UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

Trabajo monográfico para optar al título de
Ingeniero en Electrónica.

Tema

“Casos de estudio empleando la tecnología MPLS para transporte de dato y video mediante un diseño de red con equipos Cisco ASR9000 y sistema operativo XR, usando el emulador EVE-NG”.

Autor

Br. Werner E. Quintanilla López. Carné: 96-11330-4

Tutor

Msc. Ing. Cedrick Dalla Torre.

Septiembre 2023

Managua, Nicaragua.

DEDICATORIA

El presente trabajo monográfico se lo dedico a mi querida madre Thelma López y abuela Socorro Pérez (QEPD), quienes han sido mi guía, referencia e inspiración en todos los aspectos de mi vida tanto personal como profesional. Me inculcaron a través del ejemplo, valores como la honestidad, responsabilidad, esfuerzo y dedicación entre muchos otros, lo cual me ha convertido en el hombre que soy preparado para la vida. Sus sacrificios se ven hoy reflejado al culminar esta etapa pendiente en mi vida profesional con la satisfacción de ser un reflejo de ellas.

AGRADECIMIENTO

Agradezco a la Universidad Nacional de Ingeniería UNI y la Facultad de Electrotecnia y Computación FEC y sus docentes por ofrecerme la gran oportunidad excepcional de poder culminar mi carrera a través de la presentación de este trabajo monográfico.

Agradezco también a mi tutor Msc. Ing. Cedrick Dalla Torre, quien durante este proceso me brindó de forma profesional y precisa la guía necesaria para encontrar y desarrollar el tema.

Por último y no menos importante, quiero agradecer a mi esposa, compañera de vida y complemento Scarleth Ramirez quien me brindó su ayuda y apoyo incondicional en los momentos más difíciles de este proceso.

RESUMEN

El presente trabajo monográfico presenta dos casos de estudio para la transmisión de datos (unicast) y video (multicast) respectivamente utilizando una red de servicio MPLS de un ISP (Proveedor de servicios de telecomunicaciones) conformada por equipos Cisco ASR9000 que utilizan el sistema operativo XR, emulando las soluciones con la herramienta EVE-NG.

Los equipos Cisco ASR 9000 y su sistema operativo XR son los utilizados actualmente en las redes modernas de ISP, ya que son plataformas de alta densidad y desempeño diseñadas específicamente para este tipo de redes.

Previamente se presentan los conceptos y fundamentos teóricos de los temas Multicast, MPLS y sus servicios: MPLS VPN y Mutlicast VPN.

El primer caso de estudio aborda la trasmisión de datos y acceso a internet para un cliente corporativo entre su oficina central y dos oficinas remotas utilizando el servicio MPLS VPN.

El segundo caso de estudio aborda la trasmisión de tráfico multicast entre un equipo fuente ubicado en el Head-End y los equipos receptores ubicados en nodos remotos (Video-Hubs) para brindar servicio de video utilizando Multicast VPN.

Para ambos casos se presentan las configuraciones de los equipos de la red del proveedor de servicios (ISP) y la de los equipos terminales a los que se les provee el servicio de trasmisión de datos y video. Así mismo, se presentan las validaciones, utilizando los comandos apropiados, que comprueban la efectividad de la solución para ambos casos de estudio.

INDICE

I. INTRODUCCION 1

II. OBJETIVOS 2

2.1 OBJETIVO GENERAL: 2

2.2 OBJETIVOS ESPECIFICOS: 2

III. JUSTIFICACION 3

IV. MARCO TEORICO 4

4.1 Equipo Cisco ASR9000 y Sistema Operativo XR. 4

4.1.1 Precedentes 4

4.1.2 Serie Cisco ASR9000 5

4.1.3 Sistemas Operativos 7

4.2 Multicast 9

4.2.1 Direccionamiento Multicast 10

4.2.2 IGMP 12

4.2.3 Transmisión de tráfico multicast. 14

4.2.4 Arboles de Distribución Multicast (MDT) 15

4.3 Protocol Independent Multicast (PIM) 18

4.4 Fundamentos de MPLS 21

4.4.1 - Definición de MPLS 21

4.4.2 – Beneficios de MPLS 21

4.4.3 – Etiquetas MPLS 23

4.4.4 – Label Switch Router (LSR) 25

4.4.5 – Label Switched Path (LSP) 25

4.4.6 – Label Distribution Protocol (LDP) 26

4.4.7 – MPLS VPN 27

4.4.8 – Arquitectura de MPLS VPN 28
4.5 Multicast VPN (mVPN) 33
4.5.1 – Arquitectura 33
4.6 Diseño de la Red MPLS 37
4.6.1 Configuraciones 40
4.7.2 - Caso de Estudio #2: Transmisión de Video. 75
V. CONCLUSIONES 105
VI. RECOMENDACIONES 106
VII. BIBLIOGRAFIA 107
VIII. ANEXOS 109
ANEXO 1: ENCUESTA 109
ANEXO 2: SOFTWARE UTILIZADO 116
ANEXO 3: CONFIGURACIONES CASOS DE ESTUDIO 117

I. INTRODUCCION

En la actualidad, las redes de comunicaciones IP de los proveedores de servicios han evolucionado tanto en hardware como en software para hacer frente al alto volumen de tráfico de datos, voz y video que demandan los usuarios.

Hoy en día, en las redes de telecomunicaciones, específicamente en nuestro país, los proveedores de servicios de telecomunicaciones (ISP) y las empresas corporativas que hacen uso de estos servicios de transporte de datos, proporcionados por estos mismos proveedores, emplean diferentes equipos y sistemas operativos en sus respectivas redes.

En el presente protocolo monográfico se presenta el diseño de una red MPLS con servicios VPN para la transmisión de datos y video, empleando equipo Cisco ASR con sistema operativo XR, dichos elementos se encuentran presentes en las redes de los proveedores de servicios de telecomunicaciones ISP en el país.

El proyecto se desarrollará mediante la simulación de 2 casos de estudio utilizando el emulador EVE-NG:

1. Servicio de transmisión de datos para interconectar 3 oficinas de una empresa.
2. Servicio de transmisión de video digital entre el Head-End y 2 Video-Hubs remotos de una cablera.

Con estos casos de estudio se pretende brindar una versión más realista de una red IP utilizada para proveer servicios de telecomunicaciones con equipos y sistemas operativos modernos diseñados para este fin, con el propósito de que sirvan de referencia en el diseño y configuración de este tipo de redes y tecnología y le permitan al profesional estar preparados para administrar las redes modernas de ISP.

II. OBJETIVOS

2.1 OBJETIVO GENERAL:

Presentar casos de estudio que sirvan de referencia en el diseño y configuración de redes IP con tecnología MPLS para la transmisión de datos multimedia empleando equipos y sistemas operativos utilizados actualmente en las redes de telecomunicación de los proveedores de servicios ISP.

2.2 OBJETIVOS ESPECIFICOS:

1. Definir los fundamentos de las tecnologías MPLS y Multicast, que permitan la comprensión del tema a desarrollar.

2. Describir las características de los equipos Cisco ASR9000 y el sistema operativo XR para evidenciar sus ventajas en comparación a los sistemas anteriores.

3. Diseñar una red de servicio MPLS empleando equipos Cisco ASR9000 con sistema operativo XR, utilizados en las redes modernas de proveedores de servicios de telecomunicaciones (ISP), para mostrar la arquitectura básica de una red MPLS.

4. Presentar el diseño de red y las configuraciones con el sistema operativo XR a través de 2 casos de estudio utilizando el emulador EVE-NG y que sirvan de referencia para las soluciones a servicios de transporte de datos multimedia.

III. JUSTIFICACION

Los trabajos monográficos encontrados que desarrollan el tema de diseño de redes MPLS utilizan equipos y sistemas operativos obsoletos, ya que actualmente no son los utilizados en las redes modernas de los proveedores de servicio que transportan un alto tráfico multimedia (internet, video, televisión) debido a la fuerte demanda de estos tipos de servicios por parte de los usuarios (clientes masivos y corporativos).

El profesional requiere de conocimientos y habilidades teórico-prácticas para administrar redes modernas de proveedores de servicio de telecomunicaciones. En vista de ello, se presenta este trabajo monográfico con un contenido actualizado, que ayude a reducir la curva de aprendizaje de quienes se integran a laborar en redes IP de proveedores de servicios ISP, y que a la vez sea de utilidad para aquellos interesados en el estudio y comprensión de este tipo de redes.

A través del presente trabajo monográfico se dan a conocer los conceptos y fundamentos de las tecnologías MPLS y Multicast, con énfasis en 2 casos de estudio donde se aplica la tecnología MPLS para el transporte de dato y video, mediante un diseño de red que utiliza equipos Cisco ASR9000 con el sistema operativo XR, apoyándose de la herramienta EVE-NG para emular la solución. De este modo, se presenta una versión actual y moderna de redes con servicios MPLS diseñada con uno de los equipos y sistemas operativos más utilizados por los proveedores de servicios de telecomunicaciones en Nicaragua y que pueda servir como referencia para futuros trabajos enfocados en este tipo de tema.

IV. MARCO TEORICO

4.1 Equipo Cisco ASR9000 y Sistema Operativo XR.

4.1.1 Precedentes

La estructura de red de los Proveedores de Servicios de Telecomunicaciones (ISP) que utilizaban plataformas del fabricante Cisco, estaban conformadas por equipos Cisco 12000 (GSR Gigabit Switch Router) en el Core y la Serie Cisco7600 a nivel de Borde, dichos equipos ofrecían conmutación Ethernet de alta densidad, enrutamiento IP/MPLS; permitiendo a los ISP prestar servicios a usuarios y corporaciones sobre una misma red convergente.

Entre sus principales características se tenía [4]:

- Sistema Operativo IOS de Cisco.
- Alto desempeño, con 720Gbps por chasis o 40Gpbs por ranura (slot)
- Un portafolio de tarjetas SPA (Shared Port Adapters) y SIP (SPA Interface Processor) para tráfico multimedia.
- Interfaces Ethernet de 100Mbps/1Gbps/10Gbps.

Figura 4.1 - Plataformas Cisco 7600 [5].

Estas plataformas llegaron a su ciclo de fin según notificación del fabricante [6]:

End-of-Sale Date: 24/07/2016

End-of-Support Date: 31/07/2021

4.1.2 Serie Cisco ASR9000

Los Router Cisco ASR (Aggregation Services Router) de la Serie 9000 son plataformas de alta densidad y alto desempeño que están diseñadas para operar en los niveles de Core y Borde en redes de proveedores de servicios de telecomunicaciones (ISP) y que pueden cubrir mercados en crecimiento y con alta demanda de tráfico. Esta serie tiene un amplio portafolio de productos con un rango de modelos que va desde el Cisco ASR9001 hasta el Cisco ASR9922, cada uno diseñado para proveer confiabilidad para redes tipo “Carrier” usando el Sistema Operativo XR [7]. Los ASR soportan interfaces Ethernet de 1Gbps, 10Gbps, 25Gbps, 40Gbps, 100Gbps y 400Gbps. Ofrecen un Throughput por chasis que varía según el modelo, desde 7Tbps en el ASR9006 hasta 160Tbps en el ASR9922 [8].

Figura 4.2 – Plataformas Cisco ASR Serie 9000 [7].

Las principales características de esta plataforma son [7]:

- Sistema Distribuido

  La serie Cisco ASR9000 opera en un modo que se conoce como “Fully Distributed”, que consiste en que las acciones y decisiones para el envío de paquetes ocurren en las tarjetas de línea las cuales están equipadas con un procesador de red especializado, evitando así, usar el procesador central (CPU) de la plataforma.

- Hardware Redundante y Eficiente

  La serie Cisco ASR9000 provee una infraestructura en la que todos sus componentes son redundantes: Route Switch Processor (RSP), Route Processor (RP), fuentes de poder, ventiladores.

- Sistema Operativo Cisco IOS XR

  La serie Cisco ASR9000 utiliza el sistema operativo Cisco IOS XR que provee beneficios y características de alta calidad y escalables. El sistema operativo XR utiliza una arquitectura “microkernel” para alcanzar modularidad que provea una operación ininterrumpida durante las actualizaciones del software o cambio/remplazo de hardware (módulos) sin afectar la funcionalidad de la plataforma.

- Optimizado para IPv6

  La serie Cisco ASR9000 se apegan a las estrategias de construcción de redes IPv6 de próxima generación para simplificar el diseño, despliegue y administración de servicios en las redes de Proveedores de Servicios (ISP).

4.1.3 Sistemas Operativos

El sistema operativo es responsable de administrar procesos y recursos de hardware del sistema como CPU, memoria, unidades de disco.

4.1.3.1 IOS

IOS fue desarrollado en los 80's, época en que los routers tenían memorias limitadas y procesadores (CPU) de baja capacidad [9].

Características [9]

- Kernel y Programación de Procesos: El Kernel de IOS es un modelo monolítico ajustado a los limitados recursos de sistemas propio de los tiempos en que se desarrolló el sistema operativo. IOS asigna un valor de prioridad a los procesos. Procesos con un valor de alta prioridad se ejecutan antes que los de baja prioridad, al menos que un proceso de baja prioridad se esté ejecutando antes. A este sistema se le nombra como "Run to Completion Scheduler".

- Administración de memoria: IOS mapea toda la memoria física a un solo espacio de memoria virtual. IOS no implementa protección de memoria entre procesos o grupos de memoria. La ventaja de este modelo es que mejora el desempeño del sistema y mantiene al mínimo los altos requerimientos operacionales del sistema operativo. El inconveniente de este modelo es que se incrementa la complejidad del sistema y la posibilidad de corrupción de los datos en un proceso que desestabilice al sistema completo y que conlleve a la interrupción total del software, requiriendo del reinicio del sistema operativo para recuperar los servicios.

- Empacado del Software: las imágenes de IOS son compiladas en un solo archivo para cada plataforma, la disponibilidad de nuevas funciones requiere la instalación de una nueva imagen (archivo), lo que conlleva a un reinicio del sistema para la carga de la nueva imagen.

4.1.3.2 IOS XR

Este sistema operativo fue lanzado en el 2004 con los router CRS-1 (Carrier Routing System). La arquitectura de IOS XR toma ventaja de los avances en capacidades de hardware ya disponibles en ese momento (sistemas con múltiples CPU y memorias RAM con capacidades en Gigabytes) y provee un alto porcentaje de disponibilidad (99.999) y escalabilidad [9].

Características [9]:

- Kernel y Programación de Procesos: IOS XR está basado en RTOS microkernel (Real Time Operating System). La arquitectura microkernel tiene funciones reducidas y se enfoca en servicios esenciales como administración de memoria, comunicación entre procesos (IpC) y planificación de procesos. Esta arquitectura ejecuta fuera del kernel casi todos los servicios y procesos del sistema y se pueden reiniciar individualmente sin requerir de un reinicio completo del sistema.

- Administración de memoria: IOS XR provee protección completa de memoria. Las aplicaciones se ejecutan en una memoria virtual en lugar de la memoria física. Un hardware dedicado llamado MMU (Memory Management Unit) administra el mapeo entre la memoria virtual y la memoria física.

- Empacado del Software: IOS XR paquetes de software por cada característica. La modularidad de la arquitectura del software permite la instalación, eliminación o modificación de paquetes sin necesidad de reiniciar el sistema completo.

4.2 Multicast

En una red IP y los equipos que la conforman, existen 3 tipos de tráfico [10]:

Unicast (uno -> uno): Paquetes enviados desde una dirección origen a una única dirección destino. Cuando se transmite la misma información a un grupo de receptores, cada paquete se replica para cada host receptor.

Broadcast (uno -> todos): Paquetes enviados a una dirección destino tipo broadcast (Dirección MAC: FFFF.FFFF.FFFF, Dirección IP: 255.255.255.255). Comunica la misma información a todos los receptores.

Multicast (uno -> muchos): Paquetes enviados a una dirección destino multicast, este tráfico es unidireccional, de la fuente a los receptores. Las direcciones multicast son “Direcciones de Grupo”.

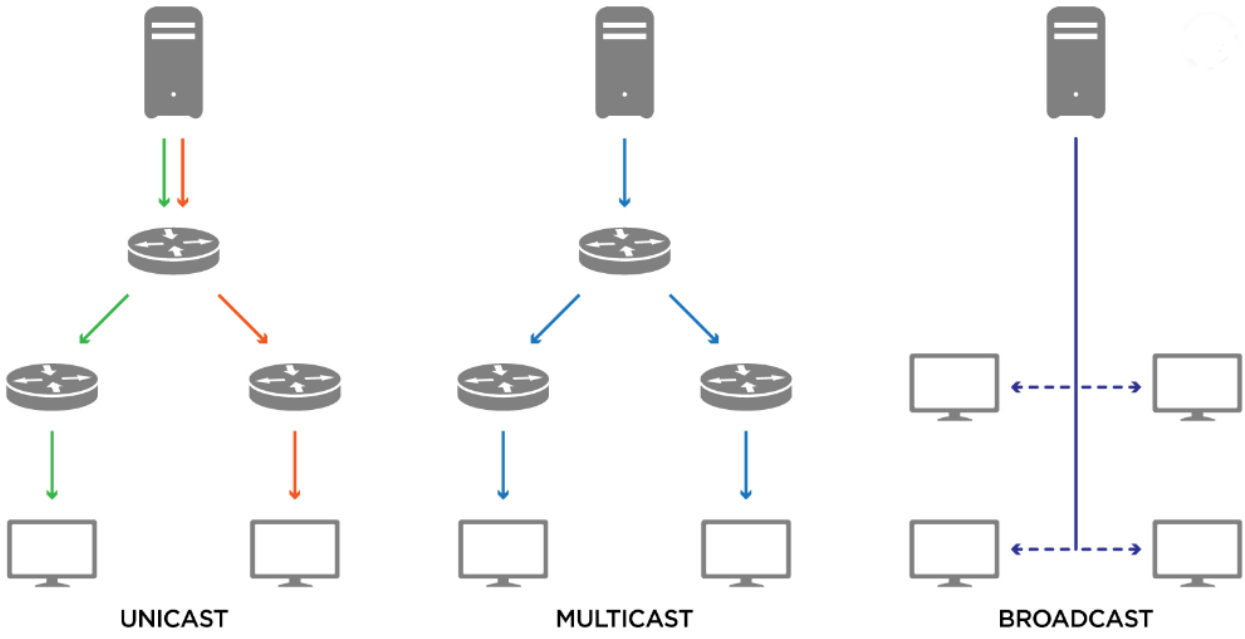


Figura 4.3 – Tipos de tráfico [11].

Multicast es un mecanismo eficiente para la transmisión de datos desde una fuente hacia múltiples receptores optimizando la utilización de ancho de banda en la red [12]. Se apoya en los protocolos IGMP y PIM para su operación en las capas de red 2 y 3. IGMP es utilizado para la comunicación entre el receptor y su router local (LHR: Last Hop Router), PIM se utiliza para la comunicación entre los router intermedios entre la fuente y el/los receptores.

4.2.1 Direccionamiento Multicast

La dirección destino de un paquete multicast es una dirección de grupo multicast que usa el rango asignado 224.0.0.0 - 239.255.255.255 (Clase D), los primeros 4 bits de este rango siempre tienen el valor binario 1110 [9].

Tabla 4.1 – Bloques de direcciones IP multicast [9].

Designation	Multicast Address Range
Local Network Control Block	224.0.0.0 – 224.0.0.255
Internetwork Control Block	224.0.1.0 – 224.0.1.255
AD-HOC Block I	224.0.2.0 – 224.0.255.255
Reserved	224.1.0.0 – 224.1.255.255
SDP/SAP Block	224.2.0.0 – 224.2.255.255
AD-HOC Block II	224.3.0.0 – 224.4.255.255
Reserved	224.5.0.0 – 224.255.255.255
Reserved	225.0.0.0 – 231.255.255.255
Source-Specific Multicast Block	232.0.0.0 – 232.255.255.255
GLOP Block	233.0.0.0 – 233.255.255.255
AD-HOC Block III	233.252.0.0 – 233.255.255.255
Reserved	234.0.0.0 – 238.255.255.255
Administratively Scoped Block	239.0.0.0 – 239.255.255.255

Local Network Control Block (224.0.0.0/24): Son utilizadas para tráfico de control de protocolo que no se transmite fuera del dominio de broadcast, son utilizadas únicamente en el segmento local (TTL=1).

Internetwork Control Block (224.0.1.0/24): Son utilizadas para tráfico de control de protocolo que se puede transmitir por internet.

Tabla 4.2 – Direcciones IP multicast reservadas (Well-Known) [9].

IP Multicast Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	All hosts in this subnet (all-hosts group)
224.0.0.2	All routers in this subnet
224.0.0.5	All OSPF routers (AllSPFRouters)
224.0.0.6	All OSPF DRs (AllDRouters)
224.0.0.9	All RIPv2 routers
224.0.0.10	All EIGRP routers
224.0.0.13	All PIM routers
224.0.0.18	VRRP
224.0.0.22	IGMPv3
224.0.0.102	HSRPv2 and GLBP
224.0.1.1	NTP
224.0.1.39	Cisco-RP-Announce (Auto-RP)
224.0.1.40	Cisco-RP-Discovery (Auto-RP)

Source Specific Multicast Block (232.0.0.0/8): SSM es una extensión de PIM. Los receptores multicast solicitan contenido (unirse a un grupo multicast) especificando la fuente multicast.

GLOP Block (233.0.0.0/8): Se asignan de forma estática a los Sistemas Autónomos que lo solicitan. Los Sistemas Autónomos de 16 bits utilizan el segundo y tercer octeto de la dirección multicast. Los Sistemas Autónomas de 32 bits utilizan AD-HOC Block III o direcciones IPv6 multicast.

Administratively Scoped Block (239.0.0.0/8): Son para uso privado en un dominio multicast de una organización, similar al rango privado de direcciones unicast definido en el RFC1918.

4.2.2 IGMP

IGMP es el protocolo utilizado para la comunicación entre los receptores multicast y su router local. Se utiliza para que el receptor solicite servicio multicast al router más cercano, así mismo, el router identifica los receptores multicast que demandan el servicio.

Cuando un receptor desea recibir tráfico multicast, le envía a su router más cercano un paquete “IGMP Join” (Unsolicited Membership Report) indicando el grupo al que desea unirse. El router local envía este paquete “Join” a la fuente multicast o al RP definido en la configuración. Cuando el router local recibe el tráfico multicast, lo envía al segmento de red del receptor(es) que lo solicitó.

El router local envía cada 60 segundos una consulta (Query) a la dirección multicast 224.0.0.1 (Todos los hosts) para validar si hay receptores interesados en recibir el contenido multicast. Si un host (receptor) responde (con un Membership Report), el router continúa enviando tráfico multicast. Si ningún host responde a la consulta en el periodo de tiempo de 180 segundos (3 veces el Query Interval) entonces el router local deja de enviar tráfico hacia ese segmento.

Existen 3 versiones de IGMP:

IGMPv1: Esta versión es la menos utilizada. No tiene un mecanismo para indicar que se desea salir del grupo multicast. Por lo tanto, se puede enviar por la red tráfico multicast innecesario en un periodo de 3 minutos.

IGMPv2: Esta versión incluye las siguientes mejoras:

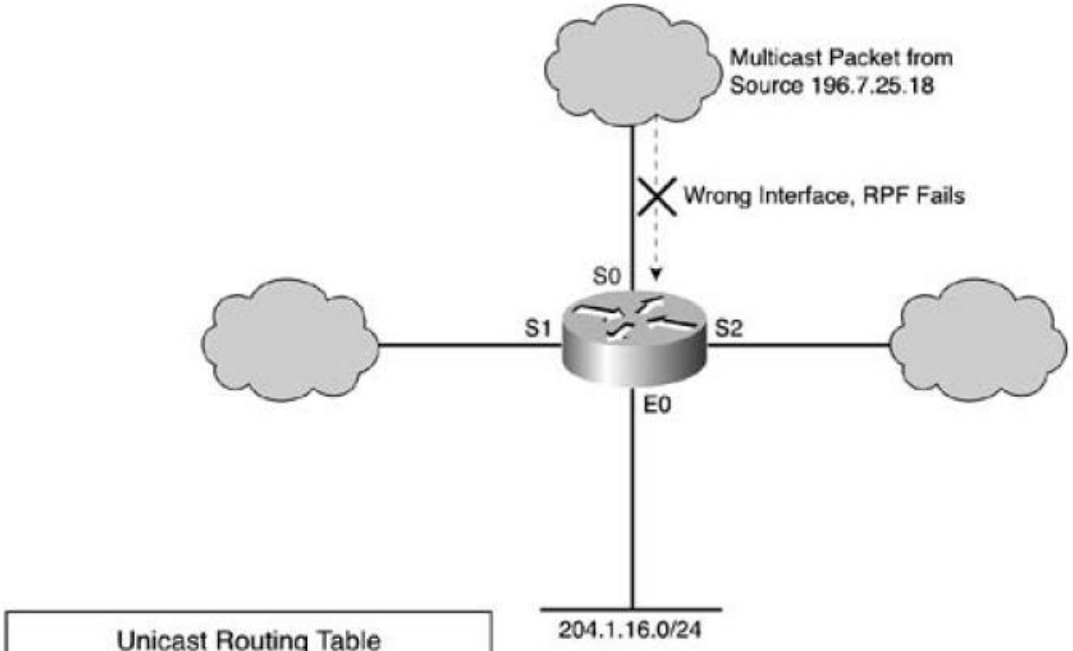
- Las consultas (Queries) se pueden enviar de forma general (General Queries), es decir, a la dirección multicast 224.0.0.1 (Todos los hosts) o solamente a los miembros de un grupo especifico (Group-Specific Queries).
- Los hosts pueden solicitar salirse de un grupo de forma dinámica, enviando el mensaje “Leave-Group” a la dirección multicast 224.0.0.2 (Todos los Rotuers).
- Mecanismo para elegir al “Querier” en caso de que exista más de un router en el segmento. El Querier elegido es el router con la dirección IP mayor.
- Se incluye un tiempo para responder a las consultas (Query-Interval Response Time) que le indica a los miembros del grupo (receptores) cuanto tiempo tienen para responder.

IGMPv3: Es una extensión de IGMPv2 y soporta el filtrado de fuentes multicast la cual brinda a los receptores la posibilidad de indicar la fuente multicast que desean utilizar para determinado grupo.

