Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

ANÁLISIS DE LOS ESCENARIOS DE IMPLEMENTACIÓN DE MULTICAST EN REDES PRIVADAS VIRTUALES DE ACUERDO CON LAS RFC 6513 Y 6514 DEL IETF

TRABAJO FIN DE MÁSTER

Celso Alberto Escobar Escobar

2013

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

ANÁLISIS DE LOS ESCENARIOS DE IMPLEMENTACIÓN DE MULTICAST EN REDES PRIVADAS VIRTUALES DE ACUERDO CON LAS RFC 6513 Y 6514 DEL IETF

Autor
Celso Alberto Escobar Escobar

Director
David Fernández Cambronero

Departamento de Ingeniería de Sistemas Telemáticos

2013

Resumen

Debido al incremento en el uso de aplicaciones que requieren el despliegue de tecnologías de transporte basadas en Multicast, como aplicaciones de video y replicación de ficheros, el entorno compuesto por los proveedores de servicios y los fabricantes de equipos ha impulsado la implementación y la estandarización del servicio Multicast en infraestructuras MPLS/BGP a través de redes virtuales denominadas MVPN (Multicast Virtual Private Networks).

Durante las dos últimas décadas, el fabricante Cisco Systems tomó la iniciativa y propuso un modelo basado en el despliegue de PIM en la red del proveedor de servicios que permite implementar MVPN. Esta solución fue documentada en el draft "Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs" conocido como draft Rosen, sin embargo, en la medida que se fueron incrementando los requerimientos de aplicaciones basadas en Multicast, el mismo IETF impulsado por los fabricantes de enrutadores IP y los proveedores de servicio, empezó a desarrollar las recomendaciones 6513 y 6514, las cuales recopilan la propuesta del draft Rosen y añaden otra posible implementación basada en Multi-Protocol BGP (MP-BGP).

Este documento analiza los bloques funcionales en los que se divide la solución planteada por las RFC 6513 y 6514 a partir de la identificación de los planos que la conforman que son el plano de control y el plano de transporte, así mismo se complementa el análisis con la revisión del estado del desarrollo de estos bloques funcionales por parte de los fabricantes, de tal forma que permita al proveedor de servicios evaluar el grado de madurez de la solución y sus funcionalidades en una implementación real.

Posteriormente se configuró un caso de estudio desarrollado en la plataforma de virtualización Junosphere del fabricante Juniper Networks. Este caso se basó en una de las posibles implementaciones del servicio MVPN con el plano de control basado en MP-BGP y el plano de transporte basado en MPLS, soportando tráfico Multicast de un cliente en una configuración SSM (Source Specific Multicast) donde el receptor indica explícitamente la fuente de la que desea recibir el tráfico Multicast, evitando que los enrutadores de la red del proveedor de servicio deban realizar labores de descubrimiento de la fuente.

Por último, se ofrecen a modo de conclusiones unas recomendaciones resultantes del análisis realizado, con el fin de que el proveedor de servicio contemple todos los aspectos relevantes antes de plantearse una implementación del servicio MVPN y que tome conciencia de la posible distancia que existe entre lo que se describe en las RFC y

lo que realmente se ha desarrollado o se tiene planificado desarrollar por parte de los fabricantes. Adicionalmente, fruto también del análisis realizado, se proponen algunos campos de investigación en los que se pueden plantear trabajos que deseen continuar analizando esta tecnología.

Abstract

Due to the increased use of applications that require the deployment of transport technologies based on Multicast, as applications of video and files replication, the environment comprised of service providers and equipment vendors, have driven the implementation and standardization of Multicast service in MPLS/BGP infrastructure through virtual networks so-called MVPN (Multicast Virtual Private Networks).

During the last two decades, the vendor Cisco Systems took the initiative to propose a model based on the deployment of PIM in the service provider network that allows to implement MVPN, this solution was documented in the draft "Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs" known as draft Rosen, however, as the requirements of Multicast-based applications were increasing, the IETF driven by routers IP vendors and service providers, began to develop recommendations 6513 and 6514, which collected the draft Rosen proposal and added another possible implementation based on multi-protocol BGP (MP-BGP).

This paper discusses the functional blocks that compose the solution described by the RFCs 6513 and 6514, from the identification of planes that make it up. These planes are the control plane and the transport plane. The analysis is complemented by the review of the development status of these functional blocks by the main IP router vendors, in order to allow the service provider to assess the degree of maturity of the solution and its features in a real deployment.

A case study developed in Junosphere virtualization platform of Juniper Networks vendor was subsequently set. This case was based on one of the possible implementations of MVPN service with control plane based on MP-BGP and the transport plane based on MPLS, supporting customer Multicast traffic in a SSM (Source Specific Multicast) configuration where the receiver identifies the source from which It wants to receive the Multicast traffic, avoiding that routers on the service provider network perform discovery of the source.

Finally, some recommendations arising from the analysis are offered as conclusions, with the purpose of allowing that the service provider acquires all relevant aspects before considering the MVPN service deployment and to take awareness of the possible distance that exists between what is described in the RFC and what actually has been developed or is planned to develop by vendors. In addition, also as a result of the analysis, it is proposed some research themes in which can be proposed works focused on continuing analyzing this technology.

Índice general

Índice de figuras

Siglas

AFI: Address Family Identifier

AS: Autonomous System

ASM: Any Source Multicast

BGP: Border Gateway Protocol

GRE: Generic Routing Encapsulation

IANA: Internet Assigned Numbers Authority

IGMP: Internet Group Management Protocol

IGP: Interior Gateway Protocol

IP: Internet Protocol

LSP: Link-State Protocol

LSP: Label Switched Path

MP-BGP: Multi Protocol Border Gateway Protocol

MPLS: Multi Protocol Label Switching

M-RIB: Multicast - Routing Information Base

MSDP: Multicast Source Discovery Protocol

NLRI: Network Layer Reachability Information

PIM: Protocol Independent Multicast

PIM-DM: Protocol Independent Multicast - Dense Mode

PIM-SM: Protocol Independent Multicast - Sparse Mode

PIM-SSM: Protocol Independent Multicast - Source Specific Multicast

PIM-BiDir: Protocol Independent Multicast - Bi-Directional

RIB: Routing Information Base

RP: Rendezvous Point

RPF: Reverse Path Forwarding

RPT: Rendezvous Path Tree

SA: Source Active

SAFI: Sub-Address Family Identifier

SPT: Shortest Path Tree

U-RIB: Unicast - Routing Information Base

1 Introducción

El proceso de estandarización del servicio Multicast en redes privadas virtuales conocido como MVPN (Multicast Virtual Private Network) ha sido excepcionalmente largo, pues desde el año 2001 la industria de las telecomunicaciones adoptó como estándar de facto el denominado draft-Rosen (Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs) propuesto por Cisco Systems al Internet Engineering Task Force (IETF). Sin embargo, este draft nunca se convirtió en un estándar y detuvo momentáneamente su evolución en el año 2005 debido a la aparición de otro draft conocido como 2547bis_mcast también enfocado a definir el servicio MVPN pero definiendo más escenarios de implementación e involucrando a otros fabricantes en su redacción, específicamente a Juniper Networks.

Finalmente el draft Rosen pasó a ser de carácter informativo y en octubre de 2010 se convirtió en la RFC histórica 6037 [1] quedando obsoleta por el draft 2547bis_mcast que a su vez se convirtió en estándar a través de la RFC 6513 [2] complementado por la RFC 6514 [3] en el mes de febrero de 2012.

Sin embargo, mientras evolucionaban las propuestas de estandarización de MVPN al interior del IETF, la necesidad de ofrecer servicios basados en Multicast por el auge de aplicaciones de replicación y servicios multimedia en escenarios corporativos como servicios de videoconferencia, replicación de video y redes de distribución de contenidos, requerían que los fabricantes de equipos y los proveedores de servicio de telecomunicaciones ofrecieran una solución, y es así como la implementación de MVPN se ajustó de manera generalizada al draft-Rosen con ciertas limitaciones de interoperabilidad ocasionadas por el hecho de que no era una recomendación formal.

Esta situación se mantuvo estable hasta la aparición de las RFC 6513 y 6514 que además de incluir las características técnicas del draft-Rosen, ofrece diversos escenarios de implementación de MVPN que plantean varios entornos tecnológicos de evolución para los proveedores de servicios de telecomunicaciones. Aunque no existe un impedimento técnico para desplegar varios escenarios en la misma red, de acuerdo con la RFC 6513, hacerlo implicaría una gran carga operativa que dificultaría la escalabilidad y el mantenimiento del servicio MVPN a mediano plazo.

Debido a lo anterior, los proveedores de servicios de telecomunicaciones interesados en ofrecer el servicio Multicast en entornos de Redes Privadas Virtuales de capa 3 (VPNL3 por sus siglas en inglés) deberán elegir entre los diferentes escenarios basándose en sus circunstancias particulares. Asimismo un proveedor que ya cuente con el servicio MVPN basado en el draft Rosen puede valorar la conveniencia de

evolucionar su servicio hacia alguno de los demás escenarios sugeridos las RFC 6513 y 6514.

Teniendo en cuenta el contexto descrito, el objetivo de este trabajo es ofrecer un análisis de las principales características técnicas de cada uno de los escenarios planteados por las recomendaciones RFC 6513 y 6514 del IETF, y las implicaciones de su implementación en la red de un proveedor de servicios de telecomunicaciones.

Este análisis se realizó basado en la documentación publicada por el IETF y por los fabricantes de enrutadores MPLS más representativos del mercado que son Alcatel-Lucent, Cisco Systems y Juniper Networks.

El documento se ha estructurado de la siguiente forma:

- En el capítulo 2 se realiza una introducción a la implementación de Multicast en redes IP planas sin una infraestructura MPLS/BGP.

- En el capítulo 3 se realiza una descripción de la solución descrita en las RFC 6513 y 6514 para ofrecer Multicast sobre redes IP utilizando un core MPLS/BGP y se analizan los bloques funcionales del servicio MVPN como lo plantean las RFC, destacando sus implicaciones y el soporte ofrecido por los fabricantes.

- En el capítulo 4 se describe la implementación de un caso de estudio de una de las variantes que ofrecen las RFC 6513/6514 para implementar el servicio MVPN, apoyado en la herramienta de virtualización de redes de telecomunicaciones *Junosphere* del fabricante de equipos Juniper Networks

- En el capítulo 5 se describen las conclusiones del trabajo realizado y los trabajos que se pueden plantear en el ámbito tecnológico del servicio Multicast IP en redes MPLS/BGP.

2 Multicast en redes IP

2.1 Descripción general

IP Multicast proporciona un mecanismo de trasporte de datos entre una fuente a varios receptores, en contraste con el servicio IP Unicast, donde un paquete es enviado desde una sola fuente a un solo receptor.

La dirección de destino de un paquete Multicast es siempre una dirección de grupo que pertenece al rango de direcciones IP clase D comprendido entre las direcciones IP 224.0.0.0-239.255.255.255. Estos rangos de direcciones son definidos por la IANA (Internet Assigned Numbers Authority) que es la entidad internacional que controla la asignación de la numeración de diferentes recursos utilizados en Internet (direcciones IP, números de puertos y sistemas autónomos entre otros).[4]

Dentro de este rango de direcciones que conforman la clase D, existen bloques reservados para diferentes objetivos, dentro de los que se destacan el rango 224.0.0.0 – 224.0.0.255 asignados a protocolos de red limitados a los segmentos de redes de área local (LAN), pues independientemente del TTL asignado en la cabecera IP, estos paquete en ningún caso serán retransmitidos por los enrutadores IP. Otro de los bloques destacados de direcciones Multicast es el integrado por el rango 239.0.0.0 - 239.255.255.255 destinado a dominios privados de redes Multicast. Este bloque de direcciones es equivalente al definido por la RFC 1918 para entornos Unicast privados [5, 6].

Básicamente, el flujo de datos en un entorno Multicast IP consiste en la transmisión de paquetes destinados a una dirección IP de grupo Multicast, la cuál ha sido previamente habilitada en los receptores interesados en este flujo para que puedan procesar los paquetes IP.

Dentro de la red IP, los enrutadores habilitados para Multicast tendrán la responsabilidad de distribuir los paquetes de forma optimizada, aumentando la eficiencia en el uso del ancho de banda.

Debe existir un mecanismo de señalización que les permita a los receptores indicarles a los enrutadores los grupos Multicast que desean recibir. Una vez se señalizan los grupos, los enrutadores establecen el camino por donde será transmitido el tráfico Multicast basados en protocolos de enrutamiento Multicast. Este camino se conoce como árbol de distribución y se ilustra en la Figura 1.

En los siguientes apartados se profundizará sobre cada uno de los aspectos técnicos que conforman el servicio Multicast en redes IP.

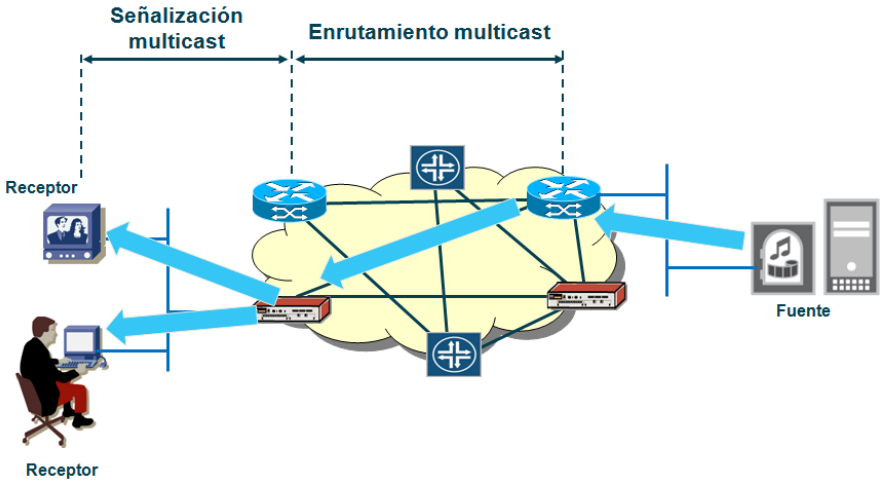

Figura 1. Escenario Multicast IP

2.2 Árboles de distribución Multicast

Los paquetes Multicast son enviados a través de la red empleando un árbol de distribución o MDT (Multicast Distribution Tree) en donde los enrutadores de la red se encargan de replicar los paquetes en cada punto de bifurcación del árbol. Esto significa que solo una copia del paquete viaja a través de un enlace particular de la red, permitiendo usar de forma eficiente el ancho de banda disponible de la red en situaciones donde se debe distribuir la misma información a varios receptores.

Existen dos tipos de MDT, los que empiezan directamente en el enrutador que proporciona conexión a la fuente o "*Source Trees*" y los que pueden ser compartidos por varias fuentes o "*Shared Trees*" [6].

2.2.1 Source Trees

En este tipo de árbol de distribución, el enrutador al que se conecta la fuente del tráfico Multicast se localiza en la raíz del árbol y los receptores se localizan en los extremos de las ramas. Con esta topología lógica, el tráfico Multicast es transportado por la red desde la fuente hasta los receptores siguiendo el árbol.

Cada uno de los enrutadores que hacen parte del árbol elije la interfaz por la que debe transmitir el tráfico Multicast basado en la tabla de conmutación Multicast o MFT (Multicast Forwarding Table). Esta tabla consiste de una serie de entradas donde registra las interfaces asociadas a la pareja de direcciones IP del grupo y la fuente de ese grupo. *Source tree* emplea la notación (S,G) para las entradas en esa tabla, donde S representa la dirección IP de la fuente y G representa la dirección IP Multicast del grupo, cada una de estas entradas se conoce como un estado.

El uso de *source trees* implica que la ruta entre la fuente y los receptores es el camino más corto, debido a esto los *source trees* también son denominados "Shortest Path Trees" (SPT).

Para cada fuente activa (transmitiendo paquetes Multicast) existe un *source tree* asociado, incluso si existen varias fuentes transmitiendo sobre el mismo grupo, ocasionando que exista una entrada (S,G) en la MFT para cada fuente activa de la red. Por lo tanto, los *source trees* proveen un encaminamiento óptimo del tráfico Multicast en la red, sin embargo, pueden comprometer la escalabilidad de los enrutadores debido a que requieren almacenar más información.

En la Figura 2 la fuente IP1 transmite al grupo G1 para el que hay dos receptores interesados. La entrada en la MFT sería (IP1,G1). Si otra fuente (IP2) empieza a transmitir sobre el mismo grupo G1, aparecerá una nueva entrada (IP2,G1) en la MFT.

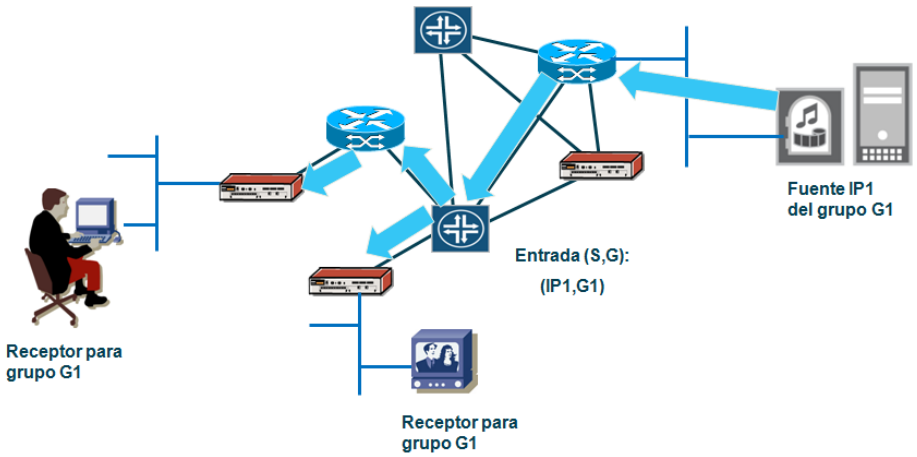

Figura 2. Source tree

2.2.2 Shared Trees

La principal diferencia de este tipo de árboles respecto a los "*source tree*" es que la raíz del árbol es un punto común en la red denominado "*Rendezvous Point*" (RP). Un solo RP puede ser la raíz para varios o todos los grupos Multicast, sin embargo, también es posible de que existan varios RP en la red.

Las fuentes transmiten el tráfico hacia el RP y cuando un receptor desea unirse al grupo Multicast debe enviar una solicitud de asociación al enrutador que tenga directamente conectado. Este enrutador le enviará la solicitud al RP que a su vez le retransmite el tráfico proveniente de la fuente y le informará a enrutador receptor sobre las fuentes activas para ese grupo.

Los *shared trees* emplean la notación (*,G) para las entradas en la MFT, donde * representa todas las fuentes para un grupo, y G representa la dirección IP Multicast del grupo. Todas las fuentes para un grupo en particular comparten el mismo *shared tree*,

por lo tanto si aparece una nueva fuente activa para un grupo, se mantendrá una única entrada en la MFT.

El uso de *shared trees* no ofrece un enrutamiento óptimo ya que el tráfico debe fluir desde las fuentes al RP y luego seguir el camino creado por los registros (*,G) hasta los receptores. Sin embargo los enrutadores deben almacenar menor cantidad de estados en la MFT comparándola con la cantidad de estados almacenados en los *source tree*.

La única dirección IP que necesitan conocer los enrutadores a los que se conectan los receptores es la asignada al RP del grupo Multicast. Esta puede ser configurada estáticamente en cada enrutador o aprendida dinámicamente mediante mecanismos como Auto-RP que es propietario de Cisco [6] o Bootstrap Router y Anycast RP definidos por el IETF [7, 8].

Tanto Auto-RP como Bootstrap (BSR) permiten varios candidatos a RP en la red, pero solamente escogen uno de ellos. Si el enrutador elegido se encuentra indisponible, estos protocolos escogen un nuevo RP entre los candidatos. Por otra parte Anycast RP permite la existencia de varios RP en la red gracias a la asignación de una dirección IP para todos, con lo que los enrutadores conectados a las fuentes y a los receptores podrán distribuir las asociaciones a los RP más convenientes de acuerdo a las políticas de enrutamiento Unicast de la red.

Así mismo, dentro de los *shared tree* existen dos categorías: unidireccionales y bidireccionales. En los unidireccionales los *shared tree* son usados para transportar el flujo de datos desde los RP hacia los receptores, pero no pueden ser usados para que el RP reciba tráfico, por esta razón las fuentes deben enviar tráfico a los RP a través de *source trees* también llamados "*shortest path trees*" como se observa en la Figura 3.

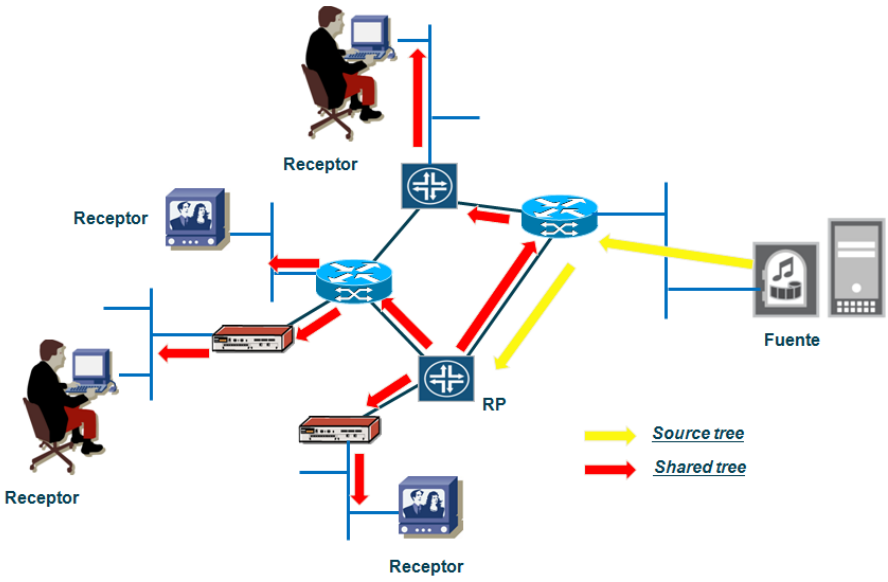

Figura 3. Shared tree unidireccional

Por otra parte, en un *shared tree* bidireccional, el tráfico puede fluir en los dos sentidos del árbol hasta llegar a los receptores sin necesidad de pasar por el RP, por lo que proveen una mayor optimización del enrutamiento, manteniendo al mismo tiempo una mínima cantidad de información de los estados a almacenar en la MFT.

La Figura 4 ilustra un *shared tree* bidireccional.

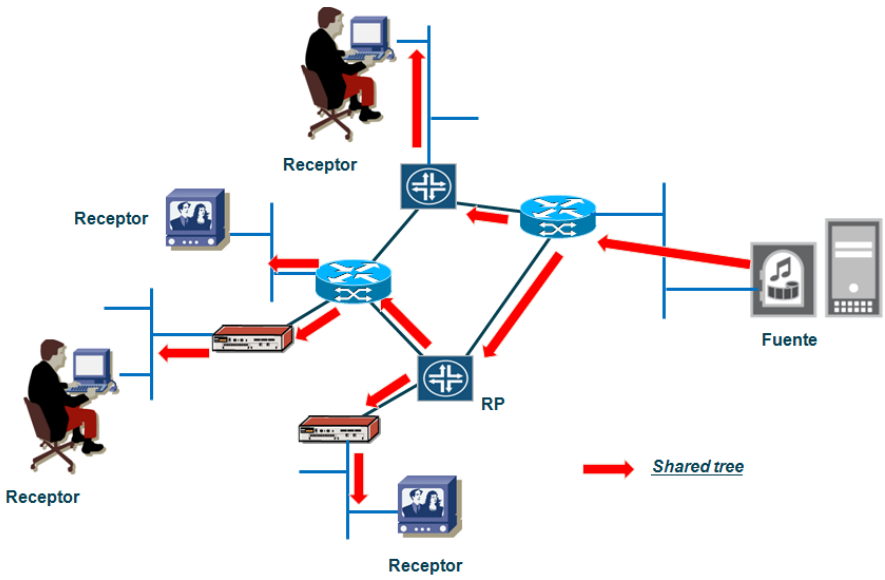

Figura 4. Shared tree bidireccional

2.3 Conmutación de tráfico Multicast

La conmutación de paquetes dentro de un enrutador puede dividirse en dos tipos: Unicast y Multicast.

En el conmutación Unicast la elección de la interfaz de salida del paquete es basada en la dirección IP de destino calculando el siguiente salto mediante la tabla de enrutamiento Unicast, sin embargo, esta decisión no es aplicable en la conmutación de paquetes Multicast, donde el destino corresponde a varios equipos receptores de los que no se puede deducir su ubicación por la dirección IP del grupo Multicast, que es la dirección incluida en el campo destino del paquete. Por esta razón se utiliza el proceso denominado *Reverse Path Forwarding* (RPF) que se basa en la ubicación de las direcciones IP de las fuentes. RPF se describe a continuación.

2.3.1 Reverse Path Forwarding

Cada paquete Multicast recibido en una interfaz de un enrutador es sometido a un test de RPF. Este test determina si el paquete es reenviado o descartado y previene bucles dentro de la red [6].

El proceso ante la llegada de un paquete Multicast es el siguiente:

- El enrutador examina la dirección IP origen del paquete Multicast para determinar si el paquete IP ha sido recibido por la interfaz que está en el camino de ida a la fuente.
- Si es cierto, entonces el paquete Multicast es reenviado por las interfaces pertenecientes al listado de interfaces de salida o "*outgoing interface list*" (olist) asociadas al grupo Multicast, excepto por el interfaz por el que ha llegado el paquete. Le creación del olist se explicará en el apartado 2.5.
- Si no es cierto, el paquete Multicast es descartado.

En la Figura 5 se representa un fallo y un éxito en el test RPF para un paquete Multicast con origen IP_B. En este caso se emplea la tabla de enrutamiento Unicast para realizar el test, al examinar la tabla de enrutamiento la entrada correspondiente es la de la red IP_B.

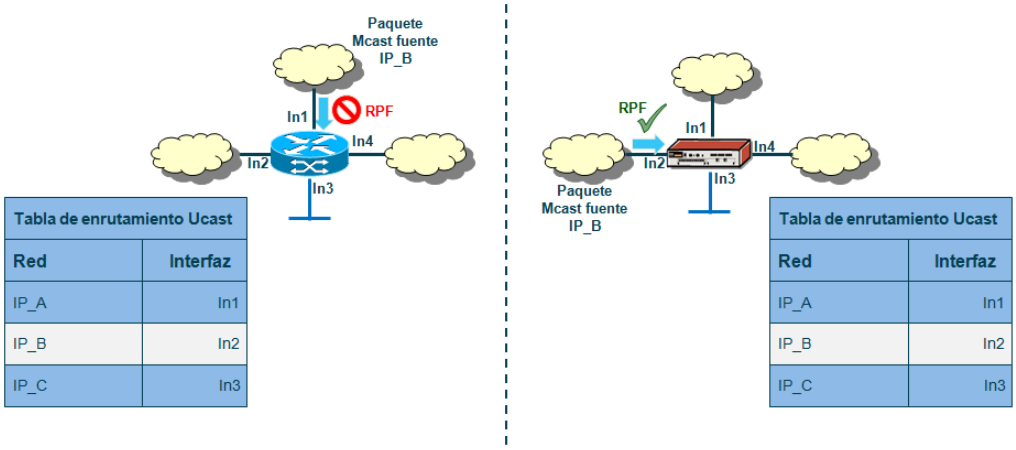

Figura 5. Reverse path forwarding

El mecanismo por el cual el enrutador determina qué interfaz se encuentra en el camino de vuelta a la fuente depende del protocolo de enrutamiento Multicast empleado. Por ejemplo, PIM (Protocol Independent Multicast) emplea la tabla de enrutamiento Unicast, mientras que DVMRP (Distance Vector Multicast Routing Protocol) emplea un mecanismo de vector de distancias para construir una tabla de enrutamiento Multicast. En este documento solo se estudiarán los mecanismos de selección de rutas desarrollados por PIM que es el protocolo referenciado en las RFC 6513 y 6514.

2.3.2 Umbrales de TTL o "TTL Scoping"

Cuando un enrutador conmuta un paquete Multicast, el valor de TTL (Time To Live) contenido en la cabecera IP se disminuye en uno. Si el valor llegar a cero, el enrutador descarta el paquete.

Mediante el establecimiento de umbrales de TTL se provee un método para evitar la conmutación de tráfico Multicast a través de la frontera de una zona basándose en el campo TTL del paquete Multicast. Esta técnica se denomina *TTL Scoping*.

Las aplicaciones Multicast que deben mantener su tráfico dentro de una determinada zona de la red transmiten su tráfico Multicast con un valor de TTL inicial que no permita cruzar las fronteras definidas por los umbrales de TTL [6].

La Figura 6 ilustra un ejemplo de *TTL scoping*, donde llega un paquete Multicast a través de In0, es replicado en In2 e In3, pero no en In4 al tener un valor de TTL menor que el umbral:

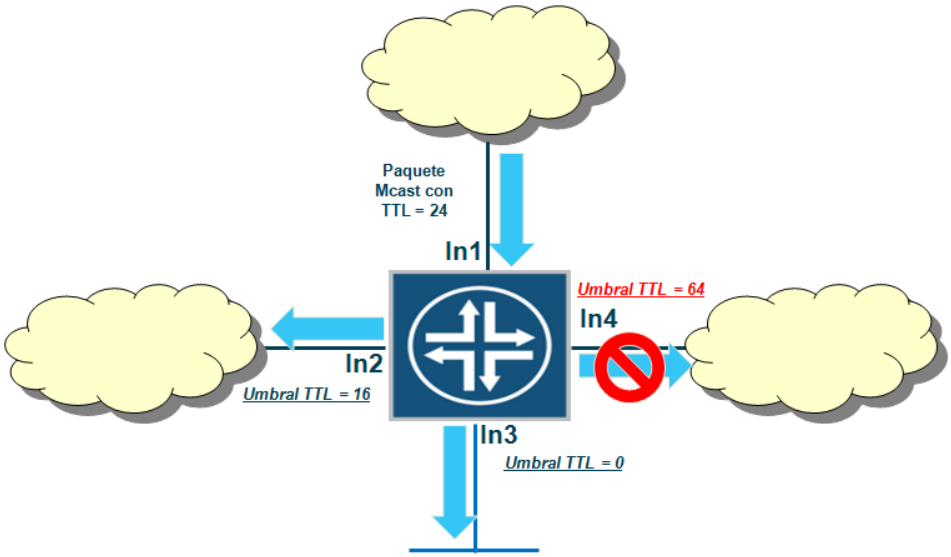

Figura 6. TTL scope

La técnica de TTL Scoping tiene la limitación de que se aplica a todos los paquetes Multicast, independientemente del grupo Multicast usado.

2.3.3 Límites administrativos o "administratively scoped boundaries"

Esta técnica proporciona un mecanismo de limitación de conmutación de tráfico Multicast fuera de un dominio o subdominio basándose en la dirección de grupo Multicast empleado.

Emplea un rango especial de direcciones Multicast como mecanismo de frontera. El rango de direcciones definido debe estar entre 239.0.0.0 y 239.255.255.255, este rango se considera como localmente asignado y no es usado en Internet [6].

Al configurar esta técnica en los interfaces de un enrutador, el tráfico Multicast cuya dirección de grupo Multicast cae dentro del rango definido, no podrá entrar ni salir del interfaz, comportándose como un corta-fuegos o *firewall* para el tráfico Multicast.

En la Figura 7 un enrutador tiene definida un límite administrativo para el rango 239.0.0.0/8 en el interfaz Int2. Todos los paquetes entrantes o salientes con dirección de grupo en ese rango no podrán atravesar la interfaz.

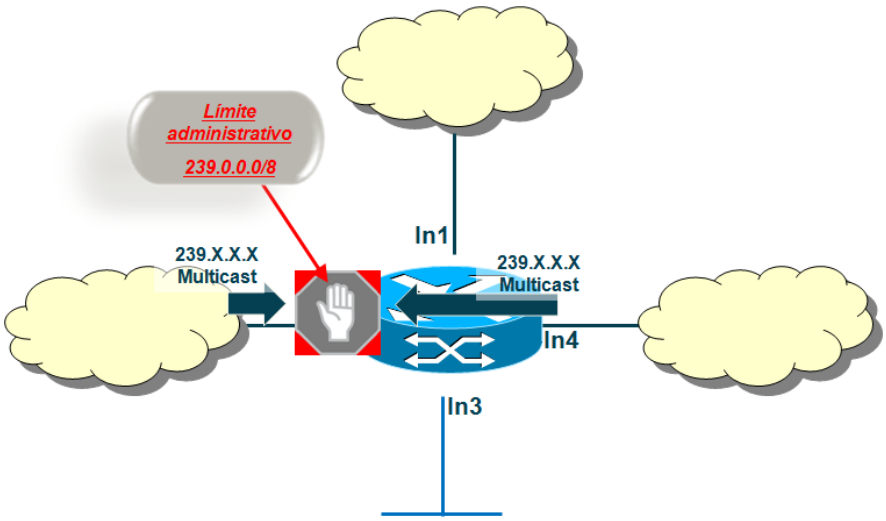

Figura 7. Límites administrativos

2.4 Internet Group Management Protocol

Este protocolo es utilizado por los receptores para indicarle los grupos en los que están interesados a los enrutadores a los que están conectados, especificando que se unen a un determinado grupo IP Multicast y así comenzar a recibir tráfico destinado a ese grupo.

Los mensajes IGMP son intercambiados entre el receptor y el enrutador al que está conectado y que le provee el servicio Multicast. Utilizando la información obtenida a través de los mensajes IGMP, los enrutadores mantienen una lista con los grupos IP Multicast y sus miembros junto a la información de las interfaces por las cuales los alcanza. Un grupo se considera activo sobre una determinada interfaz, cuando existe al menos un receptor que pertenezca a dicho grupo y al cual se llega a través de esa interfaz.

IGMPv1 utiliza un modelo de pregunta/respuesta, por el cual los enrutadores determinan si un determinado grupo está activo o no. Los enrutadores escuchan los mensajes y periódicamente envían mensajes preguntando si los miembros del grupo se encuentran activos o inactivos [9].

Utilizando IGMPv2 los receptores pueden enviar mensajes indicando que ya no desean pertenecer por más tiempo a un determinado grupo IP Multicast y de esta forma dejan de recibir tráfico destinado a dicho grupo. Entonces el enrutador pregunta si existe algún host interesado en seguir recibiendo tráfico Multicast; si no recibe respuesta dejará de enviar tráfico IP Multicast hacia el grupo [10].

En IGMPv3 los receptores pueden enviar dentro de sus mensajes una lista con las fuentes a las que desean asociarse para recibir el tráfico con lo que no solo seleccionan el grupo sino que también pueden seleccionar la fuente [11].

2.5 Protocol Independent Multicast

Existen diversos protocolos para la creación de una tabla de enrutamiento Multicast entre los que se encuentran *Distance Vector Routing Multicast Protocol* (DVRMP), *Multicast Open Short Path First* (MOSPF), *Core Based Trees* (CBT). Estos protocolos tienen en común que desarrollan sus propios mecanismos para crear la tabla de enrutamiento Multicast, por lo tanto el test RPF no usa la información disponible en la tabla de enrutamiento Unicast [6].

Por otra parte se encuentra *Protocol Independient Multicast* (PIM) que es independiente del protocolo IGP (*Interior Gateway Protocol*) empleado en la red y basa sus decisiones en la tabla de enrutamiento Unicast para comprobar que el paquete Multicast ha llegado por la interfaz correcta.

Si la comprobación es exitosa, la interfaz se identifica como interfaz RPF y es almacenada con las entradas (S,G) o (*,G) en la tabla MFT para evitar que el test RPF de cada paquete Multicast necesite consultar la tabla de enrutamiento. Si la tabla de enrutamiento Unicast cambia, entonces el interfaz RPF se actualiza en la tabla MFT para reflejar ese cambio de enrutamiento.

PIM debe establecer adyacencias entre los enrutadores directamente conectados que tengan habilitado el protocolo, para ello envía mensajes periódicos denominados "*Hello*" utilizando paquetes IP Multicast con dirección destino 224.0.13.0.

Una vez establecidas las adyacencias, PIM utiliza dos métodos para el envío de paquetes Multicast:

- *Any Source Multicast* (ASM): Emplea un modelo muchos-a-muchos donde varias fuentes están enviando tráfico a un grupo Multicast.
- *Source Specific Multicast* (SSM): Emplea un modelo uno-a-muchos donde el receptor se asocia directamente a la fuente del tráfico Multicast.

Así mismo, de forma independiente al método utilizado para transmitir el tráfico Multicast, existen tres variantes de PIM que son el modo extendido o *Dense Mode* (PIM-DM), modo disperso o *Sparse Mode* (PIM-SM) y modo bidireccional (PIM Bi-Dir). Tanto PIM-DM como PIM-SM pueden funcionar como ASM y SSM mientras que PIM-BiDir solo funciona como ASM.

