FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

ANALISIS COMPARATIVO PARA LA SELECCIÓN DEL PROTOCOLO MPLS Y SPB PARA IMPLEMENTAR UNA RED BACKBONE DE UN ISP

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:
Bach. Rudy Carlos Ostoa

Asesor:
Mg. Tuesta Monteza Víctor Alexci

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel, Perú
2020

DEDICATORIA

Gracias a mis padres por inculcarme que la educación es la base para ser el mejor profesional en el desempeño de la carrera que he elegido.

Rudy Carlos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

AGRADECIMIENTOS

Nuestro especial agradecimiento a las empresas usuarios de los servicios de interconexión de redes de datos quienes nos han brindado el apoyo necesario para la investigación referente al tema, a nuestros padres por su apoyo incondicional.

A todos ellos muchas gracias

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RESUMEN

En la actualidad los proveedores de servicio de internet son los responsables del transporte de todo el flujo de datos en cada país, para ellos es importante se garantice el buen funcionamiento y garantizar la disponibilidad de la red.
Los protocolos de transporte garantizaran el buen funcionamiento del backbone del operador no se sature y esto ocurre debido a la cantidad de paquetes que circulan por la red pueden consumir recursos de procesador y memoria de los Router.
Actualmente el protocolo MPLS (Multiprotocol Label Switching) opera en la capa de enlace y red del modelo OSI definido en la RFC 3031 es el más utilizado.

SPB (Shortest Path Bridging) es un estándar especificado en la norma IEEE 802.1aq. Es una tecnología de red destinada a simplificar la creación y configuración de redes de ordenadores al tiempo que permite el enrutamiento de trayectos múltiples. Utiliza el sistema Intermediate System to Intermediate System (IS-IS), un protocolo de estado de enlace con grado de portador probado, para construir dinámicamente la topología entre nodos de red, ahorrando tiempo y esfuerzo a los administradores de red y eliminando virtualmente el error humano.
En este trabajo se analizará, compara y determinará el protocolo apropiado en la implementación de la red backbone del operador IP para sustituir el actual protocolo.

Palabras Claves:

MPLS, MPLS VPN, VRF, LDP, TDP, LSR, LSP, VPLS, SPB, QoS calidad de servicio.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ABSTRACT

Currently, internet service providers are responsible for transporting the entire flow of data in each country, for them it is important to ensure the smooth operation and ensure the availability of the network.

Transport protocols will ensure the smooth operation of the backbone of the operator is not saturated and this occurs because the number of packets that circulate through the network can consume processor resources and memory of the Routers.

Currently the MPLS protocol (Multiprotocol Label Switching) operates in the link layer and network of the OSI model defined in RFC 3031 is the most used.

Shortest Path Bridging (SPB) is a standard specified in the IEEE 802.1aq standard. It is a network technology designed to simplify the creation and configuration of computer networks while allowing the routing of multiple paths. It uses the Intermediate System to Intermediate System (IS-IS), a link-state protocol with proven carrier grade, to dynamically construct the topology between network nodes, saving time and effort to network administrators and virtually eliminating the error human.

In this paper, we will analyze, compare and determine the appropriate protocol in the implementation of the IP operator backbone network to replace the current protocol.

Keywords:,

MPLS, MPLS VPN, VRF, LDP, TDP, LSR, LSP, VPLS, SPB, QoS calidad de servicio.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE FIGURAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICE DE TABLAS

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

I. INTRODUCCIÓN

1.1 Realidad Problemática

El servicio de internet en el Perú comenzó desde febrero de 1991, desde esa fecha el número de empresas proveedoras de servicios se ha incrementado notablemente. (Tumial y Cruz, 2004).

En la actualidad los ISP tienen una red Metro Ethernet que utiliza la red de fibra óptica este medio de transmisión brinda un gran ancho de banda para poder atender la demanda de los usuarios que utilizan aplicaciones de voz, datos y video, ahora deben definir la elección de un protocolo de transporte.

Una de las principales preocupaciones de los operadores de red es que los enrutadores actuales no son escalables para satisfacer las necesidades futuras de tráfico en el núcleo de Internet teniendo en cuenta las nuevas aplicaciones. Los enrutadores de próxima generación con capacidad de conmutación de petabit se están construyendo para satisfacer demandas más altas. Su capacidad de procesamiento se ve reforzada por recursos adicionales de memoria y computación en tarjetas de control y líneas con un gran número de interfaces de alta velocidad. (Nguyen y Jaumard, 2013)

Los estudios presentados corroboran que los usos de estos protocolos no resuelven los problemas en las empresas que los usan, estos mismos problemas son los que se evidencian en la empresa en estudio.

Actualmente MPLS es un estándar de IETF que surgió para agrupar a diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mediados de los 90. Como protocolo ofrece los servicios: MPLS VPN Layer 2, MPLS VPN Layer 3, MPLS-TE.Calidad de Servicio (QoS).

En la actualidad Shortest Path Briding (SPB) se está convirtiendo rápidamente en una de las principales tecnologías de red para ofrecer un el transporte basado en Ethernet donde todos los servicios de red ya sean IPv4, IPv6, IP Multicast y / o simplemente L2 VLAN pueden ser desacoplados de la infraestructura física y virtualizados para satisfacer las necesidades y demandas de las medianas y grandes empresas típicas. SPB fue originalmente definido para las redes Carrier Ethernet para complementar y extender Carrier MPLS backbones de la cual hereda muchos atributos deseables con una arquitectura dramáticamente simplificada. SPB es la combinación de 3 estándares

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

de IEEE que entregan un nuevo paradigma a la manera en que las redes basadas Ethernet pueden funcionar. SPB proporciona esencialmente encapsulación MAC-in-MAC con la separación de direcciones IP / MAC de cliente en el reenvío MAC de borde y columna vertebral en el núcleo. El backbone MAC (BMAC) se utiliza para la accesibilidad a otros nodos SPBM utilizando IS-IS como el protocolo de enrutamiento IGP.

Un nodo en el núcleo tiene un trabajo muy simple de hacer, ya que sólo tiene que mirar a la columna vertebral MAC para el reenvío y al mismo tiempo proporcionar una espina dorsal sigilo con el MAC-in-MAC mecanismo de encapsulación y el hecho de que no hay dirección IP necesario en el núcleo. La encapsulación MAC-in-MAC IEEE802.1ah, que es rigurosamente utilizada por SPBM, trae a Ethernet una jerarquía de direccionamiento donde el direccionamiento de red de estaciones finales y dispositivos de usuario (ya sea en L2 con direcciones MAC o en L3 con direccionamiento IPv4 o IPv6) siempre son vistos como accesibles a través de la dirección MAC del nodo SPB de una columna vertebral (BMAC). Desde cualquier nodo de origen dado, el destino BMAC define de forma única la ruta de reenvío de corte sin ningún cambio de etiqueta (MPLS) o enrutamiento IP de salto por salto. (Avaya Inc., 2015)

Los Proveedores de servicios de Internet tiene el compromiso de ofrecer la disponibilidad del 99.98% de disponibilidad dentro de su red de transporte y una pérdida de paquetes menor al 1% mensual, esto los lleva a elegir un protocolo que le permita garantizar los servicios que ofrecer a sus clientes.

Las entidades públicas solicitan en sus TDR (Términos de Referencia) el uso de un protocolo de transporte en el backbone del operador, este requerimiento obliga al ISP a elegir un buen protocolo ofrecer sus servicios.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.2 Antecedentes de estudio

(Mack-crane y Yong, 2011). En el Journal afirma "*SPB over MPLS*. Describió los casos de uso del protocolo SPB con los servicios que provee MPLS. El protocolo SPB provee servicios similares a MPLS. El uso de este protocolo es confiable en las redes de ISP" (p.4).

(Sepulveda Baldenebro, 2009) en su Investigación "*APLICACIÓN DE MPLS EN REDES VoIP* Actualmente, MPLS (Multiprotocol Label Switching) se caracteriza por ser una red bastante segura debido a que no permite la entrada o salida de datos de la trayectoria de conmutación de paquetes LSP por lugares que no han sido establecidos por el administrador de la red, además; cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores, solo por el módulo de envío MPLS, que intercambiará la etiqueta conforme a la tabla de envío del enrutador de conmutación de etiquetas LSR, lo que impide en gran medida que usuarios puedan ver información que no les corresponde" (p.19).

(Rojas Sánchez, 2013) En su tesis "*Contribuciones en Arquitecturas de Redes de Conmutadores transparentes Ethernet de altas prestaciones* La tecnología de SPB facilita la construcción de redes Ethernet lógicas sobre infraestructuras Ethernet usando un protocolo de estado de enlace para anunciar tanto la topología, como la pertenencia a cierta red lógica. Los paquetes se encapsulan en el switch frontera mediante MAC-in-MAC (IEEE 802.1ah) o tramas etiquetadas (IEEE 802.1Q/802.1ad) y son transportadas únicamente a los miembros de la red lógica." (p.16).

(Carral Pelayo y Henares, 2013) En su Tesis "*Contribución al Diseño de Conmutadores Transparentes Avanzados Basados en Tecnología Ethernet,* SPB define un núcleo de red formado por conmutadores cuyo plano de control ejecuta una extensión del protocolo IS-IS para diseminar la información topológica necesaria para el posterior cálculo de rutas mediante un algoritmo de camino más corto como Dijkstra. Dentro del núcleo SPB se calculan árboles de difusión enraizados en cada uno de los nodos y se garantiza la congruencia de los caminos (ramas de los dos árboles correspondientes) que unen dos nodos determinados" (p.4).

Si bien conceptualmente SPB es igual a TRILL (que también utiliza IS-IS para el cálculo del camino óptimo), la manera en que SPB envía los paquetes difiere ya que SPB aplica una etiqueta (VID) al paquete cuando éste ingresa al dominio (o la traduce a otra etiqueta si ya existe una) y la quita (o la vuelve a traducir) cuando el paquete sale del dominio. La otra variante de SPB es "Shortest Path Bridging MAC" (SPBM), donde se usa el

encapsulado MAC- en-MAC. Cuando un paquete ingresa al dominio, el dispositivo SPB de ingreso determina el dispositivo de egreso. El paquete original se encapsula en otro paquete Ethernet con la MAC de destino del dispositivo SPB de egreso, donde el paquete original es desencapsulado y se envía a su destino final [122]. SPB" (p.121).

1.2.1 Estado del Arte

(Orozco Lara, 2014) En su tesis afirma “MPLS es una tecnología de transmisión de paquetes de alto rendimiento que integra la gestión del rendimiento y el tráfico con capacidades de capa de enlace de datos de conmutación con la escalabilidad, flexibilidad y rendimiento de la capa de red de enrutamiento. Permite a los proveedores de servicios para responder a los desafíos provocados por crecimiento explosivo y proporciona la oportunidad para que los servicios diferenciados sin necesitar el sacrificio de la infraestructura existente” (p.23).

(Gestido, 2014) En su Tesis “VIRTUALIZACIÓN DE REDES EN LA EMPRESA, Si bien conceptualmente SPB es igual a TRILL (que también utiliza IS-IS para el cálculo del camino óptimo), la manera en que SPB envía los paquetes difiere ya que SPB aplica una etiqueta (VID) al paquete cuando éste ingresa al dominio (o la traduce a otra etiqueta si ya existe una) y la quita (o la vuelve a traducir) cuando el paquete sale del dominio. La otra variante de SPB es “Shortest Path Bridging MAC” (SPBM), donde se usa el encapsulado MAC- en-MAC. Cuando un paquete ingresa al dominio, el dispositivo SPB de ingreso determina el dispositivo de egreso. El paquete original se encapsula en otro paquete Ethernet con la MAC de destino del dispositivo SPB de egreso, donde el paquete original es desencapsulado y se envía a su destino final" (p.121).

(Ferrari, Flammini, Rinaldi, Prytz, y Hussain, 2014) En su investigación “Multipath redundancy for industrial networks using IEEE 802.1aq Shortest Path Bridging” En una red industrial basada en SPB, los nodos finales son generalmente conectados al Backbone SPB por medio de un solo enlace extremo. El conmutador SPB recibe el paquete entrante y, utilizando la tabla de filtrado (FT), envía el paquete a los puertos de salida adecuados. La regla de filtrado del FT se obtiene aplicando el Algoritmo de Dijkstra en la base de datos de estado de enlace (LSDB) constantemente actualizada por el protocolo IS-IS. Los paquetes entrantes siempre a lo largo del camino más corto (SP). En el caso de un fallo, el LSDB se actualiza y un SP nuevo es calculado por el conmutador SPB. Tenga en cuenta que durante la reconfiguración (que puede tomar hasta varios cientos de ms en una red más grande) los paquetes en la ruta afectada por el fallo son la pérdida. Una solución general para evitar la pérdida de paquetes y

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

garantizar la (a.k.a. "tiempo de recuperación cero") operación en caso de fallo es la transmisión de copias del mensaje en menos, uno físicamente ruta separada; Estas técnicas de duplicación se conocen en la literatura como enmascaramiento de fallas y se aplican en industrial aplicación por protocolo de redundancia paralela (PRP) y protocolos de redundancia continua de alta disponibilidad (HSRP).

Las conclusiones del análisis del trabajo en la redundancia para sistemas de automatización utilizando el puente IEEE 802.1aq Shortest Path Bridging (SPB). La característica clave de SPB son el tiempo de recuperación cero y la capacidad de usar la comunicación paralela multitrayecto en la misma red de malla. Se ha definido un nuevo indicador de asimetría y un indicador de redundancia para comparar fácilmente las soluciones "tradicionales" de redundancia existentes para la industria con las nuevas redes basadas en SPB. Los resultados de la simulación con topologías de red genéricas muestran que el uso del mismo porcentaje de redes de conexión más grandes ofrece mayor redundancia. Ejemplos específicos con una topología con dos anillos que funcionan en paralelo (como suele emplearse en la industria para aplicaciones de alta disponibilidad) resaltan que la SBP puede ofrecer el mismo nivel de redundancia utilizando sólo una red interconectada en aproximadamente el 85%. (p.3-4).

(Stevens, 2015) En su investigación “Avaya SPB Fabric Concept and Design” Shortest Path Bridging (SPB) se está convirtiendo rápidamente en una de las principales tecnologías de red para ofrecer la entrega basada en Ethernet en el que todos los servicios de red ya sean IPv4, IPv6, IP Multicast y / o simplemente L2 VLAN pueden ser desacoplados de la infraestructura física y virtualizados para satisfacer las necesidades y demandas de las medianas y grandes empresas típicas.

SPB fue originalmente definido para las redes Carrier Ethernet para complementar y extender Carrier MPLS backbones de la cual hereda muchos atributos deseables con una arquitectura dramáticamente simplificada.

SPB es la combinación de 3 estándares de IEEE que entregan un nuevo paradigma a la manera en que las redes basadas Ethernet pueden funcionar. SPBM proporciona esencialmente encapsulación MAC-in-MAC con la separación de direcciones IP / MAC de cliente en el reenvío MAC de borde y backbone en el núcleo. El backbone MAC (BMAC) se utiliza para la accesibilidad a otros nodos SPBM utilizando IS-IS como el protocolo de enrutamiento IGP. Un nodo en el núcleo tiene un trabajo muy simple de hacer, ya que sólo tiene que mirar a backbone MAC para el reenvío y al mismo tiempo

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

proporcionar una espina dorsal sigilo con el MAC-in-MAC mecanismo de encapsulación y el hecho de que no hay dirección IP necesario en el núcleo.

La encapsulación MAC-in-MAC IEEE802.1ah, que es rigurosamente utilizada por SPBM, trae a Ethernet una jerarquía de direccionamiento donde el direccionamiento de red de estaciones finales y dispositivos de usuario (ya sea en L2 con direcciones MAC o en L3 con direccionamiento IPv4 o IPv6) siempre son vistos como accesibles a través de la dirección MAC del nodo SPB de una columna vertebral (BMAC). Desde cualquier nodo de origen dado, el BMAC de destino define de forma única la ruta de desvío de paso sin ningún cambio de etiqueta (MPLS) o enrutamiento IP de salto por salto.

El estándar SPB IEEE802.1aq aprovecha esta jerarquía de direccionamiento reemplazando los antiguos protocolos Spanning Tree y trayendo a las redes basadas en Ethernet el conocido y muy apreciado protocolo Link State Routing IS-IS que es capaz de calcular el camino más corto a cualquier BMAC dentro de la Tela Ethernet. Como tal un tejido SPB se comporta con todas las mismas propiedades que los administradores de red esperan ver desde una red basada en IP tradicional utilizando OSPF o IS-IS como el IGP (p.9).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.3 Teorías relacionadas al tema

1.3.1 Shortest Path Bridging (SPB)

(SPB), es un estándar especificado en la norma IEEE 802.1aq. Es una tecnología de red destinada a simplificar la creación y configuración de redes de ordenadores al tiempo que permite el enrutamiento de trayectos múltiples.

La tecnología discutida en este documento de diseño hace uso de SPBM, que aprovecha los beneficios traídos por el 802.1ah Mac-in-Mac encapsulación. A lo largo de este documento, cuando nos referimos a Shortest Path Bridging como SPB, siempre nos referimos a SPBM.

Pero quizás la innovación más importante que IEEE802.1ah introduce en Ethernet es la adición de un nuevo campo de Service-ID (I-SID) de 24 bits en el encapsulado MAC-in-MAC. Esto solo trae la habilidad de virtualizar y transportar todos y cada uno de los tipos de servicio, que anteriormente sólo las backbones basadas en MPLS eran capaces de soportar, directamente sobre una red basada en Ethernet.

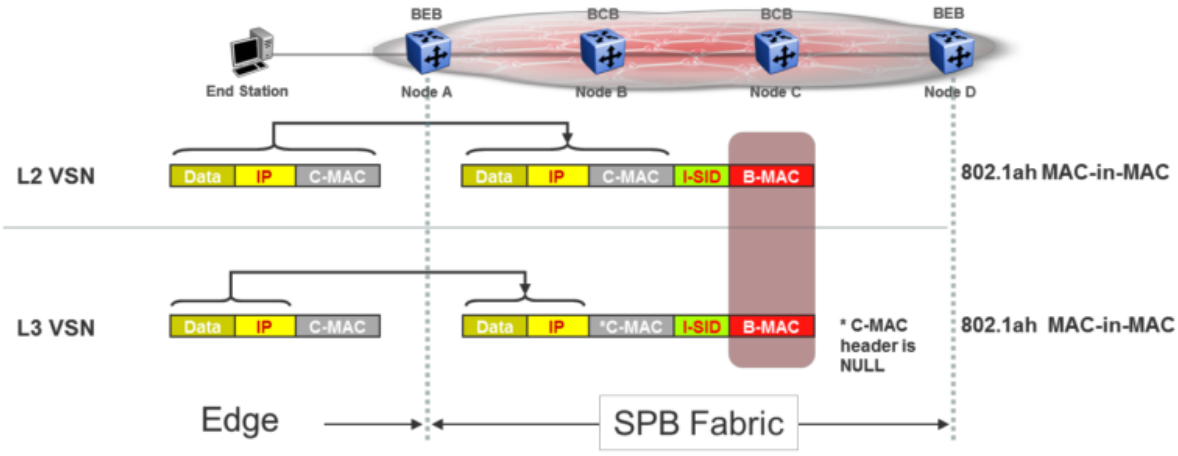

Figura 1 SPBM´s MAC-in-MAC encapsulación

Fuente. (Avaya SPB Fabric Solution, 2015)

Como comparación, MPLS empuja siempre dos o más etiquetas en un paquete Ethernet (u otro tipo de tecnología L2). Pero no todas las etiquetas de MPLS son iguales. La etiqueta más externa es una etiqueta de reenvío de paquetes que se utiliza para la etiqueta de conmutación del paquete a través de la columna vertebral MPLS (en un tejido basado en SPB esta función se lleva a cabo por la dirección de destino de BMAC). Las etiquetas MPLS internas se utilizan

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

puramente como VPN-ids, es decir, una vez que el paquete ha llegado a su destino a través del backbone MPLS, la etiqueta interna determinará si la carga útil se transmite a una u otra instancia VRF / VPLS (en un SPB-based Fabric esta función es asumida por el I-SID).

Por encima de eso, la capacidad de IS-IS para calcular árboles de trayecto más cortos es por primera vez apalancada, en la capa Ethernet, para producir árboles de multidifusión de trayecto más corto específicos de servicio para uso con tipos de servicio L2 así como para IP Corrientes de multidifusión. Los tipos de servicio L2 necesitan transportar de forma eficiente paquetes multicast y no difundidos unicast de broadcast, (non-snooped) sobre el SPB backbone para su entrega en cada otro punto final en el mismo servicio. Los flujos de multidifusión IP necesitan ser replicados en toda la estructura sólo donde existan los receptores IGMP. Por razones de comparación, la capacidad de soportar nativamente árboles multidifusión simplemente no existe con IP. La razón por la cual, para IP, el trato con IP Multicast es tan complejo es porque se implementó como un complemento que requiere complejos protocolos adicionales como PIM-SM, que ahora pueden ser completamente eliminados en un tejido basado en SPB Ethernet.

En aras de la comparación, esta es una capacidad que IP nunca ha tenido de forma nativa y para la cual gran parte de la complejidad de tratar con IP Multicast como una segunda idea descansa en protocolos complejos como PIM-SM que ahora pueden ser completamente eliminados en un SPB Tela Ethernet.

El estándar IEEE802.1ag es la nueva base de operaciones, administración y administración (OAM) sobre redes basadas en Ethernet para la configuración y administración de fallos (CFM). Definido por los transportistas para su uso en redes portadoras (incluyendo las basadas en MPLS), este estándar aporta a Ethernet y SPB un conjunto de herramientas de solución de problemas mucho más sofisticado de lo que cualquier cliente Enterprise está acostumbrado a usar con IP. El CFM basado en Ethernet es capaz de probar las pruebas de conectividad más básicas (ping) para el trazado de ruta (traceroute) sobre unicast y árboles de multidifusión específicos del servicio (tracetree y tracemroute), así como el Monitor de rendimiento de red via Y1731 extensiones.

Los beneficios de la prestación de tipos de servicio MPLS sobre un tejido basado en SPB es muchas veces. Para empezar MPLS es complejo y se basa en una multitud de protocolos de plano de control cada uno con sus propias

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

complejidades y dependencias de capa de protocolo. Ser capaz de entregar un tejido basado en Ethernet con un solo plano de control (IS-IS) que soporta todos los tipos de servicio como MPLS, pero sin necesidad de ingeniería de la columna vertebral con OSPF, Multiprotocolo BGP, BGP Ruta Reflectores, LDP y PIM-SM hace para una vida más fácil para los administradores de redes empresariales, tanto en términos de diseño como en términos de mantenimiento e inevitablemente en términos de coste.

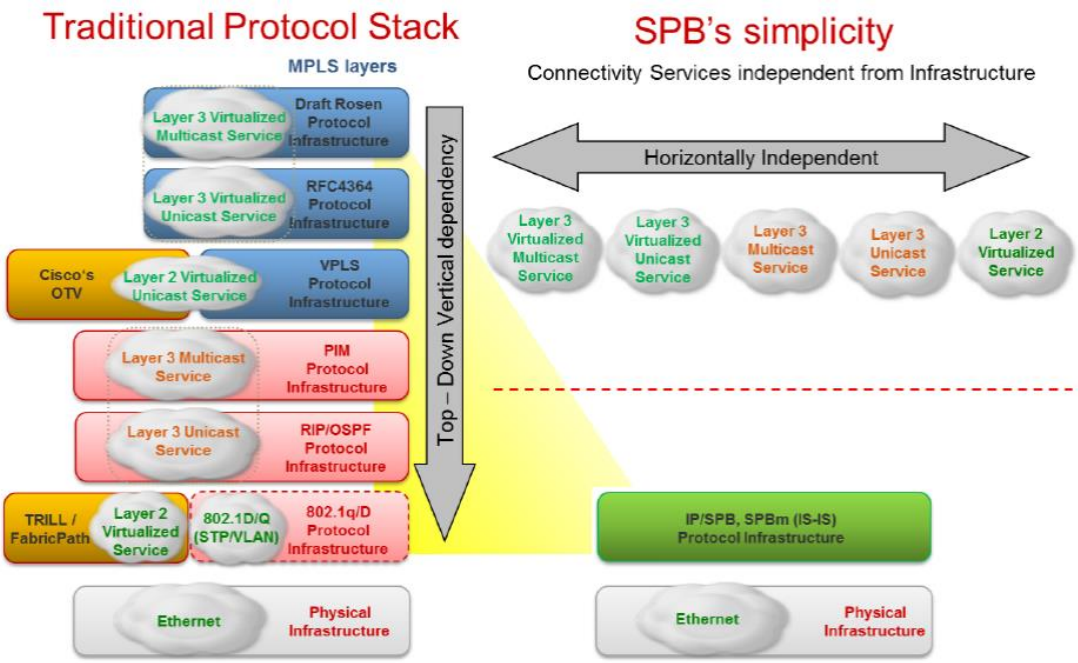

Figura 2. Comparación de SPB simplicidad con la pila del protocolo tradicional
Fuente. (Avaya SPB Fabric Solution, 2015)

1.3.2 Descripción de la virtualización L3

El despliegue de dominios de enrutamiento L3 virtualizados sobre una red SPB Ethernet se consigue de una manera que tiene muchas similitudes con los IPVPN basados en MPLS. Cada dominio de enrutamiento L3 se termina en una entidad de enrutador virtual (VRF) ubicada en los nodos de capa de distribución. Estos nodos de distribución intercambian rutas I-SID-IPv4 (o I-SID-IPv6) a través de IS-IS bien definidos Tipo Longitud Valores (TLVs). Estos TLVs existirán así en el LSDB IS-IS del SPB Fabric pero solo serán inspeccionados por otros nodos de distribución donde se terminen los mismos servicios I-SID. Los nodos principales, que no están configurados con ningún I-SID, no toman en cuenta estos TLVs y

actúan como transporte mediante el reenvío de paquetes basados en el camino más corto hacia el destino BMAC. Los nodos de distribución tienen interfaces directamente conectadas para las subredes de capa de acceso que pueden extenderse a los interruptores de borde o los conmutadores conectados a la red. Si está conectado a un conmutador Fabric Attached, la VLAN L2 correspondiente, que puede derivarse mediante una autenticación basada en la configuración o en una red basada en identidad. Estas VLAN están asociadas con un VRF en los nodos de distribución en los que una VLAN dada puede pertenecer a uno y sólo un VRF. VRF múltiples pueden configurarse en el enrutador de la capa de distribución, cada uno perteneciente a un id de servicio de ancho de banda (I-SID), proporcionando así multiten- tenance en redes de servicios virtuales de capa 3 (L3 VSN).

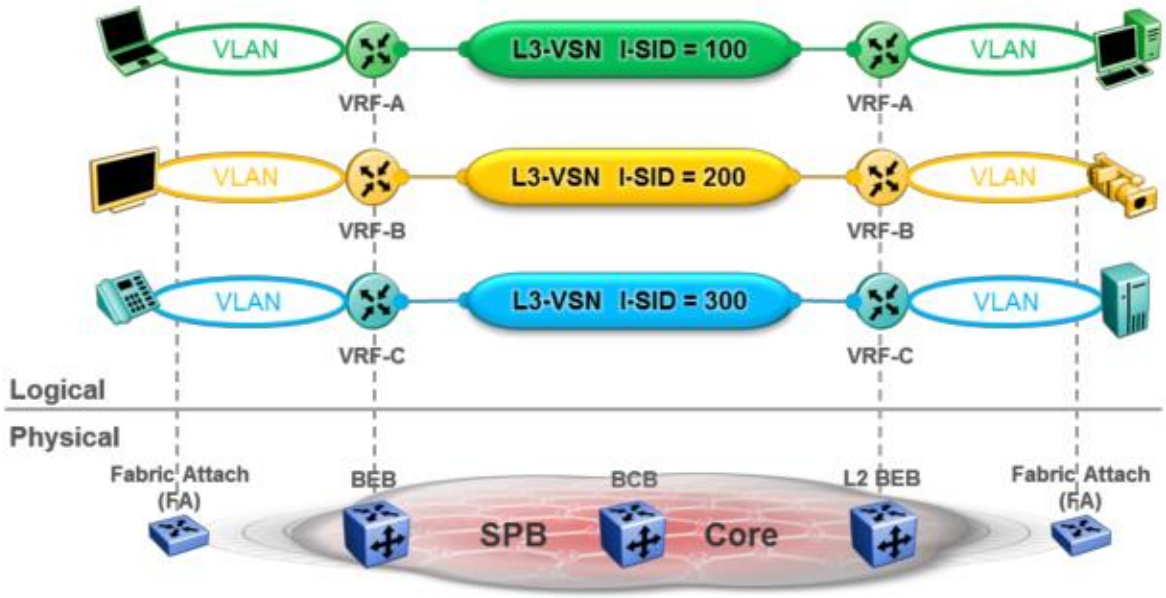

Figura 3. Virtualización L3 con SPB L3 VSNs

Fuente. (Avaya SPB Fabric Solution, 2015)

Beneficios del SPB L3 VSN sobre MPLS-VPN:

a) Definición de servicio simple a través de la configuración de ID de servicio (I-SID) en el punto final VRF en lugar de tener que definir varios importes y exportación complejos BGP Route Targets y BGP Route Descriptors
b) El mismo I-SID también se utiliza en el MAC-in-MAC encapsulación de paquetes, mientras que con MPLS-VPNs las etiquetas MPLS interno

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

(utilizado como VPN-id) sólo tienen una correlación indirecta con BGP Route Target configuración

c) No hay necesidad de BGP (por lo tanto, no hay necesidad de BGP Route Reflectores tampoco).
d) No hay necesidad de MPLS (por lo tanto, no hay necesidad de un IGP IP, o LDP).
e) De hecho, no hay interfaces IP / subredes dentro de Ethernet Fabric. Las interfaces IP sólo existen en las VLAN en las que se conectan estaciones finales. Es decir. Las interfaces IP sólo existen como puertas de enlace para los servicios VSN que terminan.
f) L3 VSNs puede ser IP Multicast habilitado con 1 clic por nodo de distribución (no hay necesidad de IETF complejo Rosen MVPNs y PIM-SM en IGP).
g) La segunda convergencia secundaria como SPB se basa en un único protocolo de enrutamiento de estado de enlace (IS-IS), mientras que MPLS depende de BGP, LDP, OSPF pila de protocolo que no puede lograr el mismo.

1.3.3 Descripción de la Virtualización L2

SPB ofrece de forma nativa una gama muy flexible de conectividad L2 a través de Ethernet Fabric para lograr servicios TLS (Transparent LAN Services). El concepto de servicios LAN transparentes es la capacidad de conectar segmentos Ethernet separados geográficamente y hacer que estas redes aparezcan como un solo dominio VLAN Ethernet o L2. Esto básicamente permite que cualquier VLAN L2 de borde sea Tela extendida a cualquier otro nodo en el backbone SPB. Esto puede aplicarse a cualquier VLAN, incluyendo las VLAN de borde usadas en el modelo de implementación de virtualización L3 anterior (que tienen una interfaz IP y están enrutadas IP como parte de un dominio L3 dado), así como segmentos de VLAN L2 aislados que no son IP enrutado en cualquier lugar. Estas redes de servicios virtuales de capa 2 (L2 VSN) ofrecen un tipo de servicio nativo (any-any) (E-LAN) que significa que un VSN L2 puede tener cualquier número de puntos finales y que el aprendizaje MAC se realiza dentro del servicio VSN.

Además del tipo de servicio E-LAN nativo, SPB L2 VSN también puede ofrecer fácilmente un servicio E-LINE (punto-punto), (que es esencialmente un servicio

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

E-LAN con sólo 2 puntos finales), así como E -TREE (private-VLAN) tipos de servicio que permite la extensión sobre el tejido Ethernet de borde privado-VLANs donde los puertos de acceso se pueden configurar como promiscua o aislada.

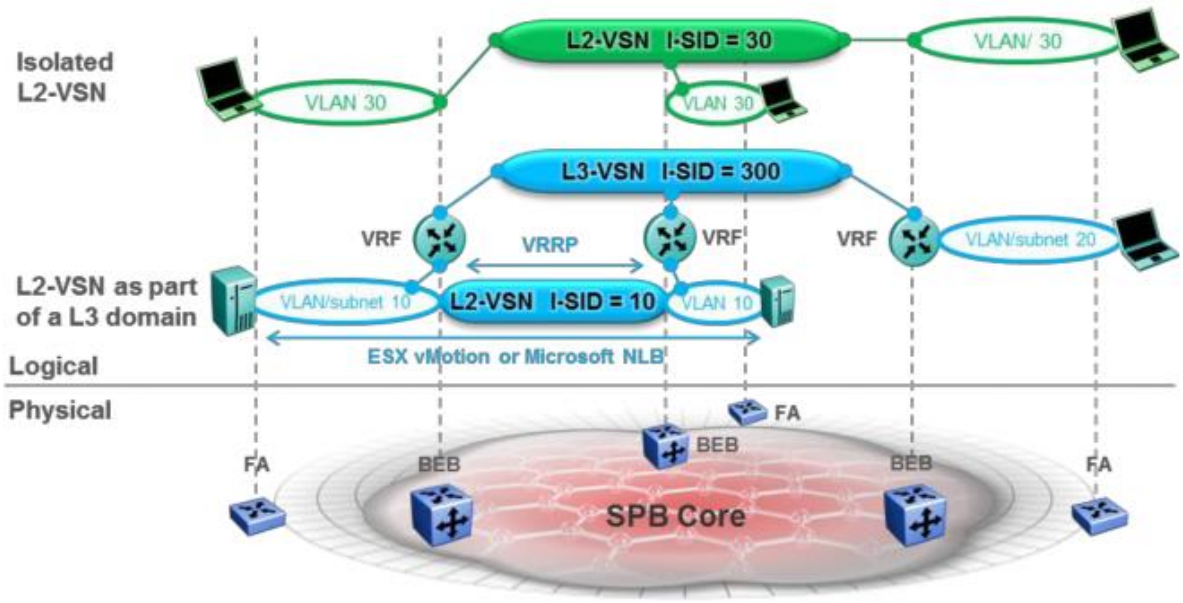

Figura 4. Virtualización L2 con SPB L2 VSNs

Fuente. (Avaya SPB Fabric Solution, 2015)

La naturaleza misma de SPB asegura que no puede haber bucles dentro del backbone de Ethernet Fabric y la implementación de Avaya admite totalmente la tecnología de Split Multi-Link Trunk (SMLT)1 en los nodos de borde SPB (BEBs) lo que significa que los VSN L2 pueden ser extendidos sin bucles y sin Spanning Tree todo el camino hasta el acceso.

Beneficios of SPB L2 VSNs sobre EoMPLS y MPLS-VPLS

a) Definición de servicio simple a través del mismo identificador de servicio (I-SID), pero esta vez configurado en la combinación de puerto VLAN y / o UNI de punto final (literalmente un comando CLI), en lugar de especificar un circuito virtual (VC) en EoMPLS o una instancia de conmutador virtual (VSI) en VPLS.
b) SPB L2 Los VSN ofrecen de forma nativa los tipos de servicio E-LAN (any-any), E-LINE (punto-punto) y E-TREE (private-VLAN). EoMPLS es sólo punto-punto y VPLS es una extensión de EoMPLS que crea dinámicamente una malla completa de circuitos de EoMPLS para

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

proporcionar cualquier tipo de servicio. Esto tiene una serie de desventajas.

c) SPB L2 Los VSN no tienen ningún problema de manipulación de la replicación de paquetes en el Fabric, que se necesita para entregar el tráfico de difusión y multidifusión dentro del servicio; esto se debe a que el SPB Fabric puede asignar árboles de trayectos más cortos específicos del servicio. Mientras que la principal deficiencia de VPLS es que todos los paquetes de difusión y multidifusión deben ser replicados por el nodo PE de entrada varias veces en la misma interfaz física (cada vez con una etiqueta MPLS diferente) que se vuelve exponencialmente ineficiente como el número de puntos finales en VPLS VSI aumenta.
d) El SPB combinado con el SMLT de Avaya ofrece una solución activa-activa con nodos redundantes de distribución (BEB-SMLT). VPLS tiene un inconveniente importante con doble homing una VLAN de acceso en 2 redundantes nodos de PE de distribución, ya que esto da como resultado un bucle L2 que ni VPLS ni Spanning Tree pueden evitar. El enfoque común es dejar que sólo uno de los PE (Primaria N-PE) realice el reenvío de tráfico y el N-PE de reserva sólo reenvíe el tráfico en caso de fallo; Primaria y Standby PEs suelen ser escalonada a través de las instancias VSI.
e) ¿No hay necesidad de BGP (por lo tanto, no hay necesidad de BGP Route Reflector tampoco)? No hay necesidad de MPLS (por lo tanto, no hay necesidad de un IGP IP subyacente, o LDP).
f) Los VSN de L2 pueden ser IP Multicast snoop-enabled con un clic por nodo de punto final. Esto simplemente no es posible con VPLS que siempre inundará el tráfico de multidifusión IP con la falla mencionada anteriormente que el tráfico de multidifusión es ineficientemente de ingreso replicado.

El service-id I-SID representa la unión para interconectar L2 VSN puntos finales juntos. Como tal, el VLAN-id solo tiene importancia local y puede volver a asignarse a diferentes valores en los extremos terminales. Esto se puede combinar con un rango de tipos de punto final de usuario a red (UNI) que permiten asignar el servicio I-SID a una VLAN-id (CVLAN UNI) en un puerto Ethernet sin procesar (UNI transparente) la combinación de VLAN-id + puerto Ethernet (UNI

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

conmutado) que permite asignar la misma VLAN-id en diferentes puertos Ethernet del mismo conmutador a diferentes VSN L2. (Stevens, 2015) (p.9-15).

1.3.4 MPLS (Multiprotocol Label Switching)

(Cisco System et al., 2016) Las etiquetas MPLS se anuncian entre enrutadores para que puedan crear una asignación de LABEL a LABEL.

Estas etiquetas se adjuntan a los paquetes IP, lo que permite a los routers reenviar el tráfico mirando la etiqueta y no la dirección IP de destino. Los paquetes se reenvían mediante conmutación de etiquetas en lugar de mediante conmutación de IP.

La técnica de cambio de etiqueta no es nueva. Frame Relay y ATM lo usan para mover cuadros o celdas a través de una red. En Frame Relay, la trama a celda de longitud fija consta de un encabezado de 5 bytes y una carga útil de 48 bytes. El encabezado de la celda ATM y el marco Frame Relay se refieren al circuito virtual en el que reside la celda o el marco. La similitud entre Frame Relay y ATM es que en cada salto a través de la red, se cambia el valor de "etiqueta" en el encabezado. Esto es diferente del reenvío de paquetes IP. Cuando un enrutador reenvía un paquete IP, no cambia un valor que pertenece al destino del paquete; es decir, no cambia la dirección IP de destino del paquete. El hecho de que las etiquetas MPLS se utilizan para reenviar los paquetes y ya no la dirección IP de destino ha llevado a la popularidad de MPLS. Estos beneficios, como la mejor integración de IP sobre ATM y la popular aplicación de red privada virtual (VPN) MPLS.

¿Cuál es la estructura de la escritura de la etiqueta?

Los primeros 20 bits son el valor de la etiqueta. Este valor puede estar entre 0 y 220-1, o 1,048,575. Sin embargo, los primeros 16 valores están exentos del uso normal; es decir, tienen un significado especial.

Los bits 20 a 22 son los tres bits experimentales (EXP). Estos bits se utilizan únicamente para la calidad del servicio (QoS).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

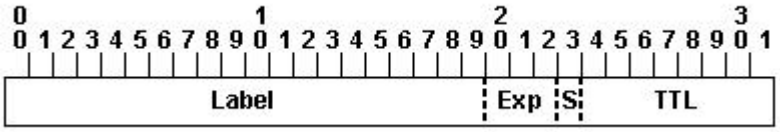

Figura 5. Estructura de una etiqueta MPLS

Fuente. (Cisco, 2016)

Escritura de la etiqueta - Valor de etiqueta (no estructurado), 20 bits

Exp - Uso experimental, 3 bits; utilizado actualmente como campo del Clase de Servicio (CoS)

S - Parte inferior del stack, 1 bit

TTL - Time to Live, 8 bits

¿Dónde la escritura de la etiqueta será impuesta en un paquete?

La etiqueta se asigna entre la capa del link de datos (encabezado y capa de red (encabezado de la capa 2) de la capa 3). Al ordenarse en la pila de protocolos primero aparece el paquete, y la parte inferior aparece la más reciente. El paquete de capas de red sigue inmediatamente la escritura de la etiqueta más reciente de la pila de etiquetas.

Figura 6. Escritura de etiqueta MPLS

Fuente. (Cisco, 2016)

Cada etiqueta contiene 4 campos:

- 20 bits - Valor de la etiqueta.
- bits - Campo experimental reservado para usos futuros.
- 1 bit - Final de la pila. Si tiene el valor 1 entonces es la última etiqueta de la pila.
- 8 bits - Campo TTL (time to live)

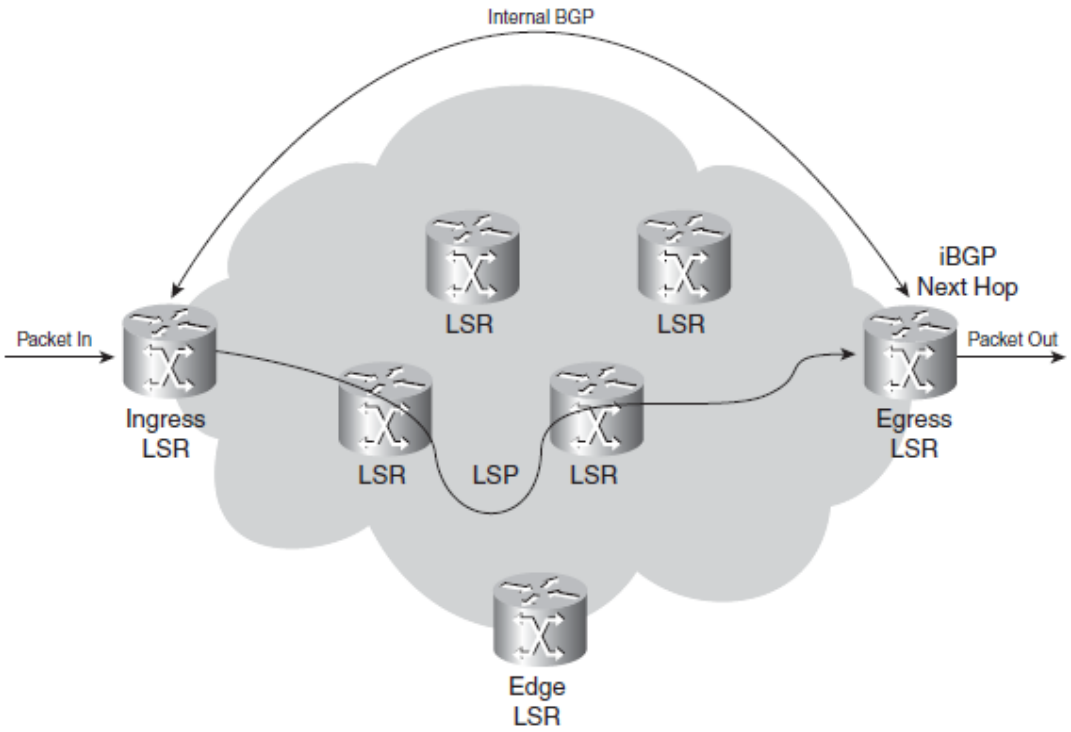

Figura 7. Ejemplo del funcionamiento de red con protocolo MPLS

Fuente. (Cisco, 2016)

Posibles usos

Los sectores donde más se utiliza este protocolo y donde se sacar más provecho a MPLS, son los Service Provider (carriers), las grandes empresas e instituciones gubernamentales (o sea, las grandes redes). Las empresas medianas contratan lo servicios de transporte de datos VPN, basado en MPLS , aunque la parte divertida la realiza el proveedor.

Los usos más importantes son:

MPLS-VPN

Con MPLS pueden realizarse enlaces VPNs point-to-point, multi-point más escalables y con costos mas accesibles para los usuarios como IPSec, ATM o frame relay; y además agrega QoS.

Ingeniería de tráfico / QoS / Congestión

El enrutamiento IP tradicional no es eficiente cuando se debe mejorar la conmutación de los paquetes y optimizando los flujos de tráficos en las aplicaciones de voz, datos y video agregando QoS en toda la ruta donde viaja

el paquete para llegar a su destino.

Respecto al problema de gestionar los flujos de tráficos MPLS puede ser utilizado para:

- Incrementar el uso de los enlaces y los nodos concentradores de datos.
- Garantizar los SLA ofrecidos a los clientes mejorando el delay.
- Minimizar el impacto de fallas en los principales protocolos utilizados para para realizar ingeniería de tráfico con MPLS son CR-LDP y RSVP-TE.

Algunas consideraciones

- Cuando se diseño la conmutación basada en etiquetas (LABEL), se esperaba que fuera mucho más rápida que la basada en los encabezados IP, por la menor cantidad de procesamiento y es posible implementarla en equipos físicos (hadware); pero el desarrollo de algunas tecnologías como los circuitos ASIC, o la conmutación basada en TCAM y CAM, han hecho posible que la conmutación basada en IP pueda ser tan rápida como la basada en etiquetas.
- Las VPN basadas en MPLS solo pueden quedar confinadas a un único proveedor de servicio. Una alternativa a MPLS es L2TPv3, aunque todavía está en borradores.

1.4 Formulación del problema

¿Qué protocolo de transporte será el más adecuado para ofrecer servicios de alta disponibilidad en un ISP?

1.4.1 Problema principal

Los Proveedores de servicio de Internet (ISP) se encuentran en el sector de las telecomunicaciones rubro que crece constantemente y las oportunidades comerciales se incrementan por lo que se debe considerar las características de la red metro ethernet:

Ventajas: Gran capacidad para el transporte de datos desde 1Mbps hasta 100Gbps, fácil operación y administración de cada circuito virtual (VLAN), al ser un estándar IEEE 802.3 muy conocido en el mundo la implementación no es compleja.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Desventajas: La red metro ethernet tiene limitaciones en la escalabilidad no fue diseñada para soportar el tráfico de miles de usuarios, no puede ofrecer calidad de servicio para aplicaciones de voz, datos y video, los equipos no pueden procesar la cantidad de paquetes debido a la conmutación que utiliza procesador y memoria esto genera problemas en la red.

Los backbones IP estaban construidos por enrutadores conectados entre sí, esto provoca saturación y congestionamiento en las redes de transmisión, al mejorar el rendimiento de los enrutadores con las capacidades de control IP y la creación de la conmutación IP como solución al rendimiento de las redes se mejoró este rendimiento, pero aparecieron nuevos problemas de congestionamiento y operatividad entre las distintas tecnologías de capa 2 o capa 3. Luego se crearon protocolos que permiten diseñar la ruta más corta de un paquete de datos debe seguir tomando en cuenta los parámetros de retardo, calidad de servicio, congestión de datos que ocasiona dificultad al momento de enviar el paquete al destino final.

Actualmente la empresa tiene estos problemas debido al crecimiento, es por ello necesario el estudio de nuevo protocolo que brinde solución a los problemas actuales.

1.5 Justificación e importancia de estudio

En los últimos años se ha presentado la aplicación de protocolos de transporte ha emergido, teniendo una gran acogida por los clientes y los ISP, las MPLS/VPN de Capa 2, estas redes tienen la naturaleza de ser multiprotocolos, es decir, pueden transportar tanto tráfico IP como tráfico no IP, gran parte de las especificaciones del IETF sobre como transportar el tráfico de Capa 2 (Ethernet, Frame Relay, ATM, HDLC, PPP) como las redes con protocolo de transporte MPLS, están ya descritas. Esto da la oportunidad a los ISP de con la misma infraestructura de red implementar un protocolo de transporte. (Rafael, Valdivia, Ms, Spíritus, y Spíritus, 2005)

El proyecto contribuye al uso de protocolos actualizados e innovadores en la implementación de una red BACKBONE para un ISP (Internet Service Provider), se debe considerar lo siguiente:

a) El protocolo de transporte debe proveer un fácil sistema de gestión y monitoreo de los nodos del acceso en el ISP que son el caso de estudio

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

de este tema para que los usuarios finales reciban un buen servicio.

b) Los problemas que enfrenta la empresa deben ser atendidos para continuar con el crecimiento, por lo que es pertinente investigar nuevas alternativas que permitan encontrar las soluciones

c) El contar con una alternativa permitirá superar los problemas actuales y supondrá enfrentar a la competencia del mercado y fortaleciendo nuestra oferta actual.

Esta investigación no comprende la implementación completa de la alternativa a elegir, solo una prueba controlada en un ambiente simulado.

1.6 Hipótesis

Si desarrollamos el análisis de los protocolos MPLS y SPB podemos recomendar la implementación de estas en una red backbone de un proveedor de servicios de internet (ISP).

1.7 Objetivos

1.7.1 Objetivo General:

Analizar los protocolos MPLS y SPB en la implementación de una red backbone de un proveedor de servicios de internet (ISP).

1.7.2 Objetivos Específicos

a) Analizar los protocolos de transporte alternativos para la red backbone de un proveedor de servicios.

b) Determinar el escenario donde se aplicarán las pruebas del protocolo.

c) Implementar los protocolos MPLS y SPB.

d) Realizar un análisis del rendimiento para los protocolos MPLS y SPB.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

II. MATERIAL Y MÉTODO

2.1 Tipo y Diseño de Investigación

2.1.1 Tipo de investigación:

Para el desarrollo de este proyecto se utilizará el tipo aplicado, por la base del conocimiento en la investigación se utilizará para alcanzar los objetivos propuestos para resolver los requerimientos del proveedor de servicios.

2.1.2 Diseño de la investigación:

Al proponer el desarrollo de la investigación, se está proponiendo emplear el Diseño de Campo por ser un diseño que mejor se adecua para una tesis de ingeniería. Esto me lleva a elegir el Diseño Estadístico y al Diseño Cuantitativo como los subtipos más convenientes. Al elegir el diseño estadístico este efectúa mediciones para determinar los valores de una variable. Es estudio considera el estudio cuantitativo o evaluación numérica de los hechos colectivos.

Se utilizarán datos reales utilizados por los proveedores de servicio y fabricantes de tecnología, para alcanzar los objetivos planteados, el diseño de investigación denominado diseño de Campo, podemos obtener los datos directamente de la realidad, tal como lo menciona FEDUPEL (2005): “los datos de recolección son recogidos en forma directa de la realidad; en este sentido se trata de investigaciones a partir de datos originales o primarios”.

2.2 Población y muestra

2.2.1 Población

La población estará conformada por los protocolos existentes en el mercado mundial y son 4 MPLS, SPB, PBB y PBB-TE quienes se configurarán en las redes de los ISP.

Tabla 1

Población Protocolos para el ISP

Nro.	Protocolos
1	MPLS (RFC 4364)
2	SPB IEEE 802.1aq
3	PBB IEEE 802.1ah
4	PBB-TE IEEE 802.1Qay

Fuente. Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.2.2 Muestra

Para el presente trabajo se ha considerado como muestra los protocolos alternativos a MPLS que son estándares en la región latinoamericana.

Tabla 2

Muestra de protocolos con los que se trabajara

Nro.	Protocolos
1	MPLS (RFC 4364)
2	SPB IEEE 802.1aq

Fuente: Elaboración propia

2.3 Variables, Operacionalización

Tabla 3

Operación de Variable

Variable Independiente	Dimensiones	Indicadores	Técnicas e instrumentos de recolección de datos
Análisis comparativo de protocolos	Protocolos analizados	Número de protocolos analizados	Análisis documental Benchmarking Juicio de expertos
	Protocolo seleccionado	Nivel de calificación del protocolo seleccionado	
Implementación de una red backbone de un ISP	Performance del nuevo protocolo	Latencia en las pruebas Tiempo de implementación	Desarrollo de escenarios de pruebas.
	Ventajas del nuevo protocolo	Costo de la implementación Número de problemas solucionados por el nuevo protocolo	

Fuente. Elaboración Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.3.1 Juicio de experto para la valorización de trabajo

FICHA DE OPINIÓN Y VALIDACIÓN DEL INSTRUMENTO FINAL

Teniendo en cuenta los aspectos que se indican, cuál es la valoración que le da al instrumento. Señale el porcentaje que le asigna, en el casillero respectivo.

I. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor del Instrumento
Canchanya Alvaro	Optical Networks	Necesidad de un protocolo de transporte eficiente para la red de ISP.	Rudy Carlos
Título: ANALISIS COMPARATIVO PARA LA SELECCIÓN DEL PROTOCOLO MPLS Y SPB PARA IMPLEMENTAR UNA RED BACKBONE DE UN ISP			

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21-40%	Buena 41- 60 %	Muy buena 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado					90
2. OBJETIVIDAD	Está expresado en conductas observables					80
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología					99
4. ORGANIZACIÓN	Existe una organización lógica.					90
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					90
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias					89
7. CONSISTENCIA	Basado en aspectos teórico-científicos					88
8. COHERENCIA	Entre los índices, indicadores y las dimensiones					89

III. OPINIÓN DE APLICACIÓN
La correcta selección de un protocolo de transporte permitirá brindan un mejor servicio a los usuarios.

IV. PROMEDIO DE VALIDACIÓN 89.3

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

FICHA DE OPINIÓN Y VALIDACIÓN DEL INSTRUMENTO FINAL

Teniendo en cuenta los aspectos que se indican, cuál es la valoración que le da al instrumento. Señale el porcentaje que le asigna, en el casillero respectivo.

IV. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor del Instrumento
Perez Moisés	CCIE Colaboración, Telefónica del Perú	Necesidad de un protocolo de transporte eficiente para la red de ISP.	Rudy Carlos

Título: ANALISIS COMPARATIVO PARA LA SELECCIÓN DEL PROTOCOLO MPLS Y SPB PARA IMPLEMENTAR UNA RED BACKBONE DE UN ISP

V. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21-40%	Buena 41- 60 %	Muy buena 61-80%	Excelente 81-100%
1. CLARIDAD	Está formulado con lenguaje apropiado					95
2. OBJETIVIDAD	Está expresado en conductas observables					83
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología					94
4. ORGANIZACIÓN	Existe una organización lógica.					93
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					95
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias					90
7. CONSISTENCIA	Basado en aspectos teórico-científicos					90
8. COHERENCIA	Entre los índices, indicadores y las dimensiones					91

VI. OPINIÓN DE APLICACIÓN

Debido al desarrollo de aplicaciones que se alojan en la nube el transporte de los datos debe ser más eficiente.

IV. PROMEDIO DE VALIDACIÓN 91.3

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

FICHA DE OPINIÓN Y VALIDACIÓN DEL INSTRUMENTO FINAL

Teniendo en cuenta los aspectos que se indican, cuál es la valoración que le da al instrumento. Señale el porcentaje que le asigna, en el casillero respectivo.

VII. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor del Instrumento
Marín Edwin	CCIE R&S Optical Networks	Necesidad de un protocolo de transporte eficiente para la red de ISP.	Rudy Carlos
Título: ANALISIS COMPARATIVO PARA LA SELECCIÓN DEL PROTOCOLO MPLS Y SPB PARA IMPLEMENTAR UNA RED BACKBONE DE UN ISP			

VIII. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21- 40%	Buena 41- 60 %	Muy buena 61-80%	Excelente 81- 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					91
2. OBJETIVIDAD	Está expresado en conductas observables					90
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología					92
4. ORGANIZACIÓN	Existe una organización lógica.					96
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					92
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias					89
7. CONSISTENCIA	Basado en aspectos teórico-científicos					92
8. COHERENCIA	Entre los índices, indicadores y las dimensiones					93

IX. OPINIÓN DE APLICACIÓN

Las redes de transporte requieren cada vez mejores instrumentos tecnológicos que permitan eficientemente una mejor gestión de los datos transportados.

IV. PROMEDIO DE VALIDACIÓN 91.87

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Tabla 4

Técnica para la recolección de datos

Método	Descripción
Entrevista	La entrevista directa a los usuarios que operan la red de transporte nos puede ayudar a confirmar personas involucradas en los procesos críticos de la empresa, se realizará entrevista focalizada a los que participan en los procesos críticos
Análisis documental	se analizará la información de fuentes secundarias publicadas como papers, tesis, boletines, páginas web que se usarán como fuentes para recolectar información.
Benchmarking	es la técnica usada para la comparación y ponderar las características y obtener un ranking
Juicio de expertos	usada para obtener respuesta de personas especialistas en los temas de la tesis, que permita contrastar los resultados
Simulación	Desarrollo de escenarios de pruebas que se usará para comprobar los resultados de la implementación

Fuente. elaboración propia

Para este proyecto de investigación que se basa en el análisis del uso de protocolos en la red de transporte el instrumento de recolección de datos fue el benchmarking, donde realiza el análisis de cada uno de los protocolos.

2.5 Procedimiento para el análisis de datos

Los datos al ser recolectados por la muestra se analizarán con los benchmarking esta información muestra el rendimiento y las funcionalidades suministradas por la muestra que se tomarán en cuenta.

Los resultados obtenidos del benchmarking se codificarán, se prepararon los cuadros estadísticos correspondientes, lo que permitirá obtener los valores absolutos y relativos. Se utilizo gráficas de barras, donde se obtendrá el resultado global de la tabulación de los datos, expresando en porcentajes en el cual se apoyó para dar los resultados finales.

Se utilizó el software de análisis estadístico SPSS para efectuar los cálculos y se utilizaron las siguientes funciones:

A. **Función Promedio. –** Utiliza la sumatoria de los valores divido entre la cantidad de elementos, se calcula de la siguiente manera.

$$P = \frac{\sum x}{n}$$

B. **Función Porcentaje-** El **porcentaje** es un valor que representa la cantidad representada en una cantidad dada de fracciones en 100 partes. Comúnmente se le conoce como **tanto por ciento**, donde *por ciento* significa «de cada cien unidades». Se utiliza para definir relaciones entre dos cantidades, de manera que la representación del *tanto* por ciento de una cantidad, donde *tanto* es un número, se refiere a la parte proporcional a ese número de unidades de cada cien de esa cantidad, se calcula utilizando regla de tres simple:

$$\left.\begin{array}{ccc} 100\% & \longrightarrow & 150 \\ 25\% & \longrightarrow & x \end{array}\right\} \rightarrow \quad x = \frac{150 \cdot 25\%}{100\%} = 37,5$$

2.6 Criterios éticos

En el desarrollo de la investigación, fue necesaria la aplicación de tres principios éticos citados por Belmont Report (Informe Belmont), el cuál es la base para las normas de conducta ética en la investigación.

A. Principio de Beneficencia

"Por sobre todas las cosas, no dañar", tomando en consideración este principio aplicado dentro de la investigación se evitó perjudicar en social, económica y psicológicamente a los estudiantes.

B. Principio de respeto a la Dignidad Humana

Este principio incluye el derecho a la autodeterminación y al conocimiento irrestricto de la información. En la investigación, el estudiante fue informado de los objetivos de la investigación donde ellos podían participar voluntariamente, con el conocimiento y comprensión para tomar una decisión adecuada.

C. Principio de Justicia

Este principio incluye el trato justo de los beneficiarios y el derecho a la privacidad. Precisamente por este principio, existe una elección justa y equitativa de los estudiantes, y reciben un trato justo y equitativo antes, durante y después de participar en el evento. Para los estudiantes que se niegan a participar, existe un tratamiento que no los afecta.

2.7 Criterios de Rigor Científico

Los criterios de rigor científico a considerar en este estudio son los siguientes:

A. Validez: El funcionamiento adecuado de la pregunta de investigación para que las variables de la investigación sean relevantes y cubran todas las dimensiones que incluyen la pregunta de investigación.

B. Generalizabilidad: También llamada validez externa, la muestra representa a la población. Por esta razón, las desviaciones deben evitarse mediante marcos de muestreo apropiados y muestreo aleatorio.

C. Fiabilidad: La medición debe tener suficiente precisión. Está relacionado con minimizar los errores aleatorios y requiere un tamaño de muestra suficiente.

Replicabilidad: Es posible repetir la encuesta y los resultados no son inconsistentes.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

III. RESULTADOS

3.1 Resultados en el uso del protocolo SPBs

3.1.1 Resultados en la implementación de servicios

La hipótesis principal planteada fue “Si desarrollamos el análisis de los protocolos MPLS y SPB podemos recomendar la implementación de estas en una red backbone de un proveedor de servicios de internet (ISP)”.

3.1.2 Proceso para la selección del protocolo de transporte

Con respecto al proceso para la selección del protocolo es una tarea que se realizará considerando las características de cada uno de ellos y pruebas de laboratorio.

Frente a la creciente necesidad de acceder a los servicios de Internet existen diferentes tecnologías para el acceso al medio como xDSL, FTTH, Metro Ethernet, Satelital todas ellas brindan acceso a los clientes al Internet por lo que es importante el protocolo de transporte para que todas las tecnologías puedan converger en la red de transporte del ISP por que la actividad de este trabajo requiere dedicar un 70% en el proceso de selección del protocolo y pruebas de homologación.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

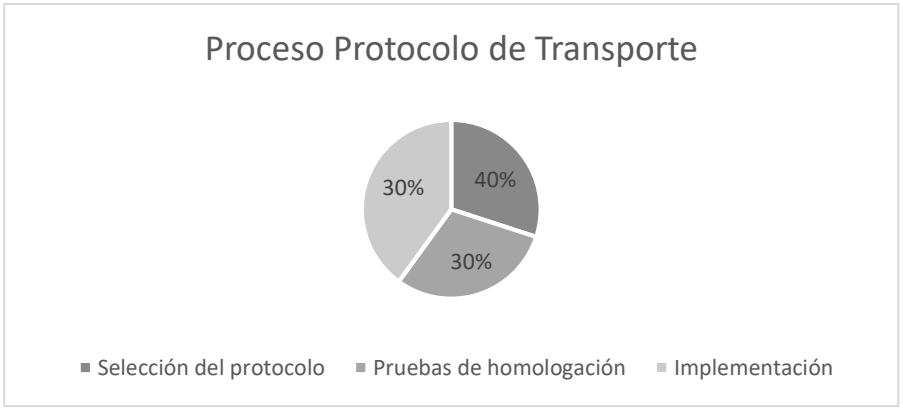

Figura 8. Proceso de Protocolo de Transporte

Fuente. Elaboración propia

3.1.3 Numero de protocolos analizados

Con respecto al número de protocolos analizados, los proveedores necesitan transportar tráfico Ethernet mediante una MAN/WAN para ello el protocolo debe tener la capacidad de identificar el tráfico de datos de los clientes, los protocolos analizados deben identificar el tráfico de cada cliente mediante etiquetado los protocolos considerados son: IEEE 802.1aq Shortest Path Bridging (SPB), IEEE 802.1ah Provider Backbone Bridges, IEEE 802.1Qay Provider Backbone Bridge Traffic Engineering y MPLS Multi Protocol Label Switching.

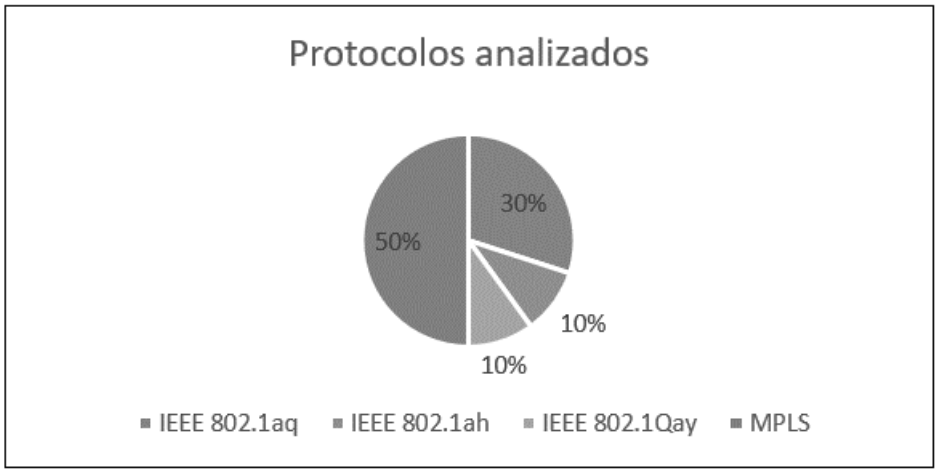

Figura 9. Número de protocolos analizados

Fuente. Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.1.4 Nivel de calificación del protocolo seleccionado

Para la calificación de cada uno de los protocolos se ha considerado las características técnicas de cada uno de los protocolos descritas en los estándares de la IEEE y la información encontrada por los fabricantes de las marcas AVAYA, BROCADE y CISCO.

Tabla 5

Nivel de calificación del protocolo seleccionado

Características técnicas	MPLS (RFC 3031)	SPB - IEEE 802.1aq	PBB - IEEE 802.1ah	PBB-TE - IEEE 802.1Qay
Aplicación	5	5	1	1
Crecimiento de VRF	5	5	2	1
Escalabilidad de IP Roete	5	5	4	4
Creación de Core	4	3	2	1
Plano de Control	3	5	3	3
Extensiones del Plano de control para Multicast	3	5	3	3
Plano de Control para extensiones Ipv6	5	5	3	3
Plano de Control para extensiones L2 VPNs.	4	4	2	2
Complejidad operacional	2	5	3	3
Virtualización sobre la WAN	5	5	4	4
Resultado	**41**	**47**	**27**	**25**

Fuente. elaboración propia

Esta calificación se realiza en base a los servicios que puede ofrecer el protocolo SPB el estándar fue su aceptado en 2012, se ha desarrollado bajo la función de redes definidas por Software (SDN) eso lo hace mucho más eficiente en la gestión e implementación de los servicios en la red del ISP, tomando en consideración la evolución de las aplicaciones.

MPLS definido en la RFC 3031 ha brindado un buen soporte al transporte de datos, sin embargo, la rápida evolución de las aplicaciones y servicios en la nube requiere una red más eficiente de gestionar.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.1.5 Servicios obtenidos con el protocolo seleccionado

El protocolo SPB seleccionado nos provee 5 servicios básicos necesarios para el transporte de los datos de los clientes del ISP, en el cuadro se ha representado los principales requisitos de los usuarios para el transporte en capa L2 y L3.

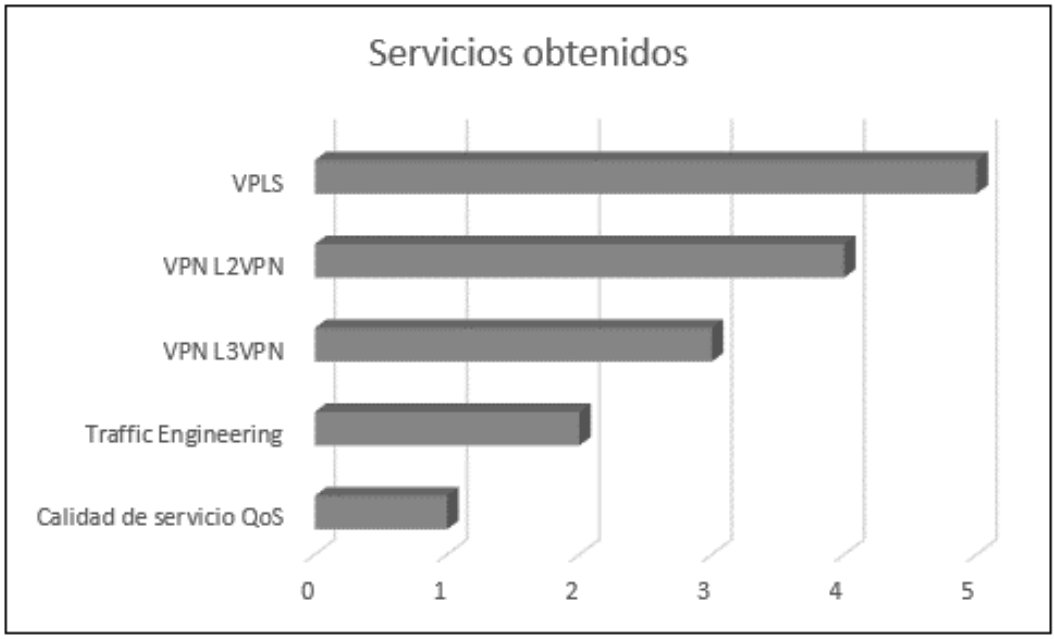

Figura 10. Servicios obtenidos para el proveedor de transporte

Fuente. Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.1.6 ANALISIS DEL PROTOCOLO DE TRANSPORTE SPB

En esta tabla permitirá evaluar y decidir qué protocolo cumple con los requerimientos de la red de transporte.

Tabla 6

Tabla de comparaciones de características MPLS con SPB

Características	MPLS (RFC 3031)	SPB (Fabric)
Aplicación	Proveedores de servicio de Internet Empresas grandes	Empresas grandes y medianas Proveedores de servicios medianos
Crecimiento de VRF	Soporta muchos dispositivos PE (típicamente 512-4000 en plataformas de los carrier)	Soporta muchos dispositivos PE (típicamente 24 - 512 en plataformas enterprise), esto va creciendo hasta 5000
Escalabilidad de IP Route	Ningún límite real impuesto por BGP. En la práctica, limitado por el número máximo de rutas IP soportadas en PE	Máximo de 200000 rutas IPv4 por BEB (limitado al tamaño máximo de IS-IS LSP), con ello soporta todo el trafico de internet debido a las rutas sumarizadas.
Creación de Core	Enrutamiento salto por salto + MPLS etiquetado switching.	Rutas más cortas con conmutación Ethernet para mejorar la conmuntación.
Plano de Control	IGP (OSPF o IS-IS) y LDP en P y nodos PE Full Mesh de MP-iBGP peering en los nodos PE. Los requisitos de BGP Route Reflector escalable.	1 instancia de IS-IS y puede transportar a otros protocolo como BGP, OSPF
Extenciones del Plano de control para Multicast	PIM-SM en el núcleo IGP, así como en el VPN VRFs donde IP Multicast requieren.	No, (Aprovecha IS-IS Shortest path trees) para el manejo del trafico Multicast
Plano de Control para extensiones Ipv6	BGP+ requiere soporte (RFC 2545)	No, (el mismo para IPv4; simplemente usa diferentes IS-IS TLVs)
Plano de Control para extensiones L2 VPNs.	Posiblemente pero requiere capacidad adicional para VPLS	Nativo (L2 VSNs)
Complejidad operacional	Alta complejidad	Simple (Para diseñar, aprovisionar y mantener)
Virtualización sobre la WAN	Si, Usando MPLS sobre GRE	Si, usando SPB sobre IP (Fabric Extend)

Fuente. Elaboración propia

Los resultados no permiten conocer que SPB es tiene características similares, pero en la aplicación a ISP no se adecua y nos permite confirmar a MPLS como el protocolo de transporte.

IV. CONCLUSIONES Y RECOMENDACIONES

¿Qué pasa con la WAN tradicional?

1) **La WAN (MPLS) no está orientada al negocio:** Se requiere una red flexible y lo suficiente ágil para poder responder con rapidez a los requerimientos del negocio.
2) Problemas para los entornos CLOUD: El tráfico de aplicaciones cloud debe estar lo más cerca al usuario posible, para mejorar su experiencia de uso, y no debe sobrecargar las redes corporativas si no es necesario.
3) Esquemas de redundancia ineficientes: El protocolo MPLS no puede manejar de manera eficientes los enlaces activo-activo.

4.1 Conclusiones

1. Se analizaron los protocolos MPLS y SPB en la implementación de una red backbone de un proveedor de servicios de internet (ISP) propósito que se ha cumplido, se utilizó un ambiente pruebas en la red de transporte utilizando router de core, distribución, acceso, medios de transmisión cobre para puertos UTP RJ-45 y fibra óptica monomodo para la interconexión con los nodos de acceso.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

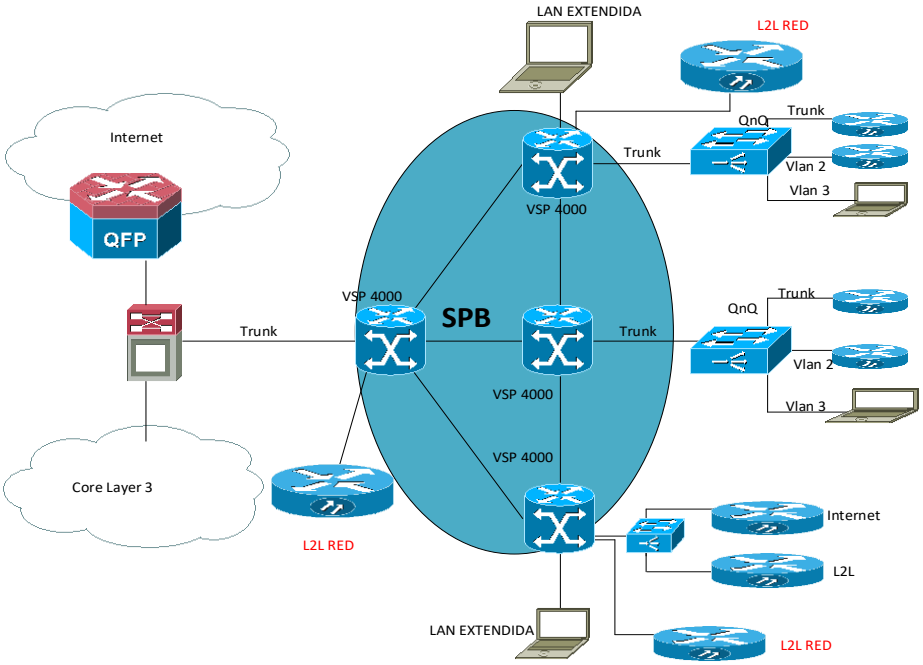

Figura 11. Short Path Bridding L2 VSN

Fuente. (Avaya Inc., 2015)

2. Se analizó el protocolo alternativo considerando la habilitación de los servicios comunes que implementaran en los ISP de acuerdo con el marco teórico que define cada funcionalidad del protocolo MPLS y SPB, aunque existen otros protocolos alternativos no existe el desarrollo y aplicación en redes de transporte y el presente trabajo ha cumplido con la comparación planteada, lo servicios validados fueron:

   A) **Servicio de LAN Extendida**, Lan Extendida es un servicio que permite la interconexión de dos sedes remotas permitiendo manejar el mismo segmento de red.

   En las pruebas realizadas en la sección 5.2.1 (a) del presente documento se realizó las configuraciones y pruebas dado el siguiente resultado:

   PC1: Conectada al equipo de borde VPS02

   Comando: Ping 192.168.20.10

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Destino PC2 conectada al equipo de borde VSP04

Resultado: Conectividad envío de 4 paquetes

Latencia: menor a 1ms

Perdida de paquetes: 0

TTL: 128

B) **Servicio L2L**, este servicio permite la interconexión de locales remotos hacia la sede central cada local se representa con un segmento de red distinto.

En las pruebas realizadas en la sección 5.2.1 (b) del presente documento se realizó las configuraciones y pruebas dado el siguiente resultado:

Router 1: Conectado al equipo de borde VSP01

Router 2: Conectado al equipo de borde VSP02

Router 3: Conectado al equipo de borde VPS04

Comando: R3#ping 192.168.1.1 source 192.168.2.1 repeat 100

Destino Router 2 conectado al equipo de borde VSP02

Resultado: Conectividad envío de 100 paquetes

Latencia: menor a 2ms

Perdida de paquetes: 0

TTL: 128

C) **Fibra Oscura QinQ:** Este servicio permite el transporte de datos de capa 2 sobre un enlace de capa 3 configurando virtualmente un enlace de capa 2 para que el cliente pueda transportar servicios de capa 2.

En las pruebas realizadas en la sección 5.2.1 (c) del presente documento se realizó las configuraciones y pruebas dado el siguiente resultado:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

SW2 : Conectado al equipo de borde VSP02.

SW3: Conectado al equipo de borde VSP03.

Router trunk-02 conectado al SW2.

Router vlan-2 conectado al SW3.

Ambos equipos se encuentran se separados y conectados sobre una red de capa 3, donde se configura QinQ.

Comando:Router_TRUNK_vsp_02#ping 192.168.1.2 source 192.168.1.1 repeat 10

Destino Router_VLAN_VSP02 conectado al SW3

Resultado: Conectividad envío de 10 paquetes

Latencia: menor a 2ms

Perdida de paquetes: 0

TTL: 128

D) Servicio L2L e Internet: Las configuraciones más comunes para acceder a los servicios de Internet recurso muy necesarios en las empresas y usuarios.

En las pruebas realizadas en la sección 5.2.1 (d) del presente documento se realizó las configuraciones y pruebas dado el siguiente resultado:

Router Internet cliente: Conectado al equipo de borde VSP04.

Router L2L RED: Conectado al equipo de borde VSP04.

Router Internet público conectado al Gateway router.

Estos equipos simulan los locales de cliente con un servicio de transporte de datos y salida centralizada de Internet..

Comando:Router_internet#ping 8.8.8.8 source 190.12.64.1 repeat 1000

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Resultado: Conectividad envío de 1000 paquetes

Latencia: menor a 2ms

Perdida de paquetes: 0

TTL: 128

3. El escenario donde se aplicaron las pruebas fue en entornos donde se puede simular las funcionalidades del protocolo y los servicios requeridos por los ISP, par aun caso práctico se ha planteado utilizar actualmente empresas que tienen un número menor de 1,000 clientes esto requiere un plan de trabajo a largo plazo, para cumplir con el objetivo planteado la simulación es el método que mejor se adapta al trabajo de investigación.
4. El análisis de rendimiento está basado en la cantidad de empresas que debe soportar el protocolo, pero en redes muy escalables se requiere un alto conocimiento para poder gestionar apropiadamente la red de transporte, por lo que se recomienda MPLS quien en los varios años de uso ya tiene un buen conocimiento.

4.2 Recomendaciones

La implementación de los servicios ofrecidos por los protocolos nos ha permitido tener los alcances de cada uno de ellos, en el caso del protocolo SPB se aplica para redes de envergadura mediana donde puede trabajar sin problemas y es una buena alternativa para los ISP que inician sus operaciones y deben proveer de buenos servicios a sus clientes; pero en empresas enterprise donde el número de clientes crece constantemente esto protocolo SPB no ofrece la confiablidad debido a las limitaciones del VLAN.

El protocolo MPLS ya ha desarrollado en los últimos 16 años mejoras en su estructura por lo que brinda mayor estabilidad en redes con una alta demanda de servicios solicitados por sus clientes, por lo que es la mejor alternativa en este momento esperando una mayor maduración de los otros protocolos.

a) Se realizó el análisis de los protocolos de transporte alternativos para la

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

red backbone de los ISP se consideró la información técnica de los estándares donde nos brindan las funcionalidades.

b) La determinación del escenario para las pruebas de obtuvo de la información de OSIPTEL a junio del 2017 donde nos mostraba la cantidad de clientes de cada operador y esto nos permitió elegir a Optical Technologies como el escenario para las pruebas.
c) Se realizaron las implementaciones de ambos protocolos en escenarios típicos para los clientes donde se vio cada proceso para habilitar los protocolos MPLS y SPB.
d) El análisis y rendimiento de cada protocolo se realizó en base la información de comparación de los fabricantes quienes ya pusieron a pusieron a prueba estos protocolos y en la implementación se confirmó las diferencias.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

V. REFERENCIAS

Avaya Inc. (2015). *Avaya SPB Fabric Solution > Network virtualization using Avaya SPB Fabric Concept and Design Avaya Networking*.

Carral Pelayo, J. A., y Henares, A. de. (2013). *Contribución al Diseño de Conmutadores Transparentes Avanzados Basados en Tecnología Ethernet*. Universidad de Alcalá.

Cisco System, S. M. L., Class, F. E., Router, L. S., Ioses, C., Encapsulation, G. R., Mpls, L. S. P., … Mpls, E. (2016). Protocolo MPLS, (Mayo), 7. Retrieved from https://www.cisco.com/c/es_mx/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc1

Ferrari, P., Flammini, A., Rinaldi, S., Prytz, G., y Hussain, R. (2014). Multipath redundancy for industrial networks using IEEE 802.1aq Shortest Path Bridging. *Multipath Redundancy for Industrial Networks Using IEEE 802.1aq Shortest Path Bridging*, p. 11. https://doi.org/10.1109/WFCS.2014.6837598

Gestido, P. A. (2014). *Virtualización de Redes en la Empresa*. Unicersidad de la República.

Mack-crane, B., y Yong, L. (2011). SPB over MPLS, 7. Retrieved from https://www.ietf.org/proceedings/82/l2vpn.html

Nguyen, K. K., y Jaumard, B. (2013). A MPLS/LDP distributed architecture for next generation routers. *Journal of Network and Systems Management*, *21*(4), 535–561. https://doi.org/10.1007/s10922-012-9250-4

Orozco Lara, F. (2014). TESIS FINAL MAGISTER EN TELECOMUNICACIONES TITULO : Diseño de una red privada virtual con tecnología MPLS para la Guayaquil Ing . Fausto Raúl Orozco Lara . Tutor :, 105.

OSIPTEL. (2017). IndInternetFijo_5. Retrieved from https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/53-conexiones-de-acceso-

a-internet-fijo-desagred/IndInternetFijo_5.3_Setiembre2017.xls

Rafael, J., Valdivia, G., Ms, C., Spíritus, S., y Spíritus, S. (2005). MPLS Y SU APLICACIÓN EN REDES PRIVADAS VIRTUALES (L2VPNs Y L3VPNs), pp. 8–10.

Rojas Sánchez, E. (2013, April). *CONTRIBUCIONES EN ARQUITECTURAS DE REDES DE CONMUTADORES TRANSPARENTES ETHERNET DE ALTAS PRESTACIONES*. *CONTRIBUCIONES EN ARQUITECTURAS DE REDES DE CONMUTADORES TRANSPARENTES ETHERNET DE ALTAS PRESTACIONES*. Universidad de Alcalá, España. Retrieved from http://dspace.uah.es/dspace/bitstream/handle/10017/20072/Tesis Elisa Rojas.pdf?

Sepulveda Baldenebro, J. A. (2009). *CENTRO DE INVESTIGACIÓN Y DESARROLLO*. INSTITUTO POLITÉCNICO NACIONAL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA DIGITAL.

Stevens, L. (Avaya N. (2015). Avaya SPB Fabric Concept and Design Avaya Networking, (February), 1–80.

Tumial, P. H., y Cruz, D. La. (2004). Internet en el Perú, *7*, 9–15.

ANEXOS

5. IMPLEMENTACION DE LOS PROTOCOLOS MPLS Y SPB

5.1 DISEÑO DE SERVICIOS SPB Y IMPLEMENTACIÓN

SPB se basa en el esquema 802.1ah encapsulación, pero no depende de árbol de expansión para proporcionar una red libre bucle de la capa 2, en su lugar utiliza el protocolo IS-IS topología. El IEEE es revisada en la que abarca la especificación 802.1D árbol para incluir la nueva solución de SPB. La intención es que una vez que la norma se aplica en los productos de red, el operador de la red será capaz de elegir un camino más corto puente protocolo de topología o la opción basada en la raíz del árbol de herencia.

Además del soporte de virtualización de capa 2 que proporciona SPBM, el modelo se está extendiendo a apoyar también la capa 3 de virtualización a través del Proyecto de IETF Draft IP/SPB-Unbehagen. Cuando L2 virtualización asocia un ISID a una VLAN borde de tal manera que se extienda que VLAN a través de la columna vertebral, con la extensión L3 un VRF también puede estar asociada a un ISID de tal manera que se extienda una instancia de enrutamiento virtualizado L3 a través del backbone.

Avaya también ha mejorado la capacidad SPBM añadiendo soporte multicast, que simplifican enormemente el despliegue de multicast y proporcionar elasticidad para multidifusión al mismo tiempo. En resumen, SPBM trae a la red empresarial las características, funcionalidades y escalabilidad exigidos por las compañías a través de la utilización de un único protocolo de enrutamiento de estado de enlace simple y dinámica que es IS-IS.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.1.1 Servicios SPB

a) **SPB L2 Virtual Services Network**

Una topología SPB L2 VSN simplemente se compone de una serie de Backbone Edge Bridges sirve para usar Layer 2 VSNs. El plano de control utiliza IS-IS para la transmisión a nivel de Capa 2. Sólo los puentes BEB son conscientes de ninguna de las direcciones de VSN y MAC asociada mientras que los backbone bridges simplemente reenviar tráfico en la red principal de MAC nivel (B-MAC). Los conmutadores de red troncal sabrán cómo llegar a cada B-MAC utilizando el camino más corto determinado por la norma IS-IS.

Tenga en cuenta que el backbone System ID o B-MAC se pueden aprovisionar manualmente para ayudar a facilitar la solución de problemas cuando se mira en la tabla de reenvío de unidifusión B-MAC. En resumen, todos los conmutadores de la red troncal solamente aprenderán B-direcciones MAC para tomar decisiones de envío mientras que la BEB aprenderá tanto los B-MAC y MAC de los clientes (C-MAC) para cada VSN.

Un Backbone Servicio Instancia Identificador (ISID) se le asignará en el BEB para cada VLAN. Todas las VLAN en la red que comparten el mismo ISID podrán participar en la misma VSN. Si se utilizan grupos SMLT, se requieren dos VLAN red principal (B-VLAN) con un B-VLAN primaria y una secundaria B-VLAN. En general dos troncal VLAN se debe utilizar siempre (incluso si no hay clúster SMLT está en uso) ya que el uso de 2 troncal VLAN permite IS-IS para calcular árboles de igual costo, donde si existen 2 caminos más cortos de igual costo, SPB carga de tráfico equilibrio VSN a través de ambos caminos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

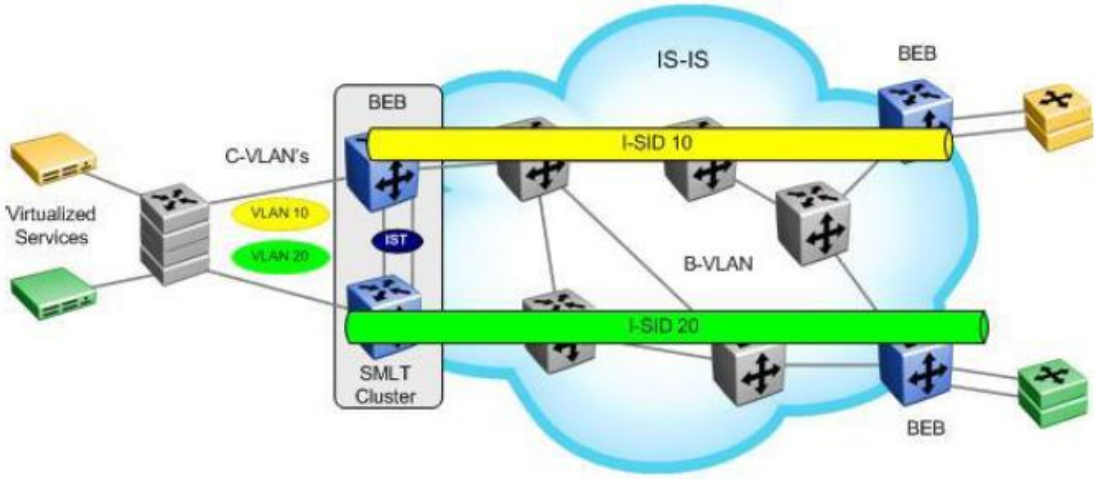

Figura 12. Short Path Bridding L2 VSN

Fuente. (Avaya Inc., 2015)

En resumen:

a) Como mínimo, un B-VLAN se debe asignar a cada conmutador SPB o Para SMLT, se requieren dos B-VLAN

b) TLV y sub-TLV se utilizan para identificar ejemplo SPB, métricas de enlace, B-VLAN, B-MAC, y el número de ISID's

b) **SPB L3 Virtual Services Network**

Una topología SPB L3 VSN es muy similar a una topología SPB L2 VSN con la excepción de que una Backbone Service Instance Identifier (ISID) se le asignará a un enrutador virtual (VRF) de nivel en lugar de a un nivel de VLAN. Todos los VRF en la red que comparten el mismo ISID podrán participar en la misma VSN.

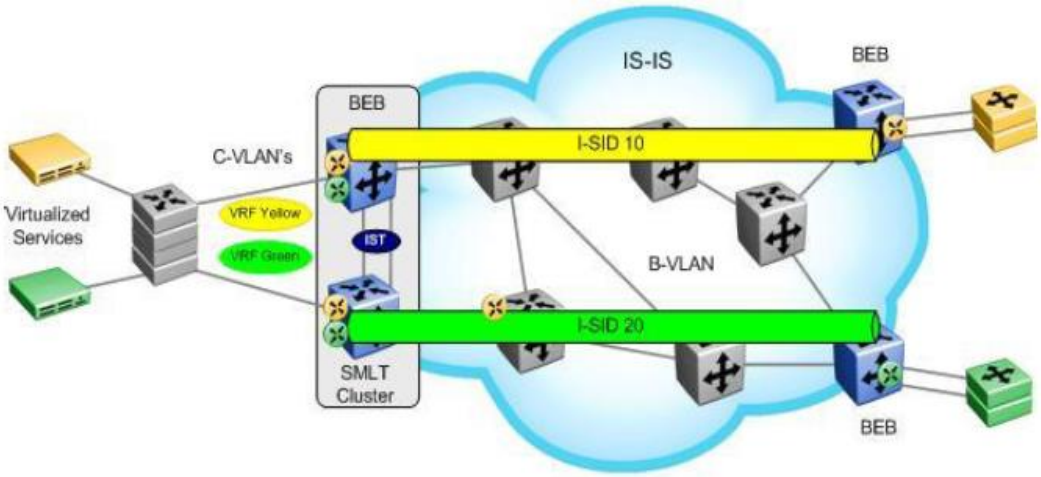

Figura 13. Short Path Bridding L3 VSN

Fuente. *(Avaya Inc., 2015)*

En resumen:

a) Uno o más VRF se crean en el BEB conmuta con un ISID asignado Todos los VRF que comparten el mismo ISID pueden participar en el mismo VSN

b) Distribución de la Ruta de las interfaces directas en casos VRF debe estar habilitado para distribuir redes VRF en IS-IS entre conmutadores BEB

c) IS-IS enrutamiento IP debe estar habilitado

c) Inter VSN Routing

Inter VSN permite el enrutamiento entre redes IP en la Layer 2 VLANs con diferentes ISIDs. Como se ilustra en la figura 14, el enrutamiento entre las VLAN 10 y 20 se produce en uno de los SPB core switches que se muestran en el centro del diagrama. Los usuarios finales de los interruptores BEB como se muestra a la derecha ya las izquierdas del diagrama son capaces de reenviar el tráfico entre las VLAN amarillo y verde (VLAN 10 y 20) a través de la instancia VRF configurado en el interruptor se muestra. Aunque el diagrama ilustra una VRF configurado en un interruptor de BCB, Inter VSN también se puede realizar a través de GRT. Además, para la redundancia, el Inter VSN también se puede configurar en otro conmutador con VRRP para eliminar un único punto de fallo.

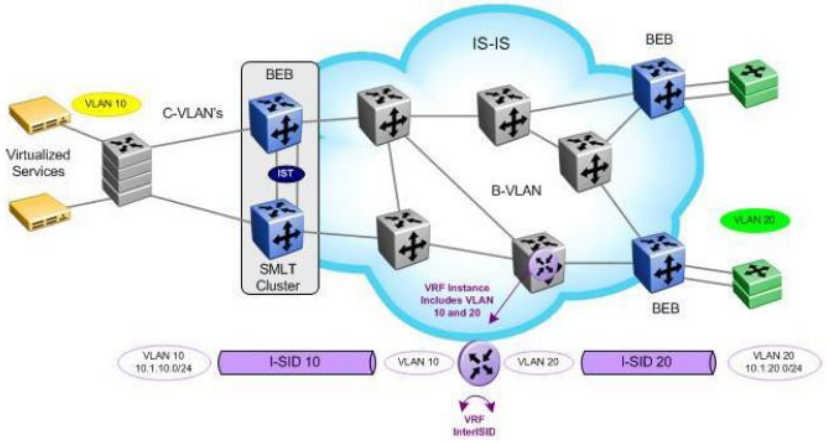

Figura 14. Inter VSN Routing

Fuente. *(Avaya Inc., 2015)*

Por favor, tenga en cuenta el Inter VSN enrutamiento sólo es normalmente usado cuando se tiene que extender una VLAN como L2VSNs para aplicaciones tales como vMotion. Normalmente, es recomendable para encaminar cuando se puede, ya sea mediante el uso de atajos de IP o L3VSNs. Como uno de los requisitos para vMotion es una red compartida de los servidores ESX, no tenemos más remedio que cerrar el tráfico entre los servidores ESX. Con el fin de reenviar el tráfico del servidor a los clientes y viceversa, es necesario ruta IP del tráfico, ya sea a través de atajos IP a través de un VRF L3VSN.

d) SPB IP Shortcuts

IP shortcuts permiten el enrutamiento entre las VLAN en el global de la tabla de enrutamiento / red motor de enrutamiento (GRT/NRE/VRF-0). No se utiliza ninguna configuración ISID. IP está habilitado en el B-VLAN IS-IS ejemplo en los interruptores BEB. Esto proporciona el reenvío de IP normal entre los sitios BEB sobre un backbone IS-IS.

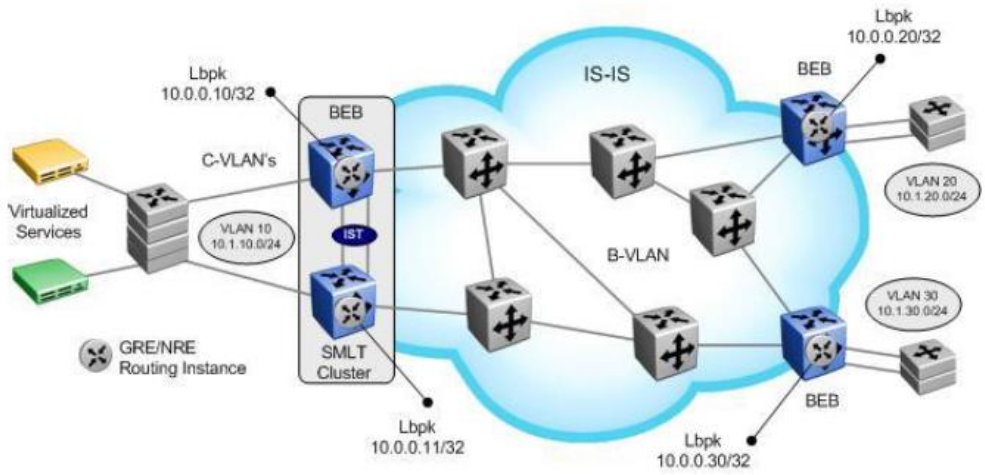

Figura 15.SPB IP Shortcuts

Fuente. *(Avaya Inc., 2015)*

En resumen:

1) IP debe estar habilitado en IS-IS, donde el IS-IS dirección de origen, que debe ser configurado, es una dirección circuitless/loopback IP address.
2) El IS-IS dirección de origen se inyecta automáticamente en IS-IS.
3) IS-IS redistribución de la directa (o OSPF, RIP, estático, BGP ...) rutas IP pueden habilitarse como un mecanismo simple para reenviar dichas redes entre vecinos BEB.
4) Esto inyectará toda directo (o OSPF, RIP, estático, BGP ...) rutas IP en IS-IS en el caso de redistribución de la ruta directa IP, una política de rutas (CLI) o route-map (ACLI) debe estar configurado para que coincida con la subred IP IST para evitar que se anuncia.
5) El Extended IP Reachability TLV 135 se utiliza para distribuir la accesibilidad IP entre peer IS-IS

e) UNI Types

L2VSN – C-VLAN UNI

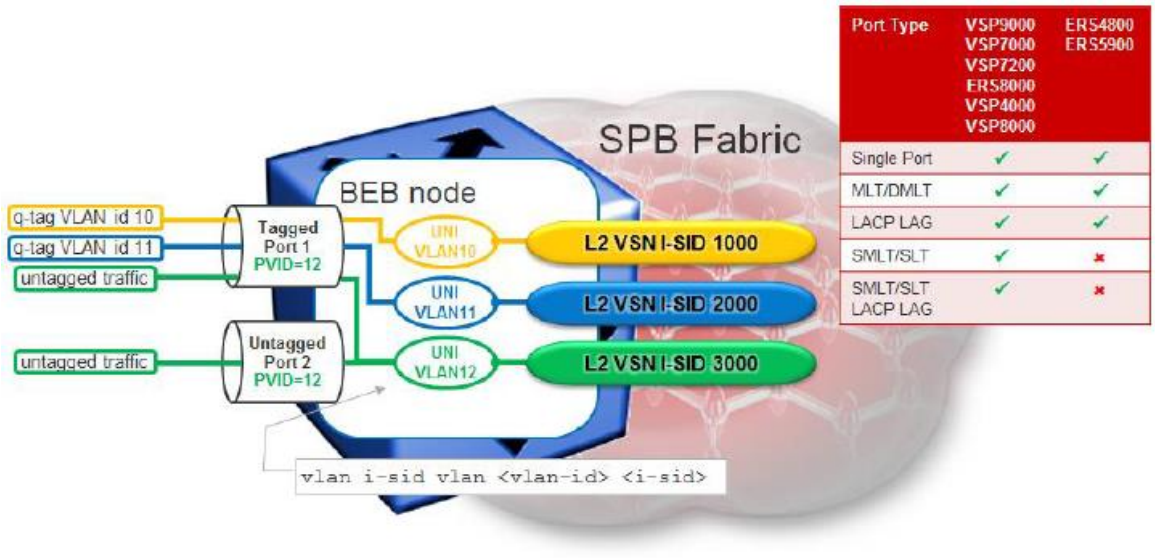

Figura 16. L2VSN – C-VLAN UNI

Fuente. *(Avaya Inc., 2015)*

UNI es una VLAN (VLAN Cliente = C-VLAN)

1) VLAN tiene un significado global en el BEB
2) VLAN realiza la conmutación L2 en los miembros de los puertos de VLAN locales y transporta más L2VSN para puntos finales remotos
3) El tráfico no etiquetado se asigna a la VLAN correspondiente a pvid configurado en el puerto o El puerto etiquetado, utilice el modo UntagPVIDOnly para forzar el tráfico a PVID también salir sin etiquetar
4) Se admite en todas las plataformas capaces SPBM
5) Switched UNIs y CVLAN UNIs puede ser asignado a la misma ISID
6) ETREE UNI y CVLAN UNI se pueden asignar a la misma ISID
7) **No se puede mezclar Transparent UNI con C-VLAN UNI**

VSN – Switched UNI

UNI es una VLAN-ID en un puerto Ethernet/MLT

1) Identificación de VLAN tiene importancia local en el puerto Ethernet/MLT.
2) Misma VLAN-ID se puede volver a utilizar en diferentes puertos y pertenecen a una diferente ISID.
3) Diferentes VLAN-ID en los puertos mismos o diferentes pueden ser asignados a los mismos ISID O puede hacer VLAN Asignación de conmutador local.
4) El tráfico no etiquetado puede ser recogido por la configuración del puerto de UntagPVIDonly y establecer el PVID en el puerto.
5) Switched UNIs and CVLAN UNIs puede ser asignado a la misma ISID.
6) Supported en el VSP 7000 versión 10.2, ERS 4800 versión 5.7, y ERS 5900 en la versión 7.0

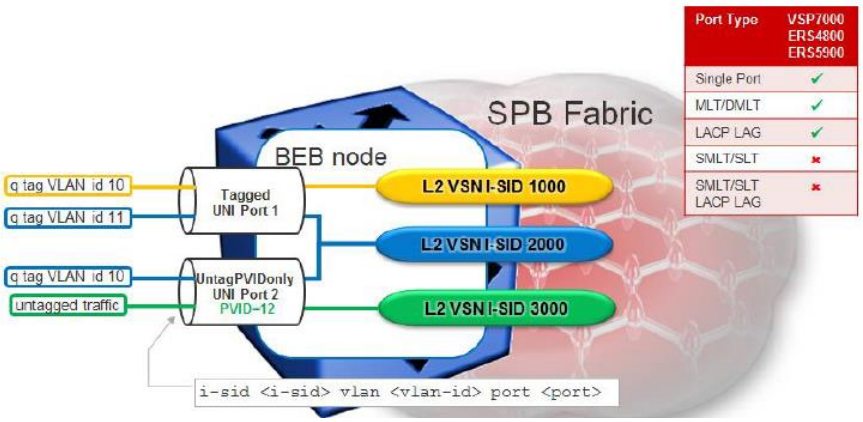

Figura 17. VSN Switched UNI

Fuente. *(Avaya Inc., 2015)*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VSN – Transparent UNI

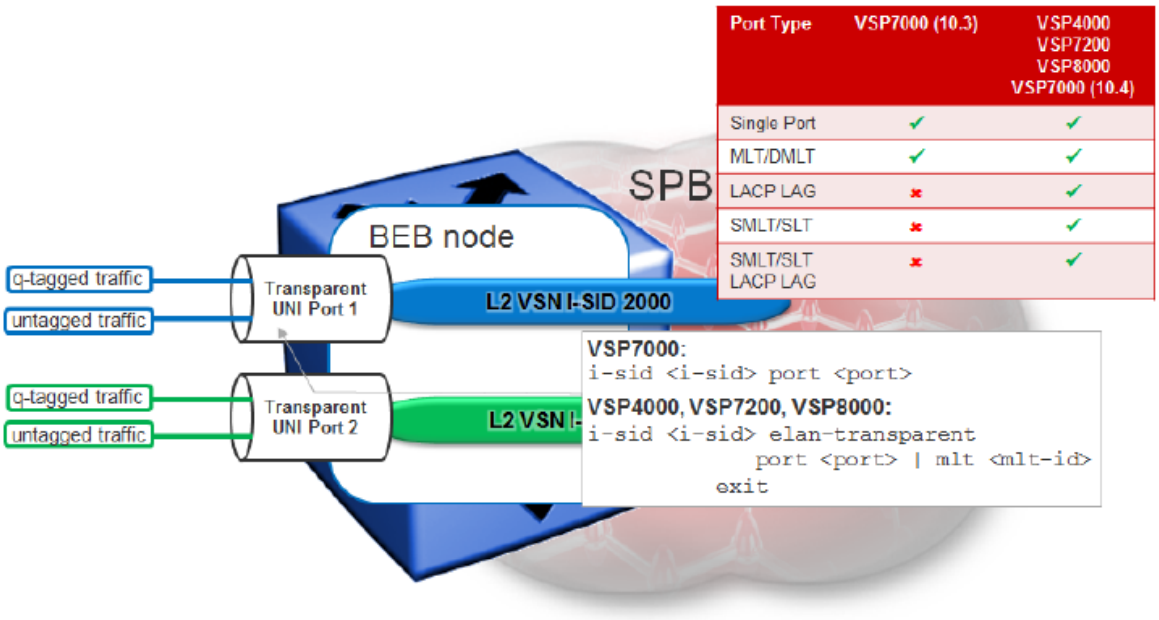

Figura 18. VSN – Transparent UNI

Fuente. *(Avaya Inc., 2015)*

UNI es un puerto Ethernet/MLT

a) Puerto Ethernet UNI/MLT no es consciente de la etiqueta de VLAN

b) Los paquetes con o sin un Q-etiqueta de VLAN se transportan en el L2VSN

c) Control de tráfico sin etiquetar (STP, VLACP, LACP, LLDP, etc.) se reenvía de forma transparente o PDU VLACP / LACP son desviadas (VSP 4000/7200/8000: menos que esté configurado en el puerto UNI / MLT)

d) aprendizaje MAC inversa todavía se utiliza, por lo que se puede utilizar con 3 o más puntos finales

e) Apoyado en el VSP 7000 Versión 10.3 con soporte para SMLT en la liberación 10.4, VSP 4000 versión 3.1, VSP 8000 en la versión 4.2, y VSP 7200 en la versión 4.2.1

f) puertos UNI transparentes MLT son compatibles (VSP en

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4000/7200/8000 incluso con LACP)

g) UNI transparente no debe asignarse a la misma ISID como Switched UNI o CVLAN

h) A partir de la versión 4.1 para el VSP 4000, UNI transparente sobre SMLT es soportado

i) UNI transparente no se puede mezclar con cualquier otro tipo de UNI

j) Usted no puede utilizar un ISID asignado a un UNI transparente, ya sea con un UNI C-VLAN o un conmutador UNI o Sólo transparente UNI puede ser asignado a la misma ISID

Flex UNI – Switched

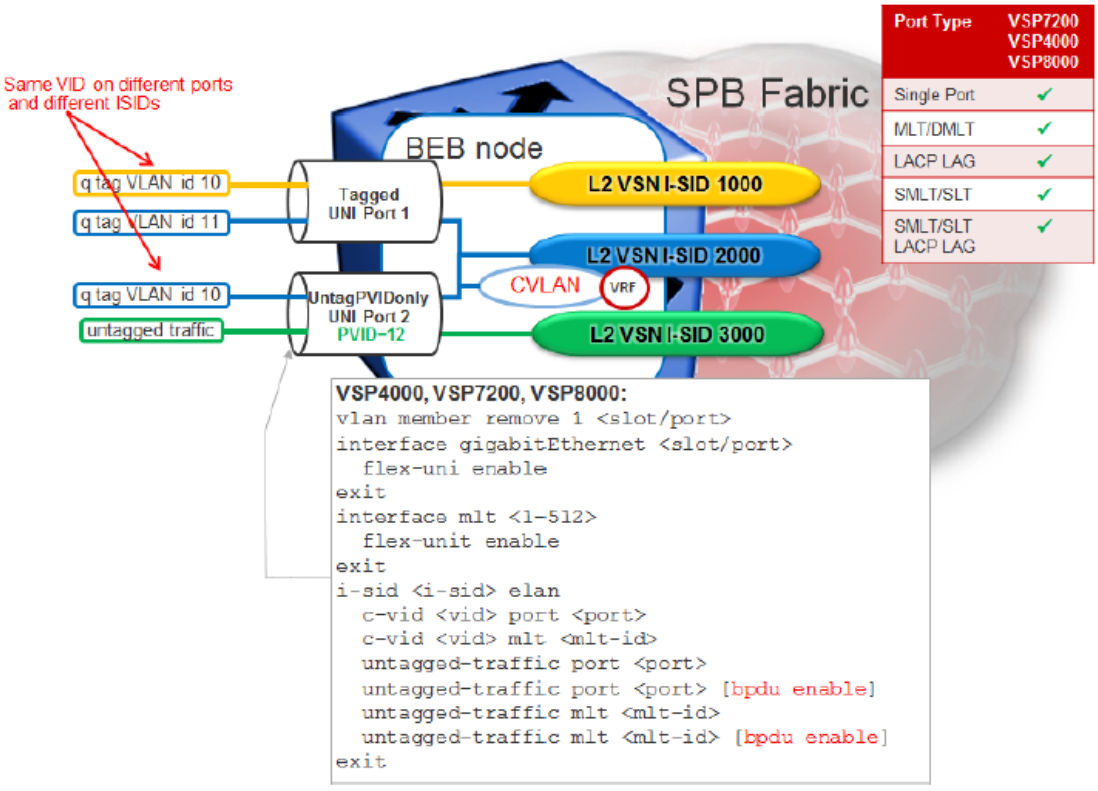

Figura 19. Flex UNIX Switched

Fuente. *(Avaya Inc., 2015)*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Un ID de VLAN (c-vid) y un puerto o MLT determinado se asigna a una L2VSN ISID

a) El c-vid no es una plataforma de VLAN, se trata simplemente de sólo un ID de VLAN en un puerto Flex UNI o MLT o Una VLAN es una plataforma de VLAN creado usando el VLAN crear <2-4059> escriba puerto-mstprstp <instancia> ACLI
b) VLAN ID única de importancia local en el puerto Ethernet o MLT
c) El mismo ID de VLAN puede volver reutilizado en puertos diferentes y pertenecen a diferentes ISID
d) Switched UNIs y una CVLAN se puede asignar a la misma ISID o Esto le permite añadir una dirección IP a la CVLAN habilitar el enrutamiento de Flex UNI
e) Para recibir tráfico sin etiquetar, la opción sin etiquetar el tráfico debe estar habilitado además Spanning Tree BPDU expulsan o inundadas en función de si las BPDU opción Habilitar está activado
f) Activación de la opción sin etiquetar-tráfico reenviar el tráfico de control tal como LACP y VLACP
g) Para habilitar la opción de BPDU, hay que habilitar la configuración sin etiquetar el tráfico de BPDU sin la opción de habilitar como se muestra en la configuración anterior.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.2 Implementación de SPB

Tarea Previa implementar las conexiones y ejecutar el script SPB a todos los equipos Avaya Fabric y verificar que todos los VSP del backbone tengan conectividad.

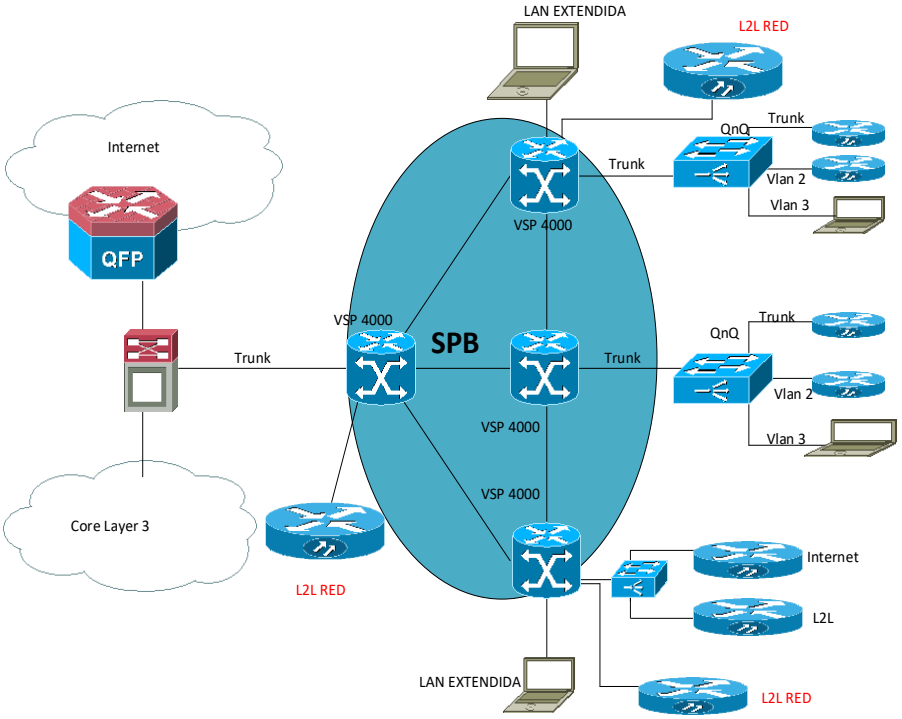

Figura 20. Topología de RED para pruebas

Fuente. Propia

ISIS SPBM CONFIGURATION

```
router isis
spbm 1
spbm 1 nick-name 7.11.11   → El Nick-name es diferente en cada VSP
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
```

VLAN CONFIGURATION

```
vlan members remove 1 1/37-1/48
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
interface GigabitEthernet 1/37-1/48
no shutdown
isis
isis spbm 1
```

```
isis enable
```

 # ISIS CONFIGURATION

```
router isis
sys-name VSP_01    → El nombre es diferente en cada VSP
ip-source-address 1.1.1.1 → El Source-address es diferente en cada VSP
is-type l1
system-id 0001.1111.0000  → El System-ID es diferente en cada VSP
manual-area 49.0000
exit
router isis enable
```

Comandos de Verificación:

VSP_01:1#SHOW ISIS

```
============================================================
ISIS General Info
============================================================
AdminState : enabled
RouterType : Level 1
System ID : 0001.0001.0001
Max LSP Gen Interval : 900
Metric : wide
Overload-on-startup : 20
Overload : false
Csnp Interval : 10
PSNP Interval : 2
Rxmt LSP Interval : 5
spf-delay : 100
Router Name : VSP_01
ip source-address : 10.27.11.1
ipv6 source-address :
Num of Interfaces : 14
Num of Area Addresses : 1
```

VSP_01:1#SHOW ISIS SPBM NICK-NAME

```
============================================================
ISIS SPBM NICK-NAME
============================================================
LSP ID                          LIFETIME  NICK-NAME HOST-NAME
------------------------------------------------------------
0001.0001.0001.00-00            1188      7.00.01   VSP_01
0002.0002.0002.00-00            1188      7.00.02   VSP_02
0003.0003.0003.00-00            1188      7.00.03   VSP_03
0004.0004.0004.00-00            1188      7.00.04   VSP_04
------------------------------------------------------------
 Total Num of Entries: 4
------------------------------------------------------------
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VSP_01:1#SHOW ISIS SPBM

```
=========================================================
ISIS SPBM Info
=========================================================================
SPBM         B-VID        PRIMARY     NICK       LSDB       IP          IPV6
MULTICAST
INSTANCE               VLAN        NAME      TRAP
-------------------------------------------------------------
1            4051-4052   4051         7.00.01   disable   enable    disable
enable
=========================================================
ISIS SPBM SMLT Info
=========================================================
SPBM       SMLT-SPLIT-BEB       SMLT-VIRTUAL-BMAC     SMLT-PEER-SYSTEM-
ID
INSTANCE
-------------------------------------------------------------
1          primary              00:00:00:00:00:00
-------------------------------------------------------------
 Total Num of SPBM instances: 1
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.2.1 Implementación de Servicios:

a) Servicio LAN Extendida

Lan Extendida es un servicio que permite la interconexión de dos sedes remotas permitiendo manejar el mismo segmento de red.

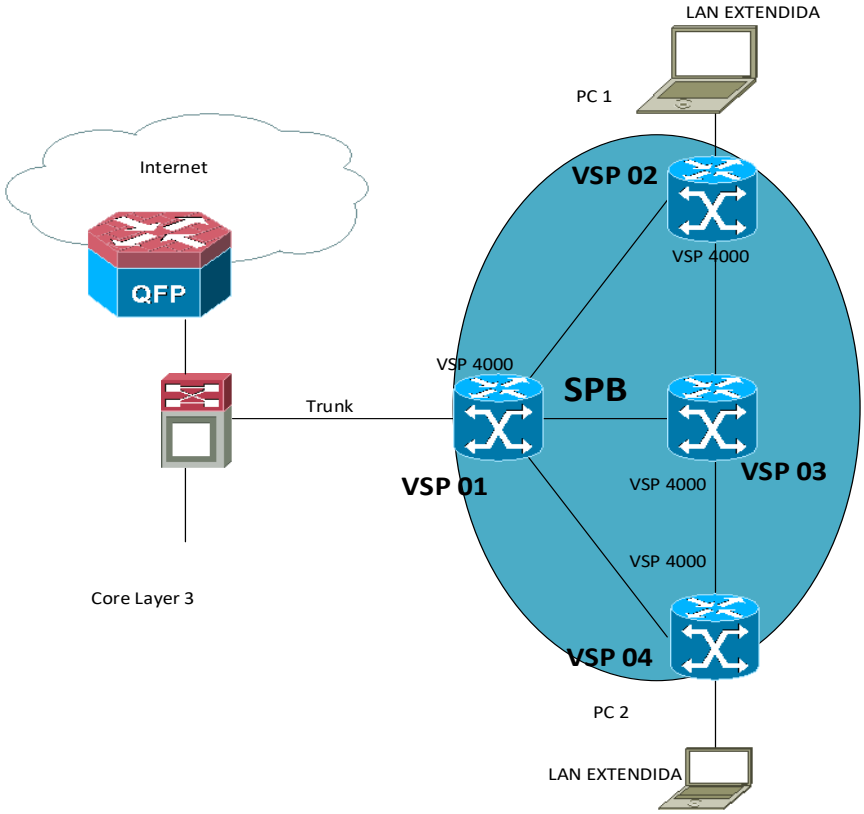

Figura 21. Topología de Lan Extendida

Fuente. Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Direccionamiento IP: 192.168.20.0/24

PC1: 192.168.20.10

PC2: 192.168.20.20

Configuración: Solo se realiza el aprovisionamiento en los bordes VSP4 y VSP02

VSP02

```
VSP_01:1(config)#vlan members remove 1 1/1
VSP_01:1(config)#vlan create 200 type port-mstprstp 1
VSP_01:1(config)#vlan members 200 1/1
VSP_01:1(config)#vlan i-sid 200 500
VSP_01:1(config)#show vlan i-sid
```

VSP04

```
VSP_04:1(config)#vlan members remove 1 1/1
VSP_04:1(config)#vlan create 200 type port-mstprstp 1
VSP_04:1(config)#vlan members 200 1/1
VSP_04:1(config)#vlan i-sid 200 500
VSP_04:1(config)#show vlan i-sid
```

Pruebas de Verificación:

PC1 PC2

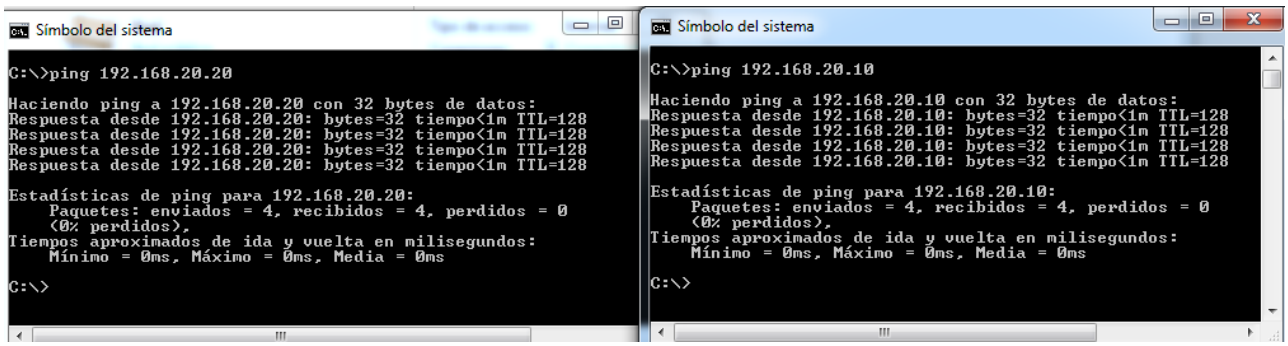

Figura 22. Pruebas de conectividad en LAN extendida

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) Servicio L2L

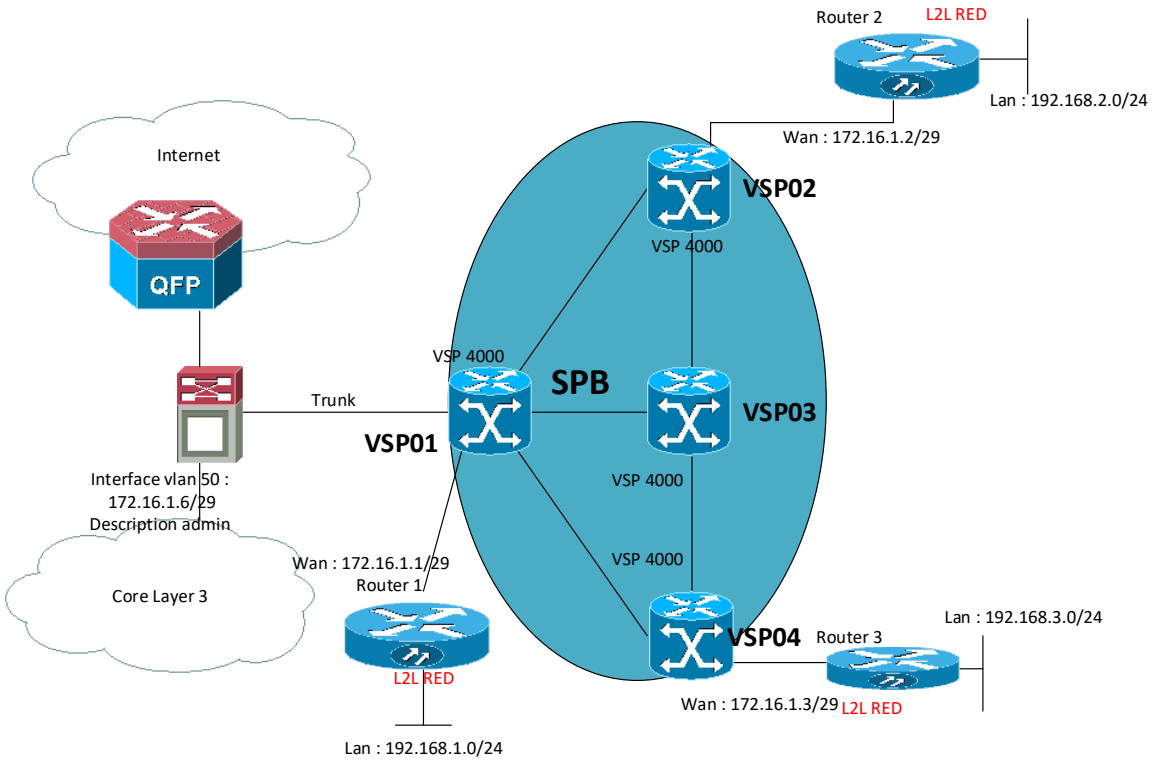

Figura 23. Topología L2L

Fuente. Propia

Configuración Routers L2L:

```
R1#show ip interface brief | e unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.1.1      YES manual up
FastEthernet1/0        192.168.1.1     YES manual up

ip route 192.168.2.0 255.255.255.0 172.16.1.2
ip route 192.168.3.0 255.255.255.0 172.16.1.3
ip route 190.12.64.138 255.255.255.255 172.16.1.5  name admin
```

```
R2#show ip interface brief | e unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.1.2      YES manual up
FastEthernet1/0        192.168.2.1     YES manual up                    up

ip route 192.168.1.0 255.255.255.0 172.16.1.1
ip route 192.168.3.0 255.255.255.0 172.16.1.3
ip route 190.12.64.138 255.255.255.255 172.16.1.5  name admin
```

```
R3#show ip interface brief | e unassigned
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.1.3      YES manual up                    up
FastEthernet1/0        192.168.3.1     YES manual up                    up

ip route 192.168.1.0 255.255.255.0 172.16.1.1
ip route 192.168.2.0 255.255.255.0 172.16.1.2
ip route 190.12.64.138 255.255.255.255 172.16.1.5  name admin
```

Configuración VSP Avaya :

VSP01

```
VSP_01:1(config)#vlan members remove 1 1/2 -1/3
VSP_01:1(config)#vlan create 201 type port-mstprstp 1
VSP_01:1(config)#vlan members 201 1/2- 1/3
VSP_01:1(config)#vlan i-sid 201 501
VSP_01:1(config)#show vlan i-sid
VSP_01:1(config)#vlan ports 1/2 tagging tag All
```

VSP02

```
VSP_02:1(config)#vlan members remove 1 /2
VSP_02:1(config)#vlan create 201 type port-mstprstp 1
VSP_02:1(config)#vlan members 201 1/2
VSP_02:1(config)#vlan i-sid 201 501
VSP_02:1(config)#show vlan i-sid
```

VSP04

```
VSP_04:1(config)#vlan members remove 1 /2
VSP_04:1(config)#vlan create 201 type port-mstprstp 1
VSP_04:1(config)#vlan members 201 1/2
VSP_04:1(config)#vlan i-sid 201 501
VSP_04:1(config)#show vlan i-sid
```

Configuracion Switch Admin

SW1

Vlan 201

```
Interface vlan 201
Ip address 172.16.1.5 255.255.255.248

Interface g0/1
Switchport mode trunk
Switchport trunk allowed vlan 27
Description conexion_vsp_01
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Pruebas de Verificacion:

Verificación **de Switch Admin:**

```
SW1#ping 172.16.1.1 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/4 ms
SW1#ping 172.16.1.2 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/8 ms
SW1#ping 172.16.1.3 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 172.16.1.3, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/8 ms
```

```
R2#ping 192.168.1.1 source 192.168.2.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/8 ms
R2#ping 192.168.3.1 source 192.168.2.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/8 ms
```

```
R3#ping 192.168.1.1 source 192.168.3.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/8 ms
R3#ping 192.168.2.1 source 192.168.3.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/8 ms
```

Figura 24. Prueba de conectividad L2L (VPLS)

Fuente. Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

c) Servicio Fibra Oscura QinQ:

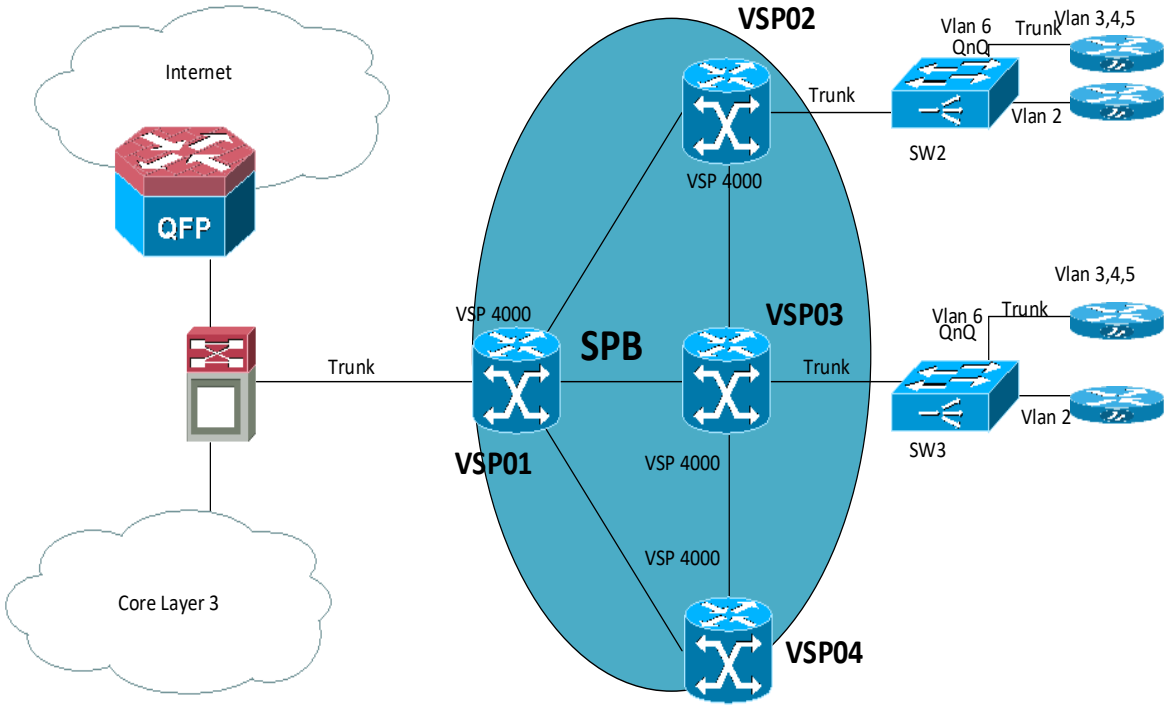

Figura 25. Servicio en fibra oscura QinQ

Fuente. Propia

Configuración Switch 2 y 3:

SW2 :

Vlan 6
Vlan 2
Interface g0/1
Switchport mode trunk
Switchport trunk allowed vlan 2,6
Description conexion VSP02

Interface g0/2
Switchport access vlan 6
switchport mode dot1q-tunnel
Description conexion trunk Router

Interface g0/2
Switchport access vlan 2

SW3 :

Vlan 6

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Vlan 2

Interface g0/1
Switchport mode trunk
Switchport trunk allowed vlan 2,6
Description conexion VSP03

Interface g0/2
Switchport access vlan 6
switchport mode dot1q-tunnel
Description conexion trunk Router

Interface g0/2
Switchport access vlan 2

Configuración Router VSP02

Router Trunk

interface FastEthernet0/0
no shutdown
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.2.1 255.255.255.0
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.3.1 255.255.255.0

Router vlan 2

interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0

Configuracion Router VSP03

Router Trunk

interface FastEthernet0/0

no shutdown

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.1.2 255.255.255.0
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.2.2 255.255.255.0
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.3.2 255.255.255.0
```

Router vlan 2

```
interface FastEthernet0/0
ip address 172.16.1.2 255.255.255.0
```

Configuración VSP02 y VSP03

VSP02

```
VSP_02:1(config)#i-sid 1000 elan-transparent
VSP_02:1(elan-tp:1000)#port 1/11
```

VSP03

```
VSP_03:1(config)#i-sid 1000 elan-transparent
VSP_03:1(elan-tp:1000)#port 1/11
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Pruebas de Verificación:

```
Router_TRUNK_vsp_02#ping 192.168.1.2 source 192.168.1.1 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms
Router_TRUNK_vsp_02#ping 192.168.2.2 source 192.168.2.1 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/8 ms
Router_TRUNK_vsp_02#ping 192.168.3.2 source 192.168.3.1 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/4 ms
```

```
Router_Vlan_VSP02#ping 172.16.1.2 source 172.16.1.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/8 ms
```

Figura 26. Prueba de conectividad QinQ

Fuente. Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

d) Servicio L2L e Internet:

Las configuraciones más comunes para acceder a los servicios de internet son importantes para las empresas que requiere un servicio de acceso dedicado.

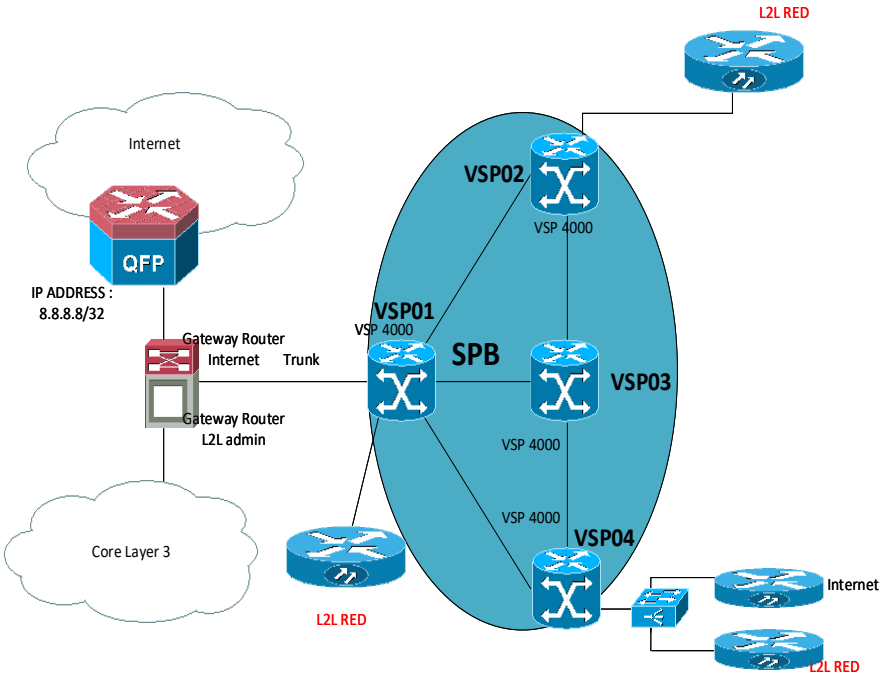

Figura 27. Topología para el acceso de Internet

Fuente. Propia.

Configuración VSP:

VSP01

VSP_01:1(config)#vlan members remove 1 1/2 -1/3

VSP_01:1(config)#vlan create 201 type port-mstprstp 1

VSP_01:1(config)#vlan create 202 type port-mstprstp 1

VSP_01:1(config)#vlan members 201 1/2- 1/3

VSP_01:1(config)#vlan members 202 1/2

VSP_01:1(config)#vlan i-sid 201 501

VSP_01:1(config)#vlan i-sid 202 502

VSP_01:1(config)#show vlan i-sid

VSP_01:1(config)#vlan ports 1/2 tagging tag All

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VSP02

VSP_02:1(config)#vlan members remove 1 /2

VSP_02:1(config)#vlan create 201 type port-mstprstp 1

VSP_02:1(config)#vlan members 201 1/2

VSP_02:1(config)#vlan i-sid 201 501

VSP_02:1(config)#show vlan i-sid

VSP04

VSP_04:1(config)#vlan members remove 1 1/2

VSP_04:1(config)#vlan create 201 type port-mstprstp 1

VSP_04:1(config)#vlan create 202 type port-mstprstp 1

VSP_04:1(config)#vlan members 201 1/2

VSP_04:1(config)#vlan members 202 1/2

VSP_04:1(config)#vlan i-sid 201 501

VSP_04:1(config)#vlan i-sid 202 502

VSP_01:1(config)#vlan ports 1/2 tagging tagAll

VSP_04:1(config)#show vlan i-sid

Config Switch VSP04

Vlan 201

Vlan 202

Interface g0/1

Switchport mode trunk

Interface g0/2

Switchport access vlan 201

Interface g0/2

Switchport access vlan 202

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Configuracion Switch Admin

SW1

Vlan 201

Vlan 202

Interface loopback 1

Ip address 8.8.8.8 255.255.255.255

Description internet

Interface vlan 201

Description admin_router_L2L

Ip address 172.16.1.5 255.255.255.248

Interface vlan 202

Description admin_router_internet

Ip address 10.100.1.1 255.255.255.252

Interface g0/1

Switchport mode trunk

Switchport trunk allowed vlan 201,202

Description conexion_vsp_01

Ip route 190.12.64.1 255.255.255.248 10.100.1.2 name cliente1

** La configuración de los Router L2L es la misma al ejemplo anterior.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Configuración de router de Internet

Router Internet

Interface f0/0

Ip add 10.100.1.2 255.255.255.252

Interface f0/1

Ip address 190.12.64.1 255.255.255.248

Ip route 0.0.0.0 0.0.0.0 10.100.1.1 name core_internet

Pruebas de Verificación: Internet

```
Router_Internet#ping 8.8.8.8 source 190.12.64.1  repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 190.12.64.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/8 ms
```

Figura 28. Prueba de conectividad L2L-Internet

Fuente. Propia.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.3 Implementación del protocolo MPLS

MPLS VPN, o MPLS Virtual Private Networks, es la más popular y extendida tecnología en redes de transporte de datos. Su popularidad ha crecido exponencialmente desde su invento, y todavía está creciendo constantemente. Aunque la mayoría de los proveedores de servicios lo han implementado, MPLS VPN ahora está viendo un interés creciente de las grandes empresas que lo ven como el siguiente paso en su diseño de red las configuraciones que se mostraran funcionan en los equipos Huawei.

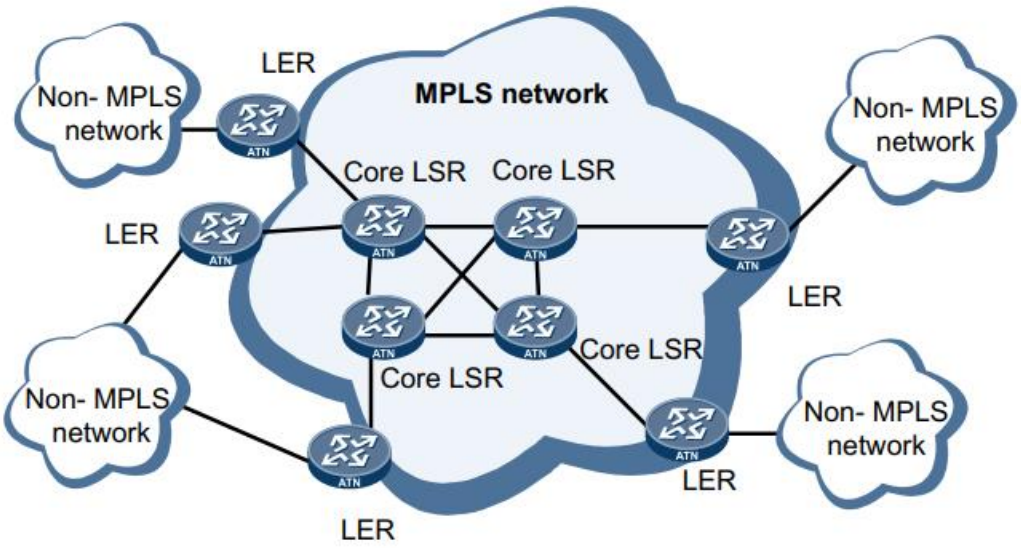

Figura 29. Red MPLS

Fuente. Huawei

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Habilitando MPLS

Paso 1 Ejecutar:

```
System-view
```

Se muestra la vista del sistema.

Paso 2 Ejecutar:

```
 mpls
```

MPLS está habilitado globalmente y se muestra la vista MPLS.

Paso 3 Ejecutar:

```
quit
```

Regrese a la vista del sistema.

Paso 4 Ejecutar:

```
Interface interface-type interface-number
```

La interfaz para participar en el reenvío MPLS está especificada. La interfaz debe ser una interfaz VLANIF.

Paso 5 Ejecutar:

```
mpls
```

MPLS está habilitado en la interfaz.

----End

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

a) MPLS Internet Static

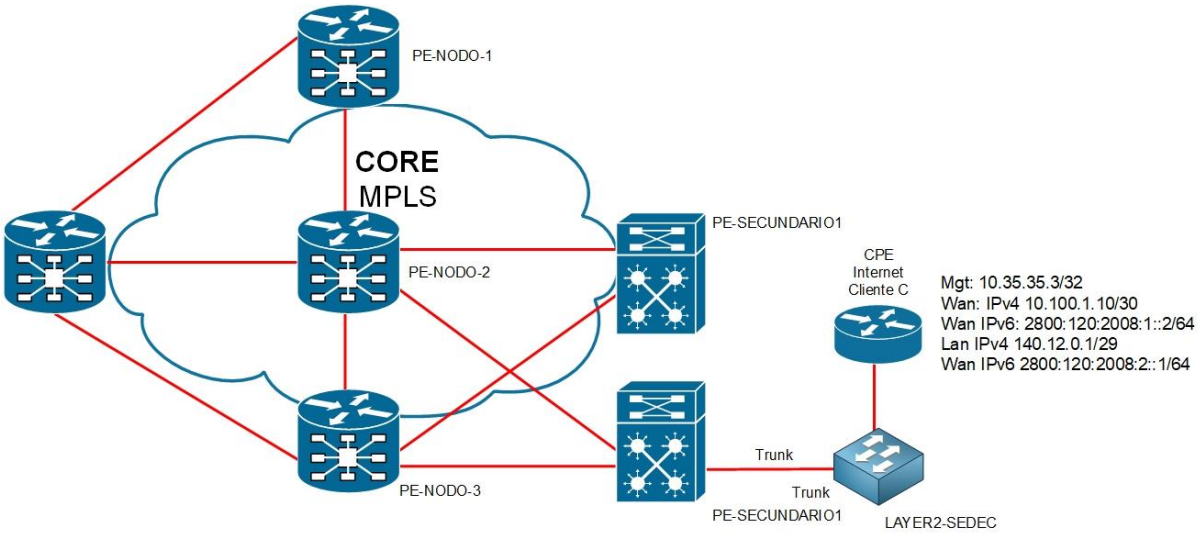

Figura 30. Diseño de RED – Internet Static MPLS

Fuente. propia

1. **CONFIGURACION EN PE-SECUNDARIO**

```
#
# Configuracion VRF Internet IPv4/IPv6.
ip vpn-instance INTERNET
 description Acceso Internet v4_v6
 ipv4-family
  route-distinguisher 27843:27843
  export route-policy MGMT_Loopback_CE
  vpn-target 27843:27843 export-extcommunity
  vpn-target 27843:27843 27843:10000 import-extcommunity
 ipv6-family
  route-distinguisher 27843:27843
  vpn-target 27843:27843 export-extcommunity
  vpn-target 27843:27843 import-extcommunity
#
# Configuracion BGP importando rutas estáticas.
```

```
bgp 27843
 #
 ipv4-family vpn-instance INTERNET
  import-route static route-policy STATIC_TO_BGP
 #
 ipv6-family vpn-instance INTERNET
  import-route direct
  import-route static
#
# Aplicando VPN-Target sobre las Loopback de gestión de CE.
route-policy MGMT_Loopback_CE permit node 10
 if-match ip-prefix LoopbacksCE
 apply extcommunity rt 27843:10001
#
route-policy MGMT_Loopback_CE permit node 1000
#
route-policy STATIC_TO_BGP permit node 10
 if-match tag 10000
#
route-policy STATIC_TO_BGP deny node 1000
#
route-policy STATIC_TO_BGP_V6 permit node 10
 if-match tag 60000
#
route-policy STATIC_TO_BGP_V6 deny node 1000
#
# Especificando segmento de Loopback de gestión de CE.
ip ip-prefix LoopbacksCE index 10 permit 10.35.35.0 24 greater-equal 24 less-
equal 32
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
#
# Creación de Interfaces de acceso a Cliente.
interface Vlanif1500
 ip binding vpn-instance INTERNET
 ipv6 enable
 ip address 10.100.1.9 255.255.255.252
 ipv6 address 2800:120:2008:1::1/64
#
interface GigabitEthernet0/0/25
 description Trunk to Access Switch
 port link-type trunk
 port trunk allow-pass vlan 1500
#
# Rutas tageadas para importarse a la sesión BGP de la VRF INTERNET.
ip route-static vpn-instance INTERNET 10.35.35.3 255.255.255.255
10.100.1.10 tag 10000 description MGMT
ip route-static vpn-instance INTERNET 140.12.0.0 255.255.255.248
10.100.1.10 tag 10000 description ClienteC
#
ipv6 route-static vpn-instance INTERNET 2800:120:2008:2:: 64
2800:120:2008:1::2 tag 60000
```

2. **CONFIGURACION EN CPE-CISCO**

```
hostname Cliente-C
ipv6 unicast-routing
interface Loopback1
 description Loopback for MGMT
 ip address 10.35.35.3 255.255.255.255
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
!
interface FastEthernet0/0
 description Interface WAN para el servicio de INTERNET
 ip address 10.100.1.10 255.255.255.252
 ipv6 address 2800:120:2008:1::2/64
 ipv6 enable
!
interface FastEthernet0/1
 description Interface LAN
 ip address 140.12.0.1 255.255.255.248
 ipv6 address 2800:120:2008:2::1/64
 ipv6 enable
!
ip route 0.0.0.0 0.0.0.0 10.100.1.9
!
ipv6 route ::/0 2800:120:2008:1::1
!
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

b) MPLS VPN L2

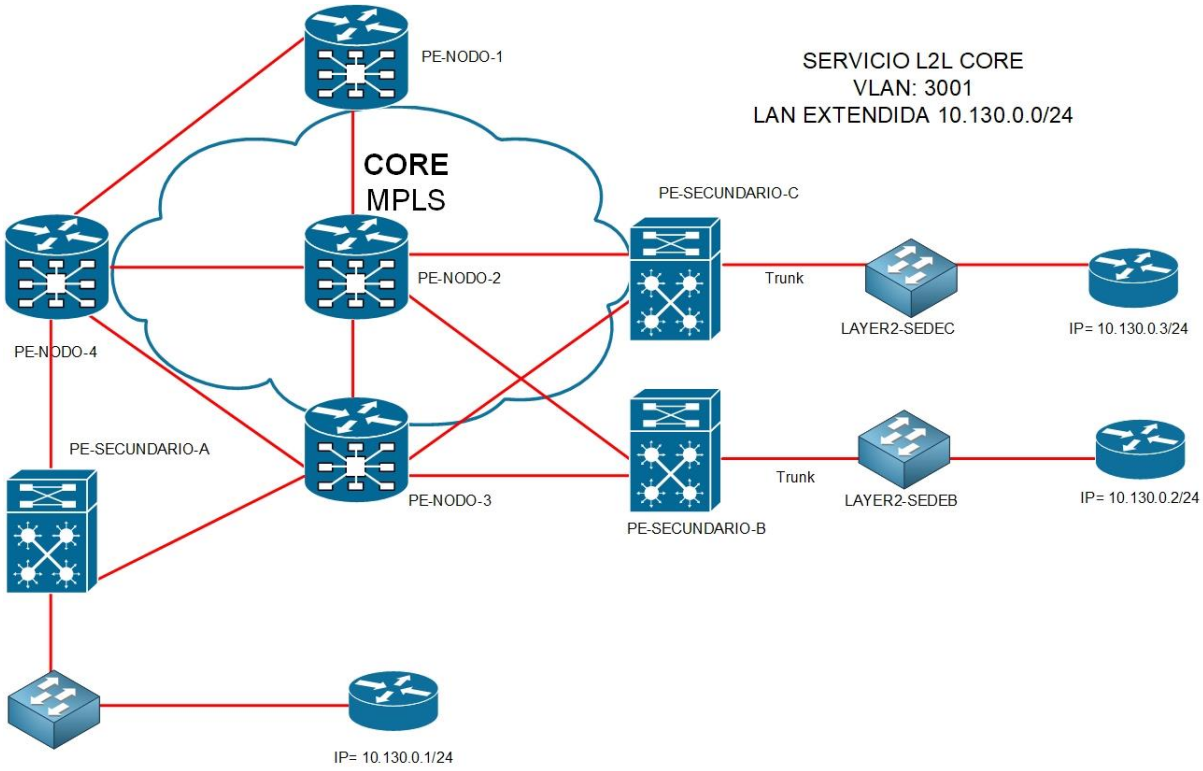

Figura 31. Diseño de Servicio MPLS L2L

Fuente. Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Configuración en los equipos

PE SECUNDARIO A

```
vlan 3005
 name VPLS
mpls l2vpn
vsi 100 static
 description CUSTOMER_VPLS
 pwsignal ldp
  vsi-id 100
  peer 10.32.2.13
  peer 10.32.2.14
mpls ldp remote-peer 10.32.2.13
 remote-ip 10.32.2.13
#
mpls ldp remote-peer 10.32.2.14
 remote-ip 10.32.2.14

interface Vlanif3005
 description CUSTOMER VPLS
 l2 binding vsi 100
```

PE SECUNDARIO B

```
vlan 3005
 name VPLS
mpls l2vpn
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
vsi 100 static
 description CUSTOMER_VPLS
 pwsignal ldp
  vsi-id 100
  peer 10.32.2.12
  peer 10.32.2.14

mpls ldp remote-peer 10.32.2.12
 remote-ip 10.32.2.12

mpls ldp remote-peer 10.32.2.14
 remote-ip 10.32.2.14

interface Vlanif3005
 description CUSTOMER VPLS
 l2 binding vsi 100
```

PE SECUNDARIO C

```
vlan 3005
 name VPLS
mpls l2vpn
vsi 100 static
 description CUSTOMER_VPLS
 pwsignal ldp
  vsi-id 100
  peer 10.32.2.12
  peer 10.32.2.13
mpls ldp remote-peer 10.32.2.12
 remote-ip 10.32.2.12
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
mpls ldp remote-peer 10.32.2.13
 remote-ip 10.32.2.13
interface Vlanif3005
 description CUSTOMER VPLS
 l2 binding vsi 100
```

Configuración equipos CPE

CPE SEDE A	CPE SEDE B	CPE SEDE C
interface FastEthernet0/0.3005	interface FastEthernet0/0.3005	interface FastEthernet0/0.3005
encapsulation dot1Q 3005	encapsulation dot1Q 3005	encapsulation dot1Q 3005
ip address 10.130.0.1 255.255.255.0	ip address 10.130.0.2 255.255.255.0	ip address 10.130.0.3 255.255.255.0

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Comandos de Verificación

Ejecutar el comando **display vsi** [**name** *vsi-name*] [**verbose**] commando para verificar la información sobre VPLS VSI.

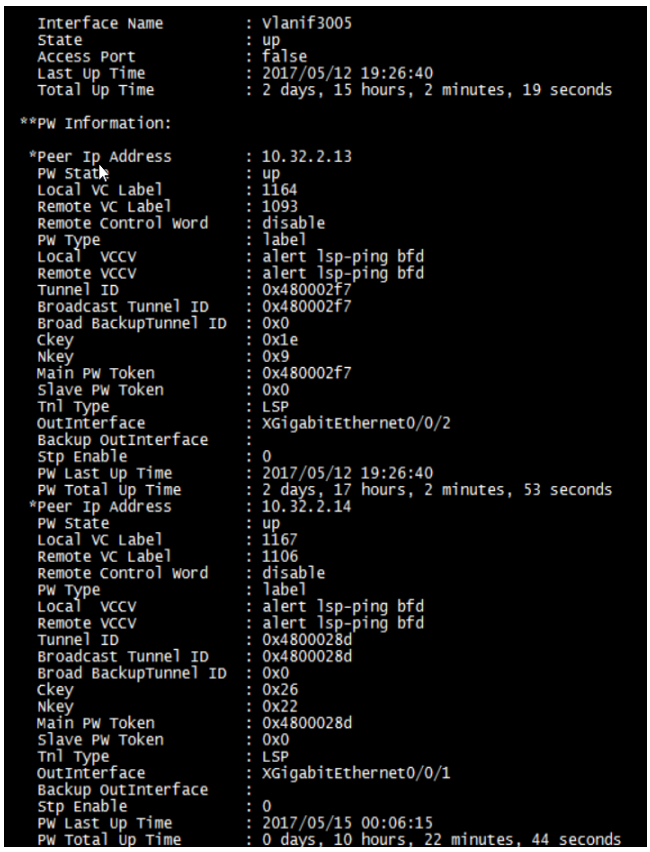

Figura 32. Visualización de VPLS VSI

Fuente: Propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

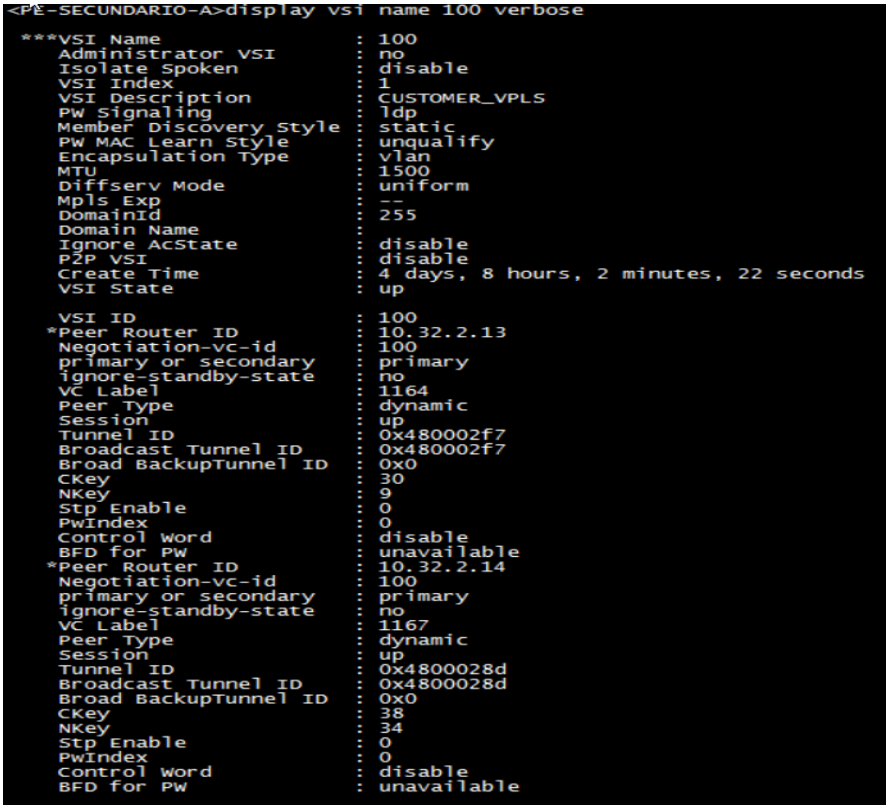

Figura 33. Visualización display VSI

Fuente. propia

Activar la función de las estadísticas de tráfico en Martini VPLS PW

vsi 100 static

pwsignal ldp

traffic-statistics enable

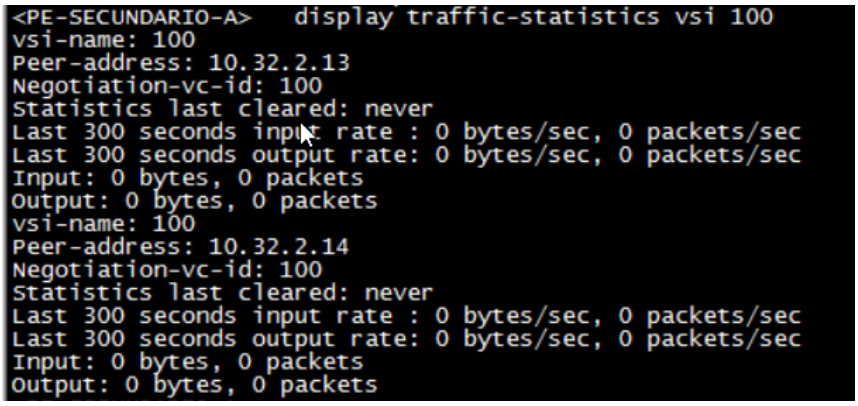

Figura 34. Visualizar estadísticas de tráfico VSI

Fuente. Propia

```
<PE-SECUNDARIO-A>display mpls l2vpn resource

 Public Capacity Statistics
 Statistics Item                    Supported Number      Used Number
 L2VPN AC Number                    2000                  2
 L2VPN VC Number                    8000                  3

 VPWS Capacity Statistics
 Statistics Item                    Supported Number      Used Number
 L2VPN Local CCC Number             512                   0
 L2VPN Remote CCC Number            1008                  0
 L2VPN SVC Number                   1008                  0
 L2VPN LDP VC Number                2000                  1
 L2VPN BGP VC Number                2000                  0
 L2VPN Switch VC Number             2000                  0

 VPLS Capacity Statistics
 Statistics Item                    Supported Number      Used Number
 L2VPN VSI Number                   1024                  1
 L2VPN BGP VSI Number               1024                  0
 L2VPN VSI VC Number                8000                  2
```

Figura 35. Visualizar estadísticas de tráfico L2

Fuente. Propia

Ejecutar el comando **display l2vpn ccc-interface vc-type** { **all** | *vc-type* } [**down** | **up**] para verificar la información de acerca de la interface que usa la conexión L2VPN.

Ejecutar el commando **display vsi remote** **ldp** [[**router-id** *ip-address*] [**pw-id** *pw-id*] | **unmatch** | **verbose**] command to check information about a remote VSI.

```
<PE-SECUNDARIO-A>display vsi pw out-interface vsi 100
Total: 2
-------------------------------------------------------------------------------
Vsi Name                        peer            vcid        interface
-------------------------------------------------------------------------------
100                             10.32.2.13      100         XGigabitEthernet0/0/2
                                10.32.2.14      100         XGigabitEthernet0/0/1
```

Run the **display vpls connection** [**ldp** | **vsi** *vsi-name*] [**down** | **up**] [**verbose**] command to check information about a VPLS connection.

```
<PE-SECUNDARIO-A>display vpls connection ldp

2 total ldp connections ,
connections: 2 up, 0 down

VSI Name: 100                                   Signaling: ldp
VsiID               EncapType       PeerAddr        InLabel   OutLabel  VCState
100                 vlan            10.32.2.13      1164      1093      up
100                 vlan            10.32.2.14      1167      1106      up
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
<PE-SECUNDARIO-A>display vpls connection vsi 100 verbose
VSI Name: 100                                    Signaling: ldp
  **Remote Vsi ID    : 100
    VC State         : up
    Encapsulation    : vlan
    Group ID         : 0
    MTU              : 1500
    Peer Ip Address  : 10.32.2.13
    PW Type          : label
    Local VC Label   : 1164
    Remote VC Label  : 1093
    Tunnel Policy    : --
    Tunnel ID        : 0x480002f7
  **Remote Vsi ID    : 100
    VC State         : up
    Encapsulation    : vlan
    Group ID         : 0
    MTU              : 1500
    Peer Ip Address  : 10.32.2.14
    PW Type          : label
    Local VC Label   : 1167
    Remote VC Label  : 1106
    Tunnel Policy    : --
    Tunnel ID        : 0x4800028d
```

Run the **display vpls forwarding-info** [**vsi** *vsi-name* [**peer** *peer-address* [**negotiation-vc-id** *vc-id* | **remote-site** *site-id*]] | **state** { **up** | **down** }] [**verbose**] command to check forwarding information of all VSIs.

```
<PE-SECUNDARIO-A>display vpls forwarding-info
Total Number    : 2,        2  up,  0  down

Vsi-Name                    PeerIP          VcOrSiteId  PwState
100                         10.32.2.13      100         UP
100                         10.32.2.14      100         UP
```

Run the **display vsi services** { **all** | *vsi-name* | **interface** *interface-type interface-number* | **vlan** *vlan-id* } command to check information about the AC interface associated with the VSI.

```
<PE-SECUNDARIO-A>display vpls forwarding-info
Total Number    : 2,        2  up,  0  down

Vsi-Name                    PeerIP          VcOrSiteId  PwState
100                         10.32.2.13      100         UP
100                         10.32.2.14      100         UP
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Run the **display vsi pw out-interface** [**vsi** *vsi-name*] command to check information about the outgoing interface of a PW in a VSI.

```
<PE-SECUNDARIO-A>display vsi pw out-interface vsi 100
Total: 2
-------------------------------------------------------------------------------
Vsi Name                        peer            vcid        interface
-------------------------------------------------------------------------------
100                             10.32.2.13      100         XGigabitEthernet0/0/2
                                10.32.2.14      100         XGigabitEthernet0/0/1
```

Run the **display l2vpn vsi-list tunnel-policy** *policy-name* command to check information about the tunnel policy applied to a VSI.

Run the **ping vpn-config peer-address** *peer-address* **vsi-name** *vsi-name* [**pw-id** *pw-id*] [**local**] [**remote**] command to check configurations of the VSI on the peer PE.

Run the **display mpls label-stack vpls vsi** *vsi-name* **peer** *peer-ip-address* **vc-id** *vc-id* command to check the information about label stacks in a VPLS scenario.

Run the **display traffic-statistics vsi** *vsi-name* command to check the public traffic statistics on all VPLS PWs in a specified VSI.

Run the **display traffic-statistics vsi** *vsi-name* **peer** *peer-address* command to check the public traffic statistics on a VPLS PW in a specified VSI.

Run the **display traffic-statistics vsi** *vsi-name* **peer** *peer-address* **remote-site** *site-id* command to check the public traffic statistics on a Kompella VPLS PW in a specified VSI.

Run the **display traffic-statistics vsi** *vsi-name* **peer** *peer-address* **negotiation-vc-id** *vc-id* command to check the public traffic statistics on a Martini VPLS PW in a specified VSI.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Run the **display traffic-statistics vsi** *vsi-name* **peer** *peer-address* **ldp129** command to check the public traffic statistics on a BGP AD VPLS PW in a specified VSI.

Run the **display interface** **vlanif** *interface-number* command to check the traffic statistics on the VLANIF interface bound to the specified VSI.

Verificaciones de conectividad VPLS

El resultado del comando ping VPLS contiene la siguiente información:

Respuesta a cada paquete ping VPLS. Si no se recibe ningún paquete de respuesta después de que expira el temporizador correspondiente, aparece el mensaje que dice "Request time out". Si se recibe un paquete de respuesta, se muestran el número de bytes de datos, el número de secuencia del paquete, el TTL y el tiempo de respuesta. Estadísticas finales: incluye el número de paquetes enviados, el número de paquetes recibidos, el porcentaje de paquetes enviados con respuestas fallidas y los tiempos de respuesta mínimo, máximo y promedio.

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*] [**control-word** [**remote** *remote-address* *remote-pw-id* [**sender** *sender-address*]]] [**bypass -si** *interface-type interface-number*]

```
<PE-SECUNDARIO-A>ping vpls vsi 100 peer 10.32.2.13
    Reply from 10.32.2.13: bytes=100 Sequence=1 time=2 ms
    Reply from 10.32.2.13: bytes=100 Sequence=2 time=2 ms
    Reply from 10.32.2.13: bytes=100 Sequence=3 time=2 ms
    Reply from 10.32.2.13: bytes=100 Sequence=4 time=2 ms
    Reply from 10.32.2.13: bytes=100 Sequence=5 time=2 ms

  --- FEC: FEC 128 PSEUDOWIRE (NEW). Type = vlan, ID = 100 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms

<PE-SECUNDARIO-A>ping vpls vsi 100 peer 10.32.2.14
    Reply from 10.32.2.14: bytes=100 Sequence=1 time=3 ms
    Reply from 10.32.2.14: bytes=100 Sequence=2 time=2 ms
    Reply from 10.32.2.14: bytes=100 Sequence=3 time=2 ms
    Reply from 10.32.2.14: bytes=100 Sequence=4 time=3 ms
    Reply from 10.32.2.14: bytes=100 Sequence=5 time=3 ms

  --- FEC: FEC 128 PSEUDOWIRE (NEW). Type = vlan, ID = 100 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Prueba de conectividad entre CPE clientes

```
CLIENTE_A#ping 10.130.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
CLIENTE_A#ping 10.130.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CLIENTE_A#ping 10.130.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
CLIENTE_B#ping 10.130.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
CLIENTE_B#ping 10.130.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
CLIENTE_B#ping 10.130.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.130.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

c) Internet con alta disponibilidad MPLS – BGP

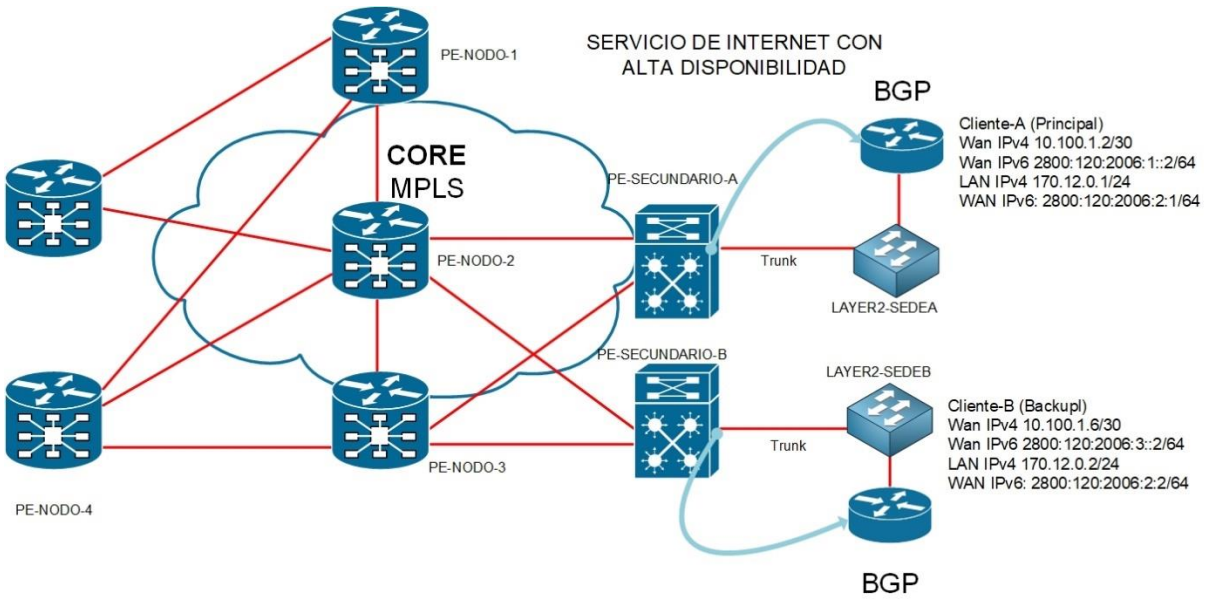

Figura 36. Servicio de Internet con alta disponibilidad

Fuente. Propia

1. CONFIGURACION EN PE-SECUNDARIO

```
# ConfiguracionVRF Internet IPv4/IPv6.
ip vpn-instance INTERNET
 description Acceso Internet v4_v6
 ipv4-family
  route-distinguisher 27843:27843
  export route-policy MGMT_Loopback_CE
  vpn-target 27843:27843 export-extcommunity
  vpn-target 27843:27843 27843:10000 import-extcommunity
 ipv6-family
  route-distinguisher 27843:27843
  vpn-target 27843:27843 export-extcommunity
  vpn-target 27843:27843 import-extcommunity
#
```

```
# Configuracion BGP importando rutas estáticas.
bgp 27843
 #
 ipv4-family vpn-instance INTERNET
  import-route static route-policy STATIC_TO_BGP
 #
 ipv4-family vpn-instance INTERNET
  preference 20 200 200
  import-route direct
  group CLIENTE_A external
  peer CLIENTE_A as-number 64512
  peer CLIENTE_A substitute-as
  peer 10.100.1.2 as-number 64512
  peer 10.100.1.2 group CLIENTE_A
  peer 10.100.1.2 description CLIENTE_A_MAIN
  peer CLIENTE_A route-policy MULTIHOMING import
 #
# Aplicando VPN-Target sobre las Loopback de gestión de CE.
route-policy MGMT_Loopback_CE permit node 10
 if-match ip-prefix LoopbacksCE
 apply extcommunity rt 27843:10001
#
route-policy MGMT_Loopback_CE permit node 1000
#
# Leer la comunidad de las rutas bgp enviadas por el CE.
ip community-filter basic COMM_LP80 permit 27843:80
ip community-filter basic COMM_LP90 permit 27843:90
ip community-filter basic COMM_LP110 permit 27843:110
ip community-filter basic COMM_LP120 permit 27843:120
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
ip community-filter basic COMM_LP100 permit 27843:100
# Aplicar LP a las rutas bgp enviadas por el CE
#
route-policy MULTIHOMING permit node 10
 if-match community-filter COMM_LP80
 apply local-preference 80
#
route-policy MULTIHOMING permit node 20
 if-match community-filter COMM_LP90
 apply local-preference 90
#
route-policy MULTIHOMING permit node 30
 if-match community-filter COMM_LP100
 apply local-preference 100
#
route-policy MULTIHOMING permit node 40
 if-match community-filter COMM_LP110
 apply local-preference 110
#
route-policy MULTIHOMING permit node 50
 if-match community-filter COMM_LP120
 apply local-preference 120
#
route-policy MULTIHOMING deny node 1000
#
# Especificando segmento de Loopback de gestión de CE.
ip ip-prefix LoopbacksCE index 10 permit 10.35.35.0 24 greater-equal 24 less-
equal 32
#
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
# Creación de Interfaces de acceso a Cliente.
interface Vlanif1500
 ip binding vpn-instance INTERNET
 ipv6 enable
 ip address 10.100.1.1 255.255.255.252
 ipv6 address 2800:120:2006:1::1/64
#
interface GigabitEthernet0/0/25
 description Trunk to Access Switch
 port link-type trunk
 port trunk allow-pass vlan 1500 2501
#
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CONFIGURACION EN CPE-CISCO

CLIENTE-A-PRINCIPAL

```
#
hostname CLIENTE-A-PRINCIPAL
!
ip sla monitor 100
 type echo protocol ipIcmpEcho 10.100.1.1 source-ipaddr 10.100.1.2
 frequency 5
ip sla monitor schedule 100 life forever start-time now
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 description Interface WAN para el servicio de INTERNET
 ip address 10.100.1.2 255.255.255.252
 ipv6 address 2800:120:2006:1::2/64
 ipv6 enable
 ipv6 nd suppress-ra
!
interface FastEthernet0/1
 description Interface LAN
 ip address 170.12.0.1 255.255.255.248
 ipv6 address 2800:120:2006:2::1/64
 ipv6 enable
 standby version 2
 standby 1 ip 170.12.0.3
 standby 1 timers 5 15
 standby 1 priority 200
 standby 1 preempt
 standby 1 track 110 decrement 100
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
 standby 3 priority 110
 standby 3 preempt
!
router bgp 64512
 bgp log-neighbor-changes
 neighbor 10.100.1.1 remote-as 27843
 neighbor 2800:120:2006:1::1 remote-as 27843
 !
 address-family ipv4
  neighbor 10.100.1.1 activate
  neighbor 10.100.1.1 send-community
  neighbor 10.100.1.1 soft-reconfiguration inbound
  neighbor 10.100.1.1 route-map INT_DEFAULT in
  neighbor 10.100.1.1 route-map NET_PRINC out
  no neighbor 2800:120:2006:1::1 activate
  no auto-summary
  no synchronization
  network 170.12.0.0 mask 255.255.255.248
 exit-address-family
 !
 address-family ipv6
  neighbor 2800:120:2006:1::1 activate
 exit-address-family
!
ip bgp-community new-format
!
ip prefix-list default_int seq 10 permit 0.0.0.0/0
ip prefix-list default_int seq 20 deny 0.0.0.0/0 le 32
!

ip prefix-list network seq 20 permit 170.12.0.0/29
ip prefix-list network seq 30 deny 0.0.0.0/0 le 32
!
route-map NET_PRINC permit 10
 match ip address prefix-list network
 set community 27843:120
!
route-map INT_DEFAULT permit 10
 match ip address prefix-list default_int
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Cliente-A-Backup

```
!
hostname Cliente-A-Backup
!
ipv6 unicast-routing
!
voice-card 0
!
interface FastEthernet0/0
 description Interface WAN para el servicio de INTERNET
 ip address 10.100.1.6 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2800:120:2006:3::2/64
 ipv6 enable
!
interface FastEthernet0/1
 description Interface LAN
 ip address 170.12.0.2 255.255.255.248
 ipv6 address 2800:120:2006:2::2/64
 ipv6 enable
 standby version 2
 standby 1 ip 170.12.0.3
 standby 1 timers 5 15
 standby 1 priority 200
 standby 1 preempt
 standby 1 track 110 decrement 100
 standby 3 priority 110
 standby 3 preempt
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
!
router bgp 64512
 bgp log-neighbor-changes
 neighbor 10.100.1.5 remote-as 27843
 !
 address-family ipv4
  neighbor 10.100.1.5 activate
  neighbor 10.100.1.5 send-community
  neighbor 10.100.1.5 soft-reconfiguration inbound
  neighbor 10.100.1.5 route-map INT_DEFAULT in
  neighbor 10.100.1.5 route-map NET_BACKUP out
  no auto-summary
  no synchronization
  network 170.12.0.0 mask 255.255.255.248
 exit-address-family
ip bgp-community new-format
ip prefix-list default_int seq 10 permit 0.0.0.0/0
ip prefix-list default_int seq 20 deny 0.0.0.0/0 le 32
ip prefix-list network seq 20 permit 170.12.0.0/29
ip prefix-list network seq 30 deny 0.0.0.0/0 le 32
route-map NET_BACKUP permit 10
 match ip address prefix-list network
 set community 27843:90
route-map INT_DEFAULT permit 10
 match ip address prefix-list default_int
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.3 Determinar el escenario donde se implementará las pruebas el protocolo

En un entorno real se puede buscar a las empresas operadoras en el Perú tienen un número menor de 1,000 cliente según el informe de OSIPTEL a junio 2017 muestra todas las empresas reportadas filtramos las que tienen menos de 100 clientes el resultado nos da 9 empresas quienes necesitarían implementar este protocolo de transporte para poder ser escalables y atender a un número mayor de clientes.

La prueba del protocolo de realizar en el ISP Optical Technologies SAC quien tiene actualmente más de 2,641 cliente con la necesidad de mejorar el transporte de los datos por lo que se ha considerado una topología base descrita en la figura 34.

Tabla 7

Empresas ISP en el Perú con necesidad de un protocolo de transporte

Empresa	Clientes
Telefónica del Perú S.A.A.	1,661,628
América Móvil Perú S.A.C.	424,594
Entel Perú S.A.	56,921
Americatel Perú S.A.	8,485
Optical Technologies S.A.C.	2,641
Supercable Televisión S.R.L.	1,668
Winner Systems S.A.C.	925
Red Intercable Perú S.A.C.	766
Fiberlux S.A.C.	661
Telefónica Multimedia S.A.C.	599
Netline Perú S.A.	566
Multiservicios de Telecomunicaciones Satelital E.I.R.L.	436
Yachay Telecomunicaciones S.A.C.	222
TVS Wireless S.A.C.	221
Wigo S.A.	173

Empresas operadoras de telecomunicaciones reportadas por Osiptel con su respectiva cantidad de clientes reportada a junio 2017, Fuente. OSIPTEL

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Para realizar las pruebas de estos protocolos se requiere un escenario donde simular las pruebas y configuración del protocolo MPLS o SPB el escenario modelo debe estar conformado con la siguiente arquitectura lógica que simule la red Backbone de transporte donde se pueda aplicar las configuraciones las opciones iniciales son utilizar los emuladores que permitan crear la topología base:

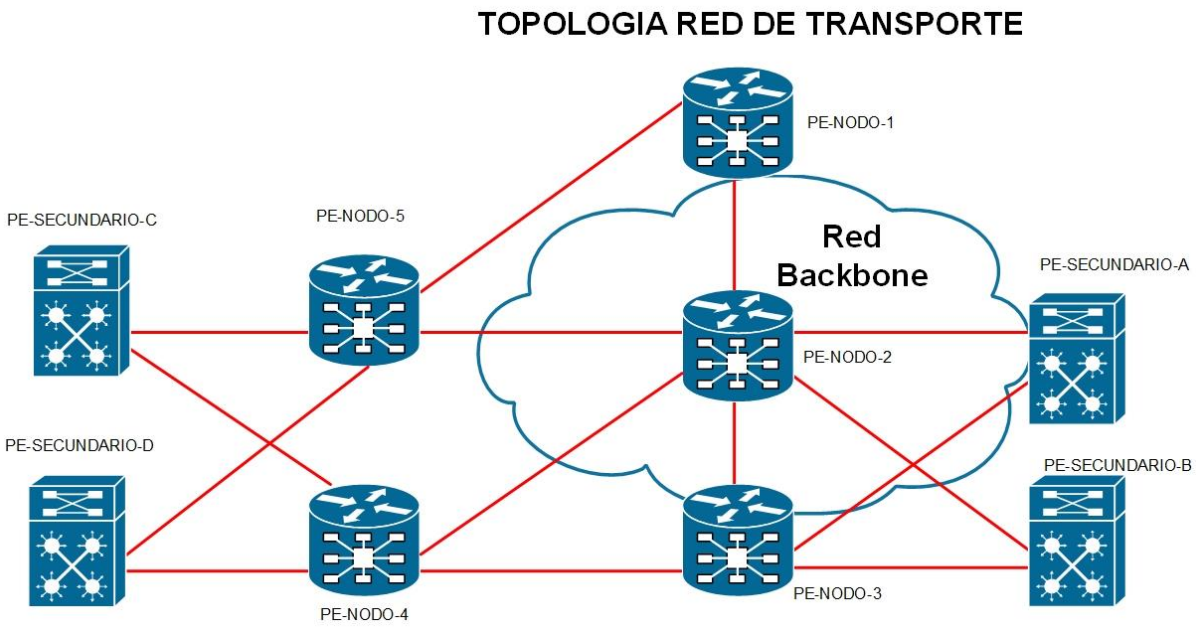

Figura 37. Topología modelo para implementar el protocolo MPLS/SPB

Fuente. Propia

La topología modelo permita realizar las pruebas en los CPE equipos finales que se ubicara en los clientes finales las funciones de los equipos serían las siguientes:

- PE-SECUNDARIO .- (Provider Edge) Reciben y mantienen información de rutas de las VPNs directamente conectadas, reducen la cantidad de información que tiene que almacenar el PE.
- PE-NODOS.- Son los equipos que realizaran el transporte, etiquetados de los datos esto permitirá poder brindar servicios a los clientes, este tipo de red puede soportar voz, datos y video.

Para realizar la emulación de la topología se utilizará el software EVE (Emulated Virtual Enviroment), la plataforma EVE-NG permite a las empresas, a los

proveedores / centros de aprendizaje electrónico, a los individuos y a los colaboradores del grupo crear pruebas virtuales de conceptos, soluciones y entornos de capacitación.

EVE-NG es el primer software de emulación de red de múltiples proveedores sin cliente que permite a los profesionales de redes y seguridad tener grandes oportunidades en el mundo de las redes.

http://www.eve-ng.net/

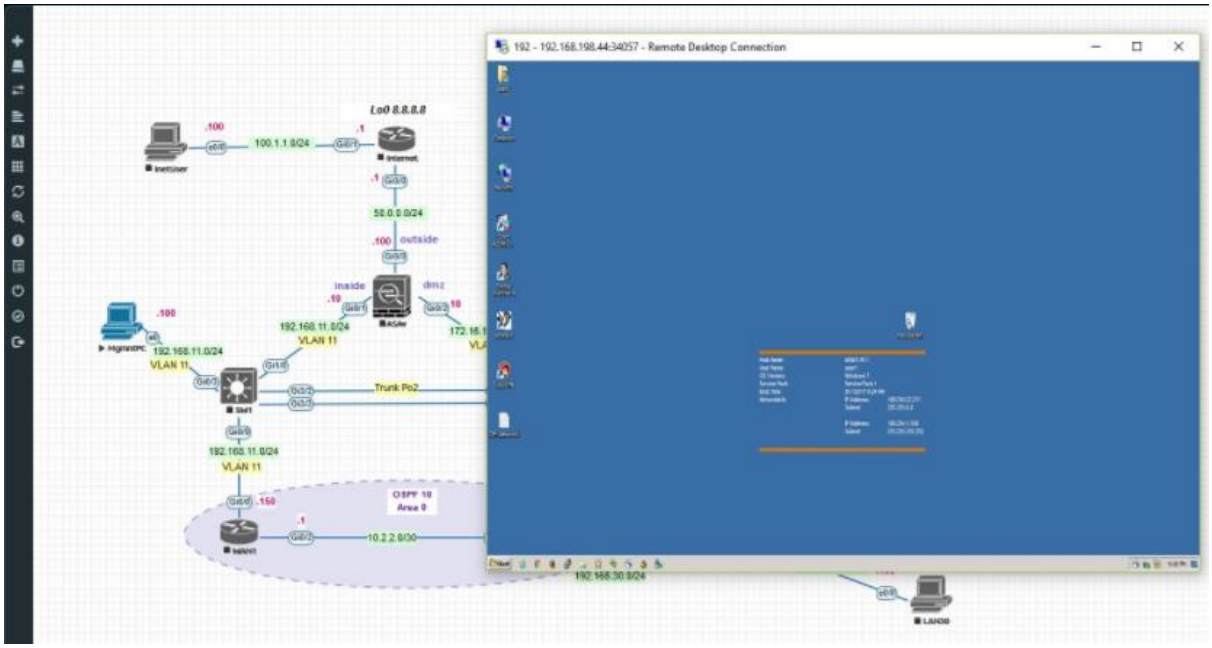

Figura 38. Entorno de emulación eve-NG

Fuente. eve-ng.net

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe