PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ESTUDIO DEL DESEMPEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN MPLS-VPN SOBRE MÚLTIPLES SISTEMAS AUTÓNOMOS

Tesis para optar el Título de Ingeniero de las Telecomunicaciones, que presenta el bachiller:

Ricardo Armando Menéndez Avila

ASESOR: Mg. Antonio Ocampo Zúñiga

Lima, agosto de 2012

Resumen

La presente tesis consiste en proporcionar una propuesta técnica para la implementación de una red MPLS-VPN sobre Múltiples Sistemas Autónomos (Multi Autonomous System VPN), a través de un estudio del desempeño de cuatro diferentes modelos de implementación para brindar dicha solución.

Durante el desarrollo de la tesis se presenta el marco teórico que permite conocer y entender tanto las redes VPN como las arquitecturas involucradas en su funcionamiento, principalmente la tecnología MPLS. Posteriormente se explica el porqué es necesario contemplar una solución soportada en más de un sistema autónomo. A continuación se presentan los distintos modelos de red para la implementación de las VPN Multi-AS y se realiza un estudio del desempeño de cada uno de ellos.

Posteriormente se hace un análisis de los resultados obtenidos durante el estudio de cada opción con el fin de conocer las ventajas, desventajas, problemas y las posibles soluciones que ofrecen. Finalmente se elabora una propuesta técnica para la implementación de la red, utilizando el **Modelo de Implementación "Multi Protocol eBGP Multisalto entre Route Reflectors"**, con los procedimientos detallados necesarios, los aspectos económicos y resultados esperados al final del proceso.

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE LAS TELECOMUNICACIONES

Título : Estudio de Desempeño e Implementación de una Solución MPLS-VPN sobre Múltiples Sistemas Autónomos

Área : REDES Y TELEMÁTICA #187

Asesor : Mg. Antonio Ocampo Zúñiga

Alumno : Ricardo Armando Menéndez Avila

Código : 20060227

Fecha : 16 de Julio de 2012

Descripción y Objetivos:

Multiprotocol Label Switching es una tecnología muy empleada dentro las redes backbone de proveedores de servicios de telecomunicaciones. Brinda alta escalabilidad y rapidez en el reenvío de paquetes, por lo que es muy usada para implementar redes privadas virtuales (VPN). Sin embargo, esta arquitectura implica que los clientes estén conectados a un solo proveedor.

Por otro lado, muchas grandes empresas cuentan con sedes en diferentes ciudades o regiones. Es por ello que sus VPNs necesitarían abarcar grandes áreas geográficas, lo puede implicar atravesar redes de múltiples proveedores. Esto crea la necesidad de contar con una solución que permita brindar servicios altamente escalables, que abarquen grandes regiones y sean capaces de integrar a más de un proveedor y sobre todo, que sean seguras.

El objetivo de la presente tesis es realizar un estudio de cuatro tipos de implementación de la solución Multi-AS VPN. Se dará a conocer las ventajas de y desventajas de cada solución mediante pruebas de laboratorio. Se buscará la mejor alternativa y se elaborará una propuesta técnica que garantice la escalabilidad y calidad de servicio que las grandes empresas requieren para sus VPNs.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Especialidad de Ingeniería de las Telecomunicaciones

Ing. LUIS ANGELO VELARDE CRIADO
Coordinador

Mg. Antonio Ocampo Zúñiga

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE LAS TELECOMUNICACIONES

Título : Estudio de Desempeño e Implementación de una Solución MPLS-VPN sobre Múltiples Sistemas Autónomos

Índice:

Máximo: 100 páginas

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Especialidad de Ingeniería de las Telecomunicaciones

Ing. LUIS ANGELO VELARDE CRIADO
Coordinador

Mg. Antonio Ocampo Zúñiga

Dedicatoria

A Alejandrina y
a Angélica.

Agradecimientos

Quiero agradecer a Dios por todas las personas y experiencias que puso en mi camino a lo largo de todo este tiempo en la universidad.

A mis padres y hermana, por haber confiado en mí como nadie y por haberme dado mucho de lo que soy hoy en día.

Al Magíster Antonio Ocampo, por haber aceptado asesorarme en este proyecto y por sus consejos y ayuda dentro y fuera de él.

A mis amigos de la carrera, porque con ellos se quedan los mejores momentos que pasé en la universidad, y porque entre broma y broma siempre hubieron palabras que motivaron el esfuerzo para desarrollar esta Tesis.

Por último, a todas las personas que en algún momento han ayudado de una u otra manera a que logre este objetivo de ser profesional.

Índice

Lista de Figuras

Lista de Tablas

Introducción

El crecimiento sostenido y cada vez más acelerado de Internet ha despertado un gran interés por los mecanismos de transporte de datos y sus diferentes aplicaciones, entre los que se encuentran las Redes Privadas Virtuales o VPNs (Virtual Private Networks). Para hacer posible su despliegue, tecnologías como MPLS (Multi Protocol Label Switching) han tenido gran aceptación debido a sus múltiples ventajas y características que la han convertido en la tecnología ideal para muchas grandes empresas. Las soluciones MPLS-VPN, además de proporcionar escalabilidad, permiten dividir una gran red en pequeñas redes separadas, lo cual es muchas veces necesario en grandes compañías, donde la infraestructura tecnológica debe ofrecer redes aisladas a áreas individuales.

Sin embargo, al igual que con el Internet, las empresas crecen junto con sus necesidades. Dichas necesidades incluyen la conectividad privada a grandes distancias, o conectividad con más de un proveedor a la vez. Por otro lado, muchos proveedores de servicios que han implementado MPLS-VPNs por años ahora apuntan a la interconexión de su red con las redes MPLS-VPN de otros proveedores para mejorar la escalabilidad y facilidad de operación de su red. Esto implica que muchas veces existirán VPNs que deban abarcar más de un sistema autónomo. Es ante esta problemática que las Inter-AS (Inter Autonomous System) VPNs aparecen como la solución.

Capítulo 1

Fundamento de la Tesis

1.1 Definición del problema y justificación

Los proveedores de servicios de telecomunicaciones buscan constantemente ampliar los alcances de sus redes MPLS. La arquitectura Multi Protocol Label Switching (MPLS) proporciona alta escalabilidad y rapidez en el reenvío de paquetes, siendo su aplicación más empleada las VPNs. Sin embargo, esta arquitectura implica que los clientes de servicios VPN estén conectados a un solo proveedor. Por otro lado, las grandes empresas cuentan generalmente con sedes en diferentes ciudades o regiones, y hacen uso de los servicios VPN para poder interconectar sus sedes.

A medida que las empresas crecen, los requerimientos de sus VPNs aumentan. Se hace necesario abarcar diferentes áreas geográficas, muchas veces cruzando más de un país. Inclusive, algunas VPNs necesitan extenderse a través de múltiples proveedores de servicios VPN.

Independientemente de la complejidad que implique este tipo de necesidad, las conexiones que se hagan deben ser totalmente transparentes de cara al cliente. Por ello, es necesario contar con una solución que permita brindar de forma eficiente servicios

VPN altamente escalables, que abarque grandes regiones, que sea capaz de integrar a más de un proveedor y sobre todo, que sea segura.

La presente tesis desarrollará un estudio de cuatro tipos de implementación de la solución Multi-AS VPN. Se buscará brindar la mejor alternativa y que garantice la escalabilidad y calidad de servicio que las grandes empresas requieren para sus VPNs.

1.2 Mercado Actual

Dentro de rubro de las telecomunicaciones, los servicios VPN han tenido un crecimiento constante tanto en el Perú como en el mundo. La figura 1-1 muestra estadísticas de los servicios MPLS-VPN de un operador mayorista de telecomunicaciones, dentro de Latinoamérica, a Junio de 2012.

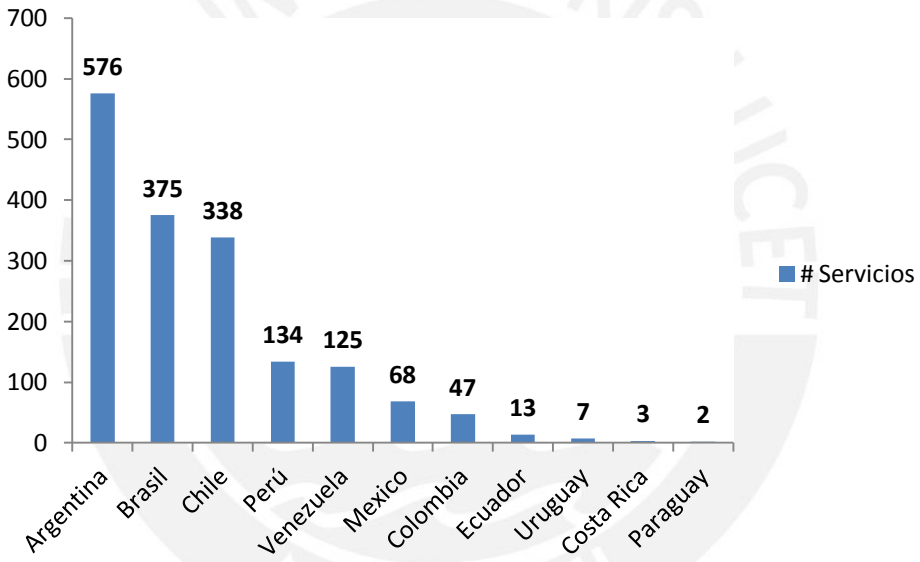

FIGURA 1-1 SERVICIOS MPLS-VPN EN LATINOAMERICA

Fuente: “Información Corporativa” [MAY2012]

Argentina, Brasil y Chile son los países donde el operador tiene mayor cantidad de circuitos MPLS-VPN implementados. Estas estadísticas se refieren al país del cliente que contrata el servicio, y no considera el país destino donde que cliente desea la conectividad. Muchos de estos servicios son contratados por un mismo cliente, por lo que es importante observar también el número de clientes del operador por país, que se detalla en la figura 1-2.

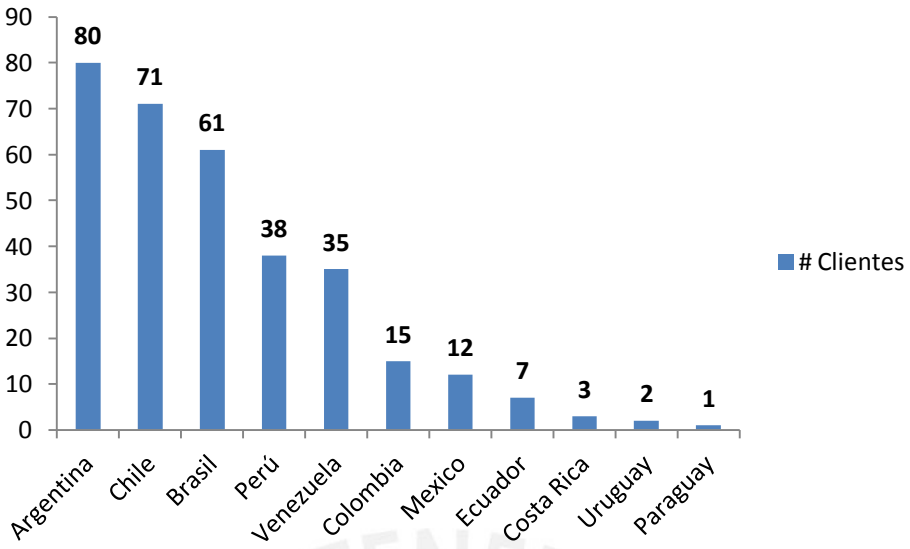

FIGURA 1-2 CLIENTES MPLS-VPN EN LATINOAMERICA

Fuente: "Información Corporativa" [MAY2012]

1.3 Crecimiento del mercado de servicios MPLS-VPN en el Perú

De acuerdo a las estadísticas mostradas, el Perú es el cuarto país en número de servicios y en número de clientes. Este número ha ido en aumento desde el año 2005, en el que el operador brinda el primer servicio MPLS-VPN en el país. Desde entonces, se ha tenido un crecimiento constante que se detalla en la figura 1-3.

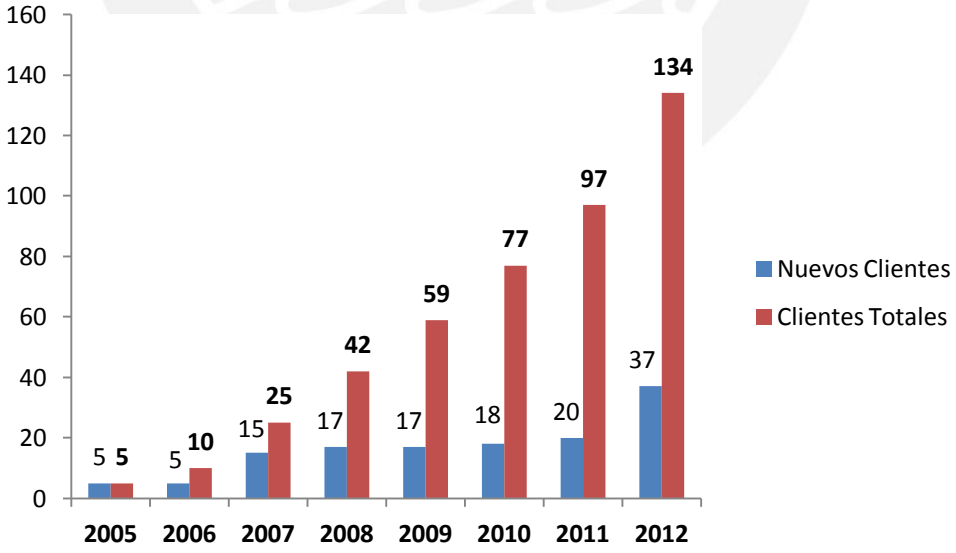

FIGURA 1-3 CLIENTES MPLS-VPN EN EL PERÚ

Fuente: "Información Corporativa" [MAY2012]

A partir de la figura 1-3 se ha obtenido una proyección al año 2017 mostrada en la figura 1-4, considerando que la tendencia del aumento de clientes y de los servicios contratados por éstos seguirá como ha sido hasta el momento.

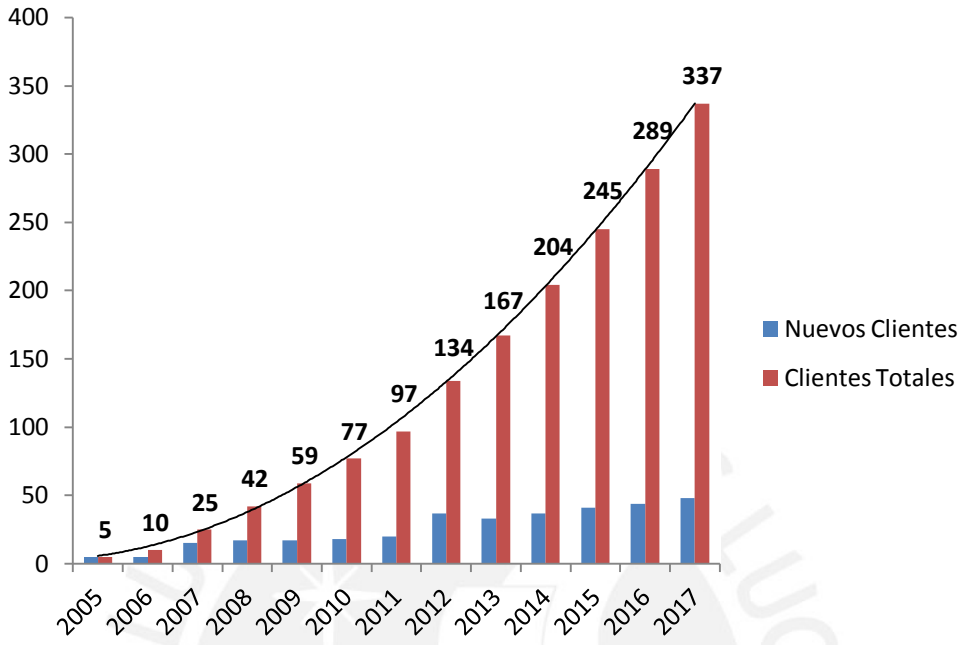

FIGURA 1-4 PROYECCIÓN DEL CRECIMIENTO DEL MERCADO MPLS-VPN EN EL PERÚ
Fuente: "Información Corporativa" [MAY2012]

Ante esta tendencia, se hace necesaria la implementación de redes capaces de soportar el aumento sostenido de clientes. Esto no supone necesariamente una renovación constante de infraestructura de red, sino que implica un desafío de diseño de la arquitectura dentro del backbone de los operadores que brinden este servicio. El presente trabajo busca dar una solución a estos requerimientos.

1.4 Objetivos de la tesis

La descripción mostrada anteriormente permite plantear los siguientes objetivos para el desarrollo de la tesis:

- Estudio de las redes MPLS-VPN, su arquitectura y protocolos asociados así como la comparación de los modelos de red que existen para su implementación.
- Brindar una propuesta técnica para la implementación de una red MPLS-VPN sobre Múltiples Sistemas Autónomos (Multi Autonomous System VPN), basado en un estudio del desempeño de cuatro modelos de red que serán implementados.

- Comprender la necesidad de utilizar este tipo de redes para brindar servicios de redes privadas virtuales a clientes corporativos.
- Conocer las ventajas que la solución propuesta brinda para la optimización de redes MPLS-VPN.

1.5 Estructura de la tesis

La presente tesis está compuesta por los cinco capítulos que a continuación se describen:

En el capítulo 1, se describe la situación actual de los servicios MPLS-VPN, la necesidad de realizar un estudio y los objetivos del trabajo.

Seguidamente, en el capítulo 2, se realiza el estudio de las redes MPLS-VPN tanto en su arquitectura así como los protocolos y tecnologías que las conforman.

A continuación, en el capítulo 3 se presentan los cuatro tipos de redes que serán implementados y sometidos a pruebas en el laboratorio.

Posteriormente, en el capítulo 4 se describe las implementaciones realizadas y se presentan los resultados de las pruebas de laboratorio.

Finalmente, en el capítulo 5 se determina la solución final y se elabora la propuesta técnica con los procedimientos, plazos y aspectos económicos necesarios.

Capítulo 2

Marco Teórico

2.1 VPNs

2.1.1 Definición

Una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios [GHE2006]. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas. La figura 2-1 muestra un esquema básico de una VPN [LIM2004] [GHE2006].

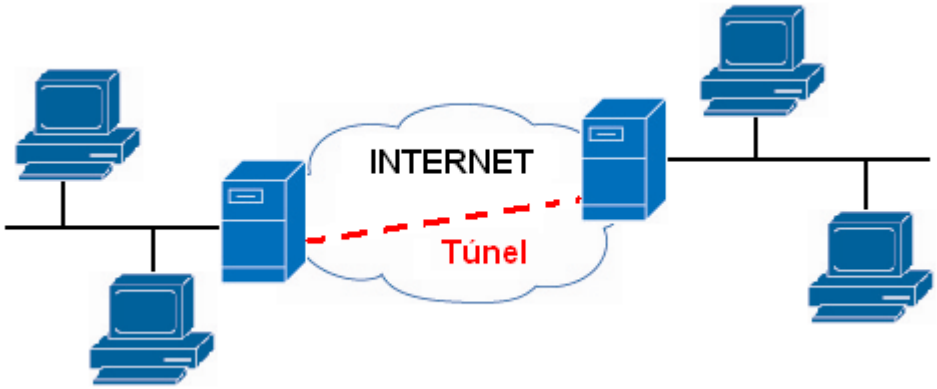

FIGURA 2-1 ESTRUCTURA DE UNA RED PRIVADA VIRTUAL

Fuente: “Estructura de una Red Privada Virtual” [LIM2004]

El equivalente lógico a esta red VPN sería un enlace privado punto a punto (peer-to-peer), que es sumamente costoso si se trata de extender la red a grandes distancias, debido al requerimiento de cableado y equipos en la localidad a la cual se quiera llegar [LIM2004].

2.1.2 Razones para implementar una VPN

Reducción de Costos

Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso ADSL. Es de bajo costo, brinda un ancho de banda alto y está disponible en la mayoría de zonas urbanas. Los usuarios remotos móviles podrán ahorrar costos de llamadas telefónicas de larga distancia, realizándolas a través de un acceso local a Internet [LIM2004].

Alta Seguridad

Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, comparables con una red punto a punto. Protocolos como 3DES (Triple data encryption standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema. También se emplean varios niveles de autenticación para el acceso a la red privada mediante llaves de acceso, para validar la identidad del usuario [LIM2004].

Escalabilidad

No es necesario realizar inversiones adicionales para agregar usuarios a la red. El servicio se provee con dispositivos y equipos configurables y manejables. La desarrollada infraestructura de los proveedores de Internet hace innecesario realizar un enlace físico que puede significar una gran inversión de dinero y de tiempo [LIM2004].

Compatibilidad con tecnologías de banda ancha

Una VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN. Con ello brinda un alto grado de flexibilidad al momento de configurar la red. Se pueden emplear tecnologías como Voz sobre IP (VoIP), que permiten ahorrar en telefonía de larga distancia [LIM2004].

Mayor Productividad

Una VPN da un nivel de acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la RED. Además, con la consecutiva reducción en las necesidades de espacio físico, se fomenta el teletrabajo [LIM2004].

2.1.3 VPNs según necesidades empresariales

Una empresa u organización normalmente implementa una VPN para satisfacer las necesidades de comunicación dentro de la organización (intranet), comunicación con otras organizaciones (extranet) y acceso de usuarios desde dispositivos móviles, computadoras en casa u oficinas remotas [PEP2002].

Las soluciones que cubren estas necesidades abarcan la gran mayoría de topologías y tecnologías que los proveedores de servicios VPN ofrecen. La diferencia se encuentra en el nivel de seguridad que maneja cada tipo de implementación [PEP2002].

En el caso de la intranet, el tráfico enviado suele no estar bien protegido por los hosts finales o los firewalls con los que cuenten. Por lo tanto, la solución VPN para este tipo de comunicación debe ofrecer altos niveles de aislamiento y seguridad. Además, el servicio debe contar con calidad de servicio (QoS) garantizada para procesos críticos [PEP2002].

Por dichas razones, una organización no suele optar por utilizar la red de Internet, pues no se puede contar con calidad de servicio de extremo a extremo, aislamiento o seguridad que las conexiones dentro de la empresa requieren [PEP2002].

Por otro lado, las conexiones con otras empresas (extranet) generalmente se encuentran entre locales centrales de las organizaciones, para las cuales se usan dispositivos de seguridad dedicados, como firewalls o equipos de encriptación. Se muestra un ejemplo en la figura 2-2. Estas conexiones no suelen contar con requerimientos rigurosos de calidad de servicio, por lo que son adecuadas para montar en ellas la comunicación. Por ello, el tráfico entre empresas se envía mayormente a través de Internet [PEP2002].

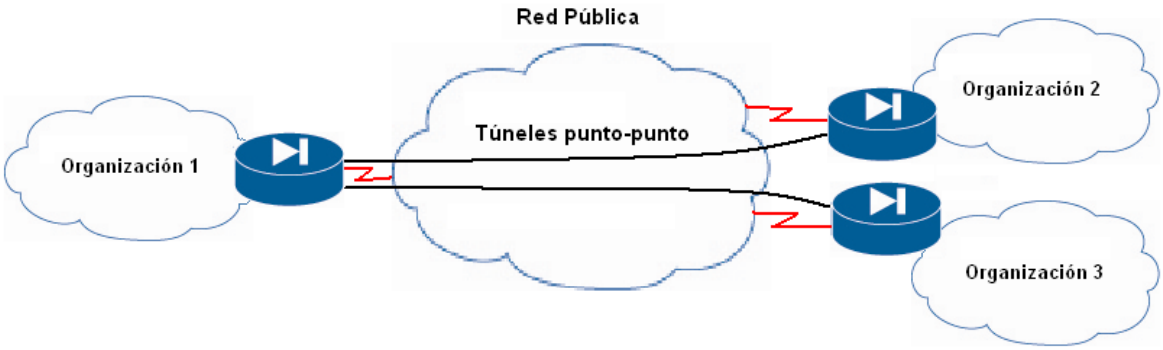

FIGURA 2-2 MODELO DE RED EXTRANET

Fuente: "Typical Extranet Setup" [PEP2002]

Los usuarios remotos acceden a la red corporativa desde ubicaciones desconocidas y no fijas. Esto produce problemas de seguridad entre los extremos del enlace, que se resuelven aplicando tecnologías de encriptación o contraseñas de un solo uso. Por lo tanto, el nivel de seguridad requerido para estas redes, llamadas VPDN (Virtual Private Dial-up Network), es significativamente menor que para redes Intranet. Actualmente, la mayoría de servicios VPDN son implementados sobre IP, ya sea a través de Internet o a través del backbone de un proveedor [PEP2002]. Se ilustra un ejemplo en la figura 2-3.

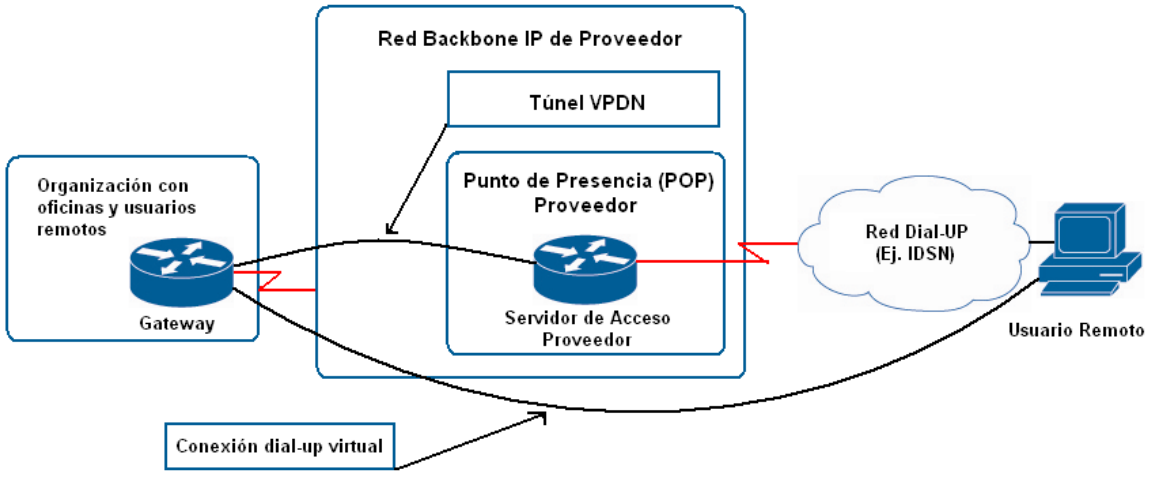

FIGURA 2-3 RED VPDN A TRAVÉS DE UN BACKBONE DE PROVEEDOR

Fuente: "Service Provider Offering Separate VPDN Backbone" [PEP2002]

A continuación se detalla la terminología empleada en un contexto VPDN [PEP2002]:

- Servidor de Acceso a Red (Network Access Server NAS): Es el servidor remoto administrado por el proveedor que acepta la llamada del cliente, realiza la autenticación inicial, y reenvía la llamada a la puerta de enlace del cliente.

- Puerta de enlace del cliente (Home Gateway): Es un router administrado por el cliente que acepta la llamada reenviada por el NAS, realiza una autenticación y autorización adicional, y finaliza la sesión desde el lado del usuario de la conexión dial-up. Los parámetros de la sesión (como direcciones IP) son negociados entre el usuario y el Home Gateway. El servidor NAS envía las tramas entre ambos.

2.1.4 Primeras Arquitecturas VPN

2.1.4.1 Modelo Overlay VPN

Las primeras VPNs se implementaron basadas en tecnologías como Frame Relay o ATM, donde el proveedor brinda conectividad a nivel de Capa 2 a los routers del cliente. Éste modelo era el llamado *Modelo Overlay.* El proveedor es el dueño de los routers de borde (Edge Routers) que se conectan a la red del cliente, o los administra. La idea es tener a los routers físicamente en el local del cliente [GHE2006].