A continuación se describen cada una de las variantes de PIM.

2.5.1 PIM-DM

Este modo asume que por cada subred existe al menos un receptor para cada flujo (S,G). Por lo tanto todos los paquetes Multicast son transmitidos a todos los puntos de la red como se ilustra en la Figura 8.

El proceso de construcción del árbol es el siguiente:

- En el momento en que una fuente comienza a transmitir, los MDT son construidos utilizando un mecanismo *flood-and-prune*, empleando la información de sus enrutadores adyacentes. Inicialmente los enrutadores adyacentes son incluidos dentro del árbol SPT, entonces el paquete IP Multicast es enviado a todos los vecinos.

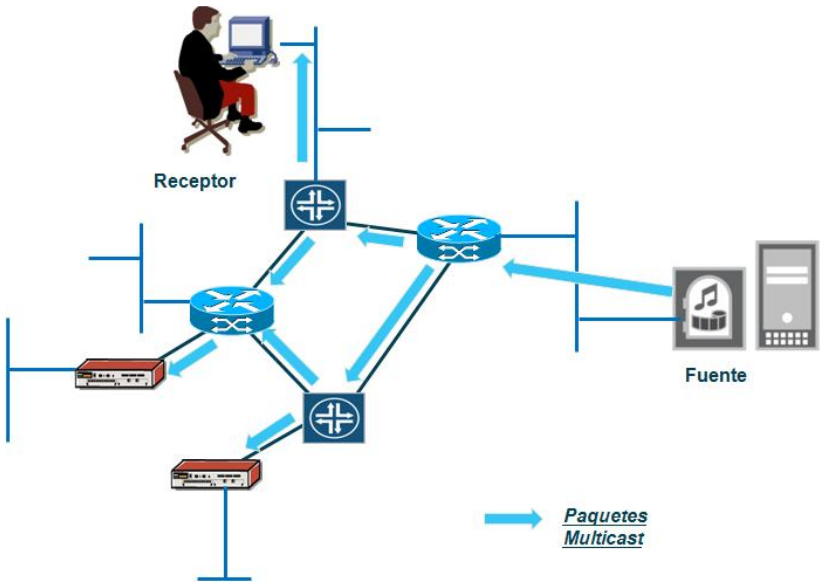

Figura 8. PIM Dense Mode

- Los enrutadores que no estén interesados en recibir el flujo Multicast por no tener un receptor para el (S,G), envían un mensaje PIM *prune* para que sea eliminado del SPT como se observa en la Figura 9. Este proceso permitirá eliminar las ramas del árbol que no contienen receptores, sin embargo, las entradas (S,G) siguen permaneciendo en todos los enrutadores.

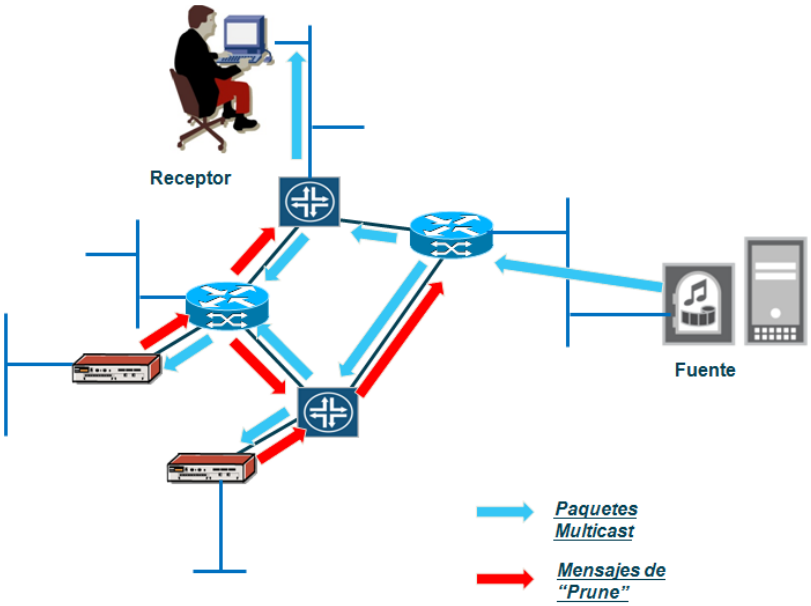

Figura 9. Mensajes de Prune en PIM DM

- El resultado es un árbol con ramas donde únicamente existen receptores como se observa en la Figura 10. Periódicamente los mensajes *prune* expiran y el tráfico Multicast vuelve a fluir por la red hasta que se recibe un nuevo mensaje *prune*.

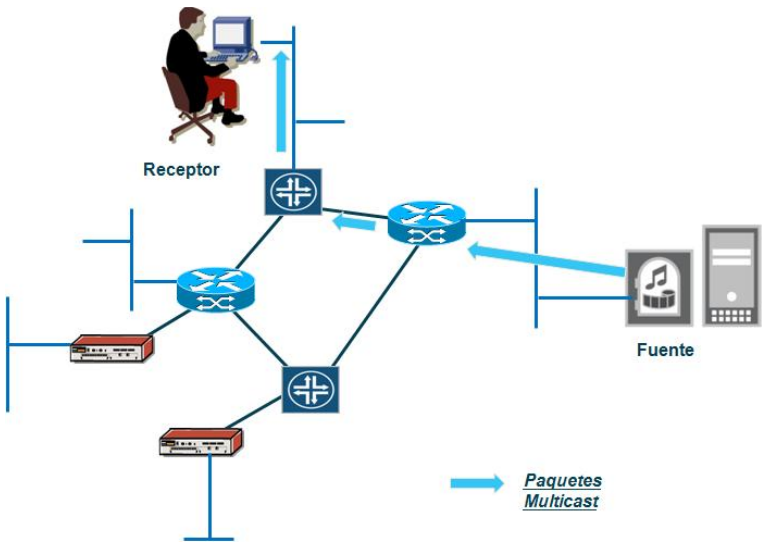

Figura 10. Flujo final de Multicast en PIM-DM

2.5.2 PIM-SM

En la variante SM el tráfico es distribuido sólo donde es requerido, si se recibe un mensaje PIM solicitando la asociación de un enrutador a un grupo Multicast, este mensaje es conocido como "*Join*".

PIM-SM soporta tanto *source trees* como *shared trees* y necesita de enrutadores que cumplan la función de RP para la coordinación del envío de paquetes Multicast. La elección de la localización del RP es muy importante para garantizar el correcto

funcionamiento del servicio Multicast. Todos los enrutadores en un dominio PIM-SM deben conocer el RP para un determinado grupo y diferentes grupos pueden tener diferentes RP. La elección del RP puede hacerse de una manera estática configurándola en cada uno de los enrutadores de la red o de manera dinámica (Auto-RP, BSR, Anycast-RP) como se explicó en el apartado 2.2.2.

PIM-SM tiene tres fases en el proceso de envío de tráfico Multicast desde una fuente a un receptor, estas son [6]:

- ***Construcción del shared tree desde el receptor al RP:*** Si un receptor está interesado en recibir un determinado grupo Multicast, envía un mensaje al enrutador con soporte PIM que haya sido seleccionado para proporcionarle servicio Multicast, en adelante será llamado enrutador de egreso; este enrutador envía mensajes (*,G) *PIM Join* a su vecino en la tabla RPF y así sucesivamente se irán retransmitiendo los mensajes hasta llegar al RP construyéndose el Rendezvous Path Tree (RPT) o *shared tree* como se observa en la Figura 11.

  Cada enrutador añade la interfaz por la que recibe el *Join* a la lista de interfaces por los que se pueden alcanzar receptores interesados en un determinado grupo (olist). Una vez se construye el *shared tree*, el tráfico Multicast fluye desde el RP a los receptores interesados. Este proceso también puede realizarse aunque no existan fuentes activas.

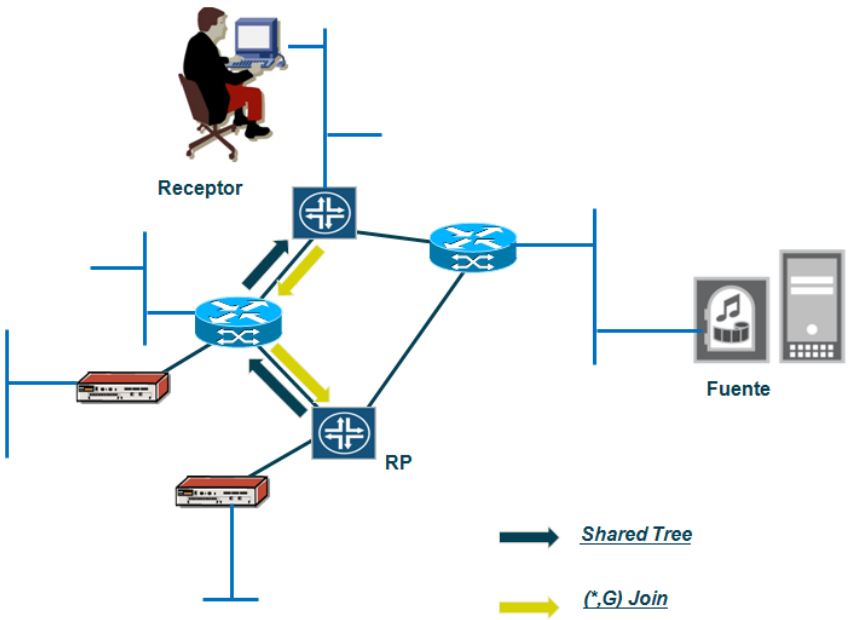

Figura 11. PIM SM - Shared Tree

- ***Construcción del árbol de distribución desde la fuente al RP:*** Cuando una fuente se activa empieza a enviar información al enrutador con soporte PIM

que haya sido seleccionado para proporcionarle servicio Multicast, en adelante será llamado enrutador de ingreso. Este enrutador le indica al RP que tiene una fuente activa mediante un mensaje PIM *register* vía Unicast, así mismo envía el paquete Multicast encapsulado en el mensaje *register*. Cuando el RP recibe el *register* desencapsula el paquete Multicast y en el caso de existir receptores interesados para el grupo, lo reenvía a través del RPT; por otra parte, envía un mensaje *PIM-Join* hacia el enrutador de ingreso para que se cree un SPT o *source tree* como se describe en Figura 12.

Una vez se ha construido el SPT desde el enrutador de ingreso hasta el RP, el RP recibe dos copias de cada paquete Multicast. Una copia llega a través del SPT y la otra llega encapsulada en los mensajes *register*. En cuanto esto ocurre, el RP envía un mensaje PIM *stop* hacia el enrutador de ingreso para que cese el envío de mensajes *register*.

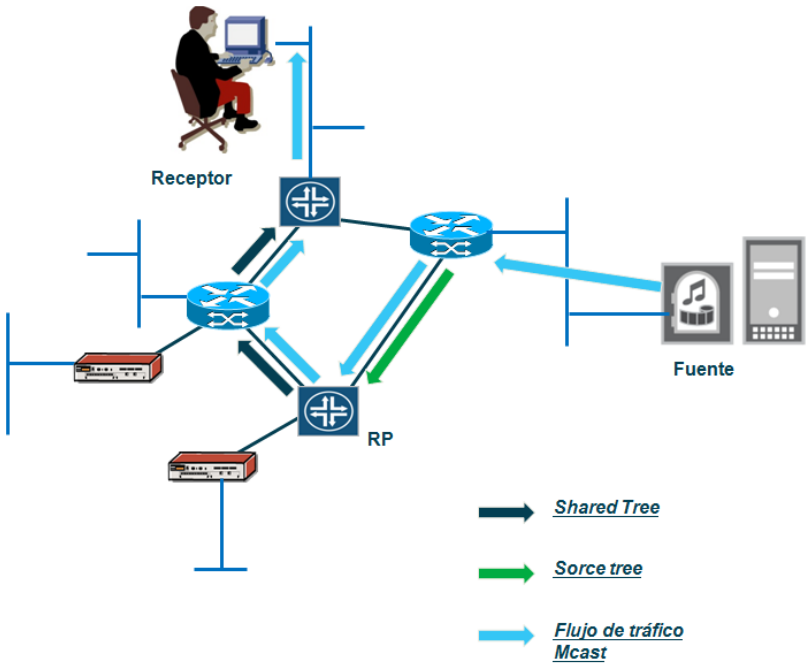

Figura 12. PIM SM - Source Tree desde el RP

- ***Construcción del SPT desde la fuente al receptor:*** Cuando el enrutador de egreso recibe un paquete Multicast, iniciará la construcción de un SPT desde el enrutador de ingreso hasta él. El enrutador de egreso envía un mensaje (S,G) *Join* a su vecino en la tabla RPF y así sucesivamente se irán retransmitiendo los mensajes hasta llegar al enrutador de ingreso [6].

  Como se observa en la Figura 13, una vez construido el SPT, el enrutador de ingreso comienza a enviar los paquetes Multicast directamente desde la fuente al receptor a través del SPT. En este momento el enrutador de egreso

recibe dos copias de cada paquete (uno a través del nuevo SPT y otro a través del RPT desde el RP), entonces el enrutador de egreso debe enviar un mensaje PIM *prune* al RP para que cese el envío de paquetes Multicast a través del RPT.

De esta manera el tráfico es enviado a los receptores sin necesidad de tener que pasar por el RP, optimizándose el camino hacia la fuente.

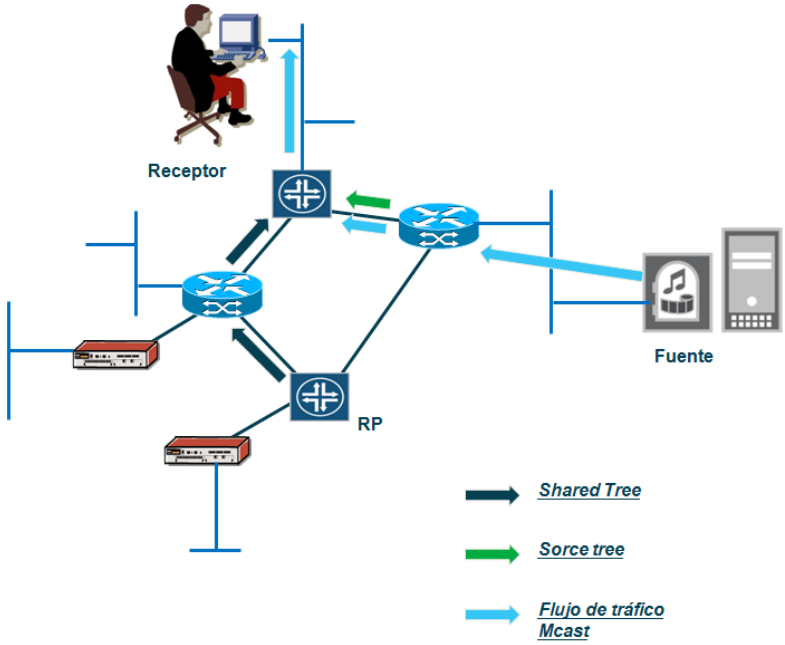

Figura 13. PIM SM - Source Tree desde la fuente

Cuando un receptor ya no está interesado en la recepción de un grupo Multicast, envía un mensaje PIM *prune* al árbol al que está conectado.

De acuerdo con el proceso de establecimiento del árbol de distribución de PIM-SM consume menos recursos de ancho de banda y es más escalable que el PIM-DM por lo que será más conveniente para servicios Multicast.

2.5.3 PIM-BiDir

Este modo está basado en PIM-SM, pero difiere en el método empleado para enviar datos desde la fuente al RP. PIM-BiDir crea un *shared tree* bidireccional donde el tráfico fluye en las dos direcciones en cada rama del árbol.

No existen *source trees* por lo que todas las entradas Multicast están en un (*,G) *shared tree* con lo que se reduce la cantidad de estados que deben ser almacenados por los enrutadores dentro del árbol de distribución, sin embargo el mecanismo RPF ya no puede ser implementado porque el tráfico puede ser recibido también por las interfaces de salida. Para garantizar entonces que no existan bucles en el tráfico Multicast, PIM-BiDir reemplaza el mecanismo RPF por una nueva categoría de enrutadores

denominada conmutador designado o *Designed Forwarder* (DF) que básicamente es el enrutador elegido para conmutar el tráfico proveniente o destinado hacia el RP, ante la posibilidad de que existan varios caminos entre el enrutador de Ingreso/Egreso y el RP [12].

La idea principal es que todo el tráfico Multicast deba ser dirigido al RP, sin embargo, al ser árboles de distribución bidireccionales, si existen receptores entre el camino desde el enrutador de ingreso al RP, el tráfico puede ser recibido a través del *shared tree* sin necesidad de que el tráfico alcance al RP.

2.5.4 PIM-SSM

Dentro de un *Source Specific Multicast* los enrutadores de egreso deben conocer la dirección IP de la fuente del grupo en el que están interesados antes de unirse al árbol de distribución, lo que implica que la dirección IP de la fuente de un grupo es conocida antes de hacer un *Join*. El enrutador de egreso reconoce las fuentes a través de los mensajes *include* de IGMPv3 en dónde el receptor le indica al enrutador de egreso el grupo en el cual está interesado y la fuente de la que quiere recibir ese grupo. Una vez conocida la fuente por parte del enrutador de egreso, este puede enviar un mensaje (S,G) *Join* sin necesidad de *shared trees* ni de RP [13].

SSM tiene reservado el rango de direcciones IP 232.0.0.0/24 que le permite al enrutador de egreso identificarlo como SSM y comienza a construir un SPT hacia el enrutador de ingreso. Al no ser requerido el RP, el enrutamiento es óptimo pues el tráfico fluye por el mejor camino entre la fuente y el receptor.

SSM puede coexistir con redes Multicast basadas en PIM-DM y PIM-SM, pero no con PIM-BiDir. Si un RP recibe un mensaje (*,G) *Join* o *register* de un grupo SSM, este es inmediatamente descartado. Asimismo los mensajes originados por MSDP (Multicast Source Discovery Protocol que será descrito en el apartado 2.6) para indicar las fuentes activas nunca incluyen aquellas pertenecientes al rango SSM.

2.6 Multicast Source Discovery Protocol

En el modelo PIM-SM, las fuentes y receptores de los grupos Multicast deben registrarse en el RP correspondiente, entonces el RP conoce todas las fuentes y receptores para un determinado grupo, sin embargo en escenarios de interconexión de varios dominios Multicast, normalmente en diferentes sistemas autónomos, los RP no tienen forma de conocer las fuentes de otros dominios Multicast. MSDP proporciona un mecanismo para resolver este problema, compartiendo información sobre las fuentes activas (SA) entre los RP de los diferentes dominios [13].

Las vecindades MSDP pueden ser externas (E-MSDP) para el intercambio de fuentes entre enrutadores de distintos dominios (*inter-domain*), o internas (I-MSDP) entre enrutadores pertenecientes a un mismo dominio (*intra-domain*).

Cuando un RP aprende una nueva fuente Multicast de su dominio (a través del mecanismo de registro normal en PIM), el RP encapsula el primer paquete de datos en un mensaje SA y lo envía a todos los vecinos MSDP internos y externos; este proceso continúa a través de los diferentes dominios.

Si un vecino MSDP es un RP y tiene una entrada (*,G) (indicando que hay un receptor interesado), entonces ese RP crea el estado (S,G) conectando al receptor con la fuente a través del camino más corto, los datos son enviados a través de un *source tree*.

En la Figura 14 existe una fuente activa en el dominio A y un receptor (*,G) en el RP del dominio E. Todos los dominios tienen establecidas las vecindades MSDP de manera que el RP del domino E recibe las SA y crea una entrada (S,G).

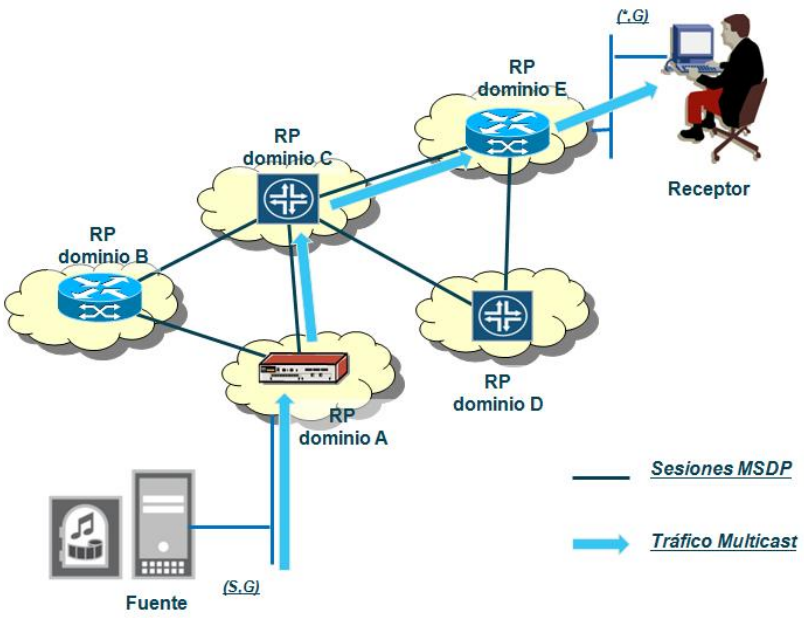

Figura 14. Funcionamiento de MSDP

El tráfico Multicast fluirá de la fuente hasta el receptor a través de los diferentes dominios MSDP, hasta llegar al receptor. Cuando el enrutador de egreso recibe el paquete Multicast, puede conectar con el camino más corto hacia la fuente a través de un *source tree*.

2.6.1 Test RPF

Para establecer una vecindad MSDP se requiere primero que se exista vecindad a nivel BGP, debido a que el mecanismo de test RPF usa el atributo AS-PATH de BGP contenido en las tablas de enrutamiento de Unicast o de Multicast conocidas como U-

RIB y M-RIB respectivamente (*Routing Information Base*). Dos excepciones a esta condición se presentan bien en el caso de existir una sola vecindad, pues no se requiere test RPF al existir solo un camino, o bien al existir grupos de vecindades MSDP denominados Mesh Groups, que serán descritos en el apartado 2.6.2.

El mecanismo de test RPF sobre los mensajes SA en MSDP sigue las siguientes reglas (evaluadas en ese orden):

- ***Si el vecino MSDP no es un vecino BGP:*** Si el primer AS del mejor camino al RP que origina el mensaje SA es el mismo que el del mejor camino al vecino MSDP que envía el mensaje SA, entonces el test tiene éxito. En caso contrario, el test falla.
- ***Si el vecino MSDP es un vecino iBGP:*** Si la dirección IP del vecino MSDP es la misma que el vecino iBGP, entonces el test tiene éxito. En caso contrario, el test falla.
- ***Si el vecino MSDP es un vecino eBGP:*** Si el primer AS del mejor camino al RP que origina el mensaje SA es el mismo que el del vecino iBGP, entonces el test tiene éxito. En caso contrario, el test falla.

Para la búsqueda de los mejores caminos se emplea la tabla M-RIB en primer lugar, y si no se encuentra se usa la tabla U-RIB [13].

No se requiere test RPF:

- Si el vecino MSDP es además el RP de la SA.
- Si el vecino MSDP pertenece al Mesh Group.
- Si el vecino MSDP es el único vecino.

2.6.2 Mesh Groups

Mesh groups son grupos de vecindades MSDP que reducen el flujo de mensajes SA en la red. Cuando un enrutador perteneciente a un *mesh group* recibe un mensaje SA desde un vecino MSDP que también pertenece al grupo, asume que ese mensaje ha sido enviado también a los demás vecinos MSDP del grupo, entonces no es necesario que envíe el mensaje al resto de los vecinos del grupo [14].

Si se emplean *mesh groups* no es necesario implementar BGP para el mecanismo de test RPF sobre los mensajes SA recibidos. Esto es debido a que los mensajes SA nunca se envían a otros vecinos pertenecientes al grupo. Todos los mensajes SA recibidos de vecinos del grupo son aceptados. Sin embargo se requiere que cada enrutador del grupo tenga una vecindad MSDP con el resto de los enrutadores pertenecientes al grupo (full mesh MSDP).

2.7 Multiprotocol Border Gateway Protocol

Multiprotocol BGP contiene extensiones al protocolo BGP para permitir el envío de otros tipos de prefijos aparte de IPv4, manteniendo varias tablas de rutas separadas (RIB). El uso principal de MP-BGP actualmente está en permitir el intercambio de prefijos en entornos MPLS, sin embargo otro de sus usos importantes se encuentra en la implementación de Multicast IP, pues permite mantener la tabla Multicast RIB (M-RIB) dedicada para prefijos Multicast separada de la tabla dedicada para prefijos Unicast (U-RIB) [13].

Vale la pena aclarar que la nueva M-RIB no contiene las direcciones de los grupos Multicast, contiene el mismo tipo de prefijos que la tabla Unicast (U-RIB) con la diferencia que son usados para el test RPF de Multicast.

Para la implementación de MP-BGP se definen dos nuevos atributos que serán intercambiados en los anuncios de BGP para el envío de rutas:

- ***MP_REACH_NLRI:*** Dentro de este atributo las características más importantes son el *Address Family Identifier* (AFI) y el *Sub-Address Family Identifier* (SAFI). Estos dos campos contienen información del tipo de enrutamiento transportado por el campo NLRI (*Network Layer Reachability Information*) que contiene información de las rutas que están siendo advertidas.

  Por ejemplo, las asignaciones de estos campos para el entorno de Multicast IP son:

  - *Address Family Information*:

    Si AFI=1, la *address family* empleada es IPv4.
    Si AFI=2, la *address family* empleada es IPv6.

  - *Sub-Address Family Identifier:*

    Si SAFI=1, NLRI es empleado para enrutamiento Unicast.
    Si SAFI=2, NLRI es empleado para test RPF Multicast.

- ***MP_UNREACH_NLRI:*** Este atributo permite la eliminación de prefijos cuando ya no son alcanzables. Contiene también los campos AFI y SAFI.

El uso de MP-BGP permite diferenciar caminos para tráfico IP Unicast e IP Multicast distribuyendo información de las direcciones IP Multicast. Estas rutas son usadas por PIM para construir los árboles de distribución.

Las vecindades MP-BGP pueden ser externas (E-MP-BGP) para la distribución de rutas entre enrutadores de distintos dominios o sistemas autónomos (inter-AS) o internas (I-MP-BGP) entre enrutadores pertenecientes a un mismo sistema autónomo (intra-AS).

3 Multicast en redes MPLS: Descripción y análisis

Una vez descrita la implementación del servicio Multicast en redes IP, se continuará con la descripción del servicio de Multicast pero ahora en redes BGP/MPLS, para luego dar paso al análisis de las recomendaciones que estandarizan el servicio a nivel del IETF.

3.1 Evolución del servicio VPN Multicast

Una VPN Multicast que en adelante será llamada MVPN, es un servicio VPN IP que soporta la transmisión de paquetes IP Multicast entre diferentes sitios de la red. Los servicios VPN IP están basados en la RFC 4364 que define la implementación de redes privadas virtuales en redes MPLS. Estos servicios han sido ampliamente desplegados por los proveedores de servicio a lo largo del mundo, sin embargo la RFC 4364 no soporta el transporte de paquetes IP Multicast; esta RFC junto a la RFC 4659 únicamente soportan el transporte de tráfico Unicast IP entre los clientes atendidos por el servicio IP VPN [15, 16].

Diferentes soluciones han sido propuestas para extender las capacidades del servicio VPN basado en BGP/MPLS y permitir que soporte el servicio Multicast. La primera de ellas fue desarrollada por Cisco Systems con el draft Rosen, actual RFC 6037. Esta propuesta ganó muchos adeptos dentro del entorno de los fabricantes y proveedores de servicios de telecomunicaciones hasta el punto de convertirse en el estándar de facto para el despliegue de servicios IP Multicast en redes MPLS.

La RFC 6037 plantea una red superpuesta a la infraestructura del servicio VPN IP basado en BGP/MPLS. En ella, la señalización de los estados Multicast del cliente son señalizados de forma separada a las rutas Unicast y adicionalmente el protocolo de encapsulación también es diferente al utilizado para los paquetes Unicast. Más específicamente, el protocolo de señalización del entorno Multicast de cliente es PIM (para el sevicio VPN IP Unicast es MP-BGP) y el tráfico Multicast es encapsulado por el protocolo GRE (*Generic Routing Encapsulation*) mientras que en el entorno Unicast es MPLS [1].

De acuerdo con lo anterior, aunque la RFC 6037 permite que un solo servicio VPN IP soporte tanto tráfico Unicast como Multicast, la adición del servicio Multicast implica el soporte de un nuevo grupo de protocolos en la infraestructura de red del proveedor de servicios [17].

Más recientemente, han surgido las RFC 6513 y 6514 que generalizan el concepto del servicio Multicast en VPN IP, introduciendo nuevas opciones para la señalización y

encapsulación del tráfico Multicast de los clientes del proveedor de servicio. Particularmente estas RFC permiten:

• Usar MP-BGP como un plano de control único para la distribución de rutas del servicio VPN IP Unicast, la distribución de rutas destinadas al autodescubrimiento de enrutadores en entornos VPN IP Multicast y la propia señalización de estados para los árboles de distribución de los clientes (C-Multicast).

• Usar MPLS como un plano de transporte único para la encapsulación de tráfico de las VPN IP tanto Unicast como Multicast en la red del proveedor de servicio.

3.2 Descripción general de una MVPN

Como se indicó en el apartado anterior, el servicio MVPN permite el flujo de datos Multicast entre diferentes sitios de la misma VPN, atravesando la red del proveedor de servicios en túneles de transporte adaptados a la naturaleza punto a multipunto del tráfico Multicast como se observa en la Figura 15.

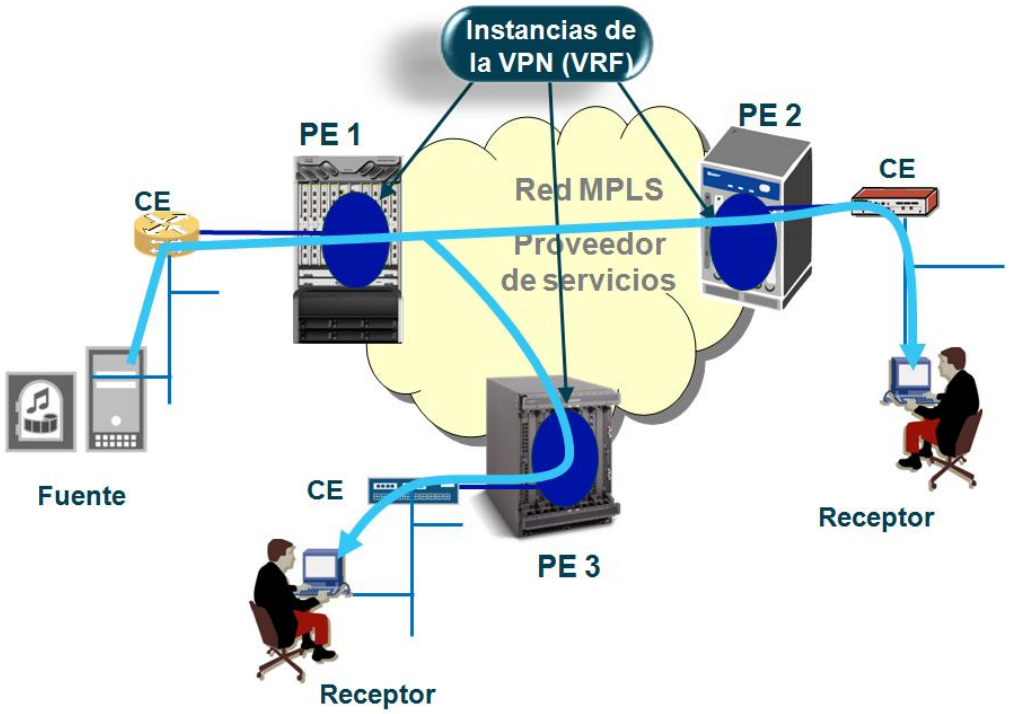

Figura 15. Multicast VPN

Para lograr el establecimiento de estos túneles y permitir el flujo de datos, la red debe desarrollar dos tareas básicas que son: la señalización de los estados Multicast del cliente a través de la red del proveedor (plano de control) y la construcción de los túneles de transporte (plano de transporte). Aunque estas dos tareas están relacionadas, es clave diferenciarlas para comprender el funcionamiento del servicio MVPN.

En el resto del presente documento se utilizan los prefijos C- y P- para diferenciar los contextos de cliente y proveedor respectivamente. Por ejemplo, aplicados a la solución VPN Unicast, en lo que se refiere al plano de control, las rutas C-Unicast son intercambiadas entre los enrutadores de borde de la red MPLS del proveedor (PE-*Provider Edge*) y los equipos de cliente (CE – *Customer Equipment*) usando protocolos de enrutamiento C-Unicast, por otra parte los PE al interior de la red del proveedor de servicios establecen vecindades MP-BGP y a través de ellas intercambian rutas C-Unicast.

Así mismo, en el plano de control de los entornos MVPN, los PE tienen instancias C-PIM habilitadas para establecer adyacencias con los CE y dependiendo del tipo de MVPN, las rutas C-Multicast son intercambiadas entre los PE usando MP-BGP o C-PIM. Mientras que en el plano de transporte, los P-Túneles usados para transportar el tráfico C-Multicast a través de la red del proveedor, normalmente son del tipo punto a multipunto y pueden estar basados en MPLS o en GRE.

En algunos casos, el establecimiento de los túneles puede requerir el establecimiento de una instancia P-PIM en la red del proveedor.

Una vez aclarados estos dos conceptos, a continuación se describe la propuesta de servicio MVPN documentada en las RFC 6513 y 6514.

3.3 Análisis de las RFC 6513 y 6514

Como se ha indicado en la introducción del presente documento, Las RFC 6513 y 6514 son el resultado del trabajo desarrollado por múltiples fabricantes con el objetivo de definir una especificación común para ofrecer el servicio MVPN. Estas especificaciones son bastante extensas y se apoyan tanto en la definición de nuevas funcionalidades como en las ya existentes en los protocolos de comunicaciones definidos por el IETF, para ofrecer varias alternativas de implementación del servicio MVPN[18].

Estas RFC definen una terminología general que es compatible también con la RFC histórica 6037 (draft-rosen). En ella se clasifican los PE en dos grupos, de acuerdo con su función en cada instancia MVPN definida en la red del proveedor:

- ***Grupo de transmisores o PE de ingreso:*** A este grupo pertenecen los PE que pueden enviar tráfico C-Multicast a otros PE a través de los P-Túneles
- ***Grupo de receptores o PE de egreso:*** A este grupo pertenecen los PE que pueden recibir el tráfico C-Multicast de los PE de ingreso a través de los P-Túneles

Un PE puede pertenecer a los dos grupos al mismo, ya que en una misma instancia MVPN se pueden presentar situaciones en las que un PE "X" de la red del proveedor proporcione servicios a una sede del cliente que sea la fuente de un grupo Multicast "A" y al mismo tiempo tenga receptores para otro grupo Multicast "B" para el que la fuente está localizada en otro punto de la red que sea atendido por el PE "Y". En este caso el PE "X" será Ingreso y Egreso para la misma instancia MVPN.

A continuación se describen y analizan los bloques funcionales del servicio MVPN definidos por las RFC 6513 y 6514, y el soporte de estos bloques funcionales por parte de los fabricantes Alcatel-Lucent, Cisco Systems y Juniper Networks con los equipos de referencia SR 7750, ASR 9000 y Series MX 480 respectivamente.

3.4 Plano de control

Como se indicó en el apartado anterior, el plano de control es el encargado de permitir el intercambio de la señalización C-Multicast entre los PE que integran el servicio MVPN. Para cumplir este objetivo, el plano de control debe desempeñar funciones de autodescubrimiento y creación de interfaces virtuales que permitan la transmisión de paquetes C-Multicast. Estas funciones se describen a continuación:

3.4.1 Autodescubrimiento de equipos PE

Descripción

En el escenario IP VPN Unicast no existen mecanismos específicos de autodescubrimiento, un PE conoce los sitios remotos inmediatamente recibe las rutas C-Unicast de otros PE que pertenecen a la misma instancia VPN, mientras que, en el caso de MVPN se requiere que la red identifique los PE de ingreso y de egreso con anticipación al intercambio de rutas y estados C-Multicast.

Autodescubrimiento se refiere entonces al proceso mediante el cual los PE de una instancia MVPN determinada aprenden dinámicamente sobre los otros PE que participan en la instancia MVPN. Esta tarea también puede ser efectuada de forma estática por el administrador de la red del proveedor, sin embargo puede ser inviable en escenarios de gran tamaño.

La principal función del proceso de autodescubrimiento es descubrir la identidad de todos los PE en la MVPN para permitir el establecimiento de las interfaces PMSI (*P-Multicast Service Interface*) que utiliza el PE de ingreso para poner el tráfico C-Multicast dentro del P-Túnel. Dentro de esta función se pueden distinguir tres objetivos fundamentales que son:

- Descubrimiento del grupo de PE de egreso para la MVPN determinada.

- Descubrimiento de los PE que cumplen funciones de interconexión con otros sistemas autónomos (ASBR - *Autonomous System Border Router*) en donde existen PE interesados en participar en la MVPN.
- Descubrimiento del grupo de PE de ingreso para la MVPN determinada.
- Descubrimiento de las asociaciones entre los flujos C-Multicast y las interfaces PMSI.

Este proceso de autodescubrimiento se puede lograr a través de dos opciones, usando MP-BGP o usando PIM. Con el autodescubrimiento basado en MP-BGP las RFC 6513 y 6514 introducen una nueva NLRI denominada MCAST-VPN con SAFI 5. Esta NLRI incluye un grupo de rutas que cubren las funcionalidades del plano de control del servicio MVPN, entre ellas el autodescubrimiento. Apoyado en esta nueva NLRI, cada PE de la MVPN advierte rutas especiales de auto-descubrimiento (A-D) a sus vecinos MP-BGP aprovechando las extensiones que ofrece el protocolo.

Específicamente, para realizar las funciones de autodescubrimiento, la NLRI MCAST-VPN tiene designadas 5 tipos de rutas que son:

- Tipo 1 o Intra-AS I-PMSI A-D. Son originadas por todos los enrutadores PE y son utilizadas para advertir y aprender información sobre los miembros de la MVPN que pertenecen al mismo sistema autónomo (Intra-AS).
- Tipo 2 o Inter-AS I-PMSI A-D. Son rutas originadas por los enrutadores de borde del sistema autónomo (ASBR) y son utilizadas para advertir y aprender información relacionada con los miembros de la MVPN que pertenecen a diferentes sistemas autónomos.
- Tipo 3 S-PMSI A-D. Son rutas originadas por los PE de ingreso y son utilizadas para iniciar los P-Túneles selectivos para una (C-S, C-G) determinado.
- Tipo 4 o Leaf A-D. Son rutas originadas por los PE de egreso en respuesta a las rutas tipo 3 y son utilizadas para indicar el interés en un flujo Multicast (C-S, C-G) determinado.
- Tipo 5 o Source Active A-D. Estas rutas son funcionalmente equivalentes a los C-Register de IGMP pero intercambiados entre los PE del proveedor, y el objetivo identificar los PE de ingreso o en otras palabras los PE que ofrecen cobertura a las fuentes.

Por otra parte, en el autodescubrimiento basado en PIM, cada uno de los PE que hacen parte de la MVPN es configurado con la dirección del grupo P-Multicast asociado a la MVPN, que le permite unirse a la interfaz PMSI y así enviar un paquete *Hello* de PIM a los demás PE de la MVPN, de tal forma que todos los PE se identifican mutuamente. El proceso de autodescubrimiento de PIM únicamente funciona sobre

interfaces MI-PMSI (*Multidirectional Inclusive PMSI*)[17]. Estas interfaces serán explicadas en el apartado 3.4.2.

Como se indicó anteriormente, el proceso de autodescubrimiento también incluye el aprendizaje de la asociación del flujo C-Multicast con su respectiva PMSI. Cuando es utilizado el proceso de autodescubrimiento basado en MP-BGP, esta función es lograda a través del anuncio de rutas de la NLRI MCAST-VPN donde existen campos específicos para esta asociación. Mientras que en el proceso de autodescubrimiento basado en PIM y en el caso de interfaces S-PMSI, es necesario utilizar un mensaje de UDP en el cuál se indica el grupo C-Multicast y la interfaz S-PMSI asociada.

Análisis

Revisando de forma detallada el proceso de autodescubrimiento se pueden destacar los siguientes aspectos relevantes al momento de decidir cuál es la mejor opción a ser implementada por el proveedor de servicios.

Como primer aspecto importante se observa el hecho de que el proceso de autodescubrimiento a través de MP-BGP es soportado en las dos opciones de plano de control (PIM y MP-BGP) mientras que el autodescubrimiento basado en los mensajes de control C-PIM no es soportado en el plano de control basado en MP-BGP.

Así mismo, se observa que el autodescubrimiento basado en MP-BGP funciona de forma similar a como lo hace actualmente el servicio VPN Unicast y no tiene restricciones respecto al tipo de P-Túneles que es utilizado en la red, mientras que el autodescubrimiento basado en los mensajes de control de P-PIM requiere que en la red se implementen P-Túneles que permitan simular un entorno LAN, de tal forma que exista un establecimiento de vecindades entre los diferentes PE, esto también excluye los túneles PIM-SSM pues para establecerlos se requiere que previamente se haya "descubierto" la fuente del túnel.

En síntesis, se observa que el uso de MP-BGP para autodescubrimiento además de abarcar los escenarios cubiertos por el autodescubrimiento basado en PIM, también ofrece un mayor nivel de seguridad al garantizar que los PE descubiertos pertenecen a la MVPN adecuada, pues es una información incluida en las rutas MP-BGP, mientras que los mensajes de control de PIM no incluyen esta información.

Soporte de los fabricantes

En cuanto al soporte de los tres fabricantes analizados, todos soportan el método de autodescubrimiento basado en MP-BGP [19-21], mientras que en el caso del autodescubrimiento basado en PIM, algunos no confirman su soporte explícitamente dentro del entorno de las RFC 6513 y 6514, sin embargo, al ser una funcionalidad basada en las características naturales del protocolo PIM, se puede asumir que el

fabricante que indique el soporte del plano de control basado en C-PIM en el entorno de las RFC 6513 y 6514 también soporta el autodescubrimiento basado en C-PIM. A esto se suma que existen algunas combinaciones de autodescubrimiento C-PIM con la señalización de los estados del entorno de C-Multicast entre los PE del proveedor que pueden ser ineficientes, como es el caso del autodescubrimiento basado en P-PIM combinado con la señalización de los estados de C-PIM basada en MP-BGP. Por lo anterior se puede deducir que si un fabricante sólo soporta la señalización de C-Multicast basada en MP-BGP dentro del entorno de las RFC 6513 y 6514, no debería soportar autodescubrimiento basado en PIM.

Siguiendo esta metodología de análisis, en el caso de Alcatel-Lucent que explícitamente indica que sólo soporta el plano de control basado en MP-BGP para MVPN basadas en la RFC 6513 y 6514 [19] se puede deducir que no soporta el autodescubrimiento basado en PIM. Así mismo podría ser el caso de Juniper que a pesar de no indicarlo explícitamente, en la documentación disponible [18, 21-23], no desarrollan implementaciones del plano de control basado en PIM, de hecho siempre se refieren a la RFC 6513 y 6514 como la nueva generación de MVPN (NG-MVPN) con plano de control basado en MP-BGP.

Por el contrario, Cisco indica que soporta el plano de control basado en PIM en el entorno de la RFC6513 por lo que implícitamente soporta el autodescubrimiento basado en PIM [20, 24].

3.4.2 Construcción de los árboles de distribución

Descripción

Los árboles de distribución se crean a partir de interfaces virtuales denominadas PMSI (P-Multicast Service Interface) que utiliza el PE de ingreso para poner el tráfico C-Multicast dentro del P-Túnel. El P-Túnel transporta el tráfico PE de egreso y es posible identificarlo como un árbol, donde el PE de ingreso es la raíz y los PE de egreso son los extremos de las ramas. Aunque los P-túneles son normalmente punto a multipunto (P2MP), también existen de naturaleza punto a punto o multipunto a multipunto, lo que permite que una interfaz PMSI pueda estar asociada a un grupo de P-Túneles, por ejemplo, si el proveedor de servicios sólo soporta túneles punto a punto (P2P), una interfaz PMSI deberá estar asociada a un conjunto de P-Túneles P2P, si por el contrario el proveedor de servicio sólo soporta túneles P2MP y se desea instanciar una interfaz PMSI multidireccional esta deberá ser asociada a un grupo de P-Túneles P2MP.

Cada PE de ingreso es la raíz de al menos un P-Túnel, lo que significa que cada uno de los PE de ingreso requiere al menos una interfaz virtual PMSI en la instancia MVPN

para poder enviar tráfico C-Multicast a los PE de egreso. Existen dos tipos de interfaces PMSI, las inclusivas denominadas I-PMSI y las selectivas denominadas S-PMSI, como se observa en la Figura 16. Un PE de ingreso puede tener hasta una I-PMSI y un número ilimitado de S-PMSI en una instancia MVPN determinada[18].

Así mismo, las interfaces I-PMSI pueden ser multidireccionales (MI-PMSI) si permiten el flujo de tráfico en los dos sentidos o unidireccionales (UI-PMSI) si permiten el flujo de tráfico únicamente en el sentido PE de ingreso hacia PE de egreso. Las interfaces virtuales del tipo MI-PMSI pueden ser instanciadas a través de un solo túnel MP2MP, o mallados totales de túneles P2MP o P2P.

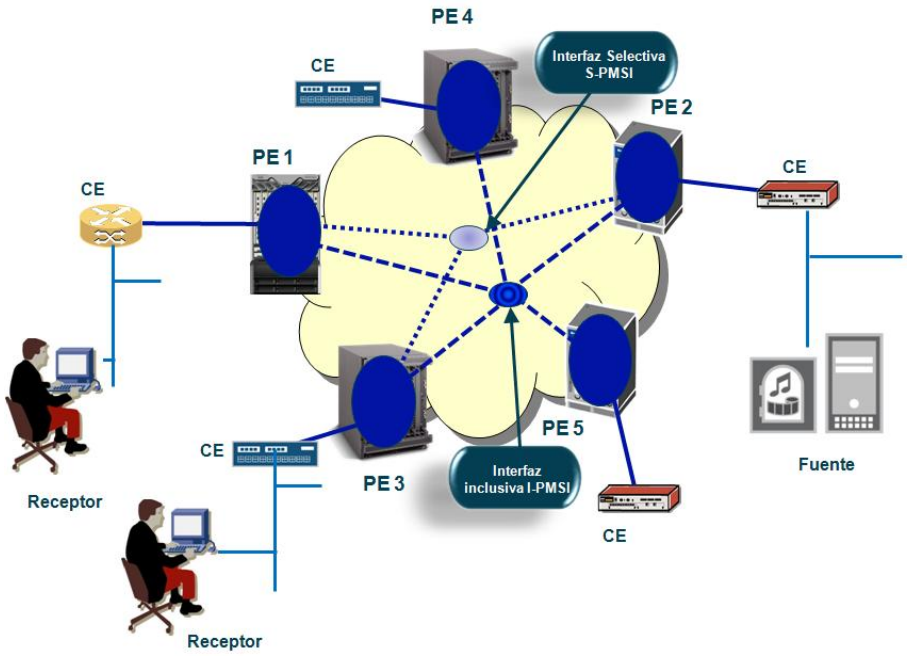

Figura 16. Árboles de distribución

Cuando un PE de ingreso transmite un paquete C-Multicast (C-S, C-G) a través del P-Túnel utiliza por defecto la interfaz I-PMSI, que transporta el paquete a todos los PE de egreso de la instancia MVPN. Por su parte, el PE de egreso envía el tráfico únicamente a los CE que tenga conectados y que al mismo tiempo hayan expresado su interés en recibir dicho tráfico a través de la señalización de estados (C-S, C-G) o (*, C-G) bien a través de mensajes *Join* de instancias C-PIM o a través de mensajes report de IGMP. Si un PE de egreso no tiene CE interesados en el flujo Multicast, descarta el paquete.

Los P-Túneles que transportan los paquetes Multicast enviados por las interfaces I-PMSI se crean a partir de la información transmitida en las rutas Tipo 1 y Tipo 2 intercambiadas en el proceso de autodescubrimiento, específicamente en los parámetros del tipo de túnel de la ruta, que dependiendo de su existencia, los PE participantes en la MVPN detectan si el PE que origina la ruta es un enrutador de

ingreso o de egreso. Si es un PE de ingreso, el atributo túnel está presente en la ruta e indica los parámetros necesarios para establecer el túnel de acuerdo con la tecnología escogida en la red. Dichos parámetros pueden ser:

- Si el túnel es un LSP P2MP basado en RSVP-TE, la ruta deberá transportar los campos Extended Tunnel ID, Reserved, Tunnel ID y P2MP ID tal y como son identificados en la RFC4875 [25].
- En el caso de que el túnel sea un LSP P2MP basado en mLDP, la ruta deberá transportar el identificador de tráfico que debe ser encapsulado o Forwarding Equivalence Class (FEC) como se describe en la [26].
- Cuando el túnel es creado a partir de un árbol de distribución establecido a través de PIM-SM, PIM-SSM o PIM BiDir, la ruta debe indicar la dirección IP del transmisor o PE de ingreso y la dirección IP del grupo P-Multicast.

Estos métodos de comunicación aplican tanto a interfaces MI-PMSI como a UI-PMSI.

Por otra parte, el árbol inclusivo puede resultar en gasto innecesario de recursos de ancho de banda en la red, especialmente en entornos donde los flujos C-Multicast tengan altos requerimientos a nivel de ancho de banda y adicionalmente pocos C-Receptores interesados en recibirlos. Flujos específicos (C-S, C-G) o (*, C-G) pueden ser opcionalmente asociados a interfaces S-PMSI. Los árboles selectivos conectan a los PE de ingreso únicamente con los PE de egreso que tengan CE interesados en el flujo C-Multicast.

En este caso, los P-Túneles que transportan los paquetes C-Multicast enviados por las interfaces S-PMSI se pueden establecer a partir de dos métodos:

- A través de la ruta tipo 3 del proceso de autodescubrimiento basado en MP-BGP en la que el PE de ingreso anuncia que un grupo C-Multicast específico va a ser asociado a una interfaz S-PMSI donde su tráfico sólo requerirá ser enviado a los PE de la MVPN con receptores interesados. A esta ruta tipo 3, los PE de la MVPN que tengan receptores interesados en el grupo anunciado, responderán con una ruta tipo 4 en la que se indicará el interés de ser un PE de egreso. A partir de este punto los PE de ingreso y egreso se identifican y se crea el túnel como se indicó previamente para el caso de las interfaces I-PMSI.
- El segundo método se aplica al plano de control basado en PIM y consiste en la transmisión de un mensaje de control sobre el túnel MI-PMSI que contiene el grupo y la fuente del cliente que quiere ser asociada a la interfaz S-PMSI. Este mensaje es transmitido en un paquete UDP dirigido a la dirección de

grupo IP Multicast ALL-PIM-ROUTERS (224.0.0.13), con el puerto UDP 3232, una vez los PE interesados reciben este mensaje, envían el *PIM Join* (*,G) del grupo que ha sido asociado a la interfaz S-PMSI.

Análisis

En el caso de la señalización PIM es indispensable que existan interfaces MI-PMSI para garantizar la vecindad entre los PE y el intercambio de estados señalización C-PIM. Mientras que en el caso de señalización MP-BGP la solución puede ser soportada a través de interfaces del tipo S-PMSI también. Está en proceso el *draft-rosen-l3vpn-mvpn-mspmsi-10.txt* que permite habilitar la señalización PIM sobre una nueva clase de interfaces virtuales multidireccionales selectivas o MS-PMSI, que evitarían el establecimiento de interfaces MI-PMSI únicamente para mantener las vecindades C-PIM, sin embargo no son soportados en el entorno de las RFC 6513 y 6514 [27].

Así mismo, la RFC 6513 indica que en el caso de ser implementada la señalización basada en PIM y la interfaz MI-PMSI utilice un solo túnel por MVPN, este se puede configurar de forma estática, sin embargo, recomienda que en todos los casos la instanciación de la interfaz se haga a través del autodescubrimiento.

En cuanto al establecimiento de los túneles asociados a las interfaces S-PMSI, el método basado en los mensajes de control a través de UDP sólo está planteado para túneles basados en PIM y únicamente en casos en los que existan interfaces MI-PMSI, mientras que la creación de las interfaces S-PMSI basada en MP-BGP está soportada por todas las tecnologías de túneles planteadas, así como para todas las interfaces I-PMSI (tanto multidireccionales como unidireccionales).

El método basado en MP-BGP cubre todos los escenarios en los que aplica el método basado en UDP, sin embargo, el método basado en UDP ha sido incluido en las RFC 6513 y 6514 por razones de compatibilidad con la RFC 6037 (draft-rosen), para permitir así la convivencia de todos los escenarios ya desplegados en el entorno de las telecomunicaciones con las nuevas propuestas planteadas en las RFC 6513 y 6514.

Soporte de los fabricantes

Sin tener en cuenta los tipos de túneles soportados que serán analizados con mayor detalle en el apartado 3.5.2, en cuanto a la creación de las interfaces MI-PMSI, los tres fabricantes analizados soportan la identificación de los túneles a través de las rutas tipo 1 [18-20]. Así mismo ocurre con la identificación de los P-Túneles asociados a las interfaces S-PMSI a partir de las rutas tipo 3 y 4, donde los tres fabricantes indican su soporte.

Por otra parte, mientras que en el caso de la identificación basada en UDP de los P-Túneles para las interfaces S-PMSI es soportada por todos los fabricantes en el entorno

de la RFC 6037, en el entorno definido por las RFC 6513 y 6514 ni Alcatel-Lucent ni Juniper soportan la señalización de rutas C-Multicast a través de un plano de control basado en C-PIM razón por la cual tampoco soportan la asociación de P-Túneles a interfaces S-PMSI basada en UDP en el entorno de las RFC 6513 y 6514.

En el caso de Cisco, aunque indica que soporta el plano de control basado en C-PIM, en la documentación disponible no se especifica si se soporta el método basado en UDP.

3.4.3 Agregación

Descripción

Por defecto existe una asociación uno a uno entre las interfaces PMSI y los P-Túneles y a su vez, una interfaz PMSI está dedicada a una instancia MVPN. Juntando estos dos factores, por defecto un P-Túnel solo transporta tráfico de una instancia MVPN,

Entendiendo un estado como el registro que tiene un enrutador del encaminamiento que debe seguir un determinado grupo Multicast, cada interfaz virtual PMSI generará un estado por cada P-Túnel que tenga asociado, en cada uno de los PE y P del proveedor de servicio que conformen el árbol de distribución, por ejemplo en el caso de una interfaz virtual del tipo MI-PMSI asociada a un P-Túnel bidireccional (PIM-BIDIR o MP2MP LDP) requerirá de un estado por cada instancia MVPN en cada PE y P que haga parte del árbol de distribución, mientras que si la interfaz virtual MI-PMSI utiliza varios túneles P2MP o P2P, el número de estados en cada PE y P aumentará dependiendo del número de P-Túneles. Esto ocurre por cada MVPN que sea habilitada en la red del proveedor de servicios, lo que en un entorno de proveedor de servicios puede ocasionar efectos negativos en el consumo de recursos de los enrutadores.

Para aliviar esta problemática, las RFC 6513 y 6514 definen una metodología opcional a través de la agregación de túneles que tengan un alto grado de congruencia, de tal forma que el número de estados en la red corresponda a uno por grupo de P-Túneles y no a uno por cada P-Túnel. El término congruencia indica el grado de coincidencia de PE de ingreso y de egreso entre diferentes MVPN. Dos MVPN con los mismos PE de ingreso y de egreso tendrán el máximo grado de congruencia, que irá disminuyendo en la medida en que los PE sean diferentes.

Los P-Túneles basados en MPLS (LDP y RSVP) que se quieran agrupar en un P-Túnel, deberán ser identificados con una etiqueta MPLS intermedia que le permita al PE de destino asociarla a la instancia MVPN adecuada. Esta información de identificador será anunciado en el intercambio de rutas tipo 1 (Intra-AS I-PMSI A-D) en el atributo PMSI Tunnel.

Análisis

Uno de los inconvenientes que tiene esta metodología propuesta es que si el proveedor de servicios decide agrupar P-Túneles que no sean totalmente congruentes, existirán PE de egreso que recibirán tráfico Multicast que no corresponde a alguna de sus instancias MVPN, con lo que se sacrifica ancho de banda en la red para disminuir el número de estados que deben mantener los enrutadores.

Por otra parte la RFC 6513 indica que en el caso de P-Túneles basados en IP (PIM) se puede utilizar cualquier tipo de información encapsulada dentro del formato IP del P-Túnel agregador para identificar los P-túneles agregados, sin embargo deja esta opción sin especificar, esto permitirá que cada fabricante que desee implementarla lo haga utilizando configuraciones propietarias, sin garantizar interoperabilidad con otros fabricantes. Esto causará que en redes multi-fabricante, la funcionalidad de agregación de P-Túneles no se pueda implementar.

Soporte de los fabricantes

De acuerdo con la documentación disponible, Juniper no soporta agregación de P-Túneles [21]

Alcatel-Lucent indica en el documento "*Next-generation Layer 3 Multicast VPN (MVPN) Services*"[17] que planea soportar la agregación de P-Túneles, sin embargo en su documentación de implementación actual no lo especifican [19], por lo que no es posible confirmarlo.

Una situación similar ocurre con Cisco, pues en la documentación de referencia consultada no se menciona esta funcionalidad, por lo que no se puede confirmar su implementación.

3.4.4 Distribución de Señalización C-Multicast

En el proceso de distribución de señalización C-Multicast se pueden diferenciar dos tipos de intercambios, el que se presenta entre el PE y el CE, y el que se presenta entre los PE de la MVPN. Estos escenarios se describen a continuación:

Intercambio de señalización C-Multicast entre el PE y el CE

Un PE con una instancia MVPN debe aprender sobre las redes y los receptores que se encuentran distribuidas en la red del cliente. Normalmente a través de los protocolos IGMP o PIM, el CE informa al PE que desea recibir un flujo Multicast particular debido a que tiene receptores interesados en él. El uso de PIM como protocolo de enrutamiento Multicast entre el PE y el CE requiere que el PE conozca las redes que puede alcanzar a través del CE y así seleccionar adecuadamente el camino para enviar los mensajes *Join/Prune* de PIM. Estos mensajes normalmente siguen el camino inverso Unicast hacia las fuentes y establecen los estados requeridos para

transmitir el tráfico Multicast en los enrutadores PE y CE habilitados con el protocolo PIM. El acceso a las redes que se encuentran en las sedes del cliente se pude dar de forma dinámica a través de protocolos de enrutamiento como OSPF, RIP o BGP, o de forma estática. Cuando se utilizan rutas estáticas o MP-BGP, entre el PE y el CE se pueden intercambiar rutas que son utilizadas para realizar el test RPF únicamente, tal y como se explicó en el apartado 2.7, sin embargo, en la red del proveedor de servicios debe usarse otra NLRI que permita diferenciar las tablas de rutas Multicast por cada instancia MVPN, con este objetivo se define la SAFI 129 y básicamente permite la traslación de las rutas recibidas en el entorno de cliente con las SAFI 2 a rutas en el entorno MVPN del mismo cliente con la SAFI 129.

Intercambio de señalización C-Multicast entre los PE

Cuando el PE recibe un requerimiento para recibir un flujo Multicast desde un CE directamente conectado a una instancia MVPN particular, este debe enviar el requerimiento al PE de ingreso. Para permitir que el PE que recibe la solicitud pueda conocer el camino hacia el PE de ingreso, previamente debieron haber intercambiado rutas VPN IP Unicast entre sí a través de MP-BGP. Las rutas VPN IP intercambiadas para tal fin pueden transportar información adicional a la que se transporta en el intercambio normal de rutas VPN IP en el entorno Unicast.

La señalización de los mensajes de *Join/prune* desde un PE de egreso hacia el PE de ingreso del respectivo flujo Multicast, es llamada señalización C-Multicast y de forma similar a lo que ocurre en el proceso de autodescubrimiento, las RFC 6513 y 6514 permiten el uso de PIM o MP-BGP para habilitar este intercambio de señalización.

Cuando se utiliza PIM para la señalización C-Multicast entre los PE, las RFC 6513 y 6514 plantean 3 modelos de implementación:

- Mallado total de vecindades entre los PE que conforman la MVPN a través de interfaces MI-PMSI.
- Una variante del mallado total de vecindades entre los PE modificando el comportamiento estándar de PIM para eliminar la transmisión de los mensajes *Hello*, que dentro del contexto LAN permiten a los enrutadores con PIM habilitado, identificar a sus vecinos, pero que en el contexto de MVPN pueden ser sustituidos por el autodescubrimiento basado en MP-BGP.
- Una tercera opción es la de implementar el envío de mensajes *Join/Prune* de forma Unicast al PE que sea la raíz del árbol de distribución, ya no serían transmitidos sobre la interfaz PMSI y por consiguiente no serán recibidos por los demás integrantes de la instancia MVPN.

En cualquiera de las tres opciones es necesario mantener vecindades P-PIM adicionales entre los PE y sus vecinos IGP (pueden ser P o PE), que son diferentes a las vecindades C-PIM establecidas a través de las interfaces virtuales MI-PMSI existentes únicamente entre los PE de la MVPN.

En primer escenario planteado (mallado total de vecindades C-PIM entre PE) existe una instancia C-PIM por cada PE que integra la instancia MVPN y a su vez dentro de cada MVPN todos los PE establecen vecindades C-PIM entre sí. Estas vecindades son formadas por el intercambio directo de mensajes PIM entre las instancias C-PIM, es necesario aclarar que estos mensajes son transparentes para los enrutadores P del proveedor. Típicamente los mensajes C-PIM son transmitidos junto a los paquetes Multicast en los P-Túneles de la interfaz MI-PMSI que simula un segmento LAN para las instancias C-PIM.

Por otra parte en el escenario MP-BGP, todos los mensajes de control provenientes de los CE, son traducidos a rutas tipo 5,6 o 7 de acuerdo con el mensaje de control recibido. La ruta tipo 5 fue descrita en el apartado 3.4.1 y las rutas tipo 6 y 7 se describen a continuación:

- Tipo 6 o Shared Tree Join. Son originadas por los PE de egreso cuando reciben un mensaje *C-PIM Join* del tipo (C-*,C-G) desde uno de los CE que tiene conectados.
- Tipo 7 o Source Tree Join. Son originados por los PE de egreso en dos situaciones, bien cuando reciben un mensaje *C-PIM Join* del tipo (C-S,C-G) desde uno de los CE que tiene conectados o bien cuando reciben una ruta tipo 5 desde el PE de ingreso.

Análisis

Debido a la relevancia de la señalización de rutas C-Multicast, su análisis se ha dividido en los aspectos más importantes que abarca y que se describen a continuación.

Escalabilidad en los PE

Para el caso del plano de control basado en PIM, las RFC 6513 y 6514 plantea tres modelos de implementación para el intercambio de señalización y de estados de enrutamiento del servicio Multicast de los clientes, sin embargo, sólo explica en detalle la opción de mallado total de vecindades PIM manteniendo los paquetes *Hello*, mientras que los otros dos escenarios, al no especificar su implementación, tácitamente deja a los fabricantes la elección de adoptarlas y el proceso para ponerlas en funcionamiento con lo que es difícil garantizar su interoperabilidad en infraestructuras de red multi-fabricante.

Así mismo, debido a su naturaleza no orientada a conexión, en el escenario de mallado total de vecindades, C-PIM requiere que los PE intercambien mensajes periódicos de *Hello* y *C-Join/Prune* a través de la interfaz MI-PMSI, lo que puede afectar la capacidad de procesamiento de los PE cuando los puntos de cobertura de la MVPN aumenten en cantidad y distribución geográfica. Para solucionar este inconveniente, se ha creado la RFC 6559 que describe la implementación de PIM a través de protocolos orientados a conexión como SCTP o TCP, sin embargo esta implementación no se contempla dentro del entorno de las RFC 6513 y 6514 [28].

También en los escenarios de mallado total de vecindades C-PIM, tal y como ocurre en implementaciones de PIM sobre entornos LAN, se debe implementar el mecanismo de *Join suppression*, que disminuye la carga del PE ingreso al evitar que deba procesar mensajes *C-PIM Join/Prune* por cada PE que haga parte de la MVPN sin embargo, esta funcionalidad requiere que todos los PE de la MVPN procesen los mensajes de *PIM Join/Prune* enviados por los demás PE de la MVPN, sin importar si son los PE de ingreso para el correspondiente grupo.

Por otra parte, el transporte de señalización y enrutamiento de Multicast de los clientes basado en MP-BGP también requiere que todos los PE de la MVPN procesen todas las rutas que son dirigidas a los PE de ingreso. Por esta razón las RFC 6513 y 6514 recomienda el uso de las comunidades extendidas de MP-BGP llamadas "route target" para diferenciar entre PE con fuentes asociadas y PE con receptores asociados, de tal forma que se disminuya el procesamiento innecesario de rutas en los PE, pues los PE con receptores asociados no procesarán las rutas dirigidas a los PE con fuentes asociadas, sin embargo todos los PE con fuentes recibirán las rutas, aunque no sean dirigidas a algunos de ellos.

Adicionalmente, gracias a ser un protocolo orientado a conexión, el plano de control basado en MP-BGP disminuye la carga de procesamiento de mensajes, eliminando la necesidad de enviar mensajes periódicos que permitan mantener los árboles de distribución, mejorando su escalabilidad con respecto a la ofrecida por el plano de control basado en PIM. Sin embargo, sus ventajas se dan a costa de que el PE de ingreso mantenga un número de estados directamente proporcional con el número de PE de egreso que hicieron *Join* a un determinado grupo C-Multicast. Este inconveniente se puede ver disminuido en la medida en que se implementen varios reflectores de rutas (RR) en la red sobre los que puedan distribuirse estos estados.

En cuanto al despliegue de RR para el servicio MVPN, puede darse la situación en la que el proveedor de servicios ya cuente con reflectores para soportar el servicio Unicast, con lo que en una red de gran tamaño los RR pueden presentar problemas de carga de procesamiento. Por este motivo es conveniente que se planteen opciones de

diseño de red en las que se separan los RR habilitados para el servicio Unicast y el servicio Multicast, esto incrementará el coste de la solución así como la complejidad, pero reduce el riesgo de fallos en red por sobrecarga de procesamiento.

Escalabilidad en los enrutadores P

Los enrutadores P se ven afectados por la cantidad de P-Túneles que requiera la MVPN, pues cada P-Túnel se ve representado en un estado dentro de la tabla de enrutamiento de los P que le den transporte. De acuerdo a esto se realizará un análisis del número de P-Túneles requeridos por cada plano de control.

Como se ha indicado anteriormente, el plano de control basado en PIM está restringido al uso de una interfaz MI-PMSI que permita interconectar todos los PE que hacen parte de la MVPN. Esto implica el despliegue de uno de los siguientes escenarios:

- El uso de una técnica de establecimiento de P-Túneles en el proveedor como PIM-SM-ASM o MP2MP.
- El uso de al menos un P-Túnel (P2MP o P2P) por PE por instancia MVPN, aun cuando no tenga fuentes conectada directamente en los sitios del cliente a los que ofrece servicio (estas fuentes se asocian al servicio de señalización del plano de control de la propia MVPN más que a las fuentes del servicio en sí) [29]. El draft MS-PMSI pretende dar una solución a este problema para que no sea necesario mantener un túnel MI-PMSI únicamente para señalización, sin embargo su uso no está soportado en las RFC 6513 y 6514 [27].

Por el contrario, debido a que la señalización del plano de control basado en MP-BGP no debe ser transportada por los P-Túneles, este no impone restricciones sobre el tipo de P-Túnel y en el caso de que se utilicen túneles P2MP sólo requiere el uso de un P-túnel por MVPN por PE de ingreso.

En conclusión, en situaciones donde sean pocos PE de ingreso, comparado con el número total de PE que integran la MVPN, el plano de control basado en MP-BGP mejora la cantidad de estados que deben ser mantenidos por los enrutadores P comparada con la cantidad de estados que deben ser mantenidos en un escenario MI-PMSI con túneles P2MP (P-Túneles).

Seguridad y mecanismos de protección

A nivel de protección de la información, las sesiones establecidas a través de MP-BGP soportan el método de autenticación MD5 de los extremos mientras que PIM permite el establecimiento de vecindades a través de IPSec como lo describe la RFC 5796 [30]. Los dos escenarios pueden ser necesarios en entornos donde existan

interconexiones Inter-AS o en entornos donde parte de la infraestructura sea soportada por otro proveedor diferente al proveedor que ofrece el servicio al cliente final.

Por otra parte a nivel de protección de la infraestructura, la capacidad de los recursos asignados a la conectividad Unicast es la clave, pues las funciones de enrutamiento de C-Multicast, especialmente en entornos de alta consumo, competirán por los recursos de la red con las funciones de enrutamiento a nivel VPN Unicast. Con el plano de control basado en PIM, las funciones de enrutamiento Unicast y Multicast solo competirán por los recursos de procesamiento en el entorno de los propios PE. Mientras que en el caso de MP-BGP las funciones de enrutamiento Unicast y Multicast competirán tanto en el PE como en los reflectores de rutas. En los dos casos son necesarios mecanismos para arbitrar el uso de recursos. En el caso de PIM esta arbitración debe ocurrir entre diferentes procesos de enrutamiento en el PE, el proceso Multicast para PIM y el proceso de Unicast para MP-BGP. En el caso de MP-BGP, el arbitramiento debe ocurrir dentro del mismo proceso, pues tanto Multicast como Unicast comparten el mismo proceso MP-BGP.

Así mismo, en el plano de control basado en MP-BGP, debido a que el proceso de enrutamiento C-Multicast es dinámico por naturaleza y a que dentro de la VPN refleja los eventos de enrutamiento generados por el cliente, los PE de la red del proveedor deben tener mecanismos de protección del plano de control, sobre todo teniendo en cuenta la importancia del proceso BGP, pues cómo se indicó anteriormente, es el encargado del enrutamiento Unicast del servicio de VPN, y la inestabilidad de las rutas Multicast puede afectar su funcionamiento. Dentro de los mecanismos de protección del plano de control se debe contemplar el retraso controlado de anuncios intermitentes y la limitación del número de rutas a nivel de MP-BGP que pueden ser almacenadas en el PE.

Retardo de los Join de C-Multicast

Gracias a que el plano de control basado en PIM simula un entorno LAN entre los PE que pertenecen a la misma MVPN, sólo hay un salto a nivel de C-PIM entre los PE de egreso y los PE de ingreso, por consiguiente el retardo percibido por los clientes al generar un *Join* es mínimo, sin embargo en condiciones de congestión o degradación de la red, el retardo se puede ver aumentado debido a que en situaciones de pérdida de mensajes de *Join*, estos se podrán recuperar únicamente después del periodo de refresco que normalmente es de 60 segundos.

Por otra parte el plano de control basado en MP-BGP utiliza el intercambio de mensajes TCP lo que introduce un retardo adicional en la traslación a rutas MP-BGP de los *C-PIM Join* generados por los clientes. Este retardo, en condiciones de funcionamiento óptimo de la red, es mayor que el presentado en el plano de control

basado en PIM, sin embargo en condiciones de degradación, los mecanismos de control de congestión de TCP, hacen que el aumento de los retardos de los *C-PIM Join* sea progresivo y pueda controlarse evitando que se llegue a alcanzar el tiempo de refresco.

Soporte de los fabricantes

Como se ha indicado en los anteriores apartados, los tres fabricantes analizados soportan el plano de control basado en MP-BGP, sin embargo, sólo Cisco soporta el plano de control basado en PIM en el entornos de las RFC 6513 y 6514. Adicionalmente, Cisco es el principal impulsor de los draft y RFC enfocados a evolucionar el plano de control basado en PIM. Algunos ejemplos de estas RFC son:

- "*MVPN: Optimized use of PIM via MS-PMSIs*" que permite el establecimiento de interfaces selectivas bidireccionales para evitar el establecimiento de MI-PMSI solo para mantener señalización del plano de control basado en C-PIM [27].
- "*MVPN: Using Bidirectional P-Tunnels*" que especifica el uso de PIM BiDir en el establecimiento de los P-Túneles que a pasar de ser nombrado en las RFC 6513 y 6514, estas no lo especifican de forma detallada [31].
- "*A Reliable Transport Mechanism for PIM*" que define mecanismos de transporte confiable para los mensajes *Join/prune* de PIM [28].

Es importante destacar que los tres fabricantes soportan el plano de control basado en PIM con la implementación planteada por la RFC 6037 (draft Rosen) [1].

3.5 Plano de transporte

El plano de transporte es el encargado de definir los procedimientos que deben implementarse en la red del proveedor de servicios para transmitir los flujos C-Multicast a través de su red, específicamente los procedimientos de asociación de las interfaces PMSI con los P-Túneles que, de acuerdo a lo indicado en el apartado 3.4.2, pueden ser del tipo P2P, P2MP o MP2MP. Básicamente estos P-Túneles transportan de forma transparente los paquetes C-Multicast a través de la red del proveedor de servicios.

En este apartado se analizará el proceso de establecimiento de estos P-Túneles identificando los principales aspectos involucrados.

3.5.1 Señalización

Una vez identificados los PE que integran la MVPN, se realiza el establecimiento de los P-Túneles que en el caso del plano de control basado en MP-BGP permitirán el flujo de datos C-Multicast o en el caso del plano de control basado en PIM junto al transporte de datos también permitirán el intercambio de rutas C-Multicast.

