UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

TEMA:

ESTUDIO DE LA TECNOLOGIA MPLS MEDIANTE LA IMPLEMENTACION DEL NUCLEO DE UNA RED DE TRANSPORTE DE DATOS MPLS/VPN EN EL SOFTWARE SIMULADOR GNS3 - DYNAMIPS

Previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

Realizado por:

GABRIEL ARTURO ANANGONO DOMINGUEZ

Director de tesis:

ING. JUAN GONZALEZ BAZÁN

Guayaquil, Octubre de 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. GABRIEL ARTURO ANANGONO DOMINGUEZ como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES CON MENCION EN GESTION EMPRESARIAL.

Guayaquil, Octubre de 2013

DIRECTOR

_____

ING. JUAN GONZALEZ BAZÁN

REVISADO POR

_____

ING. CARLOS ROMERO ROSERO

_____

ING. ORLANDO PHILCO ASQUI

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

GABRIEL ARTURO ANANGONÓ DOMINGUEZ

DECLARAMOS QUE:

El proyecto de grado denominado "ESTUDIO DE LA TECNOLOGIA MPLS MEDIANTE LA IMPLEMENTACION DE EL NUCLEO DE UNA RED DE TRANSPORTE DE DATOS MPSL/VPN EN EL SOFTWARE SIMULADOR GNS3 - DYNAMIPS", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de los párrafos correspondientes, cuyas fuentes se incorporan en la bibliografía.
Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, Octubre de 2013

AUTOR

GABRIEL ARTURO ANANGONO DOMINGUEZ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

GABRIEL ARTURO ANANGONO DOMINGUEZ

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: ANÁLISIS DE LA RED DE DATOS DE LA FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS, PARA FUTURAS AMPLIACIONES, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Guayaquil, Octubre de 2013

AUTOR

GABRIEL ARTURO ANANGONO DOMINGUEZ

AGRADECIMIENTOS

A Dios porque sin el nada de lo que tengo hubiese sido posible, ni mi familia, ni mi carrera, ni mi vida.

A mi familia por su apoyo incondicional, por su comprensión y su aliento.

A mi director de tesis MsC. Juan Gonzales Bazán por su constante apoyo, confianza e innumerables contribuciones.

A los revisores metodológicos por su colaboración, observaciones y aportes al desarrollo del presente proyecto.

Al MsC. Manuel Romero Paz, Decano de la Facultad de Educación para el Desarrollo, y a los demás profesores por su aportes en las materias impartidas en la carrera de Ingeniería en Telecomunicaciones.

DEDICATORIA

A Dios por iluminar mi camino, y darme la fuerza y la constancia necesaria para llegar a mi meta.

A mi abuela por ser mi más grande ejemplo a seguir, por su amor, por su abnegación, su lucha, su trabajo incansable y su mente siempre progresista.

A mis padres por ser la brújula que ha guiado mi camino y seguirá guiándolo hacia el éxito.

A mis hermanos, tíos, primos y demás familiares, que fueron el apoyo, el descanso y la motivación perfecta en los momentos en que hizo falta, y en los que no.

RESUMEN

El presente trabajo de tesis tiene como propósito principal realizar el estudio de la tecnología MPLS (Multi-Protocol Label Switching), para luego incluir un software simulador denominado GNS3, en el cual se pueda realizar la emulación de los equipos de Núcleo de una red de Transporte de Datos MPLS-VPN, este software nos ayudara mostrándonos la interacción de los diferentes equipos, protocolos, la topología, los enlaces utilizados, y las configuraciones que después podrán ser aplicadas en componentes reales, es decir, con su hardware correspondiente, sin obtener ningún inconveniente al momento de conectarlos, instalarlos y programarlos tal cual se realizó en la simulación.

Esta capacidad hace a este software emulador de redes, una aplicación muy importante para la práctica, enseñanza y aprendizaje de este tipo de tecnologías, ya que permite implementar y observar, muy detalladamente el funcionamiento de las redes sin la necesidad de conectarlas físicamente.

Para la elaboración de este proyecto de tesis se usaron los métodos de investigación descriptiva, documental y cuasi experimental, basándonos en un estudio cualitativo de la tecnología en estudio y el mismo se dividió en cuatro fases principales:

- Recopilar y compilar información útil sobre el protocolo para asimilarla y redactarla.
- Diseñar las topologías que sirvan para explicar el funcionamiento de MPLS.
- Configurar equipos en la simulación.
- Documentar las configuraciones realizadas, los comandos de verificación y los resultados obtenidos.

En el marco teórico que corresponde a los Capítulos I y II del proyecto se estudia la parte conceptual de los procedimientos, y la dinámica de los protocolos involucrados en esta tecnología, ya que al ser este un tema muy extenso debemos tratar cada uno de los procedimientos y reglas que lo conforman a fin de obtener comprensión global y poder aplicarlo a la práctica.

En el Capítulo IV, se trata directamente el tema de la simulación, las topologías a utilizar, sus inconvenientes, la forma de como solventar los requerimientos y las alternativas de configuración que se nos puedan presentar como solución. Cada Topología a simular se centra en un procedimiento, o problema específico y se hace énfasis en describir cómo funciona el mismo, y como se aplica en la configuración.

Con esta implementación se alcanzó los siguientes resultados:

- Se logró evidenciar los procesos mediante los cuales MPLS nos permite realizar una mezcla entre el proceso de enrutamiento y reenvió de datos con la simulación de la topología 1.
- Se pudo verificar como pueden trabajar en conjunto la tecnología MPLS con el protocolo BGP para permitir la superposición de rutas en la nube MPLS con la simulación de la Topología 2.
- Se establecieron líneas de configuración básicas para que la Red MPLS funcione y presente conectividad entre los puntos que la forman.
- Se pudo identificar una manera de ahorrar recursos y puertos físicos a la hora de la implementación de MP-BGP en la nube del proveedor mediante el uso de Peer Groups, y Route Reflectors en la simulación de la Topología 3.

En base a estas importantes resoluciones se pudo también concluir que la implementación de la tecnología estudiada presenta diversas ventajas para los proveedores, principalmente, en cuanto al ahorro de capacidades de procesamiento, equipos físicos, disminución del retardo, fluctuaciones, y perdida de paquetes, además de la mayor velocidad de transmisión, y el aumento de fiabilidad en el transporte de datos entre dos puntos distantes geográficamente, pero pertenecientes a una misma Red Privada Virtual.

ABSTRACT

This thesis has as main purpose the study of MPLS (Multi -Protocol Label Switching) and to include a software simulator called GNS3, in which we are able to perform the emulation of the Core equipment of a Data Transport Network based on MPLS -VPN, this software will help us by showing the interaction of the different equipment, protocols, topology, links used, and configurations, which can then be applied in real components with appropriate hardware without getting any inconvenience when connecting, installing and programming them as it was done in the simulation.

This capability makes this software network emulator, a very important practicing, teaching and learning tool for this technology, allowing us to implement and make an in-detail observation of the operation of network without the need of connecting them physically.

In this thesis project, descriptive, experimental and quasi-documentary research methods are used, they are based on a qualitative study of the technology and the investigation itself was divided into four main phases:

- Collect and compile useful information about the protocol to assimilate and write it.
- Design topologies that will allow the author to explain the operation of MPLS.
- Set the simulation equipment.
- Document the configurations done, verification commands and results.

In the theoretical framework that corresponds to Chapters I and II of the project the conceptual part of the proceedings, and the dynamics of the protocols involved in this technology are studied, because as this is a very

extensive topic it is necessary to study each of the procedures and rules that conform it in order to gain global understanding to apply it to practice.

In Chapter IV, the issue of simulation is reviewed, the topologies to use, the ways to overcome the requirements and configuration problems and the options that we may have as a solution. Each topology to simulation focuses on a procedure or problem and the emphasis is on describing how it works, and how it is applied to the configuration.

This implementation has reached the following results:

- It was possible to demonstrate the processes through which MPLS allows us to make a mix between the routing and forwarding processes through the simulation of topology 1.

- It was verified how MPLS and BGP protocol can work together in the same core to allow overlapping routes in the MPLS cloud through the Simulation of Topology 2.

- Basic configuration lines were established for the correct performance of MPLS Network connectivity between the nodes that form it.

- It was able to identify a way to save resources and physical ports when implementing MP- BGP in the provider´s cloud using Peer Groups and Route Reflectors in the simulation of topology 3.

Based on these important resolutions it could also be concluded that the implementation of the studied technology has several advantages for providers, mainly in terms of saving processing capabilities, physical equipment, decreasing of delay, jitter, and packet loss, and to provide higher

throughput, and reliability in the transportation of data between two geographically distant points, that are part of the same Virtual Private Network.

CONTENIDO

INDICE DE FIGURAS

CAPITULO 2

CAPITULO 3

CAPITULO 4

INDICE DE TABLAS

CAPITULO I:
GENERALIDADES

1.1.- INTRODUCCIÓN.

El presente proyecto de tesis tiene como propósito principal realizar un estudio de la tecnología Multiprotocol Label Switching (MPLS), principal herramienta de trabajo en las redes de transporte de datos en la actualidad, e implementarla en un software simulador denominado GNS3, en el cual se pueden hacer simulaciones que van desde un simple diseño de una red LAN Privada, hasta de grandes redes, cargando en la PC del Sistema operativo Cisco (IOS) real en cada uno de los routers que conformen la topología deseada.

Estas características hacen a este software una herramienta fundamental para el estudio de este tipo de tecnologías de Networking, ya que podemos probar y corroborar conocimientos, sin la necesidad de dispositivos reales, que posean estas capacidades, los cuales en el mercado son muy caros, e inaccesibles para que los alumnos puedan manipularlos libremente.

El diseño de la red con la que trataremos es una forma básica de una red MPLS, que en la práctica real puede ser mucho más grande que el mismo, pero nos permitirá tener una idea concreta de cómo funciona la tecnología y sus procesos, a esta topología se añadirán dispositivos específicos para probar alguna de sus funcionalidades.

Este procedimiento servirá para la unificación de las partes teóricas y prácticas de la tecnología, es decir, para poder aplicar los conocimientos de manera rápida y fácil.

1.2.- ANTECEDENTES.

Desde sus inicios, la Ingeniería en Telecomunicaciones se ha visto influenciada por el desarrollo de la informática y la Digitalización de la Información, de esta retroalimentación entre las dos ramas nació lo que hoy conocemos como telemática.

En base a esto, se vio la necesidad de incluir en el pensum de la carrera la materia Telemática, la cual en la Facultad de Educación Técnica para el desarrollo, se tuvo el acierto de incluirla de manera que se estudia en 2 partes Telemática I y Telemática II, esto es necesario por lo extenso de los conocimientos relacionados con la misma.

Este mismo hecho de que los temas a tratar dentro de la Telemática son muy amplios y tienen muchos casos de aplicación, es lo que provoca que en algunos casos, los temas que requieren de conocimientos más avanzados, como el Multiprotocol Label Switching, se estudien solo de una manera superficial o más bien teórica, lo que no permite una comprensión global de los mismos ya que en casos como este, es necesario priorizar la práctica para la comprensión general de las técnicas a usar con el fin solucionar problemas que se pueden presentar en el medio, sin desmerecer, la importancia y necesidad de tener bien claros los conceptos generales que son básicos en la puesta en acción.

Muchas veces estos conocimientos que no alcanzan a ser tratados por completo en clases, se pueden obtener en libros especializados que usualmente son difíciles de comprender porque al ser este un tema complejo requiere de conocimientos avanzados y de mucha practica en el campo, sobre todo en el troubleshooting.

Por estos antecedentes es de vital importancia operar y obtener el mayor provecho a cualquier herramienta que permita desarrollar habilidades en temas más complejos como lo es el Multiprotocol Label Switching, ya que hoy en día existe una visión profunda y consecuente de la necesidad de profesionales con los conocimientos generales, en cuanto a la manera como se encuentran constituidas las grandes redes de comunicaciones que son el mayor campo de acción en las telecomunicaciones de nuestro tiempo.

1.3.- JUSTIFICACION.

Las redes de comunicaciones en el mundo actual se encuentran involucradas en prácticamente todas las actividades de nuestras vidas.
Las redes informáticas y en mayor cantidad su referente principal, la Internet, permiten a las personas mantenerse en contacto, colaborar e interactuar de maneras que eran impensables hace apenas medio siglo.
Esta red de redes tiene un sin número de aplicaciones, desde la Telefonía IP, pasando por la videoconferencia, la mensajería instantánea, el comercio electrónico, la educación, los juegos en línea, entre muchas otras.

En el ámbito empresarial, las tecnologías de la información, son de vital importancia, para el crecimiento de las compañías, para agilitar los procesos, beneficiando la competencia en el mercado, y la posibilidad mediante la internet de tener publicidad presente en el medio más amplio y democrático del mundo, en donde su anuncio puede ser visto desde cualquier otro país del planeta; sin contar, con las posibilidades que el servicio de transporte de datos que brindan los proveedores, permite el crecimiento de las mismas en cuanto a locales físicos y la convergencia de la información entre puntos geográficamente distantes.

Teniendo en cuenta estos puntos, tener el adecuado diseño de las redes LAN y WAN, sería un requisito fundamental para el crecimiento y buen desempeño de cualquier empresa, basándonos en esta idea el profesional

en el campo de las Comunicaciones debe ser capaz de reconocer las herramientas y equipos apropiados para el diseño de los diferentes tipos de redes, y formas de transporte de datos y conexión a la Internet, manteniendo la idea de la escalabilidad ya que la empresa puede crecer y expandirse en un futuro, por tales razones es necesario de hacer estudios sobre las tecnologías implementadas en estas redes.

MPLS es una de las tecnologías que se implementan para realizar el transporte de datos entre dos lugares geográficamente distantes con retardo mínimo, permitiéndonos mantener la calidad en el servicio, y con la funcionalidad de que es compatible entre varias tecnologías disponibles en el orden de las comunicaciones como lo son la tecnología ATM y la IP, por esto el estudio y análisis de esta tecnología se vuelve imprescindible.

El objetivo de esta tesis se enfoca en realizar un análisis del contenido teórico, los procesos y la configuración de los routers utilizados en una red de transporte de datos sobre MPLS, determinar las falencias en cuanto a la asimilación y entendimiento completo del contenido teórico de la misma y de esta manera proceder con la implementación de una herramienta considerada indispensable la comunicación en el presente y el futuro cercano.

Esta tesis pretende ser una guía acerca de la tecnología MPLS, si bien es cierto existen otros textos escritos sobre este tema, la mayoría están en idioma inglés, y las explicaciones se realizan en términos que suponen un conocimiento muy avanzado del lector, por esto esta tesis busca generar un impacto social creando una guía de introducción a MPLS, de manera más amigable, explicativa y accesible para cualquier consultante habido de conocer más en el mundo de las redes y el networking, ayudando con esto a poner el conocimiento un paso más cerca del estudiante.

En conclusión y de acuerdo a este análisis se considera necesario que los profesionales tengan un software simulador en los que se puedan poner en práctica diferentes tipos de topologías de redes de área extensa WAN o Redes de Área Local, LAN, y en el cual se puedan identificar los diferentes tipos de dispositivos, protocolos de enrutamiento, los problemas más comunes que se pueden presentar en la vida laboral, y demás características que se ven involucradas en el mundo de las tecnologías de la información, las redes convergentes y el internet, para la asimilación de este tema tan amplio y necesario para el Ingeniero en telecomunicaciones en la actualidad.

TITULO: "ESTUDIO DE LA TECNOLOGIA MPLSMEDIANTE LA SIMULACION DEL NUCLEO DE UNA RED DE TRANSPORTE DE DATOS MPLS-VPN EN EL SOFTWARE GNS3-DYNAMIPS"

1.4.- PLANTEAMIENTO DEL PROBLEMA.

La necesidad de realizar a la fecha un análisis de la tecnología MPLS de una manera global, tanto teórica como práctica, para que sea documento de consultas posteriores, para referencia de estudio, y asimilación del contenido, con el fin de reforzar los conocimientos obtenidos en el aula, profundizarlos, y tener una visión más real de las ventajas del uso de esta tecnología.

La importancia de resolución de este inconveniente la se basa principalmente en la poca documentación que existe en español sobre la tecnología a usar, por lo cual es pertinente realizar un estudio que busque explicar con ejemplos prácticos y conceptos claros y comprensibles, las capacidades de esta herramienta, que hoy en día está presente en la mayoría de las redes de comunicaciones de gran escala.

1.5.- HIPOTESIS.

El uso de una aplicación que permita emular e implementar la forma de configuración de los equipos del núcleo de una red de transporte de datos sobre MPLS, facilitará la comprensión completa del contenido teórico, con lo cual se brinda una guía de consulta para la configuración de este tipo de redes, con explicaciones sobre los comandos utilizados, de manera que se tenga una asimilación lógica de las líneas de configuración y no solo se desarrolle mecánicamente.

1.6.- OBJETIVOS.

Los objetivos para este proyecto de tesis son los siguientes:

1.6.1.- OBJETIVO GENERAL.

Estudiar y aplicar el software simulador de redes GNS3 como herramienta de carácter práctico para el estudio de la tecnología Multiprotocol Label Switching, para redes de transporte de datos.

1.6.2.- OBJETIVOS ESPECIFICOS.

Los objetivos específicos son los siguientes:

- Explicar de una manera concisa y práctica la tecnología MPLS y su funcionamiento.
- Revisar los conceptos teóricos de los procesos globales (enrutamiento, reenvió) utilizados en una red sobre la que corre MPLS.

- Esclarecer las ventajas que se obtienen con la implementación de esta tecnología.
- Diseñar topologías que sirvan para explicar el funcionamiento de los procesos básicos MPLS.
- Promover el uso de la herramienta/software GNS3.
- Utilizar las herramientas más comunes para la manipulación de dispositivos.
- Simular las topologías creadas para corroborar el funcionamiento de la tecnología en casos reales.
- Proveer un conocimiento solido de los comandos básicos a utilizar para configurar las topologías diseñadas, y los comandos de consulta/comprobación necesarios para realizar una correcta resolución de problemas.

1.6.3.-METODOLOGIA.

Este es un proyecto que usa la investigación descriptiva, ya que busca especificar las propiedades, las características y perfiles de la tecnología que se somete a análisis.
Su enfoque es cualitativo, ya que se emplean procesos cuidadosos, sistemáticos y empíricos, además de no usar un análisis numérico, sino más bien de las propiedades de la tecnología.

Es también una investigación Documental en base a la fuente de la información recolectada, y Cuasi Experimental, por la puesta en práctica de esta información en simulaciones de red, diseñadas por el autor, para probar las propiedades y procesos principales de la tecnología.

El alcance de esta tecnología se centra en los procesos básicos de la tecnología MPLS, sus capacidades de enrutamiento y reenvío de datos y los protocolos que pueden ser usados en conjunto con el mismo para proveer un mejor desempeño de la red (BGP, OSPF, LDP).

Otros procedimientos y prácticas, específicamente la Calidad de Servicio y la Ingeniería de Trafico que también son aplicables en conjunto con MPLS, no son estudiados en el presente proyecto, puesto que estos al ser temas muy extensos, deben ser tratados independientemente, y de ellos se podría realizar dos proyectos de tesis además de este.

Para alcanzar los objetivos propuestos hemos puesto en práctica nuestra metodología dividiéndola en Fases Según se detalla a continuación:

1. Recopilar la información de las diferentes fuentes documentales, leerlas, y compilarlas para buscar la mejor forma de explicar la tecnología.
2. Diseñar las topologías necesarias, para explicar los procedimientos de la tecnología explicada.
3. Realizar las configuraciones de equipos en la simulación y realizar pruebas de conectividad.
4. En base a esto reseñar y documentar las configuraciones básicas para cada tipo de topología, de manera que si se copian exactamente en equipos reales, tendrán la misma funcionalidad y efectividad que en la simulación.

CAPITULO II:
MPLS – CONMUTACION DE ETIQUETAS MULTIPROTOCOLO / MULTIPROTOCOL LABEL SWITCHING.

2.1.- ANTECEDENTES HISTORICOS.

Para entender mejor las ventajas que ofrece la tecnología MPLS, debemos revisar cual fue el motivo por el cual dicha tecnología fue desarrollada.
Para esto debemos remontarnos a los 90's, por esa década los Proveedores de servicios manejaban dos estándares para la comunicación y el transporte de datos, el enrutamiento IP, y la Conmutación ATM.

La arquitectura de red más usada por los grandes proveedores de entonces eran routers IP simplemente conectados entre sí, esto provocaba saturación en las redes, y congestión en las transmisiones. Entonces, la solución más obvia, fue aumentar las capacidades de los equipos, fue así como surgieron los primeros conmutadores ATM con ciertas capacidades de control IP.

Se generaron entonces una gran cantidad de problemas que tenían que ver con el rendimiento óptimo de la red, con lo cual se implementaron soluciones de integración entre las que surgió la Conmutación IP, sin embargo, estas soluciones seguían causando congestionamiento y no eran operativas entre las distintas tecnologías de capa 2 y capa 3 que se utilizaban en aquel entonces.

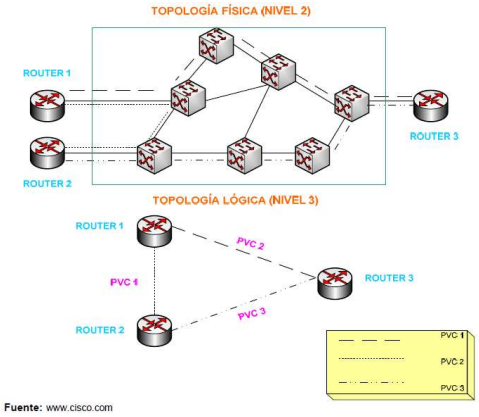

Fig. 2.1.- Topología física y lógica mezclando Routers IP y Switches ATM
Fuente: www.cisco.com

El óptimo desempeño de una red siempre ha sido de vital importancia para los administradores, es por ello que entonces surgieron un sin número de alternativas de protocolos de enrutamiento, teniendo siempre como principal meta diseñar el camino más corto que un paquete debe seguir por la red, sin embargo, no se habían tenido en cuenta los parámetros que afectan el desempeño de la red, como los retardos, la Calidad de Servicio (QoS), congestión de tráfico, entre otros.

Entre las tecnologías que fueron desarrolladas para ser una solución se encontraban las siguientes:

- Cell Switching Router de Toshiba.
- IP Switching de Ipsilon Networks.
- Tag Switching de Cisco Systems.
- Aggregate Route Base IP Switching de IBM.

Ninguna de estas fue la solución definitiva, es más, en algunos casos creaban más problemas de incompatibilidad entre ellas, es por eso que la International Engineering Task Force (IETF) en 1997, creo el grupo de trabajo MPLS para desarrollar un abordaje estandarizado común.

Para cuando el grupo de trabajo develo el estándar creado, ya en el mercado existían routers con capacidades de procesamiento muy elevadas, pero el grupo había creado un estándar tan completo, que a pesar de esto, las ventajas que MPLS proveía garantizaron rápidamente su popularidad, entre estas ventajas tenemos las siguientes capacidades:

- QoS – Calidad de Servicio.
- VPN – Redes Privadas Virtuales / Virtual Private Networks.
- TE – Ingeniería de Trafico / Traffic Engineering.
- Compatibilidad Multiprotocolo.

2.1.1.- QoS – Calidad de Servicio.

Los administradores de red están requiriendo en mayor grado de un soporte sofisticado de QoS.

Los principales requerimientos son los siguientes:

- Garantizar una cantidad definida de capacidad de transmisión para aplicaciones específicas como audio/video.
- Control de latencia y fluctuación (jitter), y garantizar la capacidad para transmitir voz.
- Proveer acuerdos de niveles de servicio, específicos, garantizados y cuantificables, o contratos de tráfico.

Una red conmutada por paquetes, no puede ofrecer compromisos firmes en cuanto a la Calidad de servicio, por el mismo hecho de que se necesita desencapsulacion de los datos para poder leer el origen y el destino en cada salto y en base a esto conocer la ruta a tomar, esta manipulación podría

contribuir a la perdida de algunos bits o datos en el proceso, inconveniente que no se tiene en una red de capa 2 en las que solo se realiza un forwarding de los datos, sin hacer mayor desencapsulamiento, MPLS, utiliza las ventajas de ambas tecnologías mezcladas para obtener mayor provecho en la transmisión.

2.1.2.- INGENIERIA DE TRÁFICO.

MPLS nos permite comprometer recursos de red fácilmente, de manera que resulte posible balancear la carga ante una demanda dada, y comprometer niveles diferenciados de soporte para satisfacer los diferentes requerimientos de tráfico del usuario, además de la habilidad de definir rutas dinámicamente, planificar los compromisos de recurso sobre la base de la demanda conocida y optimizar la utilización de red se denomina Ingeniería de tráfico. (Alvez, Rogelio. 2009)

2.1.3.- SOPORTE DE REDES VIRUTALES PRIVADAS (VPN).

MPLS ofrece soporte de VPNs. Con una VPN, el tráfico de una organización dada atraviesa transparentemente a través de una red de forma que ese tráfico queda segregado de los demás datos que pasen sobre esta red. Así, se logra obtener mayor fiabilidad en el desempeño y la seguridad.

2.1.4.- SOPORTE MULTIPROTOCOLO.

En una Red que trabaje con MPLS, los routers que soportan MPLS, pueden coexistir con routers IP ordinarios, facilitando iniciar la evolución hacia esquemas MPLS. También la tecnología está diseñada para trabajar en redes ATM y Frame Relay, es más MPLS puede implementarse en una red

IP pura, o una ATM pura, o con todas las tecnologías mencionadas coexistiendo en la misma red.

2.2.- ¿QUE ES MPLS?

El Multiprotocol Label Switching es un estándar que se encuentra situado entre la capa 2 y la capa 3 del protocolo OSI, es un protocolo de unión entre la Capa de Enlace y de Red, fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y en paquetes, y puede transportar diferentes tipos de tráfico entre ellos, tráfico de VoIP, tráfico de datos, streaming, entre otros.

Como lo define Martha Tapasco (2008):

> Como concepto MPLS, es un tanto difícil de explicar, pero como protocolo es sencillo y las implicaciones que supone su implementación son enormemente complejas, y según el énfasis en que se ponga a la hora de explicar, se puede decir que MPLS, es un sustituto perfecto de la tecnología IP sobre ATM, un protocolo para hacer túneles, o una técnica para el encaminamiento de paquetes, su ventaja es que mezcla las capacidades de enrutamiento y control de la capa 3, con la velocidad y simplicidad de la Conmutación capa 2.

Se basa en dos componentes básicos comunes:

- La separación entre las funciones de routing y de forwarding lo que significa una evolución en la manera de construir y gestionar la red.

- La función de intercambio de etiquetas para el envío de datos.

MPLS ofrece nuevas opciones en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido.

2.3.- ¿COMO FUNCIONA MPLS?

La arquitectura de una red que trabaja con MPLS, está constituida, por un conjunto de nodos, denominados, Label Switched Routers (LSR), estos son los routers dentro del dominio MPLS, ellos poseen capacidades de conmutación y de ruteo asociadas a una etiqueta que se adjunta en el paquete al ingresar al dominio. Las etiquetas definen un flujo de paquetes a través de un camino designado entre dos puntos.
Para cada tipo de flujo particular, denominado un Forwarding Equivalence Class (FEC), se define un camino específico a través de la red.

Un FEC es la agrupación de etiquetas de modo que se permita la asociación de un conjunto de paquetes sobre el mismo camino y con el mismo destino. Todos estos paquetes reciben el mismo tratamiento, entre más FECs tengamos mayor especificidad para diferenciar entre distintos tipos de flujos. Los LSR de entrada son los encargados de asociar a cada paquete un FEC, y se basan en principio por la dirección de destino IP, aunque existen otros factores.

Agustín Gonzales (2006) nos define a los FEC en dos puntos muy concisos:

- Es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte.
- La asignación de un paquete particular a un FEC es hecho solo una vez (Cuando el paquete entra a la red).

Es decir, MPLS es tecnología orientada a conexión ya que asociadas con cada FEC hay características de tráfico específicas.

Estos LSR no necesitan hacer un desencapsulamiento de los datos, para revisar el direccionamiento IP, solo les basta con ver la etiqueta que se le adjunto al entrar en la nube MPLS, revisar a que FEC está asociada dicha etiqueta, y hacer un forwarding de la información a través de la ruta determinada para dicho FEC, este camino es denominado Label Switching Paths (LSP).

La asignación de las etiquetas es elaborada en el LSR de borde por el Protocolo LDP, Label Distribution Protocol, que es un conjunto de reglas que sirven para que un LSR le informe a otro el significado de las etiquetas usadas para el forwarding del tráfico entre ellos.

La figura describe la forma como trabaja MPLS:

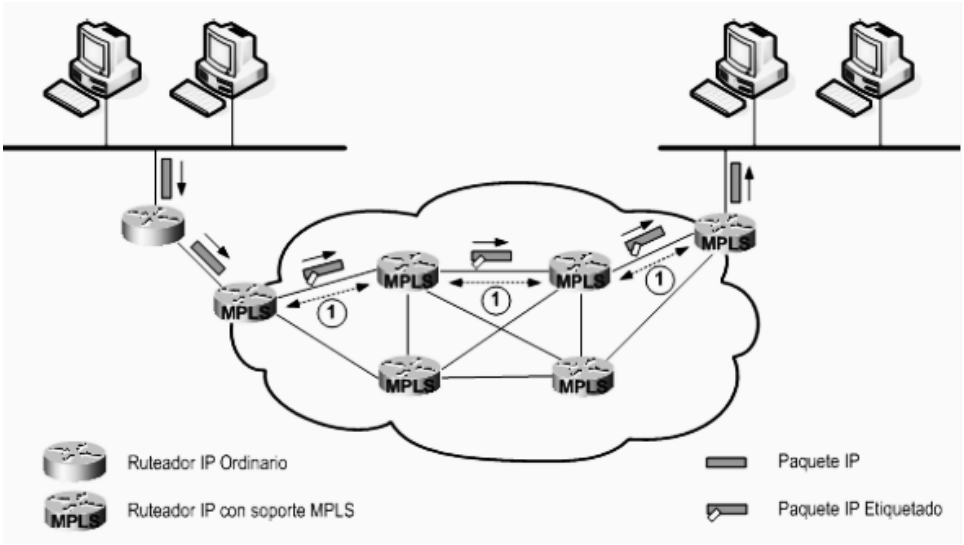

Fig.2.2.- Operación de MPLS

Fuente: www.cisco.com

Debemos tener en cuenta que en la nube MPLS, los routers interconectados deben pertenecer a una red convergente, es decir que todos los routers

deben alcanzarse entre sí, para ello habilitamos en todos un IGP, Interior Gateway Protocol, como por ejemplo: OSPF.

Debe asignarse etiquetas a los paquetes de un FEC particular, se usa también un protocolo (LDP), para determinar la ruta y establecer las etiquetas entre los LSRs adyacentes.

Entonces:
1.- El paquete ingresa al dominio MPLS mediante un LSR de borde, este analiza el paquete (su dirección de destino), lo asocia con un FEC, el cual está asociado a un camino LSP en particular, entonces se le adiciona, la etiqueta que hace referencia a este LSP, y se reenvía hacia el siguiente salto MPLS.
En caso de que no exista un LSP creado aun para este FEC, entonces los LSR deberán colaborar entre sí para definir un nuevo camino y asociarlo al FEC.

2.- Dentro del dominio MPLS, cada vez que un router recibe un paquete etiquetado, remueve la etiqueta entrante y adjunta la etiqueta saliente apropiada y reenvía el paquete hacia el destino.

3.- En el LSR de borde para egreso, el Router remueve la etiqueta lee el encabezamiento IP, y reenvía el paquete hacia su destino mediante el enrutamiento IP convencional.

2.4.- CONMUTACION DE ETIQUETAS

MPLS es una tecnología que varía la forma como se estaba llevando a cabo el reenvió tradicional de paquetes.

El reenvío usado por MPLS, se puede apreciar por una diferencia drástica con el reenvío original de paquetes, ya que en el reenvío original de paquetes en cada salto, es decir en cada router, el paquete es desencapsulado para leer el encabezamiento IP, y se hacia el análisis en la tabla de enrutamiento, para saber por qué interfaz o ruta debía enviarse, lo que consumía tiempo, procesamiento, podría producir saturación, pérdidas o paquetes corruptos.

En una red MPLS, solo se realiza este procedimiento una vez, cuando ingresa el paquete al dominio MPLS, se lee el encabezamiento IP, según la dirección de destino, se asocia con un FEC (Forwarding Equivalence Class), y luego se asigna a un LSP, y cada router que reciba el paquete solo lo reenviara dependiendo de su etiqueta. Todos los paquetes asociados a un mismo FEC, serán reenviados de la misma manera, por lo tanto atraviesan la red usando la misma ruta.

Entonces la base de MPLS se concentra en la asignación e intercambio de etiquetas. Los LSP son simplex por naturaleza, es decir para el tráfico dúplex se necesitaran dos LSP, uno por cada sentido de la transmisión. Es entonces que entendemos que MPLS separa los procesos de reenvío y enrutamiento, como tradicionalmente se concebían. (Alvez, Rogelio.2009)

No obstante, MPLS no usa ninguno de los Protocolos de señalización conocidos, el protocolo que usa para determinar el camino de reenvío de paquete es el LDP.

Una red habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución IP/ATM clásica. Un camino LSP es el circuito virtual por el que transitaran todos los paquetes asignados a la misma FEC.

Un LSR es entonces un router que se encarga de intercambiar etiquetas según una tabla de envió. La imposición de la etiqueta cuando el paquete entra a un dominio MPLS, la ejecuta un Router Edge LSR. Un LSP trabaja en un esquema orientado a conexión, es decir que el camino a recorrer por los paquetes debe estar formado antes que cualquier flujo de tráfico empiece circular por este.

Cada LSR mantiene, entonces, dos tablas que contienen la información que se refieren al componente de reenvío MPLS.
La primera se llama LIB (Label Information Base), donde se guardan todas las etiquetas asignadas por este LSR, y las correspondencias de esas etiquetas a otras recibidas desde otro LSR.

La segunda Tabla se llama LFIB (Label Forwarding Information Base) y en la cual son mantenidas únicamente las etiquetas que están usándose por el paquete de reenvío.

Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control.
Cada entrada de la tabla LFIB contiene un par de etiquetas de entrada y salida correspondiente a cada interfaz de entrada, estas se utilizan para acompañar a cada paquete que llega por esa interfaz con la misma etiqueta, y señalizar su interfaz de salida.

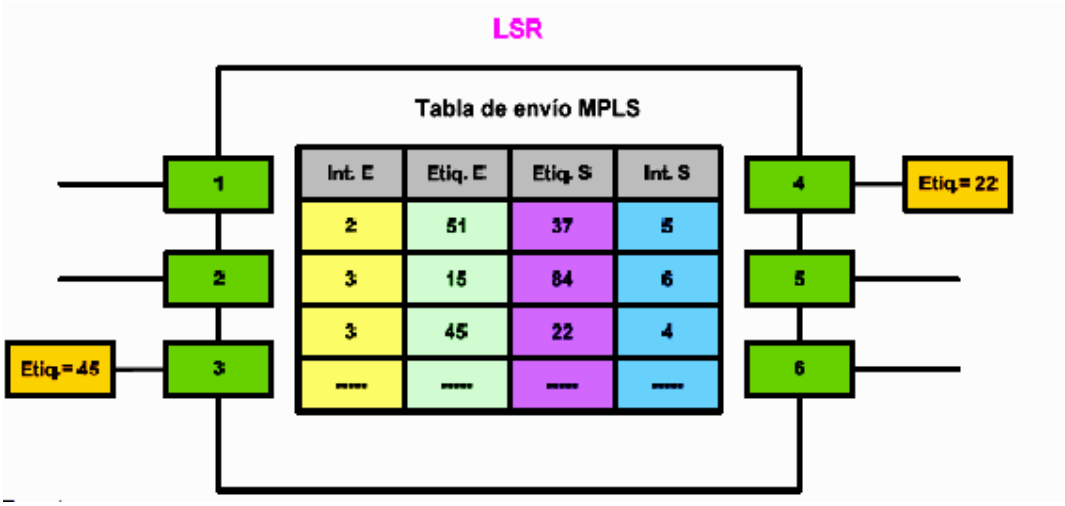

Fig.2.3.- LSR, Tabla de etiquetas - Label Switched Router.

Fuente: www.cisco.com

Ejemplo: Si un paquete llega por el puerto 3 con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por la interfaz 4 de salida.

2.5.- FORMATO Y UBICACIÓN DE LA ETIQUETA.

Es entonces que podemos constatar, que la identidad del paquete IP pasa enmascarada durante su paso por la red Backbone, en donde los nodos, solo mira las etiquetas que necesita para hacer el forwarding de los datos a través de todos los LSR. Estas etiquetas se insertan en las cabeceras MPLS, que está entre los niveles de capa 2 y 3. Es esto lo que permite que MPLS funcione sobre cualquier transporte, LAN, ATM, PPP, Frame Relay, entre otros.

En ciertos casos, si el protocolo de transporte contiene ya un campo para etiquetas, como en ATM y Frame Relay, se utilizan estos campos para las etiquetas, aunque en los casos donde la tecnología de Capa 2 no soporta campos nativos para las etiquetas, entonces se emplea una cabecera MPLS

de 4 bytes (32 bits), que tiene un campo específico para la etiqueta y se inserta entre la cabecera de capa 2 y capa 3.

El encargado de asignar la etiqueta al paquete IP es el LSR de borde o Edge LSR, en este caso este router como se mencionó en anteriores paginas revisa la información de la red de destino, la busca en las tablas de enrutamiento, lo asigna a un FEC, y con este le pone la etiqueta equivalente.

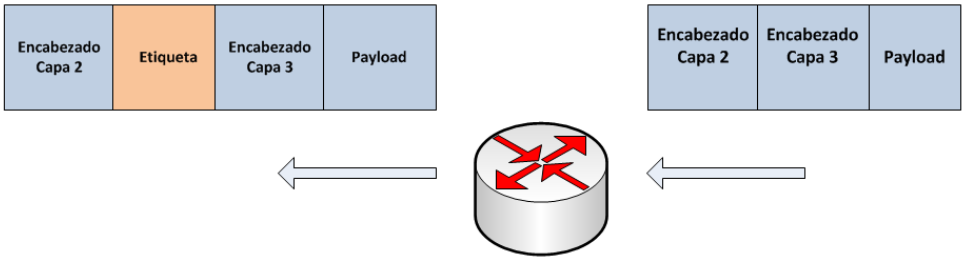

Fig.2.4.- Imposición de Label en Edge LSR.

Fuente: Elaborado por el Autor.

Los 32 bits de la cabecera MPLS se reparten en:

- 20 bits para la etiqueta MPLS.
- 3 bits para identificar la clase de Servicio en el campo EXP (QoS).
- 1 bits de stack para poder apilar etiquetas de forma jerárquica (esto se aplica en túneles MPLS, Ingeniería de tráfico).
- 8 bits para indicar el TTL (time-to-live).

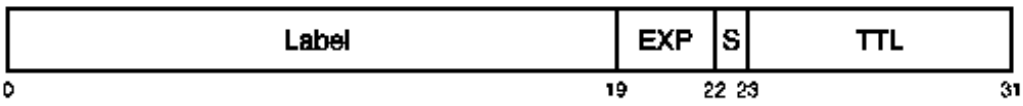

Fig. 2.5.- Etiqueta MPLS.

Fuente: Implementing MPLS on Cisco IOS – Cisco Press (2004)

Autor: Lancy Lobo

Dónde:

- Label: (20 bits) Es la etiqueta MPLS de la que hemos estado estudiando, que se asigna para determinar el FEC.

- EXP: (3 bits) Se usa para identificar la Clase de Servicio, CoS, Class of Service, como lo definen Anderson y Asati (2009) en la RFC 3032: Label Stack Entry EXP renamed as Traffic Class, este campo ha sido también renombrado como Campo de Clase de Trafico.

- S (1 bit): Este campo solo tiene 1 bit, y se usa solo para indicar si hay un apilamiento de etiquetas, lo cual se identificara con un valor de 1 y si la etiqueta es única se asignara un valor de 0.

- TTL (8 bits): Time to Live indica el número de nodos o de saltos que se ha recorrido, hasta llegar al destino, este valor es adoptado de la cabecera IP a la entrada del LSP y a la salida de este.

Las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un ISP en el momento de expandir su red (Lancy Lobo, 2005).

2.6.- APILAMIENTO DE ETIQUETAS

Un paquete etiquetado puede transportar varias etiquetas, organizadas a manera de pila con orden LIFO (Last In First Out), En cualquier LSR, puede adicionarse una etiqueta a la pila (push) o remover una etiqueta de la pila (pop).

Esto permite la agregación de LSPs en una porción de una ruta que atraviesa una red, creando un túnel.

En el comienzo del túnel, un LSR asigna la misma etiqueta a los paquetes pertenecientes a una cantidad de LSPs incorporando la etiqueta en la pila de cada paquete, y al final, otro LSR extrae el elemento ubicado al inicio de la pila dejando expuesta la etiqueta siguiente.

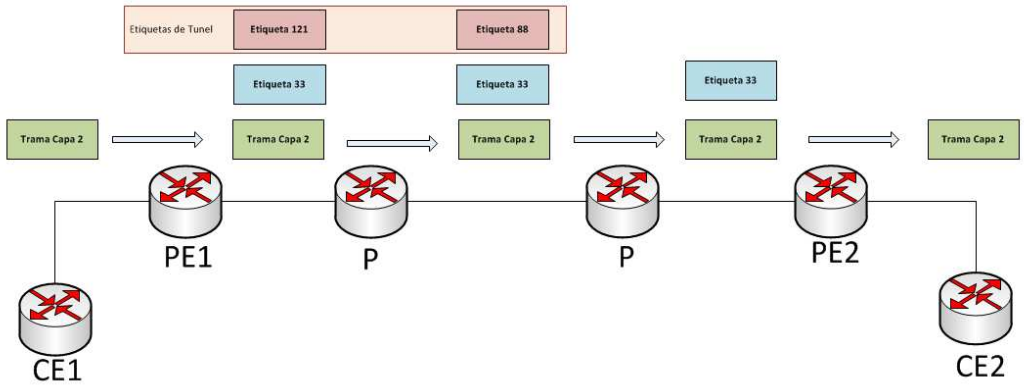

Fig. 2.6.- Ejemplo del Label Stack a través de la red.

Fuente: Elaborado por el Autor..

El objetivo de esta técnica es precisamente ese, crear túneles dentro de los otros LSPs, como se observa en la figura anterior.

Este procedimiento proporciona considerable flexibilidad. Una organización puede implementar redes MPLS en diferentes sitios y establecer numerosos LSPs en cada uno.

Luego puede emplear apilamiento de etiquetas para agregar múltiples flujos de tráfico propios antes de traspasarlos a un proveedor de acceso.

2.7.- COMPONENTES DE CONTROL Y ENVIO.

Componente de Control.

Está destinado a crear y mantener la información de las etiquetas entre un grupo de LSR interconectados, por esto dentro del Backbone MPLS se usa un IGP, como OSPF, IS-IS y BGP-4, para la construcción de rutas y su mantenimiento.
Este plano de control es el encargado de configurar los LSP entre las rutas IP y mantenerlo actualizado cuando exista algún cambio en la topología. (Lancy Lobo, 2005).

Componente de envió.

Este es el encargado del transporte de paquetes entre 2 LSRs. En este componente funcionan los dos tipos de bases de datos de etiquetas, la Label Forwarding Table, que se utiliza para el transporte de paquetes que contienen etiquetas y la Forwarding Information Table que permite transportar paquetes de datos hacia los equipos que no trabajan con etiquetas.
(Lancy Lobo, 2005).

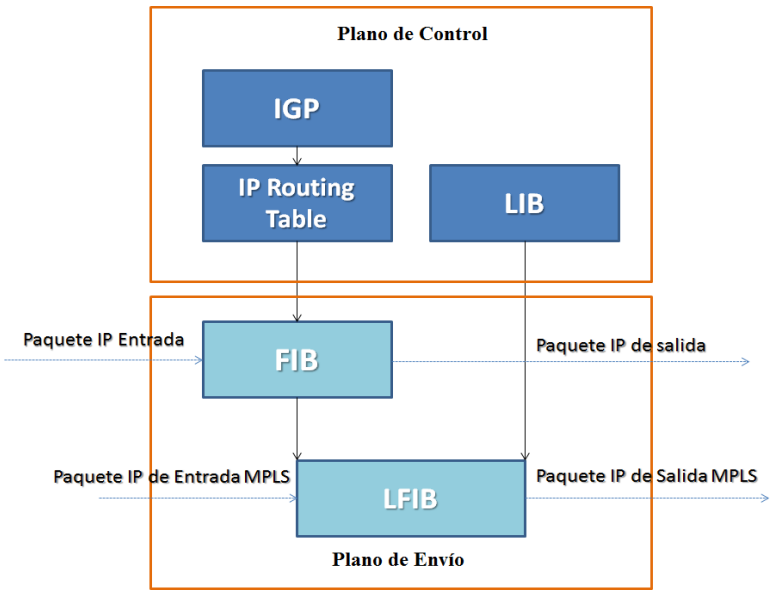

Fig.2.7.- Plano de Control y envío.

Fuente: Elaborado por el Autor.

2.8.- REENVIO EXPRES DE CISCO / CISCO EXPRESS FORWARDING (CEF).

Cisco Express Forwarding es el fundamento en el cual MPLS y sus servicios operan en un Router Cisco. CEF es un mecanismo usado en Cisco que intensifica la simplicidad y el desempeño del reenvío IPv4 en el router.

Cuando CEF es usado en un router, este mantiene como mínimo un FIB, que contiene un mapa de las redes de destino en la tabla de enrutamiento hacia sus apropiadas adyacencias de próximo salto.

El FIB reside en el plano de envío, que es la maquinaria de reenvió de los paquetes procesados por el router.

En adición al FIB, otras dos estructuras en el router son mantenidas, que son el Label Information Base (LIB), y Label Forwarding Information Base (LFIB).

El protocolo de distribución en uso entre los vecinos MPLS adyacentes es responsable de la creación de tablas LIB y LFIB.

LIB funciona en el plano de control y es usado por el LDP (Label Distribution Protocol) donde los prefijos IP de destino en la tabla de enrutamiento son mapeados hacia las etiquetas de próximo salto que son recibidas desde los vecinos downstream, así como las etiquetas locales generadas en el LDP.

La LFIB reside en plano de envío y contiene una etiqueta local hacia el mapeo de etiquetas de próximo salto junto con la interfaz de salida la misma que es usada para reenviar los paquetes etiquetados.

La información acerca de la convergencia de las redes de destino obtenida de los protocolos de enrutamiento es usada para poblar la RIB (Routing Information Base) o la tabla de enrutamiento.

La tabla de enrutamiento provee información para la FIB. El LIB es poblado usando información del LDP, y desde LIB con información de FIB que es usado para poblar el LFIB. (Lacy Lobo, 2005).

2.9.- PROTOCOLO DE DISTRIBUCION DE ETIQUETAS / LABEL DISTRIBUTION PROTOCOL (LDP).

Es el protocolo más ampliamente conocido y usado para la distribución de etiquetas y la comunicación de ellas a través de los LSRs, aunque existen otros.
LDP está contenido en la RFC 3036, funciona sobre TCP, y usa la información de enrutamiento IP existentes creadas por el Protocolo de enrutamiento para propagarse.

El LDP tiene dos funciones:

- Asocia un FEC a cada camino LSP que se crea
- Distribuye la información de la asociación FECs- Etiquetas entre dos LSR vecinos.

Pepelnjak I. & Guichard J. (2001), definen en este caso dos métodos para esta distribución:

1. ***Trafico de bajada bajo demanda (Downstream on Demand).***

   Habilita la opción de que un enrutador upstream pida directamente una etiqueta para un FEC al LSR downstream, el cual obviamente es el Next-Hop.

2. ***Trafico de Bajada no Solicitado (Unsolicited Downstream).***

   Permite que un LSR downstream asigne una etiqueta sin necesidad de recibir peticiones con anterioridad.

Para el control de Distribución de etiquetas tenemos dos modos diferentes.

- Independiente.- Cuando un LSR reconoce una FEC y decide unir una etiqueta a esta FEC, es decir cada router toma la decisión de cómo tratar cada paquete.
- Ordenado.- Cuando un Edge LSR asocia una etiqueta al FEC.

2.9.1.- CLASIFICACION DE ETIQUETAS

Se clasifican de 2 maneras:

- Por Plataforma.- las etiquetas son proporcionadas por una fuente, los valores de las etiqueta son iguales dentro de un LSR, por cada interfaz hay una etiqueta.

- Por Interfaz.- Las etiquetas son suministradas por diferentes fuentes, es decir que los valores son diferentes dentro de un LSR, pueden existir una o más interfaces con el mismo valor.

2.9.2.- ESTABLECIMIENTO DE SESION LDP.

En el siguiente ejemplo propuesto por la autora: Lancy Lobo, en su libro *"MPLS Configuration on Cisco IOS", e su versión original en inglés*, se detalla como se establece una sesión LDP.

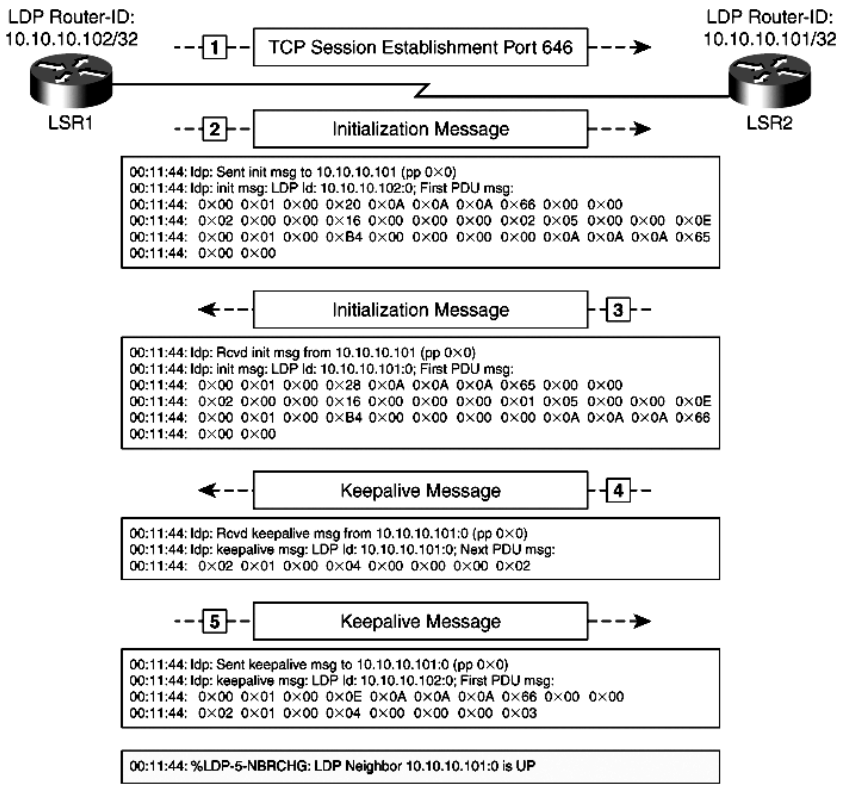

Fig.2.8.- Establecimiento de Sesion LDP.

Fuente: Implementing MPLS on Cisco IOS – Cisco Press (2004)

Autor: Lancy Lobo

.

1.- Las sesiones LDP comienzan cuando un LSR envía periódicamente mensajes de Hello, usando el multicast UDP en 224.0.0.2, en interfaces que tengan habilitado el MPLS Forwarding.

Cuando encuentre al vecino, el que tenga mayor valor en el router ID es el LSR activo. El LSR activo intenta establecer una sesión con el LSR pasivo.

2.- El LSR activo envía un mensaje de inicialización a el LSR pasivo, que contiene información como el tiempo keepalive para la sesión, el método de distribución de etiquetas, la longitud máxima de PDU, y el ID del LDP receptor, y también si es que la detección de loops está habilitada.

3.- El LSR LDP pasivo responde con un mensaje de inicialización si los parámetros son aceptables, si no es así, el LDP LSR envía un mensaje de notificación de error.

4.- El LSR Pasivo envía un mensaje Keepalive para activar LDP después de enviar el mensaje de inicialización.

5.- El LSR activo envía un mensaje keepalive al LDP LSR pasivo, y la sesión LDP se establece. Es aquí que el mapeo De Etiquetas-FEC puede ser intercambiado entre los LSRs.

2.9.3.- PENULTIMO SALTO / PENULTIMATE-HOP-POPPING

Es el proceso que se lleva a cabo en el penúltimo router del dominio MPLS, el mismo que es un LSR, en donde este tiene la misión de enviar el paquete con la última etiqueta y luego el ultimo router del dominio toma ese paquete resultante retira la etiqueta y lo reenvía hacia la ruta de la red destino, como un enrutamiento IP simple.

CAPITULO III:
MPLS-VPN
MPLS EN REDES PRIVADAS VIRUTALES

3.1.- REDES PRIVADAS VIRTUALES / VIRTUAL PRIVATE NETWORKS

Fueron originalmente usados para permitir a los ISP usar infraestructura física común para emular enlaces Punto a punto entre los locales de los clientes. Una red de cliente implementada con cualquier tecnología VPN debería contener distintas regiones bajo el control del cliente, llamadas, sitios del cliente, conectados a través de la infraestructura del ISP.

En las redes tradicionales estos enlaces se hacían con infraestructura propia para cada punto, lo que significaba mucho gastos, tanto económicos, como en procesamiento, además que estos gastos, crecían según el número de sitios conectados mediante enlaces dedicados.

En la arquitectura MPLS VPN, los routers de borde conducen la información de enrutamiento de los clientes entre sitios, proveyendo de enrutamiento óptimo para el tráfico que pertenece al dominio de red del cliente, con el fin de habilitar la comunicación entre locales físicamente distantes.

El modelo MPLS-VPN también acomoda al cliente usando espacios de direcciones superpuestas, este tema esta detallada con más profundidad en páginas posteriores.

Como lo expresa Jorge Atouguia (2008):

> MPLS VPN es una implementación del modelo Peer to Peer, los sitios de cliente intercambian tráfico e información de enrutamiento usando como medio el Backbone MPLS VPN del ISP. El dominio MPLS VPN consiste en las redes de los clientes y la red del proveedor.

Otra de definición claro acerca del uso de la tecnología de VPN lo expresan Roca T., Chica P., Muñoz M., en el informe de su trabajo sobre MPLS (2004):

> Las VPN se basan en conexiones de infraestructura compartida con funciones de red y de seguridad. El objetivo de las redes virtuales es el soporte de las aplicaciones intra/extranet, donde se puede integrar aplicaciones de multimedia de voz, de datos, y de video. La seguridad supone aislamiento y privada nos indica que el usuario cree que posee los enlaces.
>
> Las VPN están basadas en protocolo de red IP de Internet.

3.2.- COMPONENTES DE LA RED MPLS-VPN

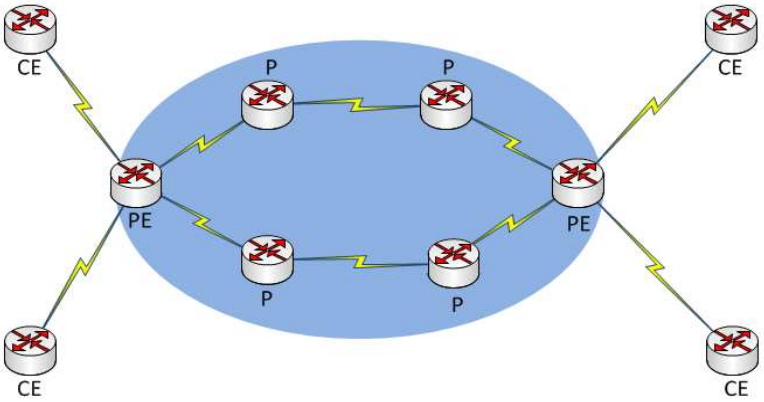

Fig. 3.1.- Arquitectura de red MPLS – VPN

Fuente: Autor.

Los componentes de la red MPLS VPN son:

- **Red del Cliente.**

  Son los equipos que el cliente tiene en sus locales, tanto en su red interna como para la conexión con el ISP.

- **CE Routers (Customer's Edge Routers)**

  Routers de borde del cliente.- son los routers que se encuentran en el sitio/local del cliente y que proporcionan la conectividad entre la red del cliente y la red del ISP. Consiste en la topología a estudiar de los routers CE1 y CE2.

- **Red del proveedor.**

  Es el dominio controlado por el proveedor, que corresponde a la infraestructura, esta controla el enrutamiento de tráfico entre los sitios pertenecientes a un cliente.

- **PE Router (Provider's Edge Routers).**

  Son los routers en la red del proveedor, que se conectan los routers de borde del cliente (CE), y crean así el enlace entre cliente e ISP, está constituido en la topología a estudiar por los routers PE1 y PE2.

- **P Router (Provider's Routers).**

  Routers del proveedor.- Que son los routers del núcleo de la red del Proveedor que hacen la conexión entre los PE's y que se encuentran localizados en la nube del ISP, y normalmente se conocen a través de un IGP.

3.3.- MODELO DE ENRUTAMIENTO DE LA RED MPLS-VPN.

El modelo de implementación MPLS–VPN en la práctica es muy parecido a un Peer-to-Peer, desde la perspectiva de un CE1, que envía datos al CE2, la información de red a compartir con el PE1 (que sería el siguiente salto), serán paquetes sencillos, sin mayor encapsulación más que la IP y de esta misma manera se verá en el CE2, al recibir los datos desde el PE2. Es entre los routers dentro de la nube del proveedor (PE1, P, PE2), es que se realiza la implementación de la tecnología MPLS, siendo este proceso transparente a los CEs, de manera que, para ellos se verá como si fuese un Peer-to-Peer.(Lacy Lobo, 2005).

Entonces en el CE el único requerimiento es un protocolo de enrutamiento, que permita intercambiar rutas e información e actualizaciones IPv4 con el PE, o una ruta por defecto que conduzca cualquier tráfico hacia el PE, este

último es el método más usado, aunque no nos provee la posibilidad de crear backups automáticos en el enlace CE-PE.

En la implementación, el router PE desempeña diferentes funciones. Este router, debe tener la capacidad de separar e aislar el tráfico de los clientes, si más de un cliente está conectado a la red. Cada cliente, tiene asignado una tabla de enrutamiento virtual independiente dentro del PE, esta tabla es llamada VRF (Virtual Routing Forwarding). El enrutamiento a través del Backbone del proveedor, es desempeñado usando el proceso de etiquetas MPLS.

Los router P proveen la conmutación de etiquetas entre los PE routers y desconocen de las rutas VPN. Los CE, no conocen de la existencia de los P, y entonces, la topología interna del Proveedor es transparente al usuario.

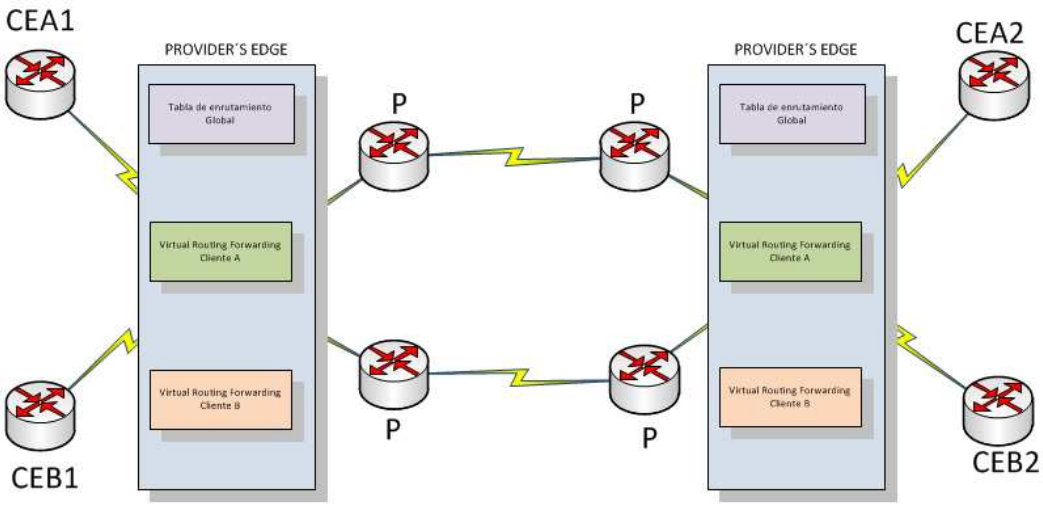

Fig. 3.2.- Modelo de enrutamiento – VPN

Fuente: Implementing MPLS on Cisco IOS – Cisco Press (2004)

Autor: Lancy Lobo

Los routers P solo son encargados de conmutar paquetes. Ellos no llevan rutas VPN y ellos no participan en el enrutamiento MPLS VPN. El PE intercambia rutas IPv4 con los routers CEs conectados usando contextos

individuales de protocolos de enrutamiento, solo para la conexión entre ellos y la red interna LAN del sitio conectado al Cliente.

Para habilitar el escalamiento de la red para un largo número de VPNs de clientes, la RFC 4364: BGP/ MPLS IP Virtual Private Networks de Rosen y Rekhter (2006), define que Multiprotocol BGP debe ser configurado entre los PE para acarrear rutas de los clientes, este tema será tratado más adelante.

3.3.1- ENRUTAMIENTO – REENVIO VIRTUAL / VIRTUAL ROUTING FORWARDING (VRF).

El aislamiento de la información entre clientes es desarrollado en el PE usando tablas de enrutamiento virtuales, una por cada cliente, para ser más específico, que también son llamadas VRF, de esta manera, aseguramos, que la información de enrutamiento de cada uno de ellos se encuentre separada del resto.

La diferencia de una tabla de enrutamiento global con una VRF es que la VRF solo tiene enrutamiento e información acerca de la VPN del cliente, mientras la tabla de enrutamiento global tiene la información de conectividad del router PE, además de las rutas del dominio MPLS. Asociada a la VRF, existe también una tabla CEF específica, análoga a la tabla CEF global que define los requerimientos de conectividad y protocolos para cada sitio del cliente en un PE sencillo.

El VRF define los contextos de los protocolos de enrutamiento que son parte de una VPN específica, por lo cual se debe asignar por lo menos una interfaz, ya sea física, o lógica a la VRF, la interfaz designada normalmente será la que forme el enlace entre el PE y el CE del cliente en mención, ya

que mediante esta se hará el respectivo forwarding de la información recibida desde y hacia la VPN.

La interfaz que es parte del VRF debe poder habilitar la conmutación CEF (Cisco Express Forwarding). El número de interfaces que se pueden atar a una VRF está limitado solamente al número de interfaces en el router, y a su vez una interfaz puede ser asociada solo con una VRF.

En su trabajo Fundamentos MPLS/VPN (2009), Rogelio Alvez define las VRF en las tres siguientes características:

- La tabla VRF contiene rutas que deberían estar disponibles para un conjunto de sitos de una misma VPN.
- Es una tabla análoga a una tabla de rutas tradicional.
- Las interfaces que se conectan a los routers de los sitios miembros son asignados a VRFs:
    - Una VRF oir interfaz.
    - Posiblemente, muchas interfaces para una VRF.

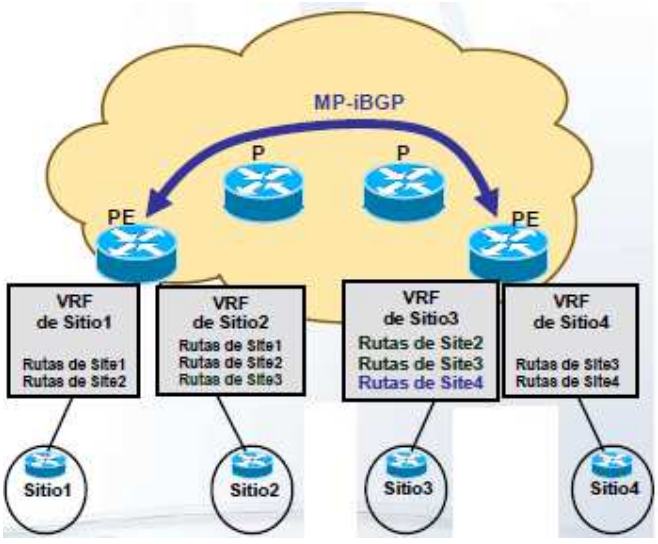

Fig. 3.3.- Modelo de funcionamiento de VRFs

Fuente: Fundamentos MPLS/VPN, Rogelio Alvez (2009)

Entonces, haciendo un resumen, La VRF es una tabla de enrutamiento IP análoga a la tabla de enrutamiento Global, en esta tabla solo se encuentra la información de enrutamiento de la VPN específica, y hay que recordar que las VPNs no tienen conocimiento de la existencia de la red MPLS, ya que esta es transparente a ellos, por lo tanto las LAN de los sitios del cliente se verán entre ellas como redes directamente conectadas.

La VRF también contiene: la tabla CEF, la lista de las interfaces que son parte de la VRF, y un set de reglas que definen el protocolo de enrutamiento con el que intercambia datos con el CE.

Por esto cada VRF también tiene identificadores, que distinguen a una VRF de otra, como son el Route Distinguisher y Route Target, que funcionan con el Protocolo de enrutamiento BGP, y sirven para implementar el aislamiento de clientes y diferenciar los paquetes que circulan por el dominio MPLS, ambas características trabajan en conjunto con MPLS y BGP (MP-BGP) para realizar el forwarding respectivo de la información a través del dominio del proveedor.

3.3.2.- PROTOCOLO DE PASARELA DE BORDE / BORDER GATEWAY PROTOCOL (BGP)

El Border Gateway Protocol, fue creado para intercambiar información entre los routers de borde de diferentes sistemas Autónomos, lo que lo convierte en un EGP, aunque también tiene funcionalidades que lo pueden hacer trabajar como IGP (iBGP).

Un Sistema Autónomo es un grupo de equipos o routers que contienen las mismas políticas de ruteo y encaminamiento, y que forman parte de una

misma organización por eso comparten la misma información interna, por ejemplo, Una compañía muy grande es un AS, y debe tener un numero identificador de AS designado, dentro de su red los routers tendrán las mismas características de enrutamiento.

Un ejemplo del uso de este protocolo es la conexión entre dos ISP, este enlace necesita usar el protocolo BGP, por el cual los routers de borde de ambas compañías intercambiaran información de enrutamiento, cada uno de estos ISP tendrá su número de AS, porque cada ISP tiene políticas de ruteo internas diferentes.
Los Números identificadores de AS van desde el 0 al 65535, y cumplen con una dinámica parecida a la de las direcciones IP, existe un rango de números AS públicos los cuales son otorgados a grandes compañías que son poseedoras de redes muy extensas, como los ISP, y existe un rango de números privados que pueden ser usados por cualquier administrador para prácticas o para que cada proveedor le otorgue un AS a los clientes que crea conveniente dentro de su red, el control y asignación de números de AS públicos lo realiza la IANA (Internet Assigned Numbers Authority) de la misma manera que se realiza con las direcciones IP públicas.

El rango de números AS, públicos o controlados por la IANA va del 0 al 64512 y el rango de números privados va desde el 64512 al 65534.

La principal diferencia entre BGP y los demás protocolos de enrutamiento, como OSPF, RIP y EIGRP, es que BGP no usa métricas como conteos de saltos, Ancho de Banda, o retardo, si no que toma decisiones de encaminamiento, en base a políticas de la red, o reglas que se definen mediante ciertos atributos de BGP.

Otra diferencia de los demás protocolos de enrutamiento con BGP, es que este último es un protocolo completamente configurable, es decir, las

políticas y los procesos de BGP pueden ser manipulados por el administrador de red, de manera que, por ejemplo, en BGP, debemos declarar los vecinos BGP que tenemos dentro de la topología, además declarar de las políticas para el intercambio de rutas, entre muchas otras opciones que los otros protocolos hacían automáticamente y en base a parámetros ya establecidos. Esto le brinda una ventaja muy grande a BGP, ya que el administrador tiene el control de la dinámica de enrutamiento y la puede personalizar, en base a sus necesidades. (Amit Rai, 2010).

El único requisito para que 2 routers sean vecinos BGP, es que sea alcanzable el uno al otro dentro de un dominio, esto significa, que estén directamente conectados, o que posean un IGP entre ellos, por medio del cual ellos se conozcan, e intercambien información.
Al declararse el uno a otro como vecinos en sus respectivas configuraciónes, estos routers intercambian un TCP Three-way handshake, (SIN, ACK, SIN-ACK) y se establece la sesión TCP.

Los routers vecinos BGP, intercambian información mediante 4 mensajes de red que son los siguientes:

OPEN: Con este se establece la sesión BGP, luego del establecimiento de sesión TCP.

UPDATE: mensajes de Actualización, se envía cada vez que una ruta cambie, o que un enlace se caiga y ya no sea factible la ruta.

KEEPALIVE: Una vez que se ha establecido sesión BGP, se envía periódicamente este mensaje para informar que la sesión se encuentra activa.

NOTIFICATION: Se envía cuando se cierra una sesión TCP, o cuando ocurre un error que requiere del cierre de la misma.

Estos mensajes sirven para el mantenimiento de la Sesión de vecinos BGP.

Para el intercambio de rutas, como se mencionó antes, se usan un grupo de políticas que serán definidas por el administrador, este es un tema muy amplio, y que sería perfectamente un tema para un nuevo proyecto, así que solo detallare los más importantes de manera superficial.

Estas políticas se definen mediante los atributos BGP, de los cuales los más importantes son:

ORIGIN: Específica el protocolo por el cual la dirección IP fue aprendido en un comienzo, tiene 3 valores posibles:

IGP.- Cuando fue aprendido por un IGP.
EGP.- Cuando fue aprendido mediante BGP.
Incomplete.- Cuando fue aprendido en primera instancia por una ruta estática.

AS-PATH.- Específica el camino o el conjunto de los AS, por los que el paquete ha pasado para llegar hasta su destino. Cada que el paquete atraviese un AS, a su salida del mismo, se añadirá el número de AS por el que pasó a esta lista.

NEXT-HOP: Especifica la ruta del siguiente salto hacia el destino, obtenida de la tabla de enrutamiento BGP.

MED (MULTI-EXIT DISCRIMATOR): Este atributo sirve cuando se tienen dos salidas del AS hacia el mismo destino, se usa para establecer prioridad

en una de las dos, se configura un valor de MED menor a la ruta preferida, o en su defecto se configura el mismo valor a ambas para realizar balanceo de carga.

LOCAL PREF: Cuando dentro de un AS, hay dos routers de borde como vecinos iBGP, este atributo configura cuál de los dos será preferido localmente en el AS para los paquetes que deben salir de él.

En base a estos atributos podemos restringir o permitir las actualizaciones, es decir, podemos impedirle que ingresen actualizaciones que tengan como origen el parámetro IGP, o podemos restringir el ingreso de actualizaciones que hayan seguido un AS_PATH determinado, o aislar aquellas que hayan pasado por un determinado AS, configurar la ruta de salida del AS con LOCAL PREFERENCE o configurar Balanceo de carga con el atributo MED, estos son solo los principales pero existe una gran cantidad de los mismos, los cuales podrían ser detallados en un estudio profundo del protocolo BGP.

Como se ha mencionado en líneas anteriores, hay dos tipos de sesiones BGP.
iBGP y eBGP. Llamamos una sesión eBGP cuando conectamos dos routers de borde de 2 AS diferentes, una sesión IBGP por el contrario es un sesión BGP entre dos routers de Borde dentro del mismo AS, esto se da cuando tenemos dos o más salidas del AS hacia otros Sistemas Autónomos.

Hay dos reglas en iBGP que lo diferencian de eBGP, y que definen el hecho de que ellos trabajen de una manera distinta como lo define Amit Rai en su trabajo “IBGP Basics” (2010):

Regla 1.- Las rutas aprendidas de un vecino IBGP no serán transmitidas a otro vecino IBGP. Esto tiene como fin evitar loops dentro del dominio BGP entre los vecinos.

Regla 2.- Para que una ruta sea aprendida desde un vecino IBGP, esta debe ser primero aprendida por un IGP.

3.3.3. – BGP MULTIPROTOCOLO / MULTIPROTOCOL BORDER GATEWAY PROTOCOL (MP-BGP).

El protocolo usado para intercambiar rutas VPNv4 entre los routers PE es el MP-BGP, que es una mezcla de procesos BGP y MPLS, que trabajan juntos. MP-BGP es también responsable de la asignación de una etiqueta VPN. El reenvió de paquetes en una red MPLS VPN obliga a que el router especificado como el próximo salto en la actualización BGP entrante sea el que asigne la etiqueta VPN. Además, este protocolo permite la superposición de segmentos de redes de los clientes.

La sesión entre los router BGP en un mismo BGP-AS es llamada una sesión MP-iBGP y sigue las mismas reglas que en la implementación de un IBGP con consideraciones hacia los atributos BGP. Si es que la VPN se extiende a más de un AS, las rutas VPNv4 serán intercambiadas entre los límites de AS usando una sesión MP-EBGP. (Amit Rai, 2009)

Es por ello que Carlos Vicente en su trabajo acerca de las Practicas Recomendadas en BGP, elaboradas para el 14º Taller sobre Tecnologías Internet para América Latina y el Caribe (2011), nos advierte que:
“IBGP debe ejecutarse en todos los enrutadores que estén en la trayectoria entre conexiones externas.”

Y nos recomienda usar el siguiente procedimiento para usar comenzar a migrar/desplegar iBGP en nuestra red:

Paso 1.- Crear una malla completa entre los enrutadores seleccionas para iBGP.

Paso 2.- Instalar los prefijos de los clientes en iBGP.

Paso 3.- Sacar con cuidado las rutas estáticas que están ahora en el IGP y en iBGP.

Paso 4.- Continuar con el despliegue de eBGP.

3.3.4.- FAMILIAS DE DIRECCIONES / ADDRESS FAMILY.

El identificador Address Family BGP fue introducido con el MP-BGP y está diseñado para ser escalable. MP-BGP transporta información de enrutamiento de diversos protocolos de capa de red y rutas multicast IP.

Cada address-family mantiene una base de datos BGP separada, que permite al administrador configurar políticas BGP en cada address-family.

Familias de Direcciones VPNv4 / VPNv4 Address-Family.

Es usado para identificar las sesiones de enrutamiento para protocolos como BGP que usan la versión estándar de prefijos de direcciones VPNv4. Las rutas VPNv4 son las mismas que las rutas IPv4, a diferencia que las rutas VPNv4 tienen una característica, llamada Route Distinguisher, que permite la replicación de prefijos. Es posible asociar cada RD distinto con una VPN diferente. Cada VPN necesita su propio set de prefijos VPNs, cuando son usadas en MPLS, permiten a diferentes sitios interconectarse transparentemente a través de la red de un proveedor de servicios. Una red de proveedor puede mantener distintas IP VPNS. Cada una de estas se verá ante sus usuarios como una red privada, separada de las otras redes.

Con una VPN, cada sitio puede enviar paquetes IP a otro sitio dentro de la misma VPN. Cada una de ellas está asociada con una o más VRFs. El

router que usa BGP distribuye la información de enrutamiento VPN usando el atributo BGP extended communities. (Amit Rai, 2010).

3.3.5.- COMUNIDADES EXTENDIDAS / EXTENDED COMMUNITY.

El Atributo Extended Community provee un mecanismo de etiquetamiento de la información acarreada en BGP-4, El libro Implementing BGP on Cisco Routers de Cisco Systems (2005), nos señala que este atributo especifico provee dos importantes realces a las características de las BGP Communities:

- Un rango extendido, asegurando que las comunidades pueden ser asignadas para muchos usos, sin temor de superposición, con esta característica particular funciona el atributo Route Distinguisher.

- La adición de un campo Type provee estructura para el espacio de comunidad.

La adición de estructura permite el uso de políticas basadas en la aplicación para la cual el valor de comunidad va a ser usado.

Por ejemplo, el administrador puede filtrar todas las comunidades de un tipo particular, o permitir solo ciertos valores para un tipo particular de comunidad.
Esto también permite a uno especificar si la comunidad particular es transitiva o no transitiva a través de los limites AS. Sin estructura, este solo puede ser alcanzado por enumeración explicita.

3.3.6.- DISTINGUIDOR DE RUTAS / ROUTE DISTINGUISHER (RD).

Los routers PE provee aislamiento entre clientes usando VRFs, sin embargo, la información necesita ser llevada a través de una topología común, por lo que se necesita que estos routers sean capaces de implementar procesos que permitan la superposición de las direcciones IP que funcionan en los Clientes, esto se debe a que, como podemos imaginar, muchos clientes usaran los mismos segmentos de red (direcciones privadas) en sus LAN, por lo que sería un caos la transmisión en un medio común, si por ejemplo:
Dos clientes tuvieran configurado el segmento 192.168.0.0/24 en sus LAN, lo más probable es que al ser transportada a través del dominio del Proveedor, se confundan, si no tuvieran el proceso para distinguirlas, para estos fines existe el RD.

El RD es un identificador de 64 bits que se adhiere a los 32 bits (IP) de prefijo del cliente o de la ruta aprendida del router CE, juntos, hacen un valor único de 96 bits, que puede ser transportada a través de los PE en un dominio MPLS. (Amit Rai, 2010).

Este valor RD único es configurado por VRF en el PE. Cada VRF tendrá un valor diferente de RD. Entonces la dirección resultante, la suma de la dirección IP (32 bits) + el RD (64 bits) es conocida como la dirección VPNv4.

De esta manera se distinguen las actualizaciones de las direcciones de clientes que tengan configurado el mismo segmento de IP privadas dentro de sus LAN.

Estas direcciones VPNv4 son intercambiadas entre los PE en la red del Proveedor.

El RD puede tener dos formatos. Si el proveedor no tiene un numero AS de BGP, se usara la IP y si lo tiene Se usara el número de AS.

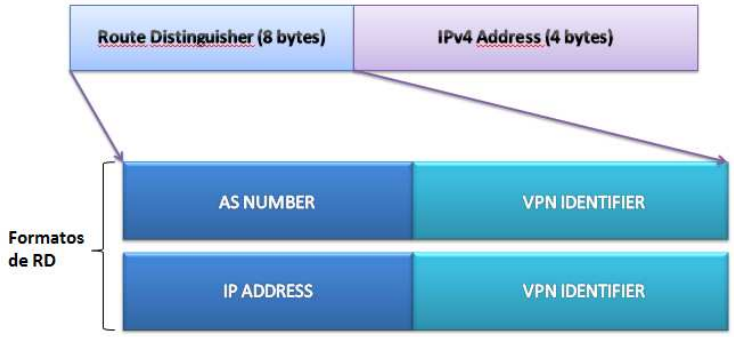

Fig. 3.4.- Formatos de Route Distinguisher

Fuente: Autor.

3.3.7.- OBJETIVOS DE RUTA / ROUTE TARGETS (RT).

Son identificadores adicionales usados en el dominio MPLS VPN que identifica la membrecía VPN de las rutas aprendidas de un sitio particular. Son implementadas por el uso de BGP extended communities.

Así como se usa el RD para mantener la unicidad entre direcciones de red idénticas que vienen de distintos clientes, los RT pueden ser usados para compartir rutas entre ellos. Podemos aplicar los RT a una VRF para controlar la importación y exportación de rutas entre ellos y los otros VRF.

Un RT toma la forma de una BGP extended community con una estructura similar a la de un RD (quizá por esto son comúnmente confundidos). El RT es en sí una comunidad BGP de 64 bits que se usa para etiquetar prefijos. Cuando exportamos prefijos desde la VRF, añadimos a los prefijos una Comunidad RT, así cuando el PE remoto tiene que importar los prefijos a la VRF, puede fácilmente determinar que prefijos importar.

Aun así, este tema, la diferenciación entre RD y RT, sigue siendo muy confuso, el siguiente ejemplo intenta despejar dudas:

En una Red supuesta estamos usando el mismo RD para todos los sitios del cliente A. Pero el administrador no quiere permitir que todos los sitios se vean entre todos. Es decir, se puede hacer que el Local 2 tenga visibilidad de los prefijos del Local 1, pero no quiero que vea los prefijos del local 3.
Y lo mismo para el local 3 quiero que tenga visibilidad con el local 1 pero no con el local 2.
Entonces aplicaremos el RT 1:100 para la VRF del local 1, el RT 1:200, para la VRF del local 2 y el RT 1:300 para la VRF del local 3.
En tal caso debemos declarar en la VRF del local 1, que importe los prefijos que vengan con los RT 1:200 y 1:300. Mientras que en los locales 2 y 3 solo importaremos rutas con el RT 1:100. De manera que entre ellos no se verán, este es el uso del RT mientras que el RD como dijimos es un diferenciador de rutas superpuestas que viajan a través del dominio MPLS.

3.3.8.- OPERACIÓN DE RT Y RD EN MPLS

El siguiente ejemplo ha sido tomado del libro *Implementing MPLS on Cisco IOS Software de Lancy Lobo* (ISBN 1-58705-199-0) en su Capítulo MPLS VPN Routing Model. El cual es un ejemplo detallado y preciso para comprender mejor la dinámica del funcionamiento de RT y RD.

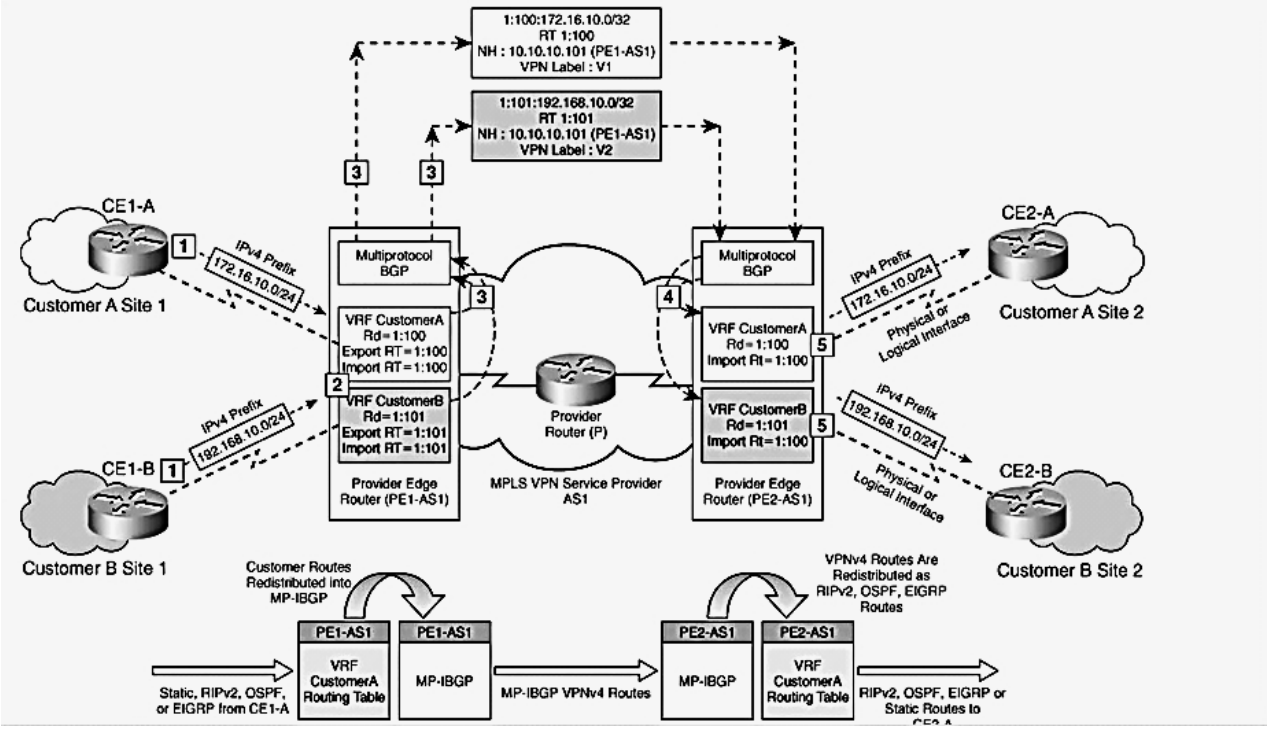

Fig. 3.5.- Modelo de enrutamiento – VPN

Fuente: Implementing MPLS on Cisco IOS – Cisco Press (2004)

1. *El prefijo 172.16.10.0/24 es recibido desde el CE1-A, que es parte de la VRF del Cliente A en PE1-AS1*
2. *PE1 asocia un valor RD de 1:100 y un valor de 1:100 al RT como configurado en la definición de VRF en el PE1-AS1*
3. *Las ruta aprendida de CE1-A es redistribuida en el proceso MP-BGP en PE1-AS1 donde al prefijo 172.16.10.0./24, se le antepone el valor de Rd de 1:100 y se le pospone con el valor export RT, que es el RT de la comunidad extendida, antes de enviar el prefijo VPNv4 como parte de la actualización MP-iBGP entre los PE.*

   La etiqueta VPN es asignada para cada prefijo aprendido del proceso de IGP de los CE conectados con una VRF por el proceso MP-BGP del PE.

MP-BGP corriendo en el dominio MPLS del Proveedor acarrea el prefijo VPNv4 en adición a el BGP RT extended community.

Nótese que a pesar que el RT es una configuración obligatoria en una MPLS VPN para todas las VRFs configuradas en un router, el valor RT puede ser usado para implementar topologías VPN complejas en las cuales un solo sitio puede ser parte de más de una VPN.

Además, el valor RT puede ser usado para desempeñar la importación de rutas selectivas a una VRF cunado las rutas VPNv4 son aprendidas en las actualizaciones MP-iBGP.
La etiqueta VPN es solo comprendida por el PE de salida que está directamente conectado al CE que comparte el prefijo.
Nota: Los próximos saltos en los PE no deben ser compartidos en el proceso BGP, pero debe ser aprendido por medio del IGP para la implementación del forwarding MPLS en el dominio.

4. *La actualización MP-BGP es recibida por el PE2, y la ruta es guardada en la apropiada VRF para el Cliente A basada en la etiqueta VPN.*

5. *Las rutas MP-BGP son redistribuidas en el proceso de enrutamiento VRF PE-CE y las rutas son propagadas en CE2-A.*

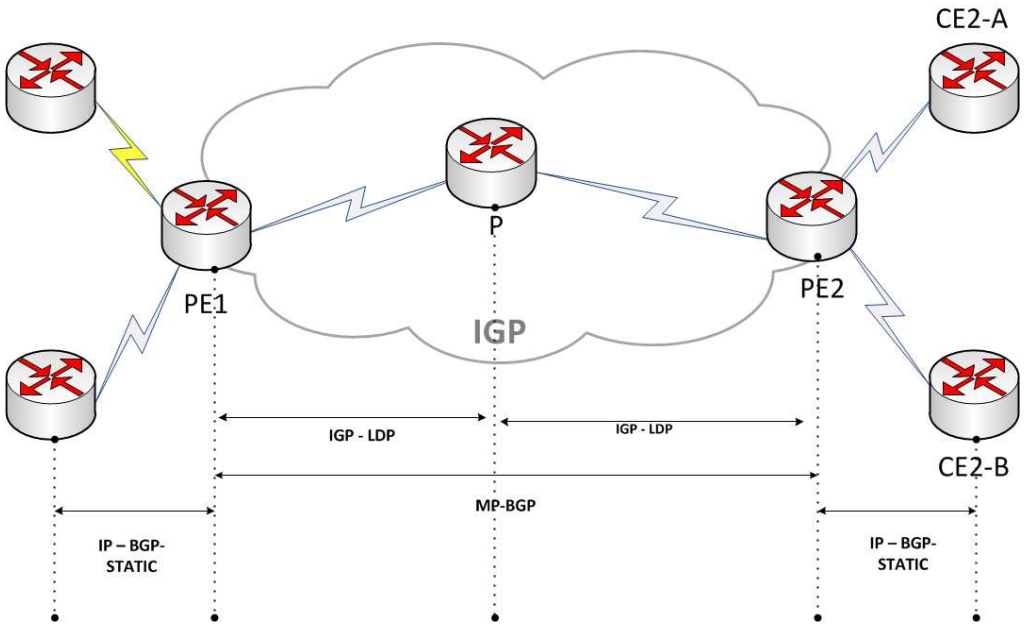

Fig. 3.6.- Protocolos en la red MPLS VPN

Fuente: Autor.

3.3.9.- PLANO DE CONTROL EN MPLS VPN

La implementación del plano de control en MPLS VPN contiene toda la información de capa 3, enrutamiento, y los procesos de LDP, el plano de datos en cambio desempeña las funciones relativas al reenvía de los paquetes IP, y los paquetes etiquetados hacia su destino.

CAPITULO IV:

DISEÑO Y CONFIGURACION DE LA RED DE TRANSPORTE DE DATOS.

4.1.- RED DE TRANSPORTE DE DATOS.

Es una red casi siempre de ámbito nacional, que sirve para transportar información de un punto a otros de forma unidireccional o bidireccional, se utiliza por los proveedores normalmente para comunicar diferentes locales de clientes conectados entre sí, haciendo un ejemplo, se puede hablar de una red de restaurantes de comida rápida que tiene un sistema contable y de facturación, el cual es compartido entre todos los puntos, para esto se necesita la red de transporte de datos para interconectar todos los puntos con una central o matriz que es donde reposaran los servidores.

A diferencia de una red de internet, las redes de transporte no necesitan hacer un enmascaramiento de las direcciones IP para poder interconectarse, es decir, normalmente en un ISP, los clientes de internet tienen configurado un NAT, que es una técnica de enmascaramiento del segmento de red de IPs privadas configuradas en los locales del cliente en un nodo central donde toda la información se disfraza con una dirección IP publica la cual se encuentra enrutada en el dominio del proveedor para tener acceso a la Internet. En este caso nuestro objetivo no es ingresar al internet sino solamente hacer una conexión entre los diferentes puntos para intercambiar información.

4.1.1.- DISEÑO DE LA RED DE TRANSPORTE DE DATOS.

Puesto que es prácticamente imposible hacer la emulación de una red completa de transporte de datos, este proyecto se trata de la configuración y diseño del Núcleo de esta red, es decir, aplicando los conocimientos anteriormente explicados, haremos la configuración de los P (Provider´s Router), PE (Provider´s Edge Router), y de los CE (Costomer´s Edge Router) del Core de esta red.

Puesto que la red de transporte de datos es de carácter nacional, en nuestro diseño utilizaremos routers concentradores, que se encontraran Ubicados estratégicamente en las Ciudades de Quito, Cuenca, Guayaquil, para estos locales utilizaremos equipos Cisco 7600.

Y estarán conectados mediante una conexión Gigabit Ethernet, en donde el medio de transmisión podría ser a través de Fibra Óptica, ese es un tema en el que no nos adentraremos mucho en este proyecto, pero es que para tener una visión completa de la red hacemos mención en esta sección.

Estos Equipos son los que funcionaran como los P o PE, dependiendo del requerimiento y la dirección de la información, estos routers servirán para realizar el proceso MPLS y también servirán para formar conexiones entre las ciudades principales.

Conectados a cada uno ellos por medio de otro enlace Gigabit Ethernet estará conectado otro router cisco 7600 el cual será el equipo de la distribución y enrutamiento para la red local de las ciudades bajo la administración de la oficina. Se ha escogido los routers 7600 pues dentro de los routers que nos presenta el simulador este es el que tiene las capacidades de MPLS y BGP que se necesita usar en la topología.

En este router se encontrara la información del enrutamiento hacia los clientes y sus direcciones de red, las mismas que servirán para realizar las pruebas para determinar si la simulación ha sido exitosa o tiene algún inconveniente.

Estos routers en la topología básica de MPLS, serán los CE, y dentro de estos routers crearemos algunos segmentos de redes con interfaces loopbacks que nos servirán para simular un enlace que siempre estará activo, puesto que finalidad de la loopback es precisamente esa, simular una interfaz que siempre estará up.

Accionaremos un protocolo OSPF, para las comunicaciones entre los routers P en el dominio MPLS y también crearemos las VPN, y el enrutamiento BGP para la conexión entre los puntos.

Hay que tener en cuenta siempre, (aunque este no sea el caso de las topología que estudiaremos), que dependiendo de la dirección de la información es decir de la red de la que sale y hace que red va dependerá el rol de los routers en la topología. Usando como ejemplo la figura 4.1, si una red en el CE de Quito quiere hacer un ping a el Router CE de Cuenca entonces los routers principales en Quito y Cuenca harán las veces de PE, mientras que el router de Ambato Hará las veces de P.

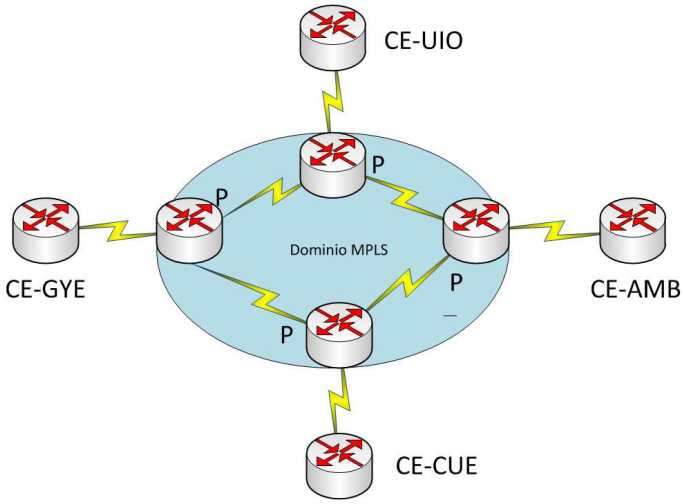

Fig. 4.1.- Modelo de Red MPLS – VPN - Con 4 routers

Fuente. Autor.

4.2.- SOFTWARE GNS3

GNS3 es un software simulador de redes, creado por Jeremy Grossman, Benjamin Marsili, Claire Godjil, Alexey Eromenko y lanzado en el mes de Octubre 2007. Este Software es parte del Conocido Freeware, su licencia no tiene costo y se encuentra fácilmente en la web. Se basa en un simulador grafico en el que se pueden crear topologías de red, desde las más básicas hasta las más complejas.

En él se puede emular routers Cisco, así como servidores Linux y sus conexiones físicas, por medio de los diferentes tipos de cables, desde los Ethernet, FastEthernet, Gigabit Ethernet, etc.

Resulta una herramienta extremadamente útil, que nos sirve para emular la red completa, sus conexiones y realizar troubleshooting para determinar los inconvenientes presentados.

Además, el GNS3 tiene una aplicación complementaria llamada Dynamips que sirve para ejecutar el IOS de los equipos Cisco directamente en los routers simulados que vamos a utilizar lo que nos permite realizar las configuraciones exactamente igual a como las haríamos en los equipos físicos, conectando un cable de consola, y usando un programa terminal.
También cuenta con compatibilidad a otras aplicaciones de simulación como el VirtualBox que permite emular tráfico de VoIP, para habilitar este tipo de redes en el programa.

4.2.1- VENTAJA Y DESVENTAJA DE GNS3 SOBRE OTROS SOFTWARES.

- **VENTAJA**

La ventaja que tiene GNS3 sobre otros software conocidos como el Packet Tracer de Cisco, es que en GNS3 las configuraciones se realizan en la imagen de un IOS que se está ejecutando en tiempo real en la PC, a diferencia de Packet Tracer, en donde es una emulación del IOS la que es muy básica. Por ejemplo en Packet Tracer no podemos utilizar Protocolos más extensos como BGP, o tecnologías más complejas como MPLS, entre otras.

- **DESVENTAJA**

Una desventaja de GNS3 es que al ser IOS una aplicación compleja, dentro de una misma simulación no se pueden utilizar una gran cantidad de routers funcionando, puesto que consumiría gran cantidad de memoria RAM, y esto haría que el procesamiento de la PC se vuelva extremadamente lento, o se inhiba.

4.2.2.- IMÁGENES DE EQUIPOS.

Para que los routers funcionen en las emulaciones, estos cargan imágenes del IOS de los routers en mención. Los Cisco que se utilizan en este programa y que vienen por defecto, en el programa son los equipos de las series 1700, 2600, 3600, 3700, 7200. Para cada uno de ellos existen imágenes del IOS mediante las cuales la aplicación Dynamips correrá una el IOS en una ventana terminal en DOS.

4.2.3.- INTERFAZ DE TRABAJO DEL GNS3

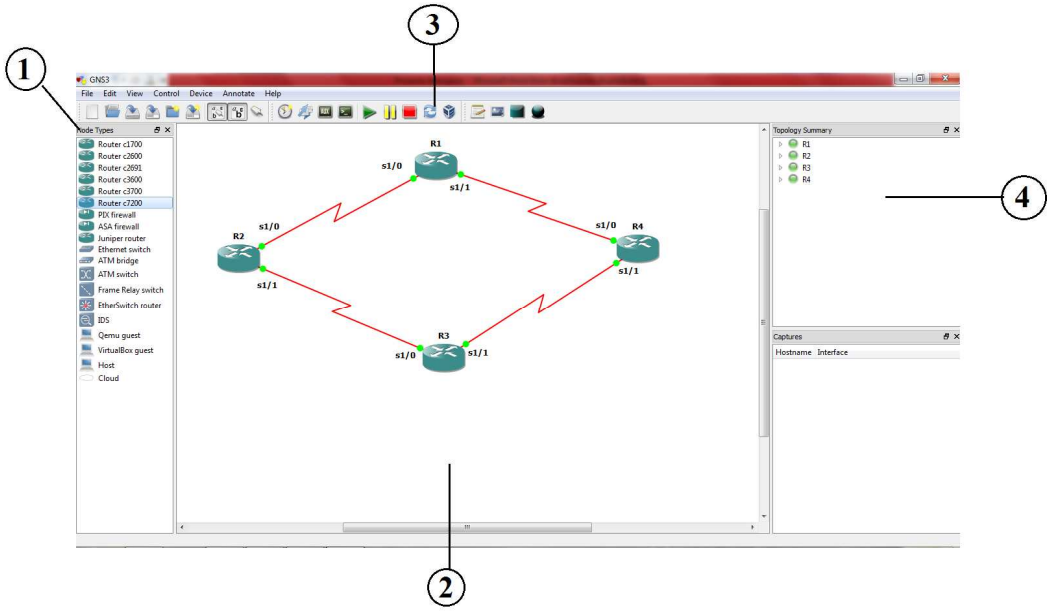

Fig. 4.2.- Área de Trabajo en GNS3

Fuente: Autor. Captura de pantalla software GNS3.

1.- Tipos de Nodos.- Aquí encontramos los diferentes dispositivos que servirán tanto como terminales o como Concentradores en la arquitectura de red.

2.- El área de trabajo grafica es en donde dibujaremos la topología de la red, hace falta solo tomar un dispositivo de la barra de nodos y arrastrarlo hacia el área de dibujo para que este se haya cargado en la topología.

3.- La barra de menú principal se divide en 3 Partes.

Fig. 4.3.- Barra de herramientas de GNS3
Fuente: Autor. Captura de pantalla software GNS3.

La cual para caso de estudio la he dividido en 3 partes en el grafico superior.

a.- General (Naranja).- Esta constituida por los botones básicos, como Nuevo archivo, Nuevo Proyecto, Guardar archivo, Guardar Como proyecto, y las últimos 3 iconos corresponden a opciones que nos permiten de izquierda a derecha respectivamente, Mostrar los nombres de las interfaces que estamos utilizando, Mostrar el Nombre de los Routers que estamos usando y la última nos permite crear el enlace o el tipo de cable que utilizaremos para unir los routers.

b.- Emulación (Azul): nos sirve para manipular la emulación, tenemos las opciones de Izquierda a derecha:

Fig. 4.4.- Barra de Emulación. Captura de pantalla software GNS3.
Fuente: Autor.

- *Snapshot, permite tomar una captura de pantalla.*
- *Import Export Start-up Configs.- como su nombre los dice nos permite grabar o import configuraciones de routers.*
- *Console AUX to all devices,- comienza a correr las conexiones por consola en los puertos auxiliares de todos los equipos.*
- *Console to all devices.- Comienza a correr las conexiones por consola de todos los equipos.*
- *Start.- Inicia la emulación de la red, arranca todos los routers y linkea todas las conexiones.*
- *Pause.- Realiza una Pausa en la emulación.*
- *Stop.- Detiene la emulación, apaga todos los routers.*
- *Reload all.- Reinicia todos los equipos en la simulación.*
- *Virtual Box Manager.- Nos ayuda a conectar una sesión en VirtualBox para emular trafico VoIP.*

c.- Dibujo (Verde).- esta barra sirve para hacer comentarios o dibujos extra en la topología, como poner un fondo al diseño, o poner nombres a las regiones, o por ejemplo, poner los segmentos de red para diferenciar las conexiones.

4.- Área de simulación.- Aquí se detallan los dispositivos que están siendo usados en la interfaz de diseño y su estado, con un círculo rojo si están detenidos, o uno verde si están encendidos.

4.3.- INTRODUCCION A LA SIMULACION.

En este proyecto vamos a realizar simulaciones que nos servirán para conocer más detalladamente la tecnología MPLS.

En ellas vamos a descubrir las topologías básicas de MPLS, y a su vez la forma de configurar los routers dentro de un dominio multiprocolo para transporte de datos.

Para realizar una simulación en GNS3, el primero paso es definir la topología a usar. Luego tomar uno de los nodos disponibles en la sección tipos de nodos y arrastrarlo al área de trabajo, repetir este procedimiento según la cantidad de routers deseados en la topología.

El segundo paso es añadir los puertos a utilizar en cada router, esto lo hacemos dando doble click sobre cada router y en la venta que se despliega (Node Configurator), verificamos el nombre del router (1), y damos click en la pestaña Slots en ella tenemos las opciones de puertos a agregar en el router, como trabajaremos con enlaces GigaEthernet y FastEthernet Seleccionaremos estas opciones:

- C7200-IO-GE-E o PA-GE para las interfaces GiEthernet.
- PA-2FE-TX para las interfaces FastEthernet.

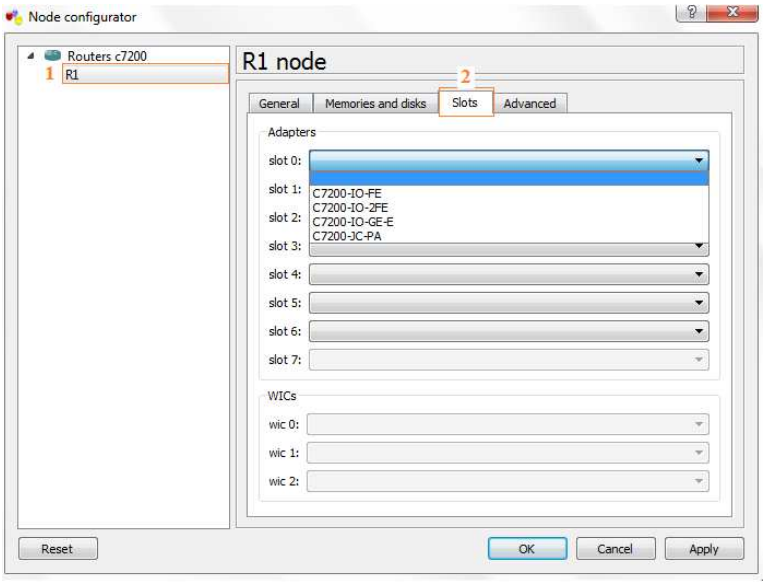

Fig. 4.5.- Ventana Node Configurator.

Fuente: Autor. Captura de pantalla software GNS3.

En los slots 1, 2 y 3. No importa el orden de los slots, pero es necesaria que esta elegida alguna opción que especifique Ge o Fa.

Este procedimiento se repite en todos los routers agregando las interfaces que necesitemos en la topología.

El tercer paso sería realizar los enlaces entre los nodos, esto se realiza dando click en el botón añadir un enlace (Add a link) de la barra del menú principal.

El mismo que está señalado en la figura 4.5.

Fig. 4.6.- Barra de Menú principal, Add a link.

Fuente: Autor. Captura de pantalla software GNS3.

Luego seleccionamos el tipo de enlace del menú que se despliega (Gigabit Eth, Fast Eth, Ethernet, Coaxial, Entre Otros), y por ultimo trazamos el enlace dando click en ambos routers a enlazar.

Y por último, y una vez que la topología física este creada completamente damos click en el botón Play (Verde en la Fig. 4.7) de la barra de herramientas con esto los routers comenzaran a correr el IOS. Luego presionamos el botón Console to all devices (Consola a todos los dispositivos) (Café en la Fig. 4.7).

Fig. 4.7. - Boton Console to all devices, y Start (Play)
Fuente: Autor. Captura de pantalla software GNS3.

Con esto comienzan a correr los IOS en todos los dispositivos y se abre una ventana de terminal para cada dispositivo conectado para en ella realizar la respectiva configuración.

Las topologías, direcciones de red y configuraciones de los equipos que se revisaran en páginas posteriores han sido implementadas por el autor de este proyecto, de manera que cumplan con el objetivo de explicar y estudiar las bases del protocolo, pero se usaron textos de referencia, sobre las cuales se realizaron consultas para el óptimo funcionamiento de la arquitectura a simular, estos tres autores fueron:

- William Parkhurst, y su libro Cisco BGP-4 Command and Configuration Handbook del año 2001 el cual es un estudio extenso sobre los comandos de configuración y forma de aplicación de los atributos BGP.

- Reagan James, y su libro Implementing Cisco MPLS del año 2002, que es un estudio a base de preguntas/respuestas sobre los temas más confusos y comunes sobre la implementación y comandos de MPLS en los IOS de Cisco.

4.4.- TOPOLOGIA #1:

RED DE TRANSPORTE MPLS/VPN BASICA.

Esta topología sirve para conocer más a fondo los pasos de configuración, los comandos y como se realiza en el router los procesos descritos teóricamente en los capítulos anteriores.

La topología a simular será la Siguiente:

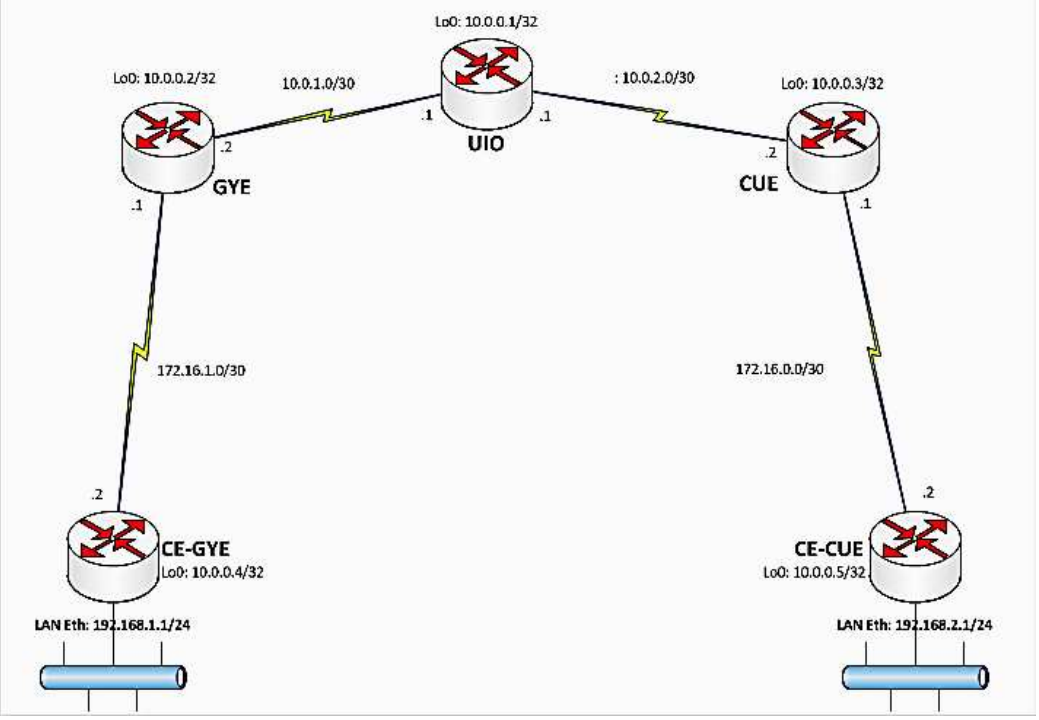

Fig. 4.8.- Topología para Simulación Básica

Fuente. Autor.

Tabla de Direcciones IP			
Router	Interfaz	Direccion IP	Mascara de red
UIO	g0/0	10.0.1.1	255.255.255.252
	g1/0	10.0.2.1	255.255.255.252
	lo0	10.0.0.1	255.255.255.255
CUE	g0/0	10.0.2.2	255.255.255.252
	fa0/0	172.16.0.1	255.255.255.252
	lo0	10.0.0.3	255.255.255.255
GYE	g0/0	10.0.1.2	255.255.255.252
	fa0/0	172.16.1.1	255.255.255.252
	lo0	10.0.0.2	255.255.255.255
CE-GYE	fa0/0	172.16.1.2	255.255.255.252
	lo1	192.168.1.1	255.255.255.255
CE-CUE	fa0/0	172.16.0.2	255.255.255.252
	lo1	192.168.2.1	255.255.255.255

Tabla.4.1.- Direccionamiento IP de Simulación #1.

Fuente: Autor.

Como Podemos observar en esta topología el router UIO está haciendo las veces de un P. Los routers GYE y CUE las veces de routers PE, y CE-GYE y CE-CUE son los routers CE que tienen a su vez conectada una LAN, como red interna para cada uno.

Entonces comenzaremos a detallar las configuraciones respectivas.
En primer lugar Configuraremos los routers CE, que son los menos complejos.

Comenzamos haciendo la topología en el el área de diseño, creando los enlaces, Una vez hecha la topología completa, y empezar a correr la simulación con el botón Play (Start) Verde, se hace click en el botón de la barra de menú: Console to All. Con lo que se abrirán las ventanas de terminal para empezar a configurar los dispositivos en la arquitectura diseñada.

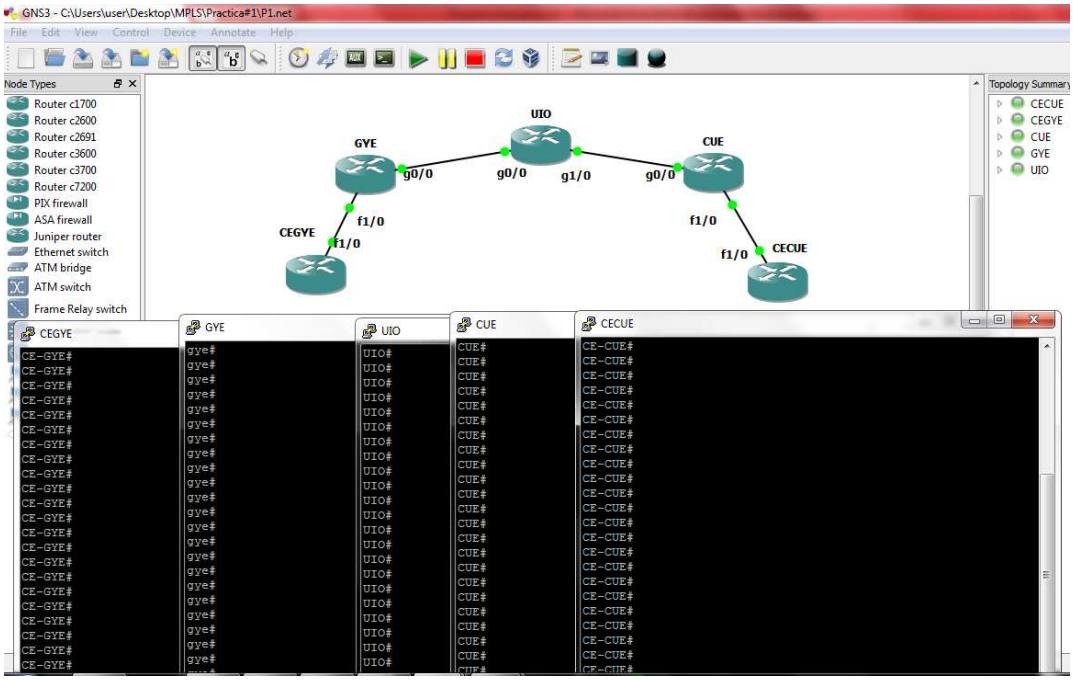

Fig. 4.9.- Simulación de Topología.

Fuente: Autor. Captura de pantalla software GNS3.

4.4.1.- CONFIGURACIONES BASICAS EN EQUIPOS

Primero detallaremos 6 pasos que se deben de configurar en todos los routers pues forman parte de la configuración básica, y se deben configurar en todas las ocasiones y todas las topologías.

1.-Habilitar el modo privilegiado con el comando enable.

ROUTER> enable

2.-Habilita el modo de configuración global

ROUTER# configure terminal

3.- Configuramos el nombre del router con el comando hostname.

Al dar enter luego de este comando el nombre del router cambiará.

ROUTER (config)# hostname CE-GYE
CE-GYE (config)#

4.-Configuramos el una clave para entrar al modo privilegiado en el router

CE-GYE (config)# enable secret cisco

Donde la clave será la palabra después de secret, en el ejemplo: cisco.

5.- Configuramos el acceso por consola en el router

CE-GYE (config)# line console 0
CE-GYE (config)# password cisco
CE-GYE (config)# login

Al habilitar este comando significa que cada vez que intentemos entrar usando un cable de consola nos pedirá una contraseña para acceder a la configuración del router, y el comando login pone en práctica la configuración.

6.- Configuramos el acceso por telnet en el router

CE-GYE (config) # line vty 0 4
CE-GYE (config) #password cisco

CE-GYE (config) # login

Al habilitar este comando queremos decir que tenemos 5 interfaces lógicas para ingresar a la configuración del dispositivo vía telnet de aquí el número 04, es decir del 0 al 4, y al habilitar la contraseña significa que cada que intentemos entrar al router por telnet nos pedirá esta contraseña para autenticación, y el comando login pone en práctica la configuración.

Estos 6 pasos descritos serán repetidos en todos los routers pues como pudimos ver es la configuración básica del dispositivo independientemente de cuantas interfaces tengan, ni su direccionamiento IP.

4.4.2.- CONFIGURACIONES DE SIMULACION

CONFIGURAMOS GYE-CE

CE-GYE (config)# interface loopback 0
CE-GYE (config-if)# ip address 10.0.0.4 255.255.255.255
CE-GYE (config-if)# no shutdown

CE-GYE (config)# interface lo1
CE-GYE (config-if)# ip address 192.168.1.1 255.255.255.0
CE-GYE (config-if)# no shutdown

CE-GYE (config)# interface fa1/0
CE-GYE (config-if)# ip address 172.16.1.2 255.255.255.252
CE-GYE (config-if)# no shutdown
CE-GYE (config)# Ip route 0.0.0.0 0.0.0.0 172.16.1.1

Podemos utilizar el comando ***show ip interface brief*** para verificar si todas las interfaces están up:

```
R1#
R1#show ip interface br
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
FastEthernet1/0            172.16.1.2      YES manual up                    up
FastEthernet1/1            unassigned      YES unset  administratively down down
FastEthernet2/0            unassigned      YES unset  administratively down down
FastEthernet3/0            unassigned      YES unset  administratively down down
FastEthernet3/1            unassigned      YES unset  administratively down down
LI-Null0                   unassigned      YES unset  up                    up
Loopback0                  10.0.0.4        YES manual up                    up
Loopback1                  192.168.1.1     YES manual up                    up
R1#
```

Fig.4.10. –Comando show ip interface brief en CE-GYE

Fuente: Autor. Captura de pantalla software GNS3.

En el caso de que en alguna de las interfaces configuradas aparezca Down debemos verificar si escribimos o no el comando no shutdown, y escribirlo para que esta levante.

Podríamos también revisar si las rutas están bien declaradas usando el comando **show ip route,** el cual mostrara las rutas y prefijos aprendidos y mediante qué proceso se aprendió, del lado izquierdo, donde la letra C: Directamente conectado; B: BGP; O: OSPF y S: Estática, como es de conocimiento básico de configuración en Cisco.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, GigabitEthernet0/0
     10.0.0.0/32 is subnetted, 1 subnets
C       10.0.0.4 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 [1/0] via 172.16.1.1
```

Fig.4.11. – Comando show ip route en CE-GYE

Fuente: Autor. Captura de pantalla software GNS3.

Como es de conocimiento básico en configuración de routers cisco estos comandos deben usarse en modo de configuración privilegiado (modo enable).

Entonces en CE-CUE y después de los 6 pasos básicos:

CE-CUE

```
CE-CUE (config) # interface loopback 0
CE-CUE (config-if) # ip address 10.0.0.5 255.255.255.255
CE-CUE (config-if) # no shutdown

CE-CUE (config) # interface lo1
CE-CUE (config-if) # ip address 192.168.2.1 255.255.255.0
CE-CUE (config-if) # no shutdown

CE-CUE (config) # interface fa1/0
CE-CUE (config-if) # ip address 172.16.0.2 255.255.255.252
CE-CUE (config-if) # no shutdown

CE-CUE (config) # Ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

Configuración en GYE

Como habíamos indicado primero realizamos los 6 pasos básicos de configuración y continuamos con los siguientes:

```
GYE (config) # interface loopback 0
GYE (config-if) # ip address 10.0.0.2 255.255.255.255
GYE (config-if) # no shutdown

GYE (config) # interface gi 0/0
GYE (config-if) # description HACIA-P
GYE (config-if) # ip address 10.0.1.2 255.255.255.252
GYE (config-if) # no shutdown
```

```
GYE (config) # interface fa 1/0
GYE (config-if) # description HACIA-CEGYE
GYE (config-if) # ip address 172.16.1.1 255.255.255.252
GYE (config-if) # no shutdown
```

Los routers en el dominio MPLS deben conocerse por medio de un IGP, que en este caso será OSPF.

```
GYE (config) # router ospf 1
GYE (config-router) # router-id 10.0.0.2
GYE (config-router) # network 10.0.0.0 0.255.255.255 area 0
```

Estamos compartiendo la dirección de loopback del router para que sea alcanzable por cualquier router en el área 0 de OSPF, y con el comando router-id estamos diciendo que el nombre de este router frente a los demás routers ejecutando OSPF será 10.0.0.2.

Luego debemos crear la vecindad BGP entre GYE y CUE, para que se compartan las rutas por medio del protocolo MP-BGP como habíamos repasado.

```
GYE (config) # router bgp 1
GYE (config-router) # neighbor 10.0.0.3 remote-as 1
GYE (config-router) # neighbor 10.0.0.3 update-source Lo0
GYE (config-router) # neighbor 10.0.0.3 next-hop self

GYE (config-router) # address-family vpnv4
GYE (config-router) # neighbor 10.0.0.3 activate
GYE (config-router) # neighbor 10.0.0.3 send-community extended
```

En BGP a diferencia de los demás protocolos de enrutamiento, hay que hacer configuraciones más específicas, por ejemplo: en OSPF hacía falta solo declarar el Comando router OSPF 1 para que el router comience a buscar vecinos mediante mensajes de Hello, y se crearan vecindades solo entre routers que corran OSPF y que estén directamente conectados, estos dispositivos responderán el mensaje de Hello y establecerán adyacencia, y cuando se establezca se añadirá el nuevo vecino a la tabla de enrutamiento, de distinta manera, en BGP el programador debe agregar manualmente cada vecino, que puede o no estar directamente conectado al router en mención, la única necesidad es que los vecinos sean alcanzables para formar una vecindad, de la misma manera los vecinos establecen un saludo TCP, y cuando se establezca la vecindad se agregara la dirección del vecino en la tabla de enrutamiento.

Al declarar neighbor 10.0.0.3 remote-as 1 decimos que declaramos el vecino 10.0.0.3 (loopbacks 0 de CUE) como vecino en el AS1 (Autonomous System), que es el mismo al que pertenecemos por eso decimos se está declarando una vecindad IBGP (Internal BGP).

El comando neighbor 10.0.0.3 update-source Lo0 nos dice que las actualizaciones que el vecino reciba de parte nuestra se verán como si su fuente fuera la IP configurada en la interfaz lo 0.

El comando neighbor 10.0.0.3 next-hop self nos dice que todas las actualizaciones que recibamos del vecino, tendrán como siguiente salto el router que estamos configurando.

Los otros tres comandos como sus nombres los presentan sirven para crear un address family que es un grupo de vecinos y direcciones IP que compartirán datos con los mismos parámetros de forwarding, para activar el vecino dentro de esta address family y para habilitar el atributo de

comunidad extendida que sirve para acarrear el RT, como se revisó en el capítulo anterior.

Entonces una vez establecidas las adyacencias podemos declarar la VFR para este cliente en el Router de Borde.

```
GYE (config) # ip vrf CEA
GYE (config) # rd 65535:100
GYE (config) # route-target both 65535:100
GYE (config) # exit
```

Con este comando declaramos la VRF que es una tabla de enrutamiento virtual, que servirá para separar la información de los diferentes clientes conectados a este router.

El RD es el route Distinguisher, recordando, es el que nos permite la sobre posición de algunas direcciones IP mientras viajan por el dominio MP-BGP, diferenciándolas con un numero de 64 bits que se añadirá a la dirección IP para formar una dirección de 96 bits.
Y el route target, es que nos permite el forwarding de los datos y los distingue asociándose con una interfaz. En el ejemplo cuando decimos both significa ambos es decir para importar información tanto como para exportar por medio de esta VRF los datos deberán tener el RT 1:65535, de otra manera los paquetes se descartaran.

Asociamos el VRF a una interfaz que en este caso debería ser la que nos conecte con el cliente en mención.

```
GYE (config) # interface g1/0
GYE (config-if) # ip vrf forwarding CEA
```

Y declaramos una ruta para toda la información dirigida a la LAN del cliente en GYE por medio de la VRF CEA y enviándola hacia la interfaz del router GYE.

GYE (config) # Ip route vrf CEA 192.168.1.0 255.255.255.0 172.16.1.2

Luego debemos declarar un address-family dentro de este router para la VRF y las actualizaciones que vengan de ella o de las interfaces asociadas a la VRF. Con el comando redistribute-static, compartimos las rutas estáticas obtenidas del VRF para que sean conocidas por los demás miembros de la comunidad MP-BGP que contengan configurada esta VRF.

GYE (config) # router bgp 1
GYE (config) # address-family ipv4 vrf CEA
GYE (config) # redistribute static
GYE (config) # redistribute connected
GYE (config) # end

Al finalizar estas configuraciones haremos la declaración de MPLS:
Comenzamos activando el Cisco Express Forwarding.

GYE (config)# ip cef

Declaramos MPLS

GYE (config) # mpls ip
GYE (config) # mpls cef

Declaramos el protocolo a usar para etiquetas.

GYE (config) # mpls ldp label protocol ldp

Declaramos el nombre de este router en el dominio MPLS.

GYE (config) #mpls ldp router-id lo0

Y declaramos MPLS también en la interfaz que tiene conexión directa con otros routers que también funcionen con MPLS, que en este caso será solo el P.

GYE (config) # interface g0/0
GYE (config-if) # mpls ip
GYE (config-if) # end

Configuración en CUE

Esta configuración es muy parecida a la GYE.

CUE (config) # interface loopback 0
CUE (config-if) # ip address 10.0.0.3 255.255.255.255
CUE (config-if) # no shutdown

CUE (config) # interface gi 0/0
CUE (config-if) # description HACIA-P
CUE (config-if) # ip address 10.0.2.2 255.255.255.252
CUE (config-if) # no shutdown

CUE (config) # interface fa 1/0
CUE (config-if) # description HACIA-CECUE
CUE (config-if) # ip address 172.16.0.1 255.255.255.252
CUE (config-if) # no shutdown

CUE (config) # router ospf 1
CUE (config-router) # router-id 10.0.0.3
CUE (config-router) # network 10.0.0.0 0.255.255.255 area 0

```
CUE (config) # router bgp 1
CUE (config-router) #neighbor 10.0.0.2 remote-as 1
CUE (config-router) #neighbor 10.0.0.2 update-source Lo0
CUE (config-router) # neighbor 10.0.0.2 next-hop self

CUE (config-router) # address-family vpnv4
CUE (config-router) #neighbor 10.0.0.2 activate
CUE (config-router) #neighbor 10.0.0.2 send-community extended

CUE (config) # ip vrf CEA
CUE (config) # rd 65535:100
CUE (config) # route-target both 65535:100
CUE (config) #exit

CUE (config) # interface g1/0
CUE (config-if) # ip vrf forwarding CEA
CUE (config) #Ip route vrf CEA 192.168.2.0 255.255.255.0 172.16.0.2

CUE (config) # router bgp 1
CUE (config) # address-family ipv4 vrf CEA
CUE (config) # redistribute static
CUE (config) # redistribute connected
CUE (config) # end

CUE (config) # ip cef
CUE (config) # mpls ip
CUE (config)# mpls cef
CUE (config) # mpls ldp label protocol ldp
CUE (config) # mpls ldp router-id lo0

CUE (config) # interface g0/0
CUE (config-if) # mpls ip
CUE (config-if) # end
```

Configuración en UIO

UIO (config) # interface loopback 0
UIO (config-if) # ip address 10.0.0.1 255.255.255.255
UIO (config-if) # no shutdown

UIO (config) # interface gi 0/0
UIO (config-if) # description HACIA-GYE
UIO (config-if) # ip address 10.0.1.1 255.255.255.252
UIO (config-if) # mpls ip
UIO (config-if) # no shutdown

UIO (config) # interface gi 1/0
UIO (config-if) # description HACIA-CUE
UIO (config-if) # ip address 10.0.2.1 255.255.255.252
UIO (config-if) # mpls ip
UIO (config-if) # no shutdown

UIO (config) # router ospf 1
UIO (config-router) #network 10.0.0.0 0.255.255.255 area 0
UIO (config-router) # exit

UIO (config) # ip cef
UIO (config) # mpls cef
UIO (config) # mpls label protocol ldp
UIO (config) # mpls ldp router-id lo0

4.4.3.- COMANDOS DE VERIFICACION.

Una vez terminadas las configuraciones podemos hacer la verificación del transporte de datos sobre MPLS hacienda un ping desde el router GYE-CEA hacia la red interna del router CE-CUE con el comando.

CE-GYE #ping 192.168.2.1

```
CE-GYE#
CE-GYE#PING 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1456/1548/1676 ms
CE-GYE#
```

Fig. 4.12.- Verificación con ping.

Fuente: Autor. Captura de pantalla software GNS3.

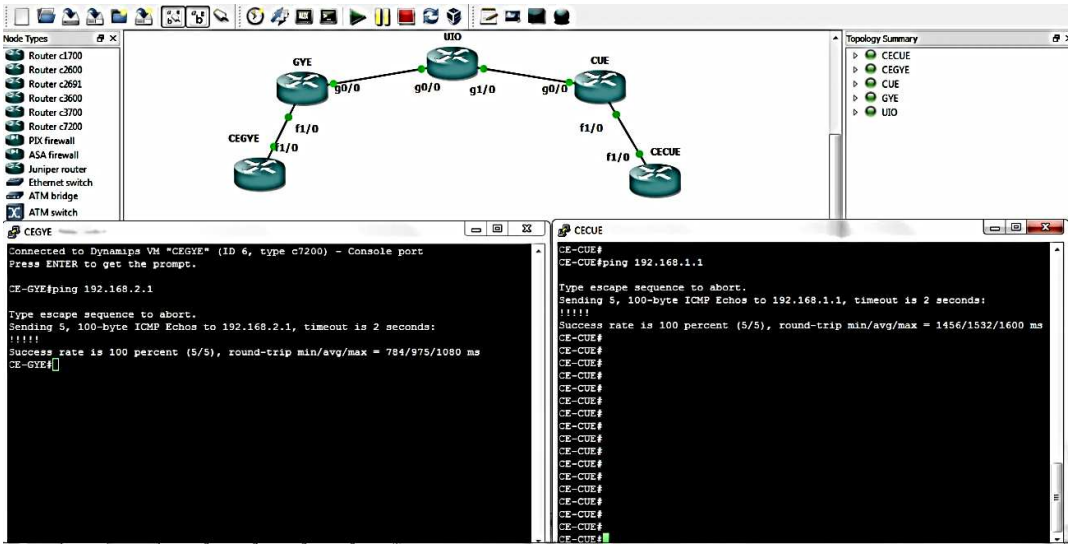

Fig. 4.13.- Verificación con ping entre las LAN de ambos puntos.

Fuente: Autor. Captura de pantalla software GNS3.

En caso de que no responda positivamente el problema puede estar en la configuración de las VRF, o quizás las interfaces involucradas pueden estar Down.

Otro caso puede ser que se quiera comprobar el forwarding de la vrf entre uno de los PE con su respectivo CE, para esto entonces se debe usar el siguiente comando.

CUE# ping vrf CEA172.16.0.2

```
*Jul 19 14:11:27.203: %SYS-5-CONFIG_I: Configured from console by console
CUE#PING VRF CEA 172.16.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/460/844 ms
CUE#
```

Fig. 4.14.- Verificación de ping con vrf.

Fuente: Autor. Captura de pantalla software GNS3.

En cada PE habrán varias VRF en la práctica, y, cada VRF es una tabla de enrutamiento diferente, por ello al hacer ping desde el PE se debe hacer referencia a que VRF se está llamando, para poder hacer el correcto forwarding.

Además de estas verificaciones se utilizan otros comandos que ayudaran mucho cuando sea necesario realizar Troubleshooting.
Entre ellos tenemos:

GYE# show ip bgp vpnv4 all summary

```
gye#
gye#show ip bgp vpnv4 all sum
gye#show ip bgp vpnv4 all summary
BGP router identifier 10.0.0.2, local AS number 1
BGP table version is 9, main routing table version 9
4 network entries using 548 bytes of memory
4 path entries using 272 bytes of memory
5/2 BGP path/bestpath attribute entries using 620 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1464 total bytes of memory
BGP activity 8/0 prefixes, 8/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.3        4     1      26      25        9    0    0 00:18:53        2
gye#
```

Fig. 4.15. - Verificación con show ip vpnv4 all summary.

Fuente: Autor. Captura de pantalla software GNS3.

Como observamos este comando muestra los vecinos BGP en el address-family.

Podemos también revisar la tabla de enrutamiento VRF con el comando:

GYE# show ip route vrf CEA

Este comando solo mostrara la tabla en CEA.

```
gye#SHOW ip route vrf
gye#SHOW ip route vrf CEA

Routing Table: CEA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
B       172.16.0.0 [200/0] via 10.0.0.3, 00:22:12
C       172.16.1.0 is directly connected, FastEthernet1/0
S    192.168.1.0/24 [1/0] via 172.16.1.2
B    192.168.2.0/24 [200/0] via 10.0.0.3, 00:22:12
gye#
```

Fig. 4.16. - Verificación con show ip route vrf.

Fuente: Autor. Captura de pantalla software GNS3.

Y por último podemos verificar la conectividad VPN de una última manera haciendo ping con source.

```
CE-GYE#
CE-GYE#PING 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1456/1548/1676 ms
CE-GYE#ping 192.168.2.1 source 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 604/820/988 ms
CE-GYE#
```

Fig. 4.17. - Verificación con ping con Source.

Fuente: Autor. Captura de pantalla software GNS3.

Podemos también comprobar la conectividad y el funcionamiento MPLS mediante los siguientes comandos:

En estos ejemplo se usa el router UIO, puesto que es el único que tiene 2 interfaces con MPLS forwarding.

UIO# Show mpls interfaces

```
UIO#SH MPLS
UIO#SH MPLS INTER
Interface              IP            Tunnel   Operational
GigabitEthernet0/0     Yes (ldp)     No       Yes
GigabitEthernet1/0     Yes (ldp)     No       Yes
UIO#SHOW MPLS FO
UIO#SHOW MPLS FOrwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     10.0.0.3/32      6749       Gi1/0      10.0.2.2
17     Pop tag     10.0.0.2/32      5761       Gi0/0      10.0.1.2
```

Fig. 4.18. –Verificación de Show MPLS Interfaces.

Fuente: Autor. Captura de pantalla software GNS3.

Al usar el comando show mpls interfaces, el los nos muestra un resumen de las interfaces en las que se ha configurado el MPLS forwarding con el comando Mpls ip, y nos muestra las etiquetas asignadas a ellos.

UIO# Show mpls ldp discovery

```
UIO#SHOW MPLS LDP disc
 Local LDP Identifier:
    10.0.1.1:0
    Discovery Sources:
    Interfaces:
        GigabitEthernet0/0 (ldp): xmit/recv
            LDP Id: 10.0.0.2:0
        GigabitEthernet1/0 (ldp): xmit/recv
            LDP Id: 10.0.0.3:0
```

Fig. 4.19. - Verificación con Show Mpls Ldp Discovery.
Fuente: Autor. Captura de pantalla software GNS3.

Con el comando show mpls discovery nos muestra las interfaces mpls a travezs de las cuales ha descubierto vecinos MPLS y sus respectivos router-id.

UIO# Show mpls ldp bindings

```
UIO#SHOW MPLS LDP BINDINGS
  tib entry: 10.0.0.1/32, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 10.0.0.3:0, tag: 19
        remote binding: tsr: 10.0.0.2:0, tag: 19
  tib entry: 10.0.0.2/32, rev 10
        local binding:  tag: 17
        remote binding: tsr: 10.0.0.3:0, tag: 20
        remote binding: tsr: 10.0.0.2:0, tag: imp-null
  tib entry: 10.0.0.3/32, rev 8
        local binding:  tag: 16
        remote binding: tsr: 10.0.0.3:0, tag: imp-null
        remote binding: tsr: 10.0.0.2:0, tag: 20
  tib entry: 10.0.1.0/30, rev 2
        local binding:  tag: imp-null
        remote binding: tsr: 10.0.0.3:0, tag: 18
        remote binding: tsr: 10.0.0.2:0, tag: imp-null
  tib entry: 10.0.2.0/30, rev 4
        local binding:  tag: imp-null
        remote binding: tsr: 10.0.0.3:0, tag: imp-null
        remote binding: tsr: 10.0.0.2:0, tag: 18
```

Fig. 4.20. - Verificación con Show MPLS LDP Bindings.
Fuente: Autor. Captura de pantalla software GNS3.

Y con el comando show mpls bindings, nos muestra las sesiones o enlaces mpls y sus entradas en la tabla de etiquetas.

4.4.4.- RESUMEN DE PROCESOS EN LA RED MPLS/VPN BASICA.

Entonces, revisando una vez mas la topologia dice la simulacion:

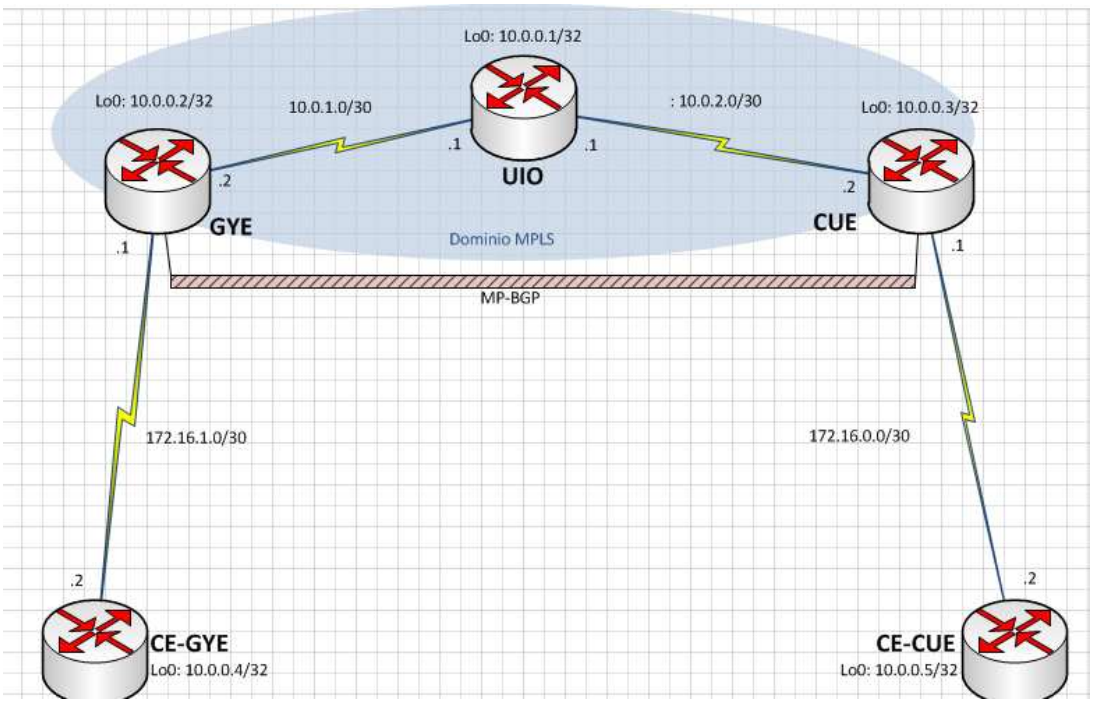

Fig. 4.21. – Rango de acción de MP-BGP.

Fuente: Autor.

En este grafico podemos ver la vecindad BGP formada entre GYE y CUE, y ver el dominio MPLS en el que se corre OSPF, para establecer convergencia y los routers que lo conforman.

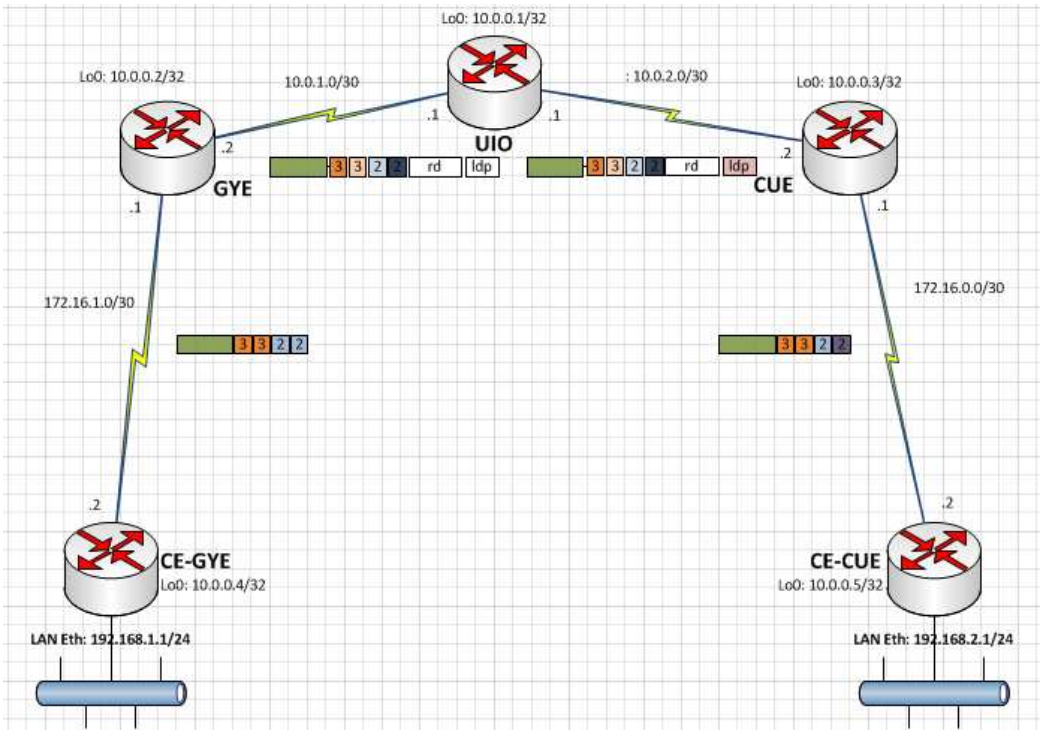

Fig. 4.22. – Funcionamiento completo de la topología #1

Fuente: Autor.

Entonces, la topología anteriormente mencionada funciono de la siguiente manera:

1.-Se hizo una petición de ping desde la LAN 192.168.1.0/24 en GYE hacia la LAN 192.168.2.0 /24 en CUE.

2.-CE- GYE consulta en su tabla de enrutamiento y tiene una ruta por defecto que envía este paquete hacia a 172.16.1.1/30 en GYE.

3.-GYE analiza el paquete y verifica que viene de la interfaz asociada a la VRF CEA, consulta su dirección de destino en la tabla VRF CEA, donde encuentra una ruta que concuerda (esta ruta fue aprendida en la address family gracias a los comandos redistribute-static y redistribute connected aplicados en los dos extremos de la VRF, GYE y CUE, los mismos que

gracias a estos comandos compartieron sus rutas estáticas y las direcciones de los dispositivos conectados directamente, para ser visibles por todos los miembros de la Address-Family)entonces, en los datos de la tabla VRF comprueba que el paquete va hacia una red (la LAN de CE-CUE) que se alcanzara mediante su vecino BGP, que es el router CUE, como los routers no están directamente conectados tendrá que usar los vecinos MPLS para poder alcanzarlo.

El uso de MPLS para alcanzar el vecino BGP, es decir el uso de ambos protocolos trabajando juntos forman el protocolo MP-BGP.

4.- En base a esta información se coloca una etiqueta y se reenvía el paquete hacia UIO, que es el próximo salto MPLS.

5.-En UIO, el router verifica la etiqueta, la compara con los datos en su LIB, verifica que el destino es CUE, y reenvía el paquete por la interfaz correspondiente.

6.- Una vez que el paquete ha llegado a CUE, este retira la etiqueta como resultado del proceso Penultimate Hop-Popping, verifica el RD, lo asocia a una VRF que encuentra en su configuración, la misma que en este ejemplo es CEA, compara los Route targets verifica que son iguales tanto en el paquete como en la VRF asociada y una vez comprobado, la reenvía por la interfaz asociada a esta VRF.

7.- El paquete llega a CE-CUE, donde se abre el paquete se revisa la dirección IP en el mismo, se reenvía por la interfaz adecuada, y llega al destino.

8.-Como esta es una solicitud de ping, entonces el host requerido produce el eco, que es esta vez tiene dirección destino 192.168.1.1/24 que es de donde salió en un principio el ping.

El router Ce-CUE, revisa en su tabla de enrutamiento, en ella tiene una ruta por defecto en donde todo paquete que contenga una red que no esté declarada será enviada a 172.16.0.2/30, el resultado de este proceso es que se reenvía el paquete llega a CUE, y el proceso se repite con el camino inverso hasta que llega a CE-GYE y con él a su destino.

4.5.- TOPOLOGIA #2:

RED DE TRANSPORTE MPLS/VPN: VRF, RT Y RD

En la Siguiente topología se usa la red de transporte de datos MPLS pero con 2 Routers conectados al PE de manera que tendremos una visión más real de cómo se utilizan las VRF en los routers de borde para realizar el forwarding.

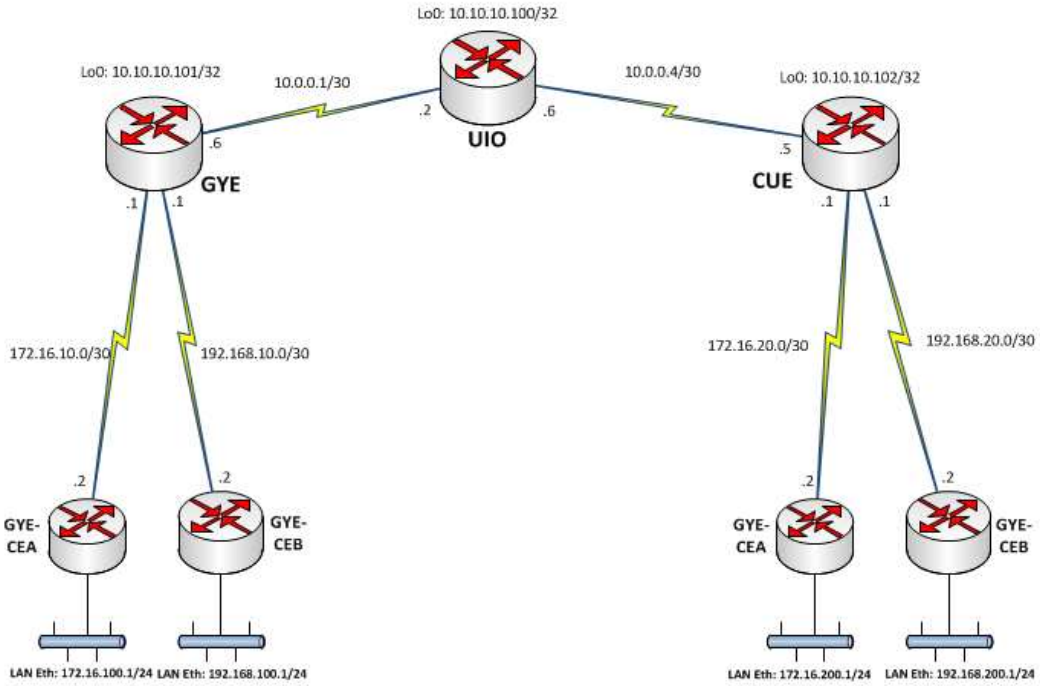

Fig. 4.23. – Topología #2.

Fuente: Autor.

Como podemos observar el tenemos 2 clientes que se conectan a nuestra Red MPLS y ambos tienen oficinas en GYE y en CUE, vamos a crear un enlaces para que sus oficinas puedan comunicarse.

En el simulador esta topología esta vista de esta manera:

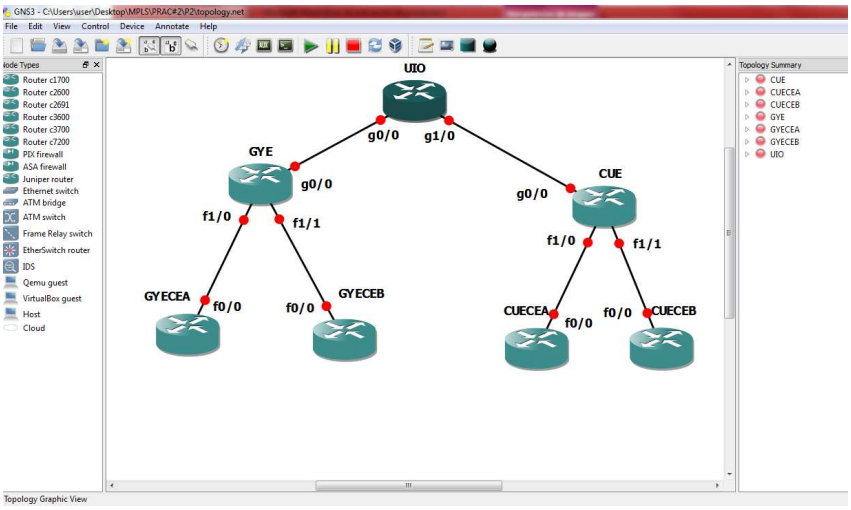

Fig. 4.24. – Topología #2 en GNS3.

Fuente: Autor. Captura de pantalla software GNS3.

Tabla de Direcciones IP			
Router	**Interfaz**	**Direccion IP**	**Mascara de red**
UIO	g0/0	10.0.0.2	255.255.225.252
	g1/0	10.0.0.6	255.255.225.252
	lo0	10.10.10.100	255.255.255.255
GYE	g0/0	10.10.10.1	255.255.225.252
	f1/0	172.16.10.1	255.255.225.252
	f1/1	192.168.10.1	255.255.225.252
	lo0	10.10.10.101	255.255.255.255
CUE	g0/0	10.0.0.5	255.255.225.252
	f1/0	172.16.20.1	255.255.225.252
	f1/1	192.168.20.1	255.255.225.252
	lo0	10.10.10.102	255.255.255.255
GYECEA	f0/0	172.16.10.2	255.255.225.252
	lo1	172.16.100.1	255.255.255.0
GYECEB	f0/0	192.168.10.2	255.255.255.252
	lo1	192.168.100.1	255.255.255.0
CUECEA	f0/0	172.16.20.2	255.255.255.252
	lo1	172.16.200.1	255.255.255.0
CUECEB	f0/0	192.168.20.2	255.255.255.252
	lo1	192.168.200.2	255.255.255.0

Tabla.4.2.- Direccionamiento IP de Simulación #2

Fuente: Autor.

4.5.1.- CONFIGURACION DE EQUIPOS.

Se detallan las líneas de configuración para compararlas con la topología 1 en ellas podemos ver la diferencia de estas dos configuraciones, que es básicamente el aumento de 1 VRF más.

En GYE-CEA

```
GYE-CEA (config)# interface fa0/0
GYE-CEA (config-if)# ip address 172.16.10.2 255.255.255.252
GYE-CEA (config-if)# no shutdown
GYE-CEA (config-if)# interface lo 1
GYE-CEA (config-if)#ip address 172.16.100.1 255.255.255.0
GYE-CEA (config)# ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

En GYE-CEB

```
GYE-CEA (config)# interface fa0/0
GYE-CEA (config-if)# ip address 192.168.10.2 255.255.255.252
GYE-CEA (config-if)# no shutdown
GYE-CEA (config-if)# interface lo 1
GYE-CEA (config-if)# ip address 192.168.100.1 255.255.255.0
GYE-CEA (config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

En CUE-CEA

```
CUE-CEA (config)# interface f0/0
CUE-CEA (config-if)# ip address 172.16.20.2 255.255.255.252
CUE-CEA (config-if)# no shutdown
CUE-CEA (config-if)# interface lo 1
CUE-CEA (config-if)# ip address 172.16.200.1 255.255.255.0
CUE-CEA (config-if)#exit
CUE-CEA (config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1
```

En CUE-CEB

```
CUE-CEA (config)# interface f0/0
CUE-CEA (config-if)# ip address 192.168.20.2 255.255.255.252
CUE-CEA (config-if)# no shutdown
CUE-CEA (config-if)# interface lo 1
CUE-CEA (config-if)# ip address 192.168.200.1 255.255.255.0
CUE-CEA (config-if)#exit
CUE-CEA (config)#ip route 0.0.0.0 0.0.0.0 192.168.20.1
```

En GYE

```
GYE (config)# ip cef
GYE (config)# mpls ip
GYE (config)# mpls label protocol ldp
GYE (config)# mpls ldp router-id lo 0

GYE (config)# interface g0/0
GYE (config-if)# ip address 10.0.0.1 255.255.255.252
GYE (config-if)# mpls ip
GYE (config-if)# no shutdown

GYE (config-if)# interface lo 0
GYE (config-if)# ip address 10.10.10.101 255.255.255.255

GYE (config)# router ospf 1
GYE (config-router)# router-id 10.10.10.101
GYE (config-router)# network 10.0.0.0 0.255.255.255 area 0
```

Configuramos las VRFs en con sus RD y RT

Como tenemos los VPNs pues entonces configuraremos 2 VRFs en los PEs.

```
GYE (config)# ip vrf CEA
GYE (config)# RD 1:100
GYE (config)# route-target both 1:100

GYE (config)# ip vrf CEB
GYE (config)# RD 2:200
GYE (config)# route-target both 2:200
```

Asignamos cada VRF a la interfaz que nos brinda conectividad con la VPN deseada, en ambas VPN, y en los 2 PEs.

```
GYE (config)# interface f1/0
GYE (config-if)# ip vrf forwarding CEA
GYE (config-if)# ip address 172.16.10.1 255.255.255.252
GYE (config-if)# mpls ip
GYE (config-if)# no shutdown

GYE (config)# interface f1/1
GYE (config-if)#ip vrf forwarding CEB
GYE (config-if)# ip address 192.168.10.1 255.255.255.252
GYE (config-if)# mpls ip
GYE (config-if)# no shutdown

GYE (config-router)# router bgp 1
```

```
GYE (config-router)# neighbor 10.10.10.102 remote-as 1
GYE (config-router)# neighbor 10.10.10.102 update-source lo0
GYE (config-router)# neighbor 10.10.10.102 next-hop self

GYE (config-router)# address-family vpnv4
GYE (config-router)# neighbor 10.10.10.102 activate
GYE (config-router)# neighbor 10.10.10.102 send-community extended

GYE (config-router)# address-family ipv4 vrf CEA
GYE (config-add)# redistribute static
GYE (config-add)#  redistribute connected

GYE (config-router)# address-family ipv4 vrf CEB
GYE (config-add)# redistribute static
GYE (config-add)#  redistribute connected
```

Configuramos las rutas estáticas para cada LAN de cada VPN en los PEs.

```
GYE (config)#  ip route vrf CEA 172.16.100.0 255.255.255.0 172.16.10.1

GYE (config)#  ip route vrf CEB 192.168.100.0 255.255.255.0 192.168.10.1
```

En CUE

```
CUE (config)# ip cef
CUE (config)# mpls ip
CUE (config)# mpls label protocol ldp
CUE (config)# mpls ldp router-id lo 0

CUE (config)# interface g0/0
CUE (config-if)# ip address 10.0.0.5 255.255.255.252
CUE (config-if)# mpls ip
CUE (config-if)# no shut

CUE (config-if)# interface lo 0
CUE (config-if)# ip address 10.10.10.102 255.255.255.255

CUE (config)# router ospf 1
CUE (config-router)# router-id 10.10.10.102
CUE (config-router)# network 10.0.0.0 0.255.255.255 area 0
```

Configuramos las VRFs en con sus RD y RT

Como tenemos los VPNs pues entonces configuraremos 2 VRFs en los PEs.

```
CUE (config)# ip vrf CEA
CUE (config)# RD 1:100
```

```
CUE (config)# route-target both 1:100

CUE (config)# ip vrf CEB
CUE (config)# RD 2:200
CUE (config)# route-target both 2:200
```

Asignamos cada VRF a la interfaz que nos brinda conectividad con la VPN deseada, en ambas VPN, y en los 2 PEs.

```
CUE (config)# interface f1/0
CUE (config-if)# ip vrf forwarding CEA
CUE (config-if)# ip address 172.16.20.1 255.255.255.252
CUE (config-if)# mpls ip
CUE (config-if)# no shut

CUE (config)# interface f1/1
CUE (config-if)#ip vrf forwarding CEB
CUE (config-if)# ip address 192.168.20.1 255.255.255.252
CUE (config-if)# mpls ip
CUE (config-if)# no shut

CUE (config-router)# router bgp 1
CUE (config-router)# neighbor 10.10.10.101 remote-as 1
CUE (config-router)# neighbor 10.10.10.101 update-source lo0
CUE (config-router)# neighbor 10.10.10.101 next-hop self

CUE (config-router)# address-family vpnv4
CUE (config-router)# neighbor 10.10.10.101 activate
CUE (config-router)# neighbor 10.10.10.101 send-community extended

CUE (config-router)# address-family ipv4 vrf CEA
CUE (config-add)# redistribute static
CUE (config-add)#  redistribute connected

CUE (config-router)# address-family ipv4 vrf CEB
CUE (config-add)# redistribute static
CUE (config-add)#  redistribute connected
```

Configuramos las rutas estáticas para cada LAN de cada VPN en los PEs.

```
CUE (config)#  ip route vrf CEA 172.16.200.0 255.255.255.0 172.16.20.1

CUE (config)#  ip route vrf CEB 192.168.200.0 255.255.255.0 192.168.20.1
```

En UIO

```
UIO (config)# ip cef
UIO (config)# mpls cef
UIO (config)# mpls label protocol ldp
UIO (config)# mpls ldp router-id lo0

UIO (config)# interface loopback 0
UIO (config-if)# ip address 10.10.10.100 255.255.255.255
UIO (config-if)# no shutdown

UIO (config)# interface gi 0/0
UIO (config-if)# description HACIA-GYE
UIO (config-if)# ip address 10.0.0.2 255.255.255.252
UIO (config-if)# mpls ip
UIO (config-if)# no shutdown

UIO (config)# interface gi 1/0
UIO (config-if)# description HACIA-CUE
UIO (config-if)# ip address 10.0.0.6 255.255.255.252
UIO (config-if)# mpls ip
UIO (config-if)# no shutdown

UIO (config)# router ospf 1
UIO (config-router)# network 10.0.0.0 0.255.255.255 area 0
UIO (config-router)# exit
```

Hacemos la verificación de la conectividad entre los PE y sus respectivos CEs con un ping con VRF.

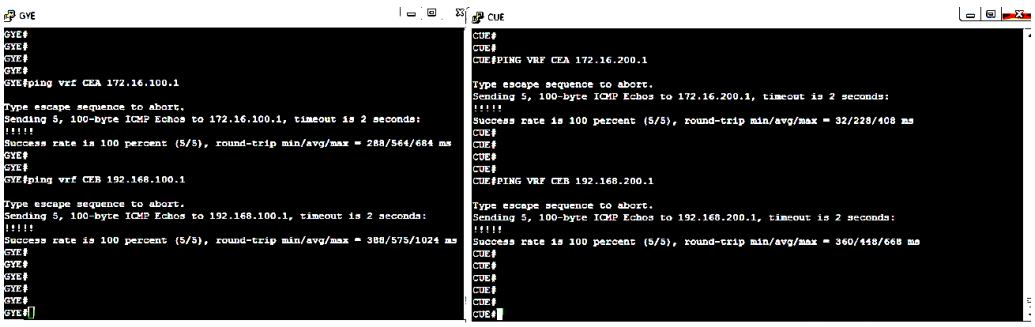

Fig. 4.25. – Ping VRF de verificación - Topología #2.

Fuente: Autor. Captura de pantalla software GNS3.

La última y definitiva prueba para saber si la Red MPLS está funcionando es siempre con un ping desde las LAN de un local hacia la otra Lan en el local del mismo cliente para probar conectividad VPN.

GVECEA

```
GYE-CEA#
GYE-CEA#
GYE-CEA#ping  172.16.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 948/1329/1788 ms
GYE-CEA#
GYE-CEA#
GYE-CEA#
GYE-CEA#
GYE-CEA#ping  192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
GYE-CEA#
GYE-CEA#
GYE-CEA#
```

GVECEB

```
GYE-CEB#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1432/1520/1796 ms
GYE-CEB#
GYE-CEB#
GYE-CEB#
GYE-CEB#
GYE-CEB#
GYE-CEB#ping 172.16.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.200.1, timeout is 2 seconds:
U.UU.
Success rate is 0 percent (0/5)
GYE-CEB#
GYE-CEB#
```

Fig. 4.26. – Ping de verificación - Topología #2.

Fuente: Autor. Captura de pantalla software GNS3.

En la figura se constata que los mensajes ping llegan de un extremo a otro de la VPN, pero si hacemos ping entre VPNs diferentes, el ping nunca llegara. De esta manera se verifica que la información de las VPNs independientes está totalmente separada.

Con esta topología se puede comprobar que cada cliente tiene su VRF, y cada VRF está asignada a la interfaz que brinda conectividad con el cliente, en ambos extremos, es esto lo que brinda el aislamiento entre diferentes VPNs ,de manera que las actualizaciones y la información de sus redes privadas no se mezclen en el medio común (dominio MPLS).

4.6.- TOPOLOGIA #3: RED DE TRANSPORTE MPLS/VPN: RR, PEERS GROUPS.

4.6.1.- REFELCTORES DE RUTAS / ROUTE REFLECTORS.

Los route reflectors son una técnica que surgió, como solución al inconveniente que se tiene por la regla número uno de iBGP, la cual dictaba lo siguiente:

"Las rutas aprendidas desde un vecino iBGP no puede ser reenviada a otro vecino iBGP.

Esto es un gran inconveniente puesto que en base a esta regla el número de routers BGP en el dominio MPLS del Proveedor quedara limitado a un número pequeño de no más de 2 routers BGP, o en su defecto, si tuviéramos muchos enrutadores en el dominio, la convergencia de la red se verá imposibilitada, ya que las rutas no serían distribuidas a todos los nodos; sería necesario, en este caso, que todos los routers estuvieran interconectados entre sí, en una topología full mesh, para que todos pudieran enviar sus actualizaciones a sus vecinos y así obtener convergencia en la red.

Esto significaría la necesidad de tener equipos con una gran cantidad de interfaces, las cuales estarían en su gran mayoría ocupadas, eso además de un gran desperdicio de recursos, tanto de ancho de banda, como en los enlaces para las conexiones, el procesamiento en los dispositivos, y la congestión en la red por las actualizaciones BGP.

Ashish Shirkar (2013), define los RR, de una manera más concisa:

> Un Route Reflector es un router al que le está permitido romper la regla 1, es decir, son routers designados que pueden advertir rutas recibidas desde un vecino iBGP hacia otros vecinos iBGP bajo condiciones específicas.

El uso de Route Reflectors en BGP está contenido en la RFC 4456 de Rosen, Callon y Viswanathan (2001):

Cuando se añaden RR, los PEs solo requerirán definir como vecino a cada RR, cualquier actualización será enviada hacia el RR. Estos serán los responsables de propagar la información recibida de un PE hacia los demás PEs. Cada vez que un PE es agregado a la topología, debe ser añadido como vecino al RR, para habilitar las actualizaciones de entrada y salida.

Para hacer más factible el uso de RR en redes de muchos dispositivos es necesario dividir el dominio BGP en clúster, y asignar ciertos routers a cada clúster, de esta manera los dividimos en grupos y cada clúster (grupo) tendrá su RR encargado.

Esto lo podemos hacer asociando los routers BGP a un BGP peer group y los peer group a su RR respectivo, según la designación del administrador de red.

4.6.2.- GRUPOS DE IGUALES / PEER GROUPS

Es un conjunto de routers BGP que tienen las mismas políticas para sus actualizaciones de salida. En lugar de configurar las políticas en cada router individualmente, BGP Peer Groups le permite al administrador asignar las políticas que se van a aplicar a los routers a un peer group y luego solo agregar el router al Peer Group respectivo. Usar BGP Peers Groups, reduce la cantidad de procesamiento requerida en el router, usándolo para permitir a la tabla de enrutamiento ser revisada una sola vez y las actualizaciones ser transmitidas a todos los miembros del peer group en vez de hacerlo uno por uno, además que simplifica la configuración y se asocia al uso de route reflectors. (Amit Rai, 2010).

4.6.3.- TOPOLOGIA DE RED MPLS/VPN CON RR Y PEER GROUPS

En la siguiente topología se estudia la configuración del funcionamiento de los Route Reflectors.

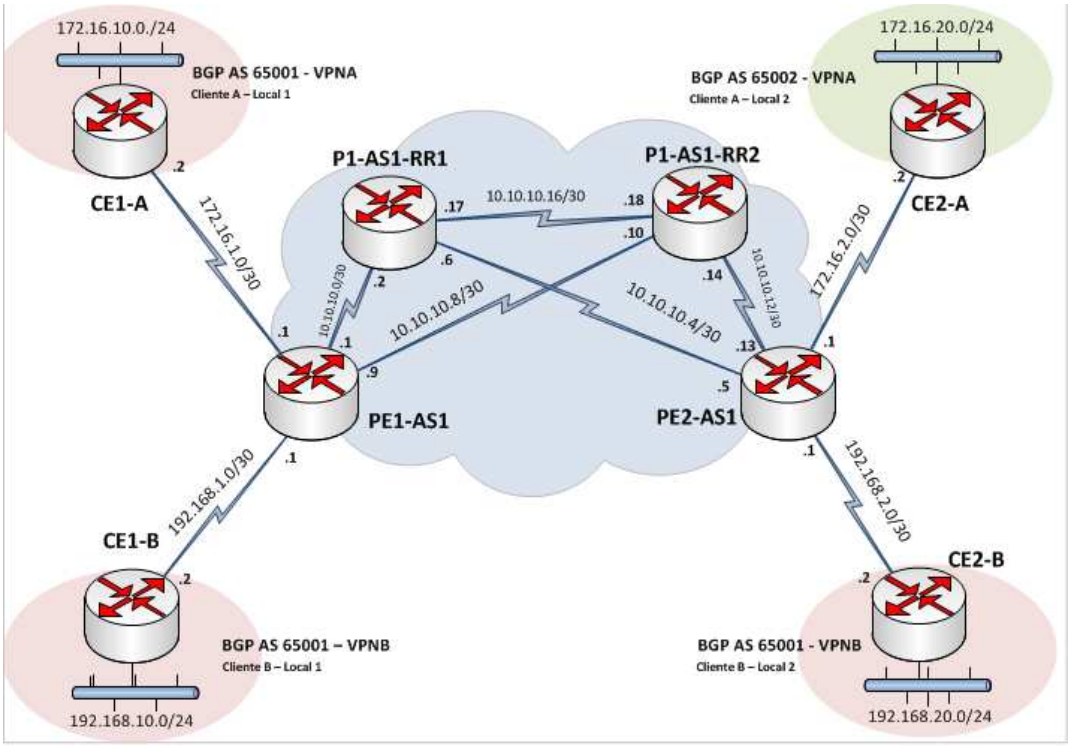

Fig. 4.27. – Topología # 3 – Route Reflectors.

Fuente: Autor.

En la topología en mención podemos comprobar que los route reflectors son enrutadores que están conectados contra todos los demás routers en el dominio BGP, esto se realiza con la finalidad de que todos comuniquen sus rutas a estos equipos centrales y ellos serán el que las compartirá a su vez a los demás vecinos iBGP, rompiendo así, la prohibición establecida en la primera regla.

En esta práctica se configuran 2 RR, es decir, estamos haciendo una partición del dominio MPLS en dos clústeres, manejado cada uno por su RR, en uno de ellos manejaremos la VPNA y en el otro la VPNB.

Tabla de Direcciones IP			
Router	**Interfaz**	**Direccion IP**	**Mascara de red**
P1-AS1-RR1	g0/0	10.10.10.17	255.255.225.252
	g1/0	10.10.10.2	255.255.225.252
	g2/0	10.10.10.6	255.255.225.252
	lo0	10.10.10.100	255.255.255.255
P2-AS1-RR2	g0/0	10.10.10.18	255.255.225.252
	g1/0	10.10.10.14	255.255.225.252
	g2/0	10.10.10.10	255.255.225.252
	lo0	10.10.10.103	255.255.255.255
PE1-AS1	g0/0	10.10.10.1	255.255.225.252
	g1/0	10.10.10.9	255.255.225.252
	f2/0	172.16.1.1	255.255.225.252
	f2/1	192.168.1.1	255.255.225.252
	lo0	10.10.10.101	255.255.255.255
PE2-AS1	g0/0	10.10.10.13	255.255.225.252
	g1/0	10.10.10.5	255.255.225.252
	f2/0	192.168.2.1	255.255.225.252
	f2/1	172.16.2.1	255.255.225.252
	lo0	10.10.10.102	255.255.255.255
CE1-A	f0/0	172.16.0.2	255.255.255.252
	lo1	172.16.10.1	255.255.255.0
CE1-B	f0/0	192.168.1.2	255.255.255.252
	lo1	192.168.10.1	255.255.255.0
CE2-A	f0/0	172.16.2.1	255.255.255.252
	lo1	172.16.20.1	255.255.255.0
CE2-B	f0/0	192.168.2.1	255.255.255.252
	lo1	192.168.20.1	255.255.255.0

Tabla 4.3. – Direcciones IP Topología #3

Fuente: Autor.

En la práctica, se asignan más VPNs a cada RR, este ejemplo está diseñado para verificar el funcionamiento de los RR, para ello es preferible hacerlo con una topología menos compleja.

Para tener un funcionamiento correcto, todos los routers deben tener sesiones BGP con todos los RR. Esta topología a pesar de ser óptima, incurre en tener una configuración más compleja para los administradores.
El aislamiento de RR puede ser alcanzado mediante dos técnicas:

1.-Filtros de Entrada y Salida.- Puede ser filtros de salidas en los PE, o filtros de entrada en los RR. En ambos casos, el filtrado puede realizarse con un route-map, asignando rutas en cada atributo BGP que es usualmente en el route target o en la comunidad BGP estándar.

2.- Configurar ORF (Outbound Route Filters). - Filtros de salida en los PE, reduce la utilización de CPU y ancho de banda de los RR. La desventaja es que este procesamiento que evitamos en los RR lo incrementamos en los PEs, pues estos necesitan constantemente darle mantenimiento a sus tablas de enrutamiento para enviar actualizaciones, por el contrario si optamos por poner Filtros de entrada en los RR, disminuimos el procesamiento en los PE, pero se enviaran más actualizaciones desde los PEs a RR por lo que se consumirá ancho de banda, aunque liberaremos de tanto procesamiento al RR, De manera que la aplicación de uno o otra técnica depende de la decisión del administrador en base a los recursos de los que disponga

BGP RR Groups.- Este comando ejecuta la misma función que un route-map, y cumplirá su función siempre y cuando este sea configurado bajo el proceso de ruteo BGP y se aplique a todos los vecinos BGP. Otro detalle operacional importante es que el Access-List de la extended-community mantenido en el RR es descargado como un ORF a los PE a través de la funcionalidad ORF.

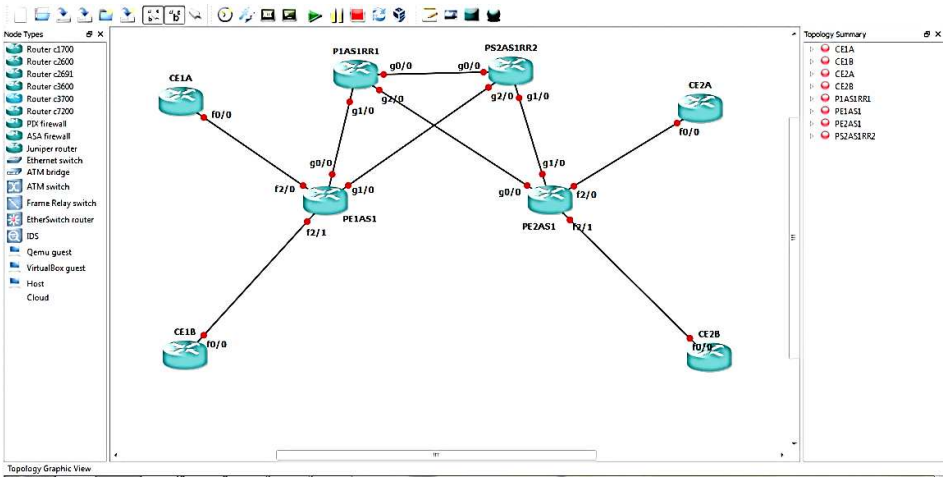

Fig. 4.28. – Topología # 3, GNS3 -Route Reflectors.

Fuente: Autor. Captura de pantalla software GNS3.

Configuraciones Topología #3

CE1A

Declaramos interfaces y vamos a usar el protocolo BGP para intercambiar rutas con el PE.

```
CE1A (config) # interface Loopback1
CE1A (config-if) # ip address 172.16.10.1 255.255.255.0

CE1A (config) # interface FastEthernet0/0
CE1A (config-if) # ip address 172.16.1.2 255.255.255.252
CE1A (config-if) # no shutdown

CE1A (config) # router bgp 65001
CE1A (config) # bgp log-neighbor-changes
CE1A (config-router) # neighbor 10.10.10.101 remote-as 1
CE1A (config-router) # neighbor 10.10.10.101 update-source FastEthernet0/0
CE1A (config-router) # network 172.16.10.0 mask 255.255.255.0
CE1A (config-router) # redistribute connected
CE1A (config-router) # redistribute static
CE1A (config) # ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

CE2A

Declaramos interfaces y vamos a usar el protocolo BGP para intercambiar rutas con el PE.

```
CE2A (config)# interface Loopback1
CE2A (config-if)# ip address 192.168.10.1 255.255.255.0
```

```
CE2A (config)# interface FastEthernet0/0
CE2A (config-if)# ip address 192.168.1.2 255.255.255.252
CE2A (config-if) # no shutdown

CE2A (config)#router bgp 65001
CE2A (config-router)# bgp log-neighbor-changes
CE2A (config-router)# neighbor 10.10.10.101 remote-as 1
CE2A (config-router)# neighbor 10.10.10.101 update-source FastEthernet0/0
CE2A (config-router)# network 192.168.10.0
CE2A (config-router)# redistribute connected
CE2A (config-router)# redistribute static
CE2A (config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

CE2B

Declaramos interfaces y vamos a usar el protocolo BGP para intercambiar rutas con el PE.

```
CE2B (config) # interface Loopback1
CE2B (config-if) # ip address 192.168.20.1 255.255.255.0

CE2B (config) # interface FastEthernet0/0
CE2B (config-if) # ip address 192.168.2.2 255.255.255.252

CE2B (config) # router bgp 1
CE2B (config-router) # bgp log-neighbor-changes
CE2B (config-router) # neighbor 10.10.10.102 remote-as 1
CE2B (config-router) # neighbor 10.10.10.102 update-source FastEthernet0/0
CE2B (config-router) # network 192.168.20.0
CE2B (config-router) # redistribute connected
CE2B (config-router) # redistribute static
CE2B (config) # ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

CE2A

Declaramos interfaces y vamos a usar el protocolo BGP para intercambiar rutas con el PE.

```
CE2A (config) # interface Loopback1
CE2A (config-if) #  ip address 172.16.20.1 255.255.255.0

CE2A (config) # interface FastEthernet0/0
 CE2A (config-if) # ip address 172.16.2.2 255.255.255.252

CE2A (config) # router bgp 65002
CE2A (config-router) # bgp log-neighbor-changes
CE2A (config-router) # neighbor 10.10.10.102 remote-as 1
CE2A (config-router) # neighbor 10.10.10.102 update-source FastEthernet0/0
CE2A (config-router) # redistribute connected
```

```
CE2A (config-router) # redistribute static
CE2A (config) # ip route 0.0.0.0 0.0.0.0 172.16.2.1
```

PE1AS1

```
PE1AS1 (config) # ip cef
PE1AS1 (config) # mpls label protocol ldp
PE1AS1 (config) # no ip domain lookup

PE1AS1 (config) # ip vrf CEA
PE1AS1 (config-vrf) # rd 1:100
PE1AS1 (config-vrf) # route-target both 1:100

PE1AS1 (config) # ip vrf CEB
PE1AS1 (config-vrf) # rd 1:200
PE1AS1 (config-vrf) #   route-target export 1:200
PE1AS1 (config-vrf) #   route-target import 1:200

PE1AS1 (config) # interface Loopback0
PE1AS1 (config-if) # ip address 10.10.10.101 255.255.255.255

PE1AS1 (config) # interface GigabitEthernet0/0
PE1AS1 (config-if) # ip address 10.10.10.1 255.255.255.252
PE1AS1 (config-if) # mpls ip

PE1AS1 (config) # interface GigabitEthernet1/0
PE1AS1 (config-if) # ip address 10.10.10.9 255.255.255.252
PE1AS1 (config-if) # mpls ip

PE1AS1 (config) # interface FastEthernet2/0
PE1AS1 (config-if) # ip vrf forwarding CEA
PE1AS1 (config-if) # ip address 172.16.1.1 255.255.255.252

PE1AS1 (config) # interface FastEthernet2/1
PE1AS1 (config-if) # ip vrf forwarding CEB
PE1AS1 (config-if) # ip address 192.168.1.1 255.255.255.252

PE1AS1 (config-router) # router ospf 1
PE1AS1 (config-router) # log-adjacency-changes
PE1AS1 (config-router) # network 10.0.0.0 0.255.255.255 area 0

PE1AS1 (config) #router bgp 1
PE1AS1 (config-router)#bgp log-neighbor-changes
PE1AS1 (config-router)# neighbor 10.10.10.100 remote-as 1
PE1AS1 (config-router)#neighbor 10.10.10.100 update-source Loopback0
PE1AS1 (config-router) #neighbor 10.10.10.102 remote-as 1
PE1AS1 (config-router) #neighbor 10.10.10.102 update-source Loopback0
PE1AS1 (config-router) #neighbor 10.10.10.103 remote-as 1
```

PE1AS1 (config-router) #neighbor 10.10.10.103 update-source Loopback0

La diferencia entre esta configuración con la de topologías anteriores es el uso de los comandos de activación del route-reflector.

Además, ya que esta topología se basa en separar las actualizaciones de cada VPN hacia un RR designado, deberemos crear route maps y a su vez asígnarle a estos un Access-list que permita el paso de los paquetes que contienen el RT de la VPN asignada.

Entonces esta topología tendrá la misma base de configuración que la topología #1 y la topología #2, los 3 procesos que se añadirán serán:

1. Designación de los clientes Route Reflector.
2. Creación de Access list para filtrar los paquetes por VPN segun el número de Route Target.
3. Asignación de Access List a su respectivo Route Map.

Estas configuraciones están resaltadas a continuación:

PE1AS1 (config-router)# address-family vpnv4
PE1AS1 (config-router) # neighbor 10.10.10.100 activate
PE1AS1 (config-router) # neighbor 10.10.10.100 send-community both
PE1AS1 (config-router) # neighbor 10.10.10.100 route-reflector-client
PE1AS1 (config-router) #neighbor 10.10.10.100 route-map allow1 out

PE1AS1 (config-router) # neighbor 10.10.10.102 activate
PE1AS1 (config-router) # neighbor 10.10.10.102 send-community extended
PE1AS1 (config-router) # neighbor 10.10.10.103 activate

PE1AS1 (config-router) # neighbor 10.10.10.103 send-community both
PE1AS1 (config-router) # neighbor 10.10.10.103 route-reflector-client
PE1AS1 (config-router) # neighbor 10.10.10.103 route-map allow2 out

PE1AS1 (config-router) #address-family ipv4 vrf CEB
PE1AS1 (config-router) # redistribute connected
PE1AS1 (config-router) #redistribute static
PE1AS1 (config-router) # neighbor 192.168.1.2 remote-as 65001
PE1AS1 (config-router) # neighbor 192.168.1.2 update-source Loopback0
PE1AS1 (config-router) # neighbor 192.168.1.2 activate
PE1AS1 (config-router) # neighbor 192.168.1.2 as-override
PE1AS1 (config-router) #exit-address-family

PE1AS1 (config-router) # address-family ipv4 vrf CEA

PE1AS1 (config-router) # redistribute connected
PE1AS1 (config-router) # redistribute static
PE1AS1 (config-router) # neighbor 172.16.1.2 remote-as 65001
PE1AS1 (config-router) # neighbor 172.16.1.2 activate
PE1AS1 (config-router) # neighbor 172.16.1.2 as-override
PE1AS1 (config-router) # network 10.10.10.101 mask 255.255.255.255
PE1AS1 (config-router) # exit-address-family

PE1AS1 (config) #ip bgp-community new-format
PE1AS1 (config) #ip route vrf CEA 172.16.10.0 255.255.255.0 172.16.1.2
PE1AS1 (config) #ip route vrf CEB 192.168.10.0 255.255.255.0 192.168.1.2

PE1AS1 (config) #access-list 10 permit 172.16.10.0 0.0.0.255
PE1AS1 (config) #access-list 20 permit 192.168.10.0 0.0.0.255

PE1AS1 (config) #route-map allow1 permit 10
PE1AS1 (config) #match ip address 10
PE1AS1 (config) # set community 1:100

PE1AS1 (config) #route-map allow2 permit 10
PE1AS1 (config) #match ip address 20
PE1AS1 (config) # set community 1:200

PE2AS1

Declaramos interfaces y vamos a usar el protocolo BGP para intercambiar rutas con el PE.

PE2AS1 (config) #ip vrf CEA
PE2AS1 (config-vrf) # rd 1:100
PE2AS1 (config-vrf) # route-target both 1:100

PE2AS1 (config) # ip vrf CEB
PE2AS1 (config-vrf) # rd 1:200
PE2AS1 (config-vrf) # route-target both 1:200

PE2AS1 (config) # mpls label protocol ldp
PE2AS1 (config) # mpls ip
PE2AS1 (config) # ip cef
PE2AS1 (config) # mpls ldp router-id lo 0

PE2AS1 (config) # interface Loopback0
PE2AS1 (config-if) # ip address 10.10.10.102 255.255.255.255

PE2AS1 (config) # interface GigabitEthernet0/0
PE2AS1 (config-if) # ip address 10.10.10.13 255.255.255.252
PE2AS1 (config-if) # mpls ip

PE2AS1 (config) # interface GigabitEthernet1/0

PE2AS1 (config-if) # ip address 10.10.10.5 255.255.255.252
PE2AS1 (config-if) # mpls ip

PE2AS1 (config) # interface FastEthernet2/0
PE2AS1 (config-if) # ip vrf forwarding CEB
PE2AS1 (config-if) # ip address 192.168.2.1 255.255.255.252

PE2AS1 (config) # interface FastEthernet2/1
PE2AS1 (config-if) # ip vrf forwarding CEA
PE2AS1 (config-if) # ip address 172.16.2.1 255.255.255.252

PE2AS1 (config) # router ospf 1
PE2AS1 (config-router) # network 10.0.0.0 0.255.255.255 area 0

PE2AS1 (config) # router bgp 1
PE2AS1 (config-router) # bgp log-neighbor-changes
PE2AS1 (config-router) #neighbor 10.10.10.100 remote-as 1
PE2AS1 (config-router) #neighbor 10.10.10.100 update-source Loopback0
PE2AS1 (config-router) # neighbor 10.10.10.101 remote-as 1
PE2AS1 (config-router) #neighbor 10.10.10.101 update-source Loopback0
PE2AS1 (config-router) # neighbor 10.10.10.103 remote-as 1
PE2AS1 (config-router) # neighbor 10.10.10.103 update-source Loopback0

PE2AS1 (config-router) #address-family vpnv4
PE2AS1 (config-router-add) # neighbor 10.10.10.100 activate
PE2AS1 (config-router-add) # neighbor 10.10.10.100 send-community both
PE2AS1 (config-router-add) # neighbor 10.10.10.100 route-map allow1 out

PE2AS1 (config-router-add) # neighbor 10.10.10.101 activate
PE2AS1 (config-router-add) # neighbor 10.10.10.101 send-community extended

PE2AS1 (config-router-add) # neighbor 10.10.10.103 activate
PE2AS1 (config-router-add) # neighbor 10.10.10.103 send-community both
PE2AS1 (config-router-add) # neighbor 10.10.10.103 route-map allow2 out
PE2AS1 (config-router-add) # exit-address-family

PE2AS1 (config-router-add) # address-family ipv4 vrf CEB
PE2AS1 (config-router-add) # redistribute connected
PE2AS1 (config-router-add) # redistribute static
PE2AS1 (config-router-add) # neighbor 192.168.2.2 remote-as 65001
PE2AS1 (config-router-add) # neighbor 192.168.2.2 update-source Loopback0
PE2AS1 (config-router-add) # neighbor 192.168.2.2 activate
PE2AS1 (config-router-add) # neighbor 192.168.2.2 as-override
PE2AS1 (config-router-add) # no synchronization
PE2AS1 (config-router-add) # exit-address-family

PE2AS1 (config-router-add) # address-family ipv4 vrf CEA
PE2AS1 (config-router-add) # redistribute connected
PE2AS1 (config-router-add) # redistribute static
PE2AS1 (config-router-add) # neighbor 172.16.2.2 remote-as 65002

PE2AS1 (config-router-add) # neighbor 172.16.2.2 update-source Loopback0
PE2AS1 (config-router-add) # neighbor 172.16.2.2 activate
PE2AS1 (config-router-add) # neighbor 172.16.2.2 as-override
PE2AS1 (config-router-add) # exit-address-family

PE2AS1 (config) # ip route vrf CEA 172.16.20.0 255.255.255.0 172.16.2.2
PE2AS1 (config) # ip route vrf CEB 192.168.20.0 255.255.255.0 192.168.2.2

PE2AS1 (config) # ip bgp-community new-format

PE2AS1 (config) # access-list 10 permit 172.16.20.0 0.0.0.255
PE2AS1 (config) # access-list 20 permit 192.168.20.0 0.0.0.255

PE2AS1 (config) # route-map allow1 permit 10
PE2AS1 (config) # match ip address 10
PE2AS1 (config) # set community 1:100

PE2AS1 (config) # route-map allow2 permit 10
PE2AS1 (config) # match ip address 20
PE2AS1 (config) # set community 1:200

A continuación se describirá la configuración de los RR en los cuales se crearan nuevamente filtros para que solo entre información y actualizaciones de la VPN designada.

P1AS1-RR

P1AS1RR (config) #ip cef
P1AS1RR (config) #no ip domain lookup
P1AS1RR (config) #mpls label protocol ldp
P1AS1RR (config) #mpls ldp router-id Loopback0

P1AS1RR (config) #interface Loopback0
P1AS1RR (config-if) # ip address 10.10.10.100 255.255.255.255

P1AS1RR (config) #interface GigabitEthernet0/0
P1AS1RR (config-if) # ip address 10.10.10.17 255.255.255.252
P1AS1RR (config-if) # mpls ip

P1AS1RR (config) #interface GigabitEthernet1/0
P1AS1RR (config-if) # ip address 10.10.10.2 255.255.255.252
P1AS1RR (config-if) #mpls ip

P1AS1RR (config) #interface GigabitEthernet2/0
P1AS1RR (config-if) # ip address 10.10.10.6 255.255.255.252
P1AS1RR (config-if) # mpls ip

P1AS1RR (config) #router ospf 1
P1AS1RR (config-router) #og-adjacency-changes

P1AS1RR (config-router) # network 10.0.0.0 0.255.255.255 area 0

P1AS1RR (config) #router bgp 1
P1AS1RR (config-router) # no bgp default ipv4-unicast
P1AS1RR (config-router) # bgp log-neighbor-changes
P1AS1RR (config-router) # neighbor 10.10.10.101 remote-as 1
P1AS1RR (config-router) # neighbor 10.10.10.101 update-source Loopback0
P1AS1RR (config-router) # neighbor 10.10.10.102 remote-as 1
P1AS1RR (config-router) #neighbor 10.10.10.102 update-source Loopback0
P1AS1RR (config-router) # neighbor 10.10.10.103 remote-as 1
P1AS1RR (config-router) # neighbor 10.10.10.103 update-source Loopback0

P1AS1RR (config-router) #address-family ipv4
P1AS1RR (config-router) # neighbor 10.10.10.101 activate
P1AS1RR (config-router) # P1AS1RR (config) # neighbor 10.10.10.102 activate
P1AS1RR (config-router) # neighbor 10.10.10.103 activate
P1AS1RR (config-router) # exit-address-family

P1AS1RR (config-router) # address-family vpnv4
P1AS1RR (config-router) # neighbor 10.10.10.101 activate
P1AS1RR (config-router) # neighbor 10.10.10.101 send-community both
P1AS1RR (config-router) # neighbor 10.10.10.101 route-reflector-client
P1AS1RR (config-router) # neighbor 10.10.10.101 route-map allow-VPNA in

P1AS1RR (config-router) # neighbor 10.10.10.102 activate
P1AS1RR (config-router) # neighbor 10.10.10.102 send-community both
P1AS1RR (config-router) # neighbor 10.10.10.102 route-reflector-client
P1AS1RR (config-router) # neighbor 10.10.10.102 route-map allow-VPNA in

P1AS1RR (config-router) # neighbor 10.10.10.103 activate
P1AS1RR (config-router) # neighbor 10.10.10.103 send-community both
P1AS1RR (config-router) # neighbor 10.10.10.103 route-reflector-client
P1AS1RR (config-router) # neighbor 10.10.10.103 route-map allow-VPNA in
P1AS1RR (config-router) # exit-address-family

P1AS1RR (config) #ip bgp-community new-format
P1AS1RR (config) #ip community-list 1 permit 1:100
P1AS1RR (config) #route-map allow-VPNA permit 10
P1AS1RR (config) # match community 1

P2AS1RR

P2AS1RR (config) # ip cef
P2AS1RR (config) #no ip domain lookup
P2AS1RR (config) #mpls label protocol ldp
P2AS1RR (config) #mpls ldp router-id Loopback0

P2AS1RR (config) #interface Loopback0
P2AS1RR (config-if) # ip address 10.10.10.103 255.255.255.255

P2AS1RR (config) #interface GigabitEthernet0/0
P2AS1RR (config-if) # ip address 10.10.10.18 255.255.255.252
P2AS1RR (config-if) # mpls ip

P2AS1RR (config) #interface GigabitEthernet1/0
P2AS1RR (config-if) # ip address 10.10.10.14 255.255.255.252
P2AS1RR (config-if) # mpls ip

P2AS1RR (config) #interface GigabitEthernet2/0
P2AS1RR (config-if) # ip address 10.10.10.10 255.255.255.252
P2AS1RR (config-if) # mpls ip

P2AS1RR (config) #router ospf 1
P2AS1RR (config-router) # log-adjacency-changes
P2AS1RR (config-router) # network 10.0.0.0 0.255.255.255 area 0

P2AS1RR (config) #router bgp 1
P2AS1RR (config-router) # no bgp default ipv4-unicast
P2AS1RR (config-router) # bgp log-neighbor-changes
P2AS1RR (config-router) # neighbor 10.10.10.100 remote-as 1
P2AS1RR (config-router) # neighbor 10.10.10.100 update-source Loopback0
P2AS1RR (config-router) # neighbor 10.10.10.101 remote-as 1
P2AS1RR (config-router) # neighbor 10.10.10.101 update-source Loopback0
P2AS1RR (config-router) # neighbor 10.10.10.102 remote-as 1
P2AS1RR (config-router) # neighbor 10.10.10.102 update-source Loopback0

P2AS1RR (config-router) #address-family vpnv4
P2AS1RR (config-router) # neighbor 10.10.10.100 activate
P2AS1RR (config-router) # neighbor 10.10.10.100 send-community both
P2AS1RR (config-router) # neighbor 10.10.10.100 route-reflector-client
P2AS1RR (config-router) # neighbor 10.10.10.100 route-map allow-VPNB in

P2AS1RR (config-router) # neighbor 10.10.10.101 activate
P2AS1RR (config-router) # neighbor 10.10.10.101 send-community both
P2AS1RR (config-router) # neighbor 10.10.10.101 route-reflector-client
P2AS1RR (config-router) # neighbor 10.10.10.101 route-map allow-VPNB in

P2AS1RR (config-router) # neighbor 10.10.10.102 activate
P2AS1RR (config-router) # neighbor 10.10.10.102 send-community both
P2AS1RR (config-router) # neighbor 10.10.10.102 route-reflector-client
P2AS1RR (config-router) # neighbor 10.10.10.102 route-map allow-VPNB in
P2AS1RR (config-router) # exit-address-family

P2AS1RR (config-) #ip bgp-community new-format
P2AS1RR (config) #ip community-list 1 permit 1:200
P2AS1RR (config) #route-map allow-VPNB permit 10
P2AS1RR (config # match community 1

Una vez que la topología ha sido creada la forma más efectiva de probar conectividad y errores en la configuración es hacer un ping de LAN a LAN, entre los dos locales de los clientes, si la respuesta es positiva la configuración está realizada correctamente, como se aprecia en las capturas tomas en la figura.

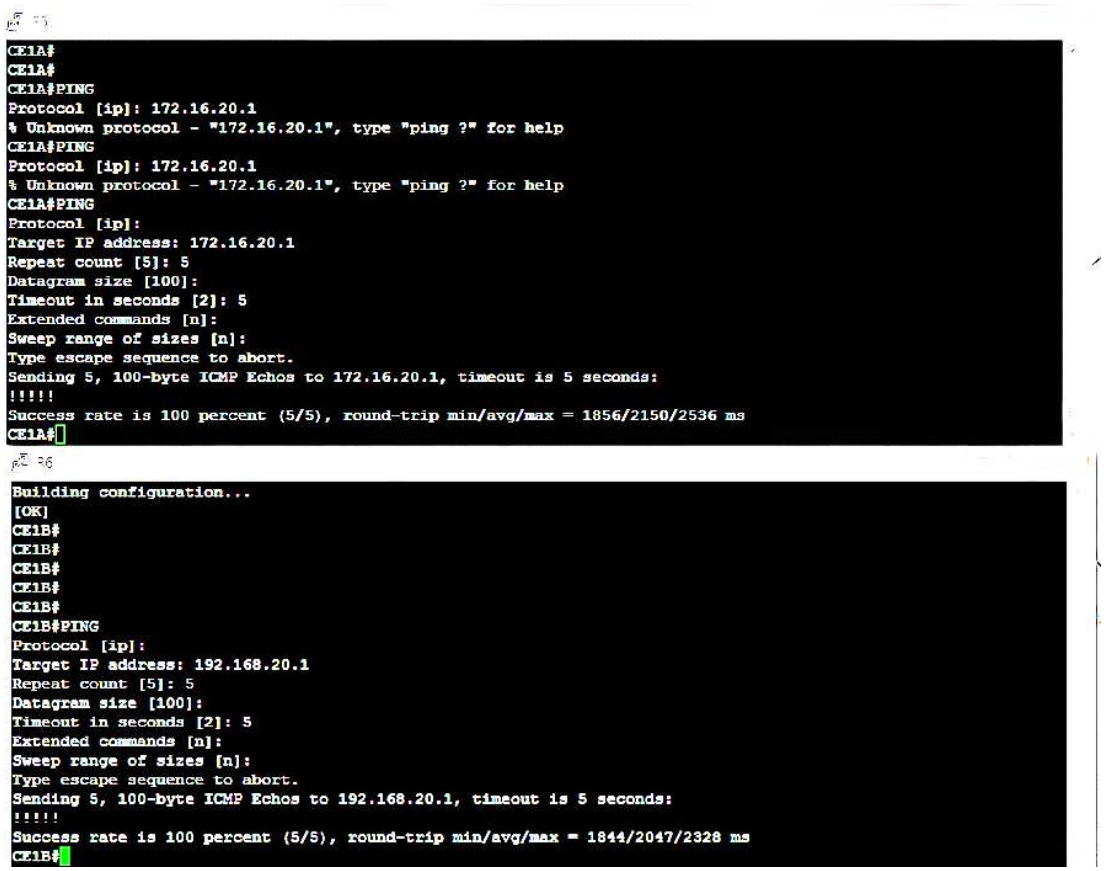

Fig. 4.29. – Topología # 3, verificación con ping de LAN a LAN.
Fuente: Autor. Captura de pantalla software GNS3.

Otra forma muy interesante de hacer verificaciones es realizar una traza con el comando traceroute desde LAN a LAN entre los sitios del cliente, en esta traza se mostraran claramente los saltos MPLS del paquete además de con que etiquetas se asoció al entrar al dominio.

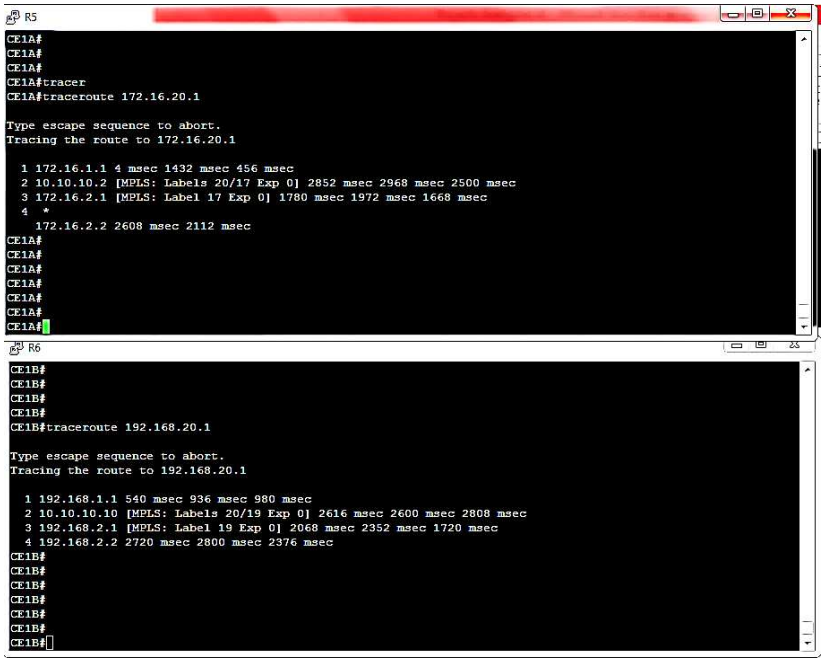

Fig. 4.30. – Topología # 3, verificación con comando traceroute. Fuente: Autor. Captura de pantalla software GNS3.

Se puede hacer verificaciones de la operación de MPLS, usando los comandos descritos en la Topología # 1. Entre esto podemos verificar las interfaces que estén trabajando con MPLS mediante el Comando show mpls interfaces.

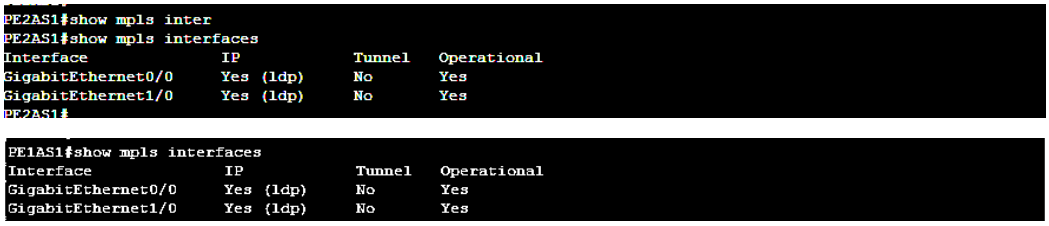

Fig. 4.31. – Topología # 3, verificación con comando show mpls interfaces. Fuente: Autor. Captura de pantalla software GNS3.

Para una revisión más detallada del funcionamiento del protocolo, LDP, y la distribución de etiquetas podemos usar el comando, show mpls forwarding-

table, con esto nos muestra la taba de asignación de etiquetas y de próximos saltos para los diversos vecinos mpls.

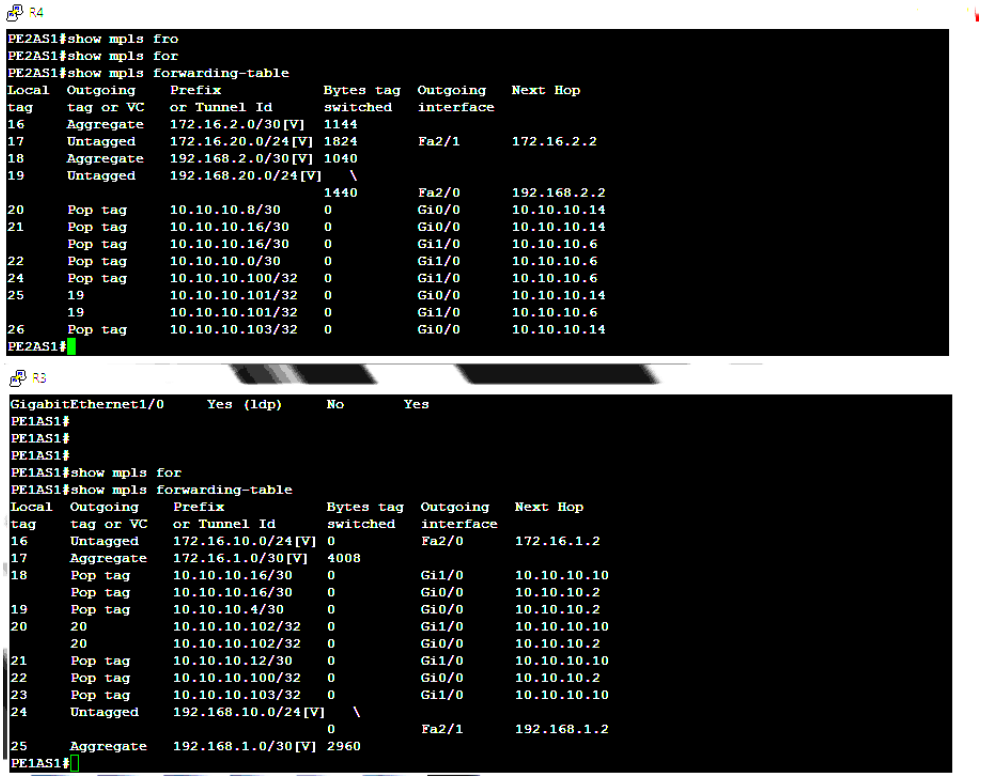

Fig. 4.32. – Topología # 3, verificación con comando show mpls forwarding-table. Fuente: Autor. Captura de pantalla software GNS3.

En esta misma topología se puede ahorrar líneas de configuración usando los ya descritos Peer Groups, el funcionamiento básico de esta funcionalidad vendrá dado de la siguiente manera:

- Definición del Peer Group

  Router (config) #router bgp 1

  *Router (config-router) # **Neighbor** nombre-del-Peer-Group **remote-as** Numero-de-AS*

- Establecer la relación del peer Group

  *Router (config-router) # **Neighbor** direccion-ip **peer-group** nombre-del-peer-group*

- Asociar los Peer groups con Vecinos PE remotos

  Router (config-router) # ***address family vpnv4***

  Router (config-router) # ***Neighbor*** *direccion-ip* ***peer-group*** *nombre-del-peer-group*

- Crear los Route Reflectors

  Router (config-router) # ***Neighbor*** *direccion-ip* ***route-reflector client***

Como se puede ver, la configuración y la lógica básica es la misma solo se agrupan los vecinos BGP en grupos, y designamos características a todo el grupo. Esto ahorra trabajo al administrador, y a su vez procesamiento al router.

4.6.4.- CONFEDERACIONES BGP

Las confederaciones BGP son otra herramienta que reduce la necesidad de hacer una topología full mesh. En esta técnica, un AS se divide en varias Sub-AS. Y cada sub-sistema se asigna a una confederación. Como nos advierte una vez más Amit Rai (2010) en su guía “Route Reflectors and Confederations”, estas confederaciones deberán trabajar bajo las siguientes condiciones:

- Cada confederación tiene que tener una topología Full-mesh física entre sus nodos, es decir, entre los routers asignados a esta confederación.

- Cada AS podrá también tener conexiones a otros sistemas autónomos dentro de la confederación.

- Cada Sub-AS debe estar emparejado por eBGP con otros sub AS.

- Aunque los Sub-AS estarán emparejados por eBGP a otros sub-sistemas autónomos dentro de la confederación, ellos intercambiaran enrutamiento como si fueran iBGP, esto significa que los atributos: Next-Hop, Metric y Local-Preference serán preservados sin ningún cambio. Aunque entre Hacia el mundo exterior ellos se verán como un solo AS.

La configuración de las confederaciones no dista en mucho de la configuración de los routers formando peer-groups. Está basada en los siguientes pasos:

- Definir el ID de la Confederación y los Peers.

  Router (config) #router bgp 1
  *Router (config-router) # **BGP confederation identifier** numero-de-as*
  *Router (config-router) # **BGP confederation peers** numero-de-as*

- Definir los vecinos BGP.

  *Router (config-router) # **neighbor** direccion-ip **remote-as** numero-de-as*
  *Router (config-router) # **neighbor** direccion-ip **update-source** interfaz*
  *Router (config-router) # **neighbor** direccion-ip **ebgp-multihop** hop*

- Activar los vecinos BGP para intercambio VPNV4.

  *Router (config-router) # **address-family vpnv4***
  *Router (config-router) # **neighbor** direccion-ip **next-hop** self*
  *Router (config-router) # **neighbor** direccion-ip **activate***

4.7.- VARIACION: VPN INTER-DOMINIO.

En una red de cliente muy grande, geográficamente hablando, es muy probable que el cliente se tenga que conectar entre Backbones de distintos ISP.

El caso más común es que el cliente tenga dos oficinas en dos ciudades diferentes y estas se conecten cada oficina a diferentes proveedores, pero requieren transporte de datos entre los dos puntos. Esto suele suceder en casos de que uno de los dos proveedores no tenga cobertura en el sector de una de las dos oficinas, entonces se contratara otro proveedor y habrá que hacer esta clase de puente entre ambos.

En estos casos se debe habilitar la continuidad de los servicios de VPN a través de los dos backbones MPLS, por lo que la información de enrutamiento debe ser redistribuida entre los dos. Para esto existe una característica de las VPN que es conocida como: Inter-AS feature.

En la RFC 2547 bis: "*BGP/MPLS IP fundamentals",* Se definen 3 opciones para esta escalabilidad:

1.- Conexiones VRF – VRF en los ASBR (Router de Borde de Sistema Autónomo / Autonomous Systems Border Router).

Este es el modelo más simple, en este los PEs de los diferentes AS funcionaran como ASBR. Estos ASBR están interconectados ya sea mediante un enlace que consiste de subinterfaces lógicas o vía varios enlaces físicos. Las VRF se configuran en los ASBR para agrupar las rutas de los Clientes. Cada subinterfaz o interfaz conectada es asociada a una sola VRF de cliente.

La VRF puede ejecutar eBGP, OSPF, RIPv2, EIGRP o rutas estáticas para distribuir las rutas VPN a su par adyacente, aunque normalmente se usa eBGP en estos casos, gracias a sus políticas, escalabilidad, seguridad, etc. En este método, los LSP en los AS MPLS VPN adyacentes están interconectados usando el mecanismo de reenvio IP entre los routers de borde de los AS.

2.-Redistribucion eBGP de rutas VPN-IPv4 etiquetadas desde el AS a los AS vecinos.

En este método, los ASBR usan MP-eBGP para emparejarse y transportar rutas VPNv4 entre AS. Esto se llama la convergencia ASBR – ASBR, también es conocido como MP-eBGP para el intercambio VPNv4. Esta convergencia entonces alivia la necesidad de tener una configuración por cada VPN en los ASBR como visto en la configuración anterior, y además, permite a los prefijos VPNv4 ser transportados a través de múltiples proveedores.

Para permitir el transporte de los prefijos VPNv4, el enlace entre los AS debe soportar el intercambio de paquetes MPLS porque las actualizaciones VPNv4 son encapsuladas en paquetes MPLS cuando ellas atraviesan un AS y por esto necesitan ser encapsuladas cuando crucen entre AS.

Hay ciertas características a tener en cuenta cuando se use esta opción:

- No hay requerimiento de habilitar LDP o ningún IGP en el enlace que conecta los dos ASBR. La sesión MP-BGP entre los dos routers ASBR conectados directamente sirve para reenviar paquetes etiquetados.

- Ningún Filtro de Route Target necesita ser habilitado en un ASBR que no tiene ninguna VRF configurada o que está funcionando como RR. El comando asegura que el ASBR acepte los prefijos BGP VPNv4 desde otro router PE dentro del AS, el comportamiento por defecto es de negar los prefijos VPNv4 que no son importados ninguna VRF.

3.- Redistribución Multi-Hop eBGP de rutas VPNV4-IPv4 entre la fuente y la AS destino, con redistribución eBGP de rutas IPv4 etiquetadas desde el AS a los vecinos AS.

Esta opción es la considerada la más escalable que la opción 1 y 2. En esta opción, la información VPNv4 es mantenida por los RR. Para poder solventar este requerimiento, cada proveedor necesita tener RR locales para la distribución de los prefijos VPNv4 y conexión eBGP para intercambiar prefijos con el par externo. Los ASBR en esta opción participan en el intercambio de direcciones BGP de próximo salto usando etiquetas IPv4 y RR formando una sesión MP-eBGP para transportar información VPNv4.

P1-AS1-RR y P1-AS2-RR son RR que son locales para cada proveedor. Una sesión MP-eBGP está formada entre los RR para transportar información VPNv4 a través de la red multi-proveedor. Una sesión eBGP está formada entre los ASBRs para intercambiar prefijos de direcciones Next-Hop.

Las configuraciones dentro del AS serán las mismas revisadas en las tres topologías básicas revisadas.
Para poder establecer adyacencia entre los dos AS a interconectarse, tendremos que añadir las siguientes características o líneas de configuración a los dispositivos dentro de las redes contiguas.

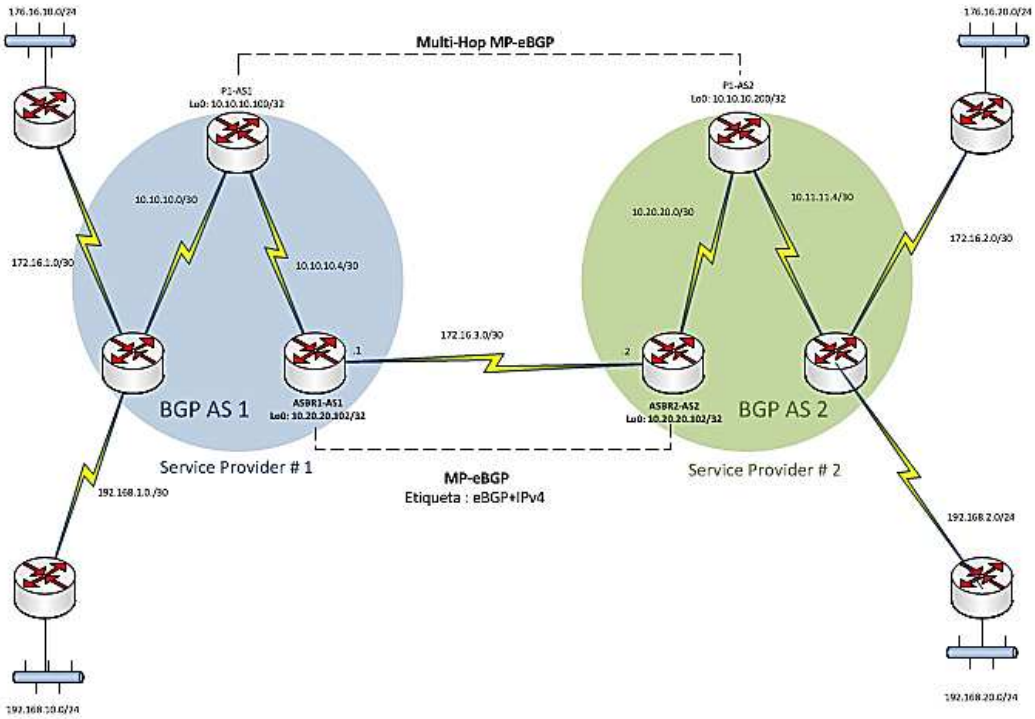

Fig. 4.33. – Variacion,Ejemplo VPN Interdominio.

Fuente: Autor.

- Configurar los routers de Borde de los AS (ASBR –AS Border Router), para que tengan intercambio de etiquetas eBGP e IPv4.

```
ASBR1-AS1 (config)#router bgp 1
ASBR1-AS1 (config-router)# no bgp default route-target filter
ASBR1-AS1 (config-router)# neighbor 172.16.3.2 remote-as 2
ASBR1-AS1 (config-router)# neighbor 172.16.3.2 send-label
```

```
ASBR2-AS2 (config)#router bgp 2
ASBR2-AS2 (config-router)# no bgp default route-target filter
ASBR2-AS2 (config-router)# neighbor 172.16.3.1 remote-as 1
ASBR2-AS2 (config-router)# neighbor 172.16.3.1 send-label
```

- Configurar la redistribución y filtrado en los ASBR.

```
ASBR1-AS1 (config)#router ospf 1
ASBR1-AS1 (config-router)# redistribute bgp 1 subnets route-map bgp-to-ospf
```

```
ASBR1-AS1 (config)#router bgp 1
ASBR1-AS1 (config-router)# network 10.10.10.101 mask 255.255.255.255
ASBR1-AS1 (config-router)# network 10.10.10.200 mask 255.255.255.255
```

```
ASBR1-AS1 (config) # ip prefix-list pref-from-AS2 seq 1 permit 10.20.20.101/32
ASBR1-AS1 (config) # ip prefix-list pref-from-AS2 seq 2 permit 10.20.20.200/32

ASBR1-AS1 (config) # route-map bgp-to-ospf permit 10
ASBR1-AS1 (config-rmap) # match ip address prefix-list pref-from-AS2


ASBR1-AS2 (config # router ospf 2
ASBR1-AS2 (config-router) # redistribute bgp 2 subnets route-map bgp-to-ospf

ASBR2-AS2 (config)#router bgp 1
ASBR2-AS2 (config-router) # network 10.20.20.101 mask 255.255.255.255
ASBR2-AS2 (config-router) # network 10.20.20.200 mask 255.255.255.255
ASBR2-AS2 (config )# ip prefix-list pref-from-AS1 seq 1 permit 10.10.10.101/32
ASBR2-AS2 (config) # ip prefix-list pref-from-AS1 seq 2 permit 10.10.10.200/32

ASBR2-AS2 (config) # route-map bgp-to-ospf permit 10
ASBR2-AS2 (config-rmap) # match ip address prefix-list pref-from-AS1
```

- Configurar sesiones MP-BGP entre los RR.

```
P1-AS1-RR(config)#router bgp 1
P1-AS1-RR(config-router)#neighbor 10.20.20.200 remote-as 2
P1-AS1-RR(config-router)#neighbor 10.20.20.200 update-source loopback0
P1-AS1-RR(config-router)#neighbor 10.20.20.200 ebgp-multihop

P1-AS1-RR(config-router)#address-family vpnv4
P1-AS1-RR(config-router-af)#neighbor 10.20.20.200 activate
P1-AS1-RR(config-router-af)#neighbor 10.20.20.200 send-community extended
P1-AS1-RR(config-router-af)#neighbor 10.20.20.200 next-hop-unchanged

P1-AS2-RR(config)#router bgp 1
P1-AS2-RR(config-router)#neighbor 10.10.10.200 remote-as 2
P1-AS2-RR(config-router)#neighbor 10.10.10.200 update-source loopback0
P1-AS2-RR(config-router)#neighbor 10.10.10.200 ebgp-multihop

P1-AS2-RR(config-router)#address-family vpnv4
P1-AS2-RR(config-router-af)#neighbor 10.10.10.200 activate
P1-AS2-RR(config-router-af)#neighbor 10.10.10.200 send-community extended
P1-AS2-RR(config-router-af)#neighbor 10.10.10.200 next-hop-unchanged
```

En este proyecto de tesis hemos estudiado las configuraciones y ventajas del uso de la tecnología MPLS.

Dentro de las características principales mencionadas en el Capítulo I que hicieron que MPLS sea tan popular y tan efectivo están las tres principales que son:

Soporte de VPN.- Este tema se ha tratado a lo largo del proyecto, ya que las redes de transporte de datos se basan principalmente en redes VPN entrelazadas.

Los otros dos temas son la Ingeniería de Trafico y la Calidad de Servicio, que nos provee MPLS, estos son temas tan extensos y complejos que serían material para otro proyecto de tesis, como estudio de estos beneficios, pero a continuación se hará un resumen de lo que representan estos dos temas tan importantes, y de que se tratan para poder visualizar el protocolo MPLS con una visión general.

4.8.- INGENIERIA DE TRAFICO (TE).

López Sarmiento y Gelvez Nancy (2009) definieron la Ingeniería de Trafico de la siguiente manera:

> La ingeniería de tráfico se define como el proceso de distribuir toda la información o el tráfico que se encuentre en el dominio MPLS, de tal manera que los enlaces no se congestionen, permitan la fluidez del tráfico, evite la saturación de los enlaces, y el efecto cuello de botella. Esto se puede realizar separando los tipos de tráfico de manera que un tipo de datos se encamine por un LSP determinado.

El objetivo de la ingeniería de tráfico es mejorar la performance del sistema.

José Barberá en su artículo para la Revista de Actas del V Congreso de usuarios del Internet (1997), definió entre los objetivos de MPLS los siguientes:

1. Enrutar el tráfico establecido por el IGP a una ruta menos congestionada, en caso de estar saturada la red.
2. Maximizar el uso de los recursos.
3. Garantizar la fiabilidad de la transmisión.
4. Establecer criterios para garantizar la preferencia de ciertos caminos que pueden ser o no obligatorios para un tipo de tráfico.

La ingeniería de tráfico permite al administrador obtener estadísticas de uso LSP, que se pueden utilizar para la planificación de la red y como herramientas de análisis de cuellos de botellas y carga en los enlaces, lo que resulta bastante útil para planes de expansión futura y determinar rutas específicas para tipos de datos y servicios especiales.

Se divide en dos tipos de ingeniería de tráfico:

- **Orientada a trafico:** Minimiza perdidas, retardos, maximiza el rendimiento

- **Orientada a recursos:** Optimiza los recursos de red: Ancho de Banda.

4.8.1.- COMPONENTES DE LA INGENIERIA DE TRÁFICO.

Existen 4 Componentes de la TE:

- **Componente Reenvío de Paquetes / Packet Forwarding.**

La componente número uno, Componente de reenvío de paquetes, será en este caso MPLS, que es el encargado del Forwarding de los datos dentro de la red.

- **Componente de Distribución de la Información.**

La segunda componente, consiste en requerir de un conocimiento detallado de la topología de la red, así como también información dinámica de la carga de la red. Cada router mantienen atributos de los enlaces de la red e información de la topología de red en una base de datos de TE. Esta base de datos es usado para el cálculo de rutas explicitas, para la ubicación de LSPs a lo largo de la topología física.

- **Componente de selección de camino.**

Esta se pone en práctica luego de que los atributos de los enlaces y la información de topología han sido inundados por IGP y localizados en la tabla de TE, cada router a lo largo del dominio de ruteo. El LSP puede ser representado tanto por una ruta explicita o sin trabas.
El router de ingreso determina el camino físico para cada LSP aplicando un algoritmo de camino más corto llamado CSPF (Constrained Shortest Path First) a la TED.

- **Componente de señalización**

La cuarta y última componente se encarga de que el LSP se establezca para que funcione por medio del cambio de etiquetas entre los routers de la red.

Entonces, en la Ingeniería de trafico sirve para definir caminos a través de la red, de manera que el administrador pueda descongestionar la red, y evitar los cuellos de botella, pero también puede definir caminos enteros para tipos de trafico especifico de manera que por ejemplo que el tráfico de voz o streaming, sigan un LSP determinado a través del dominio MPLS, esto se logra gracias a la Diferenciación de Servicios, y la Calidad de Servicio.

4.9.- CALIDAD DE SERVICIO (QoS)

Qos representa el conjunto de técnicas necesarias para administrar el ancho de banda, retardo, jitter y pérdida de paquetes.

Desde el punto de vista comercial, es esencial el asegurar que las aplicaciones críticas les sean garantizadas los recursos que necesiten, a pesar de las variaciones en la carga del tráfico de la red.

Ademas QoS es la habilidad diferenciar diversas clases de tráfico basado en criterios definidos y prioridades asignadas basadas en variables que afectan el tratamiento del tráfico en cada router en la red.

Se recomienda implementar QoS donde existen diferentes clases de tráfico que son transportados a través del dominio del proveedor.

El tráfico puede ser clasificado basado en diferentes tipos como, video, aplicaciones, datos, entre otros y también puede ser clasificado según el patrón del tráfico.

Una vez que el tráfico ha sido clasificado en diferentes clases, el siguiente paso es identificar que operaciones serán desarrolladas en cada una de las clases en el router local. Notar que a pesar que QoS es una implementación de extremo a extremo, esta debe ser configuradas tradicionalmente en todos los routers desde un extremo del camino al otro.

El proceso de definir las operaciones de QoS para cierto tipo de tráfico es llamado Política de Servicio.
Luego de que las políticas son definidas entonces son aplicados a la interfaz del dispositivo.
Entonces QoS tiene 3 pasos básicos:

1. Clasificación de tráfico basado en criterios predefinido.
2. Configuración de dispositivo para políticas QoS.
3. Asociación de políticas QoS a la interfaz.

En el modelo de Diferenciación de Servicio, los routers o Switches de L3 en la red están configurados por Políticas QoS que pueden ser aplicadas a una clase de tráfico que atraviesa el router. El tráfico de Datos puede también ser segregado en diferentes clases de tráficos basados en el tipo de datos, hay dos tipos, aplicación, y mejor esfuerzo.

En su informe MPLS Overview (2010), Riedel Wolfgang, establece los parámetros principales sobre los que actúa el Backbone del proveedor para ofrecer Calidad de Servicio, sobre los datos de los clientes transportados a través de él, los cuales son:

- Latencia.
- Jitter.
- Throughput.
- Tasa de Perdida.

Este mecanismo donde un router lee y aplica políticas basados en la clasificación es comúnmente llamado PHB (Per Hop Behavior) en el router. Dentro de la red MPLS los datos QoS serán mapeados incluyéndolos en la etiqueta MPLS los bits de QoS, dentro del campo EXP.
Cuando implementamos QoS, un término muy usado en el término encolamiento (queuing).

Administración de Congestión.- es el proceso de selectivamente encolar paquetes en los routers de manera que los paquetes de mayor prioridad asociados a una clase son procesados primero durante la transmisión.

Evitación de congestión.- Es el proceso de selectivamente descartar paquetes en miras de evitar alcanzar el 100% de la capacidad de procesamiento de la cola, ya que en el momento que se llene el 100% de la capacidad de la cola todos los paquetes serian descartados. El mecanismo usado para evitar la congestión es llamado Weighted Random Early Detection (WRED), con este proceso la cola nunca alcanzara el 100% de su capacidad y entonces, no hay descarte de paquetes por encolamiento.

El proceso de reforzar las políticas mediante el descarte de paquetes en concordancia con el perfil de tráfico asociado a la clase es realizado usando dos técnicas llamadas traffic policing y traffic shaping. En resumen, entre los esquemas más usados para la administración y evitación de congestión que pueden ser usados con MPLS, tenemos 3 principales:

- FIFO, (First In First Out),
- WRED (Weighted Random Early Detection)
- Traffic Shaping and Policing.

Con el FIFO nos aseguramos que los paquetes lleguen o se repartan de manera cronológica, con el segundo evitamos la saturación en la cola de los enlaces en caso de que exista congestión y con el tercero podemos controlar

la cantidad de trafico enviado por las interfaces, de manera que podamos manipular los caminos y la carga que por ellos circula, ayudando al balance de información entre los diferentes medios de transmisión dentro del dominio MPLS.

CAPITULO V:

CONCLUSIONES Y RECOMENDACIONES

5.1.- CONCLUSIONES

Al haber finalizado el estudio de la tecnología MPLS: Multi-Protocol Label Switching, y la utilización de del simulador de redes GNS3, herramienta de carácter práctico para el estudio de redes de Comunicaciones. Se determinó que para ejecutar este estudio fue necesario hacer un análisis minucioso del contenido de los procesos globales y procedimientos que envuelve el uso de la tecnología, además de la instrucción adquirida para el manejo adecuado de la herramienta, para lo cual se realizó la investigación respectiva obteniendo los resultados deseados y que fueron propuestos como objetivos específicos de este proyecto:

Se explicó de manera concisa, conceptual y practica la tecnología MPLS a manera global y el funcionamiento de sus componentes en el marco teórico. Después de la revisión de los antecedentes y el estudio del marco teórico de la tecnología, pudimos esclarecer las ventajas que se obtienen con la implementación de la tecnología, como: el ahorro de procesamiento, equipos, tiempo, la gran disminución de retardo, congestión, fluctuaciones, y la versatilidad y la velocidad con la que una paquete puede moverse a través de gran número de nodos, para así llegar a su punto de destino.

Al finalizar la topología 1, se realizó un resumen de los procesos globales (enrutamiento, reenvió) que se utilizan en la red MPLS, a manera de que se explique de una manera más clara, y descriptiva, paso a paso, lo que ocurre con el paquete mientras viaja a través de la red del Proveedor.

Las topologías diseñadas en el proyecto fueron adecuadas para la explicación de los procesos separados de enrutamiento y reenvío de información y para explicar en qué momento entra en acción cada una de las características y procesos de la red MPLS, como lo son la creación de VRFs, el uso de BGP como protocolo de enrutamiento entre los bordes, el proceso de etiquetado de los paquetes y el posterior reenvío hacia su destino final.

Se determinó la eficiencia del software de simulación GNS- Dynamips, se hizo uso de las herramientas más comunes para la manipulación de dispositivos en la simulación, con las cuales se realizaron las topologías diseñadas previamente y se obtuvieron los resultados deseados en las mismas, además se usaron los comandos de configuración para la programación de los dispositivos y los comandos de verificación para comprobar que los mecanismos y las bases teóricas estudiadas se cumplen a cabalidad tal como fueron descritas.

Este estudio de la tecnología MPLS, resulta una guía teórico-práctica sobre el funcionamiento de la tecnología, de manera que este proyecto se podrá usar como una referencia para cualquier consultante o estudiante de las tecnologías involucradas en este libro.

5.2.- RECOMENDACIONES

- Se recomienda realizar enlaces reales entre los CE y PE, establecer mecanismos de redundancia dinámicos, backups con OSPF, para asegurar que el tráfico no se corte si existe algún problema en el enlace.

- Se recomienda el análisis de los protocolos de enrutamiento (OSPF, EIGRP, IS-IS), antes de la implementación para poder determinar los posibles problemas relacionados con su convergencia.

- Antes de la implementación asegurarse que los routers a implementar en la topología posean capacidades BGP y MPLS, es preferible que sean de las series 7600 o 12000.

- Se sugiere a la hora de instalar el software GNS3, que la PC en la que se instale debe tener más de 1 Gigabyte de memoria RAM, y dejar de usar en lo posible otros programas mediante la simulación, para que no exista inconvenientes de inhibición.

- La implementación de softwares de simulación, como el usado en este proyecto para el aprendizaje en las aulas de la Facultad de Educación Técnica para el Desarrollo, y la inclusión de estos temas de Networking en las prácticas de las materias de Telemática II, de la Universidad Católica de Santiago de Guayaquil, para que el alumno pueda tener mayor experiencia en este campo y aprenda a diferenciar los diferentes inconvenientes que se pueden presentar.

- Se recomienda, como último punto, la realización de otros proyectos de tesis, a fin de complementar y expandir el tema del Multiprotocol Label Switching y la gestión de la red, tales como:

    - El estudio del protocolo BGP y sus atributos con simulaciones, especializadas en los más importantes.

    - Estudio de los Servicios de Ingeniería de Trafico y QoS y su aplicación en el núcleo de las redes MPLS.

    - Estudio de los parámetros y procesos que se establecen para la Diferenciación de Tipos de Servicio en un red MPLS, con funcionalidades de QoS.

    - Estudio de Aplicación de la tecnología MPLS, en las redes de Telefonía Móvil.

    - Estudio de la aplicación del Protocolo IPV6 en las redes de transporte de Datos MPLS.

GLOSARIO DE TERMINOS

ACCESS-LIST: Lista de acceso para actualizaciones IPv4 recibidas.

ACK: Mensaje de Acuse de recibo.

AS: Autonomous System, Sistema Autónomo.

ATM: Asynchronous Transfer Mode, Modo de transferencia Asíncrona.

BGP: Border Gateway Protocol, Protocolo de Puerta de enlace Borde.

CE: Customers Edge, Equipo de Borde de Cliente.

CORE Núcleo de Red.

CSPF: Constrained Short Path First, Primero el Camino corto Constreñido.

eBGP: Exterior Border Gateway Protocol, Protocolo de puerta de enlace de Borde exterior.

EGP: Gateway Protocol, Protocolo de Puerta de enlace exterior.

EIGRP: Enhanced Interior Gateway Routing Protocol, Protocolo de enrutamiento de puerta de enlace interna.

ELSR: Edge Label Switching Router, Enrutador de Conmutación de Etiquetas de Borde.

EXP: Experimental, campo experimental en paquetes MPLS-IP usado para QoS.

FEC: Forwarding Equivalence Class, Clase Equivalente de Reenvío.

FORWARDING: Mecanismo de Reenvío de paquetes.

GNS: Graphic Network Simulator, Simulador de redes Grafico

IANA: International Assign Number Authority, Autoridad Internacional de Asignación de Números.

iBGP: interior Border Gateway Protocol, protocolo de puerta de enlace de borde interno.

IETF: International Engineering Task Force, Fuerza internacional de Tareas de Ingeniería

IGP: Interior Gateway Protocol, Protocolo de Puerta de Enlace Interior

IOS: Internal Operating System, Sistema Operativo interno.

IP: Internet Protocol, Protocolo de Internet.

JITTER: Fluctuaciones de señal

LAN: Local Area Network, Red de área Local.

LDP: Label Distribution Protocol, Protocolo de distribución de etiquetas.

LFIB: Label Forwarding Information Base, base de formación de reenvío de etiquetas.

LIB: Label Information base, base de información de Etiquetas.

LIFO: Last In First Out, Ultimo que entra Primero que sale.

LSR: Label Switching Router, Enrutador de Conmutación de etiquetas

MED: Multi Exit Discriminator, Discriminador de Múltiples salidas.

MP-BGP: Multi Protocol Border Gateway Protocol, Protocolo de puerta de enlace de Borde Multiprotocolo.

MPLS: Multiprotocol Label Switching, Conmutación de Etiquetas Multiprotocolo.

NAT: Network Address Translation. Traducción de Direcciones de Red.

OSPF: Shortest Path First, Abrir el camino más corto primero.

P: Provider Router, Enrutador de Proveedor.

PE: Provider Edge, Borde de Proveedor.

PHB: Per Hop Behavior, Comportamiento por Saltos.

PPP: Point-to-Point protocol, Protocolo de enlace Punto a Punto.

QoS:	Quality of Service, Calidad de Servicio
RD:	Route Distinguisher, Distinguidor de Ruta.
RIB:	Routing Information Base, Base de información de Enrutamiento.
RIP:	Routing Information Protocol, Protocolo de Información de Enrutamiento.
ROUTE MAP:	Mapa de Enrutamiento.
RR:	Route Reflector, Reflectores de rutas.
RT:	Route Target, Destino de Ruta.
SYN:	Synchronization, Sincronización.
TCP:	Transmission Control Protocol, Protocolo de Control de Transmisión.
TE:	Traffic Engineering, Ingeniería de Trafico.
THROUGHPUT:	Volumen de trabajo o Informacion que fluye a través de un sistema o un enlace.
TTL:	Time To Live, Tiempo de Vida.
VPN:	Virtual Private Network, Redes Privadas Virtuales.
VRF:	Virtual Routing Forwarding, Reenvío Virtual de Enrutamiento.
VTY:	Virtual Tele Type, Tele tipo virtual.
WRED:	Weighted Random Early Detection, Detección Temprana Peso variable.

REFERENCIAS BIBLIOGRAFICAS

- Alvez Rogelio (2009), **Fundamentos MPLS/VPN**, TIAGORA, Cisco Systems Inc, Buenos Aires, Argentina.

- Amit Rai, (2010), **IBGP Basics**, *Blog: www.netcerts.net*, http://netcerts.net/ibgp-basics/.

- Amit Rai, (2010), **Route Refletors and Confererations**, *Blog: www.netcerts.net*, http://netcerts.net/ibgp-basics/. *Fecha de Consulta: 11 de Julio 2013.*

- Anderson L., Asati R. (2009), **RFC 3032: Multiprotocol Label Switching label stack entry, "EXP" Field renamed to "Traffic Class" Field**, California, Estados Unidos: *Network Working Group: Cisco Systems, Inc., Acreo AB Inc*.

- Ashish Shirkar, (2013), **Configuration Example: Route-Reflectors Implementation in MPLS VPN, Cisco Support Community**, Cisco Systems Inc., *Cisco Press: Support Forums, http://supportforums.cisco.com/docs/DOC-32629*. *Fecha de Consulta: 19 de Julio 2013.*

- Atouguia Dos Santos Jorge L. (2008), **Redes Privadas Virtuales (VPN) y Calidad de Servicio (QoS) en Redes de Conmutación de Paquetes basados en el Protocolo de Conmutación de Etiquetas (MPLS)**, *Trabajo de Grado,* Bogotá, Colombia: *Universidad Católica Andrés Bello*.

- Barberá, José. (1997), **MPLS: Una arquitectura de backbone para la Internet del siglo XXI,** Madrid, España: *Revista: Actas del V Congreso de Usuarios de Internet. Mundo Internet 2000*.

- Cisco Systems, (2005), **Configuring BGP on Cisco Routers, Volume 1 Student Guide***,* California, Estados Unidos*: Cisco Press*.

- Gonzales Agustín, (2006), **Introducción a MPLS**, Maryland, Estados Unidos, Departamento de Computación de la Universidad de Maryland.

- Lancy Lobo, (2005) **MPLS configuration on Cisco IOS Software**, *ISBN: 1-58705-199-0,* California, Estados Unidos*: Cisco Systems, Inc., Cisco Press*.

- López Sarmiento, Gelvez Nancy, (2009), **Ingeniera de tráfico en redes de conmutación de etiquetas**, Bogotá, Colombia: *Universidad Distrital Francisco José de Caldes*.

,

- Parkhurst William, (2001) **Cisco BGP-4 Command and Configuration handbook**, *ISBN: 1-58705-301-2*. California, Estados Unidos: *Cisco Systems Inc., Cisco Press.*

- Pepelnjak I., Guichard J. (2001). **MPLS and VPN Architectures, Volume. 1**. California, Estados Unidos: *Cisco Systems Inc., Cisco Press.*

- Reagan James, (2002) **Implementing Cisco MPLS**, *CCIP MPLS Study Guide, Londres, Inglaterra: Sibex Inc.*

- Riedel Wolfgang, (2010), **MPLS Overview**, California, Estados Unidos: *Cisco Systems, Inc., Cisco Press*.

- Roca Dominguez, Tedi; Chica Pedrero Pamela, Muñoz Bernardó, (2004), **Ingeniería de Redes: Trabajo sobre MPLS**, Nicaragua: *Universidad del Norte de Nicaragua.*

- Rosen Eric, Callon Ross, Viswanathan Arun, (2001), **RFC 4456: Multiprotocol Label Switching Architechture,** California Estados Unidos: *Network Working Group: Cisco Systems, Force10 Networks, Inc. Juniper Networks, Inc*.

- Rosen Eric, Rekhter Yakov, (2006)**, RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)**, California Estados Unidos: *Network Working Group, Cisco Systems, Inc. and Juniper Networks, Inc*.

- Tapasco García Martha Odilia, (2008), **MPLS, el Presente de las redes IP**, Tesis de Grado, Colombia: *Universidad Tecnológica de Pereira*.

- Vicente, Carlos, (2011), **Practicas Recomendadas con BGP,** Trabajo para el 14º Taller de Redes Internet de Latinoamérica y el Caribe. Guayaquil, Ecuador. Fundación Es La Red.