedencia identifica al tipo de servicio que se está transportando en el paquete.

El *delay* es el bit que sirve para identificar si el paquete es sensible o no al retardo, en donde, si arriba con el bit en 0, significa que acepta un retardo normal; y si es 1 el bit, indica que es un tráfico sensible al retardo.

En el bit de rendimiento, si este arriba marcado por un 0, este indica que acepta un nivel normal de ancho de banda; y si arriba con 1, indica que el paquete requiere mayor ancho de banda.

El campo de la confiabilidad, cuando arriba un paquete con el bit en 0, este indica probabilidad de descarte normal, mientras que, si llega con el bit en 1, el paquete requiere baja probabilidad de descarte.

2.10 Funcionalidades de redes privadas virtuales sobre redes MPLS

MPLS VPN es una tecnología que le permite a los clientes corporativos interconectar sus oficinas a través del *backbone* IP/MPLS de un SP (Khan, 2012).

2.10.1 Consideraciones de QoS en MPLS VPN

Al introducir el concepto de calidad de servicio y dominios diferenciados, es necesario considerar algunos aspectos:

- Se debe asegurar el cumplimiento de los SLA establecidos con la usuario.
- Se debe validar que un cliente en particular no consuma más ancho de banda de que debería.
- En caso de que se consuman recursos no establecidos en los SLA, los paquetes que sobrecarguen las condiciones del contrato, deberían ser descartados o tratados de forma distinta.
- Se debe considerar el hecho de que tanto el proveedor como el usuario puedan estar en dominios Diff-Serv distintos o no.

2.10.2 Modos de servicios diferenciados

Mediante la RFC 3270, se definen 3 modos de *Tunneling* de MPLS para servicios diferenciados.

- Uniform Mode

  Se utiliza cuando el cliente y el proveedor de servicios comparten el mismo dominio de servicios diferenciados. En este modo, los primeros 3 bits del campo IP ToS (bits de precedencia IP) se

asignan automáticamente a los bits EXP de MPLS en el *Ingress* PE a medida que las etiquetas se insertan en los paquetes

- Pipe Mode

  Se utiliza cuando el cliente y el proveedor de servicios están en dominios *Diff-Serv* distintos. En este modo, las políticas de egreso desde el PE hacia el CE, se aprovisionan de acuerdo con las marcas y remarcas configuradas por el SP.

- Short Pipe Mode

  Este modo es útil cuando el proveedor de servicios desea aplicar su propia política *DiffServ* y el cliente solicita que su información *DiffServ* se conserve a través del túnel MPLS VPN.

2.10.3 Manejo de congestión (Queuing)

Todos los dispositivos intermedios de red, ya sea capa 2 o capa 3, reciben información desde un origen para reenviar a su destino, pero en ocasiones las interfaces están ocupadas o congestionadas, motivo por el cual se usa el encolamiento (*queue*).

Para el manejo de la congestión, el sistema contiene 3 elementos fundamentales como son, el clasificador (*Classifier*), colas (*Queue*) y el programador (*Scheduler)*.

Estos elementos están basados en algoritmos para la gestión y tratamiento del tráfico, qué, basado en su naturaleza establecen mecanismos para la conmutación de datos aportando calidad de servicio por la manera en que manejan el encolamiento de tráfico en las interfaces de red. Entre los algoritmos que aportan al manejo se mencionan los siguientes:

Lógica de Round Robin: El programador realiza ciclos en los cuales envía la información en orden de prioridad. En cada ciclo el programador toma un mensaje de una cola o toma una cantidad de bytes de cada cola.

Cola de baja latencia (LLQ, *Low Latency Queue*): Es una herramienta que le indica al programador que debe tratar a una o varias colas con una prioridad especial. Con LLQ, aunque se esté ejecutando un ciclo, si llega un paquete de una de las colas especiales, el programador interrumpirá el ciclo momentáneamente y le dará prioridad inmediata al nuevo paquete, de tal forma se reduce la latencia y el jitter de servicios transmitidos.

Cola de ponderación justa basada en la clase (CBWFQ): *CBWFQ (Class-based Wighted Fair Queuing)* es una herramienta para garantizar una cantidad de ancho de banda mínimo a cada clase antes de ser procesada por el programador. Con esta herramienta, se transforma la lógica de *Round Robin* al algoritmo *CBWFQ Round Robin Scheduling*.

2.11 Vigilancia y modelado de tráfico de red

Cuando se habla de *Policing* se hace referencia a la vigilancia de tráfico, y cuando se habla de *Shaping* se refiere al modelado de tráfico. Ambas son herramientas diseñadas para garantizar que la tasa de transmisión de bits no supere la capacidad configurada en las interfaces en un momento determinado como se muestra en la Figura 2-14.

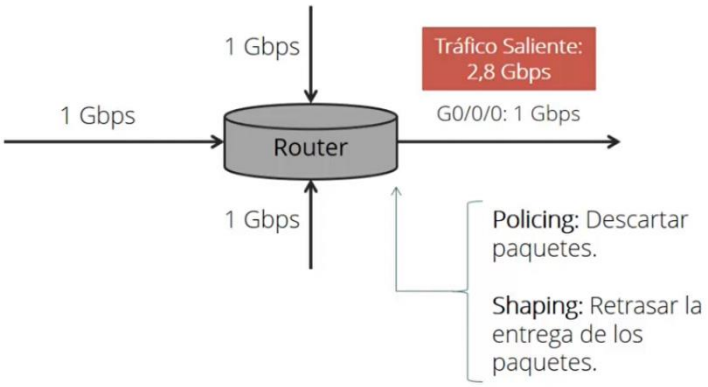


Figura 2-14: Policing & Shaping

Fuente: Elaborado por el autor

Policy y *Shaping*, son herramientas de uso muy especializado, que no son tan comunes en la mayoría de los entornos de pequeñas empresas. Desde el punto de vista de un SP, estas herramientas se utilizan en el borde

de la red hacia la *WAN*. Ambas herramientas monitorean la tasa de bits que fluye a través de un dispositivo e intentan mantener dicha tasa por debajo de la tasa configurada.

2.11.1 Vigilancia

La herramienta *Policing* aporta para una comparación de tasa de tráfico con una tasa de vigilancia (*Policing Rate*) previamente definida, y realiza la acción del descarte de paquetes que excedan dicho valor con se muestra en la Figura 2-15.

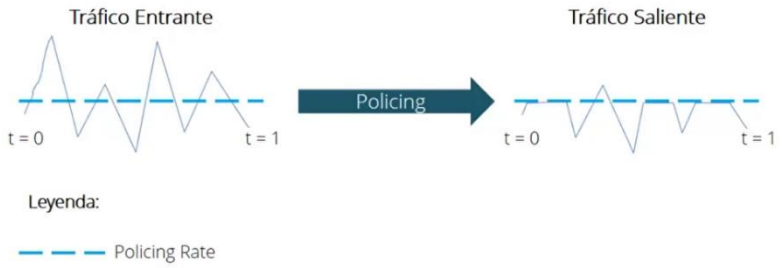


Figura 2-15: Policing Rate

Fuente: Elaborado por el autor.

2.11.2 Modelado

Mediante el uso de la herramienta *shaping* se logra reducir la tasa de transmisión del tráfico, usando colas para los paquetes. Cómo se ilustra en la siguiente figura, la tasa de transmisión es ajustada de 1 Gbps a 150 Mbps.

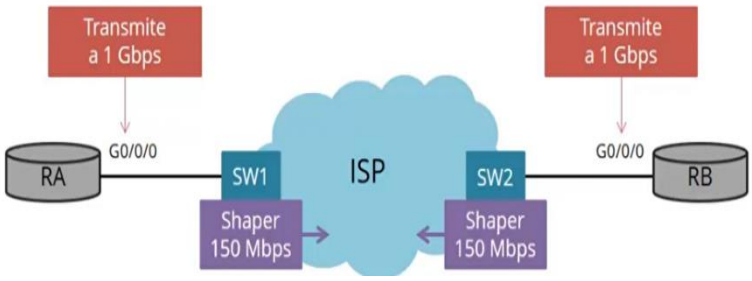


Figura 2-16: Shaping

Fuente: Elaborado por el autor.

El modelador atiende entonces a las colas modeladas *(Shaping queue)* y va reenviando los paquetes, no en función de la disponibilidad de

la interfaz física, sino de forma controlada, basándose en una tasa de transmisión especial llamada *shaping rate.*

CAPITULO 3 . DISEÑO E IMPLEMENTACIÓN

En este capítulo se presenta el diseño y la simulación de la red *Backhaul* IP/MPLS utilizando mecanismos y técnicas de ingeniería de tráfico y calidad de servicios.

3.1 Metodología de desarrollo a seguir

El desarrollo de este capítulo se basa en la metodología que se muestra en la Figura 3-1. La cual indica los procedimientos de manera general que se realizan para alcanzar el diseño y simulación de una red *Backhaul* IP/MPLS con ingeniería de tráfico y calidad de servicio.

Para ello, en primer lugar, se debe establecer el diseño de la red a simular, basado en estándares y procedimientos que se han estudiado en la tesis. Lo segundo es establecer las configuraciones iniciales de los dispositivos que forman parte del diseño, esto con las respectivas direcciones IP, y la configuración del protocolo IS-IS con protocolo IGP para el plano de control de la red.

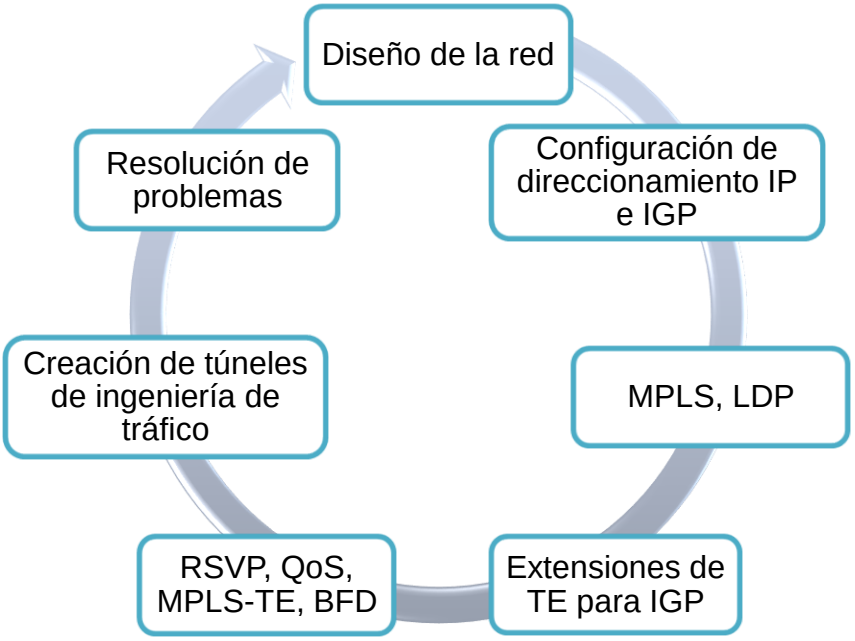


Figura 3-1: Metodología de desarrollo a seguir

Fuente: Elaborado por el autor

El siguiente paso, es establecer las configuraciones adecuadas para el funcionamiento de MPLS y protocolos que ayuden a la distribución de

etiquetas de manera dinámica como LDP, y, a su vez, los mecanismos que aporta MPLS para manipular caminos a nivel de ingeniería de tráfico.

La selección del protocolo de enrutamiento dinámico es muy importante, ya que, para este punto, éste debe soportar extensiones para ingeniería de tráfico. Se ha seleccionado IS-IS porque permite establecimiento de TE.

Seguidamente, se debe señalizar mediante RSVP los recursos de la red, para de esta manera, los túneles de ingeniería de tráfico puedan establecerse al momento de la implementación, también, la señalización del tipo de tráfico que va a cruzar por la red, y como debe ser tratado.

Una vez configurado todos los protocolos y herramientas, se deben establecer los túneles de ingeniería de tráfico basado en requerimientos de ancho de banda, prioridad y otros datos importantes de acuerdo con el tipo de tráfico que se va a transportar.

Por último, mecanismos de resolución de problemas sobre establecimientos de los túneles de ingeniería de tráfico, como el estado, etiquetas MPLS y base de datos topológica de la red.

3.2 Evaluación de características de la red

Se diseña una red *Backhaul* IP/MPLS debido qué, el protocolo IP es el más utilizado a nivel global en las redes de telecomunicaciones, especialmente para Internet. MPLS contribuye a la entrega expedita de paquetes basándose en el etiquetado de las tramas, aportando con una reducción significativa de tiempo de respuestas en las comunicaciones y menor latencia. A la vez, contribuye a manejar de manera más eficientes los recursos de la red mediante las técnicas de ingeniería de tráfico.

Se utiliza el protocolo de enrutamiento IS-IS para el intercambio de prefijos dentro del *core IP/MPLS*, debido a su compatibilidad con ingeniería de tráfico y sus aportes para garantizar alta disponibilidad a nivel de red, a su vez aporta con características para el manejo de la congestión. Las herramientas de *QoS* e ingeniería de tráfico que serán implementadas permitirán relacionar los conceptos estudiados en el capítulo anterior, por lo que se procederá a simular la red.

3.3 Diseño de la red IP/MPLS

La red para emular está orientada para ejemplificar el uso de tecnologías MPLS, túneles de ingeniería de tráfico y mecanismos de calidad de servicio aplicado a una red IP *Backhaul*. La red IP *Backhaul* está compuesta de 7 *switches* para data center de la serie *CloudEngine* 12800 del fabricante Huawei.

En la Figura 3-2, se diseña una red de tipo *full mesh* que corresponde la nube IP/MPLS de un proveedor de servicios. Los cuales van a permitir una alta disponibilidad de enlaces físicos; y, aportan sustancialmente para los caminos redundantes al momento de establecer túneles de ingeniería de tráfico para el transporte de datos de un extremo a otro.

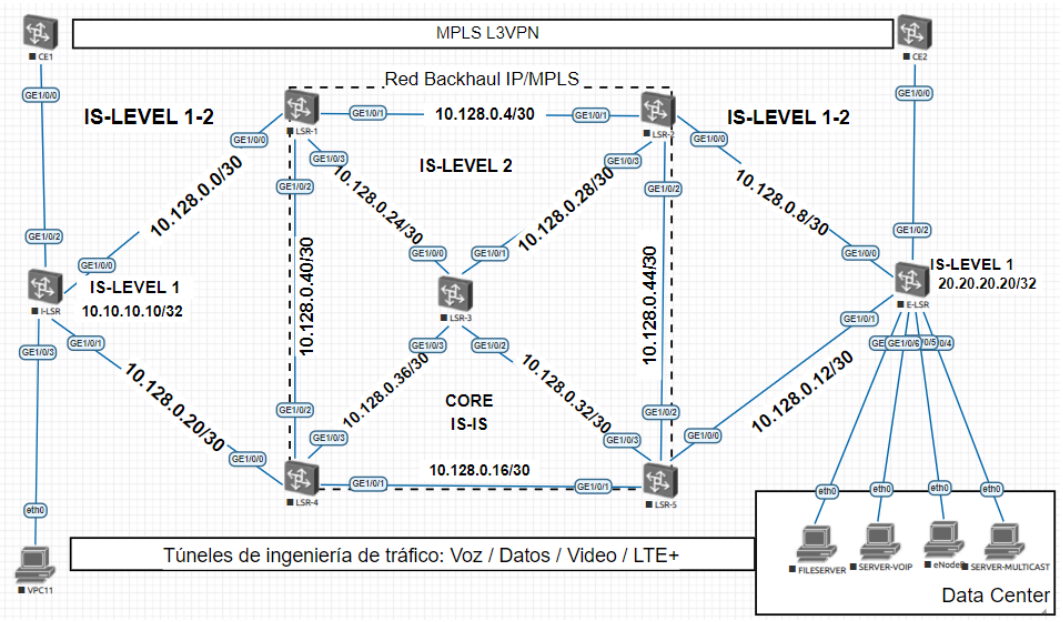


Figura 3-2: Topología de red Backhaul

Fuente: Elaborado por el autor

A su vez en la Figura 3-3, se propone otra topología para simular el escenario donde se provee de conectividad por medio de circuitos virtuales de capa 2 o L2VPN, sobre la red IP/MPLS. A su vez, establecer mecanismos de ingeniería de tráfico que permita conectividad a sedes remotas compartiendo el mismo dominio de red.

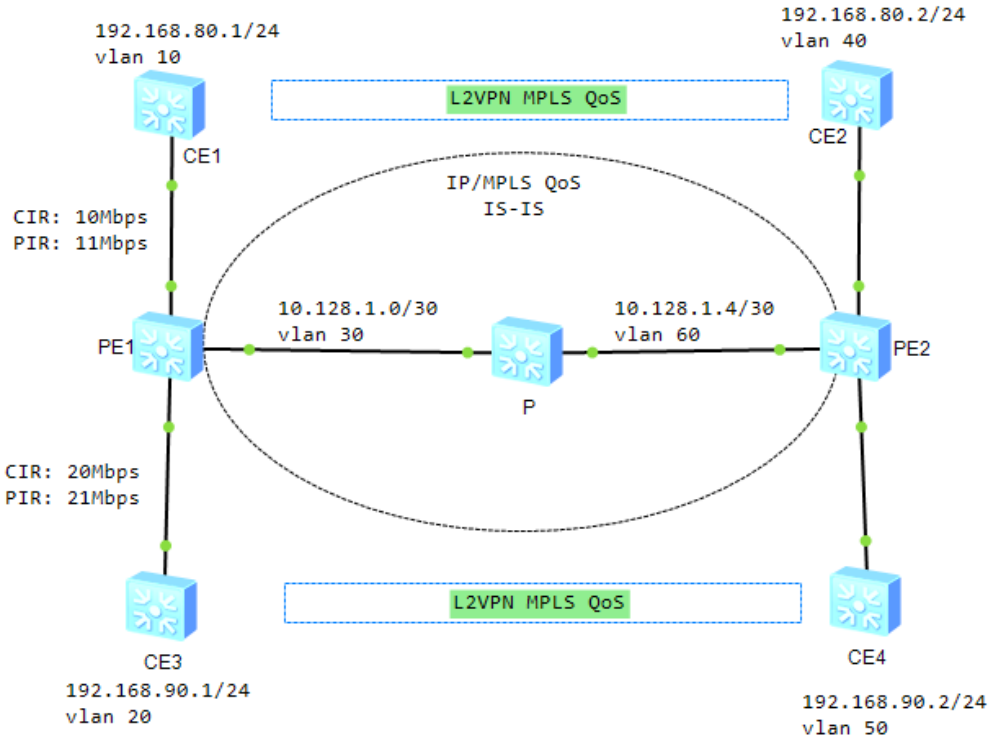


Figura 3-3: Topología de red para IP/MPLS QoS

Fuente: Elaborado por el autor

Para la ejecución de la simulación de las topologías diseñadas en la Figura 3-2 y Figura 3-3, se establece el direccionamiento IP necesario para la comunicación e intercomunicación de redes, y establecimiento de adyacencias para el correcto funcionamiento de las diferentes tecnologías que veremos a lo largo del capítulo. Esta información se encuentra en el Anexo 0-1: Direccionamiento IP de red Backhaul IP/MPLS TE y Anexo 0-2: Direccionamiento IP red IP/MPLS QoS.

3.4 Emulador EVE-NG Community

EVE Emulated Virtual Environment es una plataforma de emulación de red para diferentes fabricantes, entre ellos Huawei. Permite la simulación de equipos de red reales, esta plataforma sin cliente ayuda a los profesionales de TI a familiarizarse con equipos de Huawei y otros, donde poner en práctica en laboratorio conceptos que se adquieren con el pasar del tiempo, y poder discernir las diferentes configuraciones e implementaciones de las tecnologías de redes.

Para este proyecto se trabajará con las siguientes herramientas:

- EVE-NG OVF 2.0.3-110
- Vmware Workstation Player 16
- Windows integration pack

Las versiones del software pueden cambiar de acuerdo con las liberaciones por parte de EVE-NG en el tiempo.

3.5 Plataforma de simulación de red

El Enterprise Network Simulation Platform (eNSP) es una plataforma de simulación de red gráfica, ampliable y gratuita desarrollada por Huawei. Al simular los *routers* y *switches* empresariales de Huawei, muestra escenarios de implementación de dispositivos. eNSP puede simular redes de gran tamaño. Los usuarios pueden realizar pruebas y aprender tecnologías de red sin usar dispositivos reales (Huawei, 2019).

Para esta simulación se trabajará con los siguientes recursos:

- eNSP V100R003C00SPC100
- VirtualBox 5.2.44

3.6 Procedimiento de la simulación de una red Backhaul IP/MPLS con ingeniería de tráfico y calidad de servicio.

A continuación, se presentarán los pasos a realizar para la simulación de la red *Backhaul* IP/MPLS con técnicas de ingeniería de tráfico y calidad de servicio.

3.6.1 Creación del proyecto en EVE-NG Community

Para dar inicio con el desarrollo de la simulación, lo primero a realizar es crear una plantilla nueva de laboratorio, para eso se da *click* en Add New Lab.

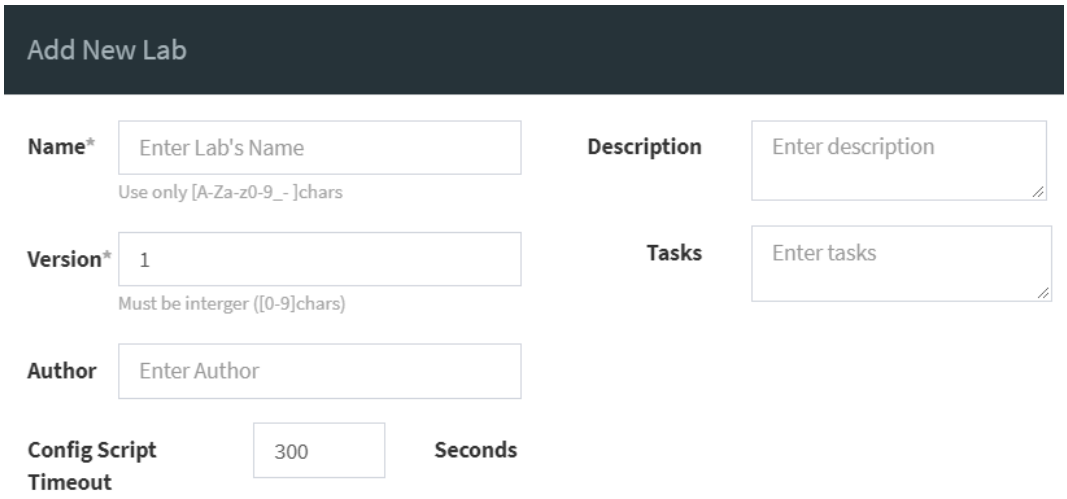


Figura 3-4: Creación de un nuevo laboratorio

Fuente: Elaborado por el autor

Se abrirá el laboratorio en blanco, donde se procederá a realizar la topología que se simulará. Para agregar los equipos Huawei CE12800 debemos dar click en Add a object->Node y se procede con la elección de Huawei CloudEngine 12800, cuantos sean necesarios para obtener la topología de red.

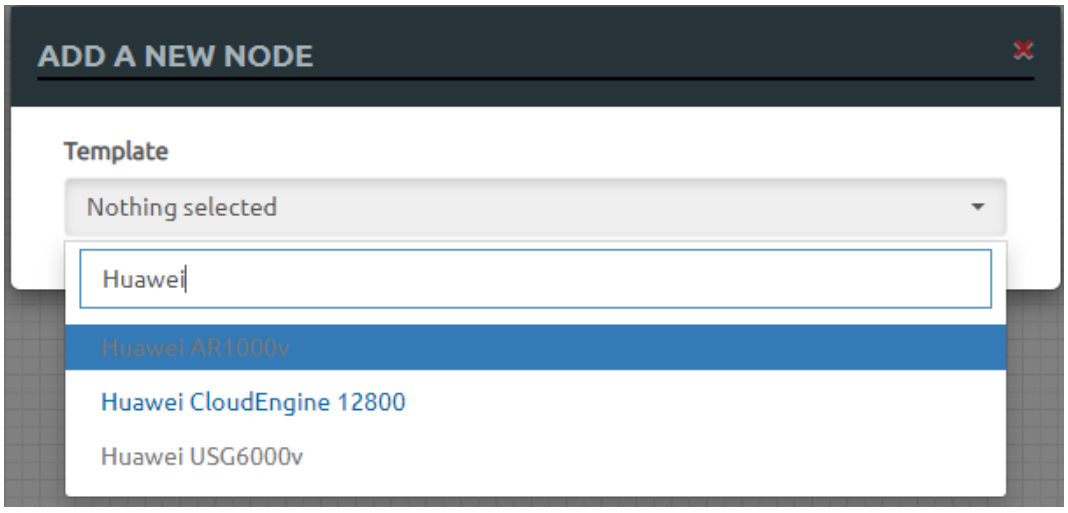


Figura 3-5: Agregar nodo a un nuevo Lab

Fuente: Elaborado por el autor.

Luego, se deberá conectar cada elemento de red con sus respectivas interfaces según lo indica el Anexo 0-1. Seguidamente, corresponde iniciar los dispositivos que conforman la topología de red; para ellos damos clic sobre cada dispositivo y seleccionamos la opción *start.*

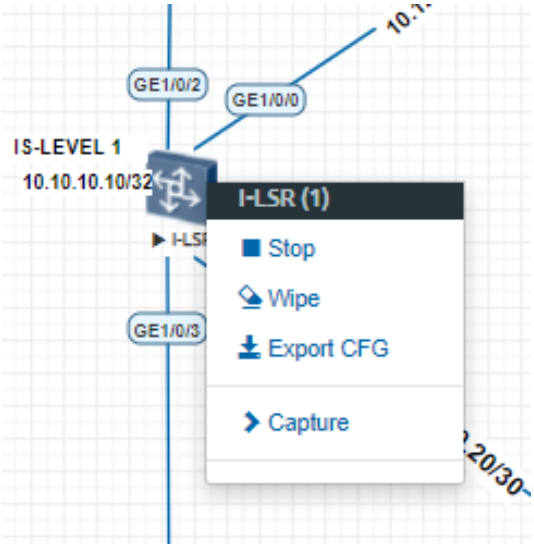


Figura 3-6: Opciones para iniciar CE12800

Fuente: Elaborado por el autor

3.6.2 Creación de topología en eNSP

Para crear la topología de red en eNSP, se debe dar click en New Topo, que se encuentra en la parte superior izquierda de la pantalla, como se muestra en la Figura 3-7.

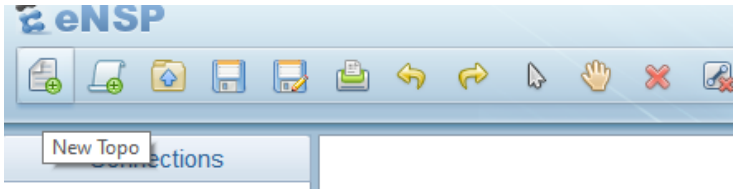


Figura 3-7: Crear una nueva topología

Fuente: Elaborado por el autor

Se abrirá una hoja nueva donde se podrá realizar la topología que se necesita. Se selecciona el dispositivo y se arrastra el elemento que se desea agregar hasta la hoja hasta obtener la topología de la red.

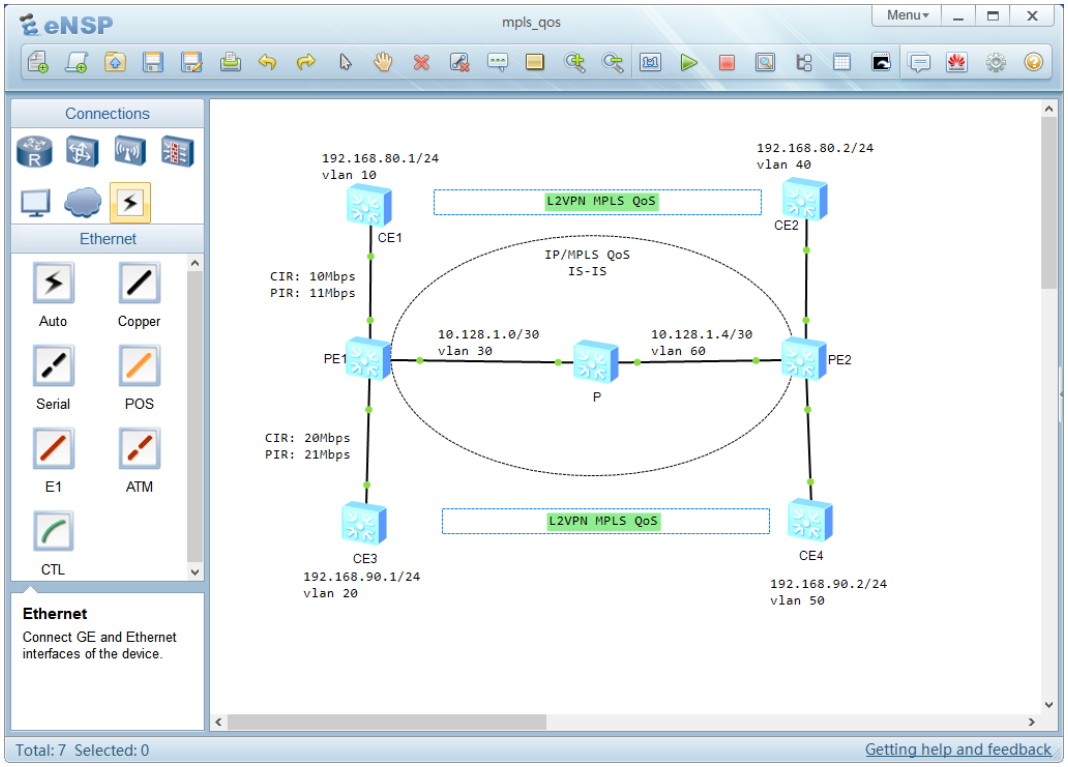


Figura 3-8: Hoja de la topología.

Fuente: Elaborado por el autor

3.6.3 Configuración de interfaces

Las configuraciones se realizarán mediante *Command-Line Interface* (CLI). La configuración inicial consiste en establecer las direcciones ip a las interfaces según corresponda a lo establecido en el Anexo 0-1.

Para una ilustración efectiva se procede a continuación, con la configuración de una interfaz con su respectiva dirección IP, descripción y modo del puerto, como se muestra en la Figura 3-9. Los comandos aplicados se deben replicar para la configuración de los otros dispositivos e interfaces de acuerdo con el Anexo 0-1.

```
<HUAWEI>
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]sysname I-LSR
[*HUAWEI]interface GE1/0/0
[*HUAWEI-GE1/0/0]undo portswitch
[*HUAWEI-GE1/0/0]description LINK->LSR-1
[*HUAWEI-GE1/0/0]ip address 10.128.0.1 255.255.255.252
[*HUAWEI-GE1/0/0]undo shutdown
[*HUAWEI-GE1/0/0]quit
[*HUAWEI]commit
[~I-LSR]
```

Figura 3-9: Configuración de direccionamiento IP

Fuente: Elaborado por el auto

3.6.4 Configuración de protocolo de enrutamiento dinámico IS-IS

Después de configurar el direccionamiento IP, ahora se debe seleccionar un protocolo de enrutamiento que soporte extensiones de ingeniería de tráfico, IS-IS y OSPF son los protocolos que soportan las herramientas de TE, la simulación estará basada en IS-IS. La configuración se la hace en las interfaces que participarán en el dominio de la red *Backhaul* IP/MPLS. Esto con el fin de proporcionar enrutamiento dinámico y proporcionar alta disponibilidad a nivel lógico, según lo estudiado en el capítulo anterior.

El protocolo IS-IS, proporciona herramientas para la ejecución de técnicas de manipulación de tráfico y establecimiento de adyacencias entre dispositivos que ejecuten el mismo protocolo. Para la configuración, se debe tener en cuenta el proceso de IS-IS es de conocimiento local; seguidamente se debe configurar la NET (*network-entity tittle*), estos parámetros son obligatorios para generar vecindad entre dos dispositivos de red que formen parte de la nube IP/MPLS.

A continuación, se muestra la configuración del protocolo IS-IS, para los demás dispositivos e interfaces se aplican los mismos comandos, teniendo en cuenta el tipo de red y el nivel de área de IS-IS, esto según el diseño de la Topología de red Backhaul.como se muestra en la Figura 3-10

```
[~I-LSR]isis 100
[*I-LSR-isis-100]network-entity 49.0001.0000.0000.0006.00
[*I-LSR-isis-100]quit
[*I-LSR]interface GE1/0/0
[*I-LSR-GE1/0/0]isis enable 100
[*I-LSR-GE1/0/0]isis circuit-type p2p
[*I-LSR-GE1/0/0]isis circuit-level level-1-2
[*I-LSR-GE1/0/0]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-10: Configuración de IS-IS

Fuente: Elaborado por el autor

Concluido la configuración del protocolo IS-IS, en todos los dispositivos e interfaces de cara a la nube de IP/MPLS que conforman la red IP *Backhaul*, se puede comprobar la base de datos de las adyacencias generadas por el protocolo, dicha información indica que las configuraciones están correctas en todas sus instancias.

En la Figura 3-11, se muestra una salida de la CLI, donde se muestra el *System* ID que se configuró previamente, las interfaces IS-IS, el tipo de nivel de área que se encuentra en cada interfaz y entre otros parámetros a considerar como tiempo de espera que IS-IS esperará antes de dar por caída la vecindad y estado de la adyacencia arriba o abajo.

```
<LSR-1>display isis peer

Peer Information for ISIS(100)
--------------------------------------------------------------------------------

  System ID     Interface       Circuit ID        State HoldTime(s) Type     PRI
--------------------------------------------------------------------------------
0000.0000.0006  GE1/0/0         0000000005         Up            28 L1L2     --
0000.0000.0002  GE1/0/1         0000000006         Up            26 L2       --
0000.0000.0004  GE1/0/2         0000000007         Up            28 L2       --
0000.0000.0003  GE1/0/3         0000000005         Up            25 L2       --

Total Peer(s): 4
<LSR-1>
```

Figura 3-11: Adyacencias de IS-IS

Fuente: Elaborador por el autor

3.6.5 Configuración de MPLS

La configuración de MPLS será establecida dentro de los equipos de la red que formen parte de la nube IS-IS, cuyas interfaces son las que participan para la conmutación por etiquetas, serán distribuidas de manera dinámica mediante el protocolo LDP. El parámetro inicial y obligatorio es el

LSR-ID cuyo identificador para todos los *routers* será la loopback 0, dicho parámetro identifica al dispositivo. Luego se procede a habilitar MPLS de manera global en cada dispositivo de la red, y a su vez en cada interfaz directamente conectada a la nube de IS-IS. En la Figura 3-12, se muestra la configuración de un dispositivo y sus interfaces, y la misma configuración aplica para los demás equipos.

```
[~I-LSR]mpls lsr-id 10.10.10.10
[*I-LSR]mpls
Info: Mpls starting, please wait... OK!
[*I-LSR-mpls]quit
[*I-LSR]mpls ldp
[*I-LSR-mpls-ldp]quit
[*I-LSR]commit
Committing....done.
[~I-LSR]interface GE1/0/0
[~I-LSR-GE1/0/0]mpls
[*I-LSR-GE1/0/0]mpls ldp
[*I-LSR-GE1/0/0]commit
[~I-LSR-GE1/0/0]
```

Figura 3-12: Configuración de MPLS y LDP

Fuente: Elaborado por el autor.

3.6.6 Configuración de MPLS TE y MPLS RSVP-TE

El siguiente paso consiste en habilitar *MPLS TE* y *MPLS RSVP-TE* serán configurados a nivel global de todos los equipos que formen parte de la nube MPLS, y en cada interfaz que esté directamente conectada con otros dispositivos que ejecuten MPLS. Como se estudió en el capítulo anterior estas herramientas permiten tener visibilidad de los recursos de toda la red, los cuales se puede disponer para manipular tráfico basado en las necesidades y requerimiento que sean solicitados.

A continuación, se muestra la configuración en un dispositivo de red y su interfaz, el mismo procedimiento aplica en todos los dispositivos e interfaces dentro del *backbone ip bakchaul* IP/MPLS, como se observa en la Figura 3-13.

```
[~I-LSR]mpls
[~I-LSR-mpls]mpls te
[*I-LSR-mpls]mpls rsvp-te
[*I-LSR-mpls]quit
[*I-LSR]interface GE1/0/0
[*I-LSR-GE1/0/0]mpls te
[*I-LSR-GE1/0/0]mpls rsvp-te
[*I-LSR-GE1/0/0]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-13:Configuración de MPLS TE y MPLS RSVP-TE

Fuente: Elaborado por el autor.

3.6.7 Configuración del protocolo CSPF

Los túneles de ingeniería de tráfico sobre MPLS son unidireccionales, por tal motivo, el protocolo CSPF será configurado en los dispositivos que a nivel lógico su comportamiento sea de tipo *Ingress*-LSR; o aquel que inicie la reserva de recursos para establecer un túnel TE. El aporte de CSPF en este diseño es, proporcionar caminos más cortos y libre de bucle, ya que al ser una extensión de SPF, tiene visibilidad de toda la red y, así poder proporcionar rutas de extremo a extremo. La configuración es la siguiente, como se muestra en la Figura 3-14

```
[~I-LSR]mpls
[~I-LSR-mpls]mpls te cspf
[*I-LSR-mpls]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-14: Configuración de CSPF

Fuente: Elaborado por el autor.

3.6.8 Configuración de IS-IS TE

IS-IS genera dos tuplas de tipo, longitud y valor (TLV), una para una adyacencia IS-IS y la segunda para un prefijo IP. Para permitir que IS-IS admita la ingeniería de tráfico, se ha agregado un segundo par de TLV a IS-IS, uno para prefijos IP y el segundo para información de ingeniería de tráfico y adyacencia IS-IS (Cisco System, 2015).

La configuración debe ser aplicada dentro del proceso IS-IS, e indicar en nivel de área al cual será aplicado para soportar una extensión del protocolo para el soporte de TE, como se observa en la Figura 3-15.

```
[~I-LSR]isis 100
[~I-LSR-isis-100]cost-style wide
Info: Cost style Changed. IS-IS process 100 will be reset.
[*I-LSR-isis-100]traffic-eng Level-1-2
[*I-LSR-isis-100]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-15: Extensión de TE en IS-IS

Fuente: Elaborado por el autor

3.6.9 Configuración de reserva de ancho de banda

Para reservar ancho de banda que permita garantizar la cantidad de recursos solicitados para establecer túneles de ingeniería de tráfico, se debe reservar en las interfaces de reenvío durante todo el camino. Una buena práctica es reservar recursos en todas las interfaces, ya que los túneles son unidireccionales. A continuación, se establece el ancho de banda máximo reservable y el ancho de banda BC0 para el enlace en cada interfaz a lo largo del túnel TE.

```
[~I-LSR]interface GE1/0/0
[~I-LSR-GE1/0/0]mpls te bandwidth max-reservable-bandwidth 100000
[*I-LSR-GE1/0/0]mpls te bandwidth bc0 100000
[*I-LSR-GE1/0/0]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-16: Reserva de ancho de banda

Fuente: Elaborado por el autor.

La configuración aplicada anteriormente, es homóloga en toda la red IP/MPLS por lo que, los comandos aplicados deben ser ejecutados en las demás interfaces de los diferentes dispositivos que participan en la nube de MPLS.

3.6.10 Configuración de Túnel dinámico.

En este paso, se creará un túnel TE de manera dinámica, basado en la base de datos y la visibilidad de los recursos de la red proporcionados por RSVP y TED. Se establecerán los requisitos necesarios para el túnel como ancho de banda.

A continuación, se muestra la creación de un túnel para el transporte de tráfico proveniente de servicios LTE *Advance*.

Entre los parámetros configurados, se especifica el tipo protocolo que será utilizado para el establecimiento del túnel, de igual manera, el protocolo que permitirá censar los recursos disponibles a lo largo del camino que cruzará el túnel; entre otros parámetros dispensables para el correcto establecimiento entre dispositivos de origen y destino.

```
[~I-LSR]interface tunnel 20
[*I-LSR-Tunnel20]description TUNNEL_LTE+
[*I-LSR-Tunnel20]ip address unnumbered interface LoopBack0
[*I-LSR-Tunnel20]tunnel-protocol mpls te
[*I-LSR-Tunnel20]mpls te signal-protocol rsvp-te
[*I-LSR-Tunnel20]destination 20.20.20.20
[*I-LSR-Tunnel20]mpls te bandwidth ct0 10000
[*I-LSR-Tunnel20]mpls te tunnel-id 200
[*I-LSR-Tunnel20]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-17: Configuración de túnel TE dinámico

Fuente: Elaborado por el autor.

3.6.11 Creación de Túnel TE auto-frr con explicit path

Otra de las técnicas que ofrece la red *Backhaul* IP/MPLS TE, es poder establecer túneles de ingeniería de tráfico que ayuden a minimizar tiempo de respuesta ante una falla. Con esta herramienta *auto-frr*, y apoyada por *explicit path*, el cual es especificado por los administradores de red para tener la alta disponibilidad de los servicios. Es decir, a más de que se genere el túnel automáticamente, se especifica una ruta de respaldo para conmutar tráfico en caso de alguna eventualidad, esto hasta que se recupere el camino principal.

Se debe habilitar la funcionalidad de *auto-frr*, luego especificar la ruta explícita por donde vamos a mover el tráfico, y finalmente configurar el túnel especificando parámetros que se han configurado previamente, a más de especificar la ruta explícita y prioridades de atributos para cuando falle el LSP.

```
[~I-LSR]mpls
[~I-LSR-mpls]mpls te auto-frr
[*I-LSR-mpls]quit
[*I-LSR]explicit-path TUNNEL-MULTICAST-PATH
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 10.128.0.2
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 10.128.0.42
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 10.128.0.37
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 10.128.0.34
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 10.128.0.14
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]next hop 20.20.20.20
[*I-LSR-explicit-path-TUNNEL-MULTICAST-PATH]quit
[*I-LSR]interface Tunnel 1
[*I-LSR-Tunnel1]description TUNNEL_MULTICAST
[*I-LSR-Tunnel1]ip address unnumbered interface LoopBack0
[*I-LSR-Tunnel1]tunnel-protocol mpls te
[*I-LSR-Tunnel1]destination 20.20.20.20
[*I-LSR-Tunnel1]mpls te record-route label
[*I-LSR-Tunnel1]mpls te priority 4 3
[*I-LSR-Tunnel1]mpls te bandwidth ct0 5000
[*I-LSR-Tunnel1]mpls te fast-reroute bandwidth
[*I-LSR-Tunnel1]mpls te tunnel-id 300
[*I-LSR-Tunnel1]mpls te path explicit-path TUNNEL-MULTICAST-PATH
[*I-LSR-Tunnel1]mpls te bypass-attributes bandwidth 3000 priority    5 4
[*I-LSR-Tunnel1]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-18: Configuración de túnel TE con auto-frr y explicit-path

Fuente: Elaborado por el autor.

3.6.12 Creación de Túnel TE con backup hot-standby y bfd.

La técnica de ingeniería de tráfico de *backup hot-standby* y *bfd*, ayuda a tener un mejor control del tráfico. Con el fin de poder manipular las rutas por donde pasar datos de un extremo a otro, y establecer caminos explícitos es de suma importancia para tráfico crítico con alta sensibilidad al retardo y *jitter*. Al juntar estas herramientas con bfd, lo que aporta es la detección de caída de algún LSP para poder conmutar el tráfico hacia otro LSP alterno, minimizando considerablemente la pérdida de paquetes.

Por lo que se configura rutas explícitas específicas para los LSPs principal y respaldo. Luego establecer la función BFD para la detección inmediata de la disponibilidad de los LSP, luego se configura el túnel con las características y necesidades donde se incluyan los caminos explícitos configurados. Posteriormente se especifica qué hacer en caso de que los LSPs no estén disponibles, para ellos se especifica que tome como último recurso una ruta proporcionada por la tabla de ruteo del protocolo IS-IS, como se muestra en la Figura 3-19.

```
[~I-LSR]bfd
[*I-LSR-bfd]quit
[*I-LSR]explicit-path MAIN
[*I-LSR-explicit-path-MAIN]next hop 10.128.0.2
[*I-LSR-explicit-path-MAIN]next hop 10.128.0.6
[*I-LSR-explicit-path-MAIN]next hop 10.128.0.10
[*I-LSR-explicit-path-MAIN]next hop 20.20.20.20
[*I-LSR-explicit-path-MAIN]quit
[*I-LSR]explicit-path BACKUP
[*I-LSR-explicit-path-BACKUP]next hop 10.128.0.22
[*I-LSR-explicit-path-BACKUP]next hop 10.128.0.18
[*I-LSR-explicit-path-BACKUP]next hop 10.128.0.14
[*I-LSR-explicit-path-BACKUP]next hop 20.20.20.20
[*I-LSR-explicit-path-BACKUP]quit
[*I-LSR]interface Tunnel 500
[*I-LSR-Tunnel500]description TUNNEL_DATOS
[*I-LSR-Tunnel500]ip address unnumbered interface LoopBack0
[*I-LSR-Tunnel500]tunnel-protocol mpls te
[*I-LSR-Tunnel500]destination 20.20.20.20
[*I-LSR-Tunnel500]mpls te record-route label
[*I-LSR-Tunnel500]mpls te priority 3 2
[*I-LSR-Tunnel500]mpls te bandwidth ct0 15000
[*I-LSR-Tunnel500]mpls te path explicit-path MAIN
[*I-LSR-Tunnel500]mpls te path explicit-path BACKUP secondary
[*I-LSR-Tunnel500]mpls te backup ordinary best-effort
[*I-LSR-Tunnel500]mpls te backup hot-standby mode revertive wtr 15
[*I-LSR-Tunnel500]mpls te reserved-for-binding
[*I-LSR-Tunnel500]mpls te tunnel-id 500
[*I-LSR-Tunnel500]mpls te bfd enable
[*I-LSR-Tunnel500]mpls te bfd min-tx-interval 3 min-rx-interval 3 detect-multipl
ier 3
[*I-LSR-Tunnel500]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-19: Configuración de túnel TE hot-standby y bfd

Fuente: Elaborado por el autor.

3.6.13 Configuración de direccionamiento ip para los servicios.

Una vez que se ha revisado e implementado las técnicas de ingeniería de tráfico, esto indica que la infraestructura está lista para poder mover cualquier tipo de tráfico desde un origen a un destino.

Lo siguiente será simular los diferentes servicios que se podrán transportar por la red *Backhaul* IP/MPLS con ingeniería de tráfico y calidad de servicio. Para ello, basado en Anexo 0-1 se procede con la configuración de las interfaces que van a permitir simular servicios como MULTICAST, DATOS, LTE+ y VOIP, esto en los dispositivos que darán acceso a la red; y, así mismo con la configuración de los dispositivos que simulan los diferentes servicios que se han mencionado.

En la Figura 3-20, se ilustra la configuración de direccionamiento ip, donde se simulan los diferentes servicios que estarán cruzando por la red *Backhaul* IP/MPLS

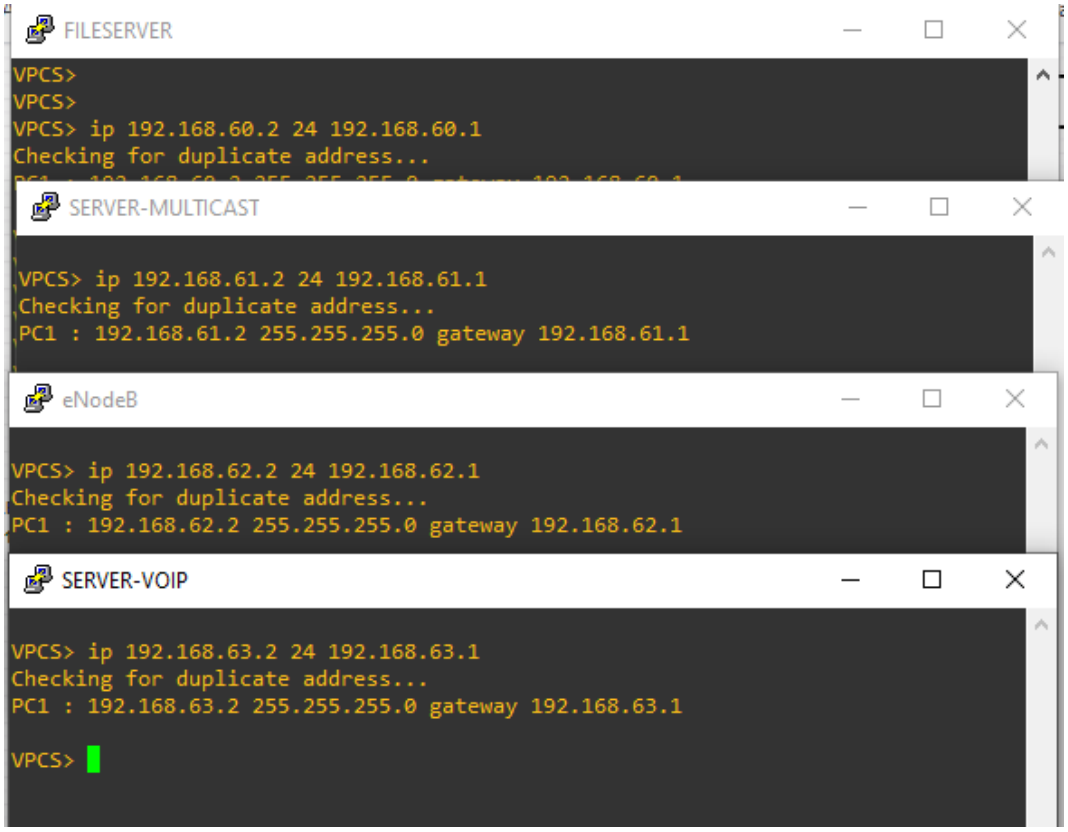


Figura 3-20: Configuración de ip a servidores para servicios

Fuente: Elaborado por el autor

3.6.14 Configuración de rutas estáticas para alcanzar los servicios.

Para que el tráfico generado por los usuarios se pueda identificar a cuál servicio corresponde, los dispositivos I-LSR, deben conocer por donde mover el tráfico relacionado a ese servicio, por tal motivo, se deben crear rutas con destino hacia los túneles de ingeniería de tráfico.

Como se muestra en la Figura 3-21, se crean rutas estáticas para alcanzar los servicios, y estas tienen como siguiente salto los túneles creados en los pasos anteriores.

```
ip route-static 192.168.60.0 255.255.255.0 Tunnel500 description DATOS
ip route-static 192.168.61.0 255.255.255.0 Tunnel1 description MULTICAST
ip route-static 192.168.62.0 255.255.255.0 Tunnel20 description LTE+
ip route-static 192.168.63.0 255.255.255.0 Tunnel10 description VOIP
```

Figura 3-21: Configuración de rutas estáticas

Fuente: Elaborado por el autor

3.6.15 Configuración de L3VPN sobre MPLS

El diseño presentado al inicio del capítulo, y con la configuración empleada permiten desplegar tecnologías como vpn de capa 3 o L3VPN.

Esto debido a que la infraestructura que corre MPLS y otras tecnologías, presta las comodidades para este tipo de soluciones para transportar datos o interconectar diferentes sitios; como es el caso de las vpn.

En este caso Tabla 3-1: Sesión iBGP, BGP nos permite establecer este tipo de soluciones, por lo cual se muestra la configuración entre dos extremos para la interconexión de dos sitios sobre la red de transporte *Backhaul* IP/MPLS con ingeniería de tráfico y calidad de servicios.

Tabla 3-1: Sesión iBGP

I-LSR	E-LSR
[~I-LSR]bgp 100 [*I-LSR-bgp] peer 20.20.20.20 as-number 100 [*I-LSR-bgp] peer 20.20.20.20 connect-interface LoopBack0 [*I-LSR-bgp]ipv4-family unicast [*I-LSR-bgp-af-ipv4] peer 20.20.20.20 enable [*I-LSR-bgp-af-ipv4]commit [~I-LSR-bgp-af-ipv4]	[~E-LSR]bgp 100 [*E-LSR-bgp] peer 10.10.10.10 as-number 100 [*E-LSR-bgp] peer 10.10.10.10 connect-interface LoopBack0 [*E-LSR-bgp]ipv4-family unicast [*E-LSR-bgp-af-ipv4] peer 10.10.10.10 enable [*E-LSR-bgp-af-ipv4]commit [~E-LSR-bgp-af-ipv4]

Fuente: Elaborado por el autor

Lo siguiente es configurar una instancia VPN o VRF, la cual será asignada a la interfaz y posteriormente asignada una dirección ip a la interfaz. Para ello se habilita la instancia VPN, luego la familia de protocolo ipv4; y luego habilitar opciones para importar y exportar rutas sobre L3VPN, como se muestra en la Figura 3-22.

```
[~I-LSR]ip vpn-instance L3VPN
[*I-LSR-vpn-instance-L3VPN]ipv4-family
[*I-LSR-vpn-instance-L3VPN-af-ipv4]route-distinguisher 100:1
[*I-LSR-vpn-instance-L3VPN-af-ipv4]vpn-target 111:1 export-extcommunity
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[*I-LSR-vpn-instance-L3VPN-af-ipv4]vpn-target 111:1 import-extcommunity
 IVT Assignment result:
Info: VPN-Target assignment is successful.
[*I-LSR-vpn-instance-L3VPN-af-ipv4]quit
[*I-LSR-vpn-instance-L3VPN]quit
[*I-LSR]interface GE 1/0/2
[*I-LSR-GE1/0/2]undo portswitch
[*I-LSR-GE1/0/2]ip binding vpn-instance L3VPN
Info: All IPv4 and IPv6 related configurations on this interface are removed.
[*I-LSR-GE1/0/2]ip address 192.168.100.1 255.255.255.252
[*I-LSR-GE1/0/2]quit
[*I-LSR]commit
[~I-LSR]
```

Figura 3-22: Configuración de L3VPN

Fuente: Elaborador por el autor.

En la Tabla 3-2 se muestra la configuración de la instancia vpn dentro del proceso de BGP, donde mediante los identificativos de *router distinguisher* y *route target* estos pueden establecer una adyacencia virtual para poder importar y exportar prefijos de red en ambos sitios remotos.

Tabla 3-2: Sesión eBGP y configuración de equipos CE

I-LSR	E-LSR
[~I-LSR]bgp 100 [*I-LSR-bgp] ipv4-family vpn-instance L3VPN [*I-LSR-bgp-L3VPN]peer 192.168.100.2 as-number 65410 [*I-LSR-bgp-L3VPN] import-route direct [*I-LSR-bgp] ipv4-family vpnv4 [*I-LSR-bgp-af-vpnv4]policy vpn-target [*I-LSR-bgp-af-vpnv4]peer 20.20.20.20 enable [*I-LSR-bgp-af-ipv4]commit [~I-LSR-bgp-af-ipv4]	[~E-LSR]bgp 100 [*E-LSR-bgp] ipv4-family vpn-instance L3VPN [*E-LSR-bgp-L3VPN]peer 192.168.100.2 as-number 65410 [*E-LSR-bgp-L3VPN] import-route direct [*E-LSR-bgp] ipv4-family vpnv4 [*E-LSR-bgp-af-vpnv4]policy vpn-target [*E-LSR-bgp-af-vpnv4]peer 20.20.20.20 enable [*E-LSR-bgp-af-ipv4]commit [~E-LSR-bgp-af-ipv4]
CE1	
[~CE1]interface ge1/0/0 [*CE1-GE1/0/0] undo portswitch [*CE1-GE1/0/0] ip address 192.168.100.2 255.255.255.252 [*CE1-GE1/0/0]quit [*CE1]bgp 65410 [*CE1-bgp] peer 192.168.100.1 as-number 100 [*CE1-bgp] ipv4-family unicast [*CE1-bgp-af-ipv4] peer 192.168.100.1 enable [*CE1-bgp-af-ipv4] import-route direct [*CE1-bgp-af-ipv4]commit [~CE1-bgp-af-ipv4]	[~CE2]interface ge1/0/0 [*CE2-GE1/0/0] undo portswitch [*CE2-GE1/0/0] ip address 192.168.200.2 255.255.255.252 [*CE2-GE1/0/0]quit [*CE2]bgp 65410 [*CE2-bgp] peer 192.168.200.1 as-number 100 [*CE2-bgp] ipv4-family unicast [*CE2-bgp-af-ipv4] peer 192.168.200.1 enable [*CE2-bgp-af-ipv4] import-route direct [*CE2-bgp-af-ipv4]commit [~CE2-bgp-af-ipv4]

Fuente: Elaborado por el autor.

3.6.16 Configuración de L2VPN IP/MPLS QoS

En este apartado se procederá a configurar una red IP/MPLS con calidad de servicio para el despliegue de *VPN* de capa 2, con el objetivo de proveer de conexión *LAN* extendida a los usuarios.

En esta parte se omitirá la configuración del direccionamiento ip de las interfaces y la configuración del protocolo IS-IS, debido a que anteriormente ya se realizaron, y el procedimiento es el mismo; incluyendo la configuración de MPLS y LDP.

Por tal motivo se partirá de la configuración de *L2VPN* y QoS. La siguiente configuración de una sesión remoto de LDP se debe crear en PE1 y PE2

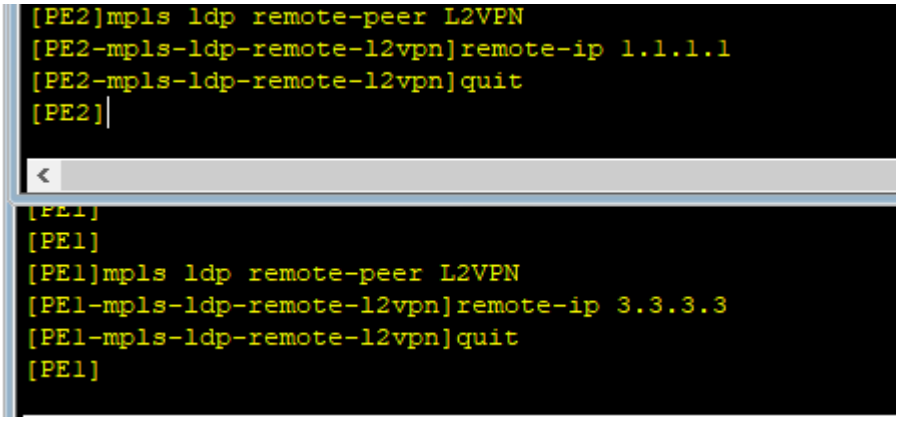


Figura 3-23: Configuración de remote-peer LDP

Fuente: Elaborado por el autor.

Lo siguiente será habilitar la extensión de MPLS para L2VPN, eso debe ser aplicado en los dispositivos PE1 y PE2 con el siguiente comando:

```
[PE1]mpls l2vpn
[PE1-l2vpn]quit
[PE1]
```

Figura 3-24: Habilitar L2VPN en MPLS

Fuente: Elaborado por el autor.

A continuación, se debe configurar el circuito de MPLS para que se establezca la VPN de capa 2, se debe considerar que el identificador debe

ser igual en ambos extremos, tanto en PE1 y PE2 de la Figura 3-25; a su vez, en este paso se manipula el campo de *EXP* de MPLS

```
[PE1]interface Vlanif 10
[PE1-Vlanif10]mpls l2vc 3.3.3.3 200
[PE1-Vlanif10] diffserv-mode pipe mpls-exp 5

[PE2]interface Vlanif 40
[PE2-Vlanif40]mpls l2vc 1.1.1.1 200
[PE2-Vlanif40] diffserv-mode pipe mpls-exp 5
```

Figura 3-25: Configuración del circuito virtual L2VC

Fuente: Elaborado por el autor.

Como se estudió en el capítulo anterior, los conceptos fundamentales sobre los dominios en calidad de servicios. Ahora se debe configurar un dominio de servicios diferenciados, esto con el objetivo manipular los bits para la calidad de servicio, y poder pasar de un *diff-serv* a otro, según el criterio del administrador.

```
[PE1] diffserv domain default
[PE1-dsdomain-default] ip-dscp-inbound 43 phb ef green

[PE2] diffserv domain default
[PE2-dsdomain-default] ip-dscp-inbound 43 phb ef green
```

Figura 3-26: Configuración de DiffServ

Fuente: Elaborado por el autor.

Lo siguiente, es crear una nueva L2VPN aplicando una política de servicios diferenciados que se creó anteriormente manipulando el campo *EXP* de la cabecera MPLS.

```
[PE1]interface Vlanif 20
[PE1-Vlanif10]mpls l2vc 3.3.3.3 300
[PE1-Vlanif10] diffserv-mode short-pipe mpls-exp 3 domain default

[PE2]interface Vlanif 40
[PE2-Vlanif40]mpls l2vc 1.1.1.1 200
[PE2-Vlanif40] diffserv-mode short-pipe mpls-exp 3 domain default
```

Figura 3-27: Configuración de QoS mediante DiffServ

Fuente: Elaborado por el autor.

Luego se procede a crear listas de control de acceso para identificar el tráfico de origen, y así poder aplicar políticas de calidad de servicio basado en criterios de consumo de ancho de banda

```
acl number 2500
 rule 5 permit source 192.168.80.1 0
#
acl number 2501
 rule 5 permit source 192.168.90.1 0
#
traffic classifier clase1 operator and
 if-match acl 2500
traffic classifier clase2 operator and
 if-match acl 2501
#
traffic behavior comportamiento1
 car cir 10000 pir 11000 cbs 11000 pbs 11000 green pass yellow pass red discard
traffic behavior comportamiento2
 car cir 20000 pir 21000 cbs 2500000 pbs 2625000 green pass yellow pass red disc
ard
#
traffic policy policy1
 classifier clase1 behavior comportamiento1
 classifier clase2 behavior comportamiento2
#
```

Figura 3-28: Configuración de QoS

Fuente: Elaborado por el autor

CAPITULO 4 . ANALISIS DE RESULTADOS

En este capítulo se presentarán los resultados obtenidos en la experimentación del establecimiento de túneles de ingeniería de tráfico y calidad de servicio.

A continuación, se mostrará las pruebas realizadas para pasar tráfico de un origen a un destino, poniendo a prueba los túneles de ingeniería de tráfico, soportados sobre la red *Backhaul* IP/MPLS.

4.1 Túnel de ingeniería de tráfico dinámico

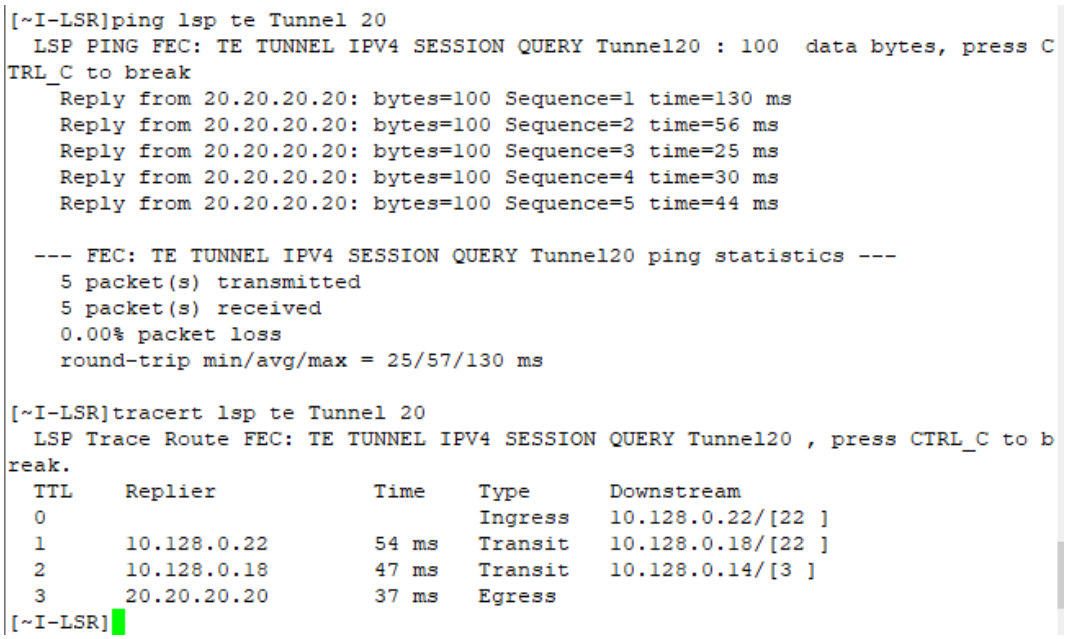
En la Figura 4-1 se puede evidenciar, que, basada en las configuraciones del capítulo anterior, se establece el túnel, ya que su estado es levantado o *UP*, entre otra información muestra el tamaño de ancho de banda asignado al túnel, el destino con el cual se está estableciendo el túnel de ingeniería de tráfico de manera dinámica.

```
[~I-LSR]display interface Tunnel 20
Tunnel20 current state : UP (ifindex: 22)
Line protocol current state : UP
Last line protocol up time : 2021-02-08 23:03:57
Description: TUNNEL_LTE+
Route Port,The Maximum Transmit Unit is 1500, Current BW: 10Mbps
Internet Address is unnumbered, using address of LoopBack0(10.10.10.10/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 20.20.20.20
Tunnel up/down statistics 1
Tunnel ct0 bandwidth is 10000 Kbit/sec
Tunnel protocol/transport MPLS/MPLS, ILM is available
primary tunnel id is 0x2182, secondary tunnel id is 0x0
Current system time: 2021-02-09 01:11:22
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
    0 output drop
    Last 300 seconds input utility rate:  0.00%
    Last 300 seconds output utility rate: 0.00%
```

Figura 4-1: Información de tunnel_LTE+ Dinámico

Fuente: Elaborado por el autor.

Para comprobar que el túnel está transportando datos, en la Figura 4-2, se evidencia que el ping es afirmativo y está cruzando tráfico mediante el túnel que ha construido su LSP de manera dinámica, basado en la información proporcionada por el protocolo IS-IS.



```
[~I-LSR]ping lsp te Tunnel 20
  LSP PING FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel20 : 100  data bytes, press C
TRL_C to break
    Reply from 20.20.20.20: bytes=100 Sequence=1 time=130 ms
    Reply from 20.20.20.20: bytes=100 Sequence=2 time=56 ms
    Reply from 20.20.20.20: bytes=100 Sequence=3 time=25 ms
    Reply from 20.20.20.20: bytes=100 Sequence=4 time=30 ms
    Reply from 20.20.20.20: bytes=100 Sequence=5 time=44 ms

  --- FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel20 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/57/130 ms

[~I-LSR]tracert lsp te Tunnel 20
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel20 , press CTRL_C to b
reak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   10.128.0.22/[22 ]
  1      10.128.0.22        54 ms   Transit   10.128.0.18/[22 ]
  2      10.128.0.18        47 ms   Transit   10.128.0.14/[3 ]
  3      20.20.20.20        37 ms   Egress
[~I-LSR]
```

Figura 4-2: Prueba de funcionamiento de túnel dinámico

Fuente: Elaborado por el autor.

A su vez, en la Figura 4-2 se puede evidenciar el camino que toma el tráfico para alcanzar su destino, esto debido a las configuraciones donde se establece calidad de servicios en las interfaces, y los recursos anunciados mediante los protocolos implementados.

4.2 Túnel de ingeniería de tráfico dinámico con auto-frr

Las herramientas de ingeniería de tráfico para la implementación de túneles te, aporta mucho para la alta disponibilidad de los servicios mediante caminos o LSP redundantes, ahora evidencia que juntando la creación de túnel dinámico más un atributo de convergencia rápida ante una falla en el LSP principal pueda conmutar de manera expedita a otro LSP.

En la Figura 4-3, se muestra el estado del túnel previamente configurado, se evidencia que el túnel tiene un estado UP, y donde se evidencia principalmente que tiene una ruta explicita por la cual se conmuta el tráfico, en caso de que ese LSP se interrumpa, se establecerá automáticamente un LSP dinámico para seguir cruzando tráfico hacia el destino. Debido a que los protocolos utilizados tienen visibilidad de todos

los recursos de la red, el túnel siempre va a estar arriba así que interrumpa el LSP explícito.

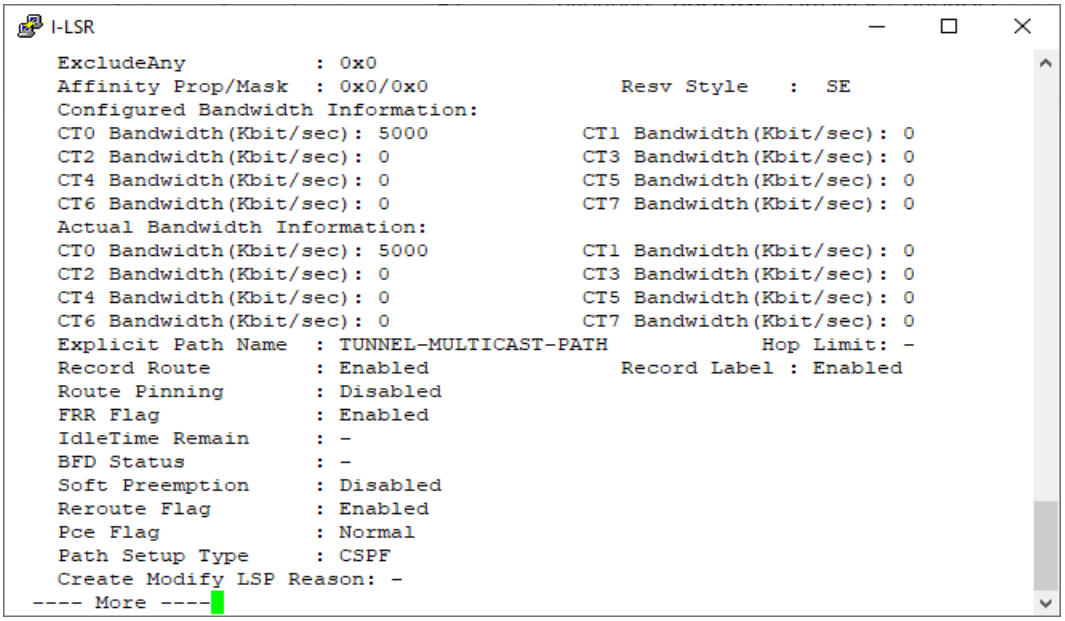


Figura 4-3: Túnel TE dinámico auto-frr

Fuente: Elaborado por el autor

En la Figura 4-4, se evidencia mediante el comando *ping* la funcionalidad del túnel, y mediante el comando *tracert* se demuestra la ruta explícita que está tomando el tráfico para mover hacia el destino especificado en la configuración del túnel en el capítulo anterior. Lo que indica que el tráfico se conmuta basado en las políticas de ingeniería de tráfico, y no sobre los caminos proporcionados por el protocolo de enrutamiento.

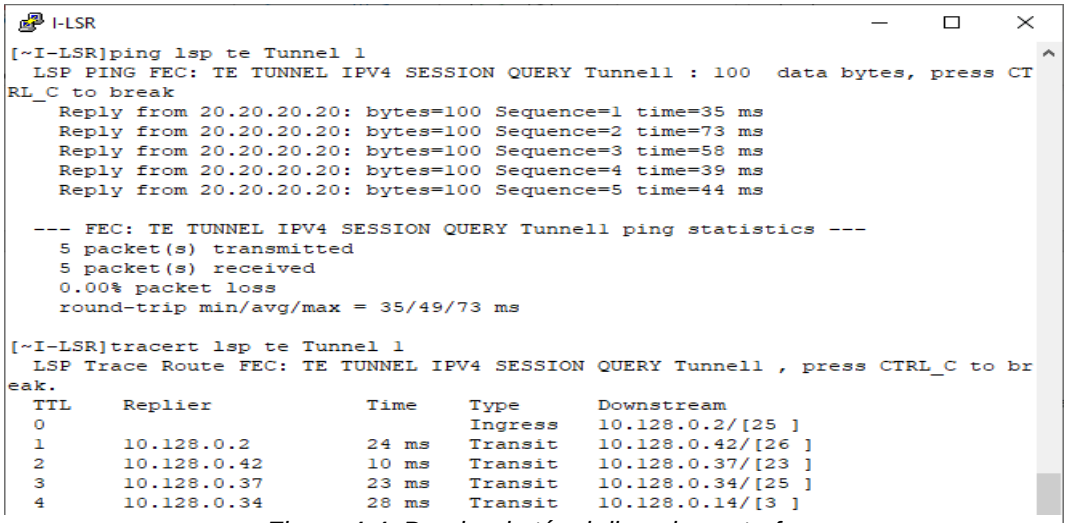


Figura 4-4: Prueba de túnel dinamico auto-frr

Fuente: Elaborado por el autor

4.3 Túnel de ingeniería de tráfico backup hot-standby y bfd

A continuación, evaluaremos otra técnica de ingeniería de tráfico y calidad de servicio, esta técnica es *backup hot-standby* con bfd, la cual se basa en las herramientas estudiadas e implementadas con el fin de proporcionar una resiliencia de la red en un menor tiempo posible, tiene caminos LSP redundantes explícitos y una ruta de mejor esfuerzo.

A su vez, apoyarse sobre bfd para la detección de caída de enlaces de manera expedita, y basado en la información del bfd el túnel de ingeniería de tráfico pueda conmutar de manera expedita minimizando pérdida de paquetes y tiempos de respuesta para servicios sensibles al retardo.

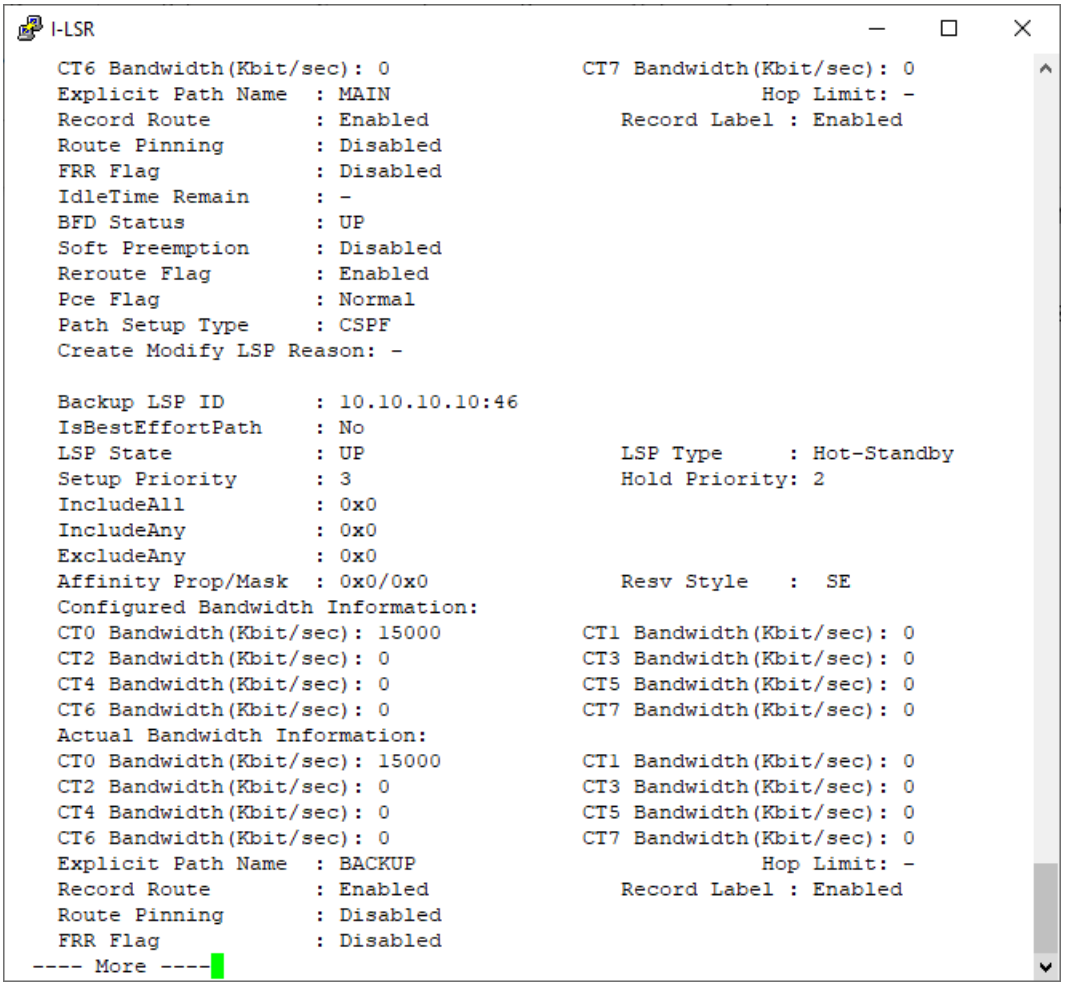


Figura 4-5: Túnel backup hot-standby y bfd

Fuente: Elaborado por el autor

Como se observa en la Figura 4-5, los LSP explícito que fueron configurados en el capítulo anterior, y tiene una tercera ruta proporcionada por el protocolo de enrutamiento.

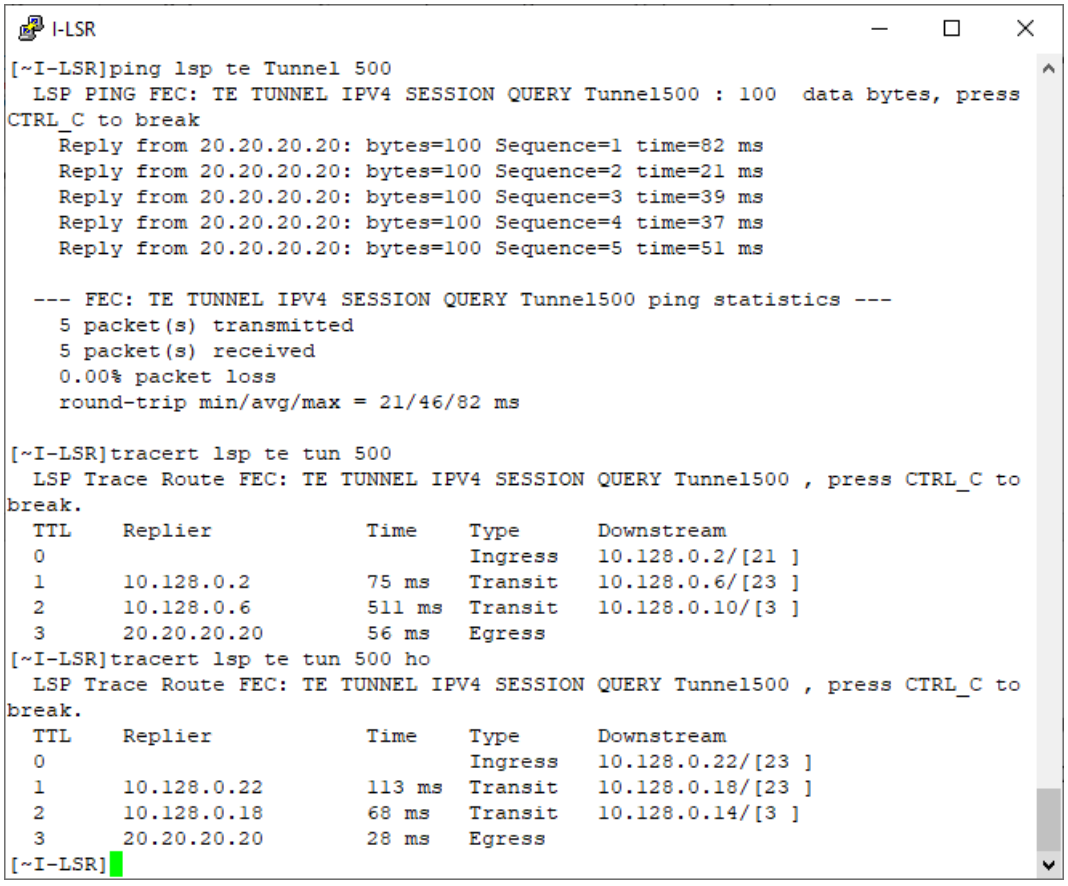


Figura 4-6: Prueba de túnel backup hot.standby y bfd

Fuente: Elaborado por el autor

En la figura anterior, se evidencia la prueba satisfactoria de cruzar tráfico sobre el túnel de ingeniería de tráfico basado en *backup hot-standby*, con la ayuda de BFD para la detección rápida de alguna caída de enlace. Se muestran las rutas explícitas que toma y tomaría en caso de que la ruta principal dejara de funcionar.

En la Figura 4-7, se observa el estado de la sesión de BFD, la cual está en levantada o UP, y censando el camino proporcionado por MPLS-TE, y en caso de que el enlace falle, este avisa de manera expedita al túnel, y esta conmuta a otro LSP de respaldo.

```
[~I-LSR]display bfd session mpls-te interface Tunnel 500 te-lsp
S: Static session
D: Dynamic session
IP: IP session
IF: Single-hop session
PEER: Multi-hop session
LDP: LDP session
LSP: Label switched path
TE: Traffic Engineering
AUTO: Automatically negotiated session
VXLAN: VXLAN session
VSI: VSI PW session
(w): State in WTR
(*): State is invalid
Total UP/DOWN Session Number : 1/0
--------------------------------------------------------------------------------
Local      Remote     PeerIpAddr      State     Type         InterfaceName
--------------------------------------------------------------------------------
16389      16389      20.20.20.20     Up        D/TE-LSP     Tunnel500
--------------------------------------------------------------------------------
```

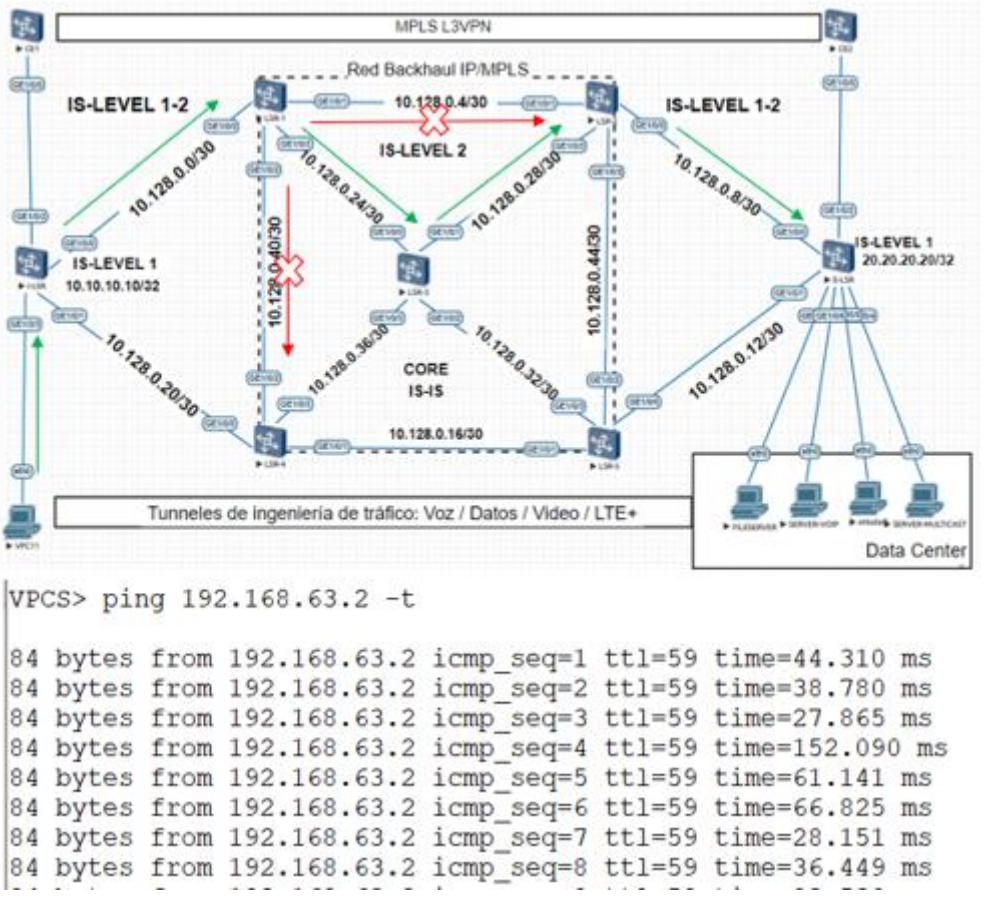
Figura 4-7: Estado de BFD

Fuente: Elaborado por el autor

Lo siguiente, una vez comprobado que los túneles de ingeniería de tráfico están funcionando y atravesando tráfico, es realizar pruebas desde los dispositivos que simulan los servicios que se van a transportar por los túneles.

Se realiza una prueba de conectividad a través del protocolo de mensajes de control de Internet o ICMP *(Internet Control Message Protocol*), para hacer uso de los túneles configurados anteriormente, esto con el fin de validar el correcto funcionamiento de los CR-LSP.

Como se puede observar en la Figura 4-8, se prueba el funcionamiento del túnel de ingeniería de tráfico para datos categorizados como VoIP, al momento de ejecutar el *PING* se empieza a apagar varias interfaces del *core* IP/MPLS, y donde se observa que, a pesar de que hay caminos caídos el tráfico sigue transitando sin ningún paquete perdido, por lo que se reduce la latencia y perdida de paquetes.




```
VPCS> ping 192.168.63.2 -t

84 bytes from 192.168.63.2 icmp_seq=1 ttl=59 time=44.310 ms
84 bytes from 192.168.63.2 icmp_seq=2 ttl=59 time=38.780 ms
84 bytes from 192.168.63.2 icmp_seq=3 ttl=59 time=27.865 ms
84 bytes from 192.168.63.2 icmp_seq=4 ttl=59 time=152.090 ms
84 bytes from 192.168.63.2 icmp_seq=5 ttl=59 time=61.141 ms
84 bytes from 192.168.63.2 icmp_seq=6 ttl=59 time=66.825 ms
84 bytes from 192.168.63.2 icmp_seq=7 ttl=59 time=28.151 ms
84 bytes from 192.168.63.2 icmp_seq=8 ttl=59 time=36.449 ms
```

Figura 4-8: Prueba de conectividad a través de icmp

Fuente: Elaborado por el autor

Una vez comprobado la funcionabilidad de los túneles de ingeniería de tráfico es necesario para realizar procesos de resolución de problemas revisando la base de datos de CSPF, la cual permite revisar adyacencias con los dispositivos vecinos, donde intercambian información como el identificador de la red, el tipo de protocolo IGP que se está utilizando. El número del proceso del protocolo de enrutamiento en el cual está ejecutándose MPLS e ingeniería de tráfico, tipo de área o nivel -en el caso

de IS-IS- y el total de enlaces que participan entre los dispositivos. Esto se evidencia en la Figura 4-9.

```
[~I-LSR]display mpls te cspf tedb all
Maximum Nodes Supported: 4096    Current Total Node Number: 8
Maximum Links Supported: 8000    Current Total Link Number: 26
Maximum SRLGs supported: 10000   Current Total SRLG Number: 0
Id     Router-Id        IGP      Process-Id     Area           Link-Count
1      10.10.10.10      ISIS     100            Level-1        2
2      1.1.1.1          ISIS     100            Level-2        4
3      2.2.2.2          ISIS     100            Level-2        4
4      3.3.3.3          ISIS     100            Level-2        4
5      4.4.4.4          ISIS     100            Level-2        4
6      5.5.5.5          ISIS     100            Level-2        4
7      10.10.10.10      ISIS     100            Level-2        2
8      20.20.20.20      ISIS     100            Level-2        2
```

Figura 4-9: Base de datos del protocolo CSPF

Fuente: Elaborado por el autor

A su vez, también es de importancia revisar el estado de sesiones remotas de LDP sobre para la distribución de etiquetas que permitan el despliegue de tecnologías con L2VPN.

```
[~I-LSR]display mpls ldp session all
 LDP Session(s) in Public Network
 LAM: Label Advertisement Mode,  KA: KeepAlive
 SsnAge: Session Age, Unit(DDDD:HH:MM)
 An asterisk (*) before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
 1.1.1.1:0          Operational DU   Active   0000:01:01   248/248
 4.4.4.4:0          Operational DU   Active   0000:01:01   248/248
 20.20.20.20:0      Operational DU   Passive  0000:01:01   247/247
------------------------------------------------------------------------------
TOTAL: 3 Session(s) Found.
```

Figura 4-10: Sesiones de LDP

Fuente: Elaborado por el autor

La implementación de túneles de ingeniería de tráfico y calidad de servicios sobre la red *Backhaul* IP/MPLS, aporta al desempeño y la administración de los recursos de la red, a su vez brinda alta disponibilidad para diferentes tipos de servicios que se pueden transportar sobre estos.

En comparación con las redes tradicionales que están basadas en el mejor esfuerzo, o mediante las rutas proporcionadas por los protocolos de enrutamiento no resultan escalables y son complejas para la administración y mantenimiento. Por tal motivo, para entornos de proveedores de servicio se necesita una expedita conmutación de paquetes, y una fácil gestión y administración de los recursos de la red, y donde IP/MPLS en conjunto con técnicas de ingeniería de tráfico y calidad de servicios aportan sustancialmente a esos requerimientos de los SP.

Conclusiones

- Mediante el análisis de los conceptos fundamentales de las tecnologías de telecomunicaciones, se pudo determinar las herramientas, métodos y modelos para el diseño y simulación de una red Backhaul basada en IP/MPLS con técnicas de ingeniería de tráfico y calidad de servicio.
- Se diseñó una red IP Backhaul, basada en IP/MPLS con MPLS-TE y QoS, mediante las técnicas y mejores prácticas proporcionadas mediante el análisis de las tecnologías de las telecomunicaciones.
- Se emuló la red con EVE-NG y eNSP lo que ha permitido experimentar configuraciones avanzadas para el manejo de protocolos y herramientas para la gestión y manipulación de tráfico.
- Se evaluó de manera exitosa la implementación de mecanismos de control de tráfico de red, aportando calidad y disponibilidad de los servicios la mayor parte del tiempo, debido a las diversas técnicas de manipulación de caminos para que los paquetes lleguen al destino.

Recomendaciones

- Los túneles de ingeniería de tráfico son unidireccionales, por lo tanto, se debe configurar correctamente la reserva de recursos durante todo el camino y la calidad de servicio para el tipo de tráfico que se va a transportar.
- Implementar esta propuesta de red Backhaul en un proveedor de servicios el cual permita evaluar el comportamiento en condiciones reales.
- Implementar el diseño de la red propuesta con programabilidad y automatización, para evaluar los tiempos de despliegue, ejecución y mantenimiento de la red.
- Implementar mecanismos de seguridad de los datos que se transportan sobre túneles de ingeniería de tráfico, para garantizar la integridad y confidencialidad de los mismos.

.

Bibliografía

AfNOG. (2013). Comparing ISIS and OSPF. Obtenido de https://networklessons.com/cisco/ccie-routing-switching-written/introduction-to-is-is#:~:text=IS%2DIS%20is%20an%20IGP,installed%20in%20the%20routing%20table.

Alvarado Rocafuerte, H. J. (2020). Simulación de túneles basados en ingeniería de tráfico sobre Core IP/MPLS usando el emulador eNSP. *UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL*.

Americas(ITLA), I. T. (2020). *forum huawei*. Obtenido de forum.huawei.com: https://forum.huawei.com/enterprise/es/mpls-ventajas-y-desventajas-miuconhuawei/thread/624052-100243

Ayala Abarca Ana Cristina, R. L. (2019). ESTUDIO Y DISEÑO DE UNA RED DE TRANSPORTE IP RAN PARA VOZ Y DATOS PARA REDES DE TELEFONÍA CELULAR DE CUARTA GENERACIÓN EN EL ECUADOR. *Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejército*, 1-8.

Bahnasse, A., Louhab, F. E., Oulahyane, H. A., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS Traffic Engineering-DiffServ Aware management. *sciencedirect*, Pages 115-126.

Bernardo A. Movsichoff, C. M. (2007). End-to-End Optimal Algorithms for Integrated QoS, Traffic Engineering, and Failure Recovery. *IEEE*, 813-823.

Brad Edgeworth, R. G. (2020). *CCNP and CCIE Enterprise Core.* Cisco Press.

Callon, R. (1990). Use of OS1 IS-IS for Routing in TCP/IP and Dual. *RFC 1195*.

Cisco System. (2005). *MPLS Basic Traffic Engineering Using IS-IS*. Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13737-mplsteisis.html

Cisco System. (2015). *Adyacencia y tipos de área IS-IS.* Obtenido de cisco.com: https://www.cisco.com/c/es_mx/support/docs/ip/integrated-intermediate-system-to-intermediate-system-is-is/200293-IS-IS-Adjacency-and-Area-Types.html

Daniel C . Frost, S. F. (2015). MPLS SEGMENT - ROUTING. *United States Patent Frost et al* .

DATTA. (5 de agosto de 2020). *DATTA*. Obtenido de https://datta.com.ec/articulo/las-telecomunicaciones-y-su-rol-decisivo

Dongli Zhang, D. I. (2007). QoS Performance Analysis in Deployment of DiffServ-aware MPLS Traffic Engineering. *IEEE Computer Society*, 963-967.

FEDERICO KUHLMANN, A. A. (s.f.). *Información y Telecomunicaciones*. Obtenido de Biblioteca Digital: http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

Huawei. (21 de 06 de 2019). *Comunidad Huawei Enterprise*. Obtenido de Forum Huawei: https://forum.huawei.com/enterprise/es/introducci%C3%B3n-al-simulador-de-red-de-huawei-ensp/thread/540753-100265#:~:text=El%20Enterprise%20Network%20Simulation%20Platform,y%20gratuita%20desarrollada%20por%20Huawei.&text=eNSP%20puede%20simular%20redes%20de

Huawei Technologies Co., Ltd. (05 de 12 de 2018). *Feature Description - IP Routing 01.* Obtenido de Huawei: https://support.huawei.com/enterprise/es/doc/EDOC1100059457/285aa82a/is-is

Huertas, J. (s.f.). *Nework Faculty.* Obtenido de https://networkfaculty.com/es/video/detail/58-mpls-te---cbr

Johanna García Andricain, S. A. (2016). GESTIÓN DE REDES IP/MPLS. *Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A*.

Johnson, G. (2017). Deploying MPLS Traffic Engineering. *Cisco Live*.

Khan, M. (2012). MPLS Traffic Engineering in ISP Network. *International Journal of Computer Applications (0975 – 8887)*, 23-32.

Li, T. (1999). MPLS and the Evolving Internet Architecture. *IEEE Communications Magazine*, 38-41.

Mijeong Yang, J. H. (2003). Design and Implementation of the IS-IS Routing Protocol. *IEEE*, 1-4.

Ming Xia, M. T. (2010). Greening the Optical Backbone Network: a Traffic Engineering Approach. *IEEE*.

Mohammad R. Abbasi, A. G. (2016). Traffic Engineering in Software Defined Networks: A Survey. *JOURNAL OF COMMUNICATIONS AND NETWORKS*, 3-14.

Ponce, J. P. (2021). Ecuador Estado Digital Ene/21. *Ecuador Estado Digital*, 2.

Radu CÂRPA, O. G. (2014). Segment Routing based Traffic Engineering for Energy Efficient Backbone Networks. *IEEE*.

RFC 1180. (1991). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc1180

RFC 1195. (1990). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc1195

RFC 1633. (1994). *IETF.* Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc1633

RFC 2474. (1998). *IETF.* Obtenido de Definition of the Differentiated Services Field (DS Field): https://tools.ietf.org/html/rfc2474

RFC 2475. (1998). *IETF.* Obtenido de An Architecture for Differentiated Services: https://tools.ietf.org/html/rfc2475

RFC 2679. (1999). *IETF.* Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc2679

RFC 3031. (2001). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc3031

RFC 3032. (2001). *IETF*. Obtenido de IETF: https://tools.ietf.org/html/rfc3032

RFC 3270. (2002). *IETF.* Obtenido de Multi-Protocol Label Switching (MPLS), Support of Differentiated Services: https://tools.ietf.org/html/rfc3270

RFC 3393. (2002). *IETF.* Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc3393

RFC 3784. (2004). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc3784

RFC 3812. (2004). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc3812

RFC 5824. (2010). *IETF*. Obtenido de IETF-related tools, standalone or hosted on tools.ietf.org.: https://tools.ietf.org/html/rfc5824

RFC Editor. (s.f.). *RFC EDITOR.* Obtenido de rfc-editor.org: https://www.rfc-editor.org/

Xipeng Xiao, A. H. (2000). Traffic Engineering with M PIS in the Internet. *IEEE*.

Yunkai Wei, X. Z. (2016). Energy-Aware Traffic Engineering in Hybrid SDN/IP Backbone Networks. *JOURNAL OF COMMUNICATIONS AND NETWORKS*, 559-566.

Glosario

3G: Tercera Generación.

AFI: Authority and Format Identifier

AS: Sistemas Autónomos

ATM: Asycronous Transfer Mode

BoS: Bottom of Stack

CE: Customer Edge

DSP: Domain Specific Part

DWDM: Dense Wavelength Division Multiplexing

EGP: External Gateway Protocol

FIFO: First In First Out

HODSP: High Order Domain Specific Part

ICMP: Internet Control Message Protocol

IDI: Initial Domain Identifier

IDP: Initial Domain Part

IETF: Internet Engineering Task Force

IGP: Interior Gateway Protocol

IP: Internet Protocol

IPX: Internet Packet Exchange

IS: Intermediate System

IS-IS: Intermediate System – Intermediate System

ISP: Internet Service Provider

L2VPN: Layer 2 Virtual Private Network

L3VPN: Layer 3 Virtual Private Network

LDP: Label Distribution Protocol

LSR: Label Switch Router

LTE: Long Term Evolution

MPLS: Multiprotocol Label Switching

OSI: Open Sytem Interconnection

P2P: Point-to-point

PE: Provider Edge

QoS: Quality of Service

RAN: Radio Access Network

RFC: Request for Comments

RSVP: Resource Reservaton Protocol

SDH: Synchronous Digital Hierarchy

SLA: Service Level Agreement

SNP: Sequence Number Packet

SP: Service Provider

SPF: Shortest Path First

TCP/IP: Transport Control Protocol / Internet Protocol

TCP: Transfer Control Protocol

TDP: Tag Distribution Protocol

TE: Traffic Engineering

UDP: User Datagram Protocol

UMTS: Universal Mobile Telecommunications System

VLSM: Variable Length Subnet Mask

WDM: Wavelength Division Multiplexing

Anexos

Archivos de simulación de red

https://drive.google.com/drive/folders/1vTVmaG3rbDvqXMdtgA8f43d7wtuQ-cZn?usp=sharing

eNSP
Características técnicas mínimas:

Windows 10 Pro
Intel(R) Core(TM)I5-8265U CPU @ 1.60GHz 1.80 GHz
RAM 16Gb
SSD: 256 Gb
Sistema Operativo basado en x64

EVE-NG
Características técnicas mínimas:

Windows 10 Pro
Intel(R) Core(TM)I5-8265U CPU @ 1.60GHz 1.80 GHz
RAM 16Gb
SSD: 256 Gb
Sistema Operativo basado en x64

Anexo 0-1: Direccionamiento IP de red Backhaul IP/MPLS TE

Fuente: Elaborado por el autor

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
I-LSR	Lo0	10.10.10.10	255.255.255.255	
	GE 1/0/0	10.128.0.1	255.255.255.252	
	GE 1/0/1	10.128.0.21	255.255.255.252	
	GE 1/0/2	192.168.100.1	255.255.255.252	
	GE 1/0/3	192.168.50.1	255.255.255.0	
PC	Eth0	192.168.50.2	255.255.255.0	192.168.50.1
LSR-1	Lo0	1.1.1.1	255.255.255.255	
	GE 1/0/0	10.128.0.2	255.255.255.252	
	GE 1/0/1	10.128.0.5	255.255.255.252	
	GE 1/0/2	10.128.0.41	255.255.255.252	
	GE 1/0/3	10.128.0.25	255.255.255.252	
LSR-2	Lo0	2.2.2.2	255.255.255.255	
	GE 1/0/0	10.128.0.9	255.255.255.252	

	GE 1/0/1	10.128.0.6	255.255.255.252	
	GE 1/0/2	10.128.0.45	255.255.255.252	
	GE 1/0/3	10.128.0.29	255.255.255.252	
LSR-3	Lo0	3.3.3.3	255.255.255.255	
	GE 1/0/0	10.128.0.26	255.255.255.252	
	GE 1/0/1	10.128.0.30	255.255.255.252	
	GE 1/0/2	10.128.0.33	255.255.255.252	
	GE 1/0/3	10.128.0.37	255.255.255.252	
LSR-4	Lo0	4.4.4.4	255.255.255.255	
	GE 1/0/0	10.128.0.22	255.255.255.252	
	GE 1/0/1	10.128.0.17	255.255.255.252	
	GE 1/0/2	10.128.0.42	255.255.255.252	
	GE 1/0/3	10.128.0.38	255.255.255.252	
LSR-5	Lo0	5.5.5.5	255.255.255.255	
	GE 1/0/0	10.128.0.13	255.255.255.252	
	GE 1/0/1	10.128.0.18	255.255.255.252	
	GE 1/0/2	10.128.0.46	255.255.255.252	
	GE 1/0/3	10.128.0.34	255.255.255.252	
E-LSR	Lo0	20.20.20.20	255.255.255.255	
	GE 1/0/0	10.128.0.10	255.255.255.252	
	GE 1/0/1	10.128.0.14	255.255.255.252	
	GE 1/0/2	192.168.200.1	255.255.255.252	
	GE 1/0/3	192.168.60.1	255.255.255.0	
	GE 1/0/4	192.168.61.1	255.255.255.0	
	GE 1/0/5	192.168.62.1	255.255.255.0	
	GE 1/0/6	192.168.63.1	255.255.255.0	
FILESERVER	Eth0	192.168.60.2	255.255.255.0	192.168.60.1
MULTICAST	Eth0	192.168.61.2	255.255.255.0	192.168.61.1
eNodeB_LTE+	Eth0	192.168.62.2	255.255.255.0	192.168.62.1
VOIP	Eth0	192.168.63.2	255.255.255.0	192.168.63.1

Anexo 0-2: Direccionamiento IP red IP/MPLS QoS

Fuente: Elaborador por el autor

Dispositivo	Interfaz	Vlan	Dirección IP	Máscara de subred
PE1	Lo0		1.1.1.1	255.255.255.255

	GigabitEthernet0/0/1	10	mpls l2vc	
	GigabitEthernet0/0/2	30	10.128.1.1	255.255.255.252
	GigabitEthernet0/0/3	20	mpls l2vc	
P	Lo0		2.2.2.2	255.255.255.255
	GigabitEthernet0/0/2	30	10.128.1.2	255.255.255.252
	GigabitEthernet0/0/3	60	10.128.1.5	255.255.255.252
PE2	Lo0		3.3.3.3	255.255.255.255
	GigabitEthernet0/0/1	40	mpls l2vc	
	GigabitEthernet0/0/2	50	mpls l2vc	
	GigabitEthernet0/0/3	60	10.128.1.6	255.255.255.252
CE1	GigabitEthernet0/0/1	10	192.168.80.1	255.255.255.0
CE2	GigabitEthernet0/0/1	40	192.168.80.2	255.255.255.0
CE3	GigabitEthernet0/0/1	20	192.168.90.1	255.255.255.0
CE4	GigabitEthernet0/0/1	50	192.168.90.2	255.255.255.0

DECLARACIÓN Y AUTORIZACIÓN

Yo, LEONIDAS ALBERTO MORAN CARREÑO, con C.C: # **1313633404** autor del trabajo de titulación: **DISEÑO Y SIMULACIÓN DE UNA RED BACKHAUL BASADA EN IP/MPLS DE ALTA DISPONIBILIDAD UTILIZANDO TÉCNICAS DE INGENIERÍA DE TRÁFICO Y CALIDAD DE SERVICIO,** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, a los 7 días del mes de junio de 2021

f. _____

Nombre: LEONIDAS ALBERTO MORAN CARREÑO

C.C: 1313633404

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	**DISEÑO Y SIMULACIÓN DE UNA RED BACKHAUL BASADA EN IP/MPLS DE ALTA DISPONIBILIDAD UTILIZANDO TÉCNICAS DE INGENIERÍA DE TRÁFICO Y CALIDAD DE SERVICIO**	
AUTOR(ES)	Leonidas Alberto Moran Carreño	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Ilen Rivero Pouymiro	
INSTITUCIÓN:	Universidad Católica Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	Guayaquil, 7 de junio de 2021	No. DE PÁGINAS: 96
ÁREAS TEMÁTICAS:	Redes de telecomunicaciones, IP Backhaul, Telefonía Móvil, Protocolos, MPLS, QoS	
PALABRAS CLAVES/ KEYWORDS:	MPLS, MPLS-TE, QoS, Ancho de Banda, Jitter, Congestión, Recursos	

RESUMEN/ABSTRACT: Debido a que los proveedores de servicios (SP, Services Providers) crecen día a día, esto representa consumo de recursos de red como ancho de banda, por lo cual, la demanda de tráfico crece exponencialmente debido a la gran cantidad de tráfico que atraviesa por la red. Para satisfacer la demanda de tráfico de red en los proveedores de servicios de Internet, es oportuno y necesario establecer mecanismos que manipulación de tráfico con el objetivo de minimizar la congestión, perdida de paquetes y el encolamiento de tráfico.Para minimizar el retardo, las redes de los SP deben implementar mecanismos que aporten con este objetivo, MPLS aporta de manera significativa el poder minimizar el retardo y, a su vez, brinda características importantes para el despliegue de tecnologías como L3VPN y MPLS TE. La disponibilidad y la tolerancia a fallos es crucial en un entorno de proveedores de servicios. Por tal razón, se deben desarrollar estrategias de ingeniería de tráfico contribuyan a minimizar y prevenir eventos como perdida de paquetes, latencia y cuellos de botella. La calidad de servicios en entornos donde la demanda de tráfico es constante y de gran tamaño, resulta de vital importancia establecer mecanismos de calidad de servicio que controlen el tráfico de red y minimicen la congestión, el retardo y fluctuación de retardo.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-994451790	**E-mail:** leal.12@live.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	