El primer paso consiste en el intercambio de mensajes de control necesarios para establecer los diferentes P-Túneles. Es necesario aclarar que este intercambio de mensajes es diferente al proceso de señalización al que se refiere el plano de control, que se encarga del descubrimiento de los PE y de la comunicación de los mensajes de control del proceso de enrutamiento del tráfico Multicast de los clientes.

En el plano de transporte existen 3 mecanismos de establecimiento de los túneles:

- A través de señalización P-PIM que permite el establecimiento de túneles GRE.
- A través de señalización mLDP para crear P-Túneles o Label Switched Path (LSP) MPLS.
- A través de señalización RSVP-TE para crear P-Túneles o Label Switched Path (LSP) MPLS.

P-PIM

En el caso de la señalización basada en P-PIM, se presentan dos variantes, la primera basada en PIM-SSM en la que la fuente es conocida con anticipación a partir del proceso de autodescubrimiento y no es necesario el funcionamiento de un RP, y la segunda variante se presenta a través de PIM-SM en la que se necesita de la existencia de un RP en la red para permitir la creación de los árboles de distribución.

Los demás procedimientos usados por la señalización basada en P-PIM son similares a los descritos en los apartados 2.5.2 y 2.5.4 por lo que no se incluyen en este apartado.

mLDP (Multipoint extensions for LDP)

Es un protocolo dirigido por el receptor, esto significa que un LSP multipunto (MP-LSP) es solamente creado si existe un receptor que esté interesado en recibir tráfico de un grupo Multicast. Todos los MP-LSP deben tener una raíz o "*root*" que será uno de los PE de ingreso. La selección del camino para el MP-LSP se hace basada en la dirección IP del PE de ingreso, que en el caso de MVPN se deduce de los anuncios de autodescubrimiento de MP-BGP. mLDP utiliza la asignación de etiquetas bajo demanda generada por los PE de egreso, y se van trasladando las asignaciones salto a salto hasta alcanzar al PE de ingreso.

LDP originalmente no ofrecía mecanismos para negociar funcionalidades o advertir capacidades como el soporte de servicios Multicast. Es así como mLDP define nuevos campos de información TLV (Type-Length-Value) destinados a negociar y advertir nuevas funcionalidades dentro de LDP, estas son negociadas bien en el intercambio de los mensajes de inicialización de la sesión o una vez establecida la sesión, en los

mensajes de notificación [26, 32]. Dentro de las nuevas capacidades negociadas se destacan las capacidades de establecimiento de LSP del tipo P2MP o MP2MP.

Aunque mLDP negocia nuevas funcionalidades, sigue manteniendo las funcionalidades de LDP, siendo el identificador de tráfico o FEC (*Forwarding Equivalency Class*) el más importante de los TLV que deben ser negociadas, pues es la que permite asociar el tipo de tráfico que será encapsulado en los LSP. Para entender su funcionamiento es importante revisar el comportamiento de los mensajes a nivel LDP.

LDP comprende varios tipos de mensajes como *Hello*, *Initialize* y *Label Mapping*. Para el caso de los FEC el mensaje que permite su identificación es "*Label Mapping*" como se muestra en la Figura 17. Este mensaje es usado por LDP para crear el MP-LSP salto a salto desde el PE de egreso hasta el PE de ingreso, y transporta información adicional denominada TLV destinada al PE de ingreso. Hay varios tipos de TLV, específicamente el TLV correspondiente al FEC o "*TLV FEC*" permite la asignación de paquetes dentro del LSP correspondiente usando las etiquetas definidas en el TLV correspondiente a la etiqueta o "*TLV Label*". El *TLV FEC* contiene el identificador del grupo de paquetes que serán encapsulados en el LSP. Por ejemplo en el caso de Unicast VPN, un elemento FEC contiene prefijos IP (normalmente las direcciones IP que identifican a los PE dentro de la red del proveedor). Entonces cualquier IP de destino que pertenezca al rango del prefijo asignado al FEC del LSP compartirá el mismo LSP.

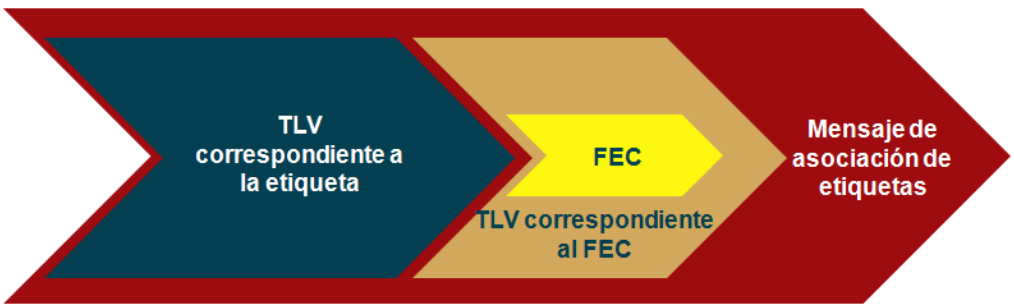

Figura 17. Mensaje de asociación de etiquetas en mLDP

En el caso de Multicast, el FEC no identifica el tráfico que puede ser transportado a través del túnel, sin embargo, si le da una identificación única al túnel, que es utilizada por el mecanismo de autodescubrimiento de MP-BGP para asociar el tráfico de un grupo Multicast al túnel mLDP que corresponda.

La Figura 18 detalla la codificación del FEC para MP-LSP.

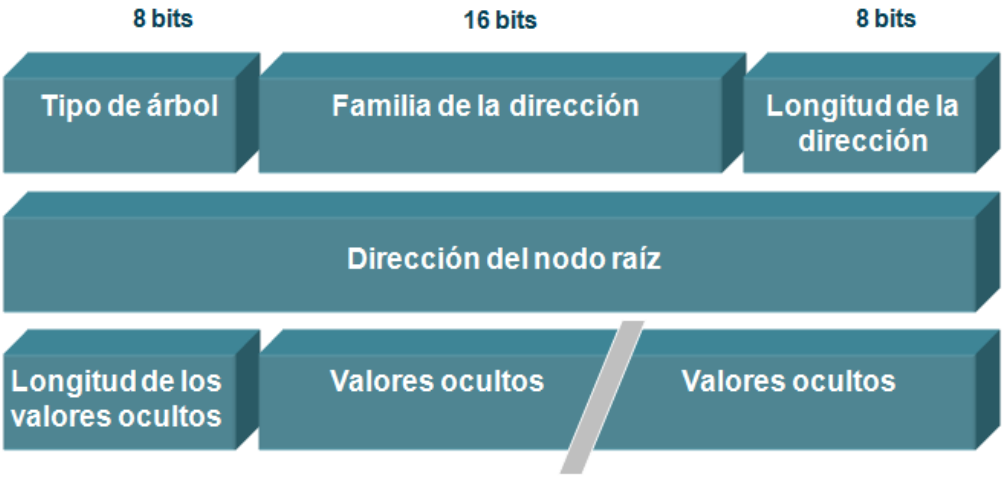

Figura 18. Codificación del FEC

Los parámetros relevantes que incluye el FEC son:

- Tipo de árbol de distribución: Si es unidireccional P2MP o Bi-direccional (MP2MP).
- Dirección del enrutador raíz: La dirección IPv4 o IPv6 del enrutador raíz o PE de ingreso.
- Valor oculto: Es información que identifica de forma unívoca al LSP (se llama oculto porque puede transportar información adicional que sólo tiene significado para los PE de ingreso o egreso pero no para los P o PE de tránsito), sin embargo no son utilizadas para la implementación de MVPN en el entorno de las RFC 6513 y 6514.

Para el caso de LSP MP2MP se definen dos tipos de FEC *MP2MP downstream* y *MP2MP upstream* que permiten establecer los LSP en dos direcciones, y la diferencia principal en su establecimiento es que al ser bidireccional, el enrutador raíz no necesita ser el PE de ingreso o egreso de los flujos, puede ser un PE de transito que se comporta como un conmutador de etiquetas.

RSVP-TE

Es un protocolo dirigido por el transmisor, esto significa que el PE de ingreso es el responsable de iniciar el establecimiento de los LSP P2MP y los Sub-LSP asociados. El procedimiento que sigue RSVP-TE describe a continuación [25]:

- La información relacionada con los LSP P2MP es anunciada a los PE de egreso y de ingreso a través de los mecanismos de autodescubrimiento de MP-BGP.
- El PE de ingreso establece la señalización del sub-LSP a través de mensajes "*P2MP RSVP Path*" dirigidos a los PE de egreso.

- El PE de ingreso aprende la identidad de los PE de egreso a partir del proceso de autodescubrimiento de MP-BGP.
- Cada uno de los mensajes "*RSVP Path*" transporta, entre otros objetos, el *S2L_Sub_LSP* que contiene la dirección IP del PE de destino (Egreso), el ERO (*Explicit Route Object*) que determinará el camino que debe seguir el sub-LSP y el objeto *P2MP Session* que indica el LSP P2MP al que pertenece el sub-LSP.
- El PE de egreso responde al mensaje *Path* originando un mensaje *Resv* a través del proceso normal de RSVP. El mensaje *Resv* contiene la etiqueta MPLS asignada por el PE de egreso para este sub-LSP y es reenviada salto a salto por los PE de transito hasta alcanzar el PE de Ingreso.

El punto clave a destacar es que, desde la perspectiva del plano de señalización, un LSP P2MP es visto como un grupo de LSP P2P (sub-LSP) desde el PE de ingreso hacia cada uno de los PE de egreso y cada Sub-LSP es señalizado a través del intercambio de mensajes *Path* y *Resv* [33] como se observa en la Figura 19.

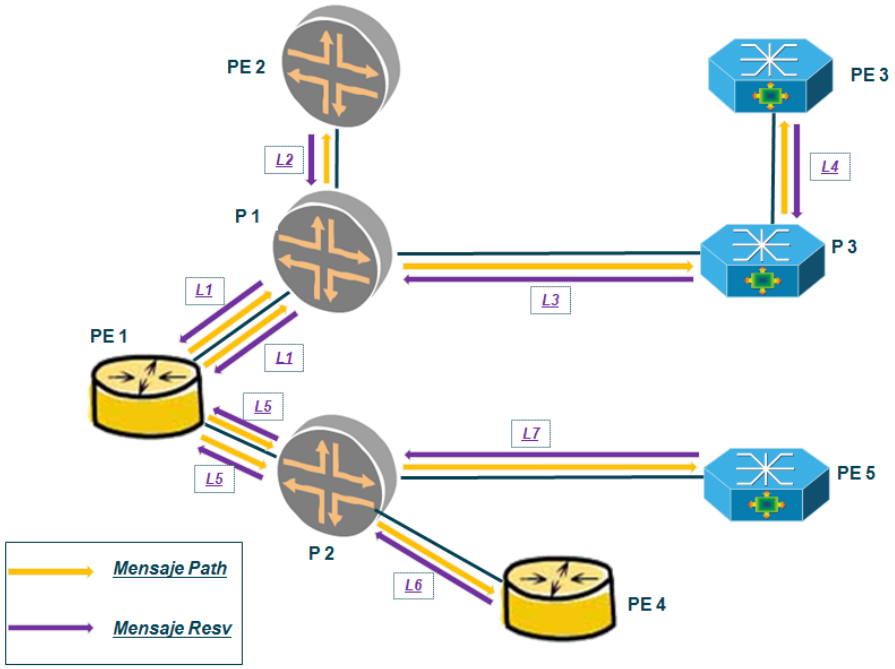

Figura 19. Señalización RSVP de un LSP P2MP

Análisis

A continuación se destacan algunos aspectos relevantes de los diferentes mecanismos de señalización de los P-Túneles y sus implicaciones en la infraestructura de red:

- Debido a que RSVP-TE y P-PIM son protocolos no orientados a conexión, requieren mensajes periódicos de mantenimiento de los árboles de

distribución (P-Túneles P2MP) mientras que en el caso de mLDP, al utilizar TCP no requiere mensajes periódicos de mantenimiento.

- Los tres protocolos (P-PIM, RSVP-TE y mLDP) deben ser habilitados en todos los PE y/o P que hagan parte del árbol de distribución, sin embargo en entornos MPLS es posible que el proveedor de servicio ya cuente en su infraestructura de red con los protocolos RSVP-TE y LDP para el servicio VPN Unicast y sólo será necesario habilitar las extensiones para soportar el servicio C-Multicast, mientras que en el caso de P-PIM es necesario habilitarlo como un segundo o tercer protocolo de señalización en el plano de transporte en la red.
- En cuanto a la cantidad de mensajes necesarios para señalizar los P-Túneles, debido a que en RSVP-TE es necesario señalizar cada uno de los sub-LSP por separado, el número de mensajes de establecimiento de los túneles es mayor que en los escenarios de PIM-SSM y mLDP, lo que presenta menor escalabilidad. En el escenario de PIM-SM, es necesario contemplar que se presentan mensajes de señalización para el establecimiento de los *Shared tree*, y también en el establecimiento de los *Source tree* cuando se presente el cambio de escenario.
- RSVP-TE permite el uso de ingeniería de tráfico que optimiza el uso de recursos de la red, pero repercute en una mayor carga administrativa para el establecimiento de los túneles, a diferencia de PIM y LDP en donde el establecimiento es dinámico.
- mLDP y PIM permiten la configuración de túneles MP2MP mientras que RSVP-TE no.
- PIM es utilizado para escenarios con túneles basados en IP o GRE mientras que RSVP-TE y mLDP es utilizado en escenarios con túneles basados en MPLS.

Por último, es importante destacar que las RFC pueden tener diferentes interpretaciones dependiendo de las circunstancias del fabricante, lo que puede afectar la interoperabilidad, específicamente la RFC 4875 define las extensiones para soportar LSP P2MP en RSVP-TE, en ella se presenta una situación indefinida que puede crear problemas de incompatibilidad y es presenta en la definición del proceso de asignación de etiquetas en los enrutadores de transito que deben hacer la replicación de tráfico a varios Sub-LSP. Allí se recomienda el uso de una sola etiqueta hacia el PE de ingreso pero deja abierta la opción de usar más de una etiqueta (dependiendo del número de Sub-LSP). El problema se da porque las dos opciones son incompatibles, es decir, si el fabricante del equipo de tránsito que debe hacer la replicación decide usar la implementación de varias etiquetas (una por Sub-LSP) y en al camino hacia el PE de

ingreso se conecta a un equipo de otro fabricante que decidió usar la implementación de una sola etiqueta para todos los Sub-LSP, el túnel P2MP no va a funcionar.

Debido a lo anterior y sumado a que mLDP y P2MP RSVP-TE son protocolos relativamente nuevos en el entorno de MVPN, y que hasta ahora están siendo desplegados por los principales fabricantes, es recomendable que los proveedores de servicio con redes multi-fabricante realicen pruebas exhaustivas de interoperabilidad pues en algunos casos el compromiso de los fabricantes con el cumplimiento de las diferentes RFC no garantiza la interoperabilidad.

Soporte de fabricantes

Los tres fabricantes indican el soporte de los tres protocolos de señalización para el establecimiento de los P-Túneles, sin embargo, la fecha en la que han empezado a ser soportados puede ofrecer una idea de la experiencia que tienen en cada implementación especialmente en el caso de mLDP y RSVP-TE que son los protocolos novedosos en las RFC 6513 y 6514. P-PIM era el único protocolo de señalización soportado por la RFC 6037 (draft Rosen).

Es así como Alcatel Lucent soporta los protocolos LSP P2MP RSVP-TE y mLDP desde el año 2010 [17], mientras que Juniper soporta RSVP-TE desde 2007 [34] pero P2MP mLDP desde 2011 [18, 23]. Por último, Cisco soporta mLDP y P2MP RSVP-TE desde el año 2011 [35]

3.5.2 Encapsulación

Descripción

En cuanto a la encapsulación de datos, las RFC 6513 y 6514 ofrecen dos opciones, la primera es utilizar P-Túneles GRE o IP y la segunda es utilizar P-Túneles MPLS.

GRE en su forma más simple, proporciona un método de encapsular cualquier protocolo de red en otro protocolo de red. En el caso de MVPN, se utiliza GRE esencialmente para ocultar los paquetes C-Multicast a la infraestructura IP del proveedor y permitir asignar varios grupos C-Multicast de una MVPN en un solo grupo P-Multicast asignado por el proveedor.

El proveedor únicamente detecta la dirección IP del encabezado exterior apareciendo con un estado (P-S, P-G) en la tabla de rutas P-Multicast global. La dirección origen de este paquete IP será la dirección IP con la que el PE originador se identifique en la red (normalmente la interfaz Loopback), y la dirección IP de destino será la dirección asignada al grupo P-Multicast asociado a la MVPN como se indica en la Figura 20.

Originalmente GRE fue implementado para soportar conexiones punto a punto, con lo que se desarrollaron funcionalidades como mensajes de mantenimiento de vecindad o "*keepalives*", campos de comprobación de integridad o "*checksum*" y números de secuencia, sin embargo, en el caso de MVPN estas funcionalidades no aplican (como los *keepalives*) o se recomienda no implementar para mejorar la velocidad de procesamiento de paquetes, como ocurre con el número de secuencia y la suma de verificación.

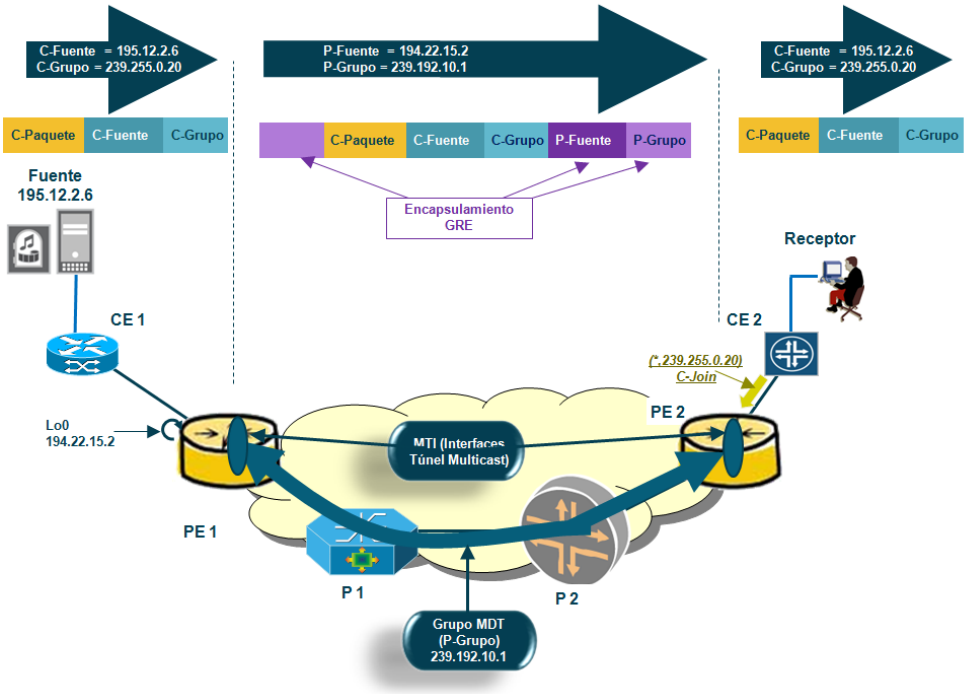

Figura 20. Encapsulación basada en GRE

Por otra parte la encapsulación de paquetes basada en MPLS permite desacoplar el entorno de Multicast del cliente del entorno de enrutamiento del proveedor de servicio y de los demás clientes a través del uso de etiquetas incrustadas entre el encabezado de nivel 2 y los datos del cliente, que en este caso son IP como se describe en la Figura 21. Estas etiquetas conmutadas salto a salto, permiten establecer LSP P2MP o MP2MP que optimizan el uso de la infraestructura del proveedor de servicios para transportar los servicios Multicast.

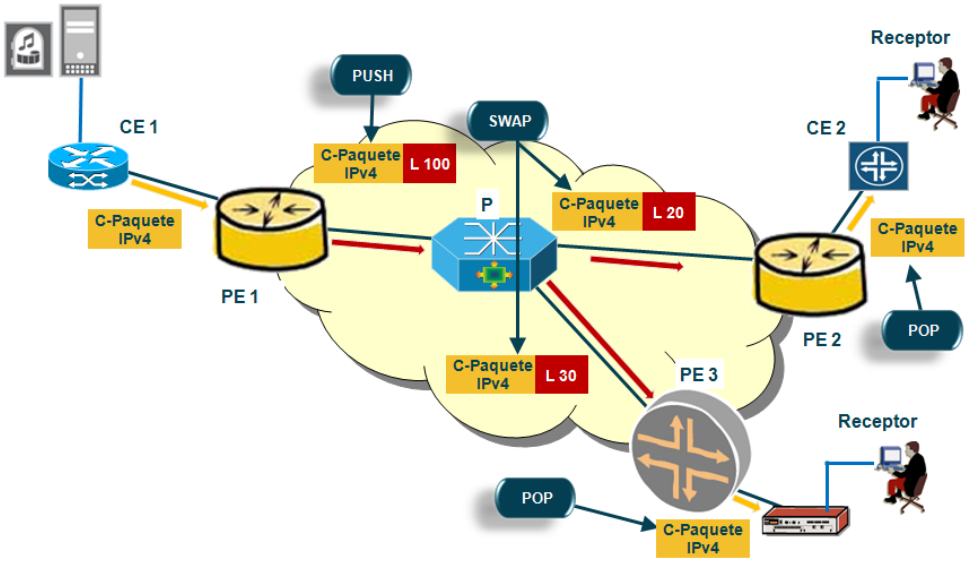

Figura 21. Encapsulación basada en MPLS

Es importante indicar que los dos métodos de encapsulación aparte de permitir establecimiento de P-Túneles P2MP o MP2MP, también pueden ser utilizados para implementar estructuras Multicast basadas en P-Túneles P2P con la replicación de tráfico por cada uno de los túneles desde el PE de ingreso, sin embargo, en este documento no son contempladas por ser una estructura ineficiente, debiendo ser implementada únicamente en escenarios temporales y muy específicos, como en el proceso de migración de servicios o en procesos de integración redes con distintos protocolos de encapsulación, pero que deben ser rápidamente modificados a una estructura multipunto.

Análisis

Los métodos de encapsulación son soportados por los dos planos de control, sin embargo en los métodos de encapsulación basados en IP (GRE e IP/IP) existen algunas limitaciones en el proceso de agregación de interfaces PMSI en un solo túnel o en la identificación de los PE originadores de tráfico cuando el cliente implementa PIM-BiDir, pues requiere del uso de etiquetas MPLS como método para identificar las diferentes interfaces PMSI agregadas en el túnel, o bien la partición a la que pertenece el PE originador del tráfico en el caso de C-PIM BiDir. Este comportamiento es claramente una deficiencia comparado con la implementación de MPLS como método de encapsulamiento de paquetes, pues la inclusión de etiquetas en el protocolo MPLS viene dada de forma natural.

Por otra parte, aunque puede no ser un punto crítico para el procesamiento de los enrutadores actualmente, es conveniente tener en cuenta que el procesamiento de paquetes encapsulados en MPLS puede representar menor consumo de recursos. Esto se debe a que la conmutación basada en etiquetas es más rápida que la conmutación de

paquetes basados en direcciones IP, gracias a la facilidad de asociación directa de interfaces con las diferentes etiquetas MPLS evaluadas en el nivel 2 del modelo OSI, mientras que en el caso de GRE o IP, la evaluación se hace a nivel 3. Adicionalmente usar MPLS para la conmutación de paquetes C-Multicast se integra de forma natural con la solución de MPLS para VPN Unicast, evitando que el proveedor maneje dos métodos de encapsulamiento en su red.

Por último, el soporte de encapsulamiento GRE e IP en las RFC6513 y 6514 parece que viene dado por la intención de soportar implementaciones legadas de clientes o proveedores de servicio, específicamente basadas en la RFC 6037 (draft Rosen), sin embargo la encapsulación basada en MPLS cumple las funcionalidades ofrecidas por GRE/IP y adicionalmente se acopla a la infraestructura MPLS Unicast de los proveedores.

Soporte de fabricantes

Como ocurre en el caso de la señalización del plano de transporte, los tres fabricantes indican el soporte de los dos métodos de encapsulamiento de paquetes, la diferencia se presenta en la fecha en la que han empezado a soportar los mecanismos de encapsulación de P-Túneles multipunto, especialmente basados en MPLS, ya que GRE es soportado con anterioridad por los tres gracias al soporte de la RFC 6037 (draft-Rosen).

Es así como Alcatel-Lucent soporta los LSP P2MP basados en los protocolos de señalización RSVP-TE y mLDP desde el año 2010 [17], mientras que Juniper soporta RSVP-TE desde 2007 [34] pero P2MP mLDP desde 2011 [18, 23]. Por último, Cisco soporta mLDP y P2MP RSVP-TE desde el año 2011 [35]

3.5.3 Protección

A continuación se analizan los mecanismos de protección ante fallos de la red utilizados por cada uno de los protocolos de señalización de los P-Túneles

PIM

En el caso de señalización basada en PIM, los mecanismos de protección ante fallos dependen del protocolo IGP que utilice el proveedor de servicios. PIM por si mismo no intercambia rutas sino que se apoya en el intercambio realizado por el IGP. En consecuencia, el camino de los túneles basados en PIM será definido por el protocolo IGP así como el periodo de convergencia después de presentarse un fallo en la red.

LDP

En el caso de LDP ocurre una situación similar a la que se presenta en PIM, en la que los caminos de protección son seleccionados por el protocolo IGP que sea implementado por el proveedor y por lo mismo, el tiempo de convergencia de LDP

ante un fallo en la red vendrá dado por el tiempo de convergencia del IGP. A pesar de esto, actualmente existe en la IETF el draft "*mLDP Node Protection*" en el que se plantean mecanismos de protección similares a los que se implementan de forma natural en RSVP-TE, que proporcionan menores tiempos de convergencia gracias a la pre-configuración de LSP P2P como caminos alternativos [36], sin embargo es una implementación que aun esta en desarrollo.

RSVP-TE

RSVP, además de apoyarse en el IGP para llevar a cabo el restablecimiento de los túneles ante fallos en la red, también cuenta con mecanismos de protección conocidos como "*Fast Rerouting*" o FRR basados en protección de nodos o de enlaces, los cuales garantizan tiempos de restablecimiento de túneles ante fallos de la red menores a 50 ms. Estos mecanismos básicamente consisten en la señalización previa de LSP (P2P o P2MP) alterativos a lo largo de los diferentes nodos que conformen el LSP P2MP principal, de tal forma que al ocurrir un fallo en la red que afecte el LSP principal, el tiempo de indisponibilidad del servicio MVPN disminuya al evitar el tiempo de recálculo de los nuevos caminos (convergencia de IGP) pues los caminos alternativos se han creado previamente.

Soporte de fabricantes

Debido a que los mecanismos de protección descritos, con excepción de FRR para mLDP, son inherentes a la definición de los protocolos de señalización, (PIM - RFC 4601, RSVP-TE – RFC 4875 y LDP - RFC 5036) los tres fabricantes analizados indican que soportan los tres mecanismos de señalización estándar.

En el caso de FRR para mLDP, a pesar de que Cisco indica que es una de las ventajas de usar mLDP comparado con PIM, no es posible confirmar que ya lo soporte pues no se encuentran referencias específicas a su implementación en los equipos ASR 9000 [24]. Adicionalmente, al no ser una definición finalizada por la IETF, no hay garantía de interoperabilidad con los demás fabricantes, especialmente si los demás fabricantes no indican su soporte.

3.5.4 Calidad de servicio

El soporte de calidad de servicio (QoS por sus siglas en inglés) tanto en el encapsulamiento basado en IP/GRE como el basado en etiquetas MPLS es totalmente compatible con las redes tradicionales VPN Unicast, pues en el primero, el manejo de QoS se hace basado en el campo de tipo de servicio (ToS) del encabezado IP y en el segundo se hace basado en los bits experimentales (EXP) de las etiquetas MPLS, que coincide con el manejo de QoS en escenarios VPN Unicast.

Es necesario tener en cuenta que en situaciones donde un operador sólo transporte los datos de los clientes a través de servicios VPN basados en MPLS, y desee implementar servicios MVPN basados en encapsulamiento GRE/IP, deberá contemplar que sus políticas de QoS definidas en los diferentes enrutadores hasta ese momento basadas en los bits EXP de las etiquetas MPLS, deberán incluir el tratamiento del campo ToS del encabezado IP de los paquetes IP/GRE de los P-Túneles del servicio MVPN.

3.6 Funcionalidades

3.6.1 Escenarios de interconexión de diferentes sistemas autónomos

Descripción

Un cliente puede tener sedes atendidas por diferentes proveedores de servicio interesadas en participar en una MVPN, normalmente cada proveedor de servicio administra al menos un sistema autónomo (AS), con lo que el servicio MVPN deberá distribuirse a través de varios sistemas autónomos. Esta implementación se denomina MVPN inter-AS.

Tal y como ocurre en el servicio VPN IP Unicast, existen varias aproximaciones para soportar la implementación de MVPN inter-AS, dichas aproximaciones se dividen en dos categorías que se describen a continuación.

La primera categoría es conocida como la opción A en la RFC 4364, en ella los P-Túneles que empiezan en el PE y ASBR de un AS finalizan en un PE y ASBR del mismo AS; en este escenario, el tráfico C-Multicast que debe atravesar la interconexión entre sistemas autónomos es manejado de forma nativa por los ASBR de cada AS. Desde la perspectiva de cada ASBR, el otro ASBR es simplemente un grupo de CE, cada uno alcanzable a través de conexiones lógicas independientes. En este tipo de despliegues no es necesario mecanismo de autodescubrimiento adicionales entre los diferentes AS y el intercambio de rutas y señalización C-Multicast utiliza los mismos protocolos y procedimientos descritos en el apartado 3.4.1.

La segunda categoría de soluciones inter-AS involucra el establecimiento de P-Túneles a través de la interconexiones entre los AS. Esto quiere decir que las interfaces PMSI estarán conectadas directamente aunque los PE de la MVPN no se encuentren en el mismo AS. A esta categoría pertenecen las opciones B y C definidas en la RFC 4364, en donde la opción B define la interconexión de AS usando sesiones eBGP establecidas entre ASBR, a través de las que se intercambian todos los prefijos de los sistemas autónomos involucrados y la opción C también permite el intercambio de prefijos a través de sesiones eBGP, pero establecidas entre los reflectores de rutas de los AS, extendiendo el dominio MPLS a los sistemas autónomos involucrados.

De forma similar a lo que ocurre con la opción A, la opción C no requiere tratamientos especiales para el establecimiento de túneles Multicast, pues a pesar de involucrar varios sistemas autónomos, el procedimiento de establecimiento de P-Túneles Multicast es el mismo que se requiere en los escenarios donde la MVPN es conformada por los PE que hacen parte de un solo sistema autónomo.

Por lo anterior, las RFC 6513 y 6514 se enfocan en dar solución a la interconexión de sistemas autónomos basados en la opción B, proponiendo dos planteamientos para ofrecer servicios MVPN a clientes con sedes distribuidas en dichos AS.

- El primer planteamiento se basa en la construcción de P-Túneles no segmentados que son establecidos extremo a extremo a través de los AS, de tal forma que los ASBR se comportan como enrutadores P.
- La segunda se realiza a través de túneles segmentados donde cada AS construye su propio P-Túnel Multicast Intra-AS y son interconectados a través de P-Túneles Unicast establecidos entre los ASBR de los AS, como se observa en la Figura 22.

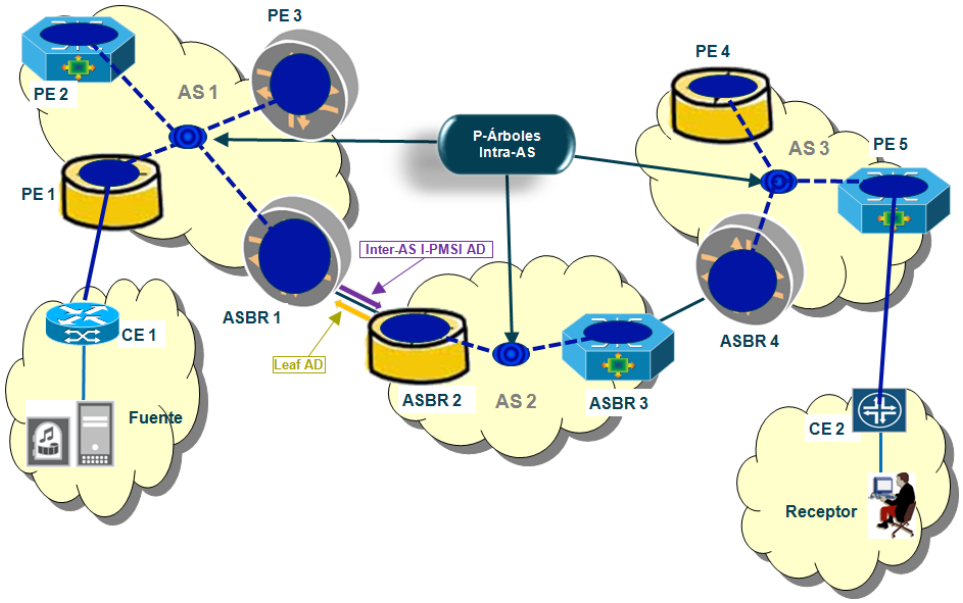

Figura 22. Escenario Inter-AS con túneles segmentados

Análisis

A continuación se realiza un breve análisis de los escenarios de interconexión de sistemas autónomos tanto segmentados como no segmentados basados en la opción B:

- La solución a través de P-Túneles segmentados ofrece mayor flexibilidad a los proveedores de servicio, ya que la conexión se hace de forma controlada a través de un P-Túnel Unicast en dónde se pueden aplicar políticas de administración del tráfico Multicast inter-AS de forma focalizada, sin embargo,

la solución no segmentada puede simplificar el despliegue de MVPN en entornos Inter-AS al comportarse como un solo dominio MPLS.

- Por otra parte, el soporte de la opción no segmentada por parte de las RFC 6513 y 6514 permiten la compatibilidad con soluciones basadas en la RFC 6037 que solamente soporta la solución no segmentada, facilitando los procesos de posibles migraciones o actualizaciones de red por parte de los proveedores de servicio.
- En cuanto la escalabilidad a nivel de interfaces PMSI, la solución segmentada es más escalable debido a que el ASBR puede agregar en un solo P-Túnel Inter-AS múltiples P-Túneles Intra-AS usados para transportar PMSI dentro de su propio AS. Mientras que en la solución no-segmentada, la agregación dependerá de la congruencia de los receptores y transmisores de los diferentes grupos C-Multicast que se quieran agrupar.
- En cuanto a la independencia de la tecnología de encapsulación utilizada en los P-Túneles seleccionada por cada AS, en la solución segmentada cada AS puede utilizar la tecnología más adecuada de acuerdo a sus necesidades, mientras que en la solución no segmentada, la tecnología debe ser la misma en los AS interconectados, lo que puede dificultar su despliegue en AS que sean administrados por distintos proveedores con diferentes planos de control o planos de transporte para el desarrollo de sus servicios MVPN.
- Por parte de la independencia del enrutamiento entre AS, uno de los beneficios de la opción B es el aislamiento que ofrece a nivel de enrutamiento entre los AS involucrados en la solución, beneficio que se mantiene en la solución segmentada gracias al establecimiento del P-Túnel Inter-AS que permite aislar los P-Túneles Intra-AS. Lo mismo ocurre con la solución no segmentada utilizando el plano de transporte basado en MPLS, sin embargo, en la solución no segmentada usando el plano de transporte basado en P-PIM, los dos AS deben convivir a nivel de direccionamiento IP, pues los PE involucrados deben alcanzar a nivel IP a todos los demás PE sin importar el sistema autónomo al que pertenecen.

  En este aspecto de independencia a nivel de enrutamiento, es importante destacar que las RFC 6513 y 6514, en la descripción de la opción no segmentada no profundiza sobre el procedimiento que se deberá seguir para establecer túneles inter-AS en tecnologías basadas en MPLS (mLDP y RSVP-TE), pues la opción B de Inter-AS para VPN Unicast, no contempla vecindades a nivel de LDP o RSVP-TE entre ASBR, lo que es una condición para que se puedan establecer LSP entre ASBR.

- Respecto al impacto del enrutamiento C-Multicast, en el contexto de la opción segmentada se puede limitar el intercambio de mensajes de control de C-PIM a los AS que deseen implementar el plano de control basado en PIM, mientras que el resto de AS sólo traducirán estos mensajes de control al plano MP-BGP cuándo sea requerido por sus PE. Por otra parte, en la solución no segmentada, en el caso de requerirse el plano de control basado en PIM por uno de los AS todos los demás AS deberán soportarlo e implementar el P-Túnel, con lo que el intercambio de mensajes de control será extendido a todas las interfaces MI-PMSI de los PE que integren la MVPN en todos los AS.

Soporte de proveedores

Alcatel-Lucent indica que únicamente soporta escenarios de interconexión de varios AS basados en la opción A descrita en la RFC 4363 [19].

Por su parte, Cisco indica que soporta las opciones A, B y C de interconexión de sistemas autónomos, sin embargo en la opción B no especifica si soporta los dos modelos segmentado y no segmentado [24].

Por último, en Juniper no es posible encontrar en su documentación el soporte de las diferentes opciones, sin embargo, como se ha indicado en la descripción de los escenarios de interconexión de AS, la opción A no requiere de procedimientos especiales diferentes a los ya expresados en entornos intra-AS por lo que se asume que al menos esta opción es soportada.

3.6.2 Manejo de la duplicidad de tráfico

Descripción y análisis

En el servicio de MVPN se presentan dos situaciones en las cuales pueden existir paquetes duplicados para un mismo grupo C-Multicast en una MVPN, estos son:

- Cuando se presentan topologías donde una fuente o un RP de un determinado cliente se interconecta a dos o más PE del proveedor de servicio (*Multi-home*).
- Cuando la MVPN ofrece transporte a tráfico C-Multicast de un C-grupo específico basado en una configuración PIM-ASM y realiza la conmutación a un escenario PIM-SSM.

Para atender estos escenarios, las RFC 6513 y 6514 plantean tres métodos que se analizan a continuación:

El primero se basa en el descarte del tráfico duplicado que provenga del PE que no haya sido seleccionado como el preferido para acceder a la fuente (UMH- Upstream Multicast Hop). Por defecto el método de elección del UMH se basa en la direcciones IP que identifican a los PE, siendo preferida la dirección más alta, con lo que todos los PE

de la MVPN seleccionarán el mismo PE. Utilizando este método, el tráfico duplicado llegará los PE de egreso y este será el encargado de descartar el tráfico.

El segundo método se basa en que sólo el PE seleccionado como UMH puede transmitir los paquetes de la fuente, con esto se optimiza la transferencia de datos a tal punto que se elimina la duplicidad en la red. Sin embargo las RFC 6513 y 6514 no especifican la forma en la que el PE de ingreso conoce que no es el UMH y que debe bloquear la conmutación de paquetes de la fuente.

El tercer método solo aplica para el plano de control basado en PIM usando túneles MI-PMSI, y se apoya en los mecanismos que tiene PIM de forma nativa para evitar la duplicidad de tráfico, como los mensajes *C-PIM assert* que permiten mantener un solo enrutador como transmisor del flujo Multicast para el segmento LAN determinado, que en este caso es la interfaz MI-PMSI.

Soporte de fabricantes

El tercer método al ser el comportamiento natural del plano de control basado en PIM, sólo es soportado por Cisco, pues como se ha indicado previamente es el único de los fabricantes analizados que soporta el plano de control basado en PIM dentro del contexto definido por las RFC 6513 y 6514.

Para el caso de Juniper, en el documento "*This Week: Deploying MBGP Multicast VPNs*" [18], deja entrever que cumple con el primer método basado en el descarte del tráfico proveniente de los PE que no son seleccionados como UMH, sin embargo, no menciona si también soporta el segundo método bloqueando la conmutación de paquetes C-Multicast de los PE de ingreso que no sean UMH.

Por último, para el caso de Alcatel-Lucent no fue posible encontrar si cumple con los métodos 1 y 2 para la eliminación de tráfico duplicado.

3.6.3 Congruencia entre rutas Unicast y rutas Multicast

Descripción y análisis

Por razones de control de tráfico de forma diferenciada a través de la red del proveedor o dentro de la propia red de los clientes, los respectivos administradores de las redes pueden preferir mantener el tráfico Unicast en enlaces separados de los destinados para el tráfico Multicast. Esto se logra a través del mantenimiento de tablas de conmutación de tráfico o FIB (Forwarding Information Base) separadas para cada tipo de tráfico dentro de una misma VPN.

A través de MP-BGP el CE puede anunciar de forma independiente las rutas Multicast usando la combinación AFI 1 - SAFI 2, y el PE mantiene y reenvía estas rutas

dentro del dominio MPLS también a través de MP-BGP, pero esta vez usando la combinación AFI 1 SAFI 129.

La FIB creada por esta combinación AFI – SAFI es la que utilizarán los enrutadores para realizar la revisión del RPF, con lo que así mismo será la base para crear los árboles de distribución Multicast.

Soporte de fabricantes

Alcatel-Lucent y Juniper indican que soportan la combinación AFI 1 SAFI 129 [18, 19], mientras que Cisco a pesar de soportarlo en algunas versiones de su sistema operativo (IOS-XE) [37], no indica su soporte en la versión del sistema operativo específica para los equipos ASR 9000 (IOS-XR) [24].

4 Caso práctico: C-PIM-SSM con plano de control basado en MP-BGP

En este capítulo se realizará la descripción de la configuración de una de las posibles implementaciones para transportar tráfico Multicast sobre una VPN en la red de un proveedor de servicios. Esta implementación se realiza con el plano de control basado en MP-BGP ofreciendo servicios a una MVPN que soporta el protocolo PIM-SSM.

Respecto al plano de control basado en MP-BGP, la implementación de C-PIM-SSM puede ser la más simple en términos de señalización, ya que los mensajes de *C-Join* de PIM contienen las direcciones IP de las fuentes, con lo que el PE de egreso que recibe este mensaje *C-Join* no debe realizar procedimientos de descubrimiento de fuentes ni reenvío de mensajes a equipos de soporte como los RP. Gracias a su sencillez, se presenta como un caso didáctico para comprender varios de los conceptos que se han planteado en este documento.

La implementación se hizo utilizando la herramienta de virtualización de enrutadores llamada *Junosphere* del fabricante Juniper Networks. A continuación se hace una breve descripción de la herramienta.

4.1 Junosphere

Junosphere es un entorno virtual basado en software y soportado por la tecnología de computación en la nube (*Cloud Computing*) que permite crear elementos y redes que utilizan el sistema operativo Junos. *Junosphere* utiliza los enrutadores virtuales de la serie VJX que funcionan con el mismo sistema operativo (SO) Junos de los dispositivos de redes y seguridad de Juniper.

4.1.1 Componentes

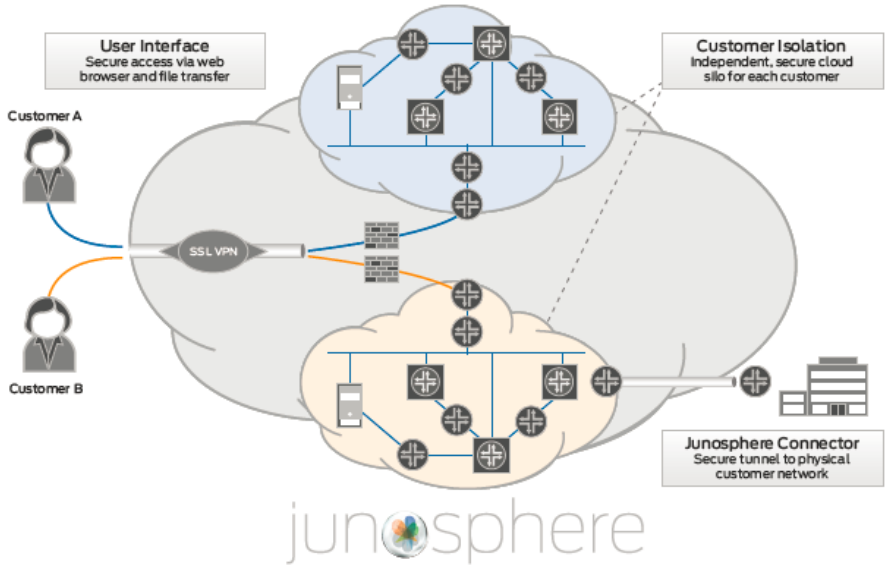

Figura 23. Componentes de plataforma Junosphere. Tomada de [38]

4.1.1.1 Serie VJX

Junosphere ofrece acceso a máquinas virtuales que funcionan con el mismo SO Junos implementado en los dispositivos de enrutamiento físico de Juniper. Las primeras de estas máquinas virtuales son las pertenecientes a la serie VJX que incluyen las funcionalidades proporcionadas por el SO Junos a los enrutadores de Juniper, las interfaces de línea de comandos (CLI), el comportamiento del plano de control, el funcionamiento de los protocolos y la mayoría de las funciones de conmutación de paquetes.

4.1.1.2 Junosphere Connector

Junosphere Connector es una función optativa que permite a los recursos de redes virtuales de *Junosphere* interactuar directamente con los elementos físicos de la red.

4.1.1.3 Junos Space

Las aplicaciones de automatización de redes de *Junos Space* pueden utilizarse dentro del entorno *Junosphere* para desplegar, supervisar y configurar la serie VJX dentro de la red virtual creada.

4.1.2 Acceso y configuración.

Se debe tener un usuario y contraseña autorizada para acceder a la herramienta a través de la dirección http://www.junosphere.net. Una vez se ha ingresado a la plataforma, es posible configurar de forma gráfica la red que se desea implementar tal y como se observa en la Figura 24:

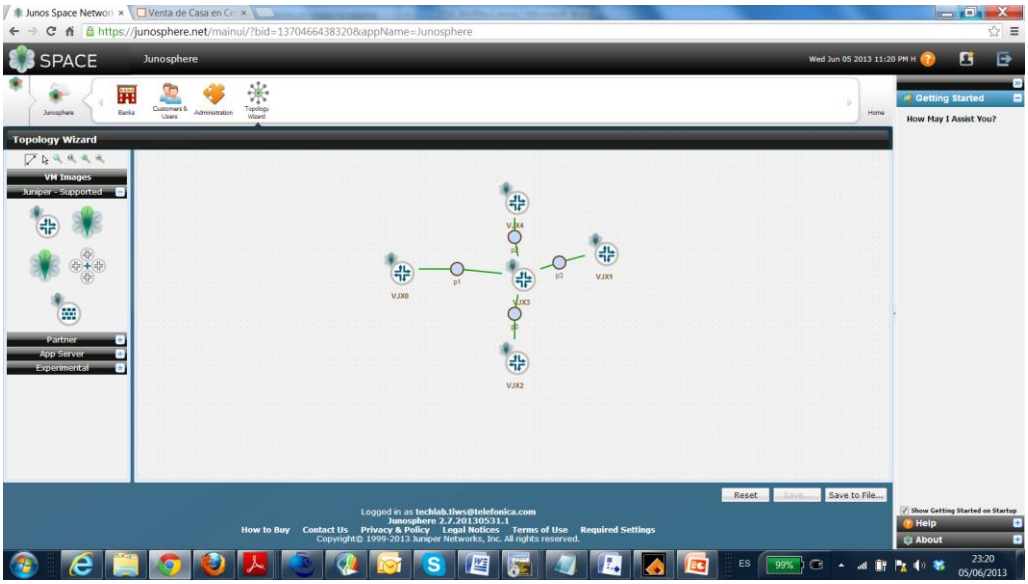

Figura 24. Creación de la topología de la red en Junosphere

Esta representación gráfica de la red se traduce en unos ficheros de configuración que hasta el momento están vacíos, pero que definen los enrutadores virtuales que serán ejecutados a partir del diseño topológico planteado. Una vez salvada la topología diseñada, se le indica a la herramienta que empiece a ejecutar las instancias virtuales de enrutamiento como se ilustra en la Figura 25.

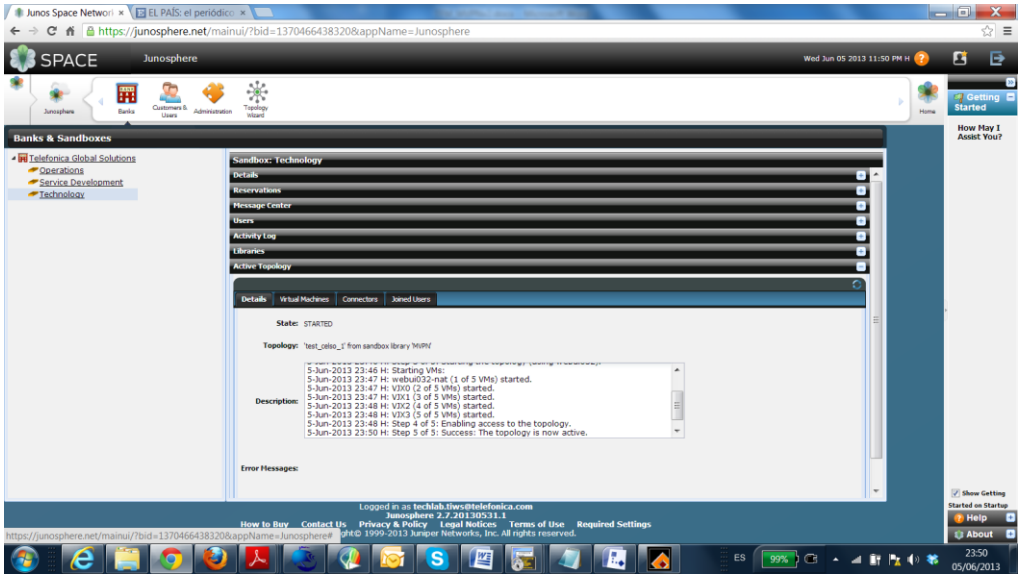

Figura 25. Ejecución de instancias virtuales en Junosphere

Después de estar en ejecución los enrutadores virtuales, se establece el túnel SSL desde el ordenador a la plataforma *Junosphere* ,con el usuario y contraseña válidos como se muestra en la Figura 26.

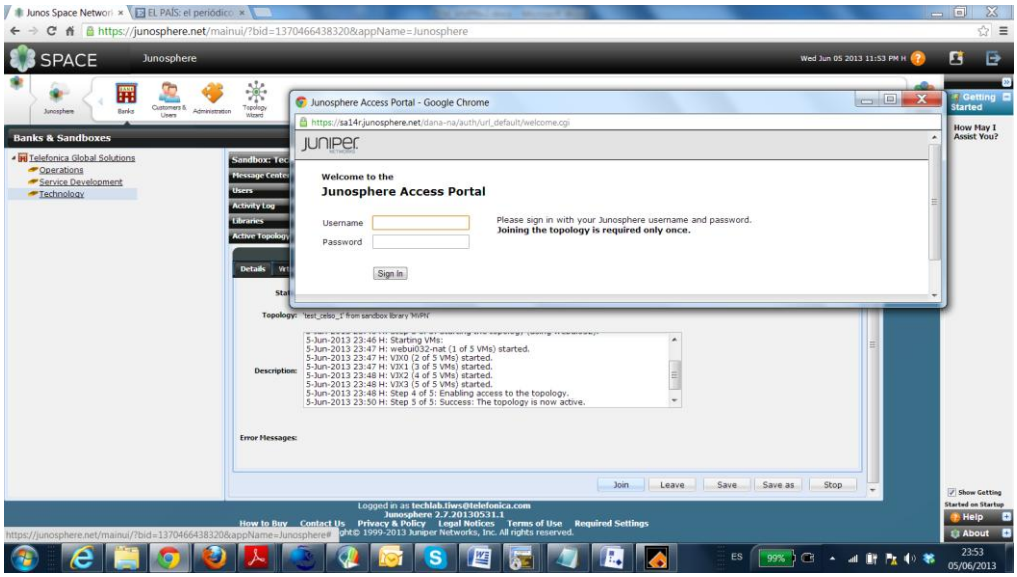

Figura 26. Establecimiento del túnel SSL con la plataforma Junosphere

Después de haber establecido el túnel SSL y a través de sesiones telnet y/o SSH los enrutadores virtuales pueden ser accedidos y configurados de acuerdo con las necesidades de la red que se desea simular. En la Figura 27 se muestra un ejemplo del acceso a las instancias virtuales a través de líneas de comandos.

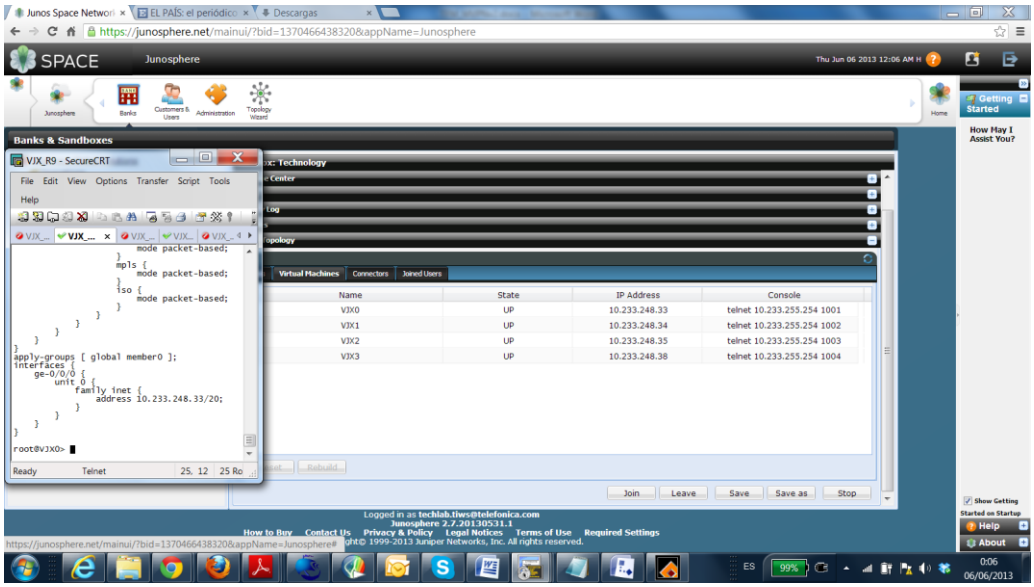

Figura 27. Conexión a las instancias virtuales través de línea de comandos

4.2 Desarrollo del caso práctico.

Para la configuración de la red que se ilustra en la Figura 28, se siguió el procedimiento descrito en el apartado anterior. Es necesario aclarar que a pesar de requerir una infraestructura MPLS/BGP, sólo se destacarán los aspectos más relevantes de su configuración pero no se profundizará detalladamente en ella, pues el

objetivo del caso de estudio planteado es revisar la configuración y el funcionamiento de una posible implementación del servicio MVPN.

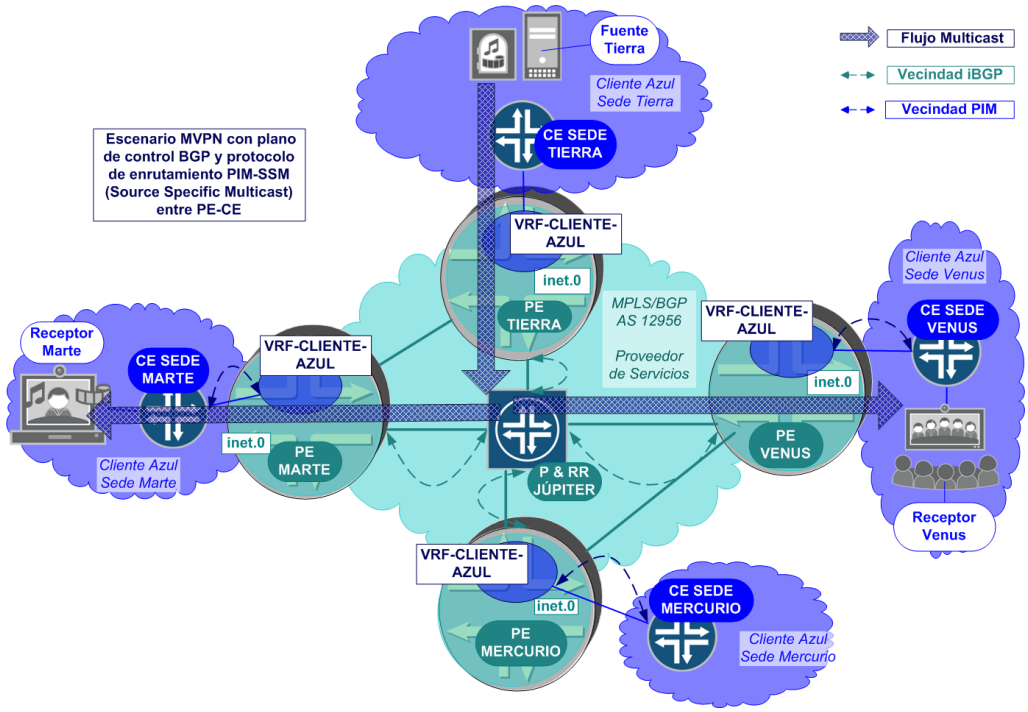

Figura 28. Topología del caso práctico

4.2.1 Arquitectura del escenario

Se implementó una red con cuatro enrutadores de borde o PE, y un enrutador P que también cumple funciones de reflector de rutas (RR). A cada uno de los PE están conectados los enrutadores de cliente o CE, simulando una red con cuatro sedes. Una de estas sedes cumple funciones de generación de tráfico Multicast (fuente), dos sedes son habilitadas como receptores de tráfico mientras que la última sede no participa en el entorno Multicast del cliente.

Por otra parte, el protocolo IGP configurado en el backbone es ISIS, aunque es importante destacar que también hubiese sido posible configurar OSPF.

El backbone es responsable de proporcionar la conectividad a nivel Unicast al interior de la VPN, usando MP-BGP para distribuir la información de las rutas y LDP para distribuir las etiquetas necesarias para transportar el tráfico Unicast a través de MPLS. Para el intercambio de etiquetas en el entorno Unicast también es posible usar RSVP-TE, sin embargo, requiere de la configuración manual de los LSP.

A nivel de MP-BGP, cada PE requiere de una sesión contra el reflector de rutas que permite la visibilidad de las redes a los demás PE.

4.2.2 Plan de direccionamiento

El plan de direccionamiento IP del escenario se describe en la Figura 29.

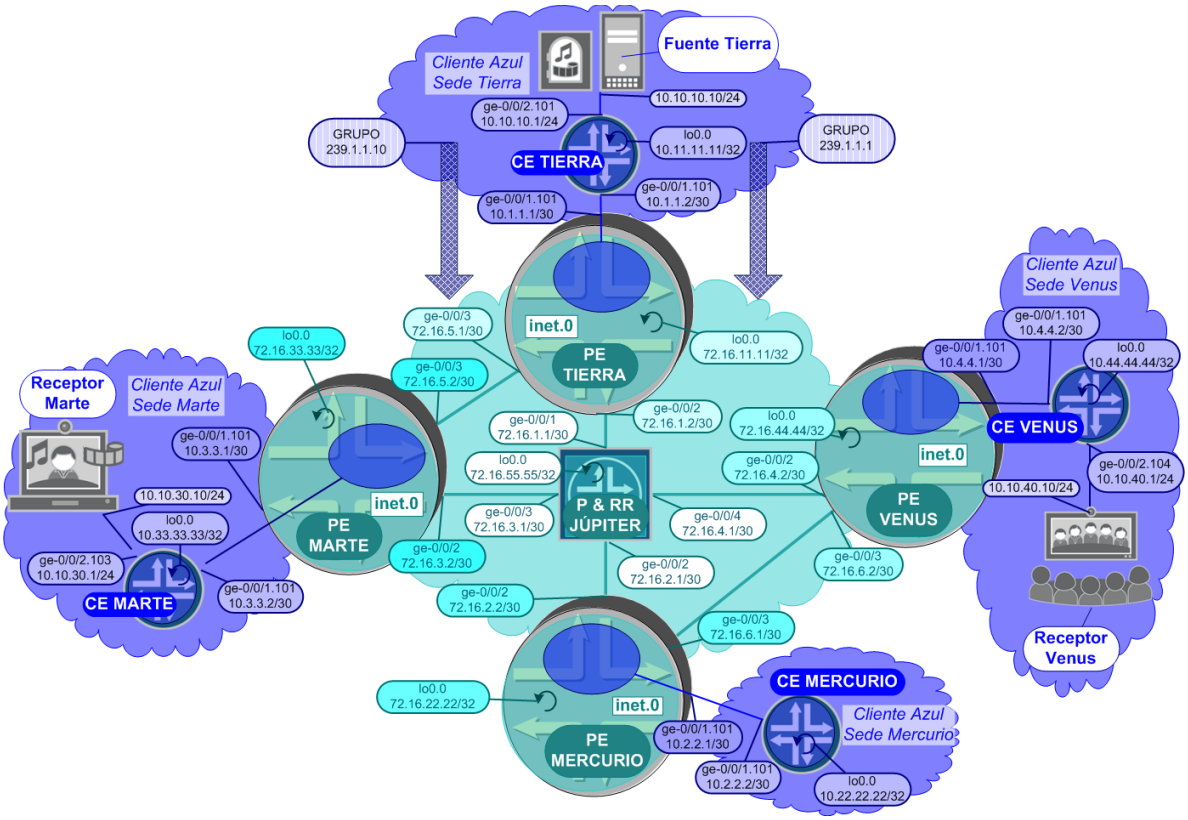

Figura 29. Plan de direccionamiento IPv4 del caso práctico

4.2.3 Verificación y pruebas

En este capítulo se principalmente se ejecutarán comandos de verificación sobre las instancias virtuales de enrutamiento definidas en la plataforma Junosphere. Únicamente se indicarán los comandos de configuración más relevantes para las pruebas realizadas, el resto de la configuración de los enrutadores virtuales se adjunta en los anexos, al final del presente documento.

Entorno Unicast

Como primer paso se verifica la operatividad de la configuración a nivel MPLS/BGP, ya que es la base para el implementar el escenario MVPN.

A nivel de IGP se implementó ISIS y su funcionamiento se verifica a continuación que las adyacencias se encuentren establecidas en todos los enrutadores de la red del proveedor de servicios:

```
root@PE_SEDE_MERCURIO# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            P_RR_JUPITER   2  Up                   20
ge-0/0/3.0            PE SEDE VENUS  2  Up                   25

[edit]
```

```
root@PE_SEDE_VENUS# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            P RR JUPITER   2  Up                   23
ge-0/0/3.0            PE SEDE MERCURIO 2 Up                 19

[edit]
```

```
root@PE_SEDE_MARTE# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            P_RR_JUPITER   2  Up                 21
ge-0/0/3.0            PE SEDE TIERRA 2  Up                 22

[edit]
```

```
root@PE_SEDE_TIERRA# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/2.0            P RR JUPITER   2  Up                 22
ge-0/0/3.0            PE SEDE MARTE  2  Up                 24

[edit]
```

```
root@P_RR_JUPITER# run show isis adjacency
Interface             System         L State       Hold (secs) SNPA
ge-0/0/1.0            PE SEDE TIERRA 2  Up                 26
ge-0/0/2.0            PE SEDE MERCURIO 2 Up               24
ge-0/0/3.0            PE SEDE MARTE  2  Up                 21
ge-0/0/4.0            PE_SEDE_VENUS  2  Up                 21

[edit]
```

Así mismo, se verifica que a nivel de LDP se encuentren establecidas las vecindades y las sesiones en todos los enrutadores de la red del proveedor de servicios:

```
root@PE_SEDE_MERCURIO> show ldp neighbor
Address            Interface          Label space ID         Hold time
72.16.2.1          ge-0/0/2.0         72.16.55.55:0            10
72.16.6.2          ge-0/0/3.0         72.16.44.44:0            10

root@PE_SEDE_MERCURIO> show ldp session
  Address           State       Connection     Hold time  Adv. Mode
72.16.44.44         Operational  Open             21         DU
72.16.55.55         Operational  Open             21         DU
```

```
root@PE_SEDE_VENUS> show ldp neighbor
Address            Interface          Label space ID         Hold time
72.16.4.1          ge-0/0/2.0         72.16.55.55:0            12
72.16.6.1          ge-0/0/3.0         72.16.22.22:0            11

root@PE_SEDE_VENUS> show ldp session
  Address           State       Connection     Hold time  Adv. Mode
72.16.22.22         Operational  Open             20         DU
72.16.55.55         Operational  Open             20         DU
```

```
root@PE_SEDE_MARTE> show ldp neighbor
Address            Interface          Label space ID         Hold time
72.16.3.1          ge-0/0/2.0         72.16.55.55:0            11
72.16.5.1          ge-0/0/3.0         72.16.11.11:0            13

root@PE_SEDE_MARTE> show ldp session
  Address           State       Connection     Hold time  Adv. Mode
72.16.11.11         Operational  Open             28         DU
72.16.55.55         Operational  Open             24         DU
```

```
root@PE_SEDE_TIERRA> show ldp neighbor
Address            Interface          Label space ID         Hold time
72.16.1.1          ge-0/0/2.0         72.16.55.55:0            14
72.16.5.2          ge-0/0/3.0         72.16.33.33:0            10

root@PE_SEDE_TIERRA> show ldp session
  Address           State       Connection     Hold time  Adv. Mode
72.16.33.33         Operational  Open             28         DU
72.16.55.55         Operational  Open             23         DU
```

```
root@P_RR_JUPITER> show ldp neighbor
Address            Interface          Label space ID         Hold time
72.16.1.2          ge-0/0/1.0         72.16.11.11:0            12
72.16.2.2          ge-0/0/2.0         72.16.22.22:0            10
72.16.3.2          ge-0/0/3.0         72.16.33.33:0            12
72.16.4.2          ge-0/0/4.0         72.16.44.44:0            12

root@P_RR_JUPITER> show ldp session
  Address           State       Connection     Hold time  Adv. Mode
72.16.11.11         Operational  Open             26         DU
72.16.22.22         Operational  Open             22         DU
```

```
72.16.33.33         Operational  Open             26         DU
72.16.44.44         Operational  Open             22         DU
```

Ahora se revisa que la base de datos de ISIS contenga todos los enrutadores de la red. Como todos los enrutadores hacen parte de la misma área (49.1111) basta con revisar la base de datos de uno de los enrutadores:

```
root@PE_SEDE_TIERRA> show isis database
IS-IS level 1 link-state database:
LSP ID                  Sequence Checksum Lifetime Attributes
PE SEDE TIERRA.00-00         0x5   0x11d8     1155 L1 L2
  1 LSPs

IS-IS level 2 link-state database:
LSP ID                  Sequence Checksum Lifetime Attributes
P RR JUPITER.00-00           0x9   0x88f1      716 L1 L2
PE_SEDE_TIERRA.00-00         0x7   0xe8b7      831 L1 L2
PE SEDE MERCURIO.00-00       0x7   0xcda3      775 L1 L2
PE SEDE MARTE.00-00          0x7   0x99c9      696 L1 L2
PE SEDE VENUS.00-00          0x7   0xac11      726 L1 L2
  5 LSPs
```

También se observa que las interfaces que no están directamente conectadas y las interfaces Loopback son alcanzables por todos los enrutadores a través del protocolo ISIS. Por simplicidad se revisa la tabla de enrutamiento de uno de los enrutadores:

```
root@P_RR_JUPITER> show route protocol isis

inet.0: 17 destinations, 17 routes (17 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

72.16.5.0/30       *[IS-IS/18] 00:59:04, metric 20
                    > to 72.16.1.2 via ge-0/0/1.0
                      to 72.16.3.2 via ge-0/0/3.0
72.16.6.0/30       *[IS-IS/18] 00:59:05, metric 20
                    > to 72.16.2.2 via ge-0/0/2.0
                      to 72.16.4.2 via ge-0/0/4.0
72.16.11.11/32     *[IS-IS/18] 00:59:04, metric 10
                    > to 72.16.1.2 via ge-0/0/1.0
72.16.22.22/32     *[IS-IS/18] 00:59:05, metric 10
                    > to 72.16.2.2 via ge-0/0/2.0
72.16.33.33/32     *[IS-IS/18] 00:59:09, metric 10
                    > to 72.16.3.2 via ge-0/0/3.0
72.16.44.44/32     *[IS-IS/18] 00:59:34, metric 10
                    > to 72.16.4.2 via ge-0/0/4.0
```

Por último se verifica que exista asignación de etiquetas MPLS para todas las interfaces Loopback que son alcanzables por cada enrutador. Por simplicidad, la verificación se hace en uno de los enrutadores, sin embargo, la base de datos es similar en los demás enrutadores.

```
root@PE_SEDE_MARTE> show ldp database
Input label database, 72.16.33.33:0--72.16.11.11:0
  Label     Prefix
      3      72.16.11.11/32
 299808      72.16.22.22/32
 299776      72.16.33.33/32
 299824      72.16.44.44/32
 299792      72.16.55.55/32

Output label database, 72.16.33.33:0--72.16.11.11:0
  Label     Prefix
 299776      72.16.11.11/32
 299808      72.16.22.22/32
      3      72.16.33.33/32
 299824      72.16.44.44/32
 299792      72.16.55.55/32

Input label database, 72.16.33.33:0--72.16.55.55:0
  Label     Prefix
 299824      72.16.11.11/32
 299792      72.16.22.22/32
 299808      72.16.33.33/32
```

```
 299776      72.16.44.44/32
      3      72.16.55.55/32

Output label database, 72.16.33.33:0--72.16.55.55:0
  Label     Prefix
 299776      72.16.11.11/32
 299808      72.16.22.22/32
      3      72.16.33.33/32
 299824      72.16.44.44/32
 299792      72.16.55.55/32
```

Para el desarrollo del servicio MVPN, es imprescindible que exista previamente una comunicación a nivel Unicast de las direcciones IP de las fuentes del tráfico C-Multicast para que los receptores puedan identificarlas. En el entorno MPLS esta comunicación de rutas se realiza a través de MP-BGP.

Por otra parte, en este escenario también se implementó BGP entre los CE y los PE con lo que todo el enrutamiento de direcciones IP Unicast se realiza a través de BGP.

En este orden de ideas, se verifica que las sesiones BGP estén establecidas tanto entre CE y PE como entre PE y P/RR.

```
root@PE_SEDE_MERCURIO> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.2.2.2             65000        297        296       0       0     2:12:19 Establ
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55          12956        292        294       0       0     2:11:45 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
```

```
root@PE_SEDE_VENUS> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.4.4.2             65000        295        296       0       0     2:12:06 Establ
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55          12956        293        296       0       0     2:12:20 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
```

```
root@PE_SEDE_MARTE> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.3.3.2             65000        299        298       0       0     2:12:27 Establ
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55          12956        293        296       0       0     2:12:23 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
```

```
root@PE_SEDE_TIERRA> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       3          3          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.1.1.2             65000        299        300       0       0     2:13:10 Establ
  VRF-CLIENTE-AZUL.inet.0: 2/2/2/0
72.16.55.55          12956        295        296       0       0     2:12:37 Establ
  bgp.l3vpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.inet.0: 3/3/3/0
```

```
root@P_RR_JUPITER> show bgp summary
Groups: 1 Peers: 4 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       5          5          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
72.16.11.11           12956        297        294       0       0     2:12:41 Establ
  bgp.l3vpn.0: 2/2/2/0
72.16.22.22           12956        295        293       0       0     2:12:19 Establ
  bgp.l3vpn.0: 1/1/1/0
72.16.33.33           12956        296        293       0       0     2:12:30 Establ
  bgp.l3vpn.0: 1/1/1/0
72.16.44.44           12956        297        292       0       0     2:12:32 Establ
  bgp.l3vpn.0: 1/1/1/0
```

Se observa que cada PE aprende cinco rutas del cliente a través de MP-BGP. El PE de la sede Tierra aprende dos rutas del CE de la misma sede y aprende tres rutas de los demás PE a través de su sesión MP-BGP con el P/RR. Los demás PE aprenden una ruta de sus respectivos CE y cuatro rutas de los demás PE a través del P/RR. Por último el P/RR como no tiene sesiones BGP contra algún CE aprende todas las rutas a través de los PE.