4.2.3 Transmisión de tráfico multicast.

4.2.3.1 Reverse Path Forwarding (RPF)

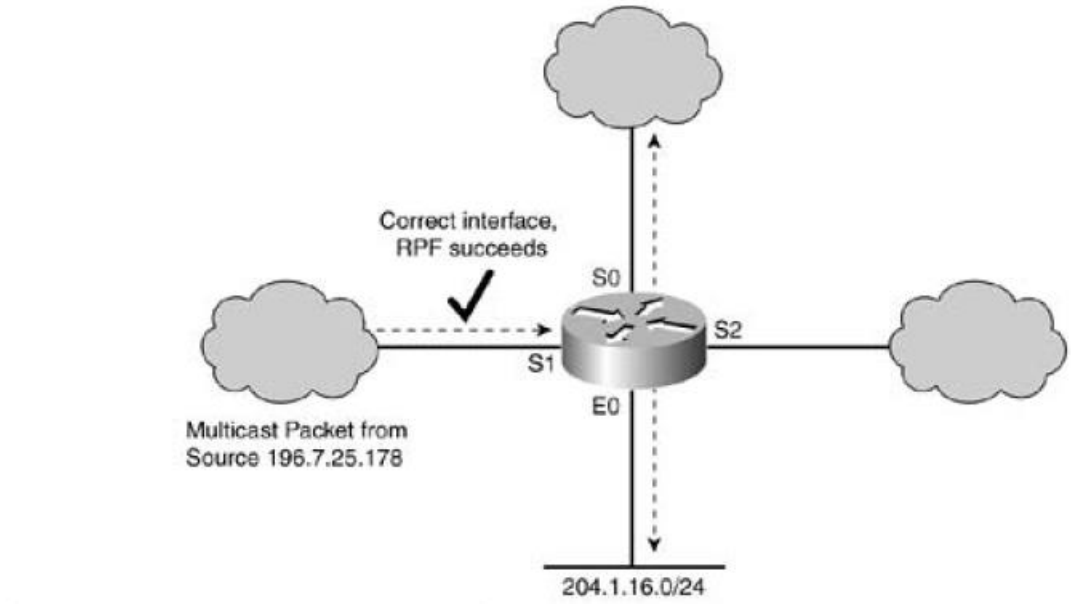
Los routers ejecutan una prueba RPF por cada paquete multicast que reciben, con el fin de verificar que el paquete arribó por la misma interfaz que se utilizaría para llegar a la fuente emisora del paquete según la tabla unicast. De ser así, el paquete se envía hacia los receptores; en caso contrario, el paquete se descarta.



Unicast Routing Table	
Network	Interface
196.7.25.0/24	S1
196.7.26.0/24	S0
204.1.16.0/24	E0

Packet arrived on wrong interface, therefore packet should be dropped.

Figura 4.4 – Verificación RPF Fallida [12].



Unicast Routing Table	
Network	Interface
196.7.25.0/24	S1
196.7.26.0/24	S0
204.1.16.0/24	E0

Packet arrived on correct interface, therefore packet should be replicated.

Figura 4.4 – Verificación RPF Exitosa [12].

4.2.4 Arboles de Distribución Multicast (MDT)

Los paquetes multicast se envían por la red usando un “Árbol de Distribución Multicast” (MDT: Multicast Distribution Tree). Los equipos de red son responsables de replicar el paquete en los puntos de bifurcación del árbol. Esto significa que solamente una única copia del paquete viaja en cada enlace de la red, distribuyendo de forma eficiente la misma información a muchos receptores [12].

Existen 2 tipos de Arboles de Distribución: Source Tree (SPT) y Shared Tree [12].

Source Tree (Shortest Path Tree):

Es el árbol de distribución más simple. La fuente del tráfico multicast se localiza en la “raíz del árbol” y los receptores se localizan en los extremos de las “ramas del árbol”. El tráfico multicast viaja desde la fuente hasta los receptores a través del árbol de distribución. El camino entre la fuente y el receptor es la ruta más corta disponible (SPT: Shortest Path Tree). Se forma un “Source Tree” por cada fuente que transmite paquetes multicast aun cuando haya fuentes transmitiendo al mismo grupo multicast. El registro en la tabla de enrutamiento multicast de un SPT se observa con la notación (S, G), donde “S” indica la fuente multicast y “G” en grupo multicast que transmite dicha fuente.

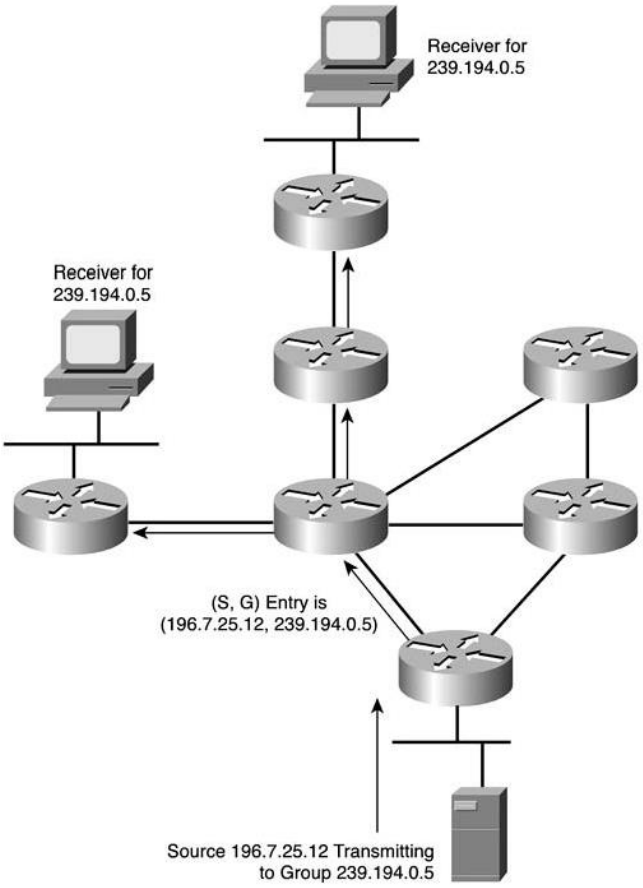


Figura 4.4 – Flujo de tráfico “Source Tree” [12].

Shared Trees:

En el tipo de árbol Shared Tree, la raíz del árbol es un punto común en la red que se le conoce como “Rendezvous Point” (RP). El RP es el punto donde los receptores consultan para conocer las fuentes multicast activas. Las fuentes multicast transmiten tráfico hacia los RP. Cuando los receptores se unen a un grupo multicast, el RP es la raíz del árbol y el tráfico multicast es transmitido desde el RP hacia los receptores. El RP es un intermediario entre las fuentes y los receptores. El camino entre la fuente y los receptores no es el más optimo como en el caso del Source Tree. El registro en la tabla de enrutamiento multicast de un árbol Shared Tree se observa con la notación (*,G), donde “*” indica cualquiere fuente multicast transmitiendo para el grupo “G”.

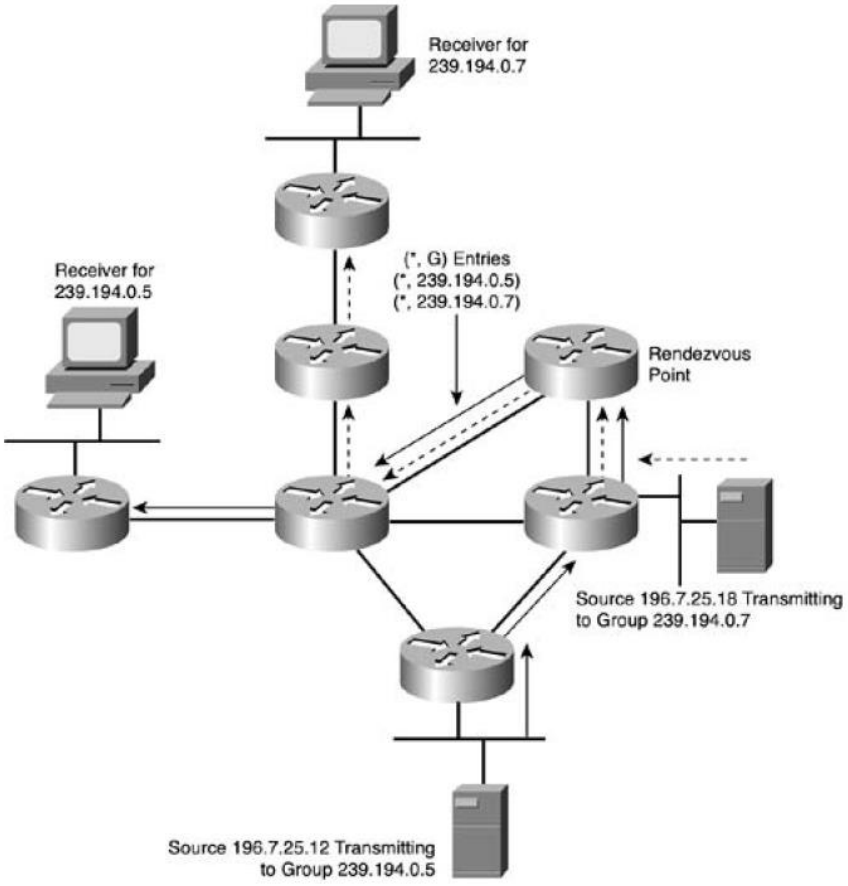


Figura 4.5 – Flujo de tráfico “Shared Tree” [12].

4.3 Protocol Independent Multicast (PIM)

PIM es un protocolo de enrutamiento multicast usado para el envío de tráfico multicast entre segmentos de red. PIM opera independiente a cualquier protocolo de enrutamiento unicast. PIM envía paquetes “Hello” cada 30 segundos (por defecto) por todas sus interfaces habilitadas con PIM, para descubrir vecinos PIM. El mensaje Hello se envía a la dirección multicast 224.0.0.13 (Todos los Routers PIM).

PIM opera en múltiples modos, pero solo se describirán los modos más utilizados comúnmente:

- PIM Dense Mode (DM)
- PIM Sparse Mode (SM)
- PIM SParse-Dense Mode
- PIM Source Specific Multicast (SSM)
- PIM Bidirectional

PIM Dense Mode

Este modo asume que hay un receptor multicast en cada segmento de red y por ende envía tráfico a todos los routers en la red. Los routers que no tienen un receptor interesado en determinado grupo multicast, tienen que mandar un mensaje “Prune” al router de quien recibe el tráfico multicast para indicarle que no está interesado en recibir dicho tráfico y de esta forma bloquear el flujo de tráfico por esa conexión. Como resultado se forma un árbol de distribución tipo fuente (Source Tree).

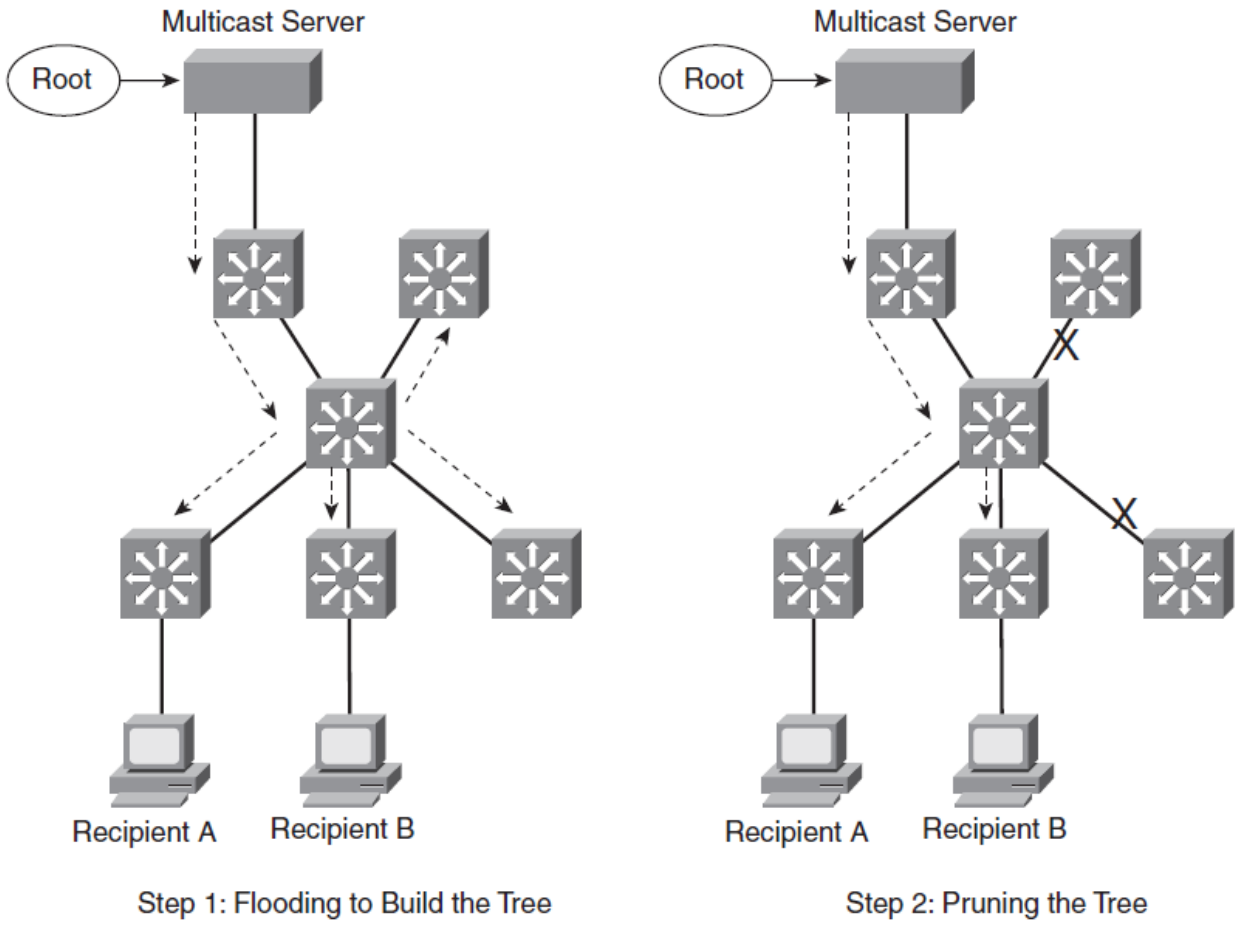


Figura 4.6 – Formación de árbol (Source Tree) con PIM Dense Mode [14].

PIM Sparse Mode

Este modo es más eficiente que PIM Dense Mode ya que no inunda la red con tráfico multicast, el tráfico se distribuye únicamente donde hay receptores interesados en dicho tráfico. Los receptores interesados en determinado grupo multicast envían un paquete o mensaje “Join” a su router local quien a su vez lo envía hacia el RP indicando la intención de recibir tráfico muticast de determinado grupo. El árbol de distribución que se forma es del tipo compartido “Shared Tree” ya que el trafico fluye desde la fuente hacia el RP y luego hacia los receptores, sin embargo, una vez que se recibe tráfico desde la fuente, ocurre un proceso llamado “SPT Switchover” en el que el árbol de distribución cambia al tipo “Source Tree” el cual utiliza la ruta más corta entre la fuente y los receptores sin pasar por el RP.

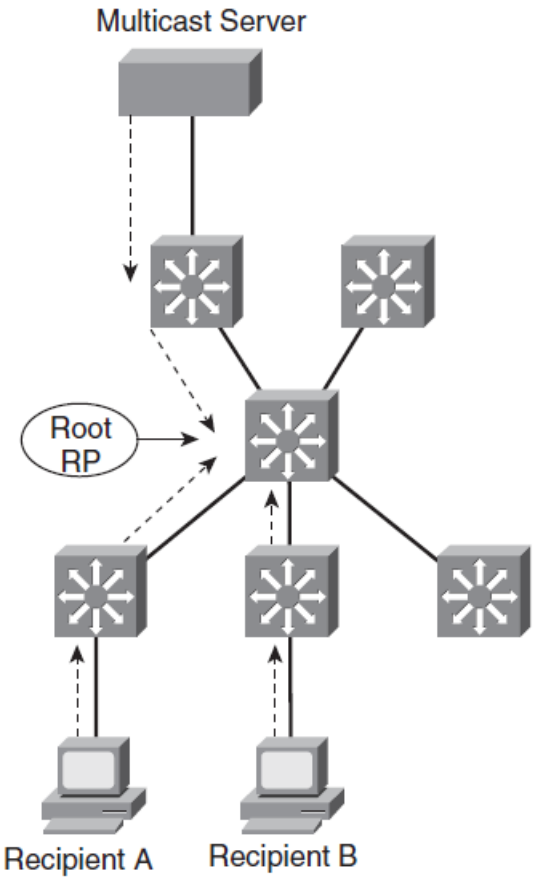


Figura 4.7 – Formación de árbol (Shared Tree) con PIM Sparse Mode [14].

PIM SSM

En los modos PIM-SM/DM los receptores utilizan IGMPv2 para enviar mensajes "Join" e indicar que desean recibir tráfico multicast de determinado grupo multicast. En el mensaje "Join" solo se especifica el grupo multicast (G) y no la fuente (S), así, el receptor puede recibir tráfico multicast de cualquier fuente que transmita en dicho grupo multicast. A este modelo de servicio multicast se le conoce como "Any Source Multicast" (ASM).

Con PIM SSM los receptores indican la fuente desde la que desean recibir tráfico multicast utilizando IGMPv3. El mensaje se envía a la dirección multicast 224.0.0.22 y en dicho mensaje el receptor especifica el grupo y la fuente desde la que desea recibir tráfico multicast. Con esto no se requiere de un router RP en la red y el árbol de distribución que se forma siempre es del tipo fuente “Source Tree”.

4.4 Fundamentos de MPLS

4.4.1 - Definición de MPLS

MPLS (Multiprocol Label Switching) es una tecnología de red que utiliza “etiquetas” para enviar paquetes a través de una red. Estas etiquetas son anunciadas entre routers para que éstos puedan construir una tabla de mapeo o correspondencia de etiquetas. Las etiquetas se adjuntan o adhieren a los paquetes IP permitiendo que los routers envíen tráfico basado en las etiquetas y no en la dirección IP destino. Los paquetes se trasmiten usando conmutación de etiquetas en vez de conmutación de paquetes. El hecho de utilizar etiquetas para transmitir paquetes en lugar de la dirección IP destino del paquete ha contribuido a la popularidad de MPLS [13].

4.4.2 – Beneficios de MPLS

1) El uso de una infraestructura de red unificada [13]

Con MPLS, el objetivo es etiquetar paquetes según su destino o algún otro criterio y transmitir el tráfico sobre una única infraestructura, representando esto la gran ventaja de MPLS. Una de las razones de por qué el protocolo IP se volvió popular y dominar las redes es porque se pueden transportar muchas tecnologías sobre este protocolo.

Con MPLS se expanden las posibilidades de lo que se puede transportar. Agregar etiquetas a los paquetes permite transportar otros protocolos además de IP sobre una red MPLS, tales como IPv4, IPv6, Ethernet, HDLC, PPP y otros protocolos de Capa 2.

En esencia, la conmutación de etiquetas de MPLS es un método simple de conmutación de múltiples protocolos en una misma red.

2) Red Core sin BGP [13]

Cuando se requiere enviar tráfico en la red IP de un ISP, cada router debe revisar la dirección IP destino del paquete. Si los paquetes requieren ser enviados a redes externas a la red del proveedor, los prefijos de esas redes externas deben estar presente en la tabla de enrutamiento de cada router. BGP es el protocolo usado para propagar prefijos externos, como prefijos de clientes o prefijos de internet, en la red del proveedor; eso significa que en toda la red del proveedor se debe utilizar BGP.

MPLS realiza el envío de paquetes basado en la inspección de la etiqueta en el paquete en vez de inspeccionar la dirección IP destino. La etiqueta está asociada a un router destino (Egress Router) y le indica a cada router intermedio (Core Router) a qué router destino se debe dirigir el paquete. Los router en el Core de la red no necesitan conocer la información de prefijos externos en su tabla de ruta, por lo tanto, no se requiere utilizar BGP en el Core de la red del proveedor de servicios.

La inspección de la dirección IP destino se realiza en el router origen (Ingress Router) y en este punto se requiere del protocolo BGP.

3) Modelo VPN Peer-to-Peer vs Modelo VPN Overlay [13]

Una VPN (Virtual Private Network) emula una red privada sobre una infraestructura común de servicios. Una red privada requiere que todos los sitios de un cliente se puedan interconectar y a su vez estar separada de otras VPNs (otros clientes/servicios).

Los 2 modelos de servicios VPN que un ISP puede ofrecer a sus clientes son:

Modelo “Overlay VPN”

En este modelo, el proveedor de servicios provee servicios de conexiones punto a punto o circuitos virtuales entre los router de cliente. Nos existe interacción en capa

3 entre los equipos de red del ISP y los equipos del cliente, es decir, los router del ISP no conocen las redes de los clientes.

Modelo “Peer to Peer VPN”

En este modelo, los router del ISP interactúan en capa 3 con los router CPE del cliente, es decir, se requiere de un protocolo de enrutamiento para el intercmabio de información de enrutamiento entre el cliente y el ISP.

4) Ingeniería de Tráfico (Traffic Engineering) [13]

Con Ingeniería de Tráfico se optimiza el uso de la red porque se pueden manipular o dirigir flujos de tráfico y utilizar enlaces o conexiones que no son considerados por los protocolos de enrutamiento. De esta forma se puede dar uso a la red y sus enlaces de una forma más balanceada.

4.4.3 – Etiquetas MPLS

Una etiqueta MPLS es un campo de 32 bits. Los primeros 20 bits representan el número de etiqueta, con un valor entre 0 y 2^{20}-1, es decir, 1,048,575, de los cuales los primeros 16 números están reservados. Los bits 20 al 22 son el campo experimental (EXP) y se utiliza para calidad de servicio. El bit 23 es el campo Bottom of Stack (BoS) para señalar la última etiqueta en caso de existir una pila de etiquetas. El campo de 8 bits TTL: Time-To-Live (bits del 24 al 31) es utilizado para evitar bucle de enrutamiento del paquete [13].

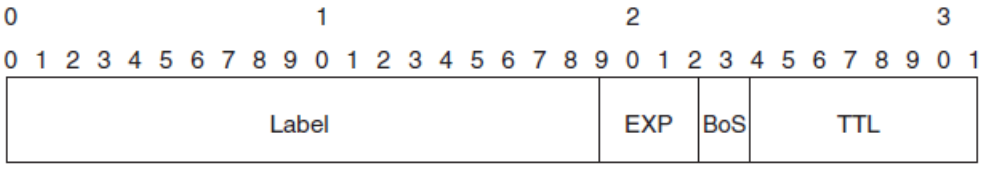


Figura 4.8 – Estructura de una Etiqueta MPLS [13].

Las etiquetas MPLS se instalan entre el encabezado de la Capa 2 y el encabezado de la Capa 3 (protocolo transportado) del paquete. El protocolo transportado puede ser IPv4, IPv6 o cualquier protocolo de Capa 2: Ethernet, Frame Relay, ATM, PPP, HDLC; usando el servicio AToM (Any Traffic over MPLS) de MPLS [13].

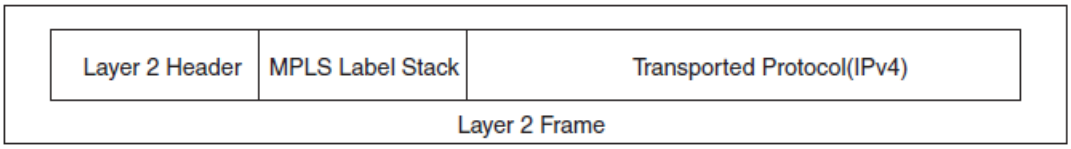


Figura 4.9 – Encapsulado de un paquete etiquetado [13].

Un paquete que se transporta por una red MPLS puede requerir mas de una etiqueta, como en el caso de servicios L2VPN y L3VPN. Las múltiples etiquetas se colocan en una pila (stack) de etiquetas. A la primera etiqueta en la pila o stack se le llama “Top Label”, a la última etiqueta en la pila se le llama “Bottom Label”, entre la primer y última etiqueta se puede tener cualquier cantidad de etiquetas.

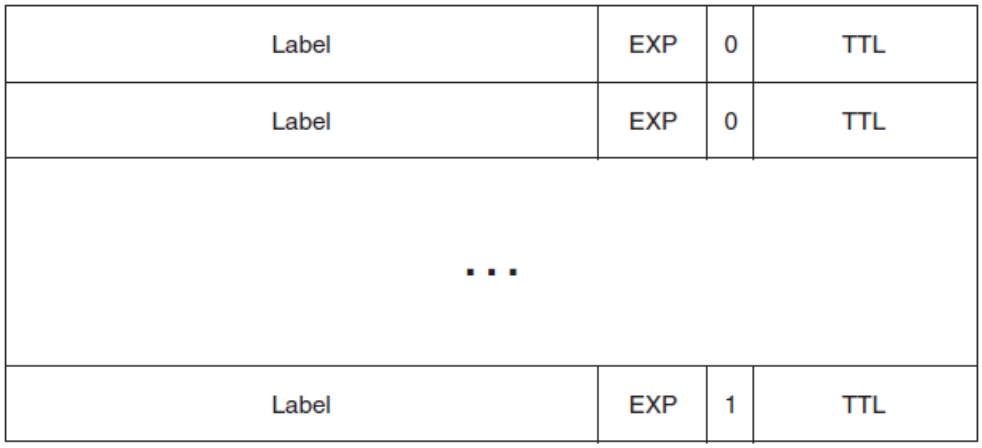


Figura 4.10 – Pila de Etiquetas (Label Stack) [13].

4.4.4 – Label Switch Router (LSR)

Un router LSR es un equipo que soporta MPLS, es decir, es capaz de recibir y transmitir paquetes etiquetados. Un LSR realiza 3 operaciones sobre el paquete: Pop (retira etiqueta), Push (agrega etiqueta) y Swap (intercambia etiqueta) [13].

Existen 3 tipos de LSR [13]:

- Ingress LSR: Recibe un paquete sin etiqueta, agrega una o más etiquetas (Push) y transmite el paquete.
- Egress LSR: Recibe un paquete con etiqueta, remueve la etiqueta (Pop) y transmite el paquete.
- Intermediate LSR: Recibe un paquete con etiqueta, intercambia la etiqueta (Swap) y transmite el paquete.

A los router Ingress LSR y Egress LSR también se les conoce como Router PE (Provider Edge) y al router Intermediate LSR se le conoce como Router P (Provider).

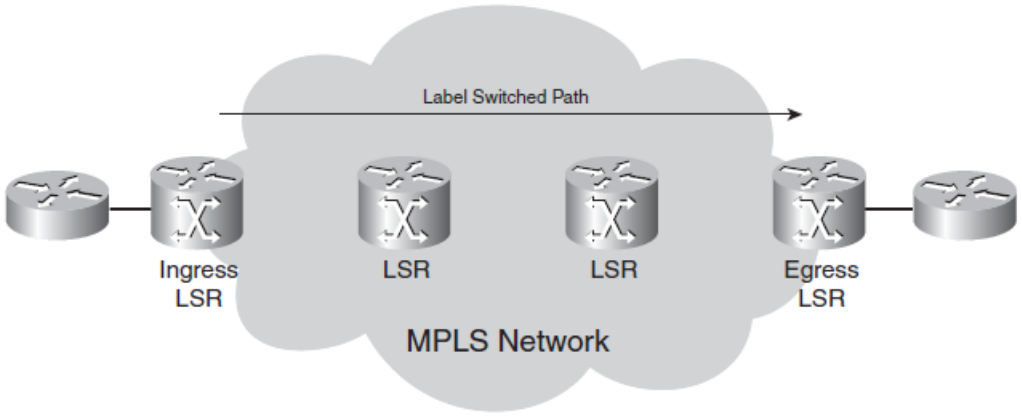


Figura 4.11 – Elementos de una red MPLS [13].

4.4.5 – Label Switched Path (LSP)

Un LSP es la ruta o camino que toma un paquete a través de la red MPLS. Es la secuencia de routers LSR que conmutan el paquete según su etiqueta. El primer router en el LSP es el “Ingress LSR”, el ultimo router en el LSP es el “Egress LSR”, todos los routers intermedios son “Intermediate LSR”.

4.4.6 – Label Distribution Protocol (LDP)

LDP es el protocolo encargado de la distribución de etiquetas entre los LSR en la red MPLS. A cada prefijo IP en la tabla de enrutamiento, el LSR le asigna una etiqueta, creando así un mapeo local de etiqueta-prefijo. El router LSR distribuye este mapeo a sus vecinos LDP, el cual se convierte en un mapeo remoto para sus vecinos LDP. Todas las asociaciones o mapeos de etiqueta-prefijo, tanto local como remota, se almacenan en una tabla llamada “Label Information Base” (LIB). El LSR debe escoger uno de estos mapeos para utilizarlo en la transmisión de paquetes hacia ese prefijo, esto se hace a través de la tabla de enrutamiento, la cual contiene la mejor ruta hacia dicho prefijo. El mapeo asociado a la mejor ruta según la tabla de enrutamiento se almacena en una tabla llamada “Label Forwarding Information Base” (LFIB) y es la utilizada para la transmisión de paquetes etiquetados. La tabla LFIB puede contener etiquetas que no fueron asignadas y distribuidas por LDP. En el caso de MPLS Traffic Engineering, las etiquetas son distribuidas por el protocolo RSVP. En el caso de MPLS VPN, la etiqueta VPN es distribuida por BGP.

LDP cumple cuatro funciones:

- Descubrir LSR que corren LDP.
- Establecer y mantener sesiones LDP.
- Anunciar el mapeo de etiquetas.
- Envío de notificaciones.

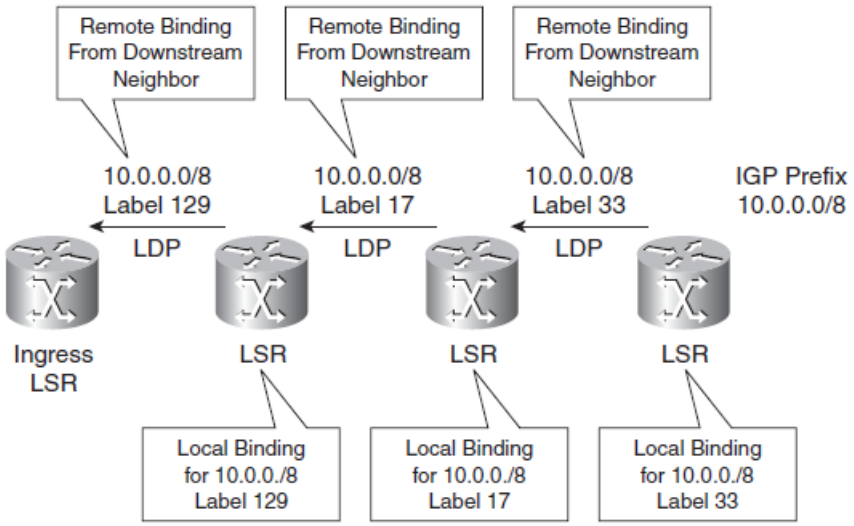


Figura 4.12 – Distribución de etiquetas con LDP [13].

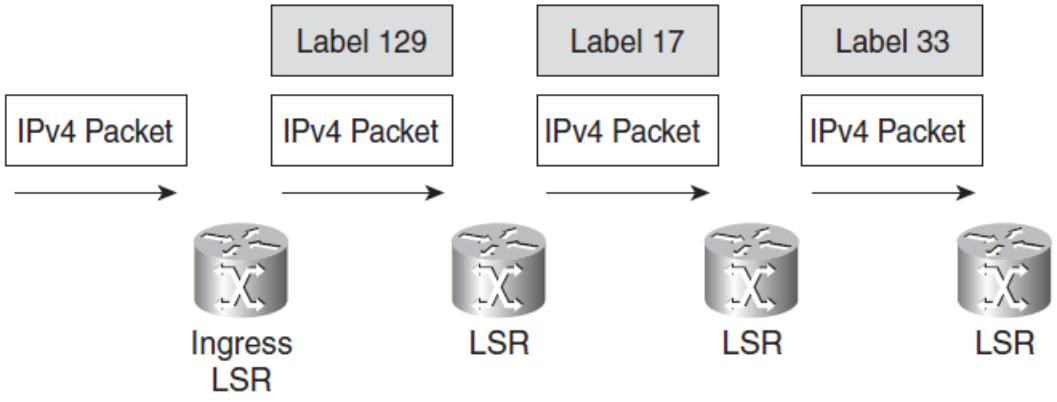


Figura 4.13 – Transmisión de un paquete etiquetado [13].

4.4.7 – MPLS VPN

Una VPN es una red que emula una red privada en una infraestructura común. La VPN puede proveer comunicación en Capa 2 o Capa 3. Una VPN se asigna a una compañía e interconecta todas sus oficinas usando la infraestructura de red del proveedor de servicios. La VPN de un servicio está aislada de otras VPNs de otros servicios, pero podrían interconectarse si así se requiere. MPLS VPN es el servicio más común popular en una red MPLS.

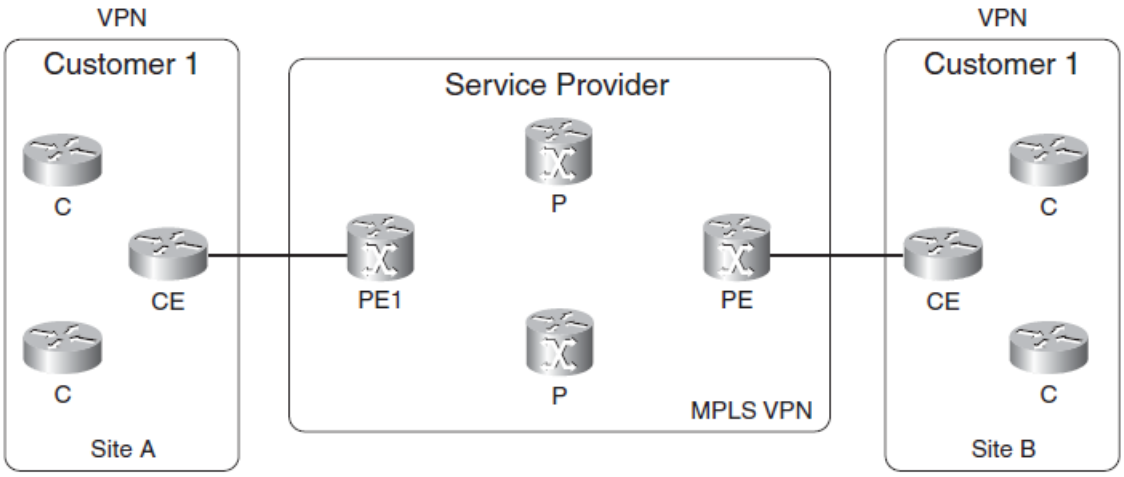


Figura 4.14 – Diagrama esquemático de un servicio MPLS VPN [13].

En la figura 5.14 se detalla la terminología concerniente al servicio MPLS VPN. Un router PE (Provider Edge) tiene conexión directa con el router CE (Customer Edge). El router P (Provider) no tiene conexión con los router del cliente. Los routers P y PE corren MPLS, es decir, son capaces de transmitir paquete etiquetados. El router CE tiene conexión directa en capa 3 con el router PE y entre ellos corren algún protocolo de enrutamiento dinámico o estático para el intercambio de información de redes. El router CE no corre MPLS. El router C (Customer) es un router interno en las premisas del cliente y no tiene conexión directa con los router del proveedor.

4.4.8 – Arquitectura de MPLS VPN

Virtual Routing and Forwarding (VRF)

Una VRF es una instancia privada para el enrutamiento y transmisión de paquetes. Un router PE tiene una VRF por cada servicio VPN. Cada VRF representa una tabla de enrutamiento privada propia de cada servicio VPN (cliente/servicio).

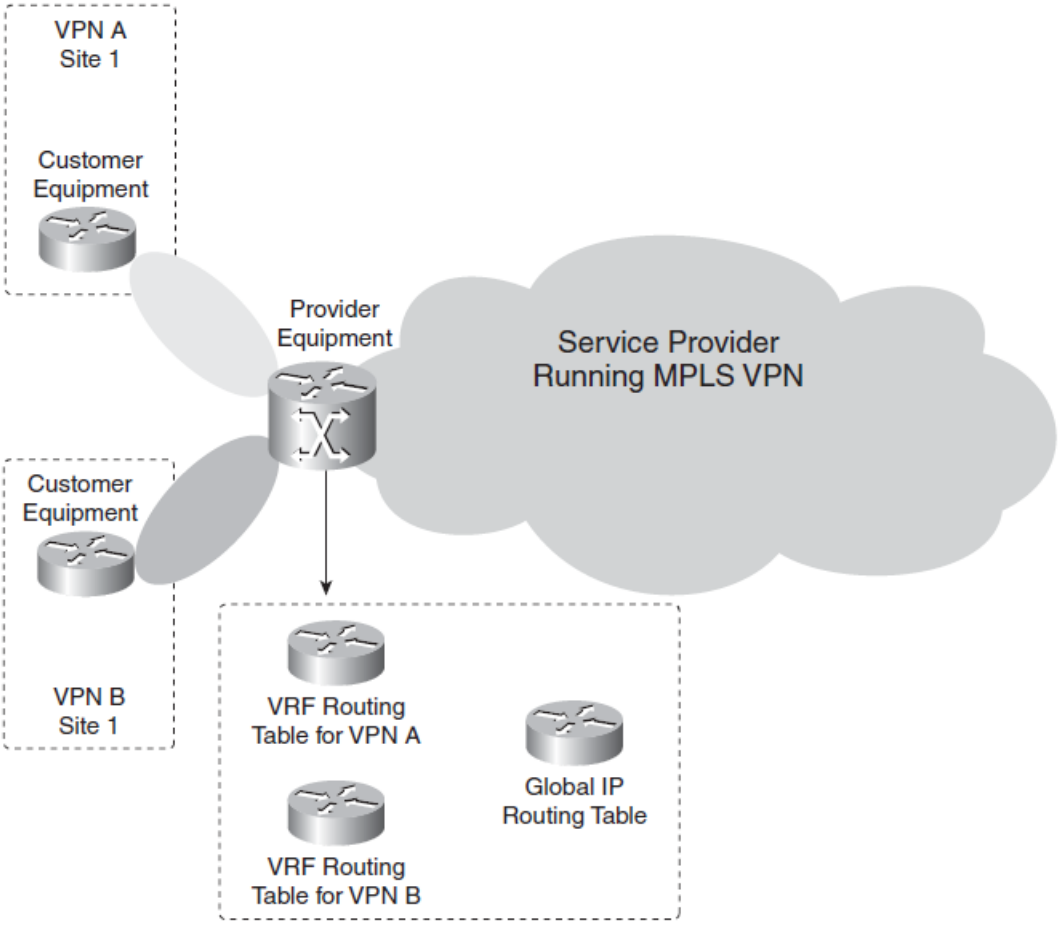


Figura 4.15 – Tablas de rutas en un Router PE [13].

Route Distinguisher (RD)

Los prefijos VPN se propagan de PE a PE en la red MPLS a través de MP-BGP (Multiprotocol BGP). El concepto de RD se utiliza para evitar traslape entre prefijos de los diferentes servicios VPN cuando son propagados por MP-BGP.

El RD es un campo de 64 bits que se agrega a los prefijos IPv4 con la finalidad de hacerlos únicos cuando son transportados por MP-BGP. El RD puede tener dos formatos: *ASN:nn* o *IP-Address:nn*, donde nn representa un número entero y ASN es el Numero de Sistema Autónomo. El formato *ASN:nn* es el más usado comúnmente. La combinación de RD+Prefijo IPv4 forma un prefijo VPNv4 de 96 bits.

Route Target (RT)

El RT es una comunidad extendida de BGP que sirve para indicar qué prefijos se deben importar desde MP-BGP a la VRF. El prefijo VPNv4 transportado en MP-BGP se verifica buscando el o los RT con el que fue exportado en la VRF origen para poder instalarlo en la tabla de ruta de la VRF destino, si no existe match con los RT del prefijo, entonces el prefijo se descarta.

Propagación de rutas VPNv4 en una red MPLS VPN

La propagación de prefijos VPNv4 en una red MPLS VPN ocurre de la siguiente forma:

El router CE anuncia al PE prefijos IPv4 por medio de un protocolo de enrutamiento IGP o eBGP o enrutamiento estático. El prefijo IPv4 se coloca en la tabla de enrutamiento de la VRF asociada a la interfaz conectada al router CE; a esos prefijos se les agrega (antepone) el RD para convertirlos en prefijos VPNv4 y así ser anunciados por MP-BGP a los otros router PE en la red MPLS. En los router PE destino se retira el RD y se instalan como prefijos IPv4 en la tabla de ruta de la VRF correspondiente. Los prefijos IPv4 son anunciados al router CE usando el protocolo de enrutamiento que este corriendo entre el PE y el CE.

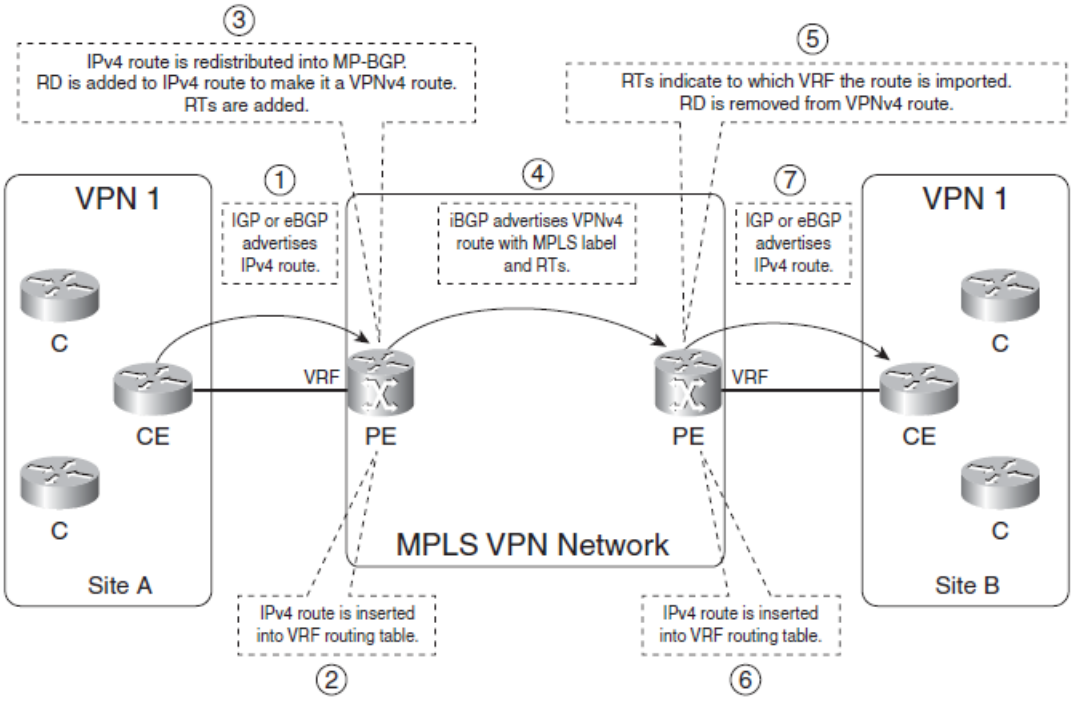


Figura 4.16 – Propagación de rutas VPNv4 en la red MPLS VPN [13].

Transmisión de paquetes en una red MPLS VPN

Un paquete IPv4 recibido en el PE de ingreso, enviado por el router CE, es etiquetado por el PE con 2 etiquetas. La etiqueta superior, llamada “IGP Label”, es la utilizada por los equipos de la red MPLS (PE y P) para trasmitir el paquete desde el PE de ingreso hacia el PE de egreso. La etiqueta “IGP Label” es distribuida en la red usando LDP

La segunda etiqueta o etiqueta inferior, llamada “VPN Label”, indica la VRF a la cual pertenece el paquete y es utilizada por el PE de egreso para enviar el paquete IPv4 al CPE correspondiente. Esta etiqueta es anunciada de PE a PE usando MP-BGP.

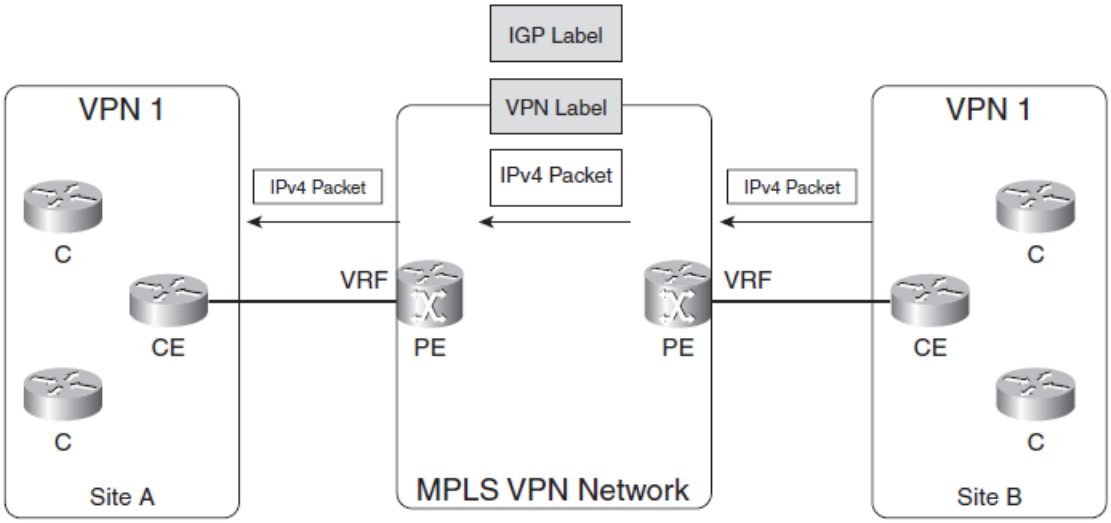


Figura 4.17 – Transmisión de paquete en la red MPLS VPN [13].

Extensiones Multiprotocolo de BGP

El RFC 2858 “Multiprotocol Extensions for BGPv4” define las extensiones de BGPv4 para que el protocolo sea capaz de transportar información adicional a IPv4. Estas extensiones son: Address Family Identifier (AFI) y Subsequent Address Family Identifier (SAFI) las cuales describen que tipo de ruta se transporta por BGP. Las AFI actualmente disponibles son IPv4, IPv6, VPNv4 y VPNv6. Las SAFI que se pueden especificar son unicast, multicast, VRF, MDT. BGP incluye los atributos AFI y SAFI en cada ruta que anuncia.

Route Reflector (RR)

En una red MPLS VPN, se requiere que cada router PE establezca sesiones iBGP con el resto de router PE de la red, es decir, en una red MPLS con “n” cantidad de router PE, cada PE debe establecer “n-1” sesiones iBGP, en la red se establece un total de n(n-1)/2 sesiones iBGP. En una red de un ISP, que puede tener un tamaño considerable, la administración del número de sesiones por PE se vuelve inmanejable. Los Route Reflector y Confederaciones BGP son soluciones para este escenario, siendo el primero la solución más utilizada en las redes de proveedores.

Un RR es un router que establece sesiones iBGP con todos los PE de la red, el RR refleja las rutas que le son anunciadas por los PE, así, los PE no requieren establecer sesiones entre ellos, únicamente contra el RR.

4.5 Multicast VPN (mVPN)

4.5.1 – Arquitectura

Dominio Multicast

Un dominio multicast es el conjunto de VRFs habilitadas con multicast (mVRF) y que pueden enviar tráfico multicast entre sí. En un dominio multicast se mapean todos los grupos multicast de una VPN en particular, a un solo grupo multicast asignado por el proveedor de servicios. Lo anterior se logra encapsulando el paquete multicast original del cliente, dentro de un paquete multicast global. La dirección origen del paquete multicast global es la dirección utilizada por el PE origen (Ingress PE) para establecer la sesión MPBGP. La dirección destino del paquete global es la dirección de grupo multicast asignada por el ISP al servicio mVPN. Se requiere una dirección global de grupo multicast para cada dominio multicast. Por cada dominio multicast se establecen túneles GRE punto-multipunto desde el PE origen hacia el resto de PE que conforman el dominio VPN. Cada PE configurado con la mVRF del cliente forma parte del dominio multicast de ese cliente.

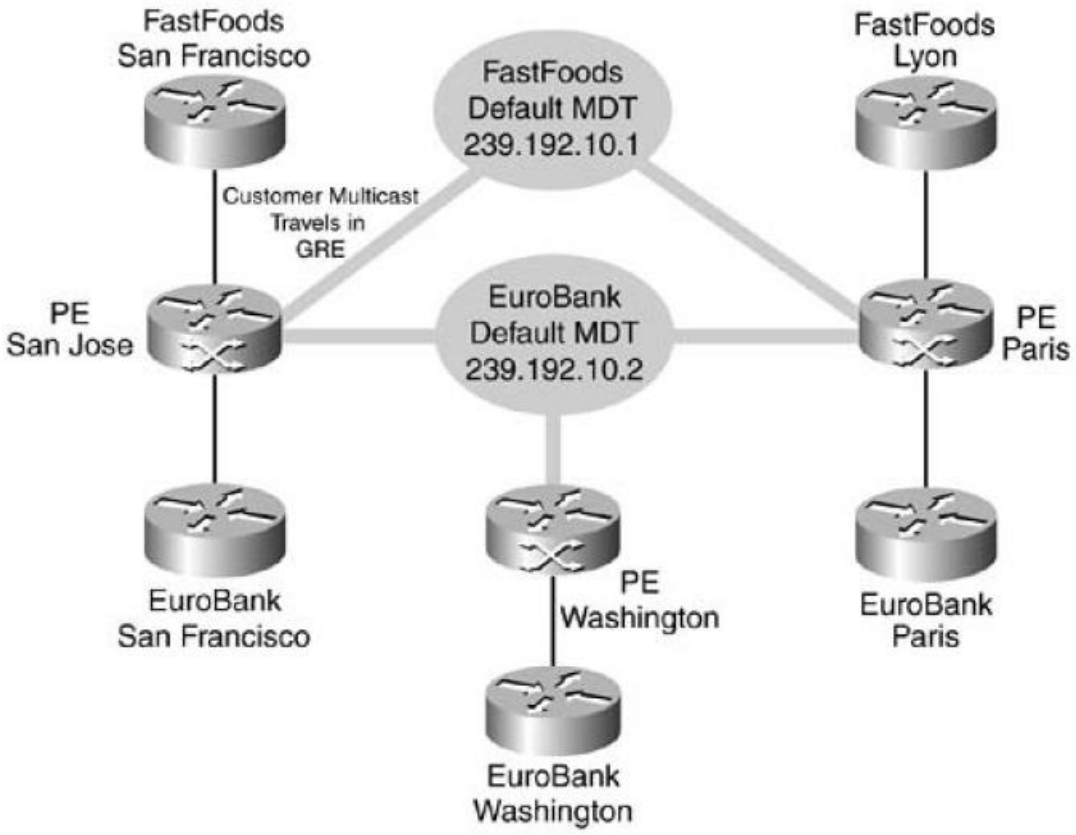


Figura 4.18 – Dominio Multicast [12].

Multicast VRF (mVRF)

Una mVRF contiene toda la información de enrutamiento multicast de un servicio VPN. Permite la separación de diferentes servicios multicast a través de una VPN, y con esto, la reutilización de grupos multicast entre los servicios sin riesgo de traslape, similar a las VPN unicast. La red del proveedor de servicios construye un árbol de distribución multicast (Default-MDT) entre los PE por cada dominio multicast. A cada dominio multicast el proveedor le asigna una dirección única de grupo mumlticast y se le conoce como “MDT-Group”. Cada mVRF pertenece a un árbol de distribución multicast (Default-MDT).

Adyacencias PIM

Cada mVRF tiene una única instancia PIM creada en el router PE. Esta instancia PIM forma una adyacencia con cada router CE cuya interfaz que lo conecta fue habilitada con el protocolo PIM dentro de la VRF. Además de esta adyacencia, el router PE forma otros dos tipos de adyacencias. La primera es una adyacencia PIM, a través de una interfaz túnel multicast (MTI: Multicast Tunnel Interface), con los otros router PE que tienen una mVRF configurada en el mismo dominio multicast. La interfaz MTI se utiliza para transportar información multicast entre las mVRF.

El segundo tipo de adyacencia PIM es la que se establece en la instancia PIM global. El router PE establece esta adyacencia con los router P o con otros router PE directamente conectados. La instancia PIM global es utilizada para crear MDT que conectan las mVRF de cada PE.

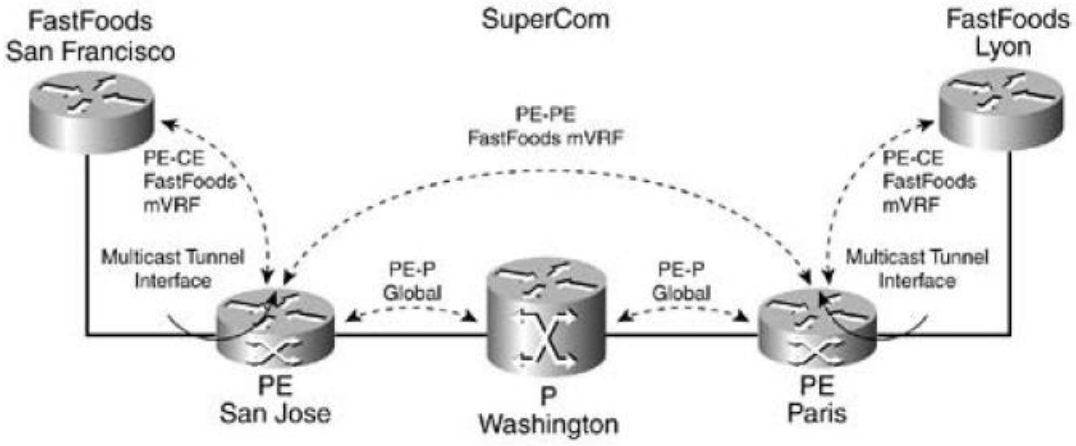


Figura 4.19 – Adyacencias PIM mVPN [12].

Multicast Distribution Tree (MDT)

Los MDT son túneles multicast en la red del proveedor de servicios. Por los MDTs se transporta el tráfico multicast de los clientes encapsulado en túneles GRE que forman parte del mismo dominio multicast.

Hay dos tipos de MDT:

Default-MDT: Una mVRF utiliza este tipo de MDT para enviar tráfico multicast con bajo consumo de ancho de banda o para enviar tráfico a un gran número de receptores. El Default-MDT es utilizado siempre para enviar tráfico de control multicast entre router PE en un dominio mulitcast.

Data-MDT: este tipo de MDT se usa para enviar alto volumen de tráfico multicast a los router PE interesados. Data-MDT evita el envío innecesario de tráfico multicast a todos los router PE de un dominio multicast.

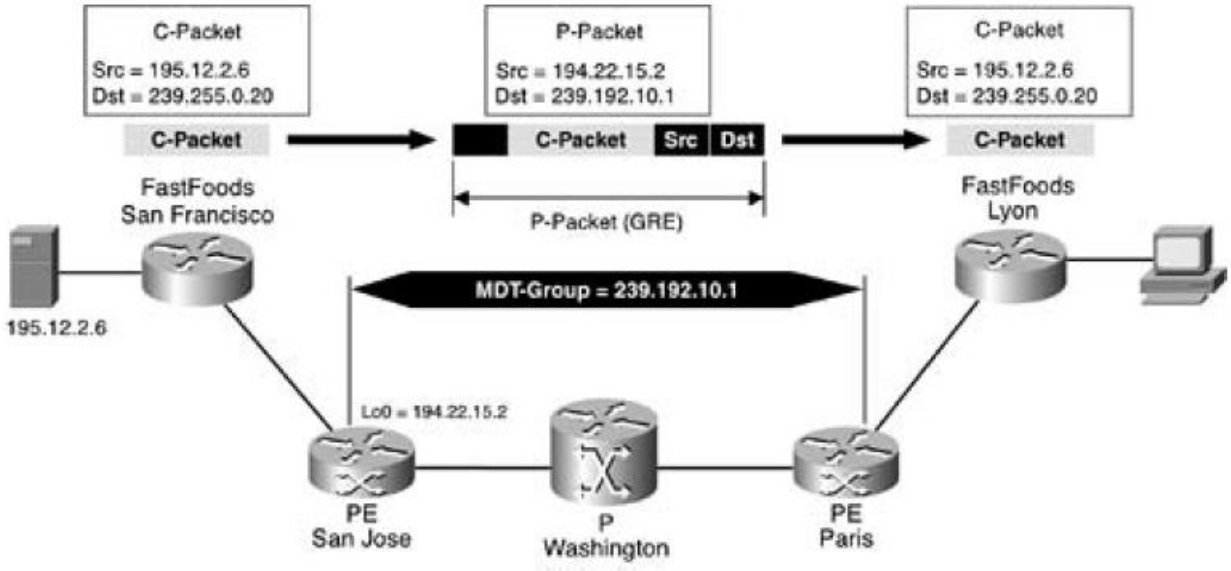


Figura 4.20 – Encapsulado de paquete MDT [12].

Multicast Tunnel Interface (MTI)

La interfaz MTI es una interfaz virtual que se forma automaticamente cuando se configura el grupo Default-MDT en la mVRF. En esta interfaz se forman las adyacencias PIM del PE local contra el resto de PE en la red del proveedor que forman parte del dominio multicast de la mVRF. La interfaz MTI no se puede configurar de forma explícita, esta interfaz deriva sus propiedades IP de la interfaz utiliza para establecer la sesión MPBGP con el resto de PE en la red MPLS.

4.6 Diseño de la Red MPLS

El diseño de la red MPLS del proveedor de servicios de telecomunicaciones (ISP) que se utilizará para los casos de estudios se define de la siguiente forma:

Backbone con capacidad de 100Gbps conformado por 2 equipos en el nivel Core, 3 equipos en el nivel de Borde y 2 equipos con funciones de Route Reflector. Se implementa OSPF como protocolo IGP para el enrutamiento dinámico y el protocolo LDP para el intercambio de etiquetas MPLS entre los equipos de la red del proveedor.

Core (P): 2 equipos Cisco CRS-8 distribuidos en Managua (nodos Villa Fontana y Las Palmas).

Edge (PE): 3 equipos Cisco ASR9006 distribuidos en Managua, Masaya y León. Cada PE se conecta hacia los Core a 100Gbps en una topología redundante “Dual-Home”.

Route Reflectors (RR): 2 equipos Cisco ASR9001 distribuidos en Managua (nodos Villa Fontana y Las Palmas). Cada RR conecta a 1Gbps hacia su Core local.

Tabla 4.1 – Descripción de equipos en la red.

NEMONICO DE EQUIPO	FUNCION	NODO DE UBICACION	CONEXIONES
CORE_1	Core (P)	Villa Fontana	RR
			CORE_2
			PE_1 - Conexión 1
			PE_2 - Conexión 1
			PE_3 - Conexión 1
CORE_2		Las Palmas	CORE_1
			PE_1 - Conexión 2
			PE_2 - Conexión 2
			PE_3 - Conexión 2
RR	Route Reflector	Villa Fontana	CORE_1
PE_1	Edge (PE)	Villa Fontana	CORE_1 – Conexión 1
			CORE_2 – Conexión 2
PE_2		Masaya	CORE_1 – Conexión 1
			CORE_2 – Conexión 2
PE_3		León	CORE_1 – Conexión 1
			CORE_2 – Conexión 2

Tabla 4.2 – Direccionamiento (IP Planning) Red MPLS.

EQUIPO	DIRECCION IP LOOPBACK	CONEXIONES	INTERFAZ	DIRECCION IP INTERFAZ
CORE_1	10.0.0.1/32	CORE_2	Gi0/0/0/0	10.0.1.1/30
		RR	Gi0/0/0/1	10.0.1.5/30
		PE_1 - Conexión 1	Gi0/0/0/2	10.0.1.9/30
		PE_2 - Conexión 1	Gi0/0/0/3	10.0.1.17/30
		PE_3 - Conexión 1	Gi0/0/0/4	10.0.1.21/30
CORE_2	10.0.0.2/32	CORE_1	Gi0/0/0/0	10.0.1.2/30
		INTERNET	Gi0/0/0/1	10.0.1.201/30
		PE_1 - Conexión 2	Gi0/0/0/2	10.0.1.13/30
		PE_2 - Conexión 2	Gi0/0/0/3	10.0.1.29/30
		PE_3 - Conexión 2	Gi0/0/0/4	10.0.1.25/30
RR	10.0.0.100/32	CORE_1	Gi0/0/0/0	10.0.1.6/30
PE_1	10.0.0.3/32	P_VF – Conexión 1	Gi0/0/0/0	10.0.1.10/30
		P_LP – Conexión 2	Gi0/0/0/1	10.0.1.14/30
PE_2	10.0.0.4/32	P_VF – Conexión 1	Gi0/0/0/0	10.0.1.18/30
		P_LP – Conexión 2	Gi0/0/0/1	10.0.1.30/30
PE_3	10.0.0.5/32	P_VF – Conexión 1	Gi0/0/0/0	10.0.1.22/30
		P_LP – Conexión 2	Gi0/0/0/1	10.0.1.26/30

Tabla 4.3 – Protocolos de enrutamiento en la Red MPLS.

EQUIPO	BGP ASN	PROCESO OSPF	AREA OSPF
CORE_1	64512	64512	0 (Backbone)
CORE_2			0 (Backbone)
RR			1
PE_MGA			2
PE_MSY			3
PE_LEO			4
INTERNET	1	-	-

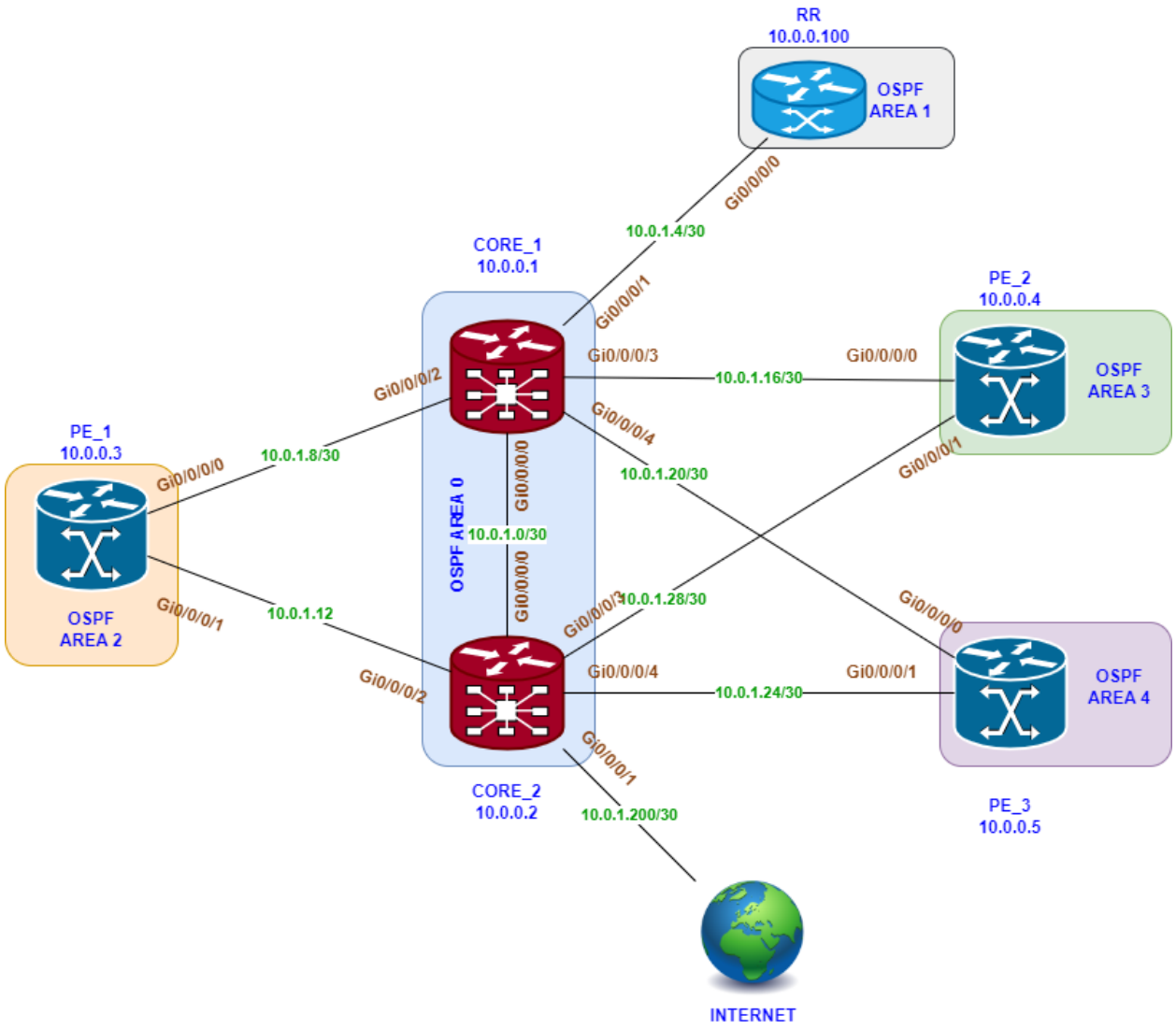


Figura 4.12 – Red de Servicio MPLS.

4.6.1 Configuraciones

En este segmento se muestran las configuraciones de los equipos de la red del ISP, éstas son las configuraciones necesarias para brindar servicios MPLS: L2VPN, L3VPN, MVPN, como son:

- OSPF como protocolo de enrutamiento dinámico IGP.
- MPLS/LDP para asignación y propagación de etiquetas.
- BGP para la propagación de prefijos en la red entre los PE.
- PIM para la transmisión de paquetes multicast para servicio de video.

Así mismo, se muestran ejemplos para validar el estado de las configuraciones, adyacencias, sesiones, etc. en los equipos.

Los equipos mostrados como ejemplo son CORE_1 (P), Route Reflector y PE_1 (PE). La configuración completa de todos los equipos de la red se encuentra en el Anexo de este documento.

Configuración Router CORE_1 (P)

- **Interfaces:**

```
interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 description CORE_2 Gi0/0/0/0
 cdp
 mtu 9000 ! MTU PARA SOPORTAR LAS MULTIPLES ETIQUETAS MPLS.
 ipv4 address 10.0.1.1 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 description RR Gi0/0/0/0
 cdp
 ipv4 address 10.0.1.5 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 description PE_1 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.9 255.255.255.252
!
```

```
interface GigabitEthernet0/0/0/3
 description PE_2 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.17 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 description PE_3 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.21 255.255.255.252
!
```

- **Validaciones - Interfaces:**

```
RP/0/0/CPU0:CORE_1#sh cdp neighbors
Tue Apr  4 22:03:06.481 UTC
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Local Intrfce    Holdtme Capability Platform  Port ID
CORE_2          Gi0/0/0/0        136     R          IOS XRv S Gi0/0/0/0
RR              Gi0/0/0/1        131     R          IOS XRv S Gi0/0/0/0
PE_1            Gi0/0/0/2        136     R          IOS XRv S Gi0/0/0/0
PE_2            Gi0/0/0/3        135     R          IOS XRv S Gi0/0/0/0
PE_3            Gi0/0/0/4        168     R          IOS XRv S Gi0/0/0/0
RP/0/0/CPU0:CORE_1#
```

Figura 4.13 – Vecinos CDP (Cisco Discovery Protocol).

- **Protocolo de enrutamiento IGP (OSPF):**

```
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.1
 passive enable ! DESACTIVA EL ENVIO DE PAQUETES HELLO OSPF EN TODAS LAS INTERFACES.
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 0
  authentication message-digest ! ACTIVA AUTENTICACION PARA OSPF EN EL AREA 0.
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   message-digest-key 1 md5 encrypted 104D000A0618 ! PASSWORD PARA LA ADAYACENCIA OSPF.
   network point-to-point
   passive disable ! ACTIVA EL ENVIO DE PAQUETES HELLO OSPF EN LA INTERFAZ.
  !
 !
 area 1
  authentication message-digest
  interface GigabitEthernet0/0/0/1
   message-digest-key 1 md5 encrypted 05080F1C2243
   network point-to-point
   passive disable
  !
 !
 area 2
```

```
  authentication message-digest
  interface GigabitEthernet0/0/0/2
   message-digest-key 1 md5 encrypted 13061E010803
   network point-to-point
   passive disable
  !
 !
 area 3
  authentication message-digest
  interface GigabitEthernet0/0/0/3
   message-digest-key 1 md5 encrypted 045802150C2E
   network point-to-point
   passive disable
  !
 !
 area 4
  authentication message-digest
  interface GigabitEthernet0/0/0/4
   message-digest-key 1 md5 encrypted 00071A150754
   network point-to-point
   passive disable
  !
 !
!
```

- **Validaciones - OSPF:**

```
RP/0/0/CPU0:CORE_1#sh ospf neighbor area-sorted
Tue Apr  4 22:08:54.748 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 64512

Area 0
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.2        1   FULL/  - 00:00:30  10.0.1.2        00:10:34 Gi0/0/0/0

Total neighbor count: 1

Area 1
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.100      1   FULL/  - 00:00:39  10.0.1.6        00:10:35 Gi0/0/0/1

Total neighbor count: 1

Area 2
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.3        1   FULL/  - 00:00:36  10.0.1.10       00:10:33 Gi0/0/0/2

Total neighbor count: 1

Area 3
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.4        1   FULL/  - 00:00:30  10.0.1.18       00:10:33 Gi0/0/0/3

Total neighbor count: 1

Area 4
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.5        1   FULL/  - 00:00:35  10.0.1.22       00:10:33 Gi0/0/0/4

Total neighbor count: 1
```

).

Figura 4.14 – Adyacencias OSPF (por área).

```
RP/0/0/CPU0:CORE_1#sh route ospf
Tue Apr  4 22:18:57.376 UTC

O    10.0.0.2/32 [110/101] via 10.0.1.2, 00:18:10, GigabitEthernet0/0/0/0
O    10.0.0.3/32 [110/101] via 10.0.1.10, 00:20:24, GigabitEthernet0/0/0/2
O    10.0.0.4/32 [110/101] via 10.0.1.18, 00:20:26, GigabitEthernet0/0/0/3
O    10.0.0.5/32 [110/101] via 10.0.1.22, 00:20:27, GigabitEthernet0/0/0/4
O    10.0.0.100/32 [110/65536] via 10.0.1.6, 00:20:37, GigabitEthernet0/0/0/1
O    10.0.1.12/30 [110/200] via 10.0.1.10, 00:20:24, GigabitEthernet0/0/0/2
O    10.0.1.24/30 [110/200] via 10.0.1.22, 00:20:27, GigabitEthernet0/0/0/4
O    10.0.1.28/30 [110/200] via 10.0.1.18, 00:20:26, GigabitEthernet0/0/0/3
```

Figura 4.15 – Prefijos en la tabla global aprendidos por OSPF.

- **MPLS:**

```
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
mpls ldp
 router-id 10.0.0.1
 neighbor ! PASSWORD PARA PROTEGER LAS SESIONES LDP.
  10.0.0.2:0 password encrypted 05080F1C2243
  10.0.0.3:0 password encrypted 094F471A1A0A
  10.0.0.4:0 password encrypted 01100F175804
  10.0.0.5:0 password encrypted 05080F1C2243
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS ! LIMITA LA PROPAGACION DE ETIQUETAS UNICAMENTE PARA ESTOS PREFIJOS.
    !
   !
  !
 !
 ! ACTIVA MPLS/LDP EN LAS INTERFACES INDICADAS.
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
```

- **Validaciones - MPLS:**

La figura 4.16 muestra la lista de interfaces en donde corre el proceso LDP Discovery para encontrar equipos que corren LDP. El formato del LDP Identifier, MPLS_ID:0, el cero indica que el modo de asignación de etiquetas en dicho equipo es “Per Platform” (Por Plataforma).

```
RP/0/0/CPU0:CORE_1#sh mpls ldp discovery
Tue Apr  4 22:37:24.560 UTC

Local LDP Identifier: 10.0.0.1:0
Discovery Sources:
  Interfaces:
    GigabitEthernet0/0/0/0 : xmit/recv
      VRF: 'default' (0x60000000)
      LDP Id: 10.0.0.2:0, Transport address: 10.0.0.2
          Hold time: 15 sec (local:15 sec, peer:15 sec)
          Established: Apr  4 21:58:15.331 (00:39:09 ago)

    GigabitEthernet0/0/0/2 : xmit/recv
      VRF: 'default' (0x60000000)
      LDP Id: 10.0.0.3:0, Transport address: 10.0.0.3
          Hold time: 15 sec (local:15 sec, peer:15 sec)
          Established: Apr  4 21:58:16.601 (00:39:08 ago)

    GigabitEthernet0/0/0/3 : xmit/recv
      VRF: 'default' (0x60000000)
      LDP Id: 10.0.0.4:0, Transport address: 10.0.0.4
          Hold time: 15 sec (local:15 sec, peer:15 sec)
          Established: Apr  4 21:58:18.121 (00:39:06 ago)

    GigabitEthernet0/0/0/4 : xmit/recv
      VRF: 'default' (0x60000000)
      LDP Id: 10.0.0.5:0, Transport address: 10.0.0.5
          Hold time: 15 sec (local:15 sec, peer:15 sec)
          Established: Apr  4 21:58:15.721 (00:39:08 ago)
```

Figura 4.16 – Estado del proceso LDP Discovery.

Las figuras 4.17 y 4.18 muestras los vecinos LDP y los puertos TCP utilizados en las sesiones. El puerto TCP 646 es utilizado para escuchar/recibir paquetes Hello LDP en cada router habilitado con LDP, los paquetes Hello de LDP se envían cada minuto.

```
RP/0/0/CPU0:CORE_1#sh mpls ldp neighbor
Tue Apr  4 23:05:10.066 UTC

Peer LDP Identifier: 10.0.0.2:0
  TCP connection: 10.0.0.2:32709 - 10.0.0.1:646; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 84/85; Downstream-Unsolicited
  Up time: 01:06:43
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/0
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (6)
      10.0.0.2       10.0.1.2       10.0.1.13      10.0.1.25
      10.0.1.29      10.0.1.201
    IPv6: (0)

Peer LDP Identifier: 10.0.0.5:0
  TCP connection: 10.0.0.5:33296 - 10.0.0.1:646; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 85/85; Downstream-Unsolicited
  Up time: 01:06:43
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/4
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (3)
      10.0.0.5       10.0.1.22      10.0.1.26
    IPv6: (0)
```

Figura 4.17 – Vecinos LDP establecidos.

```
Peer LDP Identifier: 10.0.0.3:0
  TCP connection: 10.0.0.3:27005 - 10.0.0.1:646; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 87/86; Downstream-Unsolicited
  Up time: 01:07:58
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/2
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (4)
      10.0.0.3       10.0.1.10      10.0.1.14      165.98.255.1
    IPv6: (0)

Peer LDP Identifier: 10.0.0.4:0
  TCP connection: 10.0.0.4:42043 - 10.0.0.1:646; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 86/87; Downstream-Unsolicited
  Up time: 01:07:56
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/3
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (3)
      10.0.0.4       10.0.1.18      10.0.1.30
    IPv6: (0)
```

Figura 4.18 – Vecinos LDP establecidos (Continuación).

En la figura 4.19, la columna “Local Label” muestra las etiquetas asignadas por el equipo CORE_1, la columna “Outgoing Label” muestra las etiquetas asignadas por sus vecinos LDP.

```
RP/0/0/CPU0:CORE_1#sh mpls forwarding
Tue Apr  4 23:13:11.773 UTC
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
Label  Label       or ID             Interface                    Switched
------ ----------- ----------------- ------------ --------------- ------------
24000  Unlabelled  10.0.0.100/32     Gi0/0/0/1    10.0.1.6        37285
24001  Pop         10.0.0.2/32       Gi0/0/0/0    10.0.1.2        22860
24002  Pop         10.0.0.5/32       Gi0/0/0/4    10.0.1.22       23335
24003  Unlabelled  10.0.1.24/30      Gi0/0/0/4    10.0.1.22       0
24004  Pop         10.0.0.4/32       Gi0/0/0/3    10.0.1.18       22439
24005  Unlabelled  10.0.1.28/30      Gi0/0/0/3    10.0.1.18       0
24006  Pop         10.0.0.3/32       Gi0/0/0/2    10.0.1.10       22631
24007  Unlabelled  10.0.1.12/30      Gi0/0/0/2    10.0.1.10       0
```

Figura 4.19 – Asignación de etiquetas (Tabla LFIB).

Configuración Route Reflector (RR)

- **Interfaces:**

```
interface Loopback0
 ipv4 address 10.0.0.100 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 description CORE_1 Gi0/0/0/1
 cdp
 ipv4 address 10.0.1.6 255.255.255.252
!
```

- **Validaciones - Interfaces:**

```
RP/0/0/CPU0:RR#sh cdp neighbors
Tue Apr  4 23:20:35.893 UTC
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Local Intrfce    Holdtme Capability Platform  Port ID
CORE_1          Gi0/0/0/0        131     R          IOS XRv S Gi0/0/0/1
```

Figura 4.20 – Vecinos CDP (Cisco Discovery Protocol).

- **OSPF:**

```
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.100
 authentication message-digest
 passive enable
 auto-cost reference-bandwidth 100000
 area 1
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   message-digest-key 1 md5 encrypted 121A0C041104
   network point-to-point
   passive disable
  !
 !
!
```

- **Validaciones - OSPF:**

```
RP/0/0/CPU0:RR#sh ospf neighbor area-sorted
Tue Apr  4 23:23:18.392 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 64512

Area 1
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.1        1   FULL/  - 00:00:30  10.0.1.5        01:24:58 Gi0/0/0/0

Total neighbor count: 1
```

Figura 4.21 – Adyacencias OSPF.

```
RP/0/0/CPU0:RR#sh route ospf
Tue Apr  4 23:24:13.708 UTC

O IA 10.0.0.1/32 [110/101] via 10.0.1.5, 01:25:53, GigabitEthernet0/0/0/0
O IA 10.0.0.2/32 [110/201] via 10.0.1.5, 01:23:25, GigabitEthernet0/0/0/0
O IA 10.0.0.3/32 [110/201] via 10.0.1.5, 01:25:40, GigabitEthernet0/0/0/0
O IA 10.0.0.4/32 [110/201] via 10.0.1.5, 01:25:42, GigabitEthernet0/0/0/0
O IA 10.0.0.5/32 [110/201] via 10.0.1.5, 01:25:42, GigabitEthernet0/0/0/0
O IA 10.0.1.0/30 [110/200] via 10.0.1.5, 01:25:53, GigabitEthernet0/0/0/0
O IA 10.0.1.8/30 [110/200] via 10.0.1.5, 01:25:53, GigabitEthernet0/0/0/0
O IA 10.0.1.12/30 [110/300] via 10.0.1.5, 01:25:40, GigabitEthernet0/0/0/0
O IA 10.0.1.16/30 [110/200] via 10.0.1.5, 01:25:53, GigabitEthernet0/0/0/0
O IA 10.0.1.20/30 [110/200] via 10.0.1.5, 01:25:53, GigabitEthernet0/0/0/0
O IA 10.0.1.24/30 [110/300] via 10.0.1.5, 01:25:42, GigabitEthernet0/0/0/0
O IA 10.0.1.28/30 [110/300] via 10.0.1.5, 01:25:42, GigabitEthernet0/0/0/0
```

Figura 4.22 – Prefijos en tabla de ruta aprendidos por OSPF.

- **BGP:**

```
route-policy BGP_TO_RIB
  drop
end-policy
!
router bgp 64512
 bgp router-id 10.0.0.100
 address-family ipv4 unicast
  table-policy BGP_TO_RIB ! IMPIDE LA INSTALACION DE PREFIJOS BGP EN LA TABLA DE RUTA.
 !
 address-family vpnv4 unicast
 !
 neighbor 10.0.0.2 ! SESION IBGP CONTRA EL ROUTER DE BORDE DE INTERNET (CORE_2).
  remote-as 64512
  password encrypted 070C285F4D06
  description BG_INTERNET
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client ! SE DEFINE COMO CLIENTE DEL RR.
  !
 !
 neighbor 10.0.0.3 ! SESION IBGP CONTRA EL PE PE_1.
  remote-as 64512
  password encrypted 121A0C041104
  description PE_1
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 neighbor 10.0.0.4 ! SESION IBGP CONTRA EL PE PE_2.
  remote-as 64512
  password encrypted 104D000A0618
  description PE_2
  update-source Loopback0
  address-family ipv4 unicast
```

```
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 neighbor 10.0.0.5 ! SESION IBGP CONTRA EL PE PE_3.
  remote-as 64512
  password encrypted 070C285F4D06
  description PE_3
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
!
```

- **Validaciones - BGP:**

En la figura 4.23 se observa que las sesiones iBGP se establecen con todos los PE de la red y el CORE_2 (10.0.0.2) ya que tiene la función de router de borde de Internet, de lo contrario no sería necesario establecer esta sesión contra los equipos Core.

```
RP/0/0/CPU0:RR#sh bgp summary
Tue Apr  4 23:28:20.841 UTC
BGP router identifier 10.0.0.100, local AS number 64512
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000000   RD version: 15
BGP main routing table version 15
BGP NSR Initial initsync version 10 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker              15         15         15         15          15           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.0.0.2          0 64512      94      95       15    0    0 01:29:56           2
10.0.0.3          0 64512      96     103       15    0    0 01:29:56           1
10.0.0.4          0 64512      95     103       15    0    0 01:29:54           0
10.0.0.5          0 64512      95     103       15    0    0 01:29:56           0
```

Figura 4.23 – Sesiones BGP IPv4 en el Route Reflector.

Las sesiones iBGP se establecen con los PE (10.0.0.3, 10.0.0.4 y 10.0.0.5).

```
RP/0/0/CPU0:RR#sh bgp vpnv4 unicast summary
Tue Apr  4 23:29:47.795 UTC
BGP router identifier 10.0.0.100, local AS number 64512
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 7
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker               7          7          7          7           7           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.0.0.3          0 64512      98     105        7    0    0 01:31:23           2
10.0.0.4          0 64512      97     105        7    0    0 01:31:20           2
10.0.0.5          0 64512      97     105        7    0    0 01:31:23           2
```

Figura 4.24 – Sesiones BGP VPNv4 en el Route Reflector.

En el Route Reflector no es necesario que los prefijos aprendidos por BGP se instalen en la tabla de enrutamiento, su función se limita a “reflejar” los prefijos que le anuncian.

```
RP/0/0/CPU0:RR#sh route bgp
Tue Apr  4 23:33:48.098 UTC

% No matching routes found

RP/0/0/CPU0:RR#sh route summary
Tue Apr  4 23:33:49.958 UTC
Route Source                     Routes     Backup     Deleted     Memory(bytes)
local                            2          0          0           320
connected                        1          1          0           320
ospf 64512                       12         0          0           1920
bgp 64512                        0          0          0           0
dagr                             0          0          0           0
Total                            15         1          0           2560
```

Figura 4.25 – Prefijos en tabla de ruta aprendidos por BGP.

Configuración Router PE_1 (PE)

- **Interfaces:**

```
interface Loopback0
 ipv4 address 10.0.0.3 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 description CORE_1 Gi0/0/0/2
 cdp
 mtu 9000
 ipv4 address 10.0.1.10 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 description CORE_2 Gi0/0/0/2
 cdp
 mtu 9000
 ipv4 address 10.0.1.14 255.255.255.252
!
```

- **Validaciones - Interfaces:**

```
RP/0/0/CPU0:PE_1#sh cdp neighbors
Tue Apr  4 23:57:10.922 UTC
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Local Intrfce    Holdtme Capability Platform  Port ID
CORE_1          Gi0/0/0/0        173     R          IOS XRv S Gi0/0/0/2
CORE_2          Gi0/0/0/1        173     R          IOS XRv S Gi0/0/0/2
```

Figura 4.26 – Vecinos CDP (Cisco Discovery Protocol).

- **Protocolo de enrutamiento IGP (OSPF):**

```
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.3
 authentication message-digest ! SE ACTIVA LA AUTENTICACION PARA TODAS LAS AREAS.
 message-digest-key 1 md5 encrypted 02050D480809
 passive enable
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 2
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
   passive disable
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
   passive disable
  !
 !
```

!

- **Validaciones - OSPF:**

Las adyacencias se establecen con los router P (Core).

```
RP/0/0/CPU0:PE_1#sh ospf neighbor area-sorted
Tue Apr  4 23:59:08.764 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 64512

Area 2
Neighbor ID     Pri State    Dead Time Address         Up Time  Interface
10.0.0.1        1   FULL/   - 00:00:35  10.0.1.9        02:00:46 Gi0/0/0/0
10.0.0.2        1   FULL/   - 00:00:39  10.0.1.13       02:00:42 Gi0/0/0/1

Total neighbor count: 2
```

Figura 4.27 – Adyacencias OSPF.

```
RP/0/0/CPU0:PE_1#sh route ospf
Wed Apr  5 00:03:17.707 UTC

O IA 10.0.0.1/32 [110/101] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.0.2/32 [110/101] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
O IA 10.0.0.4/32 [110/201] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
                 [110/201] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.0.5/32 [110/201] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
                 [110/201] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.0.100/32 [110/65636] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.1.0/30 [110/200] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
                 [110/200] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.1.4/30 [110/200] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.1.16/30 [110/200] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.1.20/30 [110/200] via 10.0.1.9, 02:02:29, GigabitEthernet0/0/0/0
O IA 10.0.1.24/30 [110/200] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
O IA 10.0.1.28/30 [110/200] via 10.0.1.13, 02:02:29, GigabitEthernet0/0/0/1
```

Figura 4.28 – Prefijos en la tabla global aprendidos por OSPF.

- **MPLS:**

```
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
mpls ldp
 router-id 10.0.0.3
 neighbor
  10.0.0.1:0 password encrypted 104D000A0618
  10.0.0.2:0 password encrypted 045802150C2E
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
!
```

- **Validaciones - MPLS:**

```
RP/0/0/CPU0:PE_1#sh mpls ldp neighbor
Wed Apr  5 00:05:46.967 UTC

Peer LDP Identifier: 10.0.0.2:0
  TCP connection: 10.0.0.2:646 - 10.0.0.3:20200; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 155/153; Downstream-Unsolicited
  Up time: 02:07:17
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/1
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (6)
      10.0.0.2       10.0.1.2       10.0.1.13      10.0.1.25
      10.0.1.29      10.0.1.201
    IPv6: (0)

Peer LDP Identifier: 10.0.0.1:0
  TCP connection: 10.0.0.1:646 - 10.0.0.3:27005; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 154/154; Downstream-Unsolicited
  Up time: 02:07:17
  LDP Discovery Sources:
    IPv4: (1)
      GigabitEthernet0/0/0/0
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (6)
      10.0.0.1       10.0.1.1       10.0.1.5       10.0.1.9
      10.0.1.17      10.0.1.21
    IPv6: (0)
```

Figura 4.29 – Vecinos LDP establecidos.

Las direcciones IP de las interfaces loopback de los router de la red MPLS son las únicas a las que los router propagan, con LDP, las etiquetas que les asignaron.

```
RP/0/0/CPU0:PE_1#sh mpls forwarding
Wed Apr  5 00:06:53.702 UTC
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
Label  Label       or ID             Interface                    Switched
------ ----------- ----------------- ------------ --------------- ------------
24000  Pop         10.0.0.1/32       Gi0/0/0/0    10.0.1.9        19992
24001  Pop         10.0.0.2/32       Gi0/0/0/1    10.0.1.13       19770
24002  24000       10.0.0.100/32     Gi0/0/0/0    10.0.1.9        19530
24003  24004       10.0.0.4/32       Gi0/0/0/0    10.0.1.9        0
       24007       10.0.0.4/32       Gi0/0/0/1    10.0.1.13       0
24004  24002       10.0.0.5/32       Gi0/0/0/0    10.0.1.9        0
       24003       10.0.0.5/32       Gi0/0/0/1    10.0.1.13       0
24005  Unlabelled  10.0.1.0/30       Gi0/0/0/0    10.0.1.9        0
       Unlabelled  10.0.1.0/30       Gi0/0/0/1    10.0.1.13       0
24006  Unlabelled  10.0.1.4/30       Gi0/0/0/0    10.0.1.9        0
24007  Unlabelled  10.0.1.16/30      Gi0/0/0/0    10.0.1.9        0
24008  Unlabelled  10.0.1.20/30      Gi0/0/0/0    10.0.1.9        0
24009  Unlabelled  10.0.1.24/30      Gi0/0/0/1    10.0.1.13       0
24010  Unlabelled  10.0.1.28/30      Gi0/0/0/1    10.0.1.13       0
24011  Aggregate   CORP_1: Per-VRF Aggr[V]   \
                                     CORP_1                       0
```

Figura 4.30 – Asignación de etiquetas (Tabla LFIB).

- **BGP:**

```
router bgp 64512
 bgp router-id 10.0.0.3
 address-family ipv4 unicast
  network 165.98.255.0/30
 !
 address-family vpnv4 unicast
  vrf all
   label mode per-vrf
  !
 !
 neighbor 10.0.0.100 ! SESION IBGP IPV4/VPNV4 CONTRA EL RR.
  remote-as 64512
  password encrypted 104D000A0618
  description RR
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
  address-family vpnv4 unicast
  !
 !
!
```

- **Validaciones - BGP:**

La sesión iBGP se establece con el Router Reflector.

```
RP/0/0/CPU0:PE_1#sh bgp summary
Wed Apr  5 00:18:53.663 UTC
BGP router identifier 10.0.0.3, local AS number 64512
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000000   RD version: 16
BGP main routing table version 16
BGP NSR Initial initsync version 6 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker              16         16         16         16          16           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.0.0.100        0 64512     154     147       16    0    0 02:20:28          2
```

Figura 4.31 – Sesiones BGP IPv4.

La sesión iBGP se establece con el Router Reflector.

```
RP/0/0/CPU0:PE_1#sh bgp vpnv4 unicast summary
Wed Apr  5 00:19:58.789 UTC
BGP router identifier 10.0.0.3, local AS number 64512
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 16
BGP NSR Initial initsync version 11 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker              16         16         16         16          16           0

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.0.0.100        0 64512     155     148       16    0    0 02:21:33          4
```

Figura 4.32 – Sesiones BGP VPNv4.

4.7 Casos de Estudio.

4.7.1 - Caso de Estudio #1: Transmisión de Datos.

Una empresa corporativa ha contratado a un ISP el servicio para conectar su oficina central con sus oficinas remotas distribuidas en diferentes zonas geográficas del país. Las oficinas remotas deben acceder a los servidores corporativos ubicados en el Data Center de la oficina central, así mismo, las oficinas remotas tendrán acceso a Internet a través de la oficina central quien posee un bloque público asignado por el ISP.

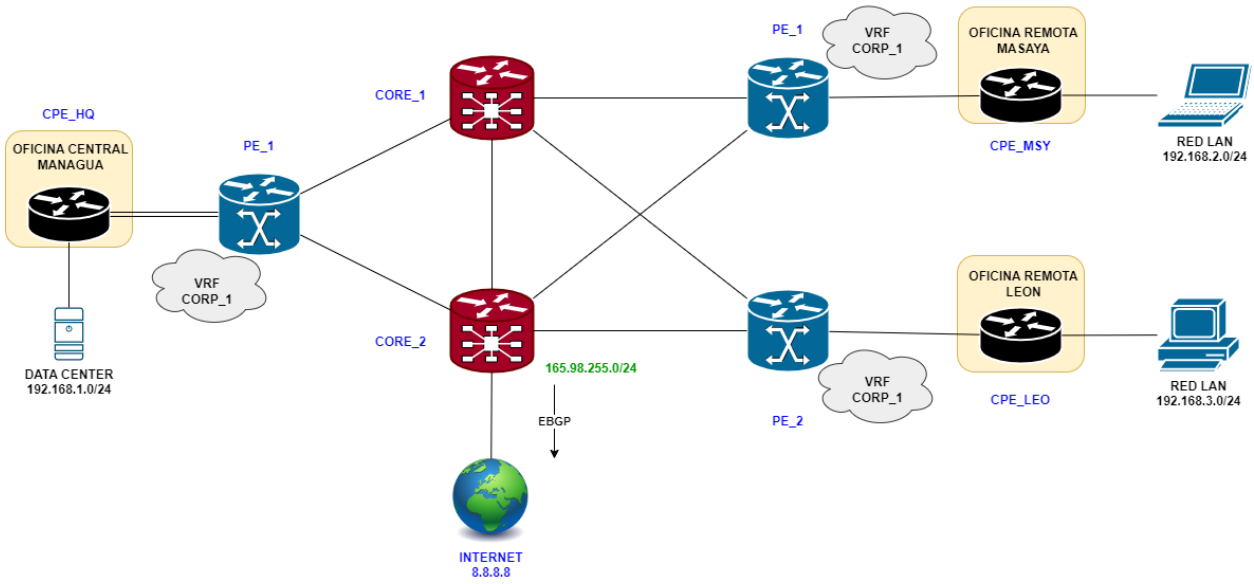


Figura 4.33 – Red de Servicio MPLS – Transmisión de Datos.

Tabla 4.4 – Recursos asignados al servicio.

SERVICIO	SITIO	VRF (RD/RT)	VLAN	RED WAN
Oficina Central	INTERNET	TABLA GLOBAL	100	165.98.255.0/30
	DATOS	CORP_1 (64512:1)	101	10.255.1.0/30
Oficina Masaya	DATOS	CORP_1 (64512:1)	-	10.255.1.4/30
Oficina León	DATOS	CORP_1 (64512:1)	-	10.255.1.8/30

Tabla 4.5 – Direccionamiento (IP Planning) cliente corporativo.

EQUIPO	RED LAN	CONEXIONES	SERVICIO	INTERFAZ	DIRECCION IP INTERFAZ
CPE_HQ	192.168.1.0/24	PE_1	INTERNET	Gi0/0.100	165.98.255.2/30
		PE_1	DATOS	Gi0/0.101	10.255.1.2/30
CPE_MSY	192.168.2.0/24	PE_2	DATOS	Gi0/0	10.255.1.6/30
CPE_LEO	192.168.3.0/24	PE_3	DATOS	Gi0/0	10.255.1.10/30

Tabla 4.6 – Protocolos de enrutamiento cliente corporativo.

EQUIPO	SERVICIO	PROTOCOLO DE ENRUTAMIENTO
CPE_HQ	INTERNET	-
	DATOS	OSPF 101
CPE_MSY	DATOS	OSPF 101
CPE_LEO	DATOS	OSPF 101

Configuración Router PE_1

- **Servicio VPN:**

```
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
```

```
router bgp 64512
 vrf CORP_1
  rd 64512:1
  default-information originate
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.1
  domain-tag 64512
  passive enable
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4.101
    network point-to-point
    passive disable
   !
  !
 !
!

interface GigabitEthernet0/0/0/4.101
 description SERVICIO DATOS
 vrf CORP_1
 ipv4 address 10.255.1.1 255.255.255.252
 encapsulation dot1q 101
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_1#sh ospf vrf CORP_1 neighbor
Wed Apr  5 17:43:00.577 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 101, VRF CORP_1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.2      1     FULL/  -        00:00:39    10.255.1.2      GigabitEthernet0/0/0/4.101
    Neighbor is up for 00:10:55

Total neighbor count: 1
```

Figura 4.34 – Adyacencia OSPF contra el router CPE de la oficina central.

```
RP/0/0/CPU0:PE_1#sh route vrf CORP_1
Wed Apr  5 17:46:13.863 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route
       M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is 10.255.1.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.255.1.2, 00:14:07, GigabitEthernet0/0/0/4.101
C    10.255.1.0/30 is directly connected, 00:14:12, GigabitEthernet0/0/0/4.101
L    10.255.1.1/32 is directly connected, 00:14:12, GigabitEthernet0/0/0/4.101
B    10.255.1.4/30 [200/0] via 10.0.0.4 (nexthop in vrf default), 00:12:48
B    10.255.1.8/30 [200/0] via 10.0.0.5 (nexthop in vrf default), 00:12:48
B    192.168.2.0/24 [200/2] via 10.0.0.4 (nexthop in vrf default), 00:12:48
B    192.168.3.0/24 [200/2] via 10.0.0.5 (nexthop in vrf default), 00:12:48
```

Figura 4.35 – Tabla de rutas en la vrf del cliente.

Configuración Router PE_2

- **Servicio VPN:**

```
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
router bgp 64512
 vrf CORP_1
  rd 64512:1
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
```

```
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.5
  domain-tag 64512
  passive enable
  default-information originate
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4
    network point-to-point
    passive disable
   !
  !
 !
!

interface GigabitEthernet0/0/0/4
 description CPE_MSY Gi0/0
 vrf CORP_1
 ipv4 address 10.255.1.5 255.255.255.252
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_2#sh ospf vrf CORP_1 neighbor
Wed Apr  5 17:54:53.058 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 101, VRF CORP_1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.6      1     FULL/  -        00:00:32    10.255.1.6      GigabitEthernet0/0/0/4
    Neighbor is up for 00:22:51

Total neighbor count: 1
```

Figura 4.36 – Adyacencia OSPF contra el router CPE de la oficina Masaya.

```
RP/0/0/CPU0:PE_2#sh route vrf CORP_1
Wed Apr  5 17:56:16.212 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route
       M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is 10.0.0.3 to network 0.0.0.0

B*   0.0.0.0/0 [200/1] via 10.0.0.3 (nexthop in vrf default), 00:22:51
B    10.255.1.0/30 [200/0] via 10.0.0.3 (nexthop in vrf default), 00:22:51
C    10.255.1.4/30 is directly connected, 00:24:20, GigabitEthernet0/0/0/4
L    10.255.1.5/32 is directly connected, 00:24:20, GigabitEthernet0/0/0/4
B    10.255.1.8/30 [200/0] via 10.0.0.5 (nexthop in vrf default), 00:22:53
O    192.168.2.0/24 [110/2] via 10.255.1.6, 00:24:14, GigabitEthernet0/0/0/4
B    192.168.3.0/24 [200/2] via 10.0.0.5 (nexthop in vrf default), 00:22:53
```

Figura 4.37 – Tabla de rutas en la vrf del cliente.

Configuración Router PE_3

- **Servicio VPN:**

```
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
router bgp 64512
 vrf CORP_1
  rd 64512:1
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
```

```
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.9
  domain-tag 64512
  passive enable
  default-information originate
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4
    network point-to-point
    passive disable
   !
  !
 !
!

interface GigabitEthernet0/0/0/4
 description CPE_LEO Gi0/0
 vrf CORP_1
 ipv4 address 10.255.1.9 255.255.255.252
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_3#show ospf vrf CORP_1 neighbor
Wed Apr  5 18:00:29.845 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 101, VRF CORP_1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.10     1     FULL/  -        00:00:34    10.255.1.10     GigabitEthernet0/0/0/4
    Neighbor is up for 00:28:24

Total neighbor count: 1
```

Figura 4.38 – Adyacencia OSPF contra el router CPE de la oficina León.

```
RP/0/0/CPU0:PE_3#show route vrf CORP_1
Wed Apr  5 18:01:29.691 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR, l - LISP
       A - access/subscriber, a - Application route
       M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is 10.0.0.3 to network 0.0.0.0

B*   0.0.0.0/0 [200/1] via 10.0.0.3 (nexthop in vrf default), 00:28:05
B    10.255.1.0/30 [200/0] via 10.0.0.3 (nexthop in vrf default), 00:28:05
B    10.255.1.4/30 [200/0] via 10.0.0.4 (nexthop in vrf default), 00:28:07
C    10.255.1.8/30 is directly connected, 00:29:32, GigabitEthernet0/0/0/4
L    10.255.1.9/32 is directly connected, 00:29:32, GigabitEthernet0/0/0/4
B    192.168.2.0/24 [200/2] via 10.0.0.4 (nexthop in vrf default), 00:28:07
O    192.168.3.0/24 [110/2] via 10.255.1.10, 00:29:23, GigabitEthernet0/0/0/4
```

Figura 4.39 – Tabla de rutas en la vrf del cliente en PE_3.

Validaciones Route Reflector

```
RP/0/0/CPU0:RR#sh bgp vpnv4 unicast rd 64512:1
Wed Apr  5 20:46:00.255 UTC
BGP router identifier 10.0.0.100, local AS number 64512
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 7
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64512:1
*>i0.0.0.0/0          10.0.0.3                 1    100      0 ?
*>i10.255.1.0/30      10.0.0.3                 0    100      0 ?
*>i10.255.1.4/30      10.0.0.4                 0    100      0 ?
*>i10.255.1.8/30      10.0.0.5                 0    100      0 ?
*>i192.168.2.0/24     10.0.0.4                 2    100      0 ?
*>i192.168.3.0/24     10.0.0.5                 2    100      0 ?

Processed 6 prefixes, 6 paths
```

Figura 4.40 – Rutas aprendidas en BGP para la vpn del cliente RD 64512:1.

Validaciones Router CPE_HQ

Adyacencia OSPF establecida con el router PE_1 del ISP.

```
CPE_HQ#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.1        0   FULL/  -        00:00:38    10.255.1.1      GigabitEthernet0/0.101
```

Figura 4.41 – Adyacencia OSPF en router CPE oficina central.

La tabla de la figura 4.42 muestra las redes LAN de las oficinas remotas 192.168.2.0/24 y 192.168.3.0/24 aprendidas por OSPF y una ruta por defecto configurada de forma estática para el acceso a Internet.

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

Gateway of last resort is 165.98.255.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 165.98.255.1, GigabitEthernet0/0.100
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.255.1.0/30 is directly connected, GigabitEthernet0/0.101
L        10.255.1.2/32 is directly connected, GigabitEthernet0/0.101
O IA     10.255.1.4/30
           [110/2] via 10.255.1.1, 02:42:19, GigabitEthernet0/0.101
O IA     10.255.1.8/30
           [110/2] via 10.255.1.1, 02:42:19, GigabitEthernet0/0.101
      165.98.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        165.98.255.0/30 is directly connected, GigabitEthernet0/0.100
L        165.98.255.2/32 is directly connected, GigabitEthernet0/0.100
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback100
L        192.168.1.1/32 is directly connected, Loopback100
O IA  192.168.2.0/24 [110/3] via 10.255.1.1, 02:42:19, GigabitEthernet0/0.101
O IA  192.168.3.0/24 [110/3] via 10.255.1.1, 02:42:19, GigabitEthernet0/0.101
```

Figura 4.42 – Tabla de ruta en router CPE oficina central.

```
CPE_HQ#ping 192.168.2.1 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/18/53 ms
CPE_HQ#ping 192.168.3.1 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/17/47 ms
```

Figura 4.43 – Prueba de conexión a las oficinas remotas.

Validaciones Router CPE_MSY

Adyacencia OSPF establecida con el router PE_2 del ISP.

```
CPE_MSY#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.5        0   FULL/  -        00:00:37    10.255.1.5      GigabitEthernet0/0
```

Figura 4.44 – Adyacencia OSPF en router CPE Masaya.

La tabla en la figura 4.45 muestra la ruta por defecto anunciada por el router CPE de la oficina central para el acceso al Data Center e Internet, además de la red LAN de la oficina en León.

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

Gateway of last resort is 10.255.1.5 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.255.1.5, 02:50:21, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA     10.255.1.0/30 [110/2] via 10.255.1.5, 02:50:21, GigabitEthernet0/0
C        10.255.1.4/30 is directly connected, GigabitEthernet0/0
L        10.255.1.6/32 is directly connected, GigabitEthernet0/0
O IA     10.255.1.8/30 [110/2] via 10.255.1.5, 02:50:23, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback100
L        192.168.2.1/32 is directly connected, Loopback100
O IA  192.168.3.0/24 [110/3] via 10.255.1.5, 02:50:23, GigabitEthernet0/0
```

Figura 4.45 – Tabla de ruta en router CPE Masaya.

Se prueba conexión a la red de Data Center en la oficina central y a la red LAN de la oficina en León, así mismo se prueba el acceso a internet (8.8.8.8).

```
CPE_MSY#ping 192.168.1.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/11 ms
CPE_MSY#ping 192.168.3.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/10 ms
CPE_MSY#ping 8.8.8.8 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 13/16/26 ms
```

Figura 4.46 – Prueba de conexión desde la oficina en Masaya.

Validaciones Router CPE_LEO

Adyacencia OSPF establecida con el router PE_3 del ISP.

```
CPE_LEO#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.255.1.9        0   FULL/  -        00:00:38    10.255.1.9      GigabitEthernet0/0
```

Figura 4.47 – Adyacencia OSPF en router CPE León.

La tabla en la figura 4.48 muestra la ruta por defecto anunciada por el router CPE de la oficina central para el acceso al Data Center e Internet, además de la red LAN de la oficina en Masaya.

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

Gateway of last resort is 10.255.1.9 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.255.1.9, 03:07:44, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA     10.255.1.0/30 [110/2] via 10.255.1.9, 03:07:44, GigabitEthernet0/0
O IA     10.255.1.4/30 [110/2] via 10.255.1.9, 03:07:46, GigabitEthernet0/0
C        10.255.1.8/30 is directly connected, GigabitEthernet0/0
L        10.255.1.10/32 is directly connected, GigabitEthernet0/0
O IA  192.168.2.0/24 [110/3] via 10.255.1.9, 03:07:46, GigabitEthernet0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback100
L        192.168.3.1/32 is directly connected, Loopback100
```

Figura 4.48 – Tabla de ruta en router CPE León.

Se prueba conexión a la red de Data Center en la oficina central y a la red LAN de la oficina en Masaya, así mismo se prueba el acceso a internet (8.8.8.8).

```
CPE_LEO#ping 192.168.1.1 source 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
CPE_LEO#ping 192.168.2.1 source 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/10 ms
CPE_LEO#ping 8.8.8.8 source 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms
```

Figura 4.49 – Prueba de conexión desde la oficina en León.

4.7.2 - Caso de Estudio #2: Transmisión de Video.

El ISP provee servicio de televisión digital a sus clientes. Para esto debe transmitir los paquetes de video originados por una fuente multicast ubicada en el Head-End hacia los receptores multicast ubicados en los Video Hubs remotos.

En la red del proveedor se tiene configurado PIM Sparse Mode (PIM-SM) y utiliza como RP el router CORE_1 (10.0.0.1).

Para el servicio MVPN se configura la VRF llamada VIDEO y se asigna el grupo MDT 239.1.2.3. La fuente multicast del servicio VPN transmite para el grupo 239.1.1.1.

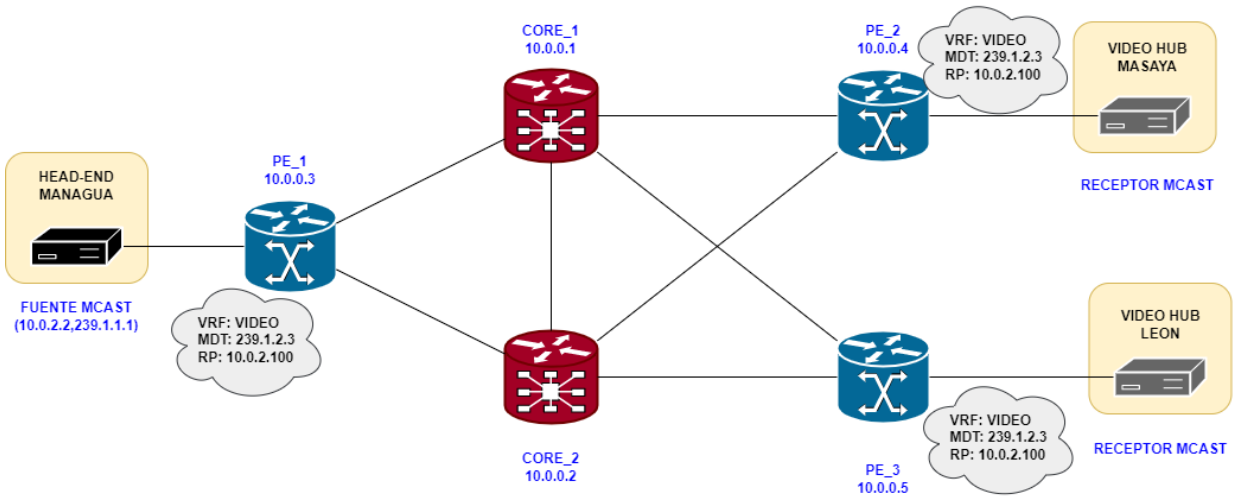


Figura 4.50 – Red de Servicio MPLS – Transmisión de Video.

Tabla 4.7 – Recursos asignados al servicio multicast.

SERVICIO	GRUPO MULTICAST	VRF	GRUPO MDT	RP
Canal XYZ	239.1.1.1	VIDEO 64512:2	239.1.2.3	10.0.2.100

Tabla 4.8 – Direccionamiento (IP Planning) servicio de video Canal XYZ.

EQUIPO MULTICAST	EQUIPO DE ACCESO	INTERFAZ	DIRECCION IP
Fuente Multicast (Managua)	PE_1	Gi0/0/0/3	10.0.2.2/30
Receptor Multicast (Masaya)	PE_2	Gi0/0/0/3	10.0.2.6/30
Receptor Multicast (León)	PE_3	Gi0/0/0/3	10.0.2.10/30

Configuración Router CORE_1

- **Servicio Multicast Global:**

```
multicast-routing
 address-family ipv4
  ! SE HABILITA PIM EN LAS INTERFACES HACIA EQUIPOS DE LA RED:
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/2
   enable
  !
  interface GigabitEthernet0/0/0/3
   enable
  !
  interface GigabitEthernet0/0/0/4
   enable
  !
 !
!

router pim
 address-family ipv4
  rp-address 10.0.0.1 ! SE DEFINE EL ROUTER RP UTILIZADO EN LA RED DEL ISP.
 !
!
```

- **Validaciones:**

La salida en la figura 4.51 muestra los siguientes datos: la columna PIM indica las interfaces habilitadas con PIM (on/off), la cantidad de vecinos en cada segmento (Nbr Count), intervalo de tiempo en el que se envían los paquetes Hello de PIM (30 segundos valor por defecto), Prioridad PIM configurada en cada interfaz (DR Prior =1), el router DR elegido en cada segmento.

En cada segmento se elige un Designated Router (DR), el router con la prioridad más alta configurada en la interfaz es elegido del DR, en caso de tener la misma prioridad, se elige el router con la dirección IP mayor.

```
RP/0/0/CPU0:CORE_1#sh pim interface
Mon Apr 17 04:59:35.305 UTC

PIM interfaces in VRF default
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.1              Loopback0                on   1     30     1     this system
10.0.1.1              GigabitEthernet0/0/0/0   on   2     30     1     10.0.1.2
10.0.1.5              GigabitEthernet0/0/0/1   off  0     30     1     not elected
10.0.1.9              GigabitEthernet0/0/0/2   on   2     30     1     10.0.1.10
10.0.1.17             GigabitEthernet0/0/0/3   on   2     30     1     10.0.1.18
10.0.1.21             GigabitEthernet0/0/0/4   on   2     30     1     10.0.1.22
```

Figura 4.51 – Interfaces configuradas con PIM en el router CORE_1.

En la figura 4.52, la salida del comando muestra el tiempo establecido de cada vecindad PIM (columna “Uptime”) y el contador descendente de tiempo en el que se espera un paquete Hello del vecino PIM (columna “Expires”).

El contador de tiempo es de 105 segundos (3.5 veces el intervalo de tiempo Hello), si este contador llega a cero el vecino PIM se da de baja.

```
RP/0/0/CPU0:CORE_1#sh pim neighbor
Mon Apr 17 05:02:58.011 UTC

PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface              Uptime    Expires  DR pri   Flags

10.0.1.1*                   GigabitEthernet0/0/0/0 00:52:05  00:01:34 1      B E
10.0.1.2                    GigabitEthernet0/0/0/0 00:51:28  00:01:32 1 (DR) B
10.0.1.9*                   GigabitEthernet0/0/0/2 00:52:05  00:01:42 1      B E
10.0.1.10                   GigabitEthernet0/0/0/2 00:51:15  00:01:29 1 (DR) B
10.0.1.17*                  GigabitEthernet0/0/0/3 00:52:05  00:01:30 1      B E
10.0.1.18                   GigabitEthernet0/0/0/3 00:51:09  00:01:33 1 (DR) B
10.0.1.21*                  GigabitEthernet0/0/0/4 00:52:05  00:01:15 1      B E
10.0.1.22                   GigabitEthernet0/0/0/4 00:51:14  00:01:23 1 (DR) B
10.0.0.1*                   Loopback0              00:52:07  00:01:39 1 (DR) B E
```

Figura 4.52 – Vecinos PIM del router CORE_1.

El router RP 10.0.0.1 (CORE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:CORE_1#sh pim rp mapping
Mon Apr 17 05:30:37.567 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.0.1 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 01:19:48, expires: never
```

Figura 4.53 – Router RP (Rendezvous Point) configurado en la red.

La dirección multicast 239.1.2.3 es el grupo MDT asignado al servicio multicast VPN. Esta dirección se utiliza para encapsular el tráfico multicast del dominio VPN para su transmisión entre los router PE.

```
RP/0/0/CPU0:CORE_1#sh mrib route 239.1.2.3
Mon Apr 17 05:45:50.745 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.2.3) RPF nbr: 10.0.0.1 Flags: C RPF
  Up: 01:34:07
  Incoming Interface List
    Decapstunnel0 Flags: A, Up: 01:34:07
  Outgoing Interface List
    GigabitEthernet0/0/0/2 Flags: F NS, Up: 01:34:07
    GigabitEthernet0/0/0/3 Flags: F NS, Up: 01:33:58
    GigabitEthernet0/0/0/4 Flags: F NS, Up: 01:34:00

(10.0.0.3,239.1.2.3) RPF nbr: 10.0.0.1 Flags: L RPF
  Up: 01:34:07
  Incoming Interface List
    Decapstunnel0 Flags: A, Up: 01:31:49

(10.0.0.4,239.1.2.3) RPF nbr: 10.0.0.1 Flags: L RPF
  Up: 01:34:01
  Incoming Interface List
    Decapstunnel0 Flags: A, Up: 01:31:49
```

Figura 4.54 – Tabla global multicast.

```
(10.0.0.5,239.1.2.3) RPF nbr: 10.0.0.1 Flags: L RPF
  Up: 01:34:00
  Incoming Interface List
    Decapstunnel0 Flags: A, Up: 01:31:49
```

Figura 4.55 – Tabla multicast para el grupo MDT 239.1.2.3 asignado al cliente VPN (continuación).

Configuración Router S_MCast (Fuente Multicast)

```
interface GigabitEthernet0/0 ! INTERFAZ CONECTADA AL PE_1 DEL ISP.
 ip address 10.0.2.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.1
```

- **Validaciones:**

En la figura 4.56, se generan 10 paquetes con origen 10.0.0.2 y destino 239.1.1.1 que es el grupo multicast al que están asociados los receptores multicast remotos de la VPN, por eso la respuesta exitosa del comando PING.

```
S_MCast#ping 239.1.1.1 source 10.0.2.2 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 239.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.2.2

Reply to request 0 from 10.0.2.6, 13 ms
Reply to request 0 from 10.0.2.10, 14 ms
Reply to request 1 from 10.0.2.6, 7 ms
Reply to request 1 from 10.0.2.10, 8 ms
Reply to request 2 from 10.0.2.6, 9 ms
Reply to request 2 from 10.0.2.10, 10 ms
Reply to request 3 from 10.0.2.10, 8 ms
Reply to request 3 from 10.0.2.6, 8 ms
Reply to request 4 from 10.0.2.6, 7 ms
Reply to request 4 from 10.0.2.10, 8 ms
Reply to request 5 from 10.0.2.10, 17 ms
Reply to request 5 from 10.0.2.6, 17 ms
Reply to request 6 from 10.0.2.6, 8 ms
Reply to request 6 from 10.0.2.10, 10 ms
Reply to request 7 from 10.0.2.10, 8 ms
Reply to request 7 from 10.0.2.6, 8 ms
Reply to request 8 from 10.0.2.6, 9 ms
Reply to request 8 from 10.0.2.10, 9 ms
Reply to request 9 from 10.0.2.10, 7 ms
Reply to request 9 from 10.0.2.6, 8 ms
```

Figura 4.56 – Generación de tráfico multicast.

Configuración router R_MCast_MSY (Receptor Multicast #1)

```
interface GigabitEthernet0/0 ! INTERFAZ CONECTADA AL PE_2 DEL ISP.
 ip address 10.0.2.6 255.255.255.252
 ip igmp join-group 239.1.1.1 ! SE ASOCIA LA INTERFAZ AL GRUPO MULTICAST DEL SERVICIO.
 duplex auto
 speed auto
 media-type rj45

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.5
```

El comando "*ip igmp join-group*" provoca que el router envie al PE_2 un paquete (mensaje) llamado "IGMP Join" (Membership Report) solicitando unirse al grupo multicast 239.1.1.1 y recibir contenido de este grupo.

Configuración router R_MCast_LEO (Receptor Multicast #2)

```
interface GigabitEthernet0/0 ! INTERFAZ CONECTADA AL PE_3 DEL ISP.
 ip address 10.0.2.10 255.255.255.252
 ip igmp join-group 239.1.1.1 ! SE ASOCIA LA INTERFAZ AL GRUPO MULTICAST DEL SERVICIO.
 duplex auto
 speed auto
 media-type rj45

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.9
```

El comando "*ip igmp join-group*" provoca que el router envie al PE_3 un paquete (mensaje) llamado "IGMP Join" (Membership Report) solicitando unirse al grupo multicast 239.1.1.1 y recibir contenido de este grupo.

Configuración Router PE_1

- **Servicio Multicast Global/VPN:**

```
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
router bgp 64512
 vrf VIDEO
  rd 64512:2
  address-family ipv4 unicast
   redistribute connected
  !
 !
!
interface Loopback100 ! INTERFAZ PARA SERVICIO RP.
 vrf VIDEO
 ipv4 address 10.0.2.100 255.255.255.255
!
interface GigabitEthernet0/0/0/3 ! INTERFAZ CONECTADA A LA FUENTE MULTICAST.
 description FUENTE MULTICAST - CANAL XYZ
 vrf VIDEO
 ipv4 address 10.0.2.1 255.255.255.252
!
multicast-routing
 address-family ipv4
  ! SE HABILITA PIM EN LAS INTERFACES HACIA EQUIPOS DE LA RED ISP:
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
   enable
  !
  mdt source Loopback0
 !
 ! SE DEFINE LA CONFIGURACION PARA LA VPN DE VIDEO:
 vrf VIDEO
  address-family ipv4
   interface Loopback100
    enable
   !
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3 ! GRUPO MDT ASIGNADO A LA VPN DE VIDEO.
  !
 !
!
```

```
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
 vrf VIDEO
  address-family ipv4
   rp-address 10.0.2.100 ! DEFINE EL ROUTER RP UTILIZADO EN LA VPN DE VIDEO.
  !
 !
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_1#show pim interface
Wed Apr 19 05:30:27.343 UTC

PIM interfaces in VRF default
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.3              Loopback0                on   1     30     1     this system
10.0.1.10             GigabitEthernet0/0/0/0   on   2     30     1     this system
10.0.1.14             GigabitEthernet0/0/0/1   on   2     30     1     this system
165.98.255.1          GigabitEthernet0/0/0/4.100 off  0     30     1     not elected
```

Figura 4.57 – Interfaces globales configuradas con PIM en el router PE_1.

```
RP/0/0/CPU0:PE_1#show pim vrf VIDEO interface
Wed Apr 19 05:32:36.514 UTC

PIM interfaces in VRF VIDEO
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.3              mdtVIDEO                 on   3     30     1     10.0.0.5
10.0.2.100            Loopback100              on   1     30     1     this system
10.0.2.1              GigabitEthernet0/0/0/3   on   1     30     1     this system
```

Figura 4.58 – Interfaces VPN configuradas con PIM en el router PE_1.

```
RP/0/0/CPU0:PE_1#show pim neighbor
Wed Apr 19 05:34:45.295 UTC

PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface             Uptime    Expires  DR pri   Flags

10.0.1.9                    GigabitEthernet0/0/0/0 02:39:17  00:01:24 1       B
10.0.1.10*                  GigabitEthernet0/0/0/0 02:39:22  00:01:16 1 (DR) B
10.0.1.13                   GigabitEthernet0/0/0/1 02:39:14  00:01:21 1       B
10.0.1.14*                  GigabitEthernet0/0/0/1 02:39:22  00:01:19 1 (DR) B E
10.0.0.3*                   Loopback0              02:39:25  00:01:32 1 (DR) B E
```

Figura 4.59 – Vecinos PIM globales del router PE_1.

Se establece vecindad con los router PE_2 (10.0.0.4) y PE_3 (10.0.0.5) a través de la interfaz túnel GRE (mdtVIDEO) la cual se utiliza para enviar tráfico multicast de la VRF VIDEO encapsulado en el grupo MDT de la VPN.

```
RP/0/0/CPU0:PE_1#sh pim vrf VIDEO neighbor
Wed Apr 19 05:36:44.627 UTC

PIM neighbors in VRF VIDEO
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface             Uptime    Expires  DR pri   Flags

10.0.2.1*                   GigabitEthernet0/0/0/3 02:41:21  00:01:35 1 (DR) B E
10.0.0.3*                   mdtVIDEO               02:41:24  00:01:23 1
10.0.0.4                    mdtVIDEO               02:41:11  00:01:20 1
10.0.0.5                    mdtVIDEO               02:41:09  00:01:18 1 (DR)
10.0.2.100*                 Loopback100            02:41:24  00:01:22 1 (DR) B E
```

Figura 4.60 – Vecinos PIM VPN del router PE_1.

El router RP 10.0.0.1 (CORE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_1#sh pim rp mapping
Wed Apr 19 05:45:35.031 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.0.1 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 02:50:15, expires: never
```

Figura 4.61 – Router RP (Rendezvous Point) configurado en la red ISP.

El router RP 10.0.2.100 (PE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_1#sh pim vrf VIDEO rp
rpf  rp  rpf-redirect
RP/0/0/CPU0:PE_1#sh pim vrf VIDEO rp mapping
Wed Apr 19 05:46:21.907 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.2.100 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 02:51:02, expires: never
```

Figura 4.62 – Router RP (Rendezvous Point) utilizado en el servicio MVPN.

La dirección multicast 239.1.2.3 es el grupo MDT asignado al servicio multicast VPN. Esta dirección se utiliza para encapsular el tráfico multicast del dominio VPN para su transmisión entre los router PE.

En la salida de la figura 4.63 se muestra el registro (*,G) del árbol “Shared Tree” indicando la interfaz Gi0/0/0/0 hacia el RP.

```
RP/0/0/CPU0:PE_1#sh mrib route 239.1.2.3
Wed Apr 19 05:48:36.548 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.2.3) RPF nbr: 10.0.1.9 Flags: C RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 02:53:16
  Incoming Interface List
    GigabitEthernet0/0/0/0 Flags: A NS, Up: 02:53:09
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 02:53:14
```

Figura 4.63 – Tabla global multicast.

La figura 4.64 muestra los registros (S,G) del árbol “Source Tree (SPT)” indicando los PE registrados como fuente para el grupo MDT 239.1.2.3. Las interfaces mostradas en el apartado “Incoming Interface List (IIL)” son las interfaces hacia el PE fuente del grupo MDT, es decir, la interfaz por donde se recibiría tráfico multicast. Las interfaces mostradas en el apartado “Outgoing Interface List (OIL)” son las interfaces hacia el PE receptor del grupo MDT.

```
(10.0.0.3,239.1.2.3) RPF nbr: 10.0.0.3 Flags: RPF ME MH
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 02:53:16
  Incoming Interface List
    Loopback0 Flags: F A, Up: 02:53:14
  Outgoing Interface List
    Loopback0 Flags: F A, Up: 02:53:14
    GigabitEthernet0/0/0/1 Flags: F NS, Up: 02:50:47

(10.0.0.4,239.1.2.3) RPF nbr: 10.0.1.13 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 02:53:03
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A NS, Up: 02:50:47
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 02:53:03

(10.0.0.5,239.1.2.3) RPF nbr: 10.0.1.13 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 02:53:01
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A, Up: 02:50:47
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 02:53:01
```

Figura 4.64 – Tabla global multicast (continuación).

En la salida de la figura 4.65 se muestra el registro (S,G):(10.0.2.2,239.1.1.1) indicando en el apartado IIL la interfaz Gi0/0/0/3 conectada a la fuente multicast del servicio VPN y en el apartado OIL la interfaz túnel mdtVIDEO hacia los PE con receptores multicast en la VPN.

```
RP/0/0/CPU0:PE_1#sh mrib vrf VIDEO route 239.1.1.1
Wed Apr 19 06:06:23.805 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.1.1) RPF nbr: 10.0.2.100 Flags: C RPF
  Up: 01:22:20
  Incoming Interface List
    Decapstunnel0 Flags: A, Up: 01:22:20
  Outgoing Interface List
    mdtVIDEO Flags: F NS MI, Up: 01:22:20

(10.0.2.2,239.1.1.1) RPF nbr: 10.0.2.2 Flags: L RPF
  Up: 00:00:16
  Incoming Interface List
    GigabitEthernet0/0/0/3 Flags: A, Up: 00:00:16
  Outgoing Interface List
    mdtVIDEO Flags: F NS MI, Up: 00:00:16
```

Figura 4.65 – Tabla VPN multicast.

Configuración Router PE_2

- **Servicio Multicast Global/VPN:**

```
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
router bgp 64512
 vrf VIDEO
  rd 64512:2
  address-family ipv4 unicast
   redistribute connected
  !
 !
!
interface GigabitEthernet0/0/0/3 ! INTERFAZ CONECTADA AL RECEPTOR MULTICAST.
 description RECEPTOR MULTICAST
 vrf VIDEO
 ipv4 address 10.0.2.5 255.255.255.252
!
multicast-routing
 address-family ipv4
  ! SE HABILITA PIM EN LAS INTERFACES HACIA EQUIPOS DE LA RED ISP:
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
   enable
  !
  mdt source Loopback0
 !
 ! SE DEFINE LA CONFIGURACION PARA LA VPN DE VIDEO:
 vrf VIDEO
  address-family ipv4
   interface Loopback100
    enable
   !
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3 ! GRUPO MDT ASIGNADO A LA VPN DE VIDEO.
  !
 !
!
```

```
router pim
 address-family ipv4
  rp-address 10.0.0.1 ! DEFINE EL ROUTER RP UTILIZADO EN LA RED ISP.
 !
 vrf VIDEO
  address-family ipv4
   rp-address 10.0.2.100 ! DEFINE EL ROUTER RP UTILIZADO EN LA VPN DE VIDEO.
  !
 !
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_2#sh pim interface
Wed Apr 19 06:57:44.764 UTC

PIM interfaces in VRF default
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.4              Loopback0                on   1     30     1     this system
10.0.1.18             GigabitEthernet0/0/0/0   on   2     30     1     this system
10.0.1.30             GigabitEthernet0/0/0/1   on   2     30     1     this system
```

Figura 4.66 – Interfaces globales configuradas con PIM en el router PE_2.

```
RP/0/0/CPU0:PE_2#sh pim vrf VIDEO interface
Wed Apr 19 06:58:23.501 UTC

PIM interfaces in VRF VIDEO
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.4              mdtVIDEO                 on   3     30     1     10.0.0.5
10.0.2.5              GigabitEthernet0/0/0/3   on   1     30     1     this system
```

Figura 4.67 – Interfaces VPN configuradas con PIM en el router PE_2.

```
RP/0/0/CPU0:PE_2#sh pim neighbor
Wed Apr 19 06:59:00.808 UTC

PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface             Uptime    Expires  DR pri   Flags

10.0.1.17                   GigabitEthernet0/0/0/0 04:03:28  00:01:20 1       B
10.0.1.18*                  GigabitEthernet0/0/0/0 04:03:36  00:01:18 1 (DR) B E
10.0.1.29                   GigabitEthernet0/0/0/1 04:03:32  00:01:32 1       B
10.0.1.30*                  GigabitEthernet0/0/0/1 04:03:36  00:01:28 1 (DR) B
10.0.0.4*                   Loopback0             04:03:37  00:01:33 1 (DR) B E
```

Figura 4.68 – Vecinos PIM globales del router PE_2.

Se establece vecindad con los router PE_1 (10.0.0.3) y PE_3 (10.0.0.5) a través de la interfaz túnel GRE (mdtVIDEO) la cual se utiliza para enviar tráfico multicast de la VRF VIDEO encapsulado en el grupo MDT de la VPN.

```
RP/0/0/CPU0:PE_2#sh pim vrf VIDEO neighbor
Wed Apr 19 06:59:51.845 UTC

PIM neighbors in VRF VIDEO
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface             Uptime    Expires  DR pri   Flags

10.0.2.5*                   GigabitEthernet0/0/0/3 04:04:27  00:01:33 1 (DR) B E
10.0.0.3                    mdtVIDEO              04:04:19  00:01:31 1
10.0.0.4*                   mdtVIDEO              04:04:28  00:01:27 1
10.0.0.5                    mdtVIDEO              04:04:18  00:01:26 1 (DR)
```

Figura 4.69 – Vecinos PIM VPN del router PE_2.

El router RP 10.0.0.1 (CORE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_2#sh pim rp mapping
Wed Apr 19 07:00:50.971 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.0.1 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 04:05:28, expires: never
```

Figura 4.70 – Router RP (Rendezvous Point) configurado en la red ISP.

El router RP 10.0.2.100 (PE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_2#sh pim vrf VIDEO rp mapping
Wed Apr 19 07:01:28.238 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.2.100 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 04:06:05, expires: never
```

Figura 4.71 – Router RP (Rendezvous Point) utilizado en el servicio MVPN.

La dirección multicast 239.1.2.3 es el grupo MDT asignado al servicio multicast VPN. Esta dirección se utiliza para encapsular el tráfico multicast del dominio VPN para su transmisión entre los router PE.

En la salida se muestra el registro (*,G) del árbol “Shared Tree” indicando la interfaz Gi0/0/0/0 hacia el RP.

```
RP/0/0/CPU0:PE_2#sh mrib route 239.1.2.3
Wed Apr 19 07:02:20.555 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.2.3) RPF nbr: 10.0.1.17 Flags: C RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:06:57
  Incoming Interface List
    GigabitEthernet0/0/0/0 Flags: A NS, Up: 04:06:45
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:06:55
```

Figura 4.72 – Tabla global multicast.

En la salida de la figura 4.73 se muestran los registros (S,G) del árbol “Source Tree (SPT)” indicando los PE registrados como fuente para el grupo MDT 239.1.2.3. Las interfaces mostradas en el apartado “Incoming Interface List (IIL)” son las interfaces hacia el PE fuente del grupo MDT, es decir, la interfaz por donde se recibiría tráfico multicast. Las interfaces mostradas en el apartado “Outgoing Interface List (OIL)” son las interfaces hacia el PE receptor del grupo MDT.

```
(10.0.0.3,239.1.2.3) RPF nbr: 10.0.1.29 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:06:48
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A, Up: 04:04:33
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:06:48

(10.0.0.4,239.1.2.3) RPF nbr: 10.0.0.4 Flags: RPF ME MH
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:06:57
  Incoming Interface List
    Loopback0 Flags: F A, Up: 04:06:55
  Outgoing Interface List
    Loopback0 Flags: F A, Up: 04:06:55
    GigabitEthernet0/0/0/1 Flags: F NS, Up: 04:04:33

(10.0.0.5,239.1.2.3) RPF nbr: 10.0.1.29 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:06:47
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A, Up: 04:04:33
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:06:47
```

Figura 4.73 – Tabla global multicast (continuación).

En la salida de la figura 4.74 se muestra el registro (S,G):(10.0.2.2,239.1.1.1) indicando en el apartado IIL la interfaz Gi0/0/0/3 conectada a la fuente multicast del servicio VPN y en el apartado OIL la interfaz túnel mdtVIDEO hacia los PE con receptores multicast en la VPN.

```
RP/0/0/CPU0:PE_2#sh mrib vrf VIDEO route 239.1.1.1
Wed Apr 19 07:03:59.138 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.1.1) RPF nbr: 10.0.0.3 Flags: C RPF
  Up: 04:08:30
  Incoming Interface List
    mdtVIDEO Flags: A NS MI, Up: 02:18:38
  Outgoing Interface List
    GigabitEthernet0/0/0/3 Flags: F NS LI, Up: 04:08:30

(10.0.2.2,239.1.1.1) RPF nbr: 10.0.0.3 Flags: RPF
  Up: 00:23:30
  Incoming Interface List
    mdtVIDEO Flags: A MI, Up: 00:23:30
  Outgoing Interface List
    GigabitEthernet0/0/0/3 Flags: F NS, Up: 00:23:30
```

Figura 4.74 – Tabla VPN multicast.

En la salida se muestra el receptor 10.0.2.6 en la interfaz Gi0/0/0/3 conectado al grupo 239.1.1.1.

```
RP/0/0/CPU0:PE_2#sh igmp vrf VIDEO groups 239.1.1.1
Wed Apr 19 07:05:26.642 UTC
IGMP Connected Group Membership
Group Address   Interface                 Uptime    Expires   Last Reporter
239.1.1.1       GigabitEthernet0/0/0/3    04:09:58  00:01:29  10.0.2.6
```

Figura 4.75 – Receptores Multicast del grupo 239.1.1.1.

Configuración Router PE_3

- **Servicio Multicast Global/VPN:**

```
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
router bgp 64512
 vrf VIDEO
  rd 64512:2
  address-family ipv4 unicast
   redistribute connected
  !
 !
!
interface GigabitEthernet0/0/0/3 ! INTERFAZ CONECTADA AL RECEPTOR MULTICAST.
 description RECEPTOR MULTICAST
 vrf VIDEO
 ipv4 address 10.0.2.9 255.255.255.252
!
multicast-routing
 address-family ipv4
  ! SE HABILITA PIM EN LAS INTERFACES HACIA EQUIPOS DE LA RED ISP:
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
   enable
  !
  mdt source Loopback0
 !
```

```
 ! SE DEFINE LA CONFIGURACION PARA LA VPN DE VIDEO:
 vrf VIDEO
  address-family ipv4
   interface Loopback100
    enable
   !
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3 ! GRUPO MDT ASIGNADO A LA VPN DE VIDEO.
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1 ! DEFINE EL ROUTER RP UTILIZADO EN LA RED ISP.
 !
 vrf VIDEO
  address-family ipv4
   rp-address 10.0.2.100 ! DEFINE EL ROUTER RP UTILIZADO EN LA VPN DE VIDEO.
  !
 !
!
```

- **Validaciones:**

```
RP/0/0/CPU0:PE_3#sh pim interface
Wed Apr 19 07:16:57.125 UTC

PIM interfaces in VRF default
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.5              Loopback0                on   1     30     1     this system
10.0.1.22             GigabitEthernet0/0/0/0   on   2     30     1     this system
10.0.1.26             GigabitEthernet0/0/0/1   on   2     30     1     this system
```

Figura 4.76 – Interfaces globales configuradas con PIM en el router PE_3.

```
RP/0/0/CPU0:PE_3#sh pim vrf VIDEO interface
Wed Apr 19 07:17:33.592 UTC

PIM interfaces in VRF VIDEO
Address               Interface                PIM  Nbr   Hello  DR    DR
                                                    Count Intvl  Prior

10.0.0.5              mdtVIDEO                 on   3     30     1     this system
10.0.2.9              GigabitEthernet0/0/0/3   on   1     30     1     this system
```

Figura 4.77 – Interfaces VPN configuradas con PIM en el router PE_3.

```
RP/0/0/CPU0:PE_3#sh pim neighbor
Wed Apr 19 07:18:05.140 UTC

PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface              Uptime    Expires  DR pri   Flags

10.0.1.21                   GigabitEthernet0/0/0/0 04:22:48  00:01:14 1       B
10.0.1.22*                  GigabitEthernet0/0/0/0 04:22:53  00:01:42 1 (DR) B
10.0.1.25                   GigabitEthernet0/0/0/1 04:22:43  00:01:27 1       B
10.0.1.26*                  GigabitEthernet0/0/0/1 04:22:53  00:01:33 1 (DR) B E
10.0.0.5*                   Loopback0              04:22:54  00:01:42 1 (DR) B E
```

Figura 4.78 – Vecinos PIM globales del router PE_3.

Se establece vecindad con los router PE_1 (10.0.0.3) y PE_3 (10.0.0.4) a través de la interfaz túnel GRE (mdtVIDEO) la cual se utiliza para enviar tráfico multicast de la VRF VIDEO encapsulado en el grupo MDT de la VPN.

```
RP/0/0/CPU0:PE_3#sh pim vrf VIDEO neighbor
Wed Apr 19 07:19:13.825 UTC

PIM neighbors in VRF VIDEO
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router

Neighbor Address            Interface              Uptime    Expires  DR pri   Flags

10.0.2.9*                   GigabitEthernet0/0/0/3 04:24:01  00:01:44 1 (DR) B E
10.0.0.3                    mdtVIDEO               04:23:41  00:01:43 1
10.0.0.4                    mdtVIDEO               04:23:42  00:01:39 1
10.0.0.5*                   mdtVIDEO               04:24:03  00:01:38 1 (DR)
```

Figura 4.79 – Vecinos PIM VPN del router PE_3.

El router RP 10.0.0.1 (CORE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_3#sh pim rp mapping
Wed Apr 19 07:19:55.622 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.0.1 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 04:24:45, expires: never
```

Figura 4.80 – Router RP (Rendezvous Point) configurado en la red ISP.

El router RP 10.0.2.100 (PE_1) está configurado de forma estática para todo el rango de direcciones multicast 224.0.0.0/4.

```
RP/0/0/CPU0:PE_3#sh pim vrf VIDEO rp mapping
Wed Apr 19 07:20:22.820 UTC
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 10.0.2.100 (?), v2
    Info source: 0.0.0.0 (?), elected via config
      Uptime: 04:25:13, expires: never
```

Figura 4.81 – Router RP (Rendezvous Point) utilizado en el servicio MVPN.

La dirección multicast 239.1.2.3 es el grupo MDT asignado al servicio multicast VPN. Esta dirección se utiliza para encapsular el tráfico multicast del dominio VPN para su transmisión entre los router PE.

En la salida de la figura 4.82 se muestra el registro (*,G) del árbol “Shared Tree” indicando la interfaz Gi0/0/0/0 hacia el RP.

```
RP/0/0/CPU0:PE_3#sh mrib route 239.1.2.3
Wed Apr 19 07:21:02.558 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.2.3) RPF nbr: 10.0.1.21 Flags: C RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:25:52
  Incoming Interface List
    GigabitEthernet0/0/0/0 Flags: A NS, Up: 04:25:40
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:25:50
```

Figura 4.82 – Tabla global multicast.

En la salida de la figura 4.83 se muestras los registros (S,G) del árbol “Source Tree (SPT)” indicando los PE registrados como fuente para el grupo MDT 239.1.2.3. Las interfaces mostradas en el apartado “Incoming Interface List (IIL)” son las interfaces hacia el PE fuente del grupo MDT, es decir, la interfaz por donde se recibiría tráfico multicast. Las interfaces mostradas en el apartado “Outgoing Interface List (OIL)” son las interfaces hacia el PE receptor del grupo MDT.

```
(10.0.0.3,239.1.2.3) RPF nbr: 10.0.1.25 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:25:30
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A, Up: 04:23:14
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:25:30

(10.0.0.4,239.1.2.3) RPF nbr: 10.0.1.25 Flags: RPF MD MH CD
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:25:31
  Incoming Interface List
    GigabitEthernet0/0/0/1 Flags: A NS, Up: 04:23:14
  Outgoing Interface List
    Loopback0 Flags: F NS, Up: 04:25:31

(10.0.0.5,239.1.2.3) RPF nbr: 10.0.0.5 Flags: RPF ME MH
  MVPN TID: 0xe0000011
  MVPN Remote TID: 0x0
  MVPN Payload: IPv4
  MDT IFH: 0x480
  Up: 04:25:52
  Incoming Interface List
    Loopback0 Flags: F A, Up: 04:25:50
  Outgoing Interface List
    Loopback0 Flags: F A, Up: 04:25:50
    GigabitEthernet0/0/0/1 Flags: F NS, Up: 04:23:14
```

Figura 4.83 – Tabla global multicast (continuación).

En la salida de la figura 4.84 se muestra el registro (S,G): (10.0.2.2,239.1.1.1) indicando en el apartado IIL la interfaz Gi0/0/0/3 conectada a la fuente multicast del servicio VPN y en el apartado OIL la interfaz túnel mdtVIDEO hacia los PE con receptores multicast en la VPN.

```
RP/0/0/CPU0:PE_3#sh mrib vrf VIDEO route 239.1.1.1
Wed Apr 19 07:22:07.423 UTC

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
    MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
    MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
    IRMI - IR MDT Interface

(*,239.1.1.1) RPF nbr: 10.0.0.3 Flags: C RPF
  Up: 04:26:50
  Incoming Interface List
    mdtVIDEO Flags: A NS MI, Up: 02:35:46
  Outgoing Interface List
    GigabitEthernet0/0/0/3 Flags: F NS LI, Up: 04:26:50

(10.0.2.2,239.1.1.1) RPF nbr: 10.0.0.3 Flags: RPF
  Up: 00:41:37
  Incoming Interface List
    mdtVIDEO Flags: A NS MI, Up: 00:41:37
  Outgoing Interface List
    GigabitEthernet0/0/0/3 Flags: F NS, Up: 00:41:37
```

Figura 4.84 – Tabla VPN multicast.

En la salida de la figura 4.85 se muestra el receptor 10.0.2.6 en la interfaz Gi0/0/0/3 conectado al grupo 239.1.1.1.

```
RP/0/0/CPU0:PE_3#sh igmp vrf VIDEO groups 239.1.1.1
Wed Apr 19 07:22:43.481 UTC
IGMP Connected Group Membership
Group Address   Interface                Uptime    Expires   Last Reporter
239.1.1.1       GigabitEthernet0/0/0/3   04:27:26  00:01:54  10.0.2.10
```

Figura 4.85 – Receptores Multicast del grupo 239.1.1.1.

V. CONCLUSIONES

Con la presentación de información de hardware actual de equipos de red y su sistema operativo, ambos diseñados específicamente para redes ISP, acompañado de los conceptos y fundamentos de MPLS y Multicast que se abordaron en este trabajo monográfico, se da lugar al desarrollo de casos de estudios que integren esos elementos y que reflejan escenarios y soluciones propias de una red IP contemporánea calificada para brindar servicios de telecomunicaciones.

Lo anterior se complementó con la utilización de un software emulador gratuito, moderno y versátil, EVE-NG en este caso particular, que es capaz de integrar equipos de alto desempeño y de distintos fabricantes, para implementar las configuraciones requeridas que permitan reconocer, entender, evaluar y validar escenarios que incluyen los principales servicios comúnmente ofrecidos en una red IP de servicios de telecomunicaciones como es la transmisión de datos y video, con el objetivo de proveer al estudiante o profesional en el campo de redes una guía actualizada que le sirva de referencia y facilite y acelere su curva de aprendizaje ya sea previo o durante su integración en este campo profesional.

Con lo descrito anteriormente, se concluye que el diseño de red presentado es funcional para enseñar la estructura básica e ideal de una red de servicios MPLS, sirviendo de guía para aprender, reforzar y ampliar los conocimientos en redes IP. También demuestra ser funcional para implementar los múltiples servicios disponibles con la tecnología MPLS. Adicionalmente, se comprobó que el software emulador utilizado facilita ejecutar diseños de red para desarrollar escenarios y soluciones que integren equipos modernos apropiados o calificados para redes ISP.

VI. RECOMENDACIONES

El profesional o estudiante en el campo de las telecomunicaciones en redes IP no debe limitarse a los conocimientos teóricos orientados a la administración de redes corporativas. Debe conocer y hacer uso de las diferentes herramientas y programas disponibles para emular distintos escenarios que le permitan desarrollar soluciones implementando diferentes tecnologías en hardware y software que lo preparen para la administración de todo tipo de redes: corporativas y de servicios de telecomunicaciones.

Se presentan las siguientes recomendaciones para estudios posteriores que utilicen este trabajo monográfico como referencia o punto de partida con el fin de darle continuidad al tema abordado:

- Rediseñar la red ISP agregando equipos del fabricante Huawei y su sistema operativo VRP, tanto en el Core como en la capa de Distribución (PE), es decir, una red que combine equipos Cisco y Huawei con el fin de desarrollar y presentar las configuraciones para los diferentes protocolos y servicios para ambas plataformas.

- Desarrollar los casos de estudio utilizando direccionamiento IPv6, protocolo que ya ha sido desplegado por los ISP nacionales en sus servicios.

- Desarrollar una solución para Implementar un servidor centralizado en el que se ejecute el emulador y que permita la conexión de múltiples usuarios para fines didácticos.

VII. BIBLIOGRAFIA

[1] J. Fuentes, R. Guido, “IMPLEMENTACION DE LA TECNOLOGIA MPLS EN EL EMULADOR GNS3 CON PROPOSITOS ACADEMICOS”, Universidad Nacional de Ingeniería, Managua, Nicaragua. 2018.

[2] L. Cruz, “Interconexión WAN de 3 sucursales de una empresa con casa matriz aplicando MPLS como tecnología de transporte mediante un diseño de red en GNS3”, Universidad Nacional de Ingeniería, Managua, Nicaragua. 2022.

[3] H. Cortez, L. Parrales, “Propuesta de configuración de una arquitectura de red MPLS con IPv6 sobre un core IPv4 en un ambiente de simulación”, Universidad Centroamericana, Managua, Nicaragua. 2014.

[4] H. Nguyen, (2009, Feb 07), “*Cisco 7600 Series Routers*”. [Online]. Available: https://community.cisco.com/t5/networking-knowledge-base/cisco-7600-series-routers/ta-p/3113431.

[5] (2015, Dic 7), “*CISCO 7600 SERIES INTERNET ROUTERS*”. [Online]. Available: https://lightriver.com/item/cisco-7600-series-internet-routers/.

[6] “*Cisco 7600 Series Routers - Retirement Notification*”. [Online]. Available: https://www.cisco.com/c/en/us/obsolete/routers/cisco-7600-series-routers.html.

[7] (2023, Feb 16), “*Cisco ASR 9000 Series Aggregation Services Routers Data Sheet*”. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/data_sheet_c78-501767.html.

[8] Content Desk, (2018, May 14), "*Cisco ASR 9000 Series Router Fast Facts*". [Online]. Available: https://www.netequity.com/cisco-asr-9000-series-router-fast-facts.

[9] Brad Edgeworth, Aaron Foss, Ramiro Garza Rios, *IP Routing on Cisco IOS, IOS XE, and IOS XR An Essential Guide to Understanding and Implementing IP Routing Protocols*. Indianapolis: Cisco Press, 2014.

[10] Ivan Pepelnjak, Jim Guichard. *MPLS and VPN Architectures, CCIP™ Edition*. Indianapolis: Cisco Press, 2002.

[11] M. Horchler. *"Unicast vs Multicast vs Broadcast: What's the Difference?"*. [Online]. Available: https://www.haivision.com/blog/all/broadcast-unicast-multicast-explained.

[12] Jim Guichard, Ivan Pepelnjak, Jeff Apcar. *MPLS and VPN Architectures*, Volume II. Indianapolis: Cisco Press, 2003.

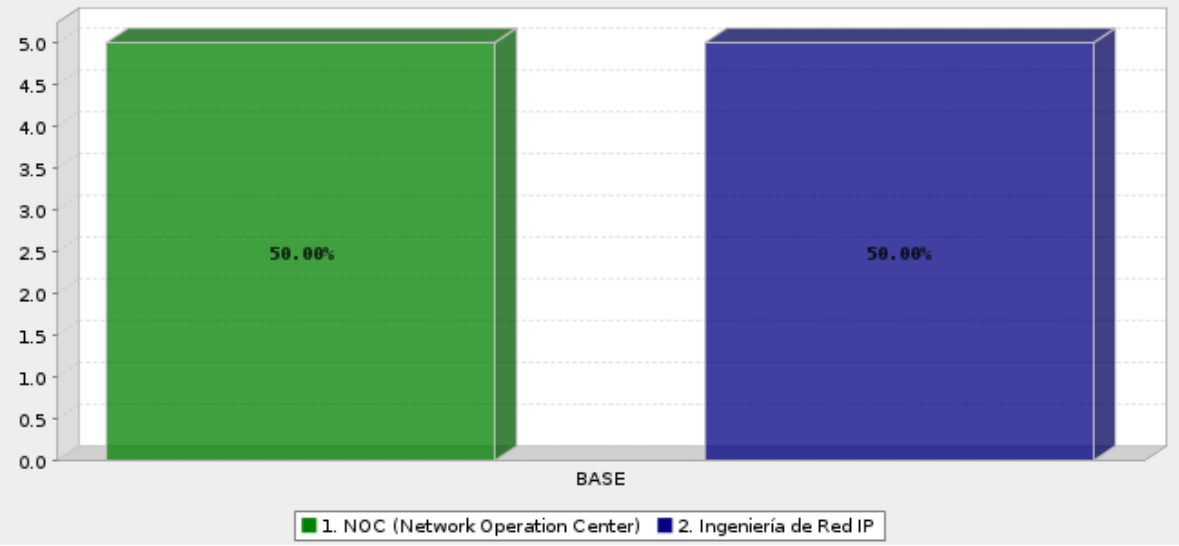
[13] Luc De Ghein. *MPLS Fundamentals*, Indianapolis: Cisco Press, 2006.

[14] Brent D. Stewart, Clare Gough. *CCNP BSCI Official Exam Certification Guide, Fourth Edition*. Indianapolis: Cisco Press, 2008.

VIII. ANEXOS

ANEXO 1: ENCUESTA

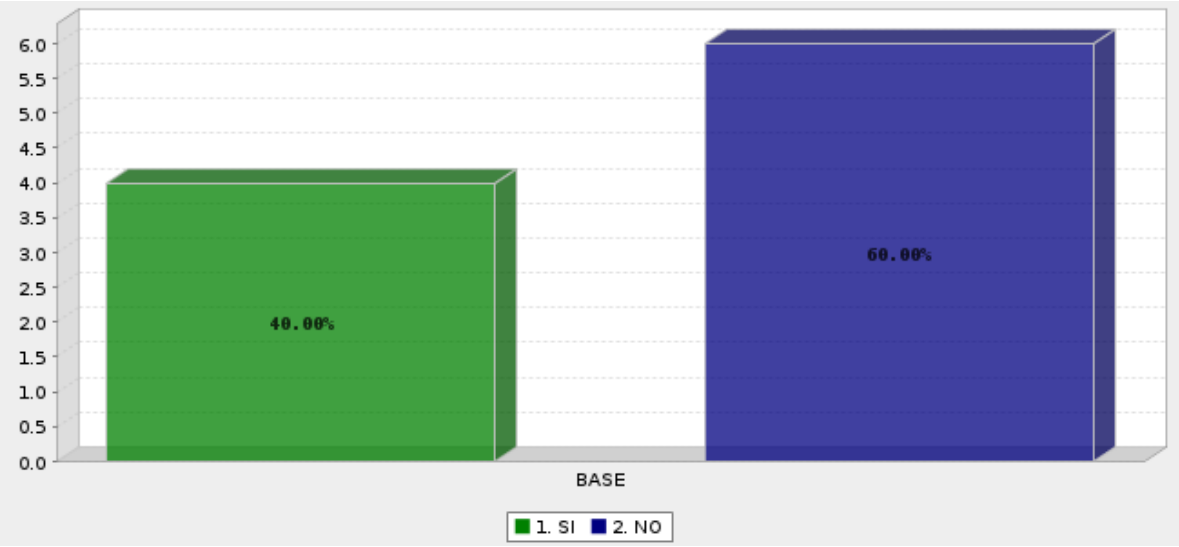
Q1. ¿A qué área perteneces?



	Answer	Contar	Percent
1.	NOC (Network Operation Center)	5	50.00%
2.	Ingeniería de Red IP	5	50.00%
	Total	10	100%

Media : **1.500**	Confidence Interval @ 95% : **[1.173 - 1.827]**	Standard Deviation : **0.527**	Standard Error : **0.167**

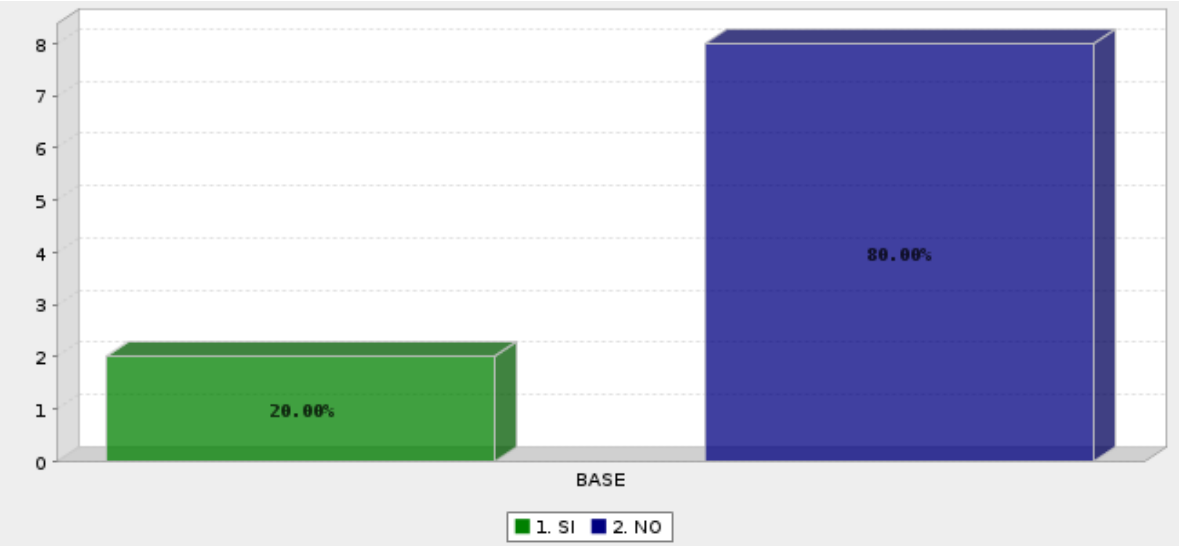
Q2. ¿Antes de trabajar en esta empresa, habías trabajado en un Proveedor de Servicios (ISP)?



	Answer	Contar	Percent
1.	SI	4	40.00%
2.	NO	6	60.00%
	Total	10	100%

Media : **1.600**	Confidence Interval @ 95% : **[1.280 - 1.920]**	Standard Deviation : **0.516**	Standard Error : **0.163**

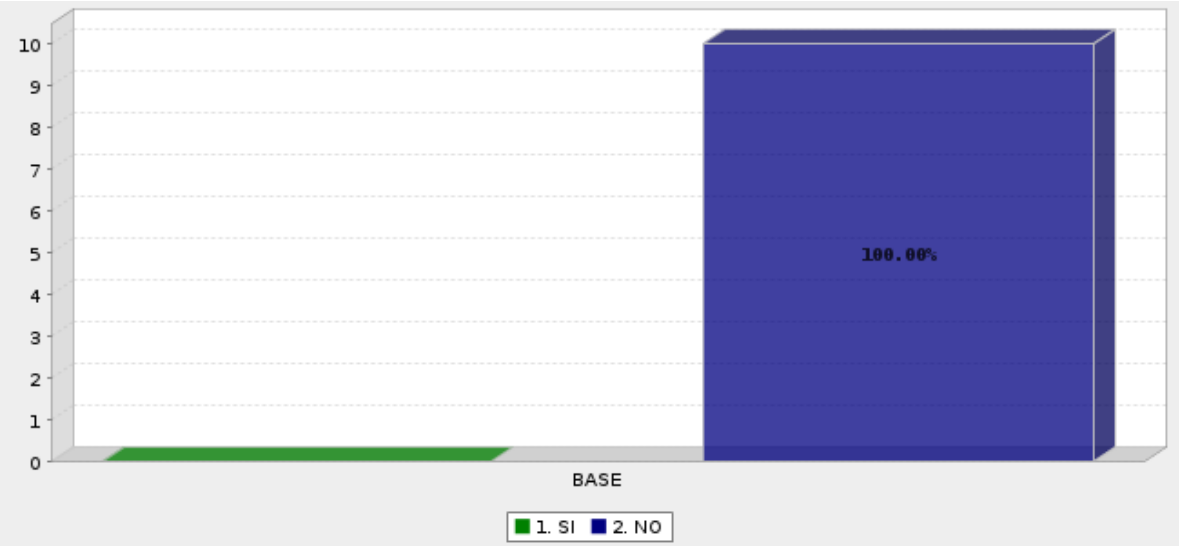
Q3. ¿Antes de trabajar en esta empresa, conocías los conceptos de MPLS y sus servicios?



	Answer	Contar	Percent
1.	SI	2	20.00%
2.	NO	8	80.00%
	Total	10	100%

Media : **1.800**	Confidence Interval @ 95% : **[1.539 - 2.061]**	Standard Deviation : **0.422**	Standard Error : **0.133**

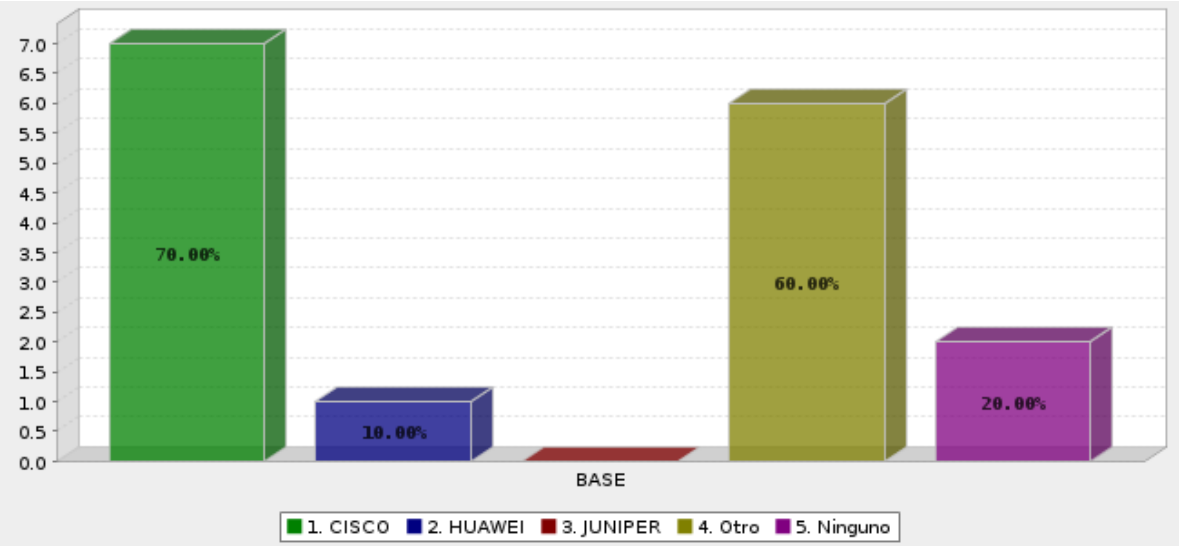
Q4. ¿Antes de trabajar en esta empresa, habías administrado/gestionado/configurado una red MPLS en servicio?



	Answer	Contar	Percent
1.	SI	0	0.00%
2.	NO	10	100.00%
	Total	10	100%

Media : **2.000**	Confidence Interval @ 95% : **[2.000 - 2.000]**	Standard Deviation : **0.000**	Standard Error : **0.000**

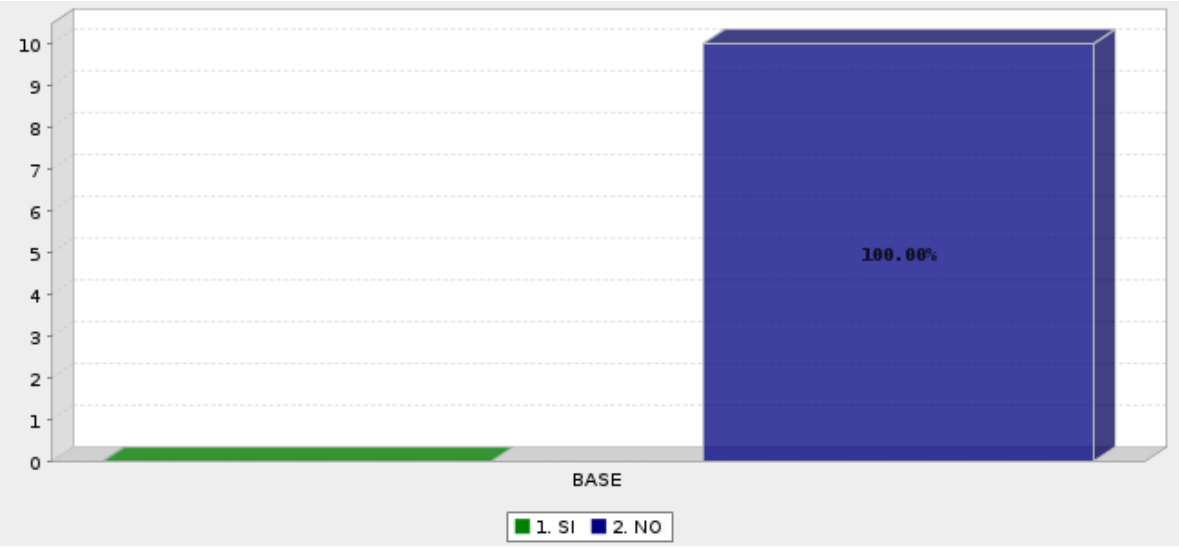
Q5. ¿Antes de trabajar en esta empresa, Con qué marca de equipo de red habías trabajado (configurado/gestionado) (Marque todas las que apliquen)?



	Answer	Contar	Percent
1.	CISCO	7	70.00%
2.	HUAWEI	1	10.00%
3.	JUNIPER	0	0.00%
4.	Otro	6	60.00%
5.	Ninguno	2	20.00%
	Total	16	n = 10.0

Media : **2.688**	Confidence Interval @ 95% : **[1.873 - 3.502]**	Standard Deviation : **1.662**	Standard Error : **0.416**

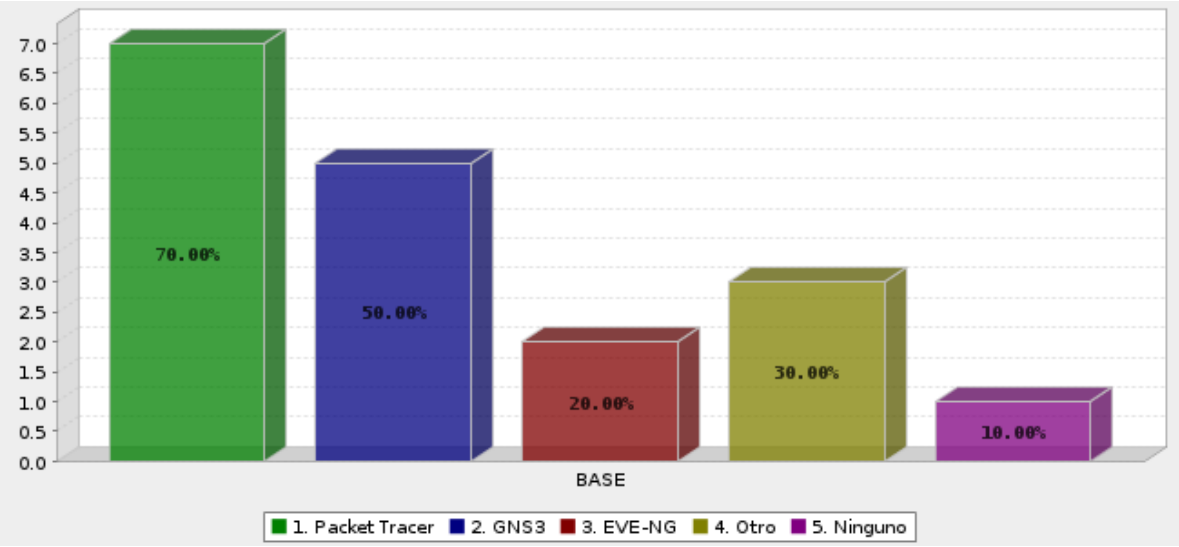
Q6. ¿Antes de trabajar en esta empresa, Configuraste equipos Cisco ASR9000 (cualquier modelo) con sistema operativo XR?



	Answer	Contar	Percent
1.	SI	0	0.00%
2.	NO	10	100.00%
	Total	10	100%

Media : **2.000**	Confidence Interval @ 95% : **[2.000 - 2.000]**	Standard Deviation : **0.000**	Standard Error : **0.000**

Q7. ¿Qué simulador/emulador de red utilizas? (Seleccione todas las que apliquen)



	Answer	Contar	Percent
1.	Packet Tracer	7	70.00%
2.	GNS3	5	50.00%
3.	EVE-NG	2	20.00%
4.	Otro	3	30.00%
5.	Ninguno	1	10.00%
	Total	18	n = 10.0

Media : **2.222**	Confidence Interval @ 95% : **[1.618 - 2.827]**	Standard Deviation : **1.309**	Standard Error : **0.308**

ANEXO 2: SOFTWARE UTILIZADO

A continuación, se detalla el software y elementos utilizados para emular la red de servicio sobre la cual se desarrollaron los casos de estudios.

Free EVE Community Edition Version 5.0.1-19

Software emulador de redes "multivendor" que permite a los profesionales en administración de redes y seguridad crear escenarios virtuales para probar soluciones o crear laboratorios de capacitación y entrenamiento.

Sitio de Descarga: Download (eve-ng.net)

VMware Workstation Player 17.0.2

Software de virtualización que se instala en un servidor físico y permite correr múltiples máquinas virtuales (VMs) en el mismo servidor.

Sitio de Descarga: VMware Workstation Player - VMware Customer Connect

xrv-k9-6.0.1

Imagen para plataforma Cisco ASR9000.

vios-adventerprisek9-m-15.6.2T

Imagen para router genérico Cisco (IOS).

c7200-[10]-adventerprisek9-mz.151-4.M2

Imagen para router Cisco 7200.

PC/Laptop de laboratorio

Equipo: LENOVO-LEGION7.

Sistema Operativo: Windows 11 Home.

Procesador: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz.

RAM: 16.0 GB.

ANEXO 3: CONFIGURACIONES CASOS DE ESTUDIO

CORE_1:

```
hostname CORE_1
cdp
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.1 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_2 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.1 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 no shutdown
 description RR Gi0/0/0/0
 cdp
 ipv4 address 10.0.1.5 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 no shutdown
 description PE_1 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.9 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 no shutdown
 description PE_2 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.17 255.255.255.252
!
```

```
interface GigabitEthernet0/0/0/4
 no shutdown
 description PE_3 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.21 255.255.255.252
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.1
 passive enable
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 0
  authentication message-digest
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   message-digest-key 1 md5 encrypted 104D000A0618
   network point-to-point
   passive disable
  !
 !
 area 1
  authentication message-digest
  interface GigabitEthernet0/0/0/1
   message-digest-key 1 md5 encrypted 05080F1C2243
   network point-to-point
   passive disable
  !
 !
 area 2
  authentication message-digest
  interface GigabitEthernet0/0/0/2
   message-digest-key 1 md5 encrypted 13061E010803
   network point-to-point
   passive disable
  !
 !
 area 3
  authentication message-digest
```

```
  interface GigabitEthernet0/0/0/3
   message-digest-key 1 md5 encrypted 045802150C2E
   network point-to-point
   passive disable
  !
 !
 area 4
  authentication message-digest
  interface GigabitEthernet0/0/0/4
   message-digest-key 1 md5 encrypted 00071A150754
   network point-to-point
   passive disable
  !
 !
!
mpls ldp
 router-id 10.0.0.1
 neighbor
  10.0.0.2:0 password encrypted 05080F1C2243
  10.0.0.3:0 password encrypted 094F471A1A0A
  10.0.0.4:0 password encrypted 01100F175804
  10.0.0.5:0 password encrypted 05080F1C2243
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
```

```
!
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/2
   enable
  !
  interface GigabitEthernet0/0/0/3
   enable
  !
  interface GigabitEthernet0/0/0/4
   enable
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
!
end
```

CORE_2

```
hostname CORE_2
cdp
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.2 255.255.255.255
!
```

```
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_1 Gi0/0/0/0
 cdp
 mtu 9000
 ipv4 address 10.0.1.2 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 no shutdown
 description INTERNET
 ipv4 address 10.0.1.201 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 no shutdown
 description PE_1 Gi0/0/0/1
 cdp
 mtu 9000
 ipv4 address 10.0.1.13 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 no shutdown
 description PE_2 Gi0/0/0/1
 cdp
 mtu 9000
 ipv4 address 10.0.1.29 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 no shutdown
 description PE_3
 cdp
 mtu 9000
 ipv4 address 10.0.1.25 255.255.255.252
!
prefix-set PFX_DEFAULT
  0.0.0.0/0
end-set
!
prefix-set PFX_RFC1918
  10.0.0.0/8 le 32,
  172.16.0.0/12 le 32,
  192.168.0.0/16 le 32
```

```
end-set
!
prefix-set PFX_INTERNET_OUT
  165.98.255.0/24 le 32
end-set
!
route-policy RPL_RR_OUT
  if destination in PFX_DEFAULT then
    pass
  else
    drop
  endif
end-policy
!
route-policy RPL_INTERNET_IN
  if destination in PFX_RFC1918 then
    drop
  else
    pass
  endif
end-policy
!
route-policy RPL_INTERNET_OUT
  if destination in PFX_INTERNET_OUT then
    pass
  endif
end-policy
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.2
 authentication message-digest
 passive enable
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   message-digest-key 1 md5 encrypted 14141B180F0B
   network point-to-point
```

```
  passive disable
 !
!
area 2
 interface GigabitEthernet0/0/0/2
  message-digest-key 1 md5 encrypted 110A1016141D
  network point-to-point
  passive disable
 !
!
area 3
 interface GigabitEthernet0/0/0/3
  message-digest-key 1 md5 encrypted 14141B180F0B
  network point-to-point
  passive disable
 !
!
area 4
 interface GigabitEthernet0/0/0/4
  message-digest-key 1 md5 encrypted 121A0C041104
  network point-to-point
  passive disable
 !
!
!
router bgp 64512
 bgp router-id 10.0.0.2
 address-family ipv4 unicast
 !
 neighbor 10.0.0.100
  remote-as 64512
  password encrypted 01100F175804
  description RR
  update-source Loopback0
  address-family ipv4 unicast
   route-policy RPL_RR_OUT out
   default-originate
   next-hop-self
  !
 !
 neighbor 10.0.1.202
```

```
  remote-as 1
  description INTERNET UPSTREAM PROVIDER
  address-family ipv4 unicast
   route-policy RPL_INTERNET_IN in
   route-policy RPL_INTERNET_OUT out
  !
 !
!
mpls ldp
 router-id 10.0.0.2
 neighbor
  10.0.0.1:0 password encrypted 070C285F4D06
  10.0.0.3:0 password encrypted 104D000A0618
  10.0.0.4:0 password encrypted 0822455D0A16
  10.0.0.5:0 password encrypted 13061E010803
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
 interface GigabitEthernet0/0/0/4
 !
!
multicast-routing
 address-family ipv4
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/2
```

```
   enable
  !
  interface GigabitEthernet0/0/0/3
   enable
  !
  interface GigabitEthernet0/0/0/4
   enable
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
!
!
end
```

ROUTE REFLECTOR

```
hostname RR
cdp
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.100 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_1 Gi0/0/0/1
 cdp
 ipv4 address 10.0.1.6 255.255.255.252
!
route-policy BGP_TO_RIB
  drop
end-policy
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.100
 authentication message-digest
 passive enable
```

```
 auto-cost reference-bandwidth 100000
 area 1
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   message-digest-key 1 md5 encrypted 121A0C041104
   network point-to-point
   passive disable
  !
 !
!
router bgp 64512
 bgp router-id 10.0.0.100
 address-family ipv4 unicast
  table-policy BGP_TO_RIB
 !
 address-family vpnv4 unicast
 !
 address-family ipv4 mdt
 !
 neighbor 10.0.0.2
  remote-as 64512
  password encrypted 070C285F4D06
  description BG_INTERNET
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
 !
 neighbor 10.0.0.3
  remote-as 64512
  password encrypted 121A0C041104
  description PE_1
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
  address-family ipv4 mdt
```

```
   route-reflector-client
  !
 !
 neighbor 10.0.0.4
  remote-as 64512
  password encrypted 104D000A0618
  description PE_2
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
  address-family ipv4 mdt
   route-reflector-client
  !
 !
 neighbor 10.0.0.5
  remote-as 64512
  password encrypted 070C285F4D06
  description PE_3
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
  address-family ipv4 mdt
   route-reflector-client
  !
 !
!
end
```

PE_1

```
hostname PE_1
cdp
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.3 255.255.255.255
!
interface Loopback100
 no shutdown
 vrf VIDEO
 ipv4 address 10.0.2.100 255.255.255.255
!
```

```
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_1 Gi0/0/0/2
 cdp
 mtu 9000
 ipv4 address 10.0.1.10 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 no shutdown
 description CORE_2 Gi0/0/0/2
 cdp
 mtu 9000
 ipv4 address 10.0.1.14 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 no shutdown
 description FUENTE MULTICAST - CANAL XYZ
 vrf VIDEO
 ipv4 address 10.0.2.1 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 no shutdown
 description CPE_1 Gi0/0
!
interface GigabitEthernet0/0/0/4.100
 no shutdown
 description SERVICIO INTERNET
 ipv4 address 165.98.255.1 255.255.255.252
 encapsulation dot1q 100
!
interface GigabitEthernet0/0/0/4.101
 no shutdown
 description SERVICIO DATOS
 vrf CORP_1
 ipv4 address 10.255.1.1 255.255.255.252
 encapsulation dot1q 101
!
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.1
```

```
  domain-tag 64512
  passive enable
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4.101
    network point-to-point
    passive disable
   !
  !
 !
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.3
 authentication message-digest
 message-digest-key 1 md5 encrypted 02050D480809
 passive enable
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 2
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
   passive disable
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
   passive disable
  !
 !
!
router bgp 64512
 bgp router-id 10.0.0.3
 address-family ipv4 unicast
  network 165.98.255.0/30
 !
 address-family vpnv4 unicast
  vrf all
   label mode per-vrf
  !
```

```
 !
 address-family ipv4 mdt
 !
 neighbor 10.0.0.100
  remote-as 64512
  password encrypted 104D000A0618
  description RR
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
  address-family vpnv4 unicast
  !
  address-family ipv4 mdt
  !
 !
 vrf VIDEO
  rd 64512:2
  address-family ipv4 unicast
   redistribute connected
  !
 !
 vrf CORP_1
  rd 64512:1
  default-information originate
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
mpls ldp
 router-id 10.0.0.3
 neighbor
  10.0.0.1:0 password encrypted 104D000A0618
  10.0.0.2:0 password encrypted 045802150C2E
 !
 address-family ipv4
  label
   local
    advertise
```

```
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
!
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
   enable
  !
  mdt source Loopback0
 !
 vrf VIDEO
  address-family ipv4
   interface Loopback100
    enable
   !
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
 vrf VIDEO
```

```
  address-family ipv4
   rp-address 10.0.2.100
  !
 !
!
end
```

PE_2

```
hostname PE_2
cdp
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.4 255.255.255.255
!
```

```
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_1 Gi0/0/0/3
 cdp
 mtu 9000
 ipv4 address 10.0.1.18 255.255.255.252
!
interface GigabitEthernet0/0/0/1
 no shutdown
 description CORE_2 Gi0/0/0/3
 cdp
 mtu 9000
 ipv4 address 10.0.1.30 255.255.255.252
!
interface GigabitEthernet0/0/0/2
 no shutdown
 shutdown
!
interface GigabitEthernet0/0/0/3
 no shutdown
 description RECEPTOR MULTICAST
 vrf VIDEO
 ipv4 address 10.0.2.5 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 no shutdown
 description CPE_MSY Gi0/0
 vrf CORP_1
 ipv4 address 10.255.1.5 255.255.255.252
!
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.5
  domain-tag 64512
  passive enable
  default-information originate
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4
    network point-to-point
```

```
    passive disable
   !
  !
 !
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.4
 authentication message-digest
 message-digest-key 1 md5 encrypted 00071A150754
 passive enable
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 3
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
   passive disable
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
   passive disable
  !
 !
!
router bgp 64512
 bgp router-id 10.0.0.4
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
  vrf all
   label mode per-vrf
  !
 !
 address-family ipv4 mdt
 !
 neighbor 10.0.0.100
  remote-as 64512
  password encrypted 060506324F41
  description RR
```

```
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
  address-family vpnv4 unicast
  !
  address-family ipv4 mdt
  !
 !
 vrf VIDEO
  rd 64512:2
  address-family ipv4 unicast
  !
 !
 vrf CORP_1
  rd 64512:1
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
mpls ldp
 router-id 10.0.0.4
 neighbor
  10.0.0.1:0 password encrypted 13061E010803
  10.0.0.2:0 password encrypted 00071A150754
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
```

```
 !
!
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
   enable
  !
  mdt source Loopback0
 !
 vrf VIDEO
  address-family ipv4
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
 vrf VIDEO
  address-family ipv4
   rp-address 10.0.2.100
  !
 !
!
end
```

PE_3

```
hostname PE_3
cdp
vrf VIDEO
 description VPN MULTICAST
 address-family ipv4 unicast
  import route-target
   64512:2
  !
  export route-target
   64512:2
  !
 !
!
vrf CORP_1
 description VPN CLIENTE 1
 address-family ipv4 unicast
  import route-target
   64512:1
  !
  export route-target
   64512:1
  !
 !
!
ipv4 access-list MPLS_LABELS
 10 permit ipv4 10.0.0.0/24 any
!
interface Loopback0
 no shutdown
 ipv4 address 10.0.0.5 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 no shutdown
 description CORE_1 Gi0/0/0/4
 cdp
 mtu 9000
 ipv4 address 10.0.1.22 255.255.255.252
!
```

```
interface GigabitEthernet0/0/0/1
 no shutdown
 description CORE_2 Gi0/0/0/4
 cdp
 mtu 9000
 ipv4 address 10.0.1.26 255.255.255.252
!
interface GigabitEthernet0/0/0/3
 no shutdown
 description RECEPTOR MULTICAST
 vrf VIDEO
 ipv4 address 10.0.2.9 255.255.255.252
!
interface GigabitEthernet0/0/0/4
 no shutdown
 description CPE_LEO Gi0/0
 vrf CORP_1
 ipv4 address 10.255.1.9 255.255.255.252
!
router ospf 101
 vrf CORP_1
  log adjacency changes detail
  router-id 10.255.1.9
  domain-tag 64512
  passive enable
  default-information originate
  redistribute bgp 64512
  area 0
   interface GigabitEthernet0/0/0/4
    network point-to-point
    passive disable
   !
  !
 !
!
router ospf 64512
 log adjacency changes detail
 router-id 10.0.0.5
 authentication message-digest
 message-digest-key 1 md5 encrypted 104D000A0618
 passive enable
```

```
 mpls ldp sync
 auto-cost reference-bandwidth 100000
 area 4
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
   network point-to-point
   passive disable
  !
  interface GigabitEthernet0/0/0/1
   network point-to-point
   passive disable
  !
 !
!
router bgp 64512
 bgp router-id 10.0.0.5
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
  vrf all
   label mode per-vrf
  !
 !
 address-family ipv4 mdt
 !
 neighbor 10.0.0.100
  remote-as 64512
  password encrypted 14141B180F0B
  description RR
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
  address-family vpnv4 unicast
  !
  address-family ipv4 mdt
  !
 !
 vrf VIDEO
  rd 64512:2
```

```
  address-family ipv4 unicast
  !
 !
 vrf CORP_1
  rd 64512:1
  address-family ipv4 unicast
   redistribute connected
   redistribute ospf 101
  !
 !
!
mpls ldp
 router-id 10.0.0.5
 neighbor
  10.0.0.1:0 password encrypted 00071A150754
  10.0.0.2:0 password encrypted 13061E010803
 !
 address-family ipv4
  label
   local
    advertise
     disable
     for MPLS_LABELS
    !
   !
  !
 !
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
!
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
  interface GigabitEthernet0/0/0/0
   enable
  !
  interface GigabitEthernet0/0/0/1
```

```
   enable
  !
  mdt source Loopback0
 !
 vrf VIDEO
  address-family ipv4
   interface GigabitEthernet0/0/0/3
    enable
   !
   mdt default ipv4 239.1.2.3
  !
 !
!
router pim
 address-family ipv4
  rp-address 10.0.0.1
 !
 vrf VIDEO
  address-family ipv4
   rp-address 10.0.2.100
  !
 !
!
!
end
```

ROUTER BORDE INTERNET

```
hostname INTERNET
!
interface Loopback0
 no shutdown
 ip address 8.8.8.8 255.255.255.255
!
interface GigabitEthernet0/0
 no shutdown
 description ROUTER ASN 64512
 ip address 10.0.1.202 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
```

```
!
router bgp 1
 bgp router-id 10.0.1.202
 bgp log-neighbor-changes
 network 8.8.8.8 mask 255.255.255.255
 neighbor 10.0.1.201 remote-as 64512
!
end
```

CPE_HQ

```
hostname CPE_HQ
!
interface Loopback100
 no shutdown
 description RED DATA CENTER
 ip address 192.168.1.1 255.255.255.0
 ip ospf network point-to-point
!
interface GigabitEthernet0/0
 no shutdown
 description ROUTER ISP
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.100
 no shutdown
 description SERVICIO INTERNET
 encapsulation dot1Q 100
 ip address 165.98.255.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
interface GigabitEthernet0/0.101
 no shutdown
 description SERVICIO DATOS
 encapsulation dot1Q 101
 ip address 10.255.1.2 255.255.255.252
 ip nat inside
```

```
 ip virtual-reassembly in
 ip ospf network point-to-point
!
router ospf 101
 router-id 10.255.1.2
 log-adjacency-changes detail
 passive-interface default
 no passive-interface GigabitEthernet0/0.101
 network 10.255.1.0 0.0.0.3 area 0
 default-information originate
!
ip nat inside source list NAT_INTERNET interface GigabitEthernet0/0.100 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.100 165.98.255.1 name RUTA_INTERNET
!
ip access-list extended NAT_INTERNET
 deny   ip 192.168.0.0 0.0.255.255 10.0.0.0 0.255.255.255
 deny   ip 192.168.0.0 0.0.255.255 172.16.0.0 0.15.255.255
 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
 permit ip 192.168.0.0 0.0.255.255 any
!
end
```

CPE_MSY

```
hostname CPE_MSY
!
interface Loopback100
 no shutdown
 description RED LAN
 ip address 192.168.2.1 255.255.255.0
 ip ospf network point-to-point
!
interface GigabitEthernet0/0
 no shutdown
 description CONEXION WAN ROUTER ISP
 ip address 10.255.1.6 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
!
```

```
router ospf 101
 router-id 10.255.1.6
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.255.1.4 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.3 area 0
!
end
```

CPE_LEO

```
hostname CPE_LEO
!
interface Loopback100
 no shutdown
 description RED LAN
 ip address 192.168.3.1 255.255.255.0
 ip ospf network point-to-point
!
interface GigabitEthernet0/0
 no shutdown
 description CONEXION WAN ROUTER ISP
 ip address 10.255.1.10 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
 media-type rj45
!
router ospf 101
 router-id 10.255.1.10
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.255.1.8 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
end
```

FUENTE MULTICAST

```
hostname S_MCast
!
interface GigabitEthernet0/0
 no shutdown
 ip address 10.0.2.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.1
!
end
```

RECEPTOR MULTICAST #1

```
hostname R_MCast_MSY
!
interface GigabitEthernet0/0
 no shutdown
 ip address 10.0.2.6 255.255.255.252
 ip igmp join-group 239.1.1.1
 duplex auto
 speed auto
 media-type rj45
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.5
!
end
```

RECEPTOR MULTICAST #2

```
hostname R_MCast_LEO
!
interface GigabitEthernet0/0
 no shutdown
 ip address 10.0.2.10 255.255.255.252
 ip igmp join-group 239.1.1.1
 duplex auto
 speed auto
 media-type rj45
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.0.2.9
!
end
```