Este modelo es sencillo de entender pues separa claramente las responsabilidades del cliente y del proveedor. El proveedor brinda al cliente un grupo de líneas dedicadas virtuales (emuladas), llamadas VCs, que pueden estar constantemente disponibles (PVCs) o ser establecidas bajo demanda (SVCs) [PEP2002].

La figura 2-4 muestra la topología de una VPN tipo Overlay y las VCs utilizadas en ella.

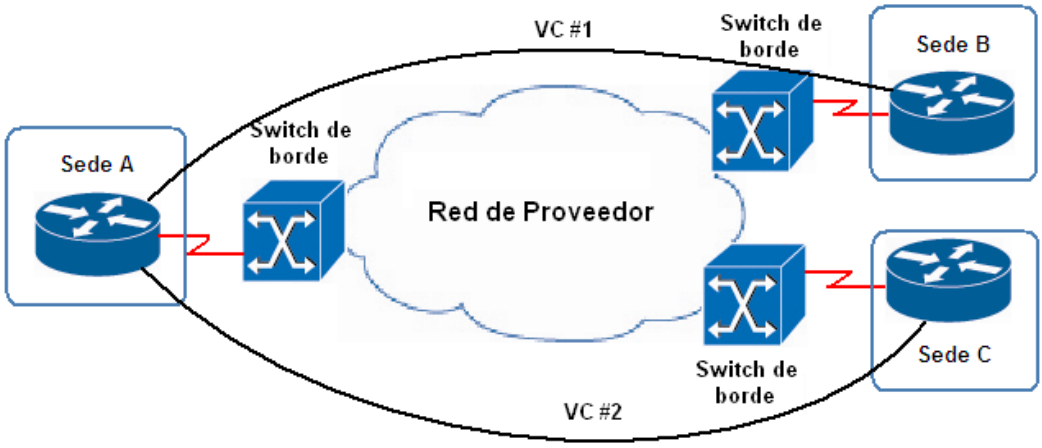

FIGURA 2-4 RED OVERLAY VPN

Fuente: "Sample Overlay VPN Network" [PEP2002]

El cliente establece una comunicación de router a router entre los equipos de cliente o *Customer Premises Equipment* (CPE) a través de las VCs. Los datos del protocolo de enrutamiento son intercambiados entre los CPE, y el proveedor no tiene conocimiento alguno de la estructura interna de la red del cliente. La figura 2-5 muestra la topología de enrutamiento de la red VPN de la figura 2-4 [PEP2002].

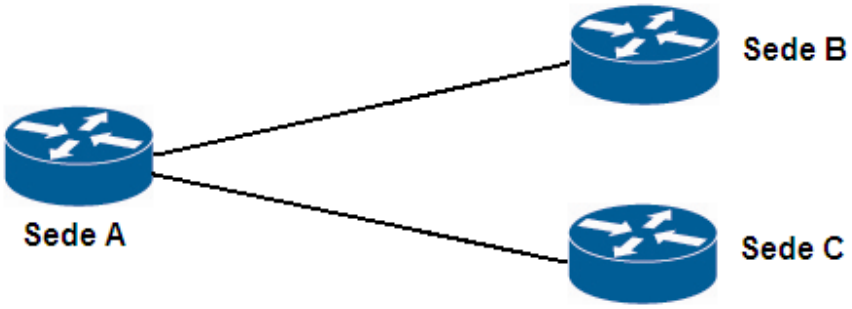

FIGURA 2-5 ENRUTAMIENTO EN UNA RED OVERLAY VPN

Fuente: "Routing in Sample Overlay VPN Network" [PEP2002]

2.1.4.2 Modelo Peer-to-peer VPN

El modelo Peer-to-peer también fue utilizado inicialmente, aunque no fue tan popular. La razón principal es que no es tan fácil de desplegar y mantener debido a que necesita listas de distribución, filtros de paquetes IP, o túneles GRE [GHE2006].

Este modelo fue introducido para contrarrestar las desventajas del modelo Overlay. En las VPNs peer-to-peer, el equipo de borde del proveedor o *Provider Edge* (PE) es un router que intercambia las rutas directamente con el router CPE [PEP2002]. La figura 2-6 muestra un ejemplo de VPN peer-to-peer equivalente a la VPN de la figura 2-4.

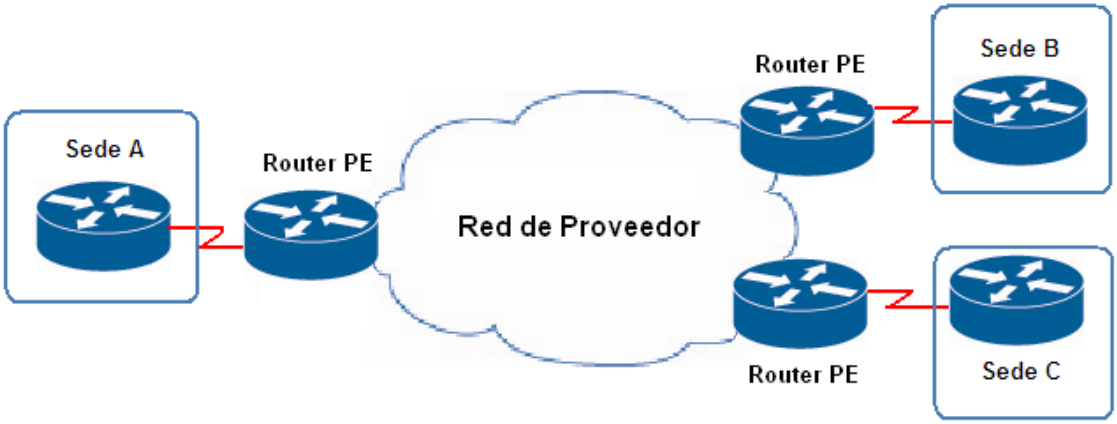

FIGURA 2-6 MODELO PEER-TO-PEER VPN

Fuente: "Sample Peer-to-peer VPN" [PEP2002]

La tabla 2-1 muestra una comparación entre ambos esquemas.

TABLA 2-1 COMPARACIÓN ENTRE OVERLAY Y PEER-TO-PEER

Fuente: [PEP2002] [LAV2010]

Modelo Overlay (Backbone Frame-Relay/ATM)	Modelo Peer-to-Peer (Backbone IP)
Conmutación veloz de tramas en el backbone (capa 2)	Velocidad de conmutación de paquetes dependiente de plataforma.
Total independencia entre redes de clientes (VPN en capa 2)	Redes de clientes sujetas a compartir una misma tabla de rutas
Puede transportar cualquier protocolo de capa 3.	Cualquier otro protocolo a transportar debe pasar encapsulado en paquetes IP
Esquema de QoS limitado, versatilidad adicional depende del protocolo de capa 3 utilizado	Esquema de QoS para aplicaciones basado en marcación de paquetes o reserva de ancho de banda
Cada cliente nuevo implica la creación de circuitos nuevos (PVCs) en el backbone (Más configuración en más equipos)	Cada cliente nuevo sólo implica la creación del circuito de acceso y del enrutamiento
Utilización no óptima de troncales FR/ATM	Troncales IP con dimensionamiento óptimo
Utilización no óptima de acceso central en esquemas hub & spoke	Utilización óptima del ancho de banda en accesos (full-mesh virtual)
Acceso de cliente a servicios en el proveedor implica nuevos circuitos en capa 2	Fácil acceso a servicios en el proveedor (data center) a través de troncales IP existentes
Elección de la mejor ruta hecha en capa 3	Elección de la mejor ruta según protocolo de enrutamiento basado sólo en métricas fijas
Se complica el intercambio de rutas debido a los múltiples vecinos del CPE	Enrutamiento simple para el cliente, ya que el CPE intercambia rutas con uno o pocos PE
Enrutamiento engorroso entre los locales del cliente	Enrutamiento óptimo entre las sedes del cliente, pues los PE conocen su topología de red
Para asignar ancho de banda, el cliente debe especificar el perfil de tráfico exacto de local a local	El cliente de especificar el ancho de banda inbound y outbound sólo para cada local

2.2 MPLS

2.2.1 Definición

Multi Protocol Label Switching es una tecnología de encapsulamiento que trabaja entre las capas 2 y 3 del modelo OSI. Acelera el transporte de paquetes IP, reemplazando el enrutamiento basado en las direcciones de capa 3 por una conmutación basada en etiquetas [LAV2010]. Para ello, se inserta entre las cabeceras de los protocolos capa 2 y capa 3 la cabecera de 32 bits mostrada en la figura 2-7 [GAR2009].

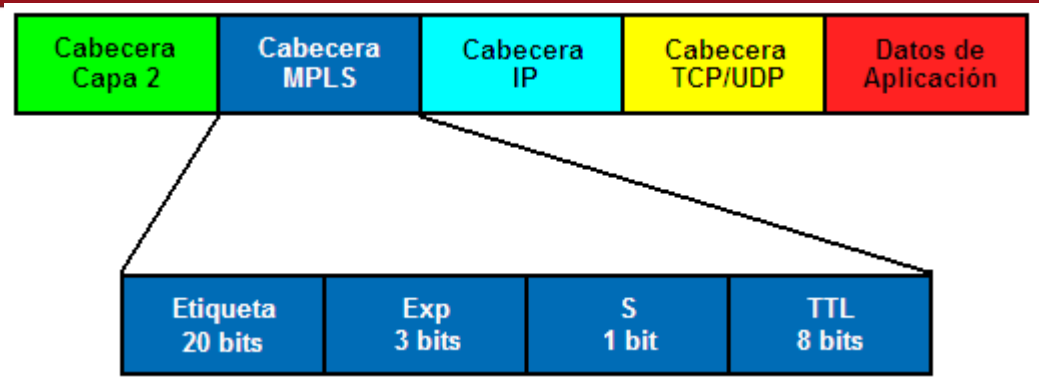

FIGURA 2-7 PAQUETE CON ETIQUETA MPLS

Fuente: "Cabecera MPLS" [GAR2009]

2.2.2 Principales ventajas de MPLS

Entre las ventajas de la tecnología MPLS se pueden resaltar [LAV2010]:

- Conmutación rápida de paquetes basado en etiquetas y no direcciones IP destino.
- Redes de clientes totalmente independientes (MPLS-VPN).
- Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
- Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
- La creación de una nueva VPN sólo implica la creación del circuito de acceso y del enrutamiento.
- Permite aplicar Ingeniería de Tráfico (TE).
- Uso eficiente del ancho de banda en accesos (full-mesh virtual).

2.2.3 Esquema básico de funcionamiento

Para poder entender el funcionamiento de MPLS, se deben tener claros los términos que describen su arquitectura.

2.2.3.1 Términos principales utilizados en MPLS

- LSR (Label Swtiching Router): Nodo interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos [GAR2009].
- Edge LSR (Edge Label Switch Router) o LER (Label Edge Router): Nodo de borde que maneja tráfico entrante y saliente de la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida la extrae y enruta según la capa de Red [GAR2009].

- LDP (Label Distribution Protocol): Protocolo que establece sesiones TCP entre LSR/LERs para intercambiar las etiquetas que estos utilizarán para la conmutación de paquetes [LAV2010].
- TDP (Tag Distribution Protocol): Protocolo similar a LDP, propietario de Cisco.
- LIB (Label Information Base): Base de datos formada en un LSR/LER que contiene información de etiquetas e interfaces asociadas a las redes destino [LAV2010].
- FEC (Forwarding Equivalence Class): Es una clase que agrupa un conjunto de paquetes que se enviarán en base a una característica común (dirección destino, clase QoS, etc). Los paquetes que pertenezcan al mismo FEC, usarán el mismo camino a lo largo de toda la red MPLS y la misma etiqueta de salida [LAV2010].
- LSP (Label Switched Path): Camino unidireccional definido con QoS y formado por una secuencia de LSRs sobre el cual se envían los paquetes que pertenecen al mismo FEC [LAV2010] [GAR2009].
- Traffic Engineering (TE): Proceso de control de flujo de tráfico a través de la red, que optimiza el uso de recursos con el objetivo de mejorar su rendimiento [GAR2009].

2.2.3.2 Modo de operación

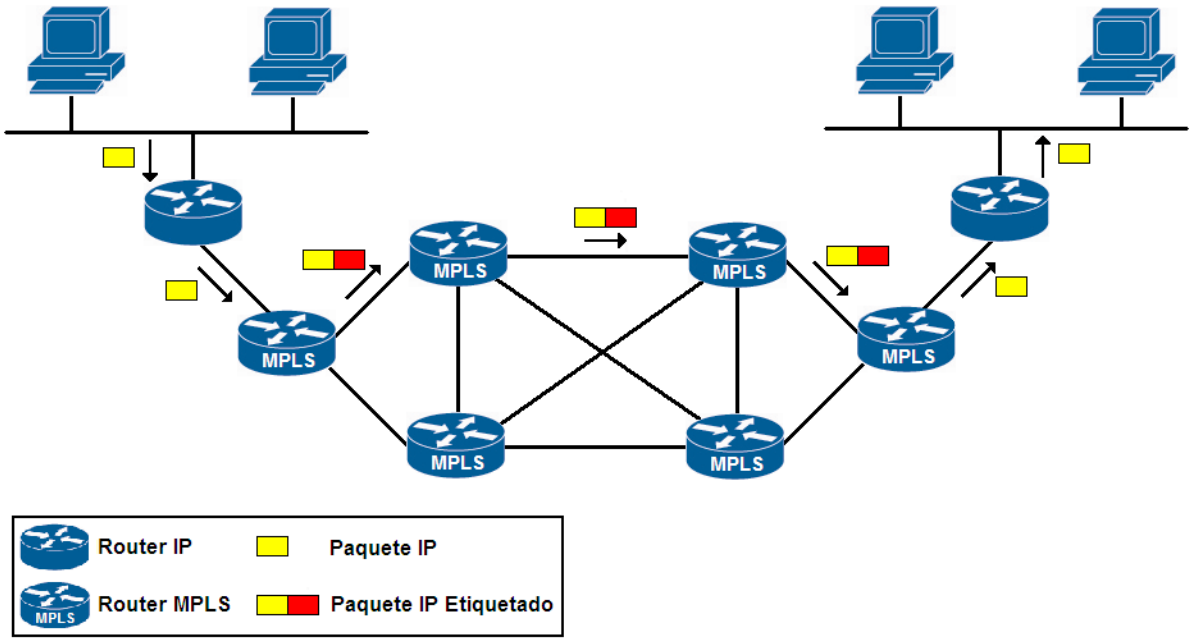

FIGURA 2-8 OPERACIÓN MPLS

Fuente: “Esquema de funcionamiento MPLS” [MOR2006]

Primero, se establece un LSP entre los routers que van a transmitir el tráfico FEC. Los LSPs hacen las veces de túneles de transporte e incluyen los parámetros QoS específicos del flujo, que sirven para determinar la cantidad de recursos a reservar para el LSP y las políticas de desechado y la cola de procesos en cada LSR [MOR2006].