A continuación se verifica en cada PE el origen de estas rutas.

```
root@PE_SEDE_MERCURIO> show route table VRF-CLIENTE-AZUL.inet.0 protocol bgp

VRF-CLIENTE-AZUL.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.0/24      *[BGP/170] 02:33:01, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.2.1 via ge-0/0/2.0, Push 16, Push 299824(top)
10.11.11.11/32     *[BGP/170] 02:33:01, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.2.1 via ge-0/0/2.0, Push 16, Push 299824(top)
10.22.22.22/32     *[BGP/170] 02:33:35, localpref 100
                      AS path: 65000 I, validation-state: unverified
                    > to 10.2.2.2 via ge-0/0/1.101
10.33.33.33/32     *[BGP/170] 02:33:01, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.2.1 via ge-0/0/2.0, Push 16, Push 299808(top)
10.44.44.44/32     *[BGP/170] 02:32:59, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.6.2 via ge-0/0/3.0, Push 16
```

```
root@PE_SEDE_VENUS> show route table VRF-CLIENTE-AZUL.inet.0 protocol bgp

VRF-CLIENTE-AZUL.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.0/24      *[BGP/170] 02:34:31, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.4.1 via ge-0/0/2.0, Push 16, Push 299824(top)
10.11.11.11/32     *[BGP/170] 02:34:31, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.4.1 via ge-0/0/2.0, Push 16, Push 299824(top)
10.22.22.22/32     *[BGP/170] 02:34:18, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.6.1 via ge-0/0/3.0, Push 16
10.33.33.33/32     *[BGP/170] 02:34:30, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.4.1 via ge-0/0/2.0, Push 16, Push 299808(top)
10.44.44.44/32     *[BGP/170] 02:34:17, localpref 100
                      AS path: 65000 I, validation-state: unverified
                    > to 10.4.4.2 via ge-0/0/1.101
```

```
root@PE_SEDE_MARTE> show route table VRF-CLIENTE-AZUL.inet.0 protocol bgp

VRF-CLIENTE-AZUL.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.0/24      *[BGP/170] 02:34:38, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.5.1 via ge-0/0/3.0, Push 16
10.11.11.11/32     *[BGP/170] 02:34:38, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.5.1 via ge-0/0/3.0, Push 16
```

```
10.22.22.22/32     *[BGP/170] 02:34:26, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.3.1 via ge-0/0/2.0, Push 16, Push 299792(top)
10.33.33.33/32     *[BGP/170] 02:34:42, localpref 100
                      AS path: 65000 I, validation-state: unverified
                    > to 10.3.3.2 via ge-0/0/1.101
10.44.44.44/32     *[BGP/170] 02:34:25, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.3.1 via ge-0/0/2.0, Push 16, Push 299776(top)
```

```
root@PE_SEDE_TIERRA> show route table VRF-CLIENTE-AZUL.inet.0 protocol bgp

VRF-CLIENTE-AZUL.inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.10.0/24      *[BGP/170] 02:35:38, localpref 100
                      AS path: 65000 I, validation-state: unverified
                    > to 10.1.1.2 via ge-0/0/1.101
10.11.11.11/32     *[BGP/170] 02:35:38, localpref 100
                      AS path: 65000 I, validation-state: unverified
                    > to 10.1.1.2 via ge-0/0/1.101
10.22.22.22/32     *[BGP/170] 02:34:43, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.1.1 via ge-0/0/2.0, Push 16, Push 299792(top)
10.33.33.33/32     *[BGP/170] 02:34:54, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.5.2 via ge-0/0/3.0, Push 16
10.44.44.44/32     *[BGP/170] 02:34:41, localpref 100, from 72.16.55.55
                      AS path: 65000 I, validation-state: unverified
                    > to 72.16.1.1 via ge-0/0/2.0, Push 16, Push 299776(top)
```

Las rutas corresponden a las direcciones IP asignadas a las interfaces Loopback de cada CE más la red 10.10.10/24 correspondiente a las fuentes del tráfico Multicast.

Ahora, se revisan las rutas aprendidas por cada uno de los CE.

```
root@CE_SEDE_TIERRA> show route receive-protocol bgp 10.1.1.1

inet.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.22.22.22/32          10.1.1.1                                12956 12956 I
* 10.33.33.33/32          10.1.1.1                                12956 12956 I
* 10.44.44.44/32          10.1.1.1                                12956 12956 I
```

```
root@CE_SEDE_MERCURIO> show route receive-protocol bgp 10.2.2.1

inet.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.10.10.0/24           10.2.2.1                                12956 12956 I
* 10.11.11.11/32          10.2.2.1                                12956 12956 I
* 10.33.33.33/32          10.2.2.1                                12956 12956 I
* 10.44.44.44/32          10.2.2.1                                12956 12956 I
```

```
root@CE_SEDE_MARTE> show route receive-protocol bgp 10.3.3.1

inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.10.10.0/24           10.3.3.1                                12956 12956 I
* 10.11.11.11/32          10.3.3.1                                12956 12956 I
* 10.22.22.22/32          10.3.3.1                                12956 12956 I
* 10.44.44.44/32          10.3.3.1                                12956 12956 I
```

```
root@CE_SEDE_VENUS> show route receive-protocol bgp 10.4.4.1

inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.10.10.0/24           10.4.4.1                                12956 12956 I
* 10.11.11.11/32          10.4.4.1                                12956 12956 I
* 10.22.22.22/32          10.4.4.1                                12956 12956 I
* 10.33.33.33/32          10.4.4.1                                12956 12956 I
```

Los CE reciben las rutas correspondientes a las direcciones IP de las interfaces Loopback de los demás CE de la red y también la dirección IP de la red donde se

encuentra la fuente, excepto el CE de la sede Tierra que no recibe por BGP la dirección IP de la fuente del tráfico Multicast pues la tiene directamente conectada.

Por último, para confirmar que el escenario Unicast está preparado para permitir la comunicación del escenario Multicast, se realizan pruebas de *ping* y *traceroute* entre todos los CE con posibles receptores y el CE de la sede Tierra que tiene la fuente.

```
root@CE_SEDE_MERCURIO> ping 10.10.10.1 source 10.22.22.22 rapid count 5
PING 10.10.10.1 (10.10.10.1): 56 data bytes
!!!!!
--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.863/34.791/42.046/4.573 ms

root@CE_SEDE_MERCURIO> traceroute 10.10.10.1 source 10.22.22.22
traceroute to 10.10.10.1 (10.10.10.1) from 10.22.22.22, 30 hops max, 40 byte packets
 1  10.2.2.1 (10.2.2.1)  18.532 ms  23.234 ms  17.886 ms
 2  72.16.2.1 (72.16.2.1)  30.054 ms  29.345 ms  28.012 ms
     MPLS Label=299824 CoS=0 TTL=1 S=0
     MPLS Label=16 CoS=0 TTL=1 S=1
 3  10.10.10.1 (10.10.10.1)  53.253 ms  47.453 ms  42.013 ms
```

```
root@CE_SEDE_MARTE> ping 10.10.10.1 source 10.33.33.33 rapid count 5
PING 10.10.10.1 (10.10.10.1): 56 data bytes
!!!!!
--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 19.953/28.203/33.824/4.565 ms

root@CE_SEDE_MARTE> traceroute 10.10.10.1 source 10.33.33.33
traceroute to 10.10.10.1 (10.10.10.1) from 10.33.33.33, 30 hops max, 40 byte packets
 1  10.3.3.1 (10.3.3.1)  20.106 ms  17.033 ms  24.042 ms
 2  10.1.1.1 (10.1.1.1)  29.895 ms  30.460 ms  28.994 ms
 3  10.10.10.1 (10.10.10.1)  29.921 ms  29.476 ms  30.059 ms
```

```
root@CE_SEDE_VENUS> ping 10.10.10.1 source 10.44.44.44 rapid count 5
PING 10.10.10.1 (10.10.10.1): 56 data bytes
!!!!!
--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 24.969/28.902/29.967/1.967 ms

root@CE_SEDE_VENUS> traceroute 10.10.10.1 source 10.44.44.44
traceroute to 10.10.10.1 (10.10.10.1) from 10.44.44.44, 30 hops max, 40 byte packets
 1  10.4.4.1 (10.4.4.1)  21.249 ms  16.578 ms  23.908 ms
 2  72.16.4.1 (72.16.4.1)  30.011 ms  29.217 ms  29.972 ms
     MPLS Label=299824 CoS=0 TTL=1 S=0
     MPLS Label=16 CoS=0 TTL=1 S=1
 3  10.10.10.1 (10.10.10.1)  46.744 ms  39.160 ms  42.213 ms
```

Entorno Multicast con PIM-SSM

Una vez establecido el escenario Unicast, se habilitaron los protocolos Multicast PIM e IGMP.

PIM se habilitó entre los enrutadores PE y CE para permitir el flujo de mensajes de señalización entre fuente y receptores como se muestra a continuación.

```
root@PE_SEDE_TIERRA# set routing-instances VRF-CLIENTE-AZUL protocols pim
interface ge-0/0/1.101 mode sparse

root@PE_SEDE_TIERRA> show pim interfaces instance VRF-CLIENTE-AZUL

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name                Stat Mode IP V State         NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101        Up   S     4 2 NotDR,NotCap       1 0/0           10.1.1.2
lsi.0               Up   SD    4 2 P2P,NotCap         0 0/0
```

```
lsi.0              Up   SD    6 2 P2P,NotCap        0 0/0

root@PE SEDE TIERRA> show pim neighbors instance VRF-CLIENTE-AZUL
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.VRF-CLIENTE-AZUL
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:01:25 10.1.1.2
```

```
root@PE_SEDE_MERCURIO# set routing-instances VRF-CLIENTE-AZUL protocols pim
interface ge-0/0/1.101 mode sparse

root@PE_SEDE_MERCURIO> show pim interfaces instance VRF-CLIENTE-AZUL

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 NotDR,NotCap      1 0/0            10.2.2.2
lsi.0              Up   SD    4 2 P2P,NotCap        0 0/0
lsi.0              Up   SD    6 2 P2P,NotCap        0 0/0

root@PE_SEDE_MERCURIO> show pim neighbors instance VRF-CLIENTE-AZUL
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.VRF-CLIENTE-AZUL
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:01:19 10.2.2.2
```

```
root@PE_SEDE_MARTE# set routing-instances VRF-CLIENTE-AZUL protocols pim
interface ge-0/0/1.101 mode sparse

root@PE_SEDE_MARTE> show pim interfaces instance VRF-CLIENTE-AZUL

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 NotDR,NotCap      1 0/0            10.3.3.2
lsi.0              Up   SD    4 2 P2P,NotCap        0 0/0
lsi.0              Up   SD    6 2 P2P,NotCap        0 0/0

root@PE_SEDE_MARTE> show pim neighbors instance VRF-CLIENTE-AZUL
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.VRF-CLIENTE-AZUL
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:01:12 10.3.3.2
```

```
root@PE_SEDE_VENUS# set routing-instances VRF-CLIENTE-AZUL protocols pim
interface ge-0/0/1.101 mode sparse

root@PE_SEDE_VENUS> show pim interfaces instance VRF-CLIENTE-AZUL

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 NotDR,NotCap      1 0/0            10.4.4.2
lsi.0              Up   SD    4 2 P2P,NotCap        0 0/0
lsi.0              Up   SD    6 2 P2P,NotCap        0 0/0

root@PE_SEDE_VENUS> show pim neighbors instance VRF-CLIENTE-AZUL
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.VRF-CLIENTE-AZUL
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:01:06 10.4.4.2
```

```
root@CE_SEDE_TIERRA# set protocols pim interface ge-0/0/1.101 mode sparse
```

```
root@CE_SEDE_TIERRA# set protocols pim interface ge-0/0/2.101 mode sparse

root@CE_SEDE_TIERRA> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 DR,NotCap         1 0/0            10.1.1.2
ge-0/0/2.101       Up   S     4 2 DR,NotCap         0 0/0            10.10.10.1

root@CE_SEDE_TIERRA> show pim neighbors
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.master
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:02:20 10.1.1.1
```

```
root@CE_SEDE_MERCURIO# set protocols igmp interface ge-0/0/1.101 disable

root@CE_SEDE_MERCURIO> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 DR,NotCap         1 0/0            10.2.2.2

root@CE_SEDE_MERCURIO> show pim neighbors
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.master
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:02:20 10.2.2.1
```

```
root@CE_SEDE_MARTE# set protocols pim interface ge-0/0/1.101 mode sparse

root@CE_SEDE_MARTE> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 DR,NotCap         1 0/0            10.3.3.2

root@CE_SEDE_MARTE> show pim neighbors
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.master
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:02:21 10.3.3.1
```

```
root@CE_SEDE_VENUS# set protocols pim interface ge-0/0/1.101 mode sparse

root@CE_SEDE_VENUS> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ge-0/0/1.101       Up   S     4 2 DR,NotCap         1 0/0            10.4.4.2

root@CE_SEDE_VENUS> show pim neighbors
B = Bidirectional Capable, G = Generation Identifier
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: PIM.master
Interface           IP V Mode        Option       Uptime Neighbor addr
ge-0/0/1.101         4 2             HPLGT      00:02:24 10.4.4.1
```

Se observa que las vecindades a nivel PIM se encuentran establecidas entre los CE y los PE, y el proceso PIM identifica que las interfaces que tiene asociadas son las de la interconexión entre PE y CE, excepto en el CE de la sede Tierra que también identifica la interfaz que conecta con la fuente. Vale la pena indicar que las LSI (Label Switched Interface) son interfaces virtuales asociadas a la instancia VPN en los PE.

Posteriormente se habilitó IGMP únicamente en las interfaces que conectaban a los CE con los receptores.

```
root@CE_SEDE_VENUS# set protocols igmp interface ge-0/0/2.104 version 3

[edit]
root@CE_SEDE_VENUS# set protocols igmp interface ge-0/0/2.104 static group
239.1.1.1 source 10.10.10.10

[edit]

root@CE_SEDE_VENUS> show igmp group 239.1.1.1
Interface: ge-0/0/2.104, Groups: 1
    Group: 239.1.1.1
        Group mode: Include
        Source: 10.10.10.10
        Last reported by: Local
        Timeout:       0 Type: Static
```

```
root@CE_SEDE_MARTE# set protocols igmp interface ge-0/0/2.103 version 3

[edit]
root@CE_SEDE_MARTE# set protocols igmp interface ge-0/0/2.103 static group
239.1.1.1 source 10.10.10.10

[edit]
root@CE_SEDE_MARTE# set protocols igmp interface ge-0/0/2.103 static group
239.1.1.10 source 10.10.10.10

[edit]

root@CE_SEDE_MARTE> show igmp group 239.1.1.1
Interface: ge-0/0/2.103, Groups: 2
    Group: 239.1.1.1
        Group mode: Include
        Source: 10.10.10.10
        Last reported by: Local
        Timeout:       0 Type: Static

root@CE_SEDE_MARTE> show igmp group 239.1.1.10
Interface: ge-0/0/2.103, Groups: 2
    Group: 239.1.1.10
        Group mode: Include
        Source: 10.10.10.10
        Last reported by: Local
        Timeout:       0 Type: Static
```

Se observa que en el CE de la sede Venus se habilitó a través de IGMP un receptor para el grupo 239.1.1.1 y en el CE Marte se habilitó el receptor para dos grupos el 239.1.1.1 y 239.1.1.10.

Hasta este punto se ha verificado la configuración de los protocolos Multicast en el escenario IP tradicional, sin embargo, para permitir el flujo de tráfico Multicast entre los CE es necesario habilitar el servicio MVPN en la red MPLS. A continuación se describe el proceso de habilitación y de verificación de operatividad en el interior de la red.

Como primer paso se habilitó la NLRI AFI =1, SAFI = 5, para permitir el intercambio de rutas Multicast en la red y se verificó que las sesiones establecieran tanto la NLRI Unicast (establecida previamente) como la NLRI Multicast.

```
root@PE_SEDE_TIERRA# set protocols bgp group RR family inet-mvpn signaling

root@PE_SEDE_TIERRA# set routing-instances VRF-CLIENTE-AZUL protocols mvpn

root@PE_SEDE_TIERRA> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       3          3          0          0          0          0
bgp.mvpn.0
                       3          3          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.1.1.2             65000        396        412       0       0     2:57:11 Establ
  VRF-CLIENTE-AZUL.inet.0: 2/2/2/0
72.16.55.55          12956        165        156       0       1       33:58 Establ
  bgp.l3vpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.inet.0: 3/3/3/0
  bgp.mvpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.mvpn.0: 3/3/3/0
```

```
root@PE_SEDE_MERCURIO# set protocols bgp group RR family inet-mvpn signaling

root@PE_SEDE_MERCURIO# set routing-instances VRF-CLIENTE-AZUL protocols mvpn

root@PE_SEDE_MERCURIO> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
bgp.mvpn.0
                       3          3          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.2.2.2             65000         79         81       0       1       34:18 Establ
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55          12956        162        157       0       1       34:14 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
  bgp.mvpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.mvpn.0: 3/3/3/0
```

```
root@PE_SEDE_MARTE# set protocols bgp group RR family inet-mvpn signaling

root@PE_SEDE_MARTE# set routing-instances VRF-CLIENTE-AZUL protocols mvpn

root@PE_SEDE_MARTE> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
bgp.mvpn.0
                       3          3          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.3.3.2             65000        399        413       0       0     2:58:09 Establ
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55          12956        163        158       0       1       34:18 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
  bgp.mvpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.mvpn.0: 3/3/3/0
```

```
root@PE_SEDE_VENUS# set protocols bgp group RR family inet-mvpn signaling

root@PE_SEDE_VENUS# set routing-instances VRF-CLIENTE-AZUL protocols mvpn

root@PE_SEDE_VENUS> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       4          4          0          0          0          0
bgp.mvpn.0
                       3          3          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.4.4.2             65000        401        419       0       0     2:58:54 Establ
```

```
  VRF-CLIENTE-AZUL.inet.0: 1/1/1/0
72.16.55.55           12956        163        157       0       1       34:25 Establ
  bgp.l3vpn.0: 4/4/4/0
  VRF-CLIENTE-AZUL.inet.0: 4/4/4/0
  bgp.mvpn.0: 3/3/3/0
  VRF-CLIENTE-AZUL.mvpn.0: 3/3/3/0
```

```
root@P_RR_JUPITER# set protocols bgp group RR-CLIENTES family inet-mvpn
signaling

root@P_RR_JUPITER> show bgp summary
Groups: 1 Peers: 4 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l3vpn.0
                       5          5          0          0          0          0
bgp.mvpn.0
                       4          4          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
72.16.11.11           12956         94         95       0       2       40:02 Establ
  bgp.l3vpn.0: 2/2/2/0
  bgp.mvpn.0: 1/1/1/0
72.16.22.22           12956         94         97       0       2       40:06 Establ
  bgp.l3vpn.0: 1/1/1/0
  bgp.mvpn.0: 1/1/1/0
72.16.33.33           12956         94         95       0       2       40:02 Establ
  bgp.l3vpn.0: 1/1/1/0
  bgp.mvpn.0: 1/1/1/0
72.16.44.44           12956         94         96       0       2       40:02 Establ
  bgp.l3vpn.0: 1/1/1/0
  bgp.mvpn.0: 1/1/1/0
```

La existencia de rutas pertenecientes a la tabla bgp.mvpn.0 confirma que la NLRI AFI=1 SAFI=5 ha sido establecida.

Se verifica entonces que todos los PE se reconozcan entre sí como vecinos de la instancia MVPN.

```
root@PE_SEDE_TIERRA> show mvpn neighbor inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  Neighbor                               Inclusive Provider Tunnel
  72.16.22.22
  72.16.33.33
  72.16.44.44
```

```
root@PE_SEDE_MERCURIO> show mvpn neighbor inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  Neighbor                               Inclusive Provider Tunnel
  72.16.11.11
  72.16.33.33
  72.16.44.44
```

```
root@PE_SEDE_MARTE> show mvpn neighbor inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
```

```
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  Neighbor                                Inclusive Provider Tunnel
  72.16.11.11
  72.16.22.22
  72.16.44.44
```

```
root@PE_SEDE_VENUS> show mvpn neighbor inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  Neighbor                                Inclusive Provider Tunnel
  72.16.11.11
  72.16.22.22
  72.16.33.33
```

Esta vecindad es producto del intercambio de rutas de autodescubrimiento tipo 1 *Intra-AS I-PMSI* que se describe a continuación, por simplicidad se muestra el intercambio de rutas a nivel MP-BGP del PE de la sede Tierra, sin embargo, ese mismo intercambio se da en todos los PE.

```
root@PE_SEDE_TIERRA> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn.0

VRF-CLIENTE-AZUL.mvpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  1:72.16.11.11:1:72.16.11.11/240
*                         Self                         100        I

root@PE_SEDE_TIERRA> show route receive-protocol bgp 72.16.55.55 table VRF-
CLIENTE-AZUL.mvpn.0

VRF-CLIENTE-AZUL.mvpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  1:72.16.22.22:1:72.16.22.22/240
*                         72.16.22.22                  100        I
  1:72.16.33.33:1:72.16.33.33/240
*                         72.16.33.33                  100        I
  1:72.16.44.44:1:72.16.44.44/240
*                         72.16.44.44                  100        I
```

En la Figura 30 se observa el formato de la ruta Tipo 1.

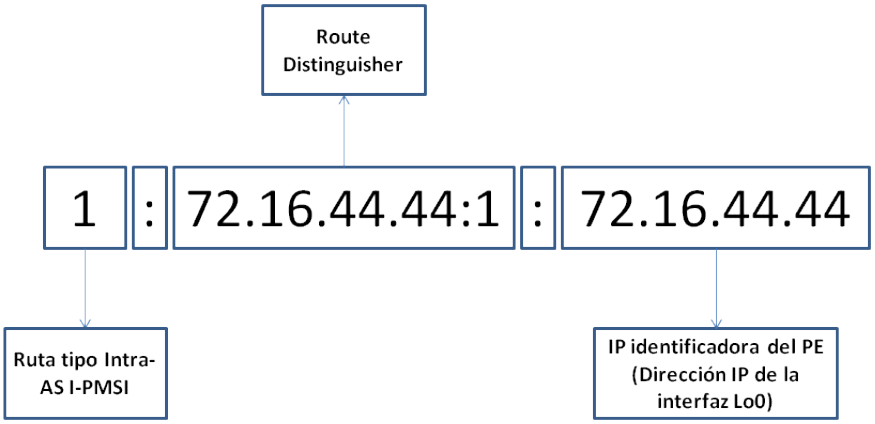

Figura 30. Formato de la ruta tipo 1 Intra-AS Auto-Discovery

Hasta este punto se han descubierto todos los PE que participan en la MVPN, el paso que sigue es permitir que el plano de transporte se establezca, en este caso se usarán túneles inclusivos MPLS P2MP a través de señalización RSVP-TE.

Se habilita el establecimiento del túnel P2MP en el PE de la sede Tierra (que es el que ofrece servicio a la fuente del tráfico Multicast) hacia los demás PE que han sido descubiertos. A continuación se comprueba el establecimiento del túnel P2MP.

```
root@PE_SEDE_TIERRA# set routing-instances VRF-CLIENTE-AZUL provider-tunnel
rsvp-te label-switched-path-template default-template

root@PE_SEDE_TIERRA> show rsvp session p2mp detail
Ingress RSVP: 3 sessions
P2MP name: 72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, P2MP branch count: 3

72.16.22.22
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 299856
--- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 1, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.1.1 (ge-0/0/2.0) 898 pkts
  RESV rcvfrom: 72.16.1.1 (ge-0/0/2.0) 898 pkts
---- more ---

72.16.33.33
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.33.33:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
---- more ---
  Resv style: 1 SE, Label in: -, Label out: 16
---- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 2, Subgroup Originator: 72.16.11.11
---- more ---
  PATH sentto: 72.16.5.2 (ge-0/0/3.0) 897 pkts
  RESV rcvfrom: 72.16.5.2 (ge-0/0/3.0) 898 pkts
---- more ---

72.16.44.44
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
---- more ---
  Resv style: 1 SE, Label in: -, Label out: 299856
---- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 3, Subgroup Originator: 72.16.11.11
---- more ---
  PATH sentto: 72.16.1.1 (ge-0/0/2.0) 897 pkts
  RESV rcvfrom: 72.16.1.1 (ge-0/0/2.0) 897 pkts
---- more ---
Total 3 displayed, Up 3, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

Se destaca que las etiquetas asignadas tanto al sub-LSP hacia el PE Venus como el destinado al PE Mercurio son las mismas (299856) pues utilizan el mismo enlace, el que interconecta el PE Tierra con el P/RR Júpiter, mientras que el sub-LSP hacia el PE Marte utiliza otra etiqueta, pues es transportado por la interfaz que interconecta a los dos PE sin pasar por el P/RR Júpiter. También se destaca el ítem "*port number*" 64298 que corresponde al objeto especial de RSVP llamado *P2MP LSP SESSION* que permite asociar todos los sub-LSP a un mismo LSP P2MP.

La creación del túnel MPLS P2MP también afecta las rutas de autodescubrimiento, que ahora incluyen el identificador del túnel, como se muestra a continuación.

```
root@PE_SEDE_TIERRA> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
* 1:72.16.11.11:1:72.16.11.11/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10
     PMSI: Flags 0x0: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64298:72.16.11.11]
```

El identificador del túnel es el mismo valor que tiene el objeto especial *P2MP LSP SESSION* descrito previamente, con lo que se ha permitido la asociación del túnel inclusivo a la MVPN.

Señalización C-Multicast

Una vez establecida la infraestructura de transporte para el tráfico Multicast, se procede a habilitar la generación y recepción de tráfico.

En el apartado relacionado con la habilitación de los protocolos de Multicast y específicamente en el caso de IGMP, los enrutadores CE Marte y Venus fueron configurados para forzar la recepción del tráfico Multicast y simular así un receptor en la red LAN de cada sede.

Esta configuración hace que los CE generen mensajes *PIM Join* hacia sus respectivos PE con los que tienen establecidas vecindades PIM.

```
root@CE_SEDE_MARTE> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse
    Upstream interface: ge-0/0/1.101

Group: 239.1.1.10
    Source: 10.10.10.10
    Flags: sparse
    Upstream interface: ge-0/0/1.101

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

```
root@CE_SEDE_VENUS> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse
    Upstream interface: ge-0/0/1.101

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

Se observa que el CE Marte genera mensajes de *PIM Join* para los grupos Multicast 239.1.1.1 y 239.1.1.10 mientras que el CE Venus solo los genera para el grupo 239.1.1.1. en los dos casos la fuente es la misma (10.10.10.10).

Se verifica que estos mensajes de *PIM Join* sean recibidos por los respectivos PE.

```
root@PE_SEDE_MARTE> show pim join instance VRF-CLIENTE-AZUL
Instance: PIM.VRF-CLIENTE-AZUL Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse
    Upstream protocol: BGP
    Upstream interface: Through BGP

Group: 239.1.1.10
    Source: 10.10.10.10
    Flags: sparse
    Upstream protocol: BGP
    Upstream interface: Through BGP

Instance: PIM.VRF-CLIENTE-AZUL Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

```
root@PE_SEDE_VENUS> show pim join instance VRF-CLIENTE-AZUL
Instance: PIM.VRF-CLIENTE-AZUL Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse
    Upstream protocol: BGP
    Upstream interface: Through BGP

Instance: PIM.VRF-CLIENTE-AZUL Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

Para permitir que los mensajes de *Join* se propagaran al interior de la red MPLS fue necesario habilitar el grupo Multicast ya que los PE Juniper por defecto tienen permitidos las IP recomendadas por la IETF para ser usadas en los grupos SSM que están en el rango de 232.0.0.0 a 232.255.255.255 [38]. Después de habilitar los grupos SSM en el rango 239.1.0.0 a 239.1.255.255, se verificó que los *PIM Join* provenientes de los CE se tradujeran a rutas MP-BGP tipo 7 *Source Tree Join*, los componentes de las rutas tipo 7 se describen en la Figura 31.

```
root@PE_SEDE_MARTE# set routing-instances VRF-CLIENTE-AZUL routing-options
multicast ssm-groups 239.1/16

root@PE_SEDE_MARTE> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive | find 7:
* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6

* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.10/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6
```

```
root@PE_SEDE_VENUS# set routing-instances VRF-CLIENTE-AZUL routing-options
multicast ssm-groups 239.1/16

root@PE_SEDE_VENUS> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive | find 7:
* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6
```

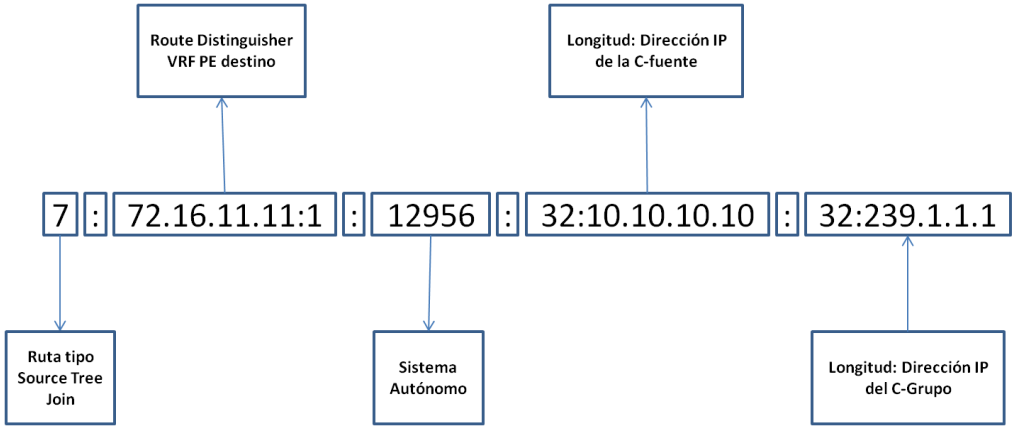

Figura 31. Formato de la ruta tipo 7 C-Multicast Source Tree Join

Se observa que se anuncia una ruta MP-BGP tipo 7 asociada a cada grupo Multicast. En este anuncio de rutas tipo 7, uno de los parámetros más importante es el RT 72.16.11.11:6 que proviene de una nueva comunidad extendida denominada *rt-import* y que es asociada a las rutas Unicast de la MVPN anunciadas por todos los PE, una vez se habilita la VPN para proporcionar servicios Multicast, en este caso particular corresponde a las rutas anunciadas por el PE Tierra que tiene la fuente directamente conectada.

A continuación, se incluyen los anuncios por el PE Tierra identificando las nuevas comunidades extendidas asociadas a las rutas Unicast

```
root@PE_SEDE_TIERRA> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.inet.0 extensive | match "routes|entry|communities"

VRF-CLIENTE-AZUL.inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
* 10.10.10.0/24 (1 entry, 1 announced)
     Communities: target:12956:10 src-as:12956:0 rt-import:72.16.11.11:6
* 10.11.11.11/32 (1 entry, 1 announced)
     Communities: target:12956:10 src-as:12956:0 rt-import:72.16.11.11:6
```

Volviendo al anuncio de la ruta Tipo 7 hecho por los PE con receptores Marte y Venus, al incluir el RT 72.16.11.11:6, aseguran que únicamente el PE Tierra importará la ruta en la VPN Azul los demás PE de la VPN la ignorarán.

Una vez recibida la ruta tipo 7 por el PE Tierra, este la convierte en mensajes *PIM Join* enviados hacia el CE.

```
root@PE_SEDE_TIERRA> show pim join instance VRF-CLIENTE-AZUL extensive
Instance: PIM.VRF-CLIENTE-AZUL Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse,spt
    Upstream interface: ge-0/0/1.101
    Upstream neighbor: 10.1.1.2
    Upstream state: Join to Source
    Keepalive timeout:
    Uptime: 03:03:37
    Downstream neighbors:
```

```
        Interface: Pseudo-MVPN
            Uptime: 03:03:37 Time since last Join: 03:03:37
    Number of downstream interfaces: 1

Group: 239.1.1.10
    Source: 10.10.10.10
    Flags: sparse,spt
    Upstream interface: ge-0/0/1.101
    Upstream neighbor: 10.1.1.2
    Upstream state: Join to Source
    Keepalive timeout:
    Uptime: 03:02:41
    Downstream neighbors:
        Interface: Pseudo-MVPN
            Uptime: 03:02:41 Time since last Join: 03:02:41
    Number of downstream interfaces: 1

Instance: PIM.VRF-CLIENTE-AZUL Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

```
root@CE_SEDE_TIERRA> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
    Source: 10.10.10.10
    Flags: sparse
    Upstream interface: ge-0/0/2.101
    Upstream neighbor: Direct
    Upstream state: Local Source
    Keepalive timeout:
    Uptime: 04:26:48
    Downstream neighbors:
        Interface: ge-0/0/1.101
            10.1.1.1 State: Join Flags: S Timeout: 162
            Uptime: 04:26:48 Time since last Join: 00:00:48
    Number of downstream interfaces: 1

Group: 239.1.1.10
    Source: 10.10.10.10
    Flags: sparse
    Upstream interface: ge-0/0/2.101
    Upstream neighbor: Direct
    Upstream state: Local Source
    Keepalive timeout:
    Uptime: 04:25:52
    Downstream neighbors:
        Interface: ge-0/0/1.101
            10.1.1.1 State: Join Flags: S Timeout: 162
            Uptime: 04:25:52 Time since last Join: 00:00:48
    Number of downstream interfaces: 1

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

Se observa que tanto el CE como el PE de la sede Tierra detectan dos *PIM Join* uno para cada grupo, esto se debe a que el P/RR Júpiter sólo transmite un anuncio por ruta tipo 7 de MP-BGP y para este enrutador las rutas se diferencian por el grupo Multicast por este motivo, aunque recibe dos rutas tipo 7 para el grupo 239.1.1.1, una proveniente del PE Venus y otra del PE Marte, el P/RR únicamente anuncia una al PE Tierra, como se observa a continuación.

```
root@P_RR_JUPITER> show route receive-protocol bgp 72.16.44.44 table
bgp.mvpn.0

bgp.mvpn.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  1:72.16.44.44:1:72.16.44.44/240
*                         72.16.44.44                  100        I
  7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240
*                         72.16.44.44                  100        I

root@P_RR_JUPITER> show route receive-protocol bgp 72.16.33.33 table
bgp.mvpn.0

bgp.mvpn.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  1:72.16.33.33:1:72.16.33.33/240
*                         72.16.33.33                  100        I
  7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240
                          72.16.33.33                  100        I
```

```
  7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.10/240
*                         72.16.33.33                 100        I

root@P_RR_JUPITER> show route advertising-protocol bgp 72.16.11.11 table
bgp.mvpn.0

bgp.mvpn.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  1:72.16.22.22:1:72.16.22.22/240
*                         72.16.22.22                 100        I
  1:72.16.33.33:1:72.16.33.33/240
*                         72.16.33.33                 100        I
  1:72.16.44.44:1:72.16.44.44/240
*                         72.16.44.44                 100        I
  7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240
*                         Self                        100        I
  7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.10/240
*                         Self                        100        I
```

Habilitación del tráfico Multicast

Una vez verificado que la señalización C-Multicast se ha intercambiado entre los extremos y que el plano de transporte se estableció a través de túneles inclusivos, se procedió a generar tráfico Multicast desde las fuentes, esto se logró a través del establecimiento de un par de pings desde la fuente con dirección destino los dos grupos Multicast 239.1.1.1 y 239.1.1.10 como se muestra a continuación.

```
root@TX_RX> ping 239.1.1.1 ttl 10 interface ge-0/0/1.101 bypass-routing
interval 0.1
PING 239.1.1.1 (239.1.1.1): 56 data bytes

root@TX_RX> ping 239.1.1.10 ttl 10 interface ge-0/0/1.101 bypass-routing
interval 0.1
PING 239.1.1.10 (239.1.1.10): 56 data bytes
```

Posteriormente se revisó que el CE Tierra estuviese enviando el tráfico Multicast de los dos grupos hacia el PE Tierra.

```
root@CE_SEDE_TIERRA> show Multicast route extensive | match "Group:|pps"
Group: 239.1.1.1
    Statistics: 1 kBps, 9 pps, 1937 packets
Group: 239.1.1.10
    Statistics: 1 kBps, 9 pps, 1132 packets

root@CE SEDE TIERRA> show Multicast route
Instance: master Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/2.101
    Downstream interface list:
        ge-0/0/1.101

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/2.101
    Downstream interface list:
        ge-0/0/1.101

Instance: master Family: INET6

root@CE SEDE TIERRA> show Multicast route extensive | match "Group:|pps"
Group: 239.1.1.1
    Statistics: 1 kBps, 9 pps, 3717 packets
Group: 239.1.1.10
    Statistics: 1 kBps, 9 pps, 2912 packets
```

Ahora se verifica que el PE Tierra esté reenviando el tráfico Multicast por el túnel inclusivo establecido previamente.

```
root@PE_SEDE_TIERRA> show Multicast route instance VRF-CLIENTE-AZUL
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
```

```
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/3.0 ge-0/0/2.0

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/3.0 ge-0/0/2.0

Instance: VRF-CLIENTE-AZUL Family: INET6
```

root@PE_SEDE_TIERRA> show mvpn c-Multicast inet instance-name VRF-CLIENTE-AZUL

```
MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  C-mcast IPv4 (S:G)            Provider Tunnel                          St
  10.10.10.10/32:239.1.1.1/32   RSVP-TE P2MP:72.16.11.11, 64298,72.16.11.11         RM
  10.10.10.10/32:239.1.1.10/32  RSVP-TE P2MP:72.16.11.11, 64298,72.16.11.11         RM
```

root@PE_SEDE_TIERRA> show route table VRF-CLIENTE-AZUL.inet.1

```
VRF-CLIENTE-AZUL.inet.1: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

224.0.0.0/4        *[Multicast/180] 2d 04:07:38
                      MultiResolve
224.0.0.0/24       *[Multicast/180] 2d 04:07:38
                      MultiDiscard
232.0.0.0/8        *[Multicast/180] 2d 04:07:38
                      MultiResolve
239.1.0.0/16       *[Multicast/180] 10:40:42
                      MultiResolve
239.1.1.1,10.10.10.10/32*[MVPN/70] 06:09:23
                     > to 72.16.5.2 via ge-0/0/3.0, Push 16
                       to 72.16.1.1 via ge-0/0/2.0, Push 299856
239.1.1.10,10.10.10.10/32*[MVPN/70] 06:08:27
                     > to 72.16.5.2 via ge-0/0/3.0, Push 16
                       to 72.16.1.1 via ge-0/0/2.0, Push 299856
```

root@PE_SEDE_TIERRA> show rsvp session statistics

```
Ingress RSVP: 3 sessions
To              From            State     Packets            Bytes LSPname
72.16.22.22     72.16.11.11     Up          30143          2652584
72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up          30143          2652584
72.16.33.33:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.44.44     72.16.11.11     Up          30143          2652584
72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
Total 3 displayed, Up 3, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

root@PE_SEDE_TIERRA> show interfaces ge-0/0/2 statistics | match pps

```
  Input rate     : 488 bps (1 pps)
  Output rate    : 13592 bps (19 pps)
```

root@PE_SEDE_TIERRA> show interfaces ge-0/0/3 statistics | match pps

```
  Input rate     : 272 bps (0 pps)
  Output rate    : 13440 bps (18 pps)
```

Como se indicó en el apartado de entorno Multicast, se señalizaron tres sub-LSP uno para cada PE, sin embargo dos de ellos, el del PE Mercurio y el del PE Venus comparten el mismo enlace físico hacia el enrutador P/RR Júpiter, con lo que a pesar de ver que las estadísticas de los tres sub-LSP registran la misma cantidad de paquetes conmutados, al revisar las estadísticas de las interfaces físicas, a través de la interfaz que interconecta el PE Tierra con el P/RR Júpiter solo se envía una copia de los

paquetes que es el principal objetivo de los Túneles P2MP, evitar la replicación de tráfico por la misma interfaz física.

Siguiendo el recorrido del túnel inclusivo P2MP, se revisan las estadísticas en el PE Marte y se encuentra lo siguiente:

```
root@PE_SEDE_MARTE> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 2d 22:24:43
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_MARTE> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 43675 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 22:36:15

root@PE_SEDE_MARTE> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 42636 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 22:36:30

root@PE_SEDE_MARTE> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 0 bps (0 pps)
  Output rate    : 12048 bps (17 pps)

root@PE_SEDE_MARTE> show interfaces ge-0/0/3 statistics | match pps
  Input rate     : 13072 bps (17 pps)
  Output rate    : 1208 bps (1 pps)
```

Se observa que la etiqueta MPLS con la que recibe el tráfico Multicast proveniente del PE Tierra (16) es eliminada (pop) y el tráfico es enviado a la instancia MVPN, además se observa que el PE Marte recibe tráfico para los dos grupos Multicast (239.1.1.1 y 239.1.1.10), que es de aproximadamente de 9 paquetes por segundo (9 pps) por cada uno y que es conmutado hacia la interfaz que interconecta al PE con el CE Marte (ge-0/0/1.101). Esto se confirma al verificar las estadísticas de tráfico de la interfaces que lo interconectan con el PE Tierra (ge-0/0/3 con 17 pps de entrada) y con el CE Marte (ge-0/0/1 con 17 pps de salida).

Se hace la misma verificación en el equipo P/RR Júpiter y se encuentra lo siguiente:

```
root@P_RR_JUPITER> show route label 299856

mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

299856             *[RSVP/7/2] 2d 03:18:24, metric 1
                    > to 72.16.2.2 via ge-0/0/2.0, Swap 16
                      to 72.16.4.2 via ge-0/0/4.0, Swap 16

root@P_RR_JUPITER> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 12832 bps (18 pps)
  Output rate    : 296 bps (0 pps)

root@P_RR_JUPITER> show interfaces ge-0/0/2 statistics | match pps
  Input rate     : 280 bps (0 pps)
  Output rate    : 13168 bps (18 pps)

root@P_RR_JUPITER> show interfaces ge-0/0/4 statistics | match pps
  Input rate     : 280 bps (0 pps)
  Output rate    : 13024 bps (18 pps)
```

Al revisar la etiqueta MPLS con la que el P/RR recibe el tráfico Multicast proveniente del PE Tierra (299856) en la tabla de conmutación, se observa que es conmutada por la etiqueta 16 (swap) y enviada a las interfaces que interconectan al P/RR con los PE Mercurio y Venus. Esta replicación de tráfico se confirma al revisar las estadísticas de las interfaces que interconectan al P/RR con el PE Tierra (ge-0/0/1 con 18 pps de entrada) y con los PE Mercurio y Venus (ge-0/0/2 y ge-0/0/4 con 18 pps de salida cada una).

Pasando al PE Venus se encuentra que:

```
root@PE_SEDE_VENUS> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 2d 23:06:06
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_VENUS> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 61578 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 23:10:00

root@PE_SEDE_VENUS> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 36484 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 01:06:53

root@PE_SEDE_VENUS> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 0 bps (0 pps)
```

```
  Output rate     : 6008 bps (8 pps)

root@PE_SEDE_VENUS> show interfaces ge-0/0/2 statistics | match pps
  Input rate      : 12592 bps (17 pps)
  Output rate     : 1016 bps (0 pps)
```

Se observa que la etiqueta MPLS con la que recibe el tráfico Multicast proveniente del P/RR Júpiter (16) es eliminada (pop) y el tráfico es enviado a la instancia MVPN, además se observa que el PE Venus recibe tráfico para los dos grupos Multicast (239.1.1.1 y 239.1.1.10) pero descarta el correspondiente al grupo 239.1.1.10, lo que es congruente con lo configurado previamente en el CE Venus donde sólo se forzó a pedir tráfico Multicast de ese grupo. Este tráfico es conmutado hacia la interfaz que interconecta al PE con el CE Venus (ge-0/0/1.101) lo que se confirma al verificar las estadísticas de tráfico de la interfaces que lo interconectan con el P/RR Júpiter (ge-0/0/2 con 17 pps de entrada) y con el CE Venus (ge-0/0/1 con 8 pps de salida).

Posteriormente se realizó la verificación en el PE Mercurio que no tiene asociados receptores que estén interesados en el tráfico Multicast y se encontró lo siguiente:

```
root@PE_SEDE_MERCURIO> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 2d 23:20:58
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_MERCURIO> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 44206 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 01:21:03

root@PE_SEDE_MERCURIO> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 43868 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 01:20:26

root@PE_SEDE_MERCURIO> show interfaces ge-0/0/1 statistics | match pps
  Input rate      : 0 bps (0 pps)
  Output rate     : 0 bps (0 pps)

root@PE_SEDE_MERCURIO> show interfaces ge-0/0/2 statistics | match pps
  Input rate      : 13136 bps (17 pps)
  Output rate     : 416 bps (0 pps)
```

Como ocurre con los PE Marte y Venus, el PE Mercurio elimina la etiqueta MPLS con la que recibe el tráfico Multicast proveniente del P/RR Júpiter (16) y envía el tráfico a la instancia MVPN, además se observa que el PE Venus recibe tráfico para los dos grupos Multicast (239.1.1.1 y 239.1.1.10) pero como era de esperar, lo descarta, pues como se indicó previamente, no tiene receptores asociados, lo que se confirma al verificar las estadísticas de tráfico de la interfaces que lo interconectan con el P/RR Júpiter (ge-0/0/2 con 17 pps de entrada) y con el CE Mercurio (ge-0/0/1 con 0 pps de salida).

Por último, se verificó el comportamiento del tráfico en los CE y en los propios receptores.

```
root@CE_SEDE_MARTE> show Multicast route extensive
Instance: master Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.103
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 1728 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:03:10

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.103
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 1603 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:02:56

Instance: master Family: INET6


root@CE_SEDE_MARTE> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:              160261                 18 pps
     Output packets:                   0                  0 pps

root@CE_SEDE_MARTE> show interfaces ge-0/0/2.103 statistics detail | match
pps
     Input  packets:                   0                  0 pps
     Output packets:              160662                 19 pps
```

```
root@CE_SEDE_MERCURIO> show Multicast route
Instance: master Family: INET

Instance: master Family: INET6

root@CE_SEDE_MERCURIO> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:                   0                  0 pps
     Output packets:                   0                  0 pps
```

```
root@CE_SEDE_VENUS> show Multicast route extensive
Instance: master Family: INET

Group: 239.1.1.1
```

```
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.104
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 1939 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:03:33

Instance: master Family: INET6

root@CE_SEDE_VENUS> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:              81263                    9 pps
     Output packets:                  0                    0 pps

root@CE_SEDE_VENUS> show interfaces ge-0/0/2.104 statistics detail | match
pps
     Input  packets:                  0                    0 pps
     Output packets:              81737                    8 pps
```

```
root@TX_RX> show Multicast route instance RECEPTOR_MARTE extensive
Instance: RECEPTOR MARTE Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.103
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 3192 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:05:51

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.103
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 3067 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:05:37

Instance: RECEPTOR MARTE Family: INET6

root@TX_RX> show Multicast route instance RECEPTOR_VENUS extensive
Instance: RECEPTOR VENUS Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.104
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 3392 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:06:13

Instance: RECEPTOR VENUS Family: INET6
```

El comportamiento es congruente con lo encontrado en los PE, los equipos CE y receptor de la sede Marte reciben el tráfico Multicast de los grupos 239.1.1.1 y 239.1.1.10, por otra parte, los equipos CE y receptor de la sede Venus reciben el tráfico

Multicast destinado al grupo 239.1.1.1 mientras que el CE de la sede Mercurio no recibe tráfico Multicast.

Escenario de túneles selectivos

Hasta este punto ya se ha logrado el intercambio de tráfico C-Multicast entre las sedes del cliente con transmisores asociados y las sedes con receptores interesados, sin embargo, en la red MPLS el tráfico Multicast está siendo recibido por todos los PE de la VPN aunque no tengan receptores interesados, debido a la existencia de los túneles inclusivos.

Para optimizar los recursos de la red y evitar consumo de ancho de banda innecesario, existe la posibilidad de implementar túneles selectivos.

En este caso se habilitó en el PE Tierra la configuración de túneles selectivos para los grupos Multicast comprendidos entre la dirección 239.1.0.0 y la 239.1.255.255, lo que produjo el anuncio de rutas tipo 3 *S-PMSI Auto-Discovery* hacia el P/RR como se describe a continuación:

```
root@PE_SEDE_TIERRA# set routing-instances VRF-CLIENTE-AZUL provider-tunnel
selective group 239.1.0.0/16 source 0.0.0.0/0 rsvp-te label-switched-path-
template default-template

root@PE_SEDE_TIERRA> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 11 destinations, 13 routes (11 active, 2 holddown, 0 hidden)
* 1:72.16.11.11:1:72.16.11.11/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10
     PMSI: Flags 0x0: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64298:72.16.11.11]

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10
     PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64299:72.16.11.11]

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10
     PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64300:72.16.11.11]
```

```
root@PE_SEDE_MARTE> show route receive-protocol bgp 72.16.55.55 table VRF-
CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
* 1:72.16.11.11:1:72.16.11.11/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.11.11:1
     Nexthop: 72.16.11.11
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.11.11
     Communities: target:12956:10
     PMSI: Flags 0x0: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64298:72.16.11.11]
```

```
* 1:72.16.22.22:1:72.16.22.22/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.22.22:1
     Nexthop: 72.16.22.22
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.22.22
     Communities: target:12956:10

* 1:72.16.44.44:1:72.16.44.44/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.44.44:1
     Nexthop: 72.16.44.44
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.44.44
     Communities: target:12956:10

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.11.11:1
     Nexthop: 72.16.11.11
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.11.11
     Communities: target:12956:10
     PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64299:72.16.11.11]

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.11.11:1
     Nexthop: 72.16.11.11
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.11.11
     Communities: target:12956:10
     PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64300:72.16.11.11]

VRF-CLIENTE-AZUL.mvpn-inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

```
root@PE_SEDE_MERCURIO> show route receive-protocol bgp 72.16.55.55 table VRF-
CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
* 1:72.16.11.11:1:72.16.11.11/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.11.11:1
     Nexthop: 72.16.11.11
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.11.11
     Communities: target:12956:10
     PMSI: Flags 0x0: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64298:72.16.11.11]

* 1:72.16.33.33:1:72.16.33.33/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.33.33:1
     Nexthop: 72.16.33.33
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.33.33
     Communities: target:12956:10

* 1:72.16.44.44:1:72.16.44.44/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.44.44:1
     Nexthop: 72.16.44.44
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.44.44
     Communities: target:12956:10

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.11.11:1
     Nexthop: 72.16.11.11
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.11.11
     Communities: target:12956:10
     PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64299:72.16.11.11]

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11/240 (1 entry, 1 announced)
```

```
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.11.11
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.11.11
      Communities: target:12956:10
      PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64300:72.16.11.11]

VRF-CLIENTE-AZUL.mvpn-inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

```
root@PE_SEDE_VENUS> show route receive-protocol bgp 72.16.55.55 table VRF-
CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
* 1:72.16.11.11:1:72.16.11.11/240 (1 entry, 1 announced)
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.11.11
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.11.11
      Communities: target:12956:10
      PMSI: Flags 0x0: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64298:72.16.11.11]

* 1:72.16.22.22:1:72.16.22.22/240 (1 entry, 1 announced)
      Import Accepted
      Route Distinguisher: 72.16.22.22:1
      Nexthop: 72.16.22.22
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.22.22
      Communities: target:12956:10

* 1:72.16.33.33:1:72.16.33.33/240 (1 entry, 1 announced)
      Import Accepted
      Route Distinguisher: 72.16.33.33:1
      Nexthop: 72.16.33.33
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.33.33
      Communities: target:12956:10

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11/240 (1 entry, 1 announced)
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.11.11
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.11.11
      Communities: target:12956:10
      PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64299:72.16.11.11]

* 3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11/240 (1 entry, 1 announced)
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.11.11
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.11.11
      Communities: target:12956:10
      PMSI: Flags 0x1: Label 0: RSVP-TE: Session_13[72.16.11.11:0:64300:72.16.11.11]

VRF-CLIENTE-AZUL.mvpn-inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

Se destaca que existen dos rutas tipo 3, cada una asociada a un grupo Multicast para el que se ha establecido el túnel selectivo. También se observa que se han asignado dos identificadores diferentes al del túnel inclusivo, estos son 64300 para el grupo 239.1.1.10 y 64299 para el grupo 239.1.1.1.

A continuación en la Figura 32 se describe el formato de la ruta tipo 3:

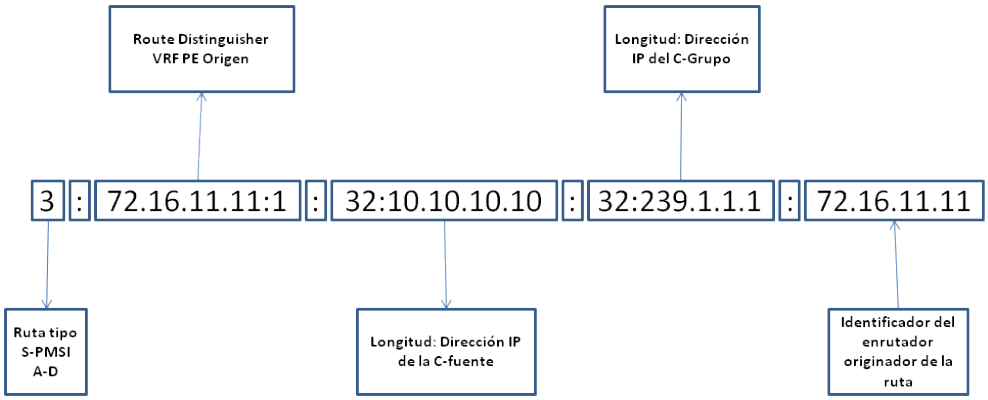

Figura 32. Formato de ruta tipo 3 S-PMSI Auto-Discovery

Posteriormente, se revisa la respuesta de los PE con receptores a través de las rutas tipo 4 *Leaf Auto-Discovery*.

```
root@PE_SEDE_MARTE> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
* 1:72.16.33.33:1:72.16.33.33/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.33.33:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11:72.16.33.33/240 (1 entry, 1
announced)
 BGP group RR type Internal
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:0

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11:72.16.33.33/240 (1 entry, 1
announced)
 BGP group RR type Internal
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:0

* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6

* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.10/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6
```

```
root@PE_SEDE_MERCURIO> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
* 1:72.16.22.22:1:72.16.22.22/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.22.22:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
```

```
     Communities: target:12956:10
```

```
root@PE_SEDE_VENUS> show route advertising-protocol bgp 72.16.55.55 table
VRF-CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
* 1:72.16.44.44:1:72.16.44.44/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.44.44:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:12956:10

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11:72.16.44.44/240 (1 entry, 1
announced)
 BGP group RR type Internal
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:0

* 7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240 (1 entry, 1 announced)
 BGP group RR type Internal
     Route Distinguisher: 72.16.11.11:1
     Nexthop: Self
     Flags: Nexthop Change
     Localpref: 100
     AS path: [12956] I
     Communities: target:72.16.11.11:6
```

```
root@PE_SEDE_TIERRA> show route receive-protocol bgp 72.16.55.55 table VRF-
CLIENTE-AZUL.mvpn extensive

VRF-CLIENTE-AZUL.mvpn.0: 11 destinations, 13 routes (11 active, 2 holddown, 0 hidden)
* 1:72.16.22.22:1:72.16.22.22/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.22.22:1
     Nexthop: 72.16.22.22
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.22.22
     Communities: target:12956:10

* 1:72.16.33.33:1:72.16.33.33/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.33.33:1
     Nexthop: 72.16.33.33
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.33.33
     Communities: target:12956:10

* 1:72.16.44.44:1:72.16.44.44/240 (1 entry, 1 announced)
     Import Accepted
     Route Distinguisher: 72.16.44.44:1
     Nexthop: 72.16.44.44
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.44.44
     Communities: target:12956:10

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11:72.16.33.33/240 (1 entry, 1
announced)
     Import Accepted
     Nexthop: 72.16.33.33
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.33.33
     Communities: target:72.16.11.11:0

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.1:72.16.11.11:72.16.44.44/240 (1 entry, 1
announced)
     Import Accepted
     Nexthop: 72.16.44.44
     Localpref: 100
     AS path: I (Originator)
     Cluster list:  72.16.55.55
     Originator ID: 72.16.44.44
     Communities: target:72.16.11.11:0

* 4:3:72.16.11.11:1:32:10.10.10.10:32:239.1.1.10:72.16.11.11:72.16.33.33/240 (1 entry, 1
announced)
     Import Accepted
```

```
      Nexthop: 72.16.33.33
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.33.33
      Communities: target:72.16.11.11:0

   7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.1/240 (2 entries, 2 announced)
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.55.55
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.55.55
      Communities: target:72.16.11.11:6

   7:72.16.11.11:1:12956:32:10.10.10.10:32:239.1.1.10/240 (2 entries, 2 announced)
      Import Accepted
      Route Distinguisher: 72.16.11.11:1
      Nexthop: 72.16.55.55
      Localpref: 100
      AS path: I (Originator)
      Cluster list:  72.16.55.55
      Originator ID: 72.16.55.55
      Communities: target:72.16.11.11:6

VRF-CLIENTE-AZUL.mvpn-inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

En la Figura 33 se describe el formato de la ruta tipo 4.

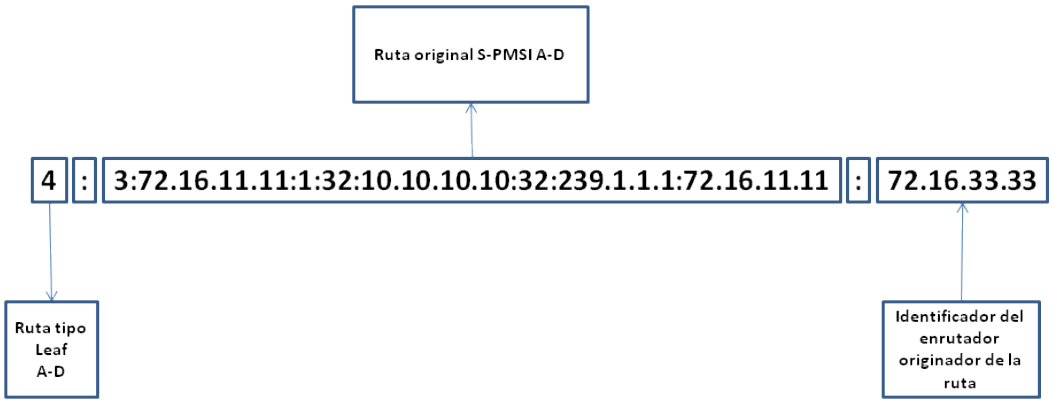

Figura 33. Formato de la ruta Tipo 4 Leaf Auto-Discovery

Se puede entender que las rutas tipo 4 son respuestas a las rutas tipo 3 y permiten identificar a los PE que tienen receptores interesados en recibir el tráfico Multicast, en este caso, se observa que el PE Marte anuncia dos rutas del tipo 4, una por cada grupo Multicast, mientras que el PE Venus anuncia una ruta tipo 4 para el grupo 239.1.1.1 y el PE Mercurio al no tener receptores asociados, no genera rutas del tipo 4.

Es importante destacar, que el PE Tierra recibe todas las rutas del tipo 4 generadas por los PE con receptores asociados, pues al incluir el identificador del enrutador que la genera, no pueden ser agrupadas por el P/RR Júpiter, y las trata como rutas diferentes, anunciándolas de forma independiente al PE Tierra.

Hasta este punto se ha verificado que los PE receptores han expresado su interés de recibir el tráfico Multicast, resta verificar que el túnel selectivo se establece únicamente hacia estos PE.

```
root@PE_SEDE_TIERRA> show mvpn c-Multicast inet instance-name VRF-CLIENTE-
AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  C-mcast IPv4 (S:G)            Provider Tunnel                          St
  10.10.10.10/32:239.1.1.1/32   S-RSVP-TE P2MP:72.16.11.11, 64299,72.16.11.11         RM
  10.10.10.10/32:239.1.1.10/32  S-RSVP-TE P2MP:72.16.11.11, 64300,72.16.11.11         RM
```

```
root@PE_SEDE_TIERRA> show rsvp session p2mp detail
Ingress RSVP: 6 sessions
P2MP name: 72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, P2MP branch count: 3

72.16.22.22
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 299856
--- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 1, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.1.1 (ge-0/0/2.0) 6574 pkts
  RESV rcvfrom: 72.16.1.1 (ge-0/0/2.0) 6574 pkts
--- more ---

72.16.33.33
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.33.33:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 16
--- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 2, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.5.2 (ge-0/0/3.0) 6573 pkts
  RESV rcvfrom: 72.16.5.2 (ge-0/0/3.0) 6573 pkts
--- more ---

72.16.44.44
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 299856
--- more ---
  Port number: sender 1 receiver 64298 protocol 0
  P2MP branch id: 3, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.1.1 (ge-0/0/2.0) 6572 pkts
  RESV rcvfrom: 72.16.1.1 (ge-0/0/2.0) 6573 pkts
--- more ---

72.16.44.44
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.44.44:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 299872
--- more ---
  Port number: sender 1 receiver 64299 protocol 0
  P2MP branch id: 1, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.1.1 (ge-0/0/2.0) 2093 pkts
  RESV rcvfrom: 72.16.1.1 (ge-0/0/2.0) 2093 pkts
--- more ---

72.16.33.33
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.33.33:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 16
--- more ---
  Port number: sender 1 receiver 64299 protocol 0
  P2MP branch id: 2, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.5.2 (ge-0/0/3.0) 2093 pkts
  RESV rcvfrom: 72.16.5.2 (ge-0/0/3.0) 2093 pkts
--- more ---

72.16.33.33
  From: 72.16.11.11, LSPstate: Up, ActiveRoute: 0
  LSPname: 72.16.33.33:72.16.11.11:1:mv2:VRF-CLIENTE-AZUL, LSPpath: Primary
--- more ---
  Resv style: 1 SE, Label in: -, Label out: 16
--- more ---
```

```
  Port number: sender 1 receiver 64300 protocol 0
  P2MP branch id: 1, Subgroup Originator: 72.16.11.11
--- more ---
  PATH sentto: 72.16.5.2 (ge-0/0/3.0) 2093 pkts
  RESV rcvfrom: 72.16.5.2 (ge-0/0/3.0) 2093 pkts
--- more ---
Total 6 displayed, Up 6, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

Se destacan los siguientes aspectos, en primer caso la instancia MVPN solo está utilizando los LSP correspondientes a los túneles selectivos a pesar de que la red haya establecido también el túnel inclusivo. Por otra parte, a diferencia del túnel inclusivo en donde se establece un LSP P2MP con sub-LSP destinados a todos los PE, en el caso de los túneles selectivos se confirma que el LSP asociado al grupo Multicast 239.1.1.1 (con el objeto P2MP *LSP SESSION* igual a 64299) solo establece dos sub-LSP, uno hacia el PE Marte y otro hacia el PE Venus, que son los PE que tienen asociados receptores a ese grupo en particular, mientras que el LSP asociado al grupo Multicast 239.1.1.10 (con P2MP *LSP SESSION* igual a 64300) sólo establece un sub-LSP hacia el PE Marte que es el único PE con receptores asociados a ese grupo.

Ahora se verifica que el PE Tierra esté reenviando el tráfico Multicast por los túneles selectivos establecidos previamente.

```
root@PE_SEDE_TIERRA> show Multicast route instance VRF-CLIENTE-AZUL
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.0 ge-0/0/3.0

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/3.0

Instance: VRF-CLIENTE-AZUL Family: INET6

root@PE_SEDE_TIERRA> show mvpn c-Multicast inet instance-name VRF-CLIENTE-
AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  C-mcast IPv4 (S:G)            Provider Tunnel                          St
  10.10.10.10/32:239.1.1.1/32   S-RSVP-TE P2MP:72.16.11.11, 64299,72.16.11.11         RM
  10.10.10.10/32:239.1.1.10/32  S-RSVP-TE P2MP:72.16.11.11, 64300,72.16.11.11         RM

root@PE_SEDE_TIERRA> show route table VRF-CLIENTE-AZUL.inet.1

VRF-CLIENTE-AZUL.inet.1: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

224.0.0.0/4        *[Multicast/180] 4d 04:06:47
                      MultiResolve
224.0.0.0/24       *[Multicast/180] 4d 04:06:47
                      MultiDiscard
232.0.0.0/8        *[Multicast/180] 4d 04:06:47
                      MultiResolve
239.1.0.0/16       *[Multicast/180] 2d 10:39:51
                      MultiResolve
239.1.1.1,10.10.10.10/32*[MVPN/70] 1d 02:56:44
```

```
                    > to 72.16.1.1 via ge-0/0/2.0, Push 299872
                      to 72.16.5.2 via ge-0/0/3.0, Push 16
239.1.1.10,10.10.10.10/32*[MVPN/70] 1d 02:56:44
                    > to 72.16.5.2 via ge-0/0/3.0, Push 16

root@PE_SEDE_TIERRA> show rsvp session statistics
Ingress RSVP: 6 sessions
To              From            State     Packets            Bytes LSPname
72.16.22.22     72.16.11.11     Up         268534         23630992
72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up         268534         23630992
72.16.33.33:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.44.44     72.16.11.11     Up         268534         23630992
72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.44.44     72.16.11.11     Up          75496          6643648
72.16.44.44:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up          75496          6643648
72.16.33.33:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up          75418          6636784
72.16.33.33:72.16.11.11:1:mv2:VRF-CLIENTE-AZUL
Total 6 displayed, Up 6, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

root@PE_SEDE_TIERRA> show interfaces ge-0/0/2 statistics | match pps
  Input rate     : 296 bps (0 pps)
  Output rate    : 7816 bps (8 pps)

root@PE_SEDE_TIERRA> show interfaces ge-0/0/3 statistics | match pps
  Input rate     : 0 bps (0 pps)
  Output rate    : 13992 bps (19 pps)
```

Como se indicó previamente, se señalizaron dos LSP, uno por cada grupo Multicast, el correspondiente al grupo 239.1.1.1 señaliza dos sub-LSP uno por la interfaz ge-0/0/2 hacia el PE Venus y otro por la interfaz ge-0/0/3 hacia el PE Marte, mientras que el LSP correspondiente al grupo 239.1.1.10 sólo señaliza un sub-LSP a través de la interfaz ge-0/0/3 hacia el PE Marte, lo que origina que las estadísticas de la interconexión con el PE Marte sean el doble de las estadísticas registradas en la interconexión hacia el P/RR Júpiter.

Siguiendo el recorrido de los túneles selectivos P2MP, se revisan las estadísticas en el PE Marte y se encuentra lo siguiente:

```
root@PE_SEDE_MARTE> show rsvp session brief
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress RSVP: 3 sessions
To              From            State   Rt Style Labelin Labelout LSPname
72.16.33.33     72.16.11.11     Up       0  1 SE      16        -
72.16.33.33:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up       0  1 SE      16        -
72.16.33.33:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL
72.16.33.33     72.16.11.11     Up       0  1 SE      16        -
72.16.33.33:72.16.11.11:1:mv2:VRF-CLIENTE-AZUL
Total 3 displayed, Up 3, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

root@PE_SEDE_MARTE> show mvpn c-Multicast inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  C-mcast IPv4 (S:G)            Provider Tunnel                        St
  10.10.10.10/32:239.1.1.1/32   S-RSVP-TE P2MP:72.16.11.11, 64299,72.16.11.11
```

```
   10.10.10.10/32:239.1.1.10/32  S-RSVP-TE P2MP:72.16.11.11, 64300,72.16.11.11

root@PE_SEDE_MARTE> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 4d 06:31:52
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_MARTE> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 225004 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 2d 06:35:56

root@PE_SEDE_MARTE> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 221197 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 2d 06:36:20

root@PE_SEDE_MARTE> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 0 bps (0 pps)
  Output rate    : 12016 bps (17 pps)

root@PE_SEDE_MARTE> show interfaces ge-0/0/3 statistics | match pps
  Input rate     : 14376 bps (19 pps)
  Output rate    : 1568 bps (1 pps)
```

Se observa un comportamiento similar al presentado en el escenario del túnel inclusivo, sin embargo, se destaca que recibe tres sub-LSP provenientes del PE Tierra con la etiqueta MPLS 16, dos sub-LSP correspondientes a los dos túneles selectivos y uno correspondiente al túnel inclusivo, esto ocurre debido a que los tres pertenecen a la misma instancia MVPN con lo que al hacer pop de la etiqueta, el enrutamiento al interior de la MVPN se realizará por la dirección IP del destino de los paquetes, donde se revisará el grupo Multicast al que pertenece cada flujo. Como ocurre en el PE Tierra, la MVPN solo se asocia a los sub-LSP de los túneles selectivos, que son por los que recibe tráfico para los dos grupos Multicast (239.1.1.1 y 239.1.1.10), siendo de aproximadamente 9 paquetes por segundo (9 pps). Este tráfico es conmutado hacia la interfaz que interconecta al PE con el CE Marte (ge-0/0/1.101), lo que se confirma al verificar las estadísticas de tráfico de la interfaces que lo interconectan con el PE Tierra (ge-0/0/3 con 17 pps de entrada) y con el CE Marte (ge-0/0/1 con 17 pps de salida).

Se hace la misma verificación en el equipo P/RR Júpiter y se encuentra lo siguiente:

```
root@P_RR_JUPITER> show rsvp session brief
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit RSVP: 3 sessions
To              From            State   Rt Style Labelin Labelout LSPname
72.16.22.22     72.16.11.11     Up       0  1 SE  299856       16
72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.44.44     72.16.11.11     Up       0  1 SE  299856       16
72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
72.16.44.44     72.16.11.11     Up       0  1 SE  299872       16
72.16.44.44:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL
Total 3 displayed, Up 3, Down 0

root@P_RR_JUPITER> show route label 299856

mpls.0: 14 destinations, 14 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

299856             *[RSVP/7/2] 5d 22:11:23, metric 1
                    > to 72.16.2.2 via ge-0/0/2.0, Swap 16
                      to 72.16.4.2 via ge-0/0/4.0, Swap 16

root@P_RR_JUPITER> show route label 299872

mpls.0: 14 destinations, 14 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

299872             *[RSVP/7/2] 3d 14:11:30, metric 1
                    > to 72.16.4.2 via ge-0/0/4.0, Swap 16

root@P_RR_JUPITER> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 6872 bps (9 pps)
  Output rate    : 912 bps (0 pps)

root@P_RR_JUPITER> show interfaces ge-0/0/2 statistics | match pps
  Input rate     : 904 bps (1 pps)
  Output rate    : 496 bps (0 pps)

root@P_RR_JUPITER> show interfaces ge-0/0/4 statistics | match pps
  Input rate     : 792 bps (0 pps)
  Output rate    : 7320 bps (9 pps)
```

Se confirma que el P/RR sirve de tránsito para tres sub-LSP provenientes del PE Tierra, dos correspondientes al túnel inclusivo (etiqueta 299856) y uno al túnel selectivo del grupo 239.1.1.1 destinado al PE Venus (etiqueta 299872). Se observa que las dos etiquetas son conmutadas a la etiqueta 16 (*swap*).

Por otra parte, al revisar las estadísticas de tráfico por las interfaces, se encuentra que se recibe 9 pps por la interfaz que interconecta al P/RR con el PE Tierra, que es el tráfico correspondiente al grupo Multicast 239.1.1.1 y es enviado por la interfaz correspondiente a la interconexión con el PE Venus, mientras que la interfaz correspondiente a la interconexión con el PE Mercurio presenta 0 pps, lo que es congruente con el escenario de túneles selectivos en donde únicamente el PE Venus tiene receptores interesados para el grupo 239.1.1.1 .

Pasando al PE Venus se encuentra que:

```
root@PE_SEDE_VENUS> show rsvp session brief
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress RSVP: 2 sessions
To              From            State   Rt Style Labelin Labelout LSPname
72.16.44.44     72.16.11.11     Up       0  1 SE      16        -
72.16.44.44:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
```

```
72.16.44.44     72.16.11.11     Up       0  1 SE      16        -
72.16.44.44:72.16.11.11:1:mv1:VRF-CLIENTE-AZUL
Total 2 displayed, Up 2, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

root@PE_SEDE_VENUS> show mvpn c-Multicast inet instance-name VRF-CLIENTE-AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY
  C-mcast IPv4 (S:G)            Provider Tunnel                          St
  10.10.10.10/32:239.1.1.1/32   S-RSVP-TE P2MP:72.16.11.11, 64299,72.16.11.11

root@PE_SEDE_VENUS> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 6d 17:22:42
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_VENUS> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive
Instance: VRF-CLIENTE-AZUL Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: lsi.0
    Downstream interface list:
        ge-0/0/1.101
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 286719 packets
    Next-hop ID: 262146
    Upstream protocol: MVPN
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: forever
    Wrong incoming interface notifications: 0
    Uptime: 4d 17:26:37

root@PE_SEDE_VENUS> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive

root@PE_SEDE_VENUS> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 0 bps (0 pps)
  Output rate    : 6048 bps (9 pps)

root@PE_SEDE_VENUS> show interfaces ge-0/0/2 statistics | match pps
  Input rate     : 6584 bps (8 pps)
  Output rate    : 1752 bps (1 pps)
```

El PE Venus recibe dos sub-LSP, uno correspondiente al túnel inclusivo y el otro correspondiente al túnel selectivo, sin embargo la MVPN sólo se asocia al del túnel selectivo que es el que transporta el tráfico Multicast sobre el que está interesado el receptor (grupo 239.1.1.1), de igual forma recibe los dos sub-LSP con la etiqueta 16 debido a que hacen parte de la misma instancia MVPN. Esta etiqueta (16) es eliminada (*pop*) y el tráfico es enviado a la instancia MVPN, además se confirma que al contrario de lo que ocurre en el escenario con túnel inclusivo, el PE Venus recibe tráfico para un grupo Multicast (239.1.1.1). Este tráfico es conmutado hacia la interfaz que interconecta al PE con el CE Venus (ge-0/0/1.101) lo que se corrobora al verificar las estadísticas de tráfico de la interfaces que lo interconectan con el P/RR Júpiter (ge-0/0/2 con 9 pps de entrada) y con el CE Venus (ge-0/0/1 con 8 pps de salida).

Posteriormente se realizó la verificación en el PE Mercurio que no tiene asociados receptores interesados en el tráfico Multicast y se encontró lo siguiente:

```
root@PE_SEDE_MERCURIO> show rsvp session brief
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
72.16.22.22     72.16.11.11     Up       0  1 SE      16        -
72.16.22.22:72.16.11.11:1:mvpn:VRF-CLIENTE-AZUL
Total 1 displayed, Up 1, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

root@PE_SEDE_MERCURIO> show mvpn c-Multicast inet instance-name VRF-CLIENTE-
AZUL

MVPN instance:
Legend for provider tunnel
S-    Selective provider tunnel

Legend for c-Multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : VRF-CLIENTE-AZUL
  MVPN Mode : SPT-ONLY

root@PE_SEDE_MERCURIO> show route label 16

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

16                 *[VPN/0] 6d 17:29:25
                      to table VRF-CLIENTE-AZUL.inet.0, Pop

root@PE_SEDE_MERCURIO> show Multicast route group 239.1.1.1 instance VRF-
CLIENTE-AZUL extensive

root@PE_SEDE_MERCURIO> show Multicast route group 239.1.1.10 instance VRF-
CLIENTE-AZUL extensive

root@PE_SEDE_MERCURIO> show interfaces ge-0/0/1 statistics | match pps
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

root@PE_SEDE_MERCURIO> show interfaces ge-0/0/2 statistics | match pps
  Input rate     : 280 bps (0 pps)
  Output rate    : 0 bps (0 pps)
```

Como se podría deducir, el PE Mercurio solo recibe el sub-LSP correspondiente al túnel inclusivo, sin embargo no tiene asociados sub-LSP a su instancia MVPN por lo que no registra tráfico conmutado a través de sus interfaces.

Por último, se verificó el comportamiento del tráfico en los CE y en los propios receptores.

```
root@CE_SEDE_MARTE> show Multicast route extensive
Instance: master Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.103
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 8876 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:16:16
```

```
Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.103
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 9104 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:16:42

Instance: master Family: INET6

root@CE_SEDE_MARTE> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:              579504                 18 pps
     Output packets:                   0                  0 pps

root@CE_SEDE_MARTE> show interfaces ge-0/0/2.103 statistics detail | match
pps
     Input  packets:                   0                  0 pps
     Output packets:              579723                 18 pps
```

```
root@CE_SEDE_MERCURIO> show Multicast route
Instance: master Family: INET

Instance: master Family: INET6

root@CE_SEDE_MERCURIO> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:                   0                  0 pps
     Output packets:                   0                  0 pps
```

```
root@CE_SEDE_VENUS> show Multicast route extensive
Instance: master Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.101
    Downstream interface list:
        ge-0/0/2.104
    Number of outgoing interfaces: 1
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 9613 packets
    Next-hop ID: 262143
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Forwarding
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:17:37

Instance: master Family: INET6

root@CE_SEDE_VENUS> show interfaces ge-0/0/1.101 statistics detail | match
pps
     Input  packets:              290996                  8 pps
     Output packets:                   0                  0 pps

root@CE_SEDE_VENUS> show interfaces ge-0/0/2.104 statistics detail | match
pps
     Input  packets:                   0                  0 pps
     Output packets:              291143                  9 pps
```

```
root@TX_RX> show Multicast route instance RECEPTOR_MARTE extensive
Instance: RECEPTOR_MARTE Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.103
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 248 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:00:27
```

```
Group: 239.1.1.10
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.103
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 416 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:00:46

Instance: RECEPTOR_MARTE Family: INET6

root@TX_RX> show Multicast route instance RECEPTOR_VENUS extensive
Instance: RECEPTOR_VENUS Family: INET

Group: 239.1.1.1
    Source: 10.10.10.10/32
    Upstream interface: ge-0/0/1.104
    Number of outgoing interfaces: 0
    Session description: Organisational Local Scope
    Statistics: 1 kBps, 9 pps, 378 packets
    Next-hop ID: 0
    Upstream protocol: PIM
    Route state: Active
    Forwarding state: Pruned
    Cache lifetime/timeout: 360 seconds
    Wrong incoming interface notifications: 0
    Uptime: 00:00:41

Instance: RECEPTOR_VENUS Family: INET6
```

Se observa el mismo comportamiento presentado en el escenario de túneles inclusivos, lo que significa que la configuración de túneles selectivos o inclusivos no afecta el intercambio de tráfico Multicast desde la perspectiva de los equipos de cliente, siendo el comportamiento esperado en una red MVPN. La selección de una u otra tecnología en la infraestructura del proveedor de servicio no debe afectar el tráfico Multicast de cliente.

5 Conclusiones y trabajos futuros

5.1 Conclusiones

La arquitectura de red propuesta por las RFC 6513 y 6514 a través del plano de control basado en MP-BGP ofrece un modelo complementario y congruente con la arquitectura de red planteada para el servicio de tráfico Unicast en redes MPLS/BGP, definida en la RFC 4364. Sin embargo, la arquitectura de red propuesta para el plano de control basado en PIM plantea un modelo heterogéneo de redes MPLS, ya que el modelo de red para el transporte de tráfico Unicast es diferente al modelo para el transporte de tráfico Multicast. El escenario basado en plano de control PIM, complica así la administración y en algunas funcionalidades requiere mayor consumo de recursos de la red.

En el contexto de MVPN que plantean las RFC 6513 y 6514, los fabricantes han dejado de lado la implementación del escenario con el plano de control basado en PIM para enfocarse en la implementación del plano de control basado en MP-BGP.

De forma similar a lo que ocurre con el plano de control, en el plano de transporte, la arquitectura de red Multicast creada a partir de los túneles P2MP basados en MPLS mantienen la homogeneidad, pues complementa el modelo de túneles MPLS P2P del servicio Unicast, mientras que el modelo de túneles GRE/IP complican la administración de la red al agregar una tecnología de túneles diferente paa el transporte de tráfico Multicast.

Los túneles GRE/IP están ligados al plano de control basado en PIM, pues a pesar de que teóricamente las RFC 6513 y 6514 permiten la combinación del plano de control basado en MP-BGP con el plano de transporte basado en PGRE/IP, los fabricantes no han desarrollado el soporte de esta combinación de tecnologías, lo que implícitamente asocia la implementación del plano de control basado en PIM con la necesidad de establecer un plano de transporte basado en túneles GRE/IP y viceversa.

Las RFC 6513 y 6514 describen la integración del nuevo modelo de arquitectura de red para el transporte de tráfico Multicast soportado por los planos de control basado en MP-BGP y plano de transporte basado en túneles MPLS, con el modelo descrito por el draft-Rosen, sin embargo, esta integración no se da a nivel práctico ya que representa una complejidad alta y los fabricantes han decidido implementar los dos modelos como escenarios aislados. Esto hace que la evolución técnológica de la solución MVPN a nivel de estandarización se vea perjudicada por la necesidad de soportar los dos escenarios. Una forma de aliviar esta complejidad podría plantearse a partir de la

separación de los dos modelos a nivel de estandarización, es decir, mantener el draft Rosen (actualmente RFC 6037) para que se encargue de la descripción del modelo basado en PIM para el plano de control, y dejar las RFC 6513 y 6514 para que se encargue de la descripción del modelo con el plano de control basado en MP-BGP, Esto permitirá que los dos modelos evolucionen de forma flexible ya que se elimina la dependencia entre ellos.

El desarrollo del servicio MVPN en un proveedor de servicios debe ser soportado por el plano de control basado en MP-BGP y únicamente debe implementarse el plano de control basado en PIM de forma temporal para soportar implementaciones legadas, pero siempre teniendo como objetivo su migración al modelo de plano de control basado en MP-BGP.

El proveedor de servicios con una red multi-fabricante debe revisar previamente los escenarios de implementación y las funcionalidades que desea soportar para garantizar la interoperabilidad del servicio, pues aún existen funcionalidades que no son soportadas por todos los fabricantes o que simplemente todavía se encuentran en desarrollo por el mismo organismo de estandarización IETF.

En cuanto al caso práctico, se recomienda el uso de túneles selectivos, ya que el hecho de consumir ancho de banda innecesario en el desarrollo de túneles inclusivos puede resultar muy costoso para el proveedor de servicios. Si bien es cierto que el escenario de túneles selectivos requiere señalizar más túneles comparado con el despliegue de túneles inclusivos, sin embargo, los enrutadores actualmente están aumentando sus capacidades a nivel de memoria, lo que les permite asimilar el posible impacto que representa el aumento de túneles.

Por último, sin importar la selección de las tecnologías utilizadas para implementar el servicio MVPN, tanto en el plano de control como en el plano de transporte, queda claro que debe ser transparente para el cliente final, quien deberá recibir el tráfico Multicast de forma óptima, es decir, el tráfico debe ser transmitido únicamente a los receptores interesados.

5.2 Trabajos futuros

Las herramientas de virtualización son muy útiles para el desarrollo de casos prácticos de nuevas tecnologías en redes de telecomunicaciones y podría plantearse la opción de habilitar gradualmente el despliegue de servicios MVPN en la herramienta VNX (*Virtual Networks over Linux*) desarrollada por el Departamento de Ingeniería Telemática de la Universidad politécnica de Madrid.

Otro posible trabajo que se puede plantear es realizar una investigación similar a la descrita en este documento para el protocolo IPv6, pues las RFC 6513 y 6514 se enfocan en el despliegue de MVPN para IPv4.

En cuanto a los temas que se plantean como evolución de la implementación de servicios MVPN se encuentra la agregación de túneles de transporte para instancias que tengan alto grado de congruencia como se describe en el capítulo 3.4.3.

Otros temas que a pesar de ser planteados desde el inicio de la descripción de las RFC 6513 y 6514, hasta ahora están siendo abordados por los fabricantes, como lo son la implementación de los túneles de transporte basados en LDP o basados en RSVP. Un posible trabajo puede plantearse en torno al estudio comparativo de los dos protocolos de señalización de LSP, analizado desde la perspectiva de la implementación de servicios MVPN.

Así mismo ocurre con las opciones de interconexión de diferentes sistemas autónomos en escenarios Inter-AS para MVPN, enfocado en la segmentación o no de los túneles de transporte y sus similitudes o convivencia con las opciones inter-AS para el entorno Unicast.

Bibliografía

[1] E. Rosen, *et al.*, "Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs," RFC 6037 ed: IETF, 2010, pp. 1-26.

[2] E. Rosen and R. Aggarwal, "Multicast in MPLS/BGP IP VPNs," RFC 6513 ed: IETF, 2012, pp. 1-88.

[3] E. C. Rosen and R. Aggarwal, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs," RFC 6514 ed: IETF, 2012, pp. 1-60.

[4] IANA. (2013, 01/05/2013). *IPv4 Multicast Address Space Registry*. Available: http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml

[5] Y. Rekhter, *et al.*, "Address allocation for private internets," RFC 1918 ed: IETF, 1996, pp. 1-10.

[6] B. Williamson, *Developing IP multicast networks* vol. 1: Cisco Systems, 2000.

[7] N. Bhaskar, *et al.*, "Bootstrap router (BSR) mechanism for protocol independent multicast (PIM)," RFC 5059 ed: IETF, 2008, pp. 1-41.

[8] D. Farinacci and Y. Cai, "Anycast-RP Using Protocol Independent Multicast (PIM)," RFC 4610 ed: IETF, 2006, pp. 1-12.

[9] S. Deering, "Host Extensions for IP Multicast," RFC 1112 ed: IETF, 1989, pp. 1-17.

[10] W. C. Fenner, "Internet group management protocol, version 2," RFC 2236 ed: IETF, 1997, pp. 1-24.

[11] H. Holbrook, *et al.*, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast," RFC 4604 ed: IETF, 2006, pp. 1-11.

[12] W. Odom, *et al.*, *CCIE Routing and Switching Official Exam Certification Guide (Exam Certification Guide)*: Cisco Press, 2006.

[13] B. Adams, *Interdomain Multicast Solutions Guide*: Cisco Systems, 2002.

[14] B. M. Edwards, *et al.*, *Interdomain Multicast Routing: Practical Juniper Networks and Cisco Systems Solutions*: Addison-Wesley Professional, 2002.

[15] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," RFC 4364 ed: IETF, 2006, pp. 1-47.

[16] J. De Clercq, *et al.*, "BGP-MPLS IP virtual private network (VPN) extension for ipv6 vpn," RFC4659 ed: IETF, 2006, pp. 1-18.

[17] Alcatel-Lucent, "Next-generation Layer 3 Multicast VPN (MVPN) Services," ed: Alcatel-Lucent, 2010, pp. 1-24.

[18] A. S. Monge, *This Week Deploying MBGP Multicast VPNs*: Juniper Networks Books, 2011.

[19] Alcatel-Lucent, "7750 SR OS Services Guide," ed: Alcatel-Lucent, 2013, pp. 1495-1512.

[20] Cisco. (2013). *NG MVPN: CKN TechAdvantage Webinar* [Webinar]. Available: https://communities.cisco.com/docs/DOC-32703

[21] Juniper, "Junos OS 13.1 Multicast over Layer 3 VPNs Feature Guide," ed. Sunnyvale, California: Juniper Networks, Inc., 2013, pp. 1-142.

[22] Juniper, "WHITE PAPER - Understanding Junos OS Next-Generation Multicast VPNS," ed: Juniper Networks, Inc., 2010, pp. 1-44.

[23] Juniper, "Junos OS 11.2 Multicast Protocols Configuration Guide," ed. Sunnyvale, California: Juniper Networks, Inc., 2011, pp. 1-832.

[24] Cisco, "Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.3.x," ed. San Jose, California: Cisco Systems, Inc., 2013, pp. 1-274.

[25] R. Aggarwal, *et al.*, "Extensions to resource reservation protocol-traffic engineering (RSVP-TE) for point-to-multipoint TE label switched paths (LSPs)," RFC 4875 ed: IETF, 2007, pp. 1-54.

[26] I. Wijnands, *et al.*, "Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths," RFC 6388 ed: IETF, 2011, pp. 1-40.

[27] M. Napierala, *et al.*, "MVPN: Optimized use of PIM via MS-PMSIs," draft-rosen-l3vpn-mvpn-mspmsi-10.txt ed: IETF, 2012, pp. 1-11.

[28] D. Farinacci, *et al.*, "A Reliable Transport Mechanism for PIM," RFC 6559 ed: IETF, 2012, pp. 1-29.

[29] T. Morin, *et al.*, "Mandatory Features in a Layer 3 Multicast BGP/MPLS VPN Solution," RFC 6517 ed: IETF, 2012, pp. 1-41.

[30] J. W. Atwood, *et al.*, "Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages," RFC 5796 ed: IETF, 2010, pp. 1-22.

[31] E. C. Rosen, *et al.*, "MVPN: Using Bidirectional P-Tunnels," draft-ietf-l3vpn-mvpn-bidir-04 ed: IETF, 2013, pp. 1-21.

[32] L. Andersson, *et al.*, "LDP specification," RFC 5036 ed: IETF, 2007, pp. 1-135.

[33] I. Minei and J. Lucek, *MPLS-enabled applications: emerging developments and new technologies*: John Wiley & Sons, Ltd., 2011.

[34] Juniper, "JUNOS 8.5 MPLS Applications Configuration Guide," ed. Sunnyvale, California: Juniper Networks, Inc., 2007, pp. 1-534.

[35] Cisco, "Cisco ASR 9000 Series Aggregation Services Routers Multicast Configuration Guide, Release 4.2.x," ed. San Jose, California: Cisco Systems, Inc., 2011, pp. 1-276.

[36] I. Wijnands, *et al.*, "mLDP Node Protection," draft-wijnands-mpls-mldp-node-protection-02 ed: IETF, 2012, pp. 1-17.

[37] Cisco, "Feature Information for BGP - mVPN BGP sAFI 129 - IPv4," in *IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S*, ed. San Jose, California: Cisco Systems, Inc., 2013, pp. 1-10.

[38] H. Holbrook and B. Cain, "Source-Specific Multicast for IP," RFC 4607 ed: IETF, 2006, pp. 1-20.

Anexos

A continuación se adjuntan las configuraciones de los enrutadores virtuales utilizados en el caso de estudio:

Configuración equipo TX_RX

```
## Last changed: 2013-06-12 15:34:29 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name TX RX;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/1p6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
```

```
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name TX RX;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.42/20;
                address 10.233.248.25/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a CE_TIERRA";
            vlan-id 101;
            family inet {
                address 10.10.10.10/24;
            }
        }
        unit 103 {
            description "Interfaz a CE MARTE";
            vlan-id 103;
            family inet {
                address 10.10.30.10/24;
            }
        }
        unit 104 {
            description "Interfaz a CE_VENUS";
            vlan-id 104;
            family inet {
                address 10.10.40.10/24;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
}
routing-instances {
    FUENTE TIERRA {
        instance-type virtual-router;
        interface ge-0/0/1.101;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.10.10.1;
            }
        }
    }
    RECEPTOR MARTE {
        instance-type virtual-router;
        interface ge-0/0/1.103;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.10.30.1;
            }
        }
        protocols {
            pim {
                interface ge-0/0/1.103 {
                    mode sparse;
                }
            }
        }
    }
    RECEPTOR VENUS {
        instance-type virtual-router;
        interface ge-0/0/1.104;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.10.40.1;
            }
        }
        protocols {
            pim {
                interface ge-0/0/1.104 {
                    mode sparse;
                }
            }
```

```
        }
    }
}
```

Configuración equipo PE_SEDE_VENUS

```
## Last changed: 2013-06-12 09:52:06 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name PE SEDE VENUS;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
```

```
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name PE SEDE VENUS;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.69/20;
                address 10.233.255.239/20;
                address 10.233.248.36/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a CE VENUS";
            vlan-id 101;
            family inet {
                address 10.4.4.1/30;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            description "Interfaz a P RR JUPITER";
            family inet {
                address 72.16.4.2/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            description "Interfaz a PE MERCURIO";
            family inet {
                address 72.16.6.2/30;
            }
            family iso;
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 72.16.44.44/32;
            }
            family iso {
                address 49.1111.1720.1604.4044.00;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    router-id 72.16.44.44;
    autonomous-system 12956;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
    }
    rsvp {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    mpls {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    bgp {
        group RR {
            type internal;
            local-address 72.16.44.44;
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
```

```
            }
            neighbor 72.16.55.55;
        }
    }
    isis {
        level 2 wide-metrics-only;
        interface ge-0/0/2.0 {
            point-to-point;
            level 1 disable;
        }
        interface ge-0/0/3.0 {
            point-to-point;
            level 1 disable;
        }
        interface lo0.0;
    }
    ldp {
        track-igp-metric;
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
}
policy-options {
    policy-statement EXPORT VRF AZUL {
        term ucast {
            from {
                family inet;
                protocol bgp;
            }
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
        term multicast {
            from family inet-mvpn;
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
    }
    policy-statement IMPORT VRF AZUL {
        term bgp-ucast {
            from {
                family inet;
                community comun-ucast-azul;
            }
            then accept;
        }
        term multicast {
            from {
                family inet-mvpn;
                community comun-ucast-azul;
            }
            then accept;
        }
    }
    policy-statement ebgp-a-CE {
        term bgp-ucast {
            from {
                family inet;
                protocol bgp;
                route-type internal;
            }
            then accept;
        }
        term rest {
            then reject;
        }
    }
    community comun-ucast-azul members target:12956:10;
}
routing-instances {
    VRF-CLIENTE-AZUL {
        instance-type vrf;
        interface ge-0/0/1.101;
        route-distinguisher 72.16.44.44:1;
        vrf-import IMPORT_VRF_AZUL;
        vrf-export EXPORT VRF AZUL;
        vrf-table-label;
        routing-options {
            multicast {
                ssm-groups 239.1.0.0/16;
            }
        }
        protocols {
            bgp {
                group CE SEDE VENUS {
                    export ebgp-a-CE;
                    peer-as 65000;
                    as-override;
                    neighbor 10.4.4.2;
                }
```

```
            }
            pim {
                interface ge-0/0/1.101 {
                    mode sparse;
                }
            }
            mvpn;
        }
    }
}
```

Configuración equipo PE_SEDE_TIERRA

```
## Last changed: 2013-06-13 13:06:27 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name PE SEDE TIERRA;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
```

```
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name PE SEDE TIERRA;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.55/20;
                address 10.233.255.201/20;
                address 10.233.248.28/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a CE_TIERRA";
            vlan-id 101;
            family inet {
                address 10.1.1.1/30;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            description "Interfaz a P RR JUPITER";
            family inet {
                address 72.16.1.2/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            description "Interfaz a PE MARTE";
            family inet {
                address 72.16.5.1/30;
            }
            family iso;
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 72.16.11.11/32;
            }
            family iso {
                address 49.1111.1720.1601.1011.00;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    router-id 72.16.11.11;
    autonomous-system 12956;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
    }
    rsvp {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    mpls {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    bgp {
        group RR {
            type internal;
            local-address 72.16.11.11;
```

```
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            neighbor 72.16.55.55;
        }
    }
    isis {
        level 2 wide-metrics-only;
        interface ge-0/0/2.0 {
            point-to-point;
            level 1 disable;
        }
        interface ge-0/0/3.0 {
            point-to-point;
            level 1 disable;
        }
        interface lo0.0;
    }
    ldp {
        track-igp-metric;
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
}
policy-options {
    policy-statement EXPORT VRF AZUL {
        term ucast {
            from {
                family inet;
                protocol bgp;
            }
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
        term multicast {
            from family inet-mvpn;
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
    }
    policy-statement IMPORT VRF AZUL {
        term bgp-ucast {
            from {
                family inet;
                community comun-ucast-azul;
            }
            then accept;
        }
        term multicast {
            from {
                family inet-mvpn;
                community comun-ucast-azul;
            }
            then accept;
        }
    }
    policy-statement ebgp-a-CE {
        term bgp-ucast {
            from {
                family inet;
                protocol bgp;
                route-type internal;
            }
            then accept;
        }
        term rest {
            then reject;
        }
    }
    community comun-ucast-azul members target:12956:10;
}
routing-instances {
    VRF-CLIENTE-AZUL {
        instance-type vrf;
        interface ge-0/0/1.101;
        route-distinguisher 72.16.11.11:1;
        provider-tunnel {
            rsvp-te {
                label-switched-path-template {
                    default-template;
                }
            }
            selective {
                group 239.1.0.0/16 {
                    source 0.0.0.0/0 {
                        rsvp-te {
                            label-switched-path-template {
```

```
                                default-template;
                            }
                        }
                    }
                }
            }
        }
        vrf-import IMPORT VRF AZUL;
        vrf-export EXPORT VRF AZUL;
        vrf-table-label;
        routing-options {
            multicast {
                ssm-groups 239.1.0.0/16;
            }
        }
        protocols {
            bgp {
                group CE SEDE TIERRA {
                    export ebgp-a-CE;
                    peer-as 65000;
                    as-override;
                    neighbor 10.1.1.2;
                }
            }
            pim {
                interface ge-0/0/1.101 {
                    mode sparse;
                }
            }
            mvpn;
        }
    }
}
```

Configuración equipo PE_SEDE_MERCURIO

```
## Last changed: 2013-06-12 05:23:18 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name PE SEDE MERCURIO;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
```

```
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name PE SEDE MERCURIO;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.59/20;
                address 10.233.255.241/20;
                address 10.233.248.23/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a CE MERCURIO";
            vlan-id 101;
            family inet {
                address 10.2.2.1/30;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            description "Interfaz a P RR JUPITER";
            family inet {
                address 72.16.2.2/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            description "Interfaz a PE VENUS";
            family inet {
                address 72.16.6.1/30;
            }
            family iso;
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 72.16.22.22/32;
            }
            family iso {
                address 49.1111.1720.1602.2022.00;
            }
        }
    }
}
```

```
routing-options {
    max-interface-supported 10;
    router-id 72.16.22.22;
    autonomous-system 12956;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
    }
    rsvp {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    mpls {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    bgp {
        group RR {
            type internal;
            local-address 72.16.22.22;
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            neighbor 72.16.55.55;
        }
    }
    isis {
        level 2 wide-metrics-only;
        interface ge-0/0/2.0 {
            point-to-point;
            level 1 disable;
        }
        interface ge-0/0/3.0 {
            point-to-point;
            level 1 disable;
        }
        interface lo0.0;
    }
    ldp {
        track-igp-metric;
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
}
policy-options {
    policy-statement EXPORT VRF AZUL {
        term ucast {
            from {
                family inet;
                protocol bgp;
            }
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
        term multicast {
            from family inet-mvpn;
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
    }
    policy-statement IMPORT VRF AZUL {
        term bgp-ucast {
            from {
                family inet;
                community comun-ucast-azul;
            }
            then accept;
        }
        term multicast {
            from {
                family inet-mvpn;
                community comun-ucast-azul;
            }
            then accept;
        }
    }
    policy-statement ebgp-a-CE {
        term bgp-ucast {
            from {
                family inet;
                protocol bgp;
                route-type internal;
            }
            then accept;
```

```
        }
        term rest {
            then reject;
        }
    }
    community comun-ucast-azul members target:12956:10;
}
routing-instances {
    VRF-CLIENTE-AZUL {
        instance-type vrf;
        interface ge-0/0/1.101;
        route-distinguisher 72.16.22.22:1;
        vrf-import IMPORT VRF AZUL;
        vrf-export EXPORT VRF AZUL;
        vrf-table-label;
        routing-options {
            multicast {
                ssm-groups 239.1.0.0/16;
            }
        }
        protocols {
            bgp {
                group CE SEDE MERCURIO {
                    export ebgp-a-CE;
                    peer-as 65000;
                    as-override;
                    neighbor 10.2.2.2;
                }
            }
            pim {
                interface ge-0/0/1.101 {
                    mode sparse;
                }
            }
            mvpn;
        }
    }
}
```

Configuración equipo PE_SEDE_MARTE

```
## Last changed: 2013-06-12 09:51:51 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name PE SEDE MARTE;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
```

```
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name PE SEDE MARTE;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.53/20;
                address 10.233.255.236/20;
                address 10.233.248.32/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a CE MARTE";
            vlan-id 101;
            family inet {
                address 10.3.3.1/30;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            description "Interfaz a P RR JUPITER";
            family inet {
                address 72.16.3.2/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            description "Interfaz a PE TIERRA";
            family inet {
                address 72.16.5.2/30;
            }
            family iso;
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 72.16.33.33/32;
            }
            family iso {
```

```
                address 49.1111.1720.1603.3033.00;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    router-id 72.16.33.33;
    autonomous-system 12956;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
    }
    rsvp {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    mpls {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
    bgp {
        group RR {
            type internal;
            local-address 72.16.33.33;
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            neighbor 72.16.55.55;
        }
    }
    isis {
        level 2 wide-metrics-only;
        interface ge-0/0/2.0 {
            point-to-point;
            level 1 disable;
        }
        interface ge-0/0/3.0 {
            point-to-point;
            level 1 disable;
        }
        interface lo0.0;
    }
    ldp {
        track-igp-metric;
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
    }
}
policy-options {
    policy-statement EXPORT VRF AZUL {
        term ucast {
            from {
                family inet;
                protocol bgp;
            }
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
        term multicast {
            from family inet-mvpn;
            then {
                community add comun-ucast-azul;
                accept;
            }
        }
    }
    policy-statement IMPORT VRF AZUL {
        term bgp-ucast {
            from {
                family inet;
                community comun-ucast-azul;
            }
            then accept;
        }
        term multicast {
            from {
                family inet-mvpn;
                community comun-ucast-azul;
            }
            then accept;
        }
    }
    policy-statement ebgp-a-CE {
        term bgp-ucast {
            from {
```

```
                family inet;
                protocol bgp;
                route-type internal;
            }
            then accept;
        }
        term rest {
            then reject;
        }
    }
    community comun-ucast-azul members target:12956:10;
}
routing-instances {
    VRF-CLIENTE-AZUL {
        instance-type vrf;
        interface ge-0/0/1.101;
        route-distinguisher 72.16.33.33:1;
        vrf-import IMPORT VRF AZUL;
        vrf-export EXPORT VRF AZUL;
        vrf-table-label;
        routing-options {
            multicast {
                ssm-groups 239.1.0.0/16;
            }
        }
        protocols {
            bgp {
                group CE SEDE MARTE {
                    export ebgp-a-CE;
                    peer-as 65000;
                    as-override;
                    neighbor 10.3.3.2;
                }
            }
            pim {
                interface ge-0/0/1.101 {
                    mode sparse;
                }
            }
            mvpn;
        }
    }
}
```

Configuración equipo P_RR_JUPITER

```
## Last changed: 2013-06-10 11:49:22 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name P RR JUPITER;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
```

```
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name P RR JUPITER;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.51/20;
                address 10.233.248.26/20;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            description "Interfaz a PE TIERRA";
            family inet {
                address 72.16.1.1/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/2 {
        unit 0 {
            description "Interfaz a PE MERCURIO";
            family inet {
                address 72.16.2.1/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            description "Interfaz a PE MARTE";
            family inet {
                address 72.16.3.1/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-0/0/4 {
        unit 0 {
```

```
            description "Interfaz a PE VENUS";
            family inet {
                address 72.16.4.1/30;
            }
            family iso;
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 72.16.55.55/32;
            }
            family iso {
                address 49.1111.0720.1605.5055.00;
            }
        }
    }
}
routing-options {
    router-id 72.16.55.55;
    autonomous-system 12956;
}
protocols {
    rsvp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    mpls {
        icmp-tunneling;
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    bgp {
        group RR-CLIENTES {
            type internal;
            local-address 72.16.55.55;
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            cluster 72.16.55.55;
            neighbor 72.16.11.11;
            neighbor 72.16.22.22;
            neighbor 72.16.33.33;
            neighbor 72.16.44.44;
        }
    }
    isis {
        level 2 wide-metrics-only;
        interface all {
            point-to-point;
            level 1 disable;
        }
        interface fxp0.0 {
            disable;
        }
    }
    ldp {
        track-igp-metric;
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
}
```

Configuración equipo CE_SEDE_VENUS

```
## Last changed: 2013-06-10 11:16:59 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name CE SEDE VENUS;
        }
    }
    global {
        system {
            time-zone America/Los Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
```

```
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name CE SEDE VENUS;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.76/20;
                address 10.233.255.203/20;
                address 10.233.248.21/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
```

```
        unit 101 {
            description "Interfaz a PE VENUS";
            vlan-id 101;
            family inet {
                address 10.4.4.2/30;
            }
        }
    }
    ge-0/0/2 {
        vlan-tagging;
        unit 104 {
            description "Interfaz a Receptor VENUS";
            vlan-id 104;
            family inet {
                address 10.10.40.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.44.44.44/32;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    autonomous-system 65000;
    multicast {
        ssm-map GRUPO-FUENTE {
            policy GRUPOS;
            source 10.10.10.10;
        }
    }
}
protocols {
    igmp {
        query-interval 10;
        query-response-interval 3;
        interface ge-0/0/2.2 {
            ssm-map GRUPO-FUENTE;
        }
        interface ge-0/0/1.101 {
            disable;
        }
        interface ge-0/0/2.104 {
            version 3;
            static {
                group 239.1.1.1 {
                    source 10.10.10.10;
                }
            }
        }
    }
    bgp {
        group PE {
            export LOOPBACK;
            peer-as 12956;
            neighbor 10.4.4.1;
        }
    }
    pim {
        interface ge-0/0/1.101 {
            mode sparse;
        }
    }
}
policy-options {
    policy-statement GRUPOS {
        term MULTICAST {
            from {
                route-filter 239.1.0.0/16 orlonger;
            }
            then accept;
        }
        term RESTO {
            then reject;
        }
    }
    policy-statement LOOPBACK {
        term LOOPBACK {
            from {
                route-filter 10.44.44.44/32 exact;
            }
            then accept;
        }
    }
}
```

Configuración equipo CE_SEDE_TIERRA

```
## Last changed: 2013-06-10 10:22:13 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name CE_SEDE_TIERRA;
        }
    }
    global {
        system {
            time-zone America/Los_Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
```

```
            }
        }
    }
}
apply-groups [ global member0 ];
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.252.224/20;
                address 10.233.255.200/20;
                address 10.233.255.237/20;
                address 10.233.248.23/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a PE_TIERRA";
            vlan-id 101;
            family inet {
                address 10.1.1.2/30;
            }
        }
    }
    ge-0/0/2 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a Fuente_TIERRA";
            vlan-id 101;
            family inet {
                address 10.10.10.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.11.11.11/32;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    autonomous-system 65000;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
        interface ge-0/0/2.101 {
            disable;
        }
    }
    bgp {
        group PE {
            export FUENTE Y LOOPBACK;
            peer-as 12956;
            neighbor 10.1.1.1;
        }
    }
    pim {
        interface ge-0/0/1.101 {
            mode sparse;
        }
        interface ge-0/0/2.101 {
            mode sparse;
        }
    }
}
policy-options {
    policy-statement FUENTE Y LOOPBACK {
        term FUENTE {
            from {
                route-filter 10.10.10.0/24 exact;
            }
            then accept;
        }
        term LOOPBACK {
            from {
                route-filter 10.11.11.11/32 exact;
            }
            then accept;
        }
    }
}
```

Configuración equipo CE_SEDE_MERCURIO

```
## Last changed: 2013-06-10 10:22:19 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name CE_SEDE_MERCURIO;
        }
    }
    global {
        system {
            time-zone America/Los_Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
```

```
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name CE SEDE MERCURIO;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.82/20;
                address 10.233.248.35/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a PE MERCURIO";
            vlan-id 101;
            family inet {
                address 10.2.2.2/30;
            }
        }
    }
    ge-0/0/2 {
        disable;
        vlan-tagging;
        unit 1 {
            vlan-id 101;
            family inet {
                address 10.10.10.2/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.22.22.22/32;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    autonomous-system 65000;
}
protocols {
    igmp {
        interface ge-0/0/1.101 {
            disable;
        }
        interface ge-0/0/2.101 {
            disable;
        }
    }
    bgp {
        group PE {
            export FUENTE-Y-LOOPBACK;
            peer-as 12956;
            neighbor 10.2.2.1;
        }
    }
    pim {
        interface ge-0/0/1.101 {
            mode sparse;
        }
        interface ge-0/0/2.101 {
            mode sparse;
        }
    }
}
policy-options {
    policy-statement FUENTE-Y-LOOPBACK {
        term FUENTE {
            from {
                route-filter 10.10.10.0/24 exact;
            }
            then accept;
        }
        term LOOPBACK {
            from {
                route-filter 10.22.22.22/32 exact;
            }
            then accept;
        }
    }
}
```

Configuración equipo CE_SEDE_MARTE

```
## Last changed: 2013-06-10 11:15:19 PDT
version "12.3I20130406 1317 anjali [anjali]";
groups {
    member0 {
        system {
            host-name CE_SEDE_MARTE;
        }
    }
    global {
        system {
            time-zone America/Los_Angeles;
            debugger-on-panic;
            debugger-on-break;
            dump-on-panic;
            root-authentication {
                encrypted-password "$1$SGUyJfYE$r5hIy2IU4IamO1ye3u70v0";
            }
            name-server {
                8.8.8.8;
            }
            login {
                message "Welcome to the cloud\npassword is Clouds\n";
                user juniper {
                    uid 2000;
                    class super-user;
                    authentication {
                        encrypted-password "$1$PndA2gfi$fxeFR06HEsQpYFB/lp6je1";
                    }
                }
            }
            services {
                finger;
                ftp;
                rlogin;
                rsh;
                ssh;
                telnet;
                xnm-clear-text;
            }
            syslog {
                host log {
                    kernel info;
                    any notice;
                    pfe info;
                    interactive-commands any;
                }
                file messages {
                    kernel info;
                    any notice;
                    authorization info;
                    pfe info;
                    archive world-readable;
                }
                file security {
                    interactive-commands any;
                    archive world-readable;
                }
            }
            archival {
                configuration {
                    transfer-on-commit;
                    archive-sites {
                        "ftp://tftp:tftp@10.233.255.254/active/configset";
                    }
                }
            }
            processes {
                routing enable;
                management enable;
                watchdog enable;
                snmp enable;
                inet-process enable;
                mib-process enable;
            }
        }
        chassis {
            dump-on-panic;
        }
        security {
            forwarding-options {
                family {
                    inet6 {
                        mode packet-based;
                    }
                    mpls {
                        mode packet-based;
                    }
                    iso {
                        mode packet-based;
                    }
                }
```

```
            }
        }
    }
}
apply-groups [ global member0 ];
system {
    host-name CE SEDE MARTE;
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.233.253.63/20;
                address 10.233.248.13/20;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        unit 101 {
            description "Interfaz a PE MARTE";
            vlan-id 101;
            family inet {
                address 10.3.3.2/30;
            }
        }
    }
    ge-0/0/2 {
        vlan-tagging;
        unit 103 {
            description "Interfaz a Receptor MARTE";
            vlan-id 103;
            family inet {
                address 10.10.30.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.33.33.33/32;
            }
        }
    }
}
routing-options {
    max-interface-supported 10;
    autonomous-system 65000;
    multicast {
        ssm-map GRUPO-FUENTE {
            policy GRUPOS;
            source 10.10.10.10;
        }
    }
}
protocols {
    igmp {
        query-interval 10;
        query-response-interval 3;
        interface ge-0/0/2.1 {
            ssm-map GRUPO-FUENTE;
        }
        interface ge-0/0/1.101 {
            disable;
        }
        interface ge-0/0/2.103 {
            version 3;
            static {
                group 239.1.1.1 {
                    source 10.10.10.10;
                }
                group 239.1.1.10 {
                    source 10.10.10.10;
                }
            }
        }
    }
    bgp {
        group PE {
            export LOOPBACK;
            peer-as 12956;
            neighbor 10.3.3.1;
        }
    }
    pim {
        interface ge-0/0/1.101 {
            mode sparse;
        }
    }
}
policy-options {
    policy-statement GRUPOS {
        term MULTICAST {
            from {
```

```
                route-filter 239.1.0.0/16 orlonger;
            }
            then accept;
        }
        term RESTO {
            then reject;
        }
    }
    policy-statement LOOPBACK {
        term LOOPBACK {
            from {
                route-filter 10.33.33.33/32 exact;
            }
            then accept;
        }
    }
}
```