



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACION:

CONTRIBUCIÓN EN EL ANÁLISIS Y SIMULACIÓN DE UNA RED IP/MPLS
PARA UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES

Previa la obtención del Grado Académico de Magíster en

Telecomunicaciones

ELABORADO POR:

Ing. Leonel Morán Rivera

Guayaquil, Marzo 2015



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Leonel Morán Rivera como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, Marzo 2015

DIRECTOR DEL TRABAJO DE TITULACION

MsC. Manuel Romero Paz

REVISORES:

MsC. Fernando Palacios.

MsC. Luzmila Ruilova

DIRECTOR DEL PROGRAMA

MSc. Manuel Romero Paz



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, Leonel Augusto Morán Rivera

DECLARO QUE:

El Trabajo de Titulación “PROPUESTA PARA LA CONTRIBUCIÓN EN EL ANÁLISIS Y SIMULACIÓN DE UNA RED IP/MPLS PARA UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP)”, previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación del Grado Académico en mención.

Guayaquil, Marzo 2015

EL AUTOR

Ing. Leonel Morán Rivera



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

Yo, Leonel Morán Rivera

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación de Maestría titulada: “PROPUESTA PARA LA CONTRIBUCIÓN EN EL ANÁLISIS Y SIMULACIÓN DE UNA RED IP/MPLS PARA UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, Marzo 2015

EL AUTOR

Ing. Leonel Morán Rivera

Dedicatoria

A Dios, mi madre, mi padre,
mi esposa e hijo que con
mucho amor y cariño les
dedico todo mi esfuerzo y
trabajo puesto para la
realización de esta tesis.

Agradecimientos

Como ser supremo y Rey Celestial, agradecemos a Dios por habernos dado vida para poder luchar sin pensar en obstáculos y seguir adelante enfrentando lo difícil y vencer adversidades.

Mi más profundo agradecimiento a mis padres que me brindaron la oportunidad de superarme en la vida, a mi gran amor y querida esposa Evelyn que ha sido un irremplazable apoyo y a mi querido hijo que es quien me da las fuerzas suficientes para lograr mis metas.

INDICE GENERAL

CAPITULO 1 :Descripción del proyecto de intervención.....	13
1.1 Antecedentes	13
1.2 Definición del problema	13
1.3 Objetivos	13
1.3.1 Objetivo Generales:	13
1.3.2 Objetivos Específicos:	14
1.4 Hipótesis	14
1.5 Metodología de la investigación.....	14
CAPITULO 2 :Introducción a la MPLS	15
2.1 Qué es MPLS?	15
2.2 Aplicaciones del MPLS	18
2.3 Arquitectura del MPLS.....	18
2.4 Funcionamiento del MPLS	25
2.5 Habilitando MPLS.....	28
2.6 Redes privadas Virtuales (VPN)	28
2.6.1 MPLS VPN	29
2.6.2 Implementación de MPLS L2VPN.....	31
2.6.3 Implementación de MPLS L3VPN.....	34
CAPITULO 3 : DISEÑO Y DESARROLLO DE LA SIMULACION	36
3.1 Plan de implementación	36
3.2 Solución Propuesta.	36
3.3 Diagrama de interconexión.....	36
3.3.1 Físico.....	36
3.3.2 Lógico.....	38
3.4 Políticas de Nombres y direccionamiento IP	39
3.4.1 Nombres de Equipos	39
3.4.2 Identificadores de Equipos	40
3.4.3 Direccionamiento IP - Loopback 100	41
3.4.4 Direccionamiento WAN	42
3.5 Asignación de VRF, RD y RT	43
3.6 Seguridad	44
3.7 Desarrollo lógico del esquema	45

3.7.1	Comprobación del IS-IS	46
3.7.2	Comprobación del LDP	47
3.7.3	Comprobación del MP-BGP	48
3.8	Pruebas de servicios diferenciados (voz, datos e internet).....	48
3.8.1	Comprobando que los servicios estén operativos	49
3.8.2	Comprobando redundancia de la red MPLS VPN.....	53
CAPITULO 4 : Conclusiones y recomendaciones.		61
4.1	Conclusiones.....	61
4.2	Recomendaciones	62
Referencia Bibliográfica		63
GLOSARIO DE TERMINOS.....		65

INDICE DE GRAFICAS

Figura 2.1.1: Diagrama de red IP/MPLS-Etiquetas	16
Figura 2.3.1: Posición de la etiqueta MPLS en la Trama de Capa2	19
Figura 2.3.2: Arquitectura básica de un nodo IP/MPLS	21
Figura 2.3.3 : División del funcionamiento interno del Router	22
Figura 2.3.4 : Formato de la MPLS Label	22
Figura 2.4.1 : Esquema Funcional de la MPLS	26
Figura 2.4.2 : Funcionamiento de un LRS del núcleo MPLS	27
Figura 2.4.3 : Envío de un Paquete por un LSP	27
Figura 2.6.1 : ESQUEMA MPLS VPN con clientes	30
Figura 2.6.2 : Esquema funcional de los RD y RT	35
Figura 3.3.1 : Diagrama de interconexión red IP/MPLS	37
Figura 3.4.1 : Definición de Nombres de Equipos MPLS	39
Figura 3.7.1 : Tabla de vecinos IS-IS	46
Figura 3.7.2 : Tabla de enrutamiento del IGP	47
Figura 3.7.3 : Sesiones LDP establecidas hacia los Vecinos	48
Figura 3.7.4 : Sesiones activas hacia los Route-reflector	48
Figura 3.8.1 : Equipos para Pruebas de servicios.....	48
Figura 3.8.2 : Rutas aprendidas en las VRF	50
Figura 3.8.3 : Pruebas de los CE - Cliente A	51
Figura 3.8.4 : Prueba de Operatividad y conectividad de la MPLS L2VPN.	52
Figura 3.8.5 : Configuración y prueba del Traffic Engineering	53
Figura 3.8.6 : Simulando afectación de RR (GYEBRSR01)	54
Figura 3.8.7 : Resultados obtenido durante el proceso de pérdida de conectividad del RR Principal.	55
Figura 3.8.8 : Pruebas de conectividad (sin perdidas de servicio)	56
Figura 3.8.9 : Confirmación de ruta principal en el CORE	57
Figura 3.8.10 : Ruta Principal y de Backup del CORE	57
Figura 3.8.11 : Convergencia de la red	58
Figura 3.8.12 : Servicios de Voz, datos e Internet sin afectación	58
Figura 3.8.13 : Traffic Engineering - explicit-path.....	59
Figura 3.8.14: Estado del Tunnel de Ingeniería de Tráfico	60
Figura 3.8.15 : Conmutación del tunnel al path secundario	60

INDICE DE TABLAS

Tabla 2.3.1 : Valores reservados de la Label	23
Tabla 2.4.1 : Acciones de la etiqueta MPLS.....	25
Tabla 2.5.1 : Pasos para configurar MPLS en un Router Cisco	28
Tabla 2.6.1 : Simbología del esquema MPLS VPN.....	30
Tabla 2.6.2 : Configurando Ethernet sobre MPLS en una interface	32
Tabla 2.6.3 : Configuración de MPLS L2VPN con Interface Vlan.....	33
Tabla 2.6.4 : Configuración Modo Trunk	33
Tabla 2.6.5 : Configuración EVC	33
Tabla 2.6.6 : Modos de Operación del RT	34
Tabla 2.6.7 : Implementando VRF (MPLS L3VPN)	34
Tabla 3.3.1 : Distribución equipos MPLS	37
Tabla 3.4.1 : Tabla de Identificadores de equipos MPLS.....	40
Tabla 3.4.2 : Ip Planning Loopback 100	42
Tabla 3.4.3 : IP Planning WAN	42
Tabla 3.5.1 : Nomenclatura del nombre de la VRF	43
Tabla 3.5.2 : Nomenclatura de la RD	44
Tabla 3.6.1 : Comando de seguridad LDP, ISIS y BGP	44
Tabla 3.8.1 : Datos clientes según el servicio.....	49
Tabla 3.8.2 : Planeamiento IP y Vlan de los servicios propuestos.	49

RESUMEN

En el presente documento se muestra el trabajo de titulación previo a la obtención del Grado Académico de Magíster en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil, en la cual se encamina a que los lectores conozcan las características, el diseño e implementación de una red **IP/MPLS** para un proveedor de servicio de Telecomunicaciones. Su planeamiento y estructura desarrollada mediante la simulación propuesta, demostrará como en una red **IP/MPLS** puede proveer servicios adicionales, que con una red netamente IP simplemente no sería posible brindarlo.

A través de la **Layer 3 MPLS VPNs**, por medio de las VRF (*Virtual Routing Forwarding*) se crearán tablas de enrutamiento virtuales, generando así una tabla de enrutamiento única para cada Cliente o servicio que se desee brindar tal como Voz, Datos e Internet; sin que las red Privadas puedan unirse entre ellas, permitiendo así la reutilización de los direccionamientos IP privados. De la misma manera se detalla las **Layer 2 MPLS VPNs** con la que se crea conexiones Punto a Punto por medio de un contenedor virtual (VC) brindando al cliente un total control de la tabla de enrutamiento, por lo que el ISP no participa en el proceso de enrutamiento a diferencia de la L3 MPLS VPN.

La simulación propuesta, se la elabora en un ambiente controlado, bajo la plataforma GNS3, con equipos de la marca Cisco (Modelos 7600 y 3725). Los procesos realizados en entornos reales pueden ser simulados, garantizando que el funcionamiento de la red sea el esperado al momento de implementarlo en los dispositivos reales. La Plataforma GNS3 es una herramienta muy poderosa y brinda la capacidad de realizar pruebas rigurosas, que en una red real, pueda afectar el rendimiento de los equipos provocando caídas de servicios y pérdidas económicas para la empresa.

ABSTRACT

The present document work prior to obtaining the academic degree of Master in Telecommunications at the Catholic University of Santiago of Guayaquil, which is aimed at readers know the characteristics, design and implementation **IP/MPLS** network for Telecommunication service provider. His planning and structure developed by simulating approach, will show as an **IP/MPLS** network may provide additional services, that a purely IP network simply not possible provide it.

With the **Layer 3 MPLS VPNs**, through the VRF (Virtual Routing Forwarding) virtual routing tables will be created, thus generating a single routing table for each customer or service you want to provide such as Voice, Data and Internet; without the private network can stick together, thus allowing reuse of private IP addresses. Likewise the **Layer 2 MPLS VPNs** with which connections Point to Point is created through a virtual container (VC) giving the customer full control of the routing table, so the ISP does not participate in the routing process unlike MPLS L3 VPN.

Simulation approach, elaborates in a controlled environment, under the GNS3 platform, the Cisco brand equipment (Models 7600 and 3725). The processes performed in real environments can be simulated, ensuring that the network performance is expected when deploying to real devices. The GNS3 Platform is a very powerful tool and provides the ability to perform rigorous testing in a real network, may affect the performance of equipment and services falls causing economic losses for the company.

CAPITULO 1 : Descripción del proyecto de intervención

1.1 Antecedentes

Durante los últimos años es evidente como la tecnología ha ido evolucionando paulatinamente, principalmente en los servicios que a telecomunicaciones se refiere, generando cada vez mayor requerimiento de ancho de banda y prestaciones de servicios cada vez más especializados. Si bien la tecnologías en IP tienen las capacidades de seguridad y convergencia, estas características por si misma son reducidas o afectadas por el incremento del flujo de tráfico IP y los costos de los equipos debido a que requieren un mayor procesamiento. Es por esto que se requiere implementar sistemas confiables y que reduzcan el procesamiento de los equipos de la red de tal forma que se pueda brindar más y mejores servicios con todas las seguridades, para que los clientes puedan interconectar sus redes con los servicios diferenciados que este solicite.

1.2 Definición del problema

Con las necesidades actuales de servicios de telecomunicaciones una red puramente IP, posee desventajas en prestación y diferenciación de servicios, por lo que es sumamente importante para una empresa proveedora de servicios de internet determinar una solución.

1.3 Objetivos

Según lo descrito en los antecedentes y definición del problema se describirán tanto el objetivo general como el objetivo específico.

1.3.1 Objetivo Generales:

Proponer la implementación de una red IP/MPLS para ofrecer mejores servicios que una red IP, ATM o *Frame Relay*.

1.3.2 Objetivos Específicos:

- ✓ Establecer los conceptos básicos de una red IP/MPLS
- ✓ Diseñar la propuesta técnica de una red IP/MPLS para un ISP.
- ✓ Simular una red IP/MPLS diferenciando servicios de voz, datos e internet

1.4 Hipótesis

La utilización de una red IP/MPLS implicará la solución del problema planteado, contribuirá al soporte para la diferenciación de cualquier tipo de tráfico y permitirá un adecuado consumo de los recursos dentro de la red.

1.5 Metodología de la investigación

En el trabajo se aplicará un método experimental ya que predice lo que ocurrirá si se produce alguna modificación en la condición actual de un hecho (por ejemplo en las caída de enlaces los paquetes conmutan por enlaces de respaldos, o al limitar el Bandwidth de un determinado servicio), para lograr esto aplica el razonamiento hipotético-deductivo y una metodología cuantitativa ya que los resultados se pueden medir y visualizar. Los experimentos pueden realizarse en el laboratorio o en el campo ya que se manipula una o más variables independientes, ejerciendo el máximo control y estableciendo las condiciones necesarias o adecua a las existentes, que son de utilidad en la tesis.

CAPITULO 2 : Introducción a la MPLS

2.1 Qué es MPLS?

Las soluciones tradicionales presentan diferentes problemas al momento de inter-operar con productos de diferentes fabricantes. Estas soluciones utilizaban para transportar la tecnología ATM, ya que podían operar sobre infraestructuras de transmisión mixtas (SONET/SDH, *Frame Relay*, PPP, y LANs. Esta es la necesidad que se tuvo para obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace, de modo que el Grupo de Trabajo de MPLS (establecido en el IETF en 1997) se propuso como objetivo la adopción de un estándar inter-operativo y unificado. (Canalis)

MPLS (Multi-Protocol Label Switching) es un estándar de arquitectura multinivel que puede soportar cualquier tipo de tráfico independiente del transporte de datos. La tesis será llevada a cabo con tráfico IPv4, que junto con las bondades de la MPLS se busca llevar las funciones de enrutamiento solamente a los equipos de borde de un dominio de red, evitando así realizar tareas de enrutamiento en el interior de dicho dominio. De esta manera, en el interior del mismo solo se realizará la conmutación de etiquetas añadidas a cada paquete en el momento de entrada al dominio, con esto se estaría evitando que cada Router aumente su procesamiento puesto que ya no realizaría la revisión de cada paquete IP destino necesaria en una red IP tradicional.

MPLS es un método mejorado para el envío de paquetes a través de una red IP, utilizando información de etiquetas colocadas al ingresar al dominio MPLS. Las etiquetas se insertan entre la cabecera de la Capa 2 y el encabezado de capa 3, y que están contenidos en el Virtual Path Identifier (VPI) y Virtual Channel Identifier (VCI), similares a las tecnologías basadas en células tales como ATM. (Alwayn, 2001)

MPLS combina tecnologías de conmutación de Capa 2 con las tecnologías de enrutamiento de nivel 3. El principal objetivo de MPLS es crear una red flexible que proporciona un mayor rendimiento y estabilidad. Este

incluye capacidades de VPN que es el principal objetivo de la tesis y Traffic Engineering (TE), que ofrecen calidad de servicio (QoS) con múltiples clases de servicio (CoS).

En una red IP/MPLS (ver Figura 1-1), los paquetes entrantes se les asigna una etiqueta por un Edge Label-Switched Router (LSR). Los paquetes se reenvían a lo largo de un Label Switched Path (LSP), donde cada LSR hace decisiones de envío (forwarding) basados únicamente en el contenido de la etiqueta. En cada salto, el LSR quita la etiquetación vigente y aplica una nueva etiqueta. La etiqueta es despojada en el LSR de borde de salida, y el paquete se reenvía a su destino tal como se envió en el origen.

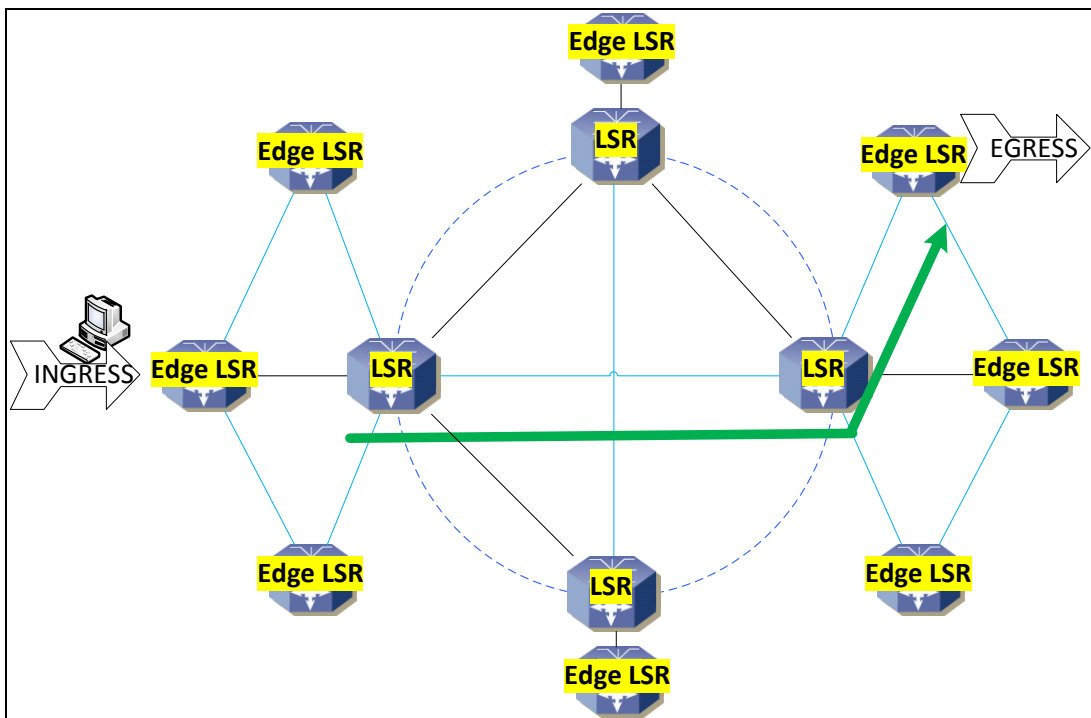


Figura 2.1.1: Diagrama de red IP/MPLS-Etiquetas

Fuente: El Autor

A pesar de que la parte MULTI-PROTOCOLO de MPLS es aplicable a cualquier Protocolo de la capa de red, en la tesis solo se hablará de IPv4 como parte del estudio.

Las principales ventajas que aporta MPLS al funcionamiento de una red pueden resumirse en:

- a) Redes Privadas Virtuales (VPN) - Es una de sus principales ventajas al permitir conectar a un cliente sobre una infraestructura compartida, bajo una VPN no habrá necesidad de realizar encriptación, ya que posee las funcionalidades de seguridad y red equivalentes a una red privada, integrando aplicaciones multimedia de datos, voz y video. Permitirá distinguir este tipo de tráfico y darle un tratamiento especial gracias a las etiquetas IP.
- b) Control de la Calidad de Servicio QoS - Con la utilización de MPLS Quality of Service (QoS), los Proveedores de Servicios pueden ofrecer clases de servicios, será compatible con los modelos IntServ y DiffServ. En el caso de las redes IP tradicionales, las direcciones de destino determinan el camino a seguir por el paquete a través de la red. Pero esto puede no ser eficiente en caso de congestión o para determinados paquetes “especiales” (Martinez). MPLS ofrece métodos para usar técnicas de encaminamiento más eficientes, proporcionando garantías necesarias para ofrecer un mejor servicio que la empresa lo considere prioritario sobre la red, tal como la voz.
- c) Ingeniería de Tráfico y control del enrutamiento del tráfico - Ofrece la posibilidad de configurar explícitamente trayectorias individuales o múltiples que el tráfico llevará a través de la red. También ofrece la posibilidad de configurar las características de rendimiento para una clase de tráfico. Esta característica optimiza la utilización del ancho de banda de caminos subutilizados, y concentra el tráfico en determinadas partes de la red. Esto será importante para optimizar los recursos más costosos de la red.
- d) Velocidad, retardo y jitter - El uso de etiquetas en el interior de la red IP/MPLS hace que el desempeño y los tiempos de respuesta sean mejores que una red IP tradicional. Esta mayor velocidad se traduce en un menor retardo y a su vez en un menor jitter (variación del retardo), un aspecto

importante para el caso de ciertas aplicaciones en tiempo real tales como el video y la voz.

- e) Escalabilidad – Una de las características de la red IP/MPLS es permitir asociar un gran número de redes IP a un número reducido de etiquetas. Esto hace que el tamaño de las tablas de etiquetas sea muy reducido, permitiendo a un router brindar servicio a una mayor cantidad de usuarios en la red. En el caso de las redes IP Privadas, estas puedan reutilizarse permitiendo así que dos clientes con la misma red (del rango de las privadas) compartan la plataforma del Proveedor de Servicio sin problema alguno ya que para el SP son simplemente etiquetas diferentes.

2.2 Aplicaciones del MPLS

Las principales aplicaciones que hoy en día tiene MPLS, sin que el orden reste mayor importancia entre ellas son:

- Servicio de Redes Privadas Virtuales (VPN)
- Diferenciación de niveles de servicio mediante clases (CoS)
- Ingeniería de tráfico

En los siguientes apartados se describirá de forma cada una de estas aplicaciones.

2.3 Arquitectura del MPLS

Desde el despliegue del precursor de la Internet - ARPANET - hoy en día, la arquitectura de la Internet ha estado en constante cambio. Su evolucionado es producto de los avances en la tecnología, el crecimiento y las ofertas de nuevos servicios. El cambio más reciente de la arquitectura de Internet es la adición de MPLS.

El impacto de MPLS ha sido en dos ámbitos, en el mecanismo de reenvío de paquetes IP y la forma en la que determina una ruta (la ruta de los paquetes deben tomar mientras transita por el Internet). Esto ha resultado en una arquitectura fundamental de la Internet.

La arquitectura MPLS describe los mecanismos para llevar a cabo la conmutación de etiquetas, que combina los beneficios de reenvío de paquetes basado en conmutación de Capa enlace con los beneficios de la capa de enrutamiento. Similar a las tecnologías de Capa 2 (por ejemplo, Frame Relay o ATM), MPLS asigna etiquetas a los paquetes para el transporte. El mecanismo de reenvío de toda la red es el intercambio etiqueta, en el que las unidades de datos (por ejemplo, un paquete o una trama) llevan una etiqueta corta, de longitud fija que indica a los nodos de conmutación localizados a lo largo de la ruta de los paquetes cómo transmitir y procesar los datos. (Headquarter, 2006)

La etiqueta MPLS se inserta entre el encabezado de Capa 2 y la Capa 3 de la trama de Capa 2, como se muestra en la Figura 2.3.1

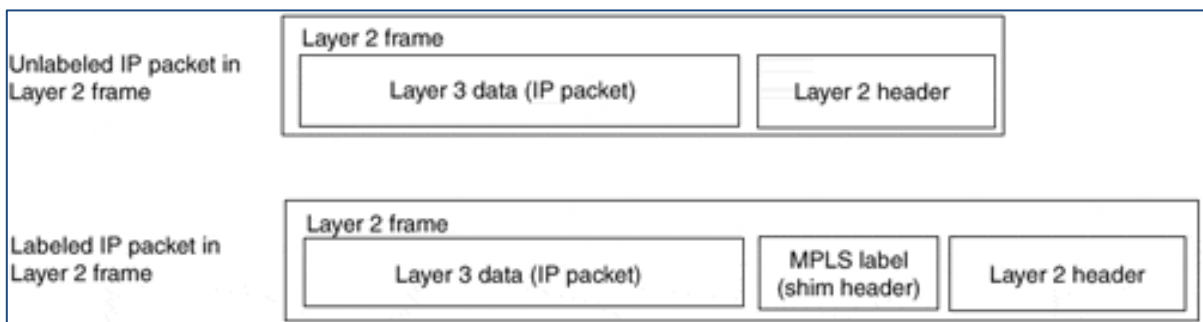


Figura 2.3.1: Posición de la etiqueta MPLS en la Trama de Capa2

Fuente: (Pepelnjak & Guichard, 201)

Se debe tener en cuenta que el mecanismo de transmisión de la Internet, que se basa en el enrutamiento basado en destino, no ha cambiado desde los días de ARPANET. Los cambios más importantes han sido la migración a Border Gateway Protocol Version 4 (BGPv4) de Exterior Gateway Protocol (EGP), la implementación de enrutamiento entre dominios sin clase (CIDR), y la actualización constante de los equipos de ancho de banda y los terminales, tales como routers más poderosos.

MPLS pueden simplificar el despliegue de IPv6 debido a que los algoritmos utilizados por reenvío de MPLS para IPv4 se pueden aplicar a IPv6 con el uso de los protocolos de enrutamiento que soportan direcciones IPv6.

MPLS está siendo implementado por muchas empresas Proveedoras de Servicios porque tiene un beneficio inmediato y directo a la Internet. El

beneficio más inmediato de MPLS con respecto a la red troncal de un proveedor de servicio de Internet es la capacidad de realizar ingeniería de tráfico permitiendo así descargar enlaces congestionados repartiendo la carga a través de enlaces subutilizados. Esto resulta en un grado mucho mayor de la utilización de recursos que se traduce en eficiencia y ahorro económico.

VPNs de Internet actualmente se implementan con IP Security (IPSec) túneles a través de Internet pública. Tales VPNs, a pesar de que trabajan son lentos. MPLS VPN a través de los ISP ofrecen VPNs basadas en Internet a los clientes con ancho de banda y de servicios de niveles comparables a los servicios tradicionales Frame Relay y ATM.

Los servicios IP VPN a través de redes backbone MPLS se puede ofrecer a un menor costo a los clientes debido a que la plataforma de aprovisionamiento, operación y mantenimiento de los servicios de VPN MPLS, son de fácil administración y requieren de poco personal capacitado según el tamaño de la red. Ingeniería de tráfico MPLS puede optimizar el uso del ancho de caminos subutilizados. Esto puede también resultar en un ahorro de costos que se pueden pasar al cliente.

La diferencia significativa entre las tecnologías tradicionales WAN MPLS y es la forma etiquetas se asignan y la capacidad para llevar una pila de etiquetas adheridas a un paquete. El concepto de una pila de etiquetas permite nuevas aplicaciones, como la ingeniería de tráfico, redes privadas virtuales, re direccionamiento rápido alrededor de enlaces y nodos fracasos, y así sucesivamente.

La arquitectura se divide en dos partes bien definidas: el Data Plane (Plano de datos) el cual cuida de reenvío en función de su dirección destino o etiquetas, y el componente de control (también llamado control plane) encargado del intercambio de información de enrutamiento y el intercambio de la etiqueta entre dispositivos adyacentes. En la figura 2.3.2 se puede visualizar la arquitectura básica de un componente MPLS con enrutamiento IP.

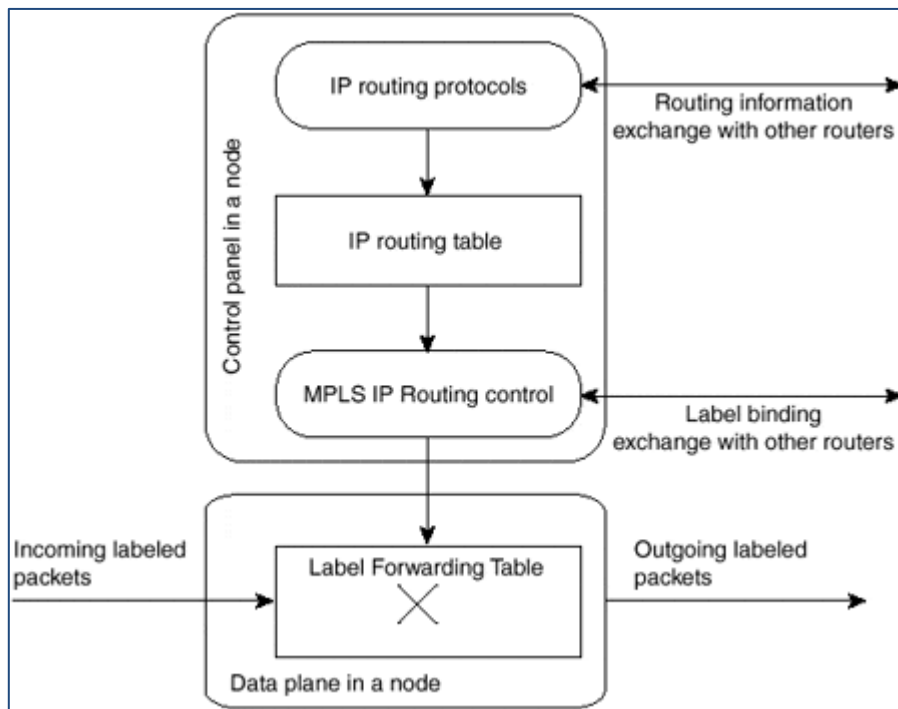


Figura 2.3.2: Arquitectura básica de un nodo IP/MPLS

Fuente: (Pepelnjak & Guichard, 201)

En los routers convencionales, la tabla de enrutamiento IP se utiliza para construir el caché de conmutación rápida o la Base de información Forwarding (FIB) utilizado por Cisco Express Forwarding (CEF). Sin embargo, en MPLS, la tabla de enrutamiento IP proporciona información sobre la red de destino y de subred prefijos utilizados para la unión etiqueta (Label), esta información se puede distribuir mediante el protocolo de distribución de etiquetas (LDP), llevando a cuentas la información vinculante etiqueta en la parte superior de los protocolos de enrutamiento modificados.

En la presente grafica 2.3.3 se registra la forma en la que interactúan los Planos de Control y de Datos. El plano de control MPLS es responsable de llenar y mantener el LFIB. Todos los nodos MPLS deben ejecutar un protocolo de enrutamiento IP como ISIS, OSFP, EIGRP, etc, para intercambiar información de enrutamiento IP con todos los demás nodos MPLS en la red.

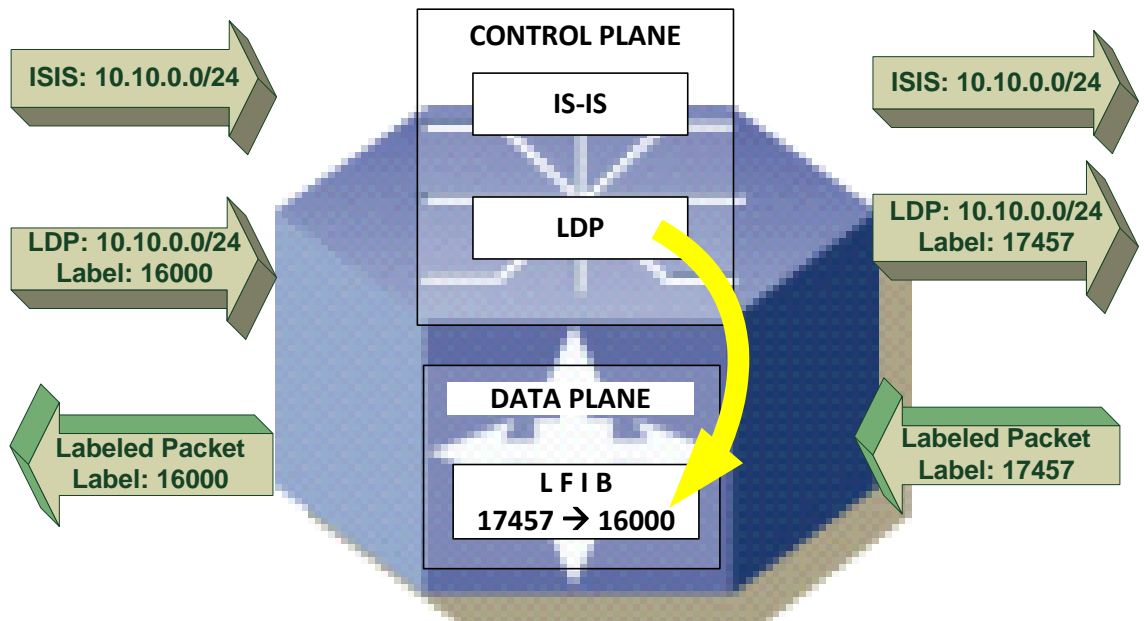


Figura 2.3.3 : División del funcionamiento interno del Router
(Control Plane | Data Plane)

Fuente: El Autor

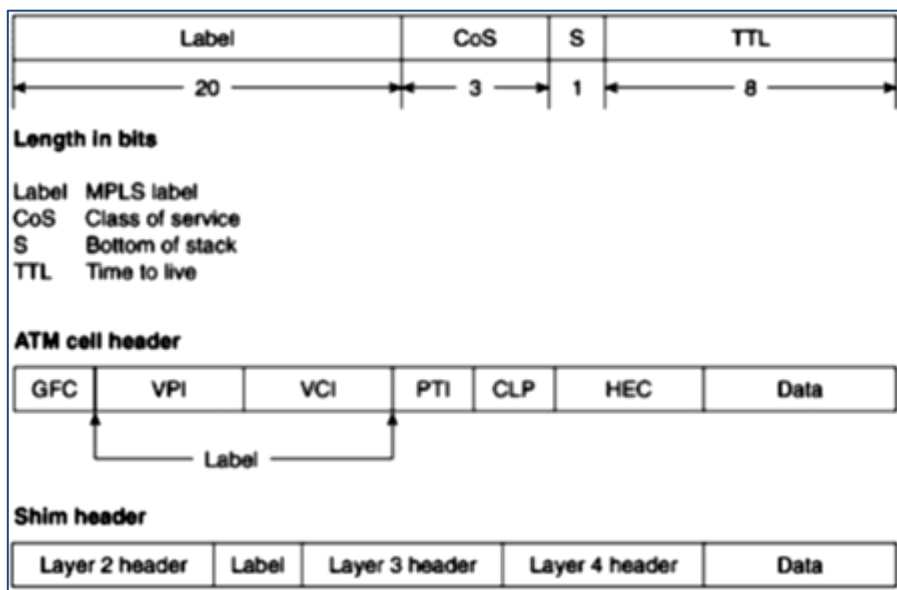


Figura 2.3.4 : Formato de la MPLS Label
(Alwayn, 2001)

Tabla 2.3.1 : Valores reservados de la Label

Label Description	
0	IPv4 explícito para el null Label. Este valor de la etiqueta es legal sólo en la parte inferior de la pila de etiquetas.
1	Etiqueta asignada para alertar al router. Esta etiqueta es análogo al uso de la opción de "alerta enrutador" en paquetes IP. Este valor de la etiqueta es cualquier lugar legal en la pila de etiquetas, excepto en la parte inferior.
2	IPv6 explícito para el null Label. Este valor de la etiqueta es legal sólo en la parte inferior de la pila de etiquetas.
3	Etiqueta nula implícita. Esta es una etiqueta que un nodo MPLS se puede asignar y distribuir, pero que en realidad nunca aparece en la encapsulación. Esto se utiliza en el penúltimo salto (penultimate hop popping).
4–15	Reservado para uso futuro.

Fuente: (Alwayn, 2001)

Los principales elementos funcionales de este protocolo son:

- a) LSR (Label Switch Router), son nodos MPLS capaces de enviar paquetes de nivel 3 nativos. Pueden ser internos o externos. Los LSR internos sustituyen etiquetas por otras, mientras que los externos añaden o eliminan etiquetas.
- b) FEC (Forwarding Equivalence Class), corresponde al conjunto de paquetes con similares atributos, tales como: dirección de destino, VPN, etc; o que requieren el mismo servicio (como multicast, QoS, etc.). El FEC se asigna en el momento en que el paquete ingresa al dominio MPLS, todos los paquetes con igual FEC siguen a un mismo camino LSP. (Ojeda & Sahily)
- c) LSP (Label Switching Path), es un camino lógico a través de uno o más LSR en el que se establece en un nivel de jerarquía que sigue un paquete de un FEC en particular. El Camino (Path) puede establecerse a través de protocolos de enrutamiento dinámicos o en forma manual.

- d) Etiquetas: son identificadores cortos, de longitud fija y con un significado local, utilizados para identificar un FEC. Un paquete puede tener una o más pilas de etiquetas, según su jerarquía. El apilamiento se produce cuando el paquete atraviesa dominios interiores hacia otros dominios. Un LSR siempre consultará a las cabeceras de nivel superior. Las etiquetas se adicionan, generalmente, entre las cabeceras de nivel 2 y 3.

Las tablas de enrutamiento o de envío se calculan con el empleo de bases de datos de estado de enlaces conjuntamente con las políticas de control de tráfico, como por ejemplo las características de los enlaces, la topología, los patrones de tráfico, etc. Esta es la información típica de los algoritmos de enrutamiento y es necesaria para que MPLS pueda establecer los caminos virtuales LSP's, para esto MPLS utiliza la propia información de enrutamiento a través de los protocolos de enrutamiento dinámicos internos IGP (OSPF, IS-IS, RIP, etc.), se genera un camino de etiquetas para cada ruta IP, por medio de la concatenación de las etiquetas de entrada y salida en cada una de las tablas de los LSR's. Para esto se vale de una Base de Información de Etiquetas, que no es otra cosa que una tabla indexada por etiquetas que se corresponden con un FEC.

También hay que mencionar al protocolo que se encarga de distribuir las etiquetas, y para dicho fin MPLS no asume un único protocolo de distribución de etiquetas. Por un lado, trabaja con el LDP (Label Distribution Protocol), desarrollado por el IETF, y por otro lado tenemos el RSVP (Resource Reservation Protocol) del IntServ.

Si lo que se necesita es suministrar calidad de servicio, el IETF ha desarrollado para MPLS el CR_LDP (Constraint-Based Routing Label Distribution Protocol), o una extensión del RSVP, y los fabricantes hasta ahora vienen utilizando una u otra alternativa.

2.4 Funcionamiento del MPLS

En el intercambio de etiquetas MPLS basa su funcionamiento, las que permiten el establecimiento de los diferentes caminos LSP a través de la red. Se tiene que tener en cuenta que los LSP son unidireccionales (un solo sentido), por lo que para el tráfico dúplex son necesarios dos LSP's, cada uno de estos LSP, se crea por la concatenación de uno o más saltos ó hops en los que se realiza el intercambio de etiquetas y a través de los cuales el paquete va de un LSR a otro. Estos LSR, son entonces routers especializados en el envío de paquetes etiquetados por MPLS.

LSRs Edge se encuentran en el punto de presencia (POP) límites de una red MPLS y aplica etiquetas (o una pila de etiquetas) a los paquetes. Imposición de etiquetas también se llama una acción de etiqueta empuje (*Push action*). Los LSRs Edge también realizan una disposición etiqueta o función de eliminación de etiqueta en el punto del dominio MPLS, que también se llama una acción de etiqueta pop salida (*Push action*). LSRs Edge también pueden realizar una función de reenvío IP convencional.

Los paquetes etiquetados por un LSR se enumeran en diferentes acciones de según la tabla 2.4.1

Tabla 2.4.1 : Acciones de la etiqueta MPLS

ACCIONES DE LA ETIQUETA	
Swap	Reemplaza con otro valor la etiqueta de pila Superior
Push	Reemplaza con un conjunto de etiquetas la etiqueta de la pila superior
Untag	Remueve la etiqueta superior y envía el paquete IP a un específico next hop.
Pop	Remueve la etiqueta superior y transmite la carga útil restante, ya sea como un paquete etiquetado o paquete IP no marcado.
Aggregate	Remueve la etiqueta superior y lleva a cabo la búsqueda de Capa 3

Fuente: Autor

Según lo establecido por el IETF el transporte de datos puede ser cualquiera, por lo que si fuera ATM, en una red IP habilitada MPLS, es mucho más fácil de gestionar que la solución clásica de IP/ATM (García). Esto es así porque no sería necesario administrar dos diferentes arquitecturas transformando las direcciones y las tablas de enrutamiento IP en las direcciones y tablas de encaminamiento ATM, ya que se resolvería con el intercambio de etiquetas MPLS. El transporte de datos basado en celdas quedaría restringido entonces al ATM. Mientras tanto, esto es indiferente para el MPLS, ya que puede implementar de forma indistinta otros transportes como Frame Relay o enlaces dedicados punto a punto. (Ojeda & Sahily)

Paralelamente, un LSP es el circuito virtual por el cual todos los paquetes asignados a una FEC son encaminados (Ojeda & Sahily). El primer LSR que ingresa en un LSP se lo denomina de entrada y el último salida o de cola, y ambos se encuentran obviamente en la frontera del dominio MPLS, tal como se muestra en la figura 2.4.1.

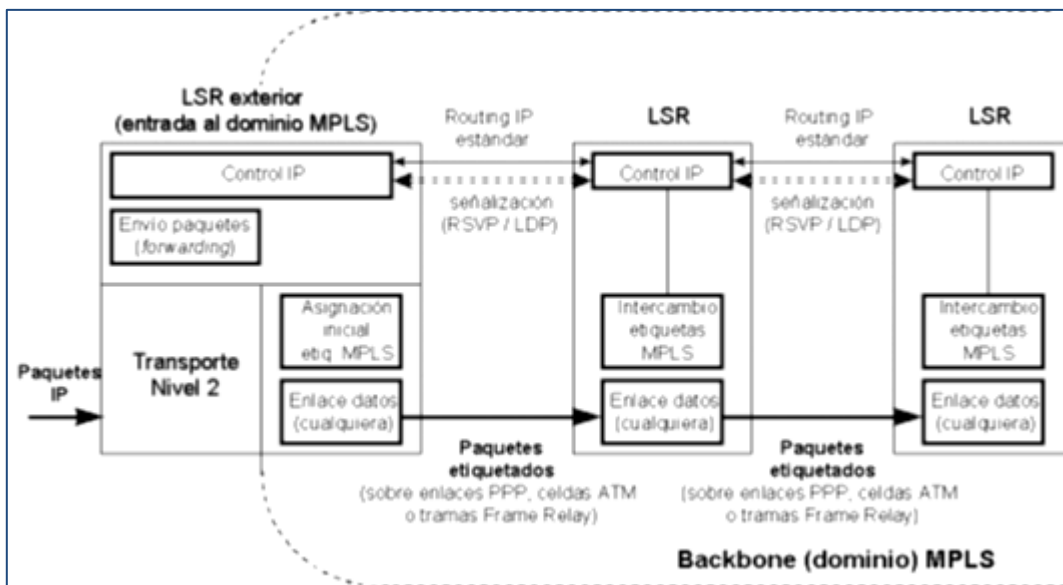


Figura 2.4.1 : Esquema Funcional de la MPLS

Fuente: (Canalis)

El funcionamiento de un LSR se basa en el intercambio de etiquetas según una tabla de envío. Esta tabla se construye en base a la información de encaminamiento que proporciona el control plane. Cada entrada de la tabla contiene un par de etiquetas, correspondientes a cada interfaz física de

entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz. (Canalis)

En la figura 2.4.2, se describe el funcionamiento de un LRS. El paquete que llega al LRS con la etiqueta 20 en la interfaz 2 de entrada, el LRS le asigna la etiqueta 11 y lo envía por el interfaz 6 de salida hacia el siguiente LRS, de acuerdo con la información contenida en la tabla de envío MPLS.

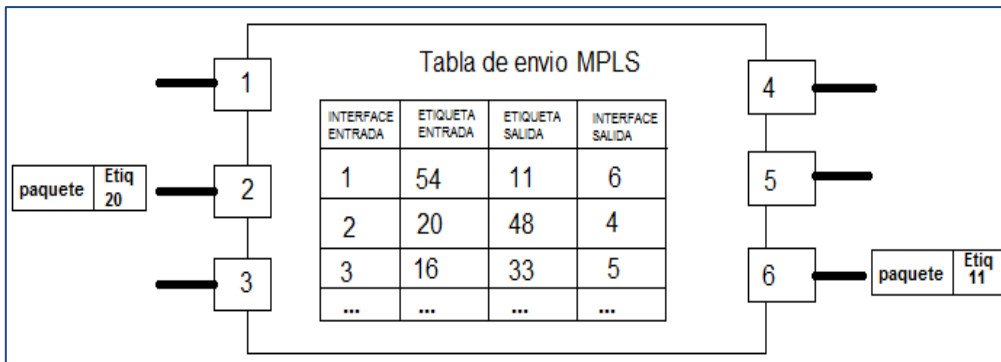


Figura 2.4.2 : Funcionamiento de un LRS del núcleo MPLS

Elaborado por el Autor

En la figura 2.4.3, se ilustra la forma en la que el paquete ingresa a la red sin etiqueta se genera el proceso de entrega dentro del dominio MPLS, en este punto los LRS ignoran la cabecera IP, y analizan la etiqueta de entrada, consultando la tabla de envío MPLS y reemplazándola por otra totalmente nueva. Al llegar al EDGE LRS, ultimo router del dominio MPLS, procede a sacar la etiqueta y enviar el paquete como originalmente había ingresado al dominio MPLS. (Canalis)

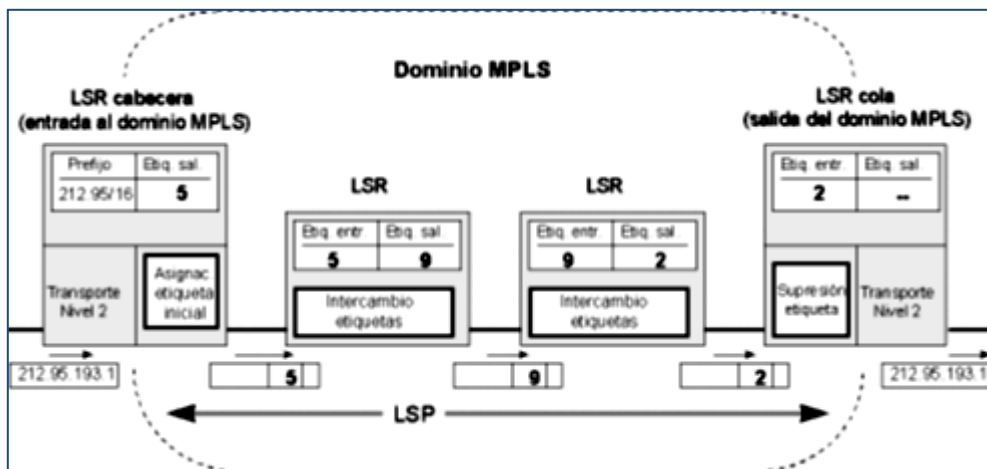


Figura 2.4.3 : Envío de un Paquete por un LSP

Fuente: (Canalis)

2.5 Habilitando MPLS

Para utilizar MPLS en una Plataforma Cisco, se tiene que activar de forma global y configurar de forma explícita en las interfaces de UpLink que interconectan los P y Pe. Comenzando en el modo EXEC privilegiado, se debe llevar a cabo los pasos detallados en la tabla 2.5.1, para implementar MPLS a través de una red Cisco.

Tabla 2.5.1 : Pasos para configurar MPLS en un Router Cisco

#	Comandos para habilitar MPLS	Significado
1	configure terminal	Configuración en modo Global
2	ip cef	Habilita de forma global una funcionalidad de envío y conmutación propietaria de cisco
3	mpls ip	Habilita envío MPLS de paquetes de longitud IPv4, normalmente caminos enrutados por la plataforma
4	mpls label protocol ldp	Habilitando etiquetado LDP
5	mpls ldp advertise-labels [for prefix-access-list]	Habilitando MPLS label advertising en el switch. Si no se incluyen palabras clave, no hay restricciones en el que se anuncian las etiquetas.
6	interface interface-id	Ingresando a la interface física
7	mpls ip	Habilita envío MPLS de paquetes de longitud IPv4, normalmente caminos enrutados en la interface en particular
8	end	Saliendo del modo global
9	show mpls forwarding table	Muestra contenido de la base de información de envío de etiquetas (FIB)
10	show mpls interfaces	Muestra la información de una o más interfaces que han sido configuradas para MPLS
11	copy running-config startup-config	Guardando la configuración.

Fuentes: (Cisco)

2.6 Redes privadas Virtuales (VPN)

Las VPNs son redes privadas de comunicaciones punto a punto o punto a multipunto que brindan conectividad por medio de una infraestructura compartida. Es importante comprender a fondo el concepto de las VPNs dado que de esa forma se podrá determinar cuándo una organización necesita de una VPN y como las MPLS puede ayudar a ahorrar mucho tiempo y dinero. (Cisco S. , 2000)

Las VPNs tienen sus bases iniciales en X25 y Frame Relay, estas reemplazan los enlaces dedicados P2P con enlaces P2P emulados compartiendo una infraestructura de red.

Los servicios de VPN son ofrecidos de dos grandes maneras:

- a) **VPNs Peer to Peer:** En este modelo el proveedor de servicio participa en el enrutamiento del cliente activamente, se convierte en responsable para la convergencia del cliente y los PE's llevan todas las rutas de todos los clientes. El único percance con este método es que proveedor de servicio tiene conocimiento de enrutamiento IP del cliente.
- b) **VPNs Overlay:** En este modelo el proveedor de servicio proporciona conexiones virtuales P2P en Nivel 2 (Modelo OSI) entre los sitios del cliente. El implementar enrutamiento óptimo requiere que se tenga un full mesh de circuitos virtuales, los circuitos virtuales deben ser proporcionados manualmente, el ancho de banda debe ser provisionado sitio a sitio y siempre incurren en encapsulación de sobre cabeceras.

MPLS ofrece muchas ventajas en cuanto a este tipo de redes, que son mucho más económicas y eficaces frente a otras soluciones tradicionales. Las VPNs basadas en MPLS permiten a los proveedores de servicios implementar soluciones escalables y construir el establecimiento para ofrecer servicios de valor agregado que justifiquen el por qué estos **deberían migrar sus clientes a MPLS VPNs L2 o L3** según sea sus necesidades.

2.6.1 MPLS VPN

Para un Proveedor de Servicio, el uso de MPLS VPN, le proporciona la capacidad de implementar y administrar los servicios de Capa 3 troncales VPN escalables, incluyendo aplicaciones, Data Center, los servicios de telefonía a clientes empresariales, etc. MPLS VPN es una red IP segura que comparte recursos en uno o más redes físicas, contiene sitios geográficamente dispersos que pueden comunicarse de forma segura a través de una red troncal compartida. El conocimiento adquirido de la arquitectura de las VPNs en MPLS ayudará para diseño y parámetros de configuración.

La siguiente figura muestra una red MPLS VPN que conecta dos sitios de una red IP que pertenece a un cliente.

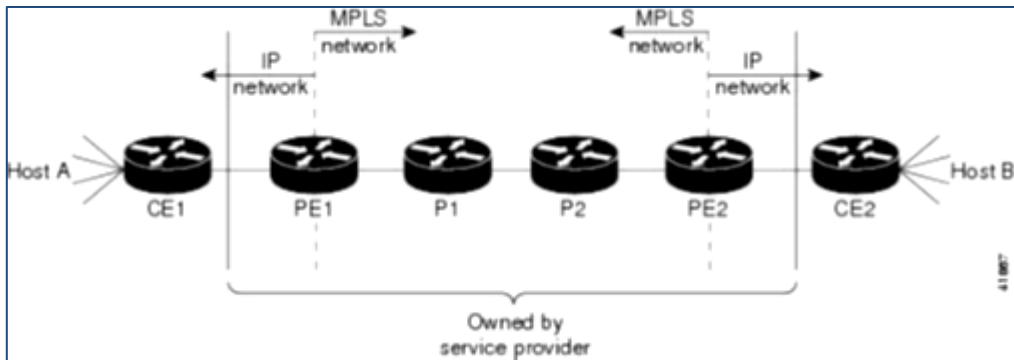


Figura 2.6.1 : ESQUEMA MPLS VPN con clientes

Fuente: (Headquarters, MPLS Basic MPLS Configuration Guide, 2011)

En la figura 2.6.1, los paquetes IP que salen del host A, ingresan a la red del Proveedor mediante el CE1 sin sufrir alteraciones hasta ahí son enviados al PE1, en este punto se les asignan una etiqueta (Label) con la cual viajan por todo el Backbone los P1 y P2, dependiendo del requerimiento del clientes y el tipo de tráfico que este envíe (voz, datos o internet) los paquetes pueden tener determinadas preferencia sobre la red. Una vez que llegan al PE2 a través del mecanismo denominado Penultime hop popping, el router de borde del proveedor quita la etiqueta de los paquetes que son entregados al CE2 integro tal como ingresaron al CE1, de esta forma concluyen su trayecto y se establece la comunicación entre los dos Host. Las nomenclaturas de los símbolos encontrados en la figura anterior se los detalla en la tabla 2.6.1.

Tabla 2.6.1 : Simbología del esquema MPLS VPN

Significado de los símbolos	
CE	Equipamiento que el Proveedor de Servicio instala al cliente - <i>Customer Equipment</i>
PE	Equipo de Frontera o de Borde (edge), generalmente sus enlaces son de 1G, equipo subtiende a los Switch y Clientes del Proveedor de Servicio - <i>Service Provider Edge router</i> .
P	Equipo de Core del Backbone, generalmente con enlaces de alta capacidad (10G) denominado Label-Switched Router (LSR), este equipo no tiene conectividad con la red del cliente - <i>Service Provider router</i> .
1,2...	Numeración generada para organización de la plataforma

Elaborado por el Autor

Mediante el uso de Extensión Multiprotocolo para BGP (MP-BGP), se encuentra una etiqueta para una red destino de VPN y el IGP es la columna vertebral que proporciona la ruta óptima hacia la dirección del siguiente salto. MPLS VPN depende de enrutamiento de VRF para aislar los dominios de enrutamiento entre sí. Cuando las rutas se aprenden a través de una MPLS VPN, el PE aprende la nueva ruta como ruta VRF normal, excepto que la dirección MAC destino para el siguiente salto no es la dirección real sino una dirección de forma especial que contiene un identificador que se asigna para la ruta. Cuando se recibe un paquete MPLS VPN en un puerto, el PE busca las etiquetas en la tabla de enrutamiento para determinar qué hacer con el paquete y enviarlo al destino.

Por tanto para levantar MPLS necesariamente se debe de habilitar BPG y los equipos deben soportar estas características, para un mejor control se deberá establecer por lo menos dos Router Reflector con los que todos los PE establecerán sesiones BGP.

MPLS VPN admite full conectividad entre las instalaciones del cliente (equivalente a la plena malla de las redes VPN de superposición) sin tener que configurar nada manualmente el cliente final. El proveedor sólo necesita configurar la VPN en el borde de proveedor (PE) routers.

El llamado topología "hub-and-spoke", que se usa principalmente para reducir el costo de la red, ya no es necesario. La interconexión de los sitios entre los CEs se hace de forma automática mediante el uso de BGP y un IGP para encontrar el camino más corto.

La Arquitectura MPLS VPN por defecto proporciona enrutamiento óptimo entre sitios CE. El Cliente CE1 puede tener enrutamiento interno completo para su VPN o simplemente una ruta por defecto que apunta al router PE1. Los routers PE, sin embargo, necesitan tener la información completa de enrutamiento para la red MPLS VPN con el fin de proporcionar conectividad total y el encaminamiento óptimo.

2.6.2 Implementación de MPLS L2VPN

ATOM es una solución para el transporte de Capa 2 a través de una red MPLS, permitiendo a los proveedores de servicio utilizar la red MPLS para

proporcionar conectividad entre dos sitios a través de la capa de enlace sin que se llegue a la capa de Red IP, simulando una LAN extendida. En lugar de redes separadas con entornos de gestión de red, los proveedores de servicios pueden utilizar la red MPLS para transportar datos en capa dos para los distintos clientes o servicios tales como PPPoE, QnQ o enlaces Punto a Punto en capa 2. (L. Martini, Exist, Level 3 Communications, E. Rosen, N. El-Aawar, & Cisco Systems)

Para transportar tráfico Ethernet de Capa 2 también denominada EoMPLS, se encapsula tramas Ethernet en paquetes MPLS y las envía a través de la red MPLS. Cada trama es transportada como un solo paquete, y los PE conectados al backbone remueven y adhieren las etiquetas según lo requiera.

El backbone MPLS utiliza las etiquetas de túnel para transportar el paquete entre los PE. El PE de salida utiliza la etiqueta VC para seleccionar la interfaz de salida para el paquete Ethernet. Los túneles EoMPLS son unidireccionales; para EoMPLS bidireccionales, es necesario configurar un túnel en cada sentido y así poder levantar el psedowires.

En la tabla 2.6.2 se puede visualizar paso a paso la forma en la que se recomienda configurar Ethernet sobre un dominio MPLS en una interface, en una plataforma Cisco.

Tabla 2.6.2 : Configurando Ethernet sobre MPLS en una interface

Pasos	Comando
1.	enable
2.	config terminal
3.	interface giga slot/port
4.	xconnect loop100-router-remoto vcid encapsulation mpls
5.	end
6.	show mpls l2transport vc vcid

Fuente: (Headquarters, MPLS Layer 2 VPNs Configuration Guide,, 2011)

En la tabla 2.6.3 se puede visualizar paso a paso la forma en la que se recomienda configurar Ethernet sobre un dominio MPLS en interface vlan para

luego entregarlo a un puerto troncal permitiendo así optimizar la plataforma, en una plataforma Cisco.

Tabla 2.6.3 : Configuración de MPLS L2VPN con Interface Vlan

Pasos	Comando
1.	enable
2.	config terminal
3.	interface vlan #vlan
4.	xconnect loop100-router-remoto vcid encapsulation mpls
5.	end

Elaborado por el autor

Para que levante el servicio del tunnel detallado en la tabla 2.6.2.2 se debe de asignar a una interface Modo Trunk o con EVC (Ethernet Virtual Connection). En las Tabla 2.6.4 y 2.6.5 se detallan estas dos configuraciones.

Tabla 2.6.4 : Configuración Modo Trunk

Pasos	Comando Modo Trunk
1.	enable
2.	configure terminal
3.	interface gigabitethernet slot /port
4.	switchport mode trunk
4.	switchport trunk allowed vlan [add] vlan-id
5.	end

Elaborado por el autor

Tabla 2.6.5 : Configuración EVC

Pasos	Comando EVC
1.	enable
2.	configure terminal
3.	interface gigabitethernet slot /interface
4.	service instance vlan-id ethernet
5.	encapsulation dot1q vlan-id
6.	rewrite ingress tag pop 1 symmetric
7.	bridge-domain vlan-id
8.	end

Elaborado por el autor

Es de aclarar que también existen las MPLS L2VPN Punto Multipunto, pero estas no son parte de este estudio.

2.6.3 Implementación de MPLS L3VPN

Las arquitecturas MPLS L3VPN difieren de manera importante de las tradicionales Peer to Peer ya que soportan el overlapping del espacio de direcciones IP, para permitir este Overlapping protocolos como BGP expanden los prefijos marcándolos con un identificador de 64bits llamado RD (Route Distinguishers). Lo que indica que la dirección del cliente pasará a tener 96 Bits en IPv4(32+64), de manera que sea globalmente única, a esto se le llama VPNv4 y son intercambiadas entre routers PE vía MP-BGP.

Los RD únicamente definen localmente el sitio VRF de un cliente. Es el identificador VPN que permite que la dirección sea globalmente única, y su formato está dado por *ASN:nn*, donde ASN es el sistema autónomo proporcionado por el IANA y *nn* es el número que el proveedor de Servicio asigna a las VRF. Los RT (Router Targets) fueron introducidos en la arquitectura MPLS L3VPN para soportar completas topologías VPN e identifica un sitio que participa en más de una VPN, por lo que es de significancia Global.

En la tabla 2.6.6 se puede observar los dos modos de operación del Route Target y en la figura 2.6.2 se refleja la operatividad y funcionalidad del RT.

Tabla 2.6.6 : Modos de Operación del RT

Modo Operación	Función
EXPORT:	Identifican la membresía de la VPN.
	Se agregan a la ruta del cliente cuando esta es convertida en prefijo VPNv4
IMPORT	Son asociados con cada VRF
	Selecciona las rutas a ser insertadas en la VRF

Fuente: (Ghein, 2006)

Comenzando en el modo EXEC privilegiado, se debe llevar a cabo los pasos detallados en la tabla 2.6.7, para implementar MPLS L3VPN a través de una red Cisco.

Tabla 2.6.7 : Implementando VRF (MPLS L3VPN)

Pasos	Comandos
1	enable
2	configure terminal

3	ip routing
4	ip vrf vrf-name
5	description nombre-servicio
6	rd route-distinguisher
7	route-target [import export both]
8	exit
9	router bgp AS
10	address-family ipv4 vrf vrf-name
11	redistribute connected
12	redistribute static
13	exit-address-family
14	interface vlan vlan-id
15	ip vrf forwarding vrf-name
16	end
17	show ip vrf
18	show ip route vrf vrf-name
19	ping vrf vrf-name ip-address-wan
20	copy running-config startup-config

Fuente: (Headquarters, MPLS Layer 3 VPNs Configuration Guide, 2011)

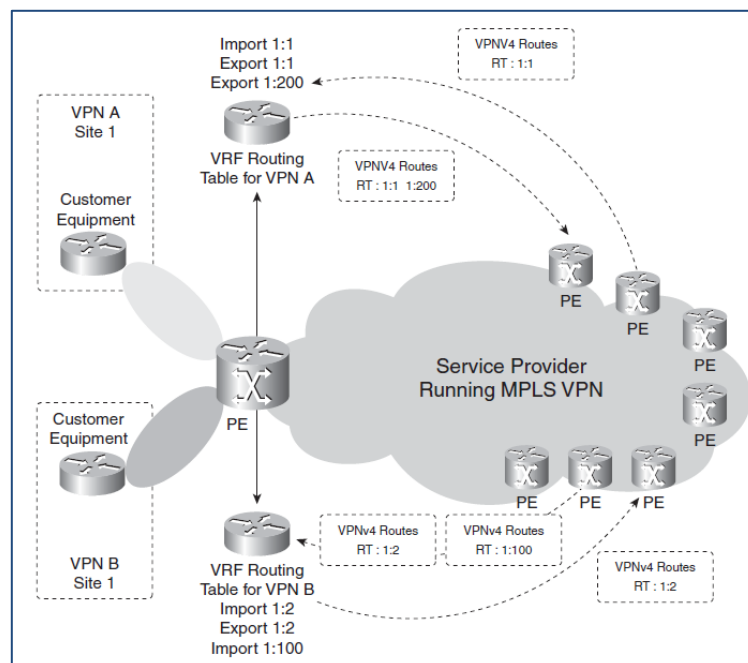


Figura 2.6.2 : Esquema funcional de los RD y RT

Fuente: (Ghein, 2006)

Puesto que el estudio se basa en el estudio de los servicio de MPLS L2VPN y L3VPN no se va a profundizar en el estudio del BGP, este será habilitado con las configuraciones básicas para que MPLS sea funcional.

CAPITULO 3 : DISEÑO Y DESARROLLO DE LA SIMULACION

3.1 Plan de implementación

En este capítulo se detallarán paso a paso más la simulación propuesta para establecer una red IP/MPLS escalable y confiable, con un ambiente controlado, bajo la plataforma GNS3. Los equipos de la marca Cisco (Modelos 7600 y 3745), son los óptimos para establecer la simulación y en un ambiente real son los más comunes para establecer el CORE y la DISTRIBUCION. Por medio de la simulación se pretende garantizar que el funcionamiento de la red sea el esperado al momento de implementarlo en los dispositivos reales. La Plataforma GNS3 es una herramienta muy poderosa y brinda la capacidad de realizar pruebas rigurosas, que de hacerla en una red real, pueda afectar el rendimiento de los equipos, provocando caídas de servicios y pérdidas económicas para la empresa.

3.2 Solución Propuesta.

El propósito del diseño se basa en la implementación de la red IP/MPLS en la cual un Proveedor de servicios de Telecomunicaciones busca fortalecer y expandir su plataforma tecnológica.

El diseño se basa en la configuración de los equipos routers Cisco de Core y Distribución, para efecto de la simulación se tomarán en cuenta cuatro routers 7600 de Core (**P**) y 6 Routers 3745 de Distribución (**PE**) y dos Route-reflectors, este es un modelo escalable para una red en crecimiento, sobre los cuales colocará los servicios de Voz, Datos e Internet.

3.3 Diagrama de interconexión

3.3.1 Físico

A continuación se muestra el diagrama físico general de la solución planteada para la red IP/MPLS, en la figura 3.3.1 se detallan todos los equipos que componen la red propuesta para la simulación. Las líneas negras representan enlaces de fibra ópticas sin ningún medio de transmisión de por medio, denominadas fibras oscuras, de la misma manera encontramos DWDM o SDH como medio de TX. En cada esquina de los enlaces se pueden observar los puertos de los equipos MPLS a los que se conectan las transmisiones. Las asignaciones de la IP y los hostname asignado se detallan más adelante.

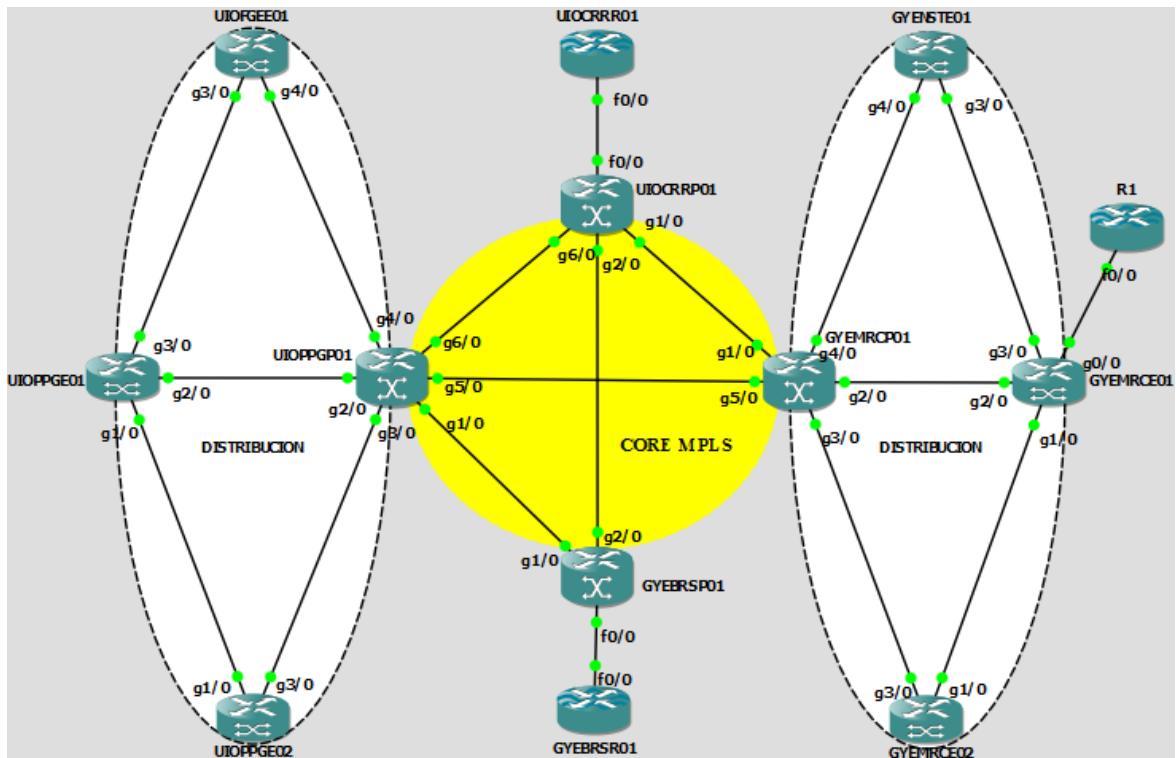


Figura 3.3.1 : Diagrama de interconexión red IP/MPLS

Elaborado por el autor

En la tabla 3.3.1 se resumen la función de cada uno de estos equipos.

Tabla 3.3.1 : Distribución equipos MPLS

NIVEL	EQUIPOS
CORE	GYEMRCP01
	GYBRSP01
	UIOCRRP01
	UIOPPGP01
DISTRIBUCION	GYENSTE01
	GYEMRCE01
	GYEMRCE02
	UIOFGEE01
	UIOPPGE01
	UIOPPGE02
REFLECTOR	GYBRSR01
	UIOCRRR01

Elaborado por el autor

3.3.2 Lógico

En el esquema lógico de la red se tienen las vecindades a nivel MP-BGP, ISIS y LDP como protocolos fundamentales en la implementación del BACKBONE IP/MPLS, a continuación se realizan algunas consideraciones a tener en cuenta en cada uno de los protocolos, así como esquemas de implementación y vecindades:

3.3.2.1 ISIS

El protocolo IGP a utilizar es IS-IS. Todos los nodos serán de nivel 2 y el área a utilizar es: 49.0008.0100.0800.XXXX.00 donde XXXX es el identificador del nodo loopback 100. Los criterios que se tomaron en cuenta son:

- a) Presenta una vista global de la red para una decisión de routing óptimo.
- b) Manejo eficiente de parámetros de operación tales como Utilización de CPU y memoria del equipo, ancho de banda de la red, enrutamiento.
- c) IS-IS tiene una rápida convergencia y es muy escalable, siendo un protocolo flexible que ha sido extendido para incorporar nuevas tecnologías como Multiprotocol Label Switching Traffic Engineering (MPLS/TE).
- d) Es recomendable que el IS-IS estén como Level2 dentro de la misma área.
- e) Se utilizará autenticación MD5 en el protocolo.

Por ende IS-IS será el IGP para la red MPLS, si un cliente requiere levantar su protocolo de enrutamiento dinámico, se hará a través de la vrf asignada a dicho cliente y se redistribuirá en BGP.

Las únicas redes que deben verse en la tabla de enrutamiento global son las siguientes redes:

- a) Direcciones Loopback globales de todos los equipos de la red IP/MPLS.
- b) Direcciones WAN de toda la red IP/MPLS.

Este direccionamiento se establecerá controladamente en base a un planeamiento IP establecido en los próximos capítulos.

3.3.2.2 LDP

El protocolo que se utilizará para el intercambio de Labels en la red IP/MPLS será LDP, de acuerdo a los estándares, se establecerán sesiones LDP entre todos los equipos vecinos de manera conjunta a las sesiones de ISIS, para tal fin se utilizarán como identificadores las loopbacks.

El comando a utilizar para establecer las sesiones es el siguiente:

```
mpls ldp neighbor ip-address-loopback-next-hop password 7 password
```

3.3.2.3 MP-BGP

Este protocolo será utilizado debido a que permite transportar una gran cantidad de prefijos, los cuales estarán ligados a una importante cantidad de atributos.

A nivel de iBGP necesario en la red para la implementación de IP/MPLS-VPN se debe contar con un esquema de Route-Reflectors para que la red sea escalable y el crecimiento no implique impacto en la red, para esto el esquema ideal propuesto es el contar con al menos dos dispositivos que cumplan dicha función exclusivamente, tal como se detalla en la figura 3.3.1 los equipos asignados para este propósito son (GYEBRSR01 y UIOCR01).

3.4 Políticas de Nombres y direccionamiento IP

3.4.1 Nombres de Equipos

La definición de nombres para los equipos de la red se ha realizado de la siguiente manera:

PROVINCIA			NODO			FUNC	SECUEN	
P	P	P	N	N	N	F	#	#

Figura 3.4.1 : Definición de Nombres de Equipos MPLS

Elaborado por el autor

PPP – Son tres caracteres que identifican la ubicación geográfica (Capital Provincial) donde están instalados los equipos, en donde se utilizara el código IATA internacional. Ejemplo: GYE – Guayaquil, UIO – Quito, CUE – Cuenca, etc.

NNN – Identificarán cada uno de los nodos dentro de cada ciudad, esta asignación se realizará de acuerdo a los parámetros identifique geográficamente en cada uno de los sitios, ya sea el nombre de un edificio, sector o particular a cada nodo, se establecerán solo consonantes y se eliminarán vocales. Es importante aun así garantizar que dicho identificador sea único en toda la red. Ejemplo: NOROESTE – NRS, CERRO AZUL – CRR, etc.

F – Corresponde a la función del equipo dentro de la red, corresponde a un acrónimo de una letra que identificará la función y objetivo de dicho dispositivo, los valores para F pueden ser:

- a) **P** – P de la red IP/MPLS
- b) **E** – PE de la red IP/MPLS
- c) **R** – Route Reflector
- d) **B** – Border Router
- e) **M** – Switch Metro


– Es un valor numérico que identifica en orden la cantidad de dispositivos que cumplen el rol definido por Función en la misma ubicación o nodo, siempre empezando por 01, dentro de su correspondiente función.






3.4.2 Identificadores de Equipos

La planificación propuesta tiene que ser jerárquica y escalable en el tiempo, para cumplir este objetivo se define un esquema de identificador de equipos, con el que se asignará el direccionamiento IP lógico y reglas a seguir para las diferentes sesiones de los protocolos.

En la tabla 3.4.1 se detallan los equipos simulados, la nomenclatura utilizada y el detalle

Tabla 3.4.1 : Tabla de Identificadores de equipos MPLS

FIGURA	NOMENCLATURA	DETALLE
	P – LSR	Equipo de Core

	PE – Edge LSR	Equipo de Distribución
	R – Route-Reflector Cisco	Equipo exclusivo para BGP peering, esencial para MPLS VPN
	FIBRA OSCURA	Enlace de 1G o 10G donde no existe equipo de Tx intermedio.
	DWDM	Tecnología más reciente (Multiplexado compacto por división en longitudes de onda), por redundancia es la más viable y se recomienda en el CORE.
	HOST – CLIENTE	Equipo simula al cliente y con el que se van a registrar el correcto funcionamiento de la red.

Elaborado por el autor

3.4.3 Direccionamiento IP - Loopback 100

En la tabla 3.4.2 se puede observar el planteamiento IP asignado a la red IP/MPLS. Para crear las IP de Loopback 100, el primer octeto siempre será el número 10 correspondiente a la Clase A privada según la *RFC 1918* (Rekhter & Moskowitz, 1996), el segundo octeto corresponde a la región a la que pertenece, para efecto de simulación se han planteado dos regiones R1-Pacífico y RG2-Andina - pueden aumentarse según las necesidades-, el tercer octeto identifica la secuencia de los equipos perteneciente a las regiones, números bajos identifica equipo del Core según la funcionabilidad los P y del 10 en 10 para identificar a los equipos de distribución los PE de diferente nodos, para los PE que correspondan al mismo nodos se le suma 1 al segundo octeto del PE ya existente, el número 100 en este octeto es reservado para los Route Reflector y el último octeto será siempre el número 100 para identificar los Router pertenecientes al Backbone de la red, la máscara a usar será la 255.255.255.255 (/32) según la RFC 1518 (Yakov & Li, 1993).

Tabla 3.4.2 : Ip Planning Loopback 100

NIVEL	REGION	NOMBRE NODO	EQUIPOS	IP LOOKBACK 100 /32
CORE	R1	MARACAIBO	GYEMRCP01	10.1.1.100
	R1	BRASIL	GYEBRSP01	10.1.2.100
	R2	PPG	UIOPPGP01	10.2.1.100
	R2	CERRO	UIOCRRP01	10.2.2.100
DISTRIBUCION	R1	MARACAIBO	GYEMRCE01	10.1.10.100
	R1	MARACAIBO	GYEMRCE02	10.1.11.100
	R1	NUSITA	GYENSTE01	10.1.20.100
	R2	PPG	UIOPPGE01	10.2.10.100
	R2	PPG	UIOPPGE02	10.2.11.100
	R2	FAGEE	UIOFGEE01	10.2.20.100
REFLECTOR	R1	BRASIL	GYEBRSR01	10.1.100.100
	R2	CERRO	UIOCRRR01	10.2.100.100

Elaborado por el autor

3.4.4 Direccionamiento WAN

Para asignar las IP de WAN se le sumarán 50 al segundo octeto del P y PE de la loopback 100 perteneciente a cada equipo, es muy importante tener en cuenta que entre más bajo sea el segundo y tercer octeto de la loopback 100 más prioridad va a tener al momento de decidir dicho número, el tercer octeto se asignará de manera consecutiva según la prioridad ya mencionada, siempre se implementará con una máscara 255.255.255.252 (/30) (Yakov & Li, 1993).

Tabla 3.4.3 : IP Planning WAN

ORIGEN	DESTINO	RED WAN	IP WAN ORIGEN	IP WAN DESTINO	Broadcast
GYEMRCP01 1.1	UIOPPGP01	10.51.1.0	10.51.1.1	10.51.1.2	10.51.1.3
	UIOCRRP01	10.51.1.4	10.51.1.5	10.51.1.6	10.51.1.7
	GYEMRCE01	10.51.1.8	10.51.1.9	10.51.1.10	10.51.1.11
	GYEMRCE02	10.51.1.12	10.51.1.13	10.51.1.14	10.51.1.15
	GYENSTE01	10.51.1.16	10.51.1.17	10.51.1.18	10.51.1.19
GYEBRSP01	UIOPPGP01	10.51.2.0	10.51.2.1	10.51.2.2	10.51.2.3

1.2	UIOCRRP01	10.51.2.4	10.51.2.5	10.51.2.6	10.51.2.7
	GYEBRSR01	10.51.2.8	10.51.2.9	10.51.2.10	10.51.2.11
UIOPPGP01 2.1	UIOCRRP01	10.52.1.0	10.52.1.1	10.52.1.2	10.52.1.4
	UIOPPGE01	10.52.1.4	10.52.1.5	10.52.1.6	10.52.1.7
	UIOPPGE02	10.52.1.8	10.52.1.9	10.52.1.10	10.52.1.11
	UIOFGEE01	10.52.1.12	10.52.1.13	10.52.1.14	10.52.1.15
UIOCRRP01 2.2	UIOCRRR01	10.52.2.0	10.52.2.1	10.52.2.2	10.52.2.3
GYEMRCE01 1.10	GYEMRCE02	10.51.10.0	10.51.10.1	10.51.10.2	10.51.10.3
	GYENSTE01	10.51.10.4	10.51.10.5	10.51.10.6	10.51.10.7
UIOPPGE01 2.10	UIOPPGE02	10.52.10.0	10.52.10.1	10.52.10.2	10.52.10.3
	UIOFGEE01	10.52.10.4	10.52.10.5	10.52.10.6	10.52.10.7

Elaborado por el autor

3.5 Asignación de VRF, RD y RT

La definición de las VRF permitirá identificar los servicios que cada cliente tendrá dentro de la red IP/MPLS, para diferenciar estos servicios se han creado cuatro grandes grupos voz, datos e internet, dentro de estos grupos encontramos dos subgrupos masivos y corporativos. Adicional a estos tres grupos vamos a encontrar las VRF de administración diseñadas para la gestión remota de las plataformas que se interconecten a la red IP/MPLD, tales como DSLAM, MSAN, GPON, NODOS B, etc.

En la tabla 3.4.5 se detalla la nomenclatura que se llevará a cabo para diferenciar estos grupos, los nombres de las VRF tendrán una longitud máxima de 7 caracteres alfanuméricos, se definirán en letra minúscula los primeros tres dígitos corresponderán al tipo de servicio y de los cuatro siguientes corresponderán a la secuencia lógica generada **YYYY**.

Tabla 3.5.1 : Nomenclatura del nombre de la VRF

Servicios	Tres primeros Dígitos Alfabéticos	Cuatro Dígitos Numéricos restantes
VOZ	voz	YYYY
DATOS	dat	
INTERNET	int	
ADMINISTRACION	adm	

Elaborado por el Autor

Los criterios para elaborar los RD y DT si bien en su contexto general son simples, los criterios con los que se basará la simulación se consideran como los más óptimos para tener una plantilla en la cual el Service Provider se pueda regir para un mejor control.

El RD se basará en el formato *AS:nn*, donde el AS corresponde al Sistema Autónomo proporcionado por el IANA, y el *nn* corresponderá una aparte al identificativo del servicio y la otra estará conformada por a los cuatro dígitos numéricos correspondiente al nombre de la VRF (ver tabla 3.5.1). En la tabla 3.5.2 se resumen los criterios para elaborar el RD en la red IP/MPLS.

Tabla 3.5.2 : Nomenclatura de la RD

Servicios	AS	Identificativo del Servicio	Cuatro Dígitos del nombre de la VRF
VOZ	65000	10	YYYY
DATOS		20	
INTERNET		30	
ADMINISTRACION		40	

Elaborado por el Autor

El RT generalmente es el mismo valor de la RD, solo para el caso de VRF complex cambian el import y export al momento de crear el servicio.

3.6 Seguridad

La seguridad es una parte primordial en una red ya que a través de esta aseguramos que equipos ajenos a la red ingrese a formar parte de ella, para el caso de la IP/MPLS se centrar en dar seguridades al LDP, IS-IS y BGP que conforman los puntos claves para que la red funciones correctamente.

No se va a plantear un formato para la misma ya que perdería su sentido, en la simulación se colocará una clave encriptada para levantar los servicios.

Tabla 3.6.1 : Comando de seguridad LDP, ISIS y BGP

Protocolo	Comando
LDP	<code>mpls ldp neighbor <i>ip-100-neighbor</i> password 7 <i>password-encrypted-ldp</i></code>

IS-IS	<pre> key chain ISIS key 1 key-string 7 password-encrypted-isis router isis 1 authentication mode md5 level-2 authentication key-chain ISIS </pre>
BGP	<pre> router bgp AS neighbor ip-100-routereflector password 7 password-encrypted-bgp </pre>

Elaborado por el Autor

3.7 Desarrollo lógico del esquema

En el anexo 1 se pueden observar las configuraciones lógicas de cada uno de los equipos de la Red IP MPLS. En este capítulo se van a detallar los puntos primordiales para que se pueda poner en producción la red planteada

En la figura 3.7 se puede observar la implementación del IP Planning propuesto del CORE de la red, acorde a lo establecido en el tema Políticas de Nombres IP – Loopback 100, los equipos de distribución se los omiten, pero pueden ser corroborados en el anexo 1.

Se precisa que para los equipo de CORE no se configuran BGP puesto que no participan en el proceso para habilitar las L3VPN. Por lo que solo se va a encontrar configuración de MPLS, LDP, ISIS y QoS.

El uso de los Route reflector es de gran importancia puesto que reduce procesamiento en los equipos y la configuración de BGP de los PE, puesto que todos los equipos de la red van a establecer secciones BGP únicamente con dos equipos de la red, en caso de que uno falle no habrá afectación de servicio puesto que siempre va a ver otro que este anunciando las redes por MP-BGP. Los dos equipos dedicados a que sean Route Reflector no tendrán servicios de clientes conectados directamente pero sí tendrán configurado MPLS.

3.7.1 Comprobación del IS-IS

Con el comando **show isis neighbor**, visualizamos los equipos directamente conectados que establecen sesión IS-IS con el PE y a través de comando **show isis route**, se refleja la tabla de enrutamiento total del IGP, el resultado es este comando tiene que reflejar todas las WAN y Loopback100 de la red y el principal indicativo de para poder levantar los servicios MPLS, en la figura 3.7.1 y 3.7.2 se confirman los resultados esperados, ya que aprende todas las redes resumidas en la tabla 3.4.2 y 3.4.3.

```
GYEMRCE01#show isis neighbors
```

System Id	Type	Interface	IP Address	State	Holdtime	Circuit Id
GYENSTE01	L2	Gi3/0	10.51.10.6	UP	20	00
GYEMRCP01	L2	Gi2/0	10.51.1.9	UP	19	01
GYEMRCE02	L2	Gi1/0	10.51.10.2	UP	20	00

Figura 3.7.1 : Tabla de vecinos IS-IS

Elaborado por el Autor

```

GYEMRCE01#show ip route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 29 subnets, 2 masks
i L2  10.2.100.100/32      [115/120] via 10.51.1.9, GigabitEthernet2/0
i L2  10.1.100.100/32     [115/130] via 10.51.1.9, GigabitEthernet2/0
i L2  10.51.1.16/30       [115/20] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.10.4/30       [115/170] via 10.51.1.9, GigabitEthernet2/0
C     10.51.1.8/30 is directly connected, GigabitEthernet2/0
i L2  10.52.1.12/30      [115/120] via 10.51.1.9, GigabitEthernet2/0
C     10.51.10.0/30 is directly connected, GigabitEthernet1/0
i L2  10.51.2.8/30       [115/130] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.10.0/30     [115/170] via 10.51.1.9, GigabitEthernet2/0
i L2  10.51.1.12/30     [115/60] via 10.51.10.2, GigabitEthernet1/0
                               [115/60] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.1.8/30      [115/120] via 10.51.1.9, GigabitEthernet2/0
C     10.51.10.4/30 is directly connected, GigabitEthernet3/0
i L2  10.51.1.0/30      [115/20] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.1.4/30     [115/120] via 10.51.1.9, GigabitEthernet2/0
i L2  10.51.2.0/30     [115/30] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.2.0/30     [115/120] via 10.51.1.9, GigabitEthernet2/0
i L2  10.51.1.4/30     [115/20] via 10.51.1.9, GigabitEthernet2/0
i L2  10.52.1.0/30     [115/30] via 10.51.1.9, GigabitEthernet2/0
i L2  10.51.2.4/30     [115/30] via 10.51.1.9, GigabitEthernet2/0
i L2  10.1.11.100/32   [115/50] via 10.51.10.2, GigabitEthernet1/0
C     10.1.10.100/32 is directly connected, Loopback100
i L2  10.2.10.100/32   [115/120] via 10.51.1.9, GigabitEthernet2/0
i L2  10.2.11.100/32  [115/120] via 10.51.1.9, GigabitEthernet2/0
i L2  10.2.1.100/32   [115/20] via 10.51.1.9, GigabitEthernet2/0
i L2  10.1.2.100/32   [115/30] via 10.51.1.9, GigabitEthernet2/0
i L2  10.2.2.100/32   [115/20] via 10.51.1.9, GigabitEthernet2/0
i L2  10.1.1.100/32   [115/10] via 10.51.1.9, GigabitEthernet2/0
i L2  10.2.20.100/32  [115/120] via 10.51.1.9, GigabitEthernet2/0

```

Figura 3.7.2 : Tabla de enrutamiento del IGP

Elaborado por el Autor

3.7.2 Comprobación del LDP

Para comprobar que el LDP está operativo vamos a usar el comando **show mpls ldp neighbor**, este es de vital importancia para levantar los servicios L2VPN y L3VPN, en la figura 3.7.2 se comprueba que el LDP está operativo en los dos equipos con los que se a probar los tres servicios que son motivo de estudio en el presente documento.

```

GYEMRCE01#show mpls ldp neighbor | i Peer
Peer LDP Ident: 10.1.1.100:0; Local LDP Ident 10.1.10.100:0
Peer LDP Ident: 10.1.11.100:0; Local LDP Ident 10.1.10.100:0
Peer LDP Ident: 10.1.20.100:0; Local LDP Ident 10.1.10.100:0

```

Figura 3.7.3 : Sesiones LDP establecidas hacia los Vecinos

Elaborado por el Autor

3.7.3 Comprobación del MP-BGP

Para comprobar la cantidad de prefijos que se está aprendiendo por MP-BGP se usará el comando **show ip bgp vpnv4 all summary**, el resultado que tiene que reflejarse será los prefijos que son redistribuidos en BGP a través de los route-reflector, ciertamente en la figura 3.7.4 se observan las dos sesiones correspondientes a los Route-reflector configurados en la Red IP/MPLS.

```

GYEMRCE01#sho ip bgp vpnv4 all summary | b Neighbor
Neighbor      V   AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
10.1.100.100  4 65000    88     50     71   0    0 00:35:47      3
10.2.100.100  4 65000    91     51     71   0    0 00:36:22      3

```

Figura 3.7.4 : Sesiones activas hacia los Route-reflector

Elaborado por el Autor

3.8 Pruebas de servicios diferenciados (voz, datos e internet)

Estas pruebas demostrarán la robustez de la red y confirmar la hipótesis planteada. Para la realización de las pruebas se trabajara en con los dos PE ubicados a los extremos de la red. Estos son el **GYEMRCE01** y **UIOPPG01**, tal como se muestra en la figura 3.8.1 y es donde albergarán los servicios que van a ser tema de estudio.

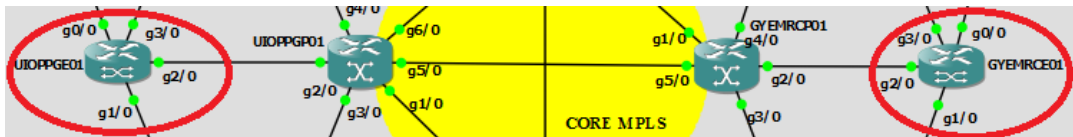


Figura 3.8.1 : Equipos para Pruebas de servicios

Elaborado por el Autor

3.8.1 Comprobando que los servicios estén operativos.

3.8.1.1 Servicios MPLS L3VPN

Se han creado tres servicios específicos, la tabla 3.8.1 detalla las VRF asignadas a cada servicio con las que se van a realizar las pruebas. A través de estos se van a comprobar que los diferentes servicios son absolutamente independientes compartiendo una sola plataforma, esto no se puede realizar en una red IP convencional, por lo que se corrobora el último objetivo específico establecido (*Simular una red IP/MPLS diferenciando servicios de voz, datos e internet*).

Tabla 3.8.1 : Datos clientes según el servicio.

Servicio	Nombre Vrf	Nombre Cliente	Red Origen	Red Destino
VOZ	voz1001	Cliente-A	10.10.10.0/30	10.10.10.4/30
DATOS	dat1010	Cliente-A	10.20.10.0/30	10.20.10.0/30
INTERNET	int1100	Cliente-B	10.10.10.0/30	10.10.10.4/30

Elaborado por el Autor

Las redes de voz del cliente-A y de internet del Cliente-B son iguales, pero estas no se sobrepone ni entran en conflicto de direccionamiento IP duplicada debido a que corresponden a diferentes VRF, una de las características importante de la MPLS. Hay que tomar en cuenta que al momento de configurar la primera IP disponible de la subred asignada se colocará del lado del PE y la segunda en el cliente, para el caso de las vlan se recomienda llevar un Vlan Planning o usar la una vlan disponible en el PE. En la tabla 3.8.2 se registra el planeamiento IP desde el PE hacia el cliente de cada servicio.

Tabla 3.8.2 : Planeamiento IP y Vlan de los servicios propuestos.

Nombre Cliente	Nombre Vrf	Vlan	Origen		Destino	
			IP del PE	IP del cliente	IP del cliente	IP del cliente
Cliente-A	voz1001	400	10.10.10.1/30	10.10.10.2/30	10.10.10.5/30	10.10.10.6/30
Cliente-A	dat1010	500	10.20.10.1/20	10.20.10.2/20	10.20.10.5/20	10.20.10.6/20
Cliente-B	int1100	600	10.10.10.1/30	10.10.10.2/30	10.10.10.5/30	10.10.10.6/30

Elaborado por el autor

Con el comando **show ip route vrf XXXX** comprobamos que las redes remotas se estén aprendiendo a través de la redistribución en BGP y las redes locales como directamente conectadas. Para comprobar conectividad punto a punto se usa el comando **ping vrf XXXX ip-destino-cliente** complementario a este comando esta la opción **source ip-origen-cliente** que nos permite discriminar de donde va a salir el requerimiento origen cuando tenemos ip secundarias dentro del servicio. En la figura 3.8.2 y 3.8.3 se determinan estas pruebas para cada uno de los clientes.

```
VOZ
GYEMRCE01#show ip route vrf voz1001
    10.0.0.0/30 is subnetted, 2 subnets
B       10.10.10.0 [200/0] via 10.2.10.100, 00:00:27
C       10.10.10.4 is directly connected, GigabitEthernet0/0.400

DATOS
GYEMRCE01#show ip route vrf dat1010
    10.0.0.0/30 is subnetted, 2 subnets
C       10.20.10.4 is directly connected, GigabitEthernet0/0.500
B       10.20.10.0 [200/0] via 10.2.10.100, 00:00:47

INTERNET
GYEMRCE01#sho ip route vrf int1100
Gateway of last resort is 10.2.10.100 to network 0.0.0.0


S       200.20.250.0/24 [1/0] via 10.10.10.6
    10.0.0.0/30 is subnetted, 2 subnets
B       10.10.10.0 [200/0] via 10.2.10.100, 00:01:18
C       10.10.10.4 is directly connected, GigabitEthernet4/0.600
B*     0.0.0.0/0 [200/0] via 10.2.10.100, 00:01:18
```

Figura 3.8.2 : Rutas aprendidas en las VRF

Elaborado por el Autor

Los códigos de cada uno de los protocolos se han omitido, para los resultados obtenidos se puede detallar los siguientes códigos: B – Ruta aprendidas por BGP, C – redes directamente conectadas, S – rutas estáticas del PE.

```

PRUEBA CONECTIVIDAD VRF VOZ
GYEMRCE01#ping vrf voz1001
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]: 10
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 184  dscp is ef
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 336/465/584 ms

```

```

CLIENTE_A_2#ping 10.20.10.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.20.10.2, timeout is 2 seconds:
!!!!!!!!!!!!
Success rate is 90 percent (9/10), round-trip min/avg/max = 532/700/876 ms
CLIENTE_A_2#sho run inter fast0/0.400
Building configuration...

Current configuration : 101 bytes
!
interface FastEthernet0/0.400
 encapsulation dot1q 400
 ip address 10.10.10.6 255.255.255.252
end

CLIENTE_A_2#ping 10.10.10.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 344/632/1324 ms

```

```

CLIENTE_A_2#sho run inter fast0/0.500
Building configuration...

Current configuration : 101 bytes
!
interface FastEthernet0/0.500
 encapsulation dot1q 500
 ip address 10.20.10.6 255.255.255.252
end

CLIENTE_A_2#ping 10.20.10.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.20.10.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 336/674/1092 ms

```

Figura 3.8.3 : Pruebas de los CE - Cliente A

3.8.1.2 Servicios MPLS L2VPN

Para comprobar este tipo de servicios se utilizará la solución de transporte AToM por medio de esta se encapsula tramas de nivel 2 en el ingreso PE y los envía a un PE remoto a través de un pseudowire, a la salida

el PE remoto quita la encapsulación y envía la trama de Capa 2. A esto se le suma la creación de un Tunnel de Ingeniería de tráfico que nos ayudará a manipular el cambio a seguir dentro de la red permitiendo así utilizar enlaces que no están siendo utilizados optimizando la red, estas siempre serán en un solo sentido.

Este tipo de servicios se los utiliza en la mayoría de los caso para establecer enlaces PPPoE entre cliente, BRAS y AAA; creados para servicios de internet masivos.

La figura 3.8.4 detalla las pruebas llevadas a cabo para la comprobación del servicio propuesto, se lo ha dividido en pruebas de operatividad y conectividad del pseudowire; y en la figura 3.8.5 demuestra la operatividad del Tunnel de ingeniería de tráfico.

```

GYEMRCE01#sho run inter gi4/0.700
Building configuration...

Current configuration : 151 bytes
!
interface GigabitEthernet4/0.700
 encapsulation dot1Q 700
 no snmp trap link-status
 no cdp enable
 xconnect 10.2.10.100 700 encapsulation mpls
end

GYEMRCE01#sho mpls l2transport vc 700

```

Local intf	Local circuit	Dest address	VC ID	Status
Gi4/0.700	Eth VLAN 700	10.2.10.100	700	UP

```

CLIENTE-B#sho run inter fast 0/0.700
Building configuration...

Current configuration : 102 bytes
!
interface FastEthernet0/0.700
 encapsulation dot1Q 700
 ip address 192.168.100.2 255.255.255.0
end

CLIENTE-B#ping 192.168.100.1 re 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 408/675/1216 ms

```

Figura 3.8.4 : Prueba de Operatividad y conectividad de la MPLS L2VPN.

Elaborado por el autor

```

UIOPPG01#show running-config inter tunnel2600
Building configuration...

Current configuration : 477 bytes
!
interface Tunnel2600
description ### TE_PPPOE_CLIENTE-B ###
ip unnumbered Loopback100
load-interval 30
tunnel destination 10.1.10.100
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 explicit name UIOE01_UIOP01_GYEP01_GYEE01
tunnel mpls traffic-eng path-option 20 explicit name UIOE01_UIOP01_RRP01_GYEP01
tunnel mpls traffic-eng path-option 30 dynamic
tunnel mpls traffic-eng record-route
no routing dynamic
ip rsvp bandwidth 800000
end
UIOPPG01#show mpls traffic-eng tunnels Tu2600
Name: ### TE_PPPOE_CLIENTE-B ### (Tunnel2600) Destination: 10.1.10.100
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit UIOE01_UIOP01_GYEP01_GYEE01 (Basis for Setup, path weight 30)
path option 20, type explicit UIOE01_UIOP01_RRP01_GYEP01_GYEE01
path option 30, type dynamic

Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled

InLabel : -
OutLabel : GigabitEthernet2/0, 38
RSVP Signalling Info:
Src 10.2.10.100, Dst 10.1.10.100, Tun_Id 2600, Tun_Instance 109
RSVP Path Info:
My Address: 10.2.10.100
Explicit Route: 10.52.1.5 10.51.1.1 10.51.1.10 10.1.10.100
Record Route:
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 10.52.1.5 10.51.1.1 10.51.1.10
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path Weight: 30 (TE)
Explicit Route: 10.52.1.5 10.51.1.1 10.51.1.10 10.1.10.100
History:
Tunnel:
Time since created: 1 hours, 29 minutes
Time since path change: 39 seconds
Current LSP:
Uptime: 39 seconds
Selection: reoptimization
Prior LSP:
ID: path option 30 [108]
Removal Trigger: path verification failed
Last Error: PCALC:: Can't use link 10.52.10.2 on node 10.2.11.100

```

Figura 3.8.5 : Configuración y prueba del Traffic Engineering

Elaborado por el Autor

3.8.2 Comprobando redundancia de la red MPLS VPN

Para establecer estas pruebas deliberadamente se apagaran uno de los dos Route-Reflector y luego la ruta principal entre el GYEMRCP01 y el UIOPPGP01 evidenciando que no se caigan los servicios de los clientes MPLS VPN y que todos los servicios converjan.

3.8.2.1 Apagando el Route-Reflector - GYEBRSR01.

En el mundo real es usual que los equipos se apaguen por problema de energía o algún Crash (termino referido a falla crítica de un dispositivo de red), producto del mal funcionamiento del mismo, por lo que la realización de esta prueba es sustentada y los resultados obtenidos valederos. En las figuras 3.8.6 y 3.8.7 se registran los eventos luego de que se apaga el route-reflector GYEBRSR01 (10.1.100.100), y la figura 3.8.8 detalla la operatividad de los servicios.

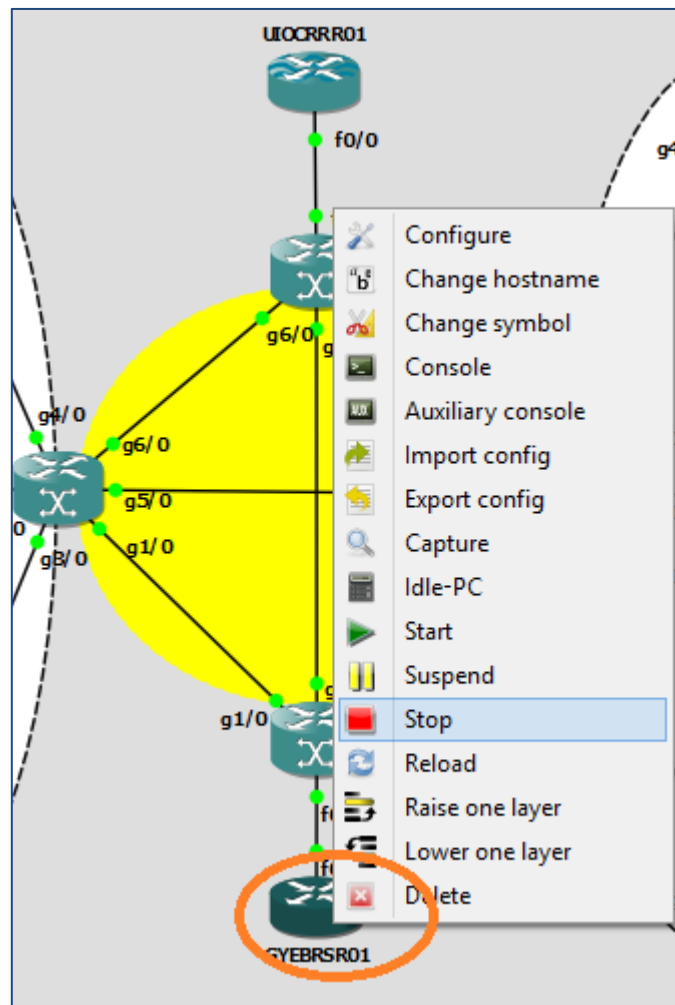


Figura 3.8.6 : Simulando afectación de RR (GYEBRSR01)

Elaborado por el Autor

```

ANTES DE APAGAR EL GYEBRSR01
GYEMRCE01#sho ip bgp vpnv4 all summary | b Neighbor
Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.1.100.100  4 65000    114    106     25   0    0 01:38:00    4
10.2.100.100  4 65000    109    106     25   0    0 01:38:12    4
GYEMRCE01#sho ip route vrf voz1001 10.10.10.0 | i (update|from)
  Last update from 10.2.10.100 01:37:50 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.1.100.100, 01:37:50 ago
GYEMRCE01#sho ip route vrf dat1010 10.20.10.0 | i (update|from)
  Last update from 10.2.10.100 01:38:04 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.1.100.100, 01:38:04 ago
GYEMRCE01#sho ip route vrf int1100 10.10.10.0 | i (update|from)
  Last update from 10.2.10.100 01:38:19 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.1.100.100, 01:38:19 ago

DESPUES DE APAGAR EL GYEBRSR01

GYEMRCE01#ping 10.1.100.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.100.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
GYEMRCE01#sho ip bgp vpnv4 all summary | b Neighbor
Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.1.100.100  4 65000    119    114     0    0    0 00:00:44  Active
10.2.100.100  4 65000    117    114     33   0    0 01:46:03    4
GYEMRCE01#sho ip route vrf voz1001 10.10.10.0 | i (update|from)
  Last update from 10.2.10.100 00:00:50 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.2.100.100, 00:00:50 ago
GYEMRCE01#sho ip route vrf dat1010 10.20.10.0 | i (update|from)
  Last update from 10.2.10.100 00:01:00 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.2.100.100, 00:01:00 ago
GYEMRCE01#sho ip route vrf int1100 10.10.10.0 | i (update|from)
  Last update from 10.2.10.100 00:01:15 ago
  * 10.2.10.100 (Default-IP-Routing-Table), from 10.2.100.100, 00:01:15 ago

```

Figura 3.8.7 : Resultados obtenido durante el proceso de pérdida de conectividad del RR Principal.

Elaborado por el Autor

Se aclarar que los servicios se mantienen operativos gracias al único Route-Reflector de la red el UIOCR01, para este caso se considera que la red va a contener más de 100 equipos, de ser una red pequeña no será necesario utilizarlos, simplemente usar un "full-mesh" es más simple.

```

CONECTIVIDAD DESDE EL CUSTOMER EQUIPMENT (CE)

CLIENTE-B#ping 8.8.8.8 re 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 252/490/884 m

interface FastEthernet0/0.600
  description ###CLIENTE_B_INTERNET###
  encapsulation dot1Q 600
  ip address 10.10.10.6 255.255.255.252
end

CLIENTE-B#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

 1 10.10.10.5 164 msec 188 msec 140 msec
 2 10.10.10.1 [MPLS: Label 27 Exp 0] 344 msec 392 msec 420 msec
 3 10.10.10.2 400 msec 404 msec 400 msec

CONECTIVIDAD DESDE EL SERVICE PROVIDER Edge (PE)

GYEMRCE01#sho run inter gig4/0.600
Building configuration...

Current configuration : 157 bytes
!
interface GigabitEthernet4/0.600
  encapsulation dot1Q 600
  ip vrf forwarding int1100
  ip address 10.10.10.5 255.255.255.252
  no snmp trap link-status
end

GYEMRCE01#traceroute vrf int1100 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

 1 10.51.1.9 [MPLS: Labels 35/27 Exp 0] 340 msec 336 msec 416 msec
 2 10.51.1.2 [MPLS: Labels 16/27 Exp 0] 352 msec 312 msec 352 msec
 3 10.10.10.1 [MPLS: Label 27 Exp 0] 252 msec 400 msec 380 msec
 4 10.10.10.2 412 msec 300 msec 208 msec

```

Figura 3.8.8 : Pruebas de conectividad (sin perdidas de servicio)

Elaborado por el Autor

3.8.2.2 Afectando enlaces del CORE

Para el caso de estudio la ruta principal entre los dos PE (GYEMRCE01-UIOPPPGE01) son los equipos de Core (GYEMRCP01- UIOPPPGP01), tal como se detalla en la figura 3.8.1. En el equipo del Core al cual se va inducir la afectación de transmisión se debe de comprobar el camino que toma el paquete para llegar al destino en este caso sería la loopback 100 del PE-UIOPPPGE01. Al ingresar el comando **show ip route 10.2.10.100** en el GYEMRCP01, se comprueba que para le IGP el camino principal para llegar a esta red es a través de GYEPPGP01.

Al momento de colocar el comando shutdown en la interface Giga5/0 del GYEMRCP01, la ruta debe de converger a través de los demás equipos de Core y no se debe de registrar pérdidas de paquetes a nivel de IGP y de la VPN creadas. Las figuras 3.8.9, 3.8.10 y 3.8.11 resumen estos procesos y la figura 3.8.12 confirman el resultado esperado.

```

GYEMRCP01#show ip route 10.2.10.100
Routing entry for 10.2.10.100/32
  Known via "isis", distance 115, metric 110
  Tag 20, type level-2
  Redistributing via isis
  Last update from 10.51.1.2 on GigabitEthernet5/0, 00:04:14 ago
  Routing Descriptor Blocks:
  * 10.51.1.2, from 10.2.10.100, via GigabitEthernet5/0
    Route metric is 110, traffic share count is 1
    Route tag 20

GYEMRCP01#show interface GigabitEthernet5/0 description
Interface Status Protocol Description
Gi5/0 up up ### LINK TO UIOPPGP01 - Gi5/0 - DWDM ###
  
```

Figura 3.8.9 : Confirmación de ruta principal en el CORE

Elaborado por el Autor

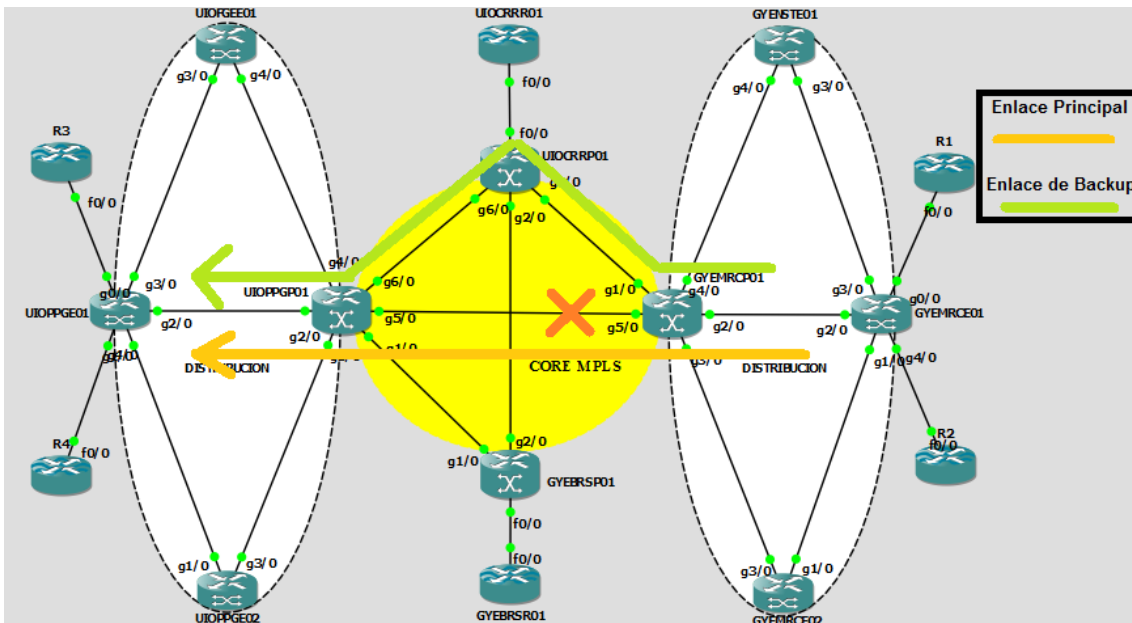


Figura 3.8.10 : Ruta Principal y de Backup del CORE

Realizado por el Autor

```

GYEMRCP01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
GYEMRCP01(config)#interface GigabitEthernet5/0
GYEMRCP01(config-if)#shut
GYEMRCP01(config-if)#end
GYEMRCP01#show ip route 10.2.10.100
Routing entry for 10.2.10.100/32
  Known via "isis", distance 115, metric 120
  Tag 20, type level-2
  Redistributing via isis
  Last update from 10.51.1.6 on GigabitEthernet1/0, 00:00:01 ago
  Routing Descriptor Blocks:
  * 10.51.1.6, from 10.2.10.100, via GigabitEthernet1/0
    Route metric is 120, traffic share count is 1
    Route tag 20

GYEMRCP01#show interface GigabitEthernet1/0 description
Interface status Protocol Description
Gi1/0          up          up          ### LINK TO UIOCRRP01 - Gi1/0 - DWDM ###

```

Figura 3.8.11 : Convergencia de la red

Elaborado por el Autor

```

GYEMRCE01#show ip route vrf voz1001
Gateway of last resort is not set

  10.0.0.0/30 is subnetted, 2 subnets
B       10.10.10.0 [200/0] via 10.2.10.100, 01:01:34
C       10.10.10.4 is directly connected, GigabitEthernet0/0.400

GYEMRCE01#show ip route vrf dat1010
Gateway of last resort is not set

  10.0.0.0/30 is subnetted, 2 subnets
C       10.20.10.4 is directly connected, GigabitEthernet0/0.500
B       10.20.10.0 [200/0] via 10.2.10.100, 01:01:34

GYEMRCE01#show ip route vrf int1100
Gateway of last resort is 10.2.10.100 to network 0.0.0.0

S       200.20.250.0/24 [1/0] via 10.10.10.6
  10.0.0.0/30 is subnetted, 2 subnets
B       10.10.10.0 [200/0] via 10.2.10.100, 01:01:34
C       10.10.10.4 is directly connected, GigabitEthernet4/0.600
B*     0.0.0.0/0 [200/0] via 10.2.10.100, 01:01:34

```

Figura 3.8.12 : Servicios de Voz, datos e Internet sin afectación

Elaborado por el autor

3.8.2.3 Afectando ruta explícita del Traffic Engineering.

Bajo un ambiente controlado se afectará la transmisión según se muestra en la figura 3.8.13 correspondiente al path principal ilustrado en con línea verde, simultáneamente se comprueba que no exista afectación y que el tunnel haya conmutado al path de backup. Esta prueba confirma una de las

principales virtudes de MPLS L2VPN puesto que siempre que tengamos rutas de respaldos adicionales o enlaces saturados podemos manipular el camino que queremos que siga un paquete dentro de la red.

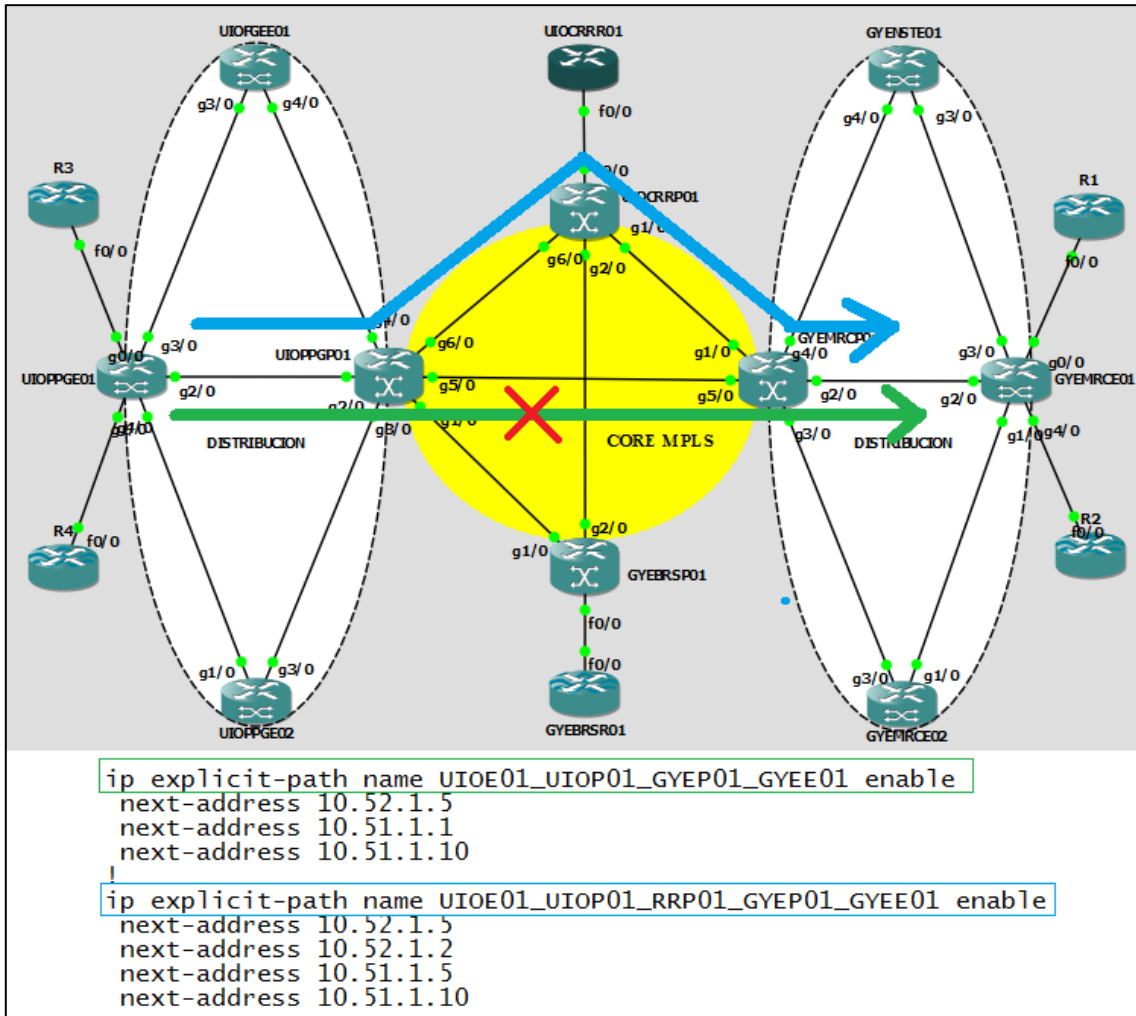


Figura 3.8.13 : Traffic Engineering - explicit-path

Elaborado por el Autor

Para comprobar que el Tunnel de ingeniería de tráfico esté funcionando correctamente se utilizará el comando **show mpls traffic-eng tunnels TuXXX**, siendo XXX el valor asignado al tunnel, de esta manera se puede determinar los path (caminos) del tunnel principal. En la figura 3.8.14 se registra el estatus del tunnel antes que el camino principal resulte afectado y en la figura 3.8.15 demuestra la conmutación al path secundario y si este fallará el tunnel dinámicamente escogería un camino aleatorio para llegar al destino.

```

UIOPPG01#show mpls traffic-eng tunnels Tu2600
Name: ### TE_PPPOE_CLIENTE-B ### (Tunnel2600) Destination: 10.1.10.100
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit UIOE01_UIOP01_GYEP01_GYEE01 (Basis for Setup, path weight 30)
path option 20, type explicit UIOE01_UIOP01_RRP01_GYEP01_GYEE01
path option 30, type dynamic

Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled

InLabel : -
OutLabel : GigabitEthernet2/0, 38
RSVP Signalling Info:
Src 10.2.10.100, Dst 10.1.10.100, Tun_Id 2600, Tun_Instance 109
RSVP Path Info:
My Address: 10.2.10.100
Explicit Route: 10.52.1.5 10.51.1.1 10.51.1.10 10.1.10.100
Record Route:
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 10.52.1.5 10.51.1.1 10.51.1.10
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path Weight: 30 (TE)
Explicit Route: 10.52.1.5 10.51.1.1 10.51.1.10 10.1.10.100
History:
Tunnel:
Time since created: 1 hours, 29 minutes
Time since path change: 39 seconds
Current LSP:
Uptime: 39 seconds
Selection: reoptimization
Prior LSP:
ID: path option 30 [108]
Removal Trigger: path verification failed
Last Error: PCALC:: Can't use link 10.52.10.2 on node 10.2.11.100

```

Figura 3.8.14: Estado del Tunnel de Ingeniería de Tráfico

Elaborado por el Autor

```

UIOPPG01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
UIOPPG01(config)#inter gig5/0
UIOPPG01(config-if)#shut
UIOPPG01(config-if)#end
UIOPPG01#sho inter des | i GYMRC01
Gi5/0      -      admin down      down      ### LINK TO GYMRC01 - Gi5/0 - F.O. ###

UIOPPG01#show mpls traffic-eng tunnels Tu2600
Name: ### TE_PPPOE_CLIENTE-B ### (Tunnel2600) Destination: 10.1.10.100
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 20, type explicit UIOE01_UIOP01_RRP01_GYEP01_GYEE01 (Basis for Setup, path weight 40)
path option 10, type explicit UIOE01_UIOP01_GYEP01_GYEE01
path option 30, type dynamic

Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled

UIOPPG01#sho run inter gig4/0.700
Building configuration...

Current configuration : 181 bytes
!
interface GigabitEthernet4/0.700
 encapsulation dot1q 700
 no snmp trap link-status
 no cdp enable
 xconnect 10.1.10.100 700 encapsulation mpls pw-class PPPOE_CLIENTE_B_2600
end

UIOPPG01#show mpls l2
UIOPPG01#show mpls l2transport vc 700
-----
Local intf   Local circuit   Dest address   VC ID   Status
-----
Gi4/0.700   Eth VLAN 700   10.1.10.100   700     UP

DESDE EL CLIENTE

interface FastEthernet0/0.700
 description ### CLIENTE_B_PPPOE###
 encapsulation dot1q 700
 ip address 192.168.100.1 255.255.255.0
end

CLIENTE_B_1#ping 192.168.100.2 re 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 236/395/648 ms

```

Figura 3.8.15 : Conmutación del tunnel al path secundario

Elaborado por el Autor

CAPITULO 4 : Conclusiones y recomendaciones.

4.1 Conclusiones

La implementación de una red IP/MPLS ofrece a cualquier empresa que brinda servicios de telecomunicaciones enormes ventajas sobre las técnicas actuales de encaminamiento IP, principalmente al momento de brindar servicios diferenciados.

Gracias a la conmutación de etiquetas y al sencillo manejo de la misma se reduce procesamiento en los equipos de la red aumentando la capacidad de manejar un mayor tráfico que en una red IP convencional.

La planificación que se planteada es de gran utilidad ya que marca la pauta para el crecimiento controlado de la red, evitando así confusión, malas configuraciones del IGP, duplicaciones de enlaces WAN, ingreso no autorizados de equipos ajenos a la red, etc.

Las pruebas de servicios diferenciados que se han planteado corresponden a situaciones reales que cualquier red experimenta, tales como, caídas de enlaces, apagado de equipos, saturación de enlaces, etc; pero que gracias a una topología redundante a la rápida conmutación del protocolo de enrutamiento implementado y a las técnicas y métodos ceñidos a la MPLS, hacen de esta una red robusta.

La implementación de Traffic Engineering (TE), es uno de los puntos clave al momento de establecer optimización sobre la red, ya que nos ayuda a manipular el tráfico por enlaces que no están siendo utilizados y que por el IGP son considerado como rutas de respaldos.

4.2 Recomendaciones

Se recomienda siempre conectar los PE directo a los P, solo en casos donde la topología no sea favorable se podrá conectar entre PE. Se considera esta topología más eficiente

Si para estas pruebas se en el CORE se ha utilizado el IOS convencional, se recomienda para la implementación utilizar IOS XR, el cual es un sistema operativo multitarea basado en micro Kernel, con sistema de protección de memoria, funciones mejoradas de alta disponibilidad, escalabilidad para configuraciones de hardware más importantes y permite la instalación de parches mientras el equipo está operativo, este sistema es implementado en equipos cisco CRS-1, CRS-3, ASR9K, XR12K.

Debido a que las pruebas fueron realizadas en un entorno de simulación los tiempos de los ping no representan los valores reales de los servicios puesto que estos tiempos dependen del procesador y la memoria de la maquina con la que se esté realizando la simulación.

Un parámetro que no se ha tomado en cuenta en la simulación es la habilitación del protocolo que agiliza la detección y control de Fallos denominado BFD, este protocolo es de suma importancia ya que ayuda a una rápida conmutación de los protocolos de enrutamiento dinámicos utilizados para el IGP, por lo que se recomienda sea considerado al momento de habilitar el IGP.

El correcto funcionamiento de la red va a depender de un personal debidamente capacitado, de los mantenimientos preventivos y correctivos que se le realicen y de unas adecuadas rutinas de mantenimiento que resuelvan fallas que a la larga podrían afectar el correcto funcionamiento del equipo.

Toda red debe que tener un software de monitoreo, que genere alertas por eventos, y que pueda sacar backup de todos los equipos operativos de la red.

Referencia Bibliográfica

Alwayn, V. (2001). *Advance MPLS Design and Implementation*. Indianapolis, IN 46290 USA.

Canalis, M. S. (n.d.). *MPLS"Multiprotocolo Label Switching" : Una Arquitectura de Backbone para la internet del siglo XXI*. Retrieved from <http://www.exa.unne.edu.ar/informatica/SO/MPLS.PDF>

Cisco. (n.d.). *Configuring MPLS and EoMPLS*. Retrieved Diciembre 8, 2014, from http://www.cisco.com/c/en/us/td/docs/switches/metro/catalyst3750m/software/release/12-1_14_ax/configuration/guide/3750mscg/swmpls.pdf

Cisco, S. (2000). *Advanced MPLS VPN Solutions*. USA.

Garcia, M. O. (n.d.). *MPLS, el presente de las redes IP*. Retrieved from <http://repositorio.utp.edu.co/dspace/bitstream/11059/13111/1/0046T172.pdf>

Ghein, L. D. (2006). *MPLS Fundamentals*. Indianapolis, IN 46240 USA.

Headquarter, C. (2006). *Cisco IOS Multiprotocol Label Switching Configuration Guide*. San Jose, CA 95134-1706.

Headquarters, A. (2011). *MPLS Basic MPLS Configuration Guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/12-4/mp-basic-12-4-book.pdf

Headquarters, A. (2011). *MPLS Layer 2 VPNs Configuration Guide*,. Retrieved from Cisco Systems: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/12-4/mp-l2-vpns-12-4-book.pdf

Headquarters, A. (2011). *MPLS Layer 3 VPNs Configuration Guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/12-4/mp-l3-vpns-12-4-book.pdf

L. Martini, Exist, E., Level 3 Communications, E. Rosen, N. El-Aawar, & Cisco Systems. (n.d.). *Transport of Layer 2 Frames Over MPLS, rfc4906*. Retrieved from <https://tools.ietf.org/html/rfc4906>

Martinez, D. (n.d.). *Redes MPLS*. Retrieved from <https://prezi.com/s9rucral-3jg/copy-of-red-mpls/>

Ojeda, G., & Sahily, D. (n.d.). *Estudio de los protocolos de enrutamiento de internet y utilización en la arquitectura de red MPLS*. Retrieved from <http://saber.ucv.ve/xmlui/bitstream/123456789/617/1/tesis%20Protocolos%20y%20MPLS.pdf>

Pepelnjak, I., & Guichard, J. (201). *MPLS and VPN Architectures*. Indianapolis.

Rekhter, Y., & Moskowitz, R. (1996, Febrero 1). *Asignación de direcciones para Internet privadas*. Retrieved from <http://www.rfc-es.org/rfc/rfc1918-es.txt>

Yakov , R., & Li, T. (1993, Setiembre 1). *RFC 1518 - An Architecture for IP Address Allocation with CIDR*. Retrieved from https://datatracker.ietf.org/doc/rfc1518/?include_text=1

GLOSARIO DE TERMINOS

AS – Autonomous System. Sistema Autónomo.

ATM – Asynchronous Transfer Mode. Modo de Transferencia Asíncrono.

ATOM - Any Transport over MPLS. Cualquier Transporte sobre MPLS.

BDR – Backup Designed Router. Ruteador designado de respaldo.

BGP – Border Gateway Protocol. Protocolo de puerta de frontera.

BFP – Bidereccional Forwarding detection. Detección de envío Bidereccional.

CB - Marking – Class Based Marking. Marcado basado en clases

CE – Customer Equipment. Equipo instalado en el Cliente

CEF – Cisco Express Forwarding. Protocolo de Envío propietario de Cisco.

CIR – Committed Information Rate. Tasa de información Obligatoria

CLI – Command Line Interface. Interface de línea de comandos

CRASH – Choque. Termino referido a falla crítica de un dispositivo de red.

DR – Designed Router. Ruteador designado

DWDM – Dense Wavelength Division Multiplexing. Multiplexado compacto por división en longitudes de onda.

E-BGP – Exterior Border Gateway Protocol. Extrenal BGP.

EIGRP – Enhanced Interior Gateway Routing Protocol. IGRP mejorado.

EVC – Ethernet Virtual Connection. Conexión Virtual Ethernet.

EXP – Campo “Experimental”, usado por MPLS para QoS.

FEC – Forwarding Equivalence Class. Clase equivalente de envío de paquetes.

FIB – Forwarding Information Base. Base de información de envío.

FIFO – First Input First Output. Primero en entrar, primero en salir.

FTN – FEC To NHLFE.

FTP – File Transfer Protocol. Protocolo de transferencia de archivos.

IANA – Internet Assignment Numbers Association.

IATA – International Air Transport Association. Asociación Internacional de Transporte Aéreo

I-BGP – Interior Border Gateway Protocol. BGP interno.

IGRP - Interior Gateway Routing Protocol. Protocolo de enrutamiento de gateway interior

IGP – Interior Gateway protocol. Protocolo de pasarela interior.

IETF – Internet Engineering Task Force. Fuerza de tareas de ingeniería de Internet

IOS – Internetworking Operative System. Sistema operativo de internetwork

IP – Internet Protocol. Protocolo de Internet.

IS – IS – Intersystem – Intersystem. Protocolo de enrutamiento inter - sistemas

ISP – Internet Service Provider. Proveedor de servicios de internet.

LAN – Local Area Network. Red de área local.

LDP – Label Distribution Protocol. Protocolo de distribución de etiquetas.

LER – Label Edge Router. Ruteador de frontera de etiquetas

LIB – Label Information Base. Base de información de etiquetas.

LLQ – Low Latency Queuing. Encolamiento de baja latencia

LSA – Link State Advertisement. Publicación de estado de enlace.

LSP – Label Switched Path. Ruta conmutada de etiquetas.

LSR – Label Switch Router. Ruteador conmutador de etiquetas

LSU – Link State Updates. Actualizaciones de estado de enlace.

MAC – Media Access Control. Control de acceso al medio

MP-BGP – Multi Protocol Border Gateway Protocol. Extensión Multiprotocolo para BGP.

MPLS – Multiprotocol Label Switching.

NBMA – Non Broadcast Multi Access. Multi acceso sin *broadcast*.

OIR – Online Insertion and Removal. Inserción y remoción en línea.

OSPF – Only Shortest Path First. El camino más corto primero, protocolo de enrutamiento dinámico.

P – Provider. Router del proveedor.

PE – Provider Edge. Ruteador del frontera al proveedor.

PPPoE -- Point to Point Protocol over Ethernet. Protocolo de enlace punto a punto sobre Ethernet.

PQ – Priority Queuing. Encolamiento de prioridad.

QoS – Quality of Service. Calidad de servicio.

RD – Route Distinguisher. Distinguidor de ruta.

RFC – Request For Comment. Petición para comentarios.

RIP – Routing Information Protocol. Protocolo de información de enrutamiento dinámico.

RSVP – Resource Reservation Protocol. Protocolo de reservación de recursos.

S – “Stack”. Campo de Pila Usado por MPLS.

TCP/IP – Transport Control Protocol / Internet Protocol. Protocolo de control de transporte sobre el Protocolo de internet.

TOS – Type of Service. Tipo de servicio.

TTL – Time To Live. Tiempo de existencia.

UDP -- User Datagram Protocol. Protocolo del nivel de transporte basado en el intercambio de datagrama.

VPN – Virtual Private Network. Red privada virtual.

VC – Virtual Connection. Conexión Virtual.

VRF – VPN Routing and Forwarding Instances. Enrutamiento y reenvío de instancias VPN.

WAN - Wide Area Network. Red de área grande o amplia.