Para intercambiar información los routers MPLS usan los protocolos LDP o TDP. Cada flujo de tráfico FEC es asignado a una etiqueta particular. La asignación de nombres y rutas se puede realizar manualmente o bien a través del protocolo empleado [MOR2006].

Cuando un paquete ingresa al dominio MPLS, el Edge LSR determina los servicios de red que requiere. Luego, asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router de borde trabaja en conjunto con los demás LSRs para definirlo. Una vez dentro del dominio MPLS, en cada LSR que recibe el paquete se llevan a cabo los siguientes procesos [MOR2006]:

- Se retira la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
- Se envía el paquete al siguiente LSR dentro del LSP.

Finalmente, El LSR de salida “abre” la etiqueta y lee el encabezado IP para enviarlo a su destino final [MOR2006].

2.2.4 Arquitectura MPLS

A continuación de describen los principales elementos que conforman una red MPLS.

2.2.4.1 Componentes lógicos

La arquitectura MPLS comprende 2 componentes lógicos principales [LAV2010]:

- Plano de Control (control plane): Hace el intercambio de etiquetas y rutas en capa 3.
- Plano de Datos (data plane): Reenvía los paquetes basado en las etiquetas.

2.2.4.2 Componentes físicos

Un término muy importante en MPLS es el Label Switch Router (LSR). Cualquier router o switch que implemente procedimientos de distribución de etiquetas y pueda enviar paquetes basándose en etiquetas se encuentra en esta categoría. Los diferentes tipos de LSR pueden ser descritos dependiendo de la arquitectura donde se encuentren como Edge-LSRs (LSRs de borde), ATM-LSRs, y ATM Edge-LSRs [PEP2002].

Un Edge-LSR es un router que realiza ya sea *label imposition* (o push action) o *label disposition* (o pop action) en el borde de la red MPLS. *Label imposition* es el acto de anteponer etiquetas a un paquete en el punto donde ingresa al dominio MPLS. *Label disposition*, por otro lado, es el acto de remover la última etiqueta de un paquete en el punto de salida para luego enviarlo a un vecino fuera del dominio MPLS [PEP2002].

Cualquier LSR que tenga vecinos que no tienen implementado MPLS es considerado un Edge-LSR. Sin embargo, si ese LSR tiene interfaces que se conectan a un ATM-LSR a través de MPLS, también se considera un ATM Edge-LSR. Los Edge-LSRs usan una tabla de reenvío IP tradicional con la información adicional de etiquetado, para poder etiquetar y desetiquetar los paquetes [PEP2002].

Un ATM-LSR es un switch ATM que puede actuar como un LSR. El ATM-LSR realiza enrutamiento IP y asignación de etiquetas en el plano de control y reenvía los paquetes utilizando mecanismos de conmutación ATM tradicional (ATM cell switching) en el plano de datos. En otras palabras, la matriz de conmutación de un switch ATM es utilizada como una tabla de reenvío de un nodo MPLS. Lo switches ATM tradicionales, pueden ser reasignados como ATM-LSRs a través de una actualización del software de su componente de control [PEP2002].

La tabla 2-2 resume las funciones que realizan los diferentes tipos de LSRs. Es importante notar que cualquier dispositivo en la red puede realizar más de una función. (Por ejemplo, puede ser un Edge-LSR y ATM Edge-LSR al mismo tiempo) [PEP2002].

TABLA 2-2 ACCIONES QUE REALIZAN LOS TIPOS DE LSR

Fuente: “Actions Performed by Various LSR Types” [PEP2002]

Tipo de LSR	Acciones que realiza
LSR	Reenvía paquetes etiquetados.
Edge-LSR	Recibe un paquete IP, realiza el análisis de capa 3 e inserta la etiqueta antes de reenviar el paquete.
	Recibe un paquete etiquetado, remueve la etiqueta, realiza el análisis de capa 3, y reenvía el paquete IP.
ATM-LSR	Ejecuta protocolos MPLS en el plano de control para implementar circuitos ATM virtuales. Reenvía paquetes etiquetados como ATM cells.
ATM edge-LSR	Recibe un paquete etiquetado o no etiquetado, lo segmenta en ATM cells y los reenvia.
	Recibe los ATM cells desde un ATM-LSR adyacente, los rearma en el paquete original y lo reenvia como un paquete etiquetado o no etiquetado.

2.2.4.3 Tipos de encapsulamiento MPLS

MPLS presenta dos modos de encapsulamiento:

- **Modo trama (frame-mode)**: Los LSR son routers conectados por cualquier enlace de capa 2 (Ethernet, FR, ATM, PPP, etc) [LAV2010].

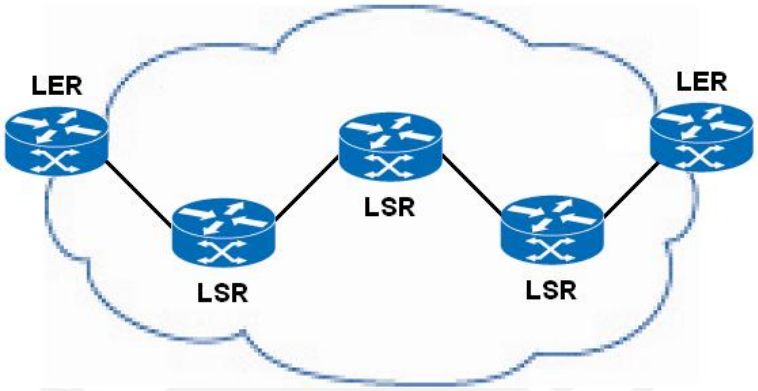

FIGURA 2-9 ESQUEMA MODO TRAMA

Fuente: "Frame Mode" [LAV2010]

Se inserta un campo de 32 bits denominado 'Shim Header' que contiene la etiqueta, 3 bits experimentales (QoS), 1 bit 'S' que permite agregar más de una etiqueta en una trama y 8 bits para tiempo de vida del paquete o TTL (Time-to-live - similar a IP) [LAV2010].

- **Modo celda (cell-mode):** Los LSR son Switches ATM, que conectan los routers de cliente [LAV2010].

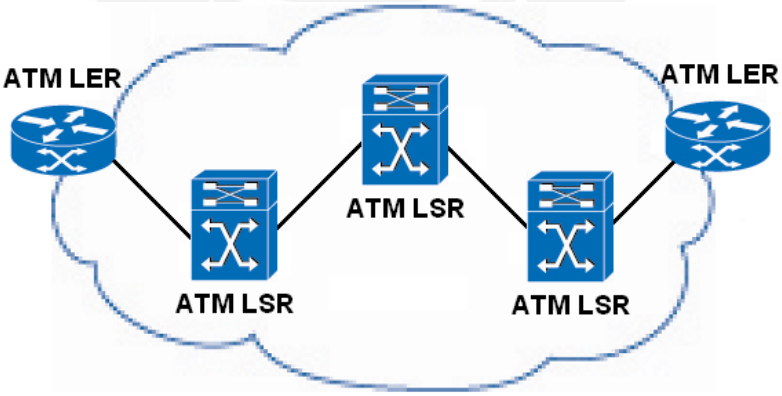

FIGURA 2-10 ESQUEMA MODO CELDA

Fuente: "Cell Mode" [LAV2010]

La etiqueta usada es el VPI/VCI del PVC, los demás campos se insertan en forma similar a la encapsulación genérica [LAV2010].

2.2.4.4 Etiquetado en el borde de la red

El encapsulamiento previamente descrito es una función de borde, que implica que los paquetes sean etiquetados antes de ser reenviados a través del dominio MPLS [PEP2002].

Para realizar esta función, un Edge-LSR necesita entender hacia dónde va el paquete y qué etiqueta, o pila de etiquetas, debe asignar al paquete. En el reenvío convencional de paquetes IP, en cada salto dentro de la red se busca en la tabla de reenvío la dirección IP destino que se encuentra en la cabecera de Capa 3 del paquete. Se selecciona una dirección IP como siguiente salto en cada iteración de la búsqueda y finalmente envía el paquete por una interface a su destino final [PEP2002].

El proceso de escoger el siguiente salto para el paquete IP consiste en dos funciones. La primera particiona todo el conjunto de paquetes posibles en un conjunto de prefijos destino. La segunda mapea cada prefijo IP destino con una dirección IP de siguiente salto. Esto significa que cada destino en la red es alcanzable por una ruta en lo que respecta a flujo de tráfico desde un dispositivo de ingreso hacia un dispositivo de destino (Múltiples caminos pueden estar disponibles si el balanceo de carga es realizado usando rutas de igual costo o de diferente costo, como ocurre con los protocolos IGP) [PEP2002].

Los resultados de la primera función vienen a ser las FECs. Una FEC puede corresponder a una subred IP destino pero también puede corresponder a cualquier clase de tráfico que el Edge-LSR considere significativo. Por ejemplo, todo el tráfico interactivo hacia cierto destino o todo el tráfico con un cierto valor de prioridad IP pueden conformar una FEC. Puede ser inclusive un subconjunto de la tabla BGP, incluyendo todos los prefijos de destino alcanzables a través del mismo punto de salida [PEP2002].

En el reenvío IP convencional, el procesamiento de paquetes se realiza en cada salto dentro de la red. En cambio, en MPLS un paquete individual es asignado a una FEC particular solo una vez en el dispositivo de borde cuando el paquete entra a la red. Luego se codifica la FEC en un identificador corto de longitud fija, que viene a ser la etiqueta [PEP2002].

Cuando el paquete es reenviado hacia su siguiente salto, se antepone la etiqueta al paquete IP para que el siguiente dispositivo en la ruta pueda reenviarlo basándose en la etiqueta codificada en lugar de analizar la información de la cabecera de capa 3. En la figura 2-11 se ilustra mejor el proceso [PEP2002].

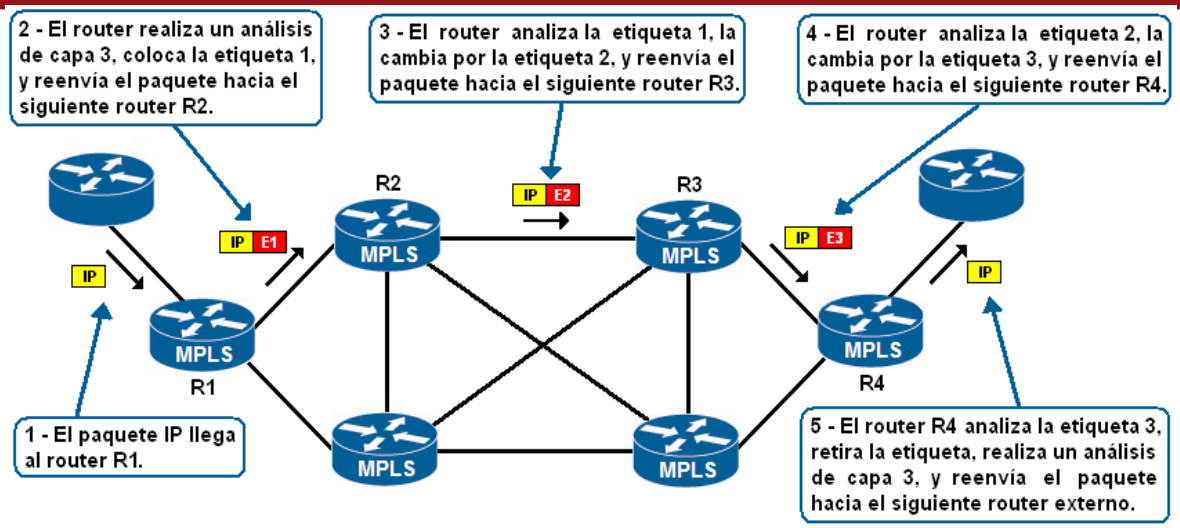

FIGURA 2-11 ETIQUETADO Y REENVÍO MPLS

Fuente: "MPLS Label Imposition and Forwarding" [PEP2002]

2.2.4.5 Reenvío de paquetes MPLS y LSPs (Label Switched Paths)

Se definió previamente un Label Switched Path (LSP) como el conjunto de LSRs que un paquete etiquetado debe atravesar para alcanzar el LSR de salida para una FEC particular. Al ser unidireccional, se utiliza un FEC diferente para el tráfico de retorno [PEP2002].

La creación del LSP es un esquema orientado a conexión porque la ruta está priorizada antes que cualquier flujo de tráfico. Esto quiere decir que la ruta es creada independientemente de si hay requerimiento de tráfico para ser enviado por ella hacia un conjunto particular de FECs [PEP2002].

Mientras el paquete atraviesa la red MPLS, cada LSR cambia la etiqueta entrante por una saliente, de forma similar al mecanismo usado en ATM donde el VPI/VCI es cambiado a un par VPI/VCI diferente al salir del switch ATM. Esto continúa hasta que el último LSR, conocido como el LSR de egreso, es alcanzado [PEP2002].

Cada LSR tiene dos tablas, que guardan información relevante para el reenvío. La primera, conocida en Cisco IOS como Tag Information Base (TIB) y en términos estándar como Label Information Base (LIB), contiene todas las etiquetas asignadas por el LSR y las asignaciones de éstas etiquetas a etiquetas recibidas de cualquier vecino. Estas asignaciones de etiquetas son distribuidas a través de LDP o TDP [PEP2002].

La segunda tabla, conocida en Cisco IOS como Tag Forwarding Information Base (TFIB) y en términos estándar como Label Forwarding Information Base (LFIB), es usada

durante el enrutamiento de paquetes y mantiene sólo las etiquetas que están siendo utilizadas por el componente de reenvío MPLS. La LFIB vendría a ser el equivalente MPLS de la matriz de conmutación de un switch ATM [PEP2002].

2.2.4.6 Aplicaciones de MPLS

Ya se mencionó que MPLS permite la integración de routers tradicionales y switches ATM en un backbone IP (arquitectura IP+ATM). Sin embargo, su verdadero potencial se encuentra en otras aplicaciones que van desde ingeniería de tráfico hasta Redes Privadas Virtuales punto a punto (peer-to-peer Virtual Private Networks). Todas ellas usan una funcionalidad del plano de control similar al plano de control del enrutamiento IP. La figura 2-12 muestra la interacción entre estas aplicaciones y la matriz de conmutación de etiquetas [PEP2002].

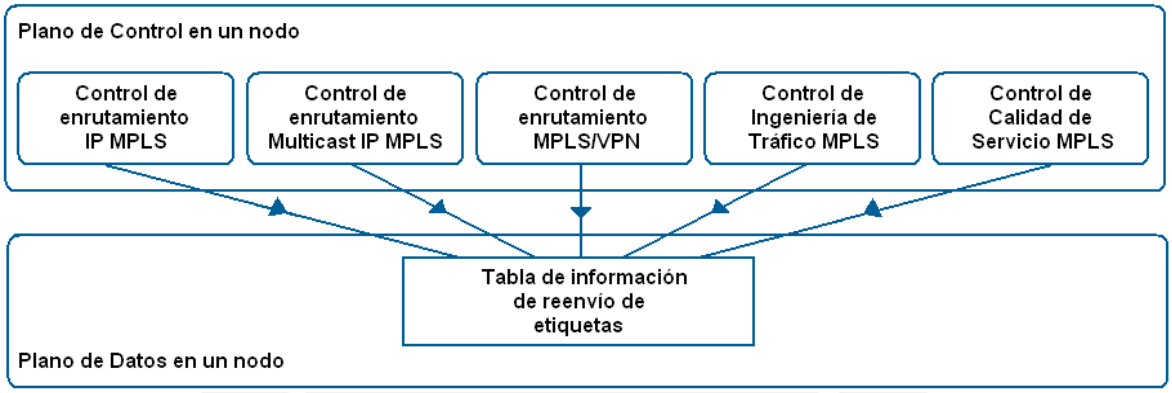

FIGURA 2-12 APLICACIONES MPLS

Fuente: “Various MPLS Applications and Their Interactions” [PEP2002]

Cada aplicación MPLS tiene el mismo conjunto de componentes que una aplicación con enrutamiento IP [PEP2002]:

- Una base de datos que define la tabla FEC para la aplicación (En IP, la tabla de enrutamiento IP).
- Protocolos de control que intercambian el contenido de la tabla FEC entre los LSRs (Protocolos de enrutamiento IP o enrutamiento estático en IP).
- Un proceso de control que realiza el enlazado de etiquetas con las FECs y un protocolo para intercambiar los enlazados de etiquetas entre LSRs (TDP o UDP en una aplicación con enrutamiento IP).
- Opcionalmente, una base de datos interna del trazado FECs-etiquetas (Base de datos con información de etiquetas para el caso de IP).

Cada aplicación usa su propio conjunto de protocolos para intercambiar tablas FEC o trazados FEC-etiquetas entre los nodos. La tabla 2-3 resume dichos protocolos y las estructuras de datos empleados [PEP2002].

TABLA 2-3 PROTOCOLOS DE CONTROL EN APLICACIONES MPLS

Fuente: "Control Protocols Used in Various MPLS Applications" [PEP2002]

Aplicación	Tabla FEC	Protocolo empleado para construir la tabla FEC	Protocolo empleado para intercambiar el trazado FEC-Etiqueta
Enrutamiento IP	Tabla de enrutamiento IP	Cualquier protocolo de enrutamiento IP	Tag Distribution Protocol (TDP) ó Label Distribution Protocol (LDP)
Enrutamiento IP Multicast	Tabla de enrutamiento Multicast	PIM	Extensiones PIM version 2
Enrutamiento VPN	Tabla de enrutamiento Por-VPN	Protocolos de enrutamiento IP entre proveedores y clientes. Multi Protocol BGP dentro de la red del proveedor de servicio.	Multi Protocol BGP
Ingeniería de Tráfico	Definición de túneles MPLS	Definición manual de interfaces, extensiones a IS-IS u OSPF	RSVP ó CR-LDP
Calidad de Servicio MPLS	Tabla de enrutamiento IP	Protocolos de enrutamiento IP	Extensiones a TDP LDP

2.3 MPLS-VPNs

Al inicio del capítulo se describió a las redes VPN y su arquitectura. Posteriormente, se presentó la tecnología MPLS, su funcionamiento y se mencionaron las distintas aplicaciones posibles, entre ellas, las VPNs. A continuación se tratará en detalle esta aplicación, y se presentará el caso del que se ocupa la presente tesis: Inter-AS VPNs.

2.3.1 Introducción a MPLS-VPNs

Una red privada requiere que todos los locales del cliente puedan interconectarse y sean completamente separadas de otras VPNs. Ese es el mínimo requisito de interconectividad que debe cumplirse. Sin embargo, algunos modelos de VPN de Capa 3 pueden requerir más que eso. Deben ser capaces de brindar conectividad entre diferentes VPNs e incluso proveer conexión a Internet. Las MPLS-VPNs ofrecen todo lo anterior, lo cual es posible debido a que existe un desacoplamiento del plano de reenvío y el plano de control que no es posible con IP [GHE2006].

2.3.2 Modelo MPLS-VPN

A continuación un esquema general del modelo MPLS-VPN [GHE2006]:

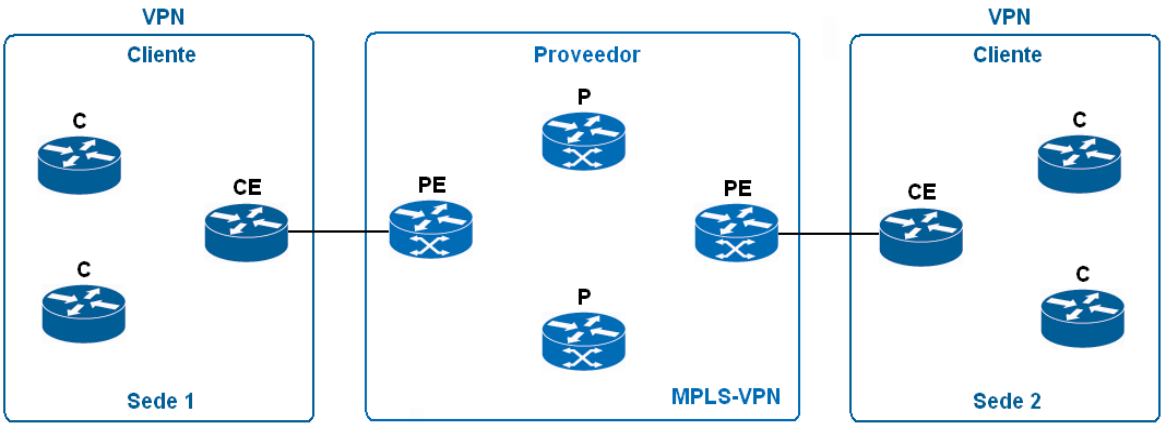

FIGURA 2-13 ESQUEMA GENERAL MPLS VPN

Fuente: "MPLS VPN Schematic Overview" [GHE2006]

La figura 2-13 muestra a un proveedor de servicios conectando dos sedes de un cliente. Un router de borde del proveedor se denomina Provider Edge (PE) router, el cual tiene conexión directa a nivel de capa 3 con el router de borde del cliente denominado Customer Edge (CE) router. Un router de proveedor o Provider (P) router es un router sin conexión directa con los routers del cliente. Un router de cliente, o Customer (C) router es un router sin conexión directa con el router PE. Tanto los routers P como los PE tienen implementado MPLS, mientras que los routers CE no lo necesitan [GHE2006].

Como los routers CE y PE interactúan en la Capa 3, deben trabajar con un protocolo de enrutamiento (o enrutamiento estático) entre ellos. El router CE tiene solo un vecino fuera de su propio local: el router PE. Si el router CE es *multihomed* (está conectado a más de un ISP a la vez), puede ser vecino de múltiples routers PE. El router CE no es vecino de otros routers CE de otros locales conectados a la red del proveedor, como en el modelo *Overlay*. El nombre peer-to-peer (punto a punto) deriva del hecho que los routers CE y PE forman una "pareja" a nivel de Capa 3 [GHE2006].

Ya que el principal propósito de una VPN es ser privada, el cliente puede tener su propio esquema de direccionamiento IP. Esto significa que pueden usar direcciones IP públicas, direcciones IP privadas o incluso direcciones IP que también son usadas por otros clientes conectados al mismo proveedor (a esto se le denomina *overlapping IP addressing*). Si los paquetes fueran reenviados como paquetes IP a través de la red del proveedor, causarían confusión en los routers P. Cada cliente debería usar un único rango de direcciones y los paquetes se reenviarían mirando la dirección IP destino en

cada router. Esto implica que todos los routers P y PE tengan la tabla de enrutamiento completa de cada cliente, lo que haría que manejen una larga tabla de enrutamiento. Este no es un esquema VPN, pues no es privado de cara a los clientes [GHE2006].

Otra solución es que todos los routers P y PE tengan una tabla de enrutamiento privada para cada cliente. Esto haría que varios procesos se lleven a cabo en todos los routers para distribuir las rutas de las VPNs. Esta no es una solución muy escalable, ya que cada vez que una VPN sea agregada a la red, se debe agregar un nuevo proceso de enrutamiento a cada router P. Además, si un paquete IP entra a un router P, ¿Cómo determinaría el router P a que VPN pertenece el paquete para poder usar la tabla de enrutamiento que le corresponde? Si el paquete es un paquete IP, esto no es posible. Se podría agregar un campo extra al paquete IP indicando a que VPN pertenece para que el router P lo reenvíe basándose en este campo y en la dirección IP destino. También en este caso, todos los routers P deberían conocer este campo extra [GHE2006].

Una solución escalable sería que los routers P desconozcan totalmente a las VPNs para que no estén cargados con la información de enrutamiento cada una de ellas. Esto es posible con MPLS. Inclusive, los routers P ya no necesitan tener la tabla de enrutamiento de los clientes, y en su lugar usan dos etiquetas MPLS. Además, ya no es necesario configurar BGP en los routers P. Las rutas VPN solo son conocidas en los routers PE, lo que hace que la información de las VPN se encuentre sólo en los routers de borde. Ésta sí es una solución escalable, la cual se muestra en la figura 2-14 [GHE2006].

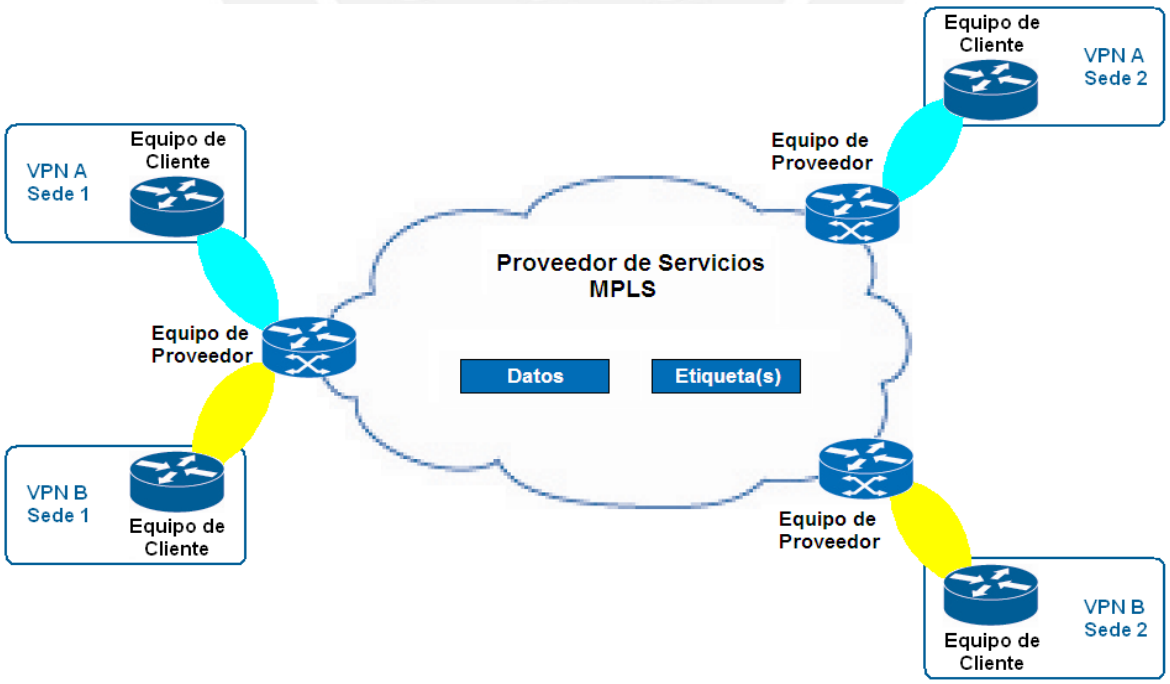

FIGURA 2-14 MODELO MPLS-VPN

Fuente: “MPLS VPN Model” [GHE2006]

2.3.3 Arquitectura MPLS-VPN

2.3.3.1 Caso de Estudio

Para entender la arquitectura MPLS-VPN, se presentará un caso de estudio. Tomaremos como ejemplo una empresa proveedora de servicios VPN llamada InterCom, con dos puntos de presencia o Points of presence (POP), uno en Arequipa y otro en Chiclayo. Los POPs están enlazados por un router en Lima [PEP2002].

La empresa proveedora tiene dos clientes: Ibank y La Marea. Ibank tiene su sede central en Chiclayo y sucursales en Cuzco y Trujillo, mientras que La Marea tiene su sede central en Arequipa y sucursales en Piura y Tacna. Además, Ibank tiene una oficina en Tumbes que está conectada directamente a su sede central. La topología de red se muestra en la figura 2-15 [PEP2002].

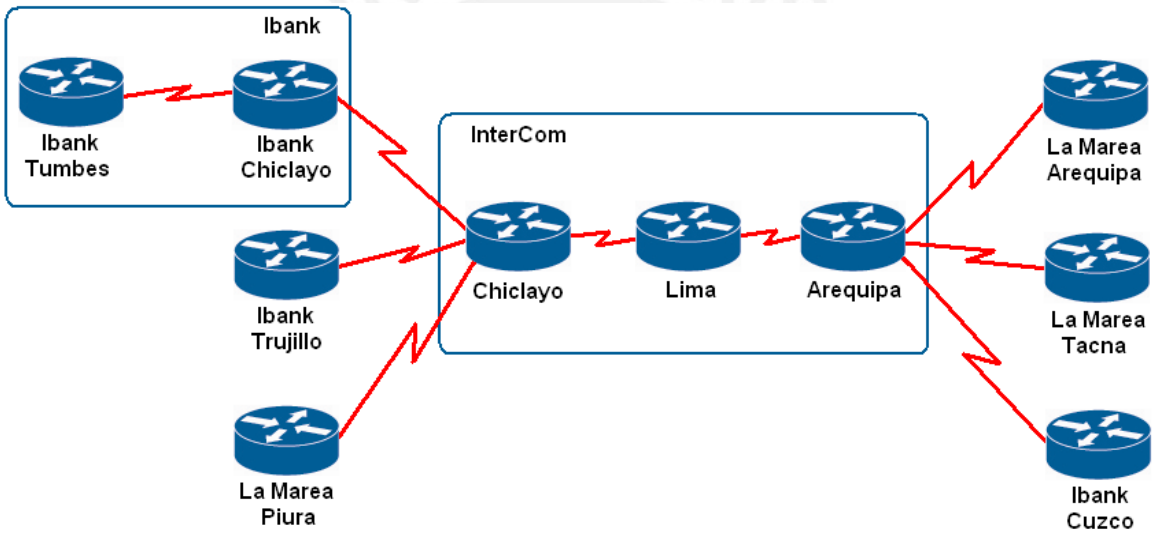

FIGURA 2-15 RED DE INTERCOM Y SUS CLIENTES

Fuente: “SuperCom Network and Its Customers” [PEP2002]

Las funciones de cada router son las siguientes:

Los routers de Arequipa y Chiclayo harán las veces de routers PE (Provider Edge), mientras que el router de Lima será el router P (Provider). Los routers de Ibank en Chiclayo, Cuzco y Trujillo, así como los de La Marea en Arequipa, Piura y Tacna, serán los routers CE (Customer Edge). El router de la oficina de Ibank en Tumbes será el router C (Customer). El proveedor InterCom no tiene responsabilidad alguna sobre este equipo, y no tiene porqué conocerlo [PEP2002].

2.3.3.2 Enrutamiento VPN y Tablas de reenvío (VRF)

Debido a que los clientes pueden utilizar direcciones IP privadas en sus redes, podrían generar un obstáculo al momento de implementar VPNs peer-to-peer. Las MPLS-VPNs solucionan esto brindando a cada VPN su propia tabla de enrutamiento y reenvío en el router, por lo que cualquier cliente que pertenezca a esa VPN accede solo al conjunto de direcciones de esa tabla. Cualquier router PE contiene dichas tablas y las emplea para alcanzar otros routers en la red del proveedor, así como destinos externos (Ej. Internet). De esta manera, se crean *routers virtuales* en un router físico, como se muestra en la figura 2-16 [PEP2002].

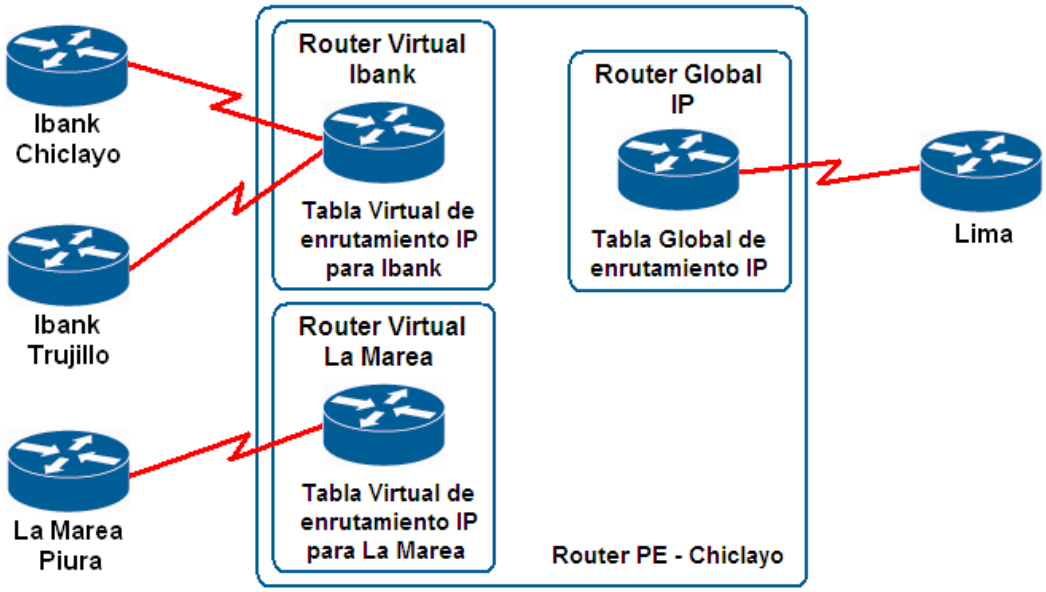

FIGURA 2-16 ROUTERS VIRTUALES EN UN ROUTER PE

Fuente: "Virtual Routers Created in a PE Router" [PEP2002]

El concepto de routers virtuales permite que el cliente utilice direcciones privadas o públicas. Como cada cliente pertenece a una VPN en particular, las direcciones deben ser únicas sólo dentro de la VPN. Esta condición no es necesaria entre diferentes VPNs a menos de que se quieran comunicar entre sí [PEP2002].

La combinación de la tabla en enrutamiento VPN IP con la tabla de reenvío VPN IP asociada se denomina **Virtual Routing and Forwarding** ó **VPN Routing and Forwarding** (VRF) [PEP2002].

Para el caso de estudio, el router de Chiclayo tiene 3 VRFs: Una por cada cliente, y una global para reenviar paquetes IP y para enrutar paquetes VPN entre routers PE [PEP2002].

2.3.3.3 Superposición de VPNs

Ahora supongamos que InterCom también ofrece servicios de Voz sobre IP (VoIP) tanto en Chiclayo como en Arequipa. Las centrales VoIP se encuentran en una VPN individual por motivos de seguridad. La figura 2-17 ilustra la nueva red [PEP2002].

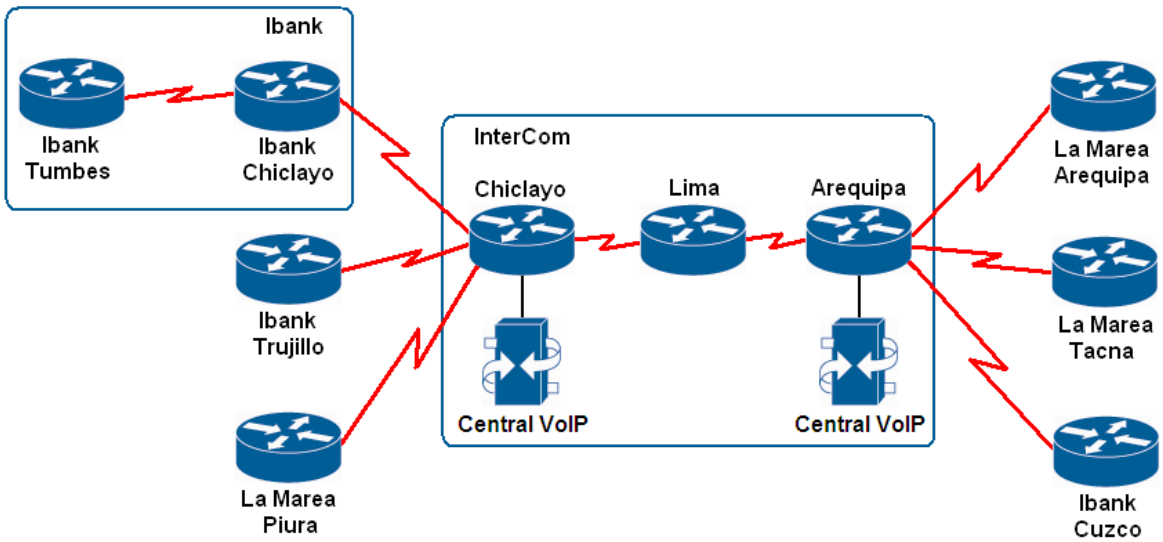

FIGURA 2-17 CENTRALES VoIP EN LA RED DE INTERCOM

Fuente: "VoIP Gateways in SuperCom Network" [PEP2002]

Tanto Ibank como La Marea deciden usar el servicio, pero solamente desde sus sedes centrales. Para lograrlo, ambas sedes necesitan estar en dos VPNs: Una para comunicarse con sus sucursales y otra para enlazarse a las centrales VoIP, como se ve en la figura 2-18 [PEP2002].

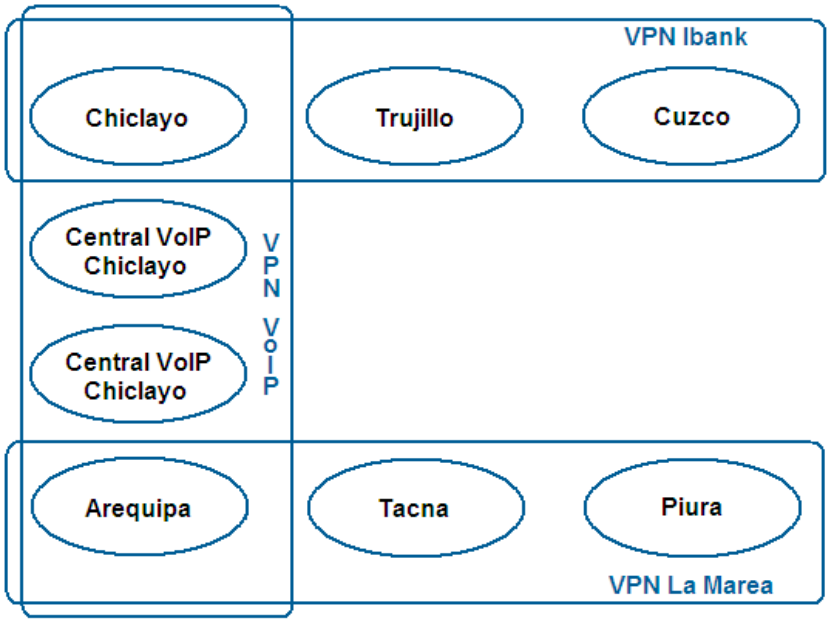

FIGURA 2-18 CONECTIVIDAD VPN EN LA RED DE INTERCOM

Fuente: "VPN Connectivity Requirements in SuperCom Network" [PEP2002]

Las MPLS-VPNs manejan el concepto de sedes. Cada VPN está conformada por una o múltiples sedes, las cuales tienen información de enrutamiento en común. Esto quiere decir que una sede puede pertenecer a más de una VPN si tiene rutas de VPNs separadas. De esta forma, se tiene la capacidad de construir intranets, extranets o esquemas aún más complejos [PEP2002].

Entonces, las VRFs también deben soportar el concepto de sedes. Por ejemplo, las sedes centrales de Ibank y La Marea no pueden usar la misma VRF que las demás sedes conectadas al mismo router PE. La sede central de Ibank necesita acceder a las centrales VoIP, por lo que las rutas hacia las centrales deben estar en la VRF para esa sede. En consecuencia, las VRFs son ahora una colección de rutas que deben estar disponibles en una sede (o conjunto de sedes) conectada a un router PE, los cuales pueden pertenecer a más de una VPN. La tabla 2-4 muestra el conjunto de VRFs para la red de InterCom [PEP2002].

TABLA 2-4 VRFs EN LOS ROUTERS PE DE LA RED DE INTERCOM

Fuente: "VRFs in the PE Routers in the SuperCom Network" [PEP2002]

Router PE	VRF	Sedes en la VRF	VPNs a las que pertenecen
Chiclayo	Ibank_Central	Ibank sede Chiclayo	Ibank, VoIP
	Ibank	Ibank sede Trujillo	Ibank
	La Marea	La Marea sede Piura	La Marea
	VoIP	VoIP Chiclayo	VoIP
Arequipa	La Marea_Central	La Marea sede Arequipa	La Marea, VoIP
	La Marea	La Marea sede Tacna	La Marea
	Ibank	Ibank sede Cuzco	Ibank
	VoIP	VoIP Arequipa	VoIP

2.3.3.4 Route Targets

Ahora que ya no se maneja el concepto de una sola VRF para una sola VPN, el router necesita una forma para saber qué rutas insertar en cada VRF. El *route target* soluciona este problema. Cada ruta VPN es etiquetada con uno o más route targets cuando es exportada de una VRF para ser ofrecida a otras VRFs. Se puede asociar un grupo de route targets a una VRF, y todas las rutas etiquetabas con al menos uno de los route targets serán insertadas en la VRF. El route target tiene 64 bits y, vendría a ser lo más cercano a un *VPN identifier* en la arquitectura MPLS-VPN [PEP2002].

La red de InterCom tiene tres VPNs, por lo que necesita tres route targets. La asociación entre route targets y las VRFs se muestra en la tabla 2-5 [PEP2002].

TABLA 2-5 CORRESPONDENCIA ENTRE VRFs Y ROUTE TARGETS

Fuente: "Correspondence Between VRFs and Route Targets in SuperCom Network" [PEP2002]

Router PE	VRF	Sedes en la VRF	Route Target para exportar	Route Target para importar
Chiclayo	Ibank_Central	Ibank sede Chiclayo	Ibank, VoIP	Ibank, VoIP
	Ibank	Ibank sede Trujillo	Ibank	Ibank
	La Marea	La Marea sede Piura	La Marea	La Marea
	VoIP	VoIP Chiclayo	VoIP	VoIP
Arequipa	La Marea_Central	La Marea sede Arequipa	La Marea, VoIP	La Marea, VoIP
	La Marea	La Marea sede Tacna	La Marea	La Marea
	Ibank	Ibank sede Cuzco	Ibank	Ibank
	VoIP	VoIP Arequipa	VoIP	VoIP

Es importante indicar que en escenarios VPN más complejos, los route targets exportados desde una VRF no siempre coinciden con el conjunto de route targets importados de una VRF [PEP2002].

2.3.3.5 Propagación de Rutas en la Red de Proveedor

Ahora que ya se revisó el funcionamiento de una MPLS-VPN enfocado en un router PE a la entrada de la red, toca analizar cómo se intercambia la información de los clientes y las rutas dentro del backbone [PEP2002].

Hay dos formas diferentes de realizar el intercambio de rutas VPN entre routers PE [PEP2002]:

- Los routers PE ejecutan un protocolo de enrutamiento por cada VPN (como OSPF o EIGRP). Esta solución presenta problemas de escalabilidad en redes de proveedor con muchas VPNs (Ej. 100 VPNs), además se requerir un diseño mucho más complejo.
- Los routers PE ejecutan un protocolo de enrutamiento para intercambiar todos los prefijos VPN. Para evitar conflictos entre direcciones IP de los clientes, a sus direcciones IP se les debe agregar información adicional que las haga únicas.

Las MPLS-VPNs utilizan el segundo método, el cual se muestra en la figura 2-19.

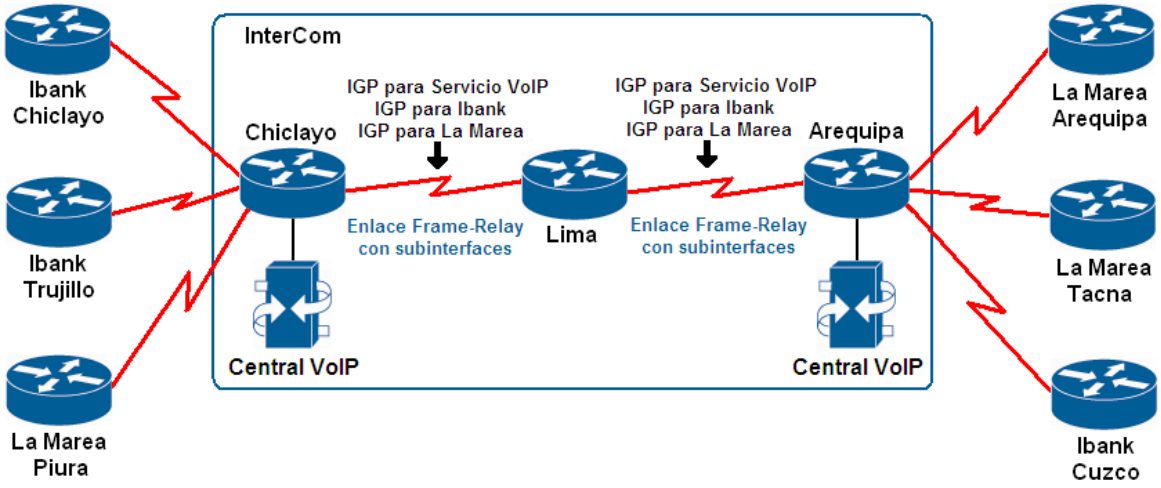

FIGURA 2-19 RED INTERCOM CON UN IGP POR VPN

Fuente: "SuperCom Network with One IGP per VPN" [PEP2002]

A las subredes que los routers CE anuncian a los routers PE se les agrega un prefijo de 64 bits llamado route distinguisher. El resultado es una dirección de 96 bits que se intercambia dentro de la red a través de una extensión del protocolo BGP denominado "Multi Protocol BGP" (MP-BGP). Las siguientes son las razones por las que se escoge el protocolo BGP para transportar rutas VPN [PEP2002]:

- BGP es el único protocolo de enrutamiento que soporta un gran número de rutas.
- BGP, EIGRP, y IS-IS son los únicos protocolos de enrutamiento diseñados para ser Multiprotocolo (pueden llevar información de diferentes familias de direcciones). Sin embargo, IS-IS and EIGRP no son tan escalables como BGP.
- BGP puede llevar información adjuntada a una ruta como un atributo adicional. Es más, se pueden definir atributos que BGP enviará sin necesidad de entenderlos.

2.3.3.6 Multi Protocol BGP

Multi Protocol BGP es una extensión del protocolo BGP-4. Permite anunciar rutas VPN de clientes entre los routers PE que éstos aprendieron de los routers CE directamente conectados. Estas rutas pueden ser aprendidas ya sea con BGP-4, RIP Versión 2, rutas estáticas o a través de OSPF [PEP2002].

MP-BGP es necesario únicamente en el backbone del proveedor, por lo que las sesiones MP-BGP son sesiones internas. Es necesario porque no sólo transportan prefijos IPv4, sino también prefijos VPN-IPv4, etiquetas MPLS y comunidades BGP [PEP2002].

Retomando el caso de estudio, tomemos el caso del cliente Ibank. Asumamos que la sede de Chiclayo utiliza OSFP para interactuar con el backbone de InterCom, la de Trujillo usa RIP, y la de Cuzco tiene configurado enrutamiento por defecto mientras que del otro lado, se tiene enrutamiento estático. Es importante aclarar que el router de Lima no participa del escenario MP-BGP. El proceso que se realiza para recolectar información de las rutas se ilustra en la figura 2-20 [PEP2002].

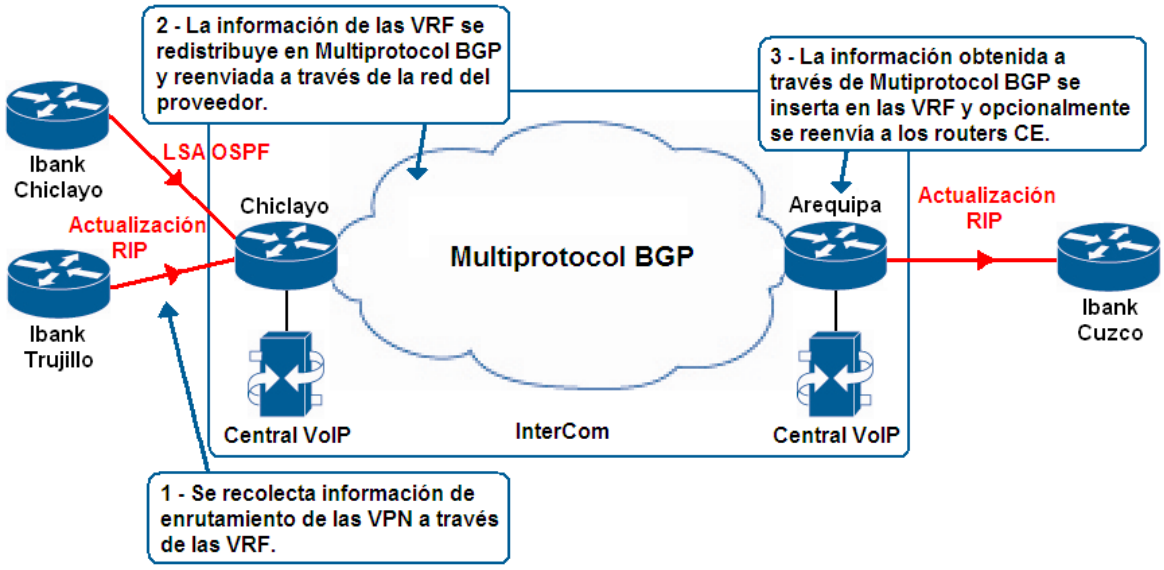

FIGURA 2-20 PROTOCOLOS DE ENRUTAMIENTO EN LA RED DE INTERCOM

Fuente: "Routing Protocol Operation in SuperCom Network" [PEP2002]

Para que la red soporte la superposición de VPNs, cada protocolo de enrutamiento debe limitarse a una sola VRF de una VPN. La información de los diferentes protocolos y las rutas estáticas se redistribuyen a través de MP-BGP. Se agregan los route distinguishers necesarios al momento de la redistribución y también el route target definido en la VRF de origen [PEP2002].

La redistribución en MP-BGP no es automática y debe configurarse manualmente en cada router de la VRF, a menos que la información se haya aprendido del cliente a través de BGP [PEP2002].

2.3.3.7 Reenvío de Paquetes VPN

Se ha visto previamente que a las direcciones IP usadas dentro de una VPN se les agrega un route distinguisher para hacerlas únicas. De forma similar, cuando los paquetes originados en la VPN se envían por la red backbone, se les debe agregar información para que sean reconocibles por los routers P. Esto se logra de dos formas [PEP2002]:

- Se rearma el paquete para que incluya direcciones de 96 bits. Esto es lento y complejo de realizar.
- El paquete se envía a través de un túnel VPN-over-IP. Esto haría de la red MPLS-VPN tan compleja como las soluciones que utilizan el modelo overlay.

Cada paquete VPN es etiquetado en el router PE de ingreso con una etiqueta que identifica solamente al router PE de salida, y se envía dentro de la red. Los demás routers cambian las etiquetas sin tomar en cuenta el contenido del paquete [PEP2002]. Este proceso se explica en la figura 2-21.

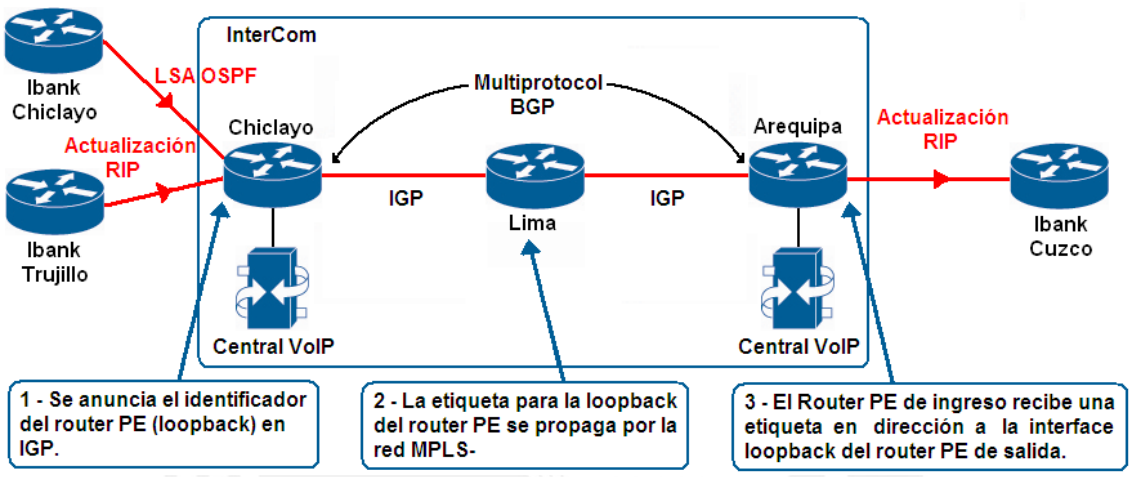

FIGURA 2-21 REENVÍO DE PAQUETES VPN – PRIMEROS PASOS

Fuente: "VPN Packet Forwarding - Preparatory Steps" [PEP2002]

Cuando el router PE de entrada recibe la etiqueta del router PE de salida, se inicia el intercambio de paquetes VPN. Cuando el router PE de egreso recibe el paquete, necesita saber la VPN a la que el paquete está destinado. Para ello, se usa una etiqueta adicional, como se muestra en la figura 2-22 [PEP2002].

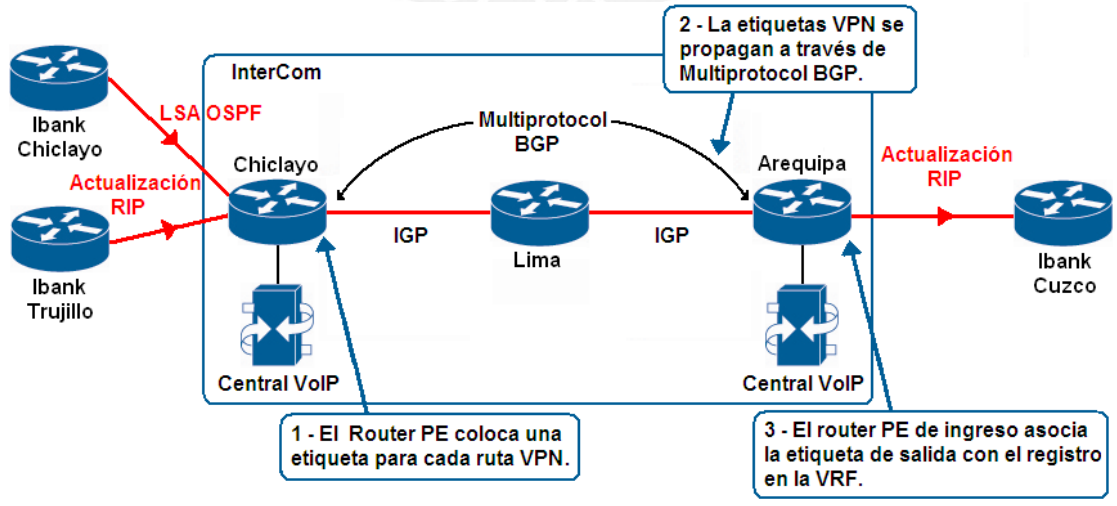

FIGURA 2-22 ASIGNACIÓN DE ETIQUETAS VPN

Fuente: "VPN Label Allocation" [PEP2002]

Cuando un paquete VPN llega al router PE de ingreso, se examina la VRF correspondiente y se busca la etiqueta asociada con la dirección del router PE de salida. Otra etiqueta, que apunta hacia el router PE de salida se obtiene de la tabla global de reenvío. Se apilan ambas etiquetas y se agregan al inicio del paquete, y se envía hacia el router PE de salida [PEP2002].

Todos los routers P reenvían el paquete basándose únicamente en la primera etiqueta, nunca analizan la información de la segunda etiqueta, por lo que desconocen que se trata de un paquete VPN. El router PE de salida remueve la primera etiqueta, y analiza la segunda que identifica a la VRF y algunas veces también a la interface de salida en el router PE. Si es necesario, también se analiza la VRF y se envía el paquete al router CE correspondiente [PEP2002].

2.4 Inter-AS VPNs

Hasta este punto se ha asumido que los clientes VPN están conectados a un único proveedor de servicio. Sin embargo, es posible que el cliente tenga sedes dispersas en un área geográfica muy grande (abarcando en muchos casos, varios países), por lo que se hace necesaria la conexión entre múltiples proveedores de servicios para poder brindar el servicio VPN requerido [PEP2002].

Esta extensión del concepto inicial de MPLS-VPN se puede entender como arquitecturas Carrier's carrier (Proveedor de proveedor) o Inter-provider (Inter proveedores) [PEP2002]. Cada segmento de red bajo la administración un proveedor en particular, se conoce como Sistema Autónomo. Entonces se puede generalizar la nueva arquitectura MPLS-VPN como Inter-AS MPLS-VPNs (Inter Autonomous System MPLS-VPNs), como se muestra en la figura 2-23.

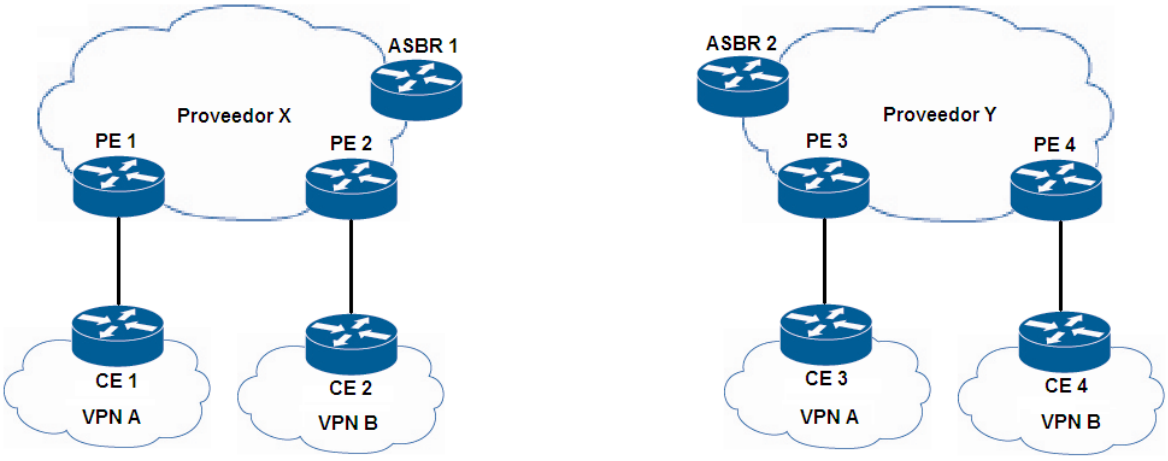

FIGURA 2-23 ESCENARIO QUE REQUIERE IMPLEMENTAR INTER-AS VPN

Fuente: “Why Inter-AS VPN?” [HAS2005]

El tema de estudio de la presente tesis abarca el desempeño de este tipo de arquitectura. Para ello se han tomado cuatro modelos de implementación, que son los ampliamente utilizados en los servicios VPN de grandes dimensiones. Dichos modelos de red son presentados a en el siguiente capítulo.

Capítulo 3

Análisis Previo de las Soluciones

3.1 Modelos de Inter-AS VPNs

A continuación se presentan las soluciones que serán motivo de análisis. Esta descripción se basa en la documentación RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)" y en la documentación del fabricante de equipos que se utilizarán (Cisco). Sin embargo, para la simulación estas soluciones serán acondicionadas de acuerdo a los alcances que de este trabajo, y se detallarán más adelante.

3.1.1 Conexión VRF-VRF:

Este modelo esta descrito en el RFC 4364 como "VRF-to-VRF connections at the ASBRs" y en la documentación de Cisco como "Back-to-Back VRF". Es el método más simple de implementar una MPLS-VPN entre diferentes proveedores [MAH2008].

Los routers que interconectan los sistemas autónomos funcionan como routers de borde (ASBRs), y están interconectados ya sea por un solo enlace físico dividido en varias subinterfaces o por múltiples enlaces físicos. En cada ASBR se configuran VRFs para recolectar las rutas VPNv4, y cada subinterfaz o interfaz conectada entre ASBRs está asociada a una única VRF [MAH2008].

En cada VRF se puede configurar eBGP, RIPv2, EIGRP, OSPF, o enrutamiento estático para distribuir las rutas a su par adyacente aunque eBGP es el más usado debido a su escalabilidad y seguridad. Cada ASBR trata al ASBR vecino como un router CE, e intercambian las rutas de la misma manera que lo hacen un PE y un CE. Las rutas LSP de los sistemas autónomos adyacentes se interconectan usando el mecanismo tradicional de direccionamiento IP. Es decir, los paquetes se envían como paquetes IP puros entre los ASBRs [MAH2008] [LOB2005].

La limitación de esta opción radica en la necesidad de separar interfaces o subinterfaces y sesiones eBGP para cada VRF en los ASBRs, lo cual no es conveniente para un futuro incremento de clientes. Sin embargo, esta solución es una de las más ampliamente usadas hoy en día, y se ilustra en la figura 3-1 [MAH2008].

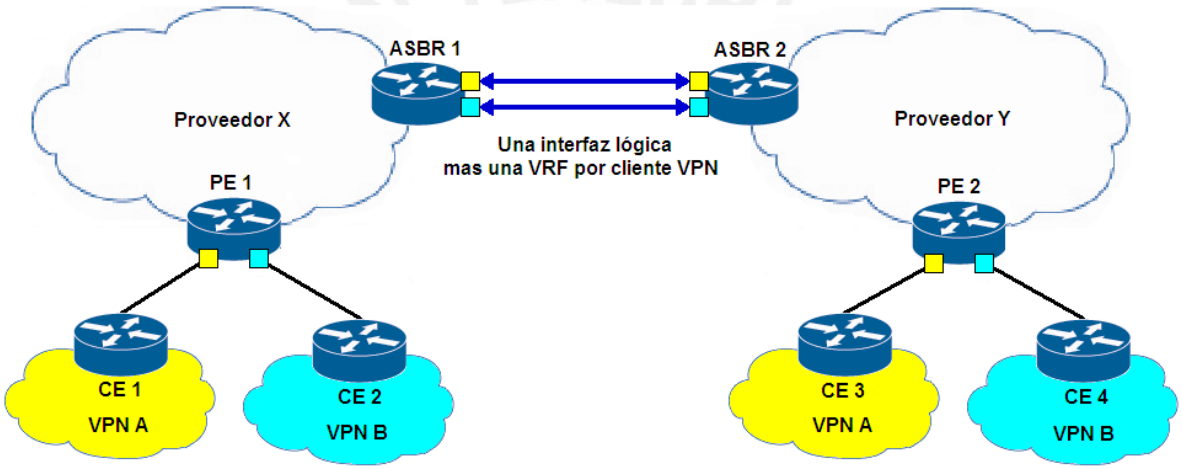

FIGURA 3-1 MODELO VRF-VRF

Fuente: "VRF-VRF" [HAS2005]

La figura 3-1 muestra una red MPLS-VPN con dos clientes cuyas sedes están dispersas. Se observa que el enlace que interconecta los ASBRs tiene una subinterfaz y una VRF asociada para cada cliente (representadas por los colores amarillo y turquesa). Asimismo, los PEs también tienen asociada una interfaz física y una VRF, ya que en este caso se conectan a distintos equipos CE.

En caso de agregar un cliente, además de agregar una interfaz y VRF en los PEs, se debe configurar una subinterfaz y VRF adicionales en el enlace entre los ASBRs.

3.1.2 Conexión MP-eBGP

Este modelo también esta descrito en el RFC 4364 como "eBGP redistribution of labeled VPN-IPv4 routes from AS to neighboring AS" y en la documentación de Cisco figura como "ASBR-to-ASBR" [MAH2008].

Para esta solución ya no hay necesidad de configurar VRFs por cada cliente en los ASBRs, pues en su lugar se intercambian prefijos VPNv4 para diferenciar los clientes VPN [MAH2008]. Los ASBRs usan MP-eBGP para intercambiar las rutas VPNv4, y los paquetes son transportados con etiquetas desde un ASBR a otro [LOB2005].

En una red MPLS-VPN tradicional, el envío de paquetes se realiza sólo si el router especificado con el siguiente salto en la ruta BGP es el mismo que asignó la etiqueta VPN en la cabecera MPLS-VPN. Sin embargo, cuando las VPNs están dispersas y atraviesan más de un proveedor, el siguiente salto es cambiado cuando existe una sesión eBGP entre los ASBRs. Entonces, para este caso, una etiqueta VPN es asignada cada vez que el siguiente salto es cambiado. Esto hace que el LSP termine en el ASBR que anuncia la ruta, y éste tiene que asignar una nueva etiqueta para dicha ruta antes de enviarla a través de un mensaje MP-eBGP a su ASBR vecino [LOB2005].

Otro punto a tener en cuenta, es que por defecto un router de borde descarta prefijos VPNv4 entrantes que no son importados a ninguna de las VRFs que tiene configuradas (MP-BGP automatic route filtering mechanism). Entonces, los ASBRs que no tienen VRFs configuradas deben configurarse para que puedan aceptar los prefijos BGP VPNv4 de los routers PE dentro del AS. La figura 3-2 muestra este modelo [MAH2008].

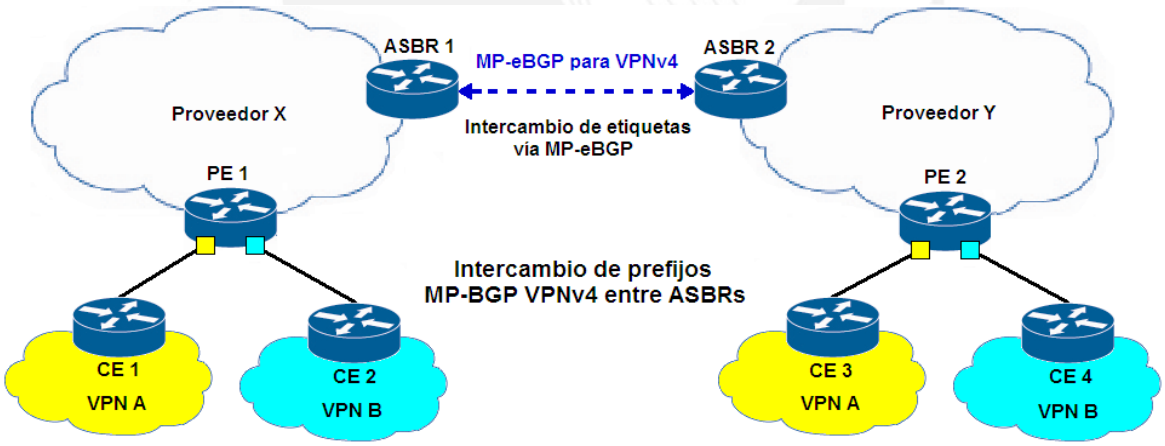

FIGURA 3-2 MODELO MP-eBGP

Fuente: “MP-eBGP for VPNv4” [HAS2005]

La principal desventaja del modelo se presenta en la calidad de servicio (QoS) y la garantía de entrega de extremo a extremo. Esto se debe a que el tráfico de todos los clientes es transmitido por un único enlace como paquetes etiquetados, y el ancho de banda dentro del enlace no es ilimitado [MAH2008].

Este modelo tiene tres submodelos que difieren principalmente en la forma como se establece la sesión MP-eBGP entre los ASBRs [MAH2008]. A continuación se explica cada uno de ellos.

3.1.2.1 2a – Next-hop-self

Se establece una sesión MP-eBGP entre las interfaces físicas directamente conectadas. Cada ASBR debe anunciarse a sí mismo como el siguiente salto de la ruta MP-eBGP recibida por el ASBRs vecino cuando publica la ruta dentro de su propio sistema autónomo a través de MP-iBGP [MAH2008].

Para esto se debe tener en cuenta que cada vez que el siguiente salto cambia, una nueva etiqueta se anuncia para el prefijo BGP [MAH2008].

3.1.2.2 2b – Redistribute connected

En esta opción, la sesión MP-eBGP también se establece entre las interfaces físicas directamente conectadas. Cada ASBR debe hacer que la dirección del siguiente salto del ASBR vecino sea alcanzable para su propio sistema autónomo y así ya no sea necesario que se anuncie a sí mismo como el siguiente salto de la ruta [MAH2008].

El ASBR acepta la ruta sin cambiar el siguiente salto ni la etiqueta, que continúan siendo los del ASBR remoto. Lo que se hace en su lugar es redistribuir las redes directamente conectadas dentro del IGP para anunciar el siguiente salto de las rutas recibidas desde el ASBR remoto [MAH2008].

En el caso de los submodelos a y b, no hay necesidad de habilitar TDP/LDP o algún IGP entre los ASBRs. La sesión MP-eBGP que se establece en su lugar permite a las interfaces involucradas transmitir paquetes etiquetados, pues ambos ASBRs conocen las etiquetas VPN [MAH2008].

3.1.2.3 2c – eBGP entre ASBRs y MP-eBGP entre Loopbacks

Esta es una variación de las dos opciones anteriores, donde la sesión MP-eBGP entre los ASBRs se hace utilizando las IPs loopback en lugar de las interfaces físicas (para ello se emplea MP-eBGP Multisalto). Se debe configurar estáticamente las direcciones IPs loopback como el siguiente salto en cada ASBR. Además, se puede usar tanto el método “next-hop-self” como “redistribute connected” (“redistribute static” en este caso, ya que el siguiente salto en el AS vecino es una ruta estática hacia la loopback) dentro del IGP en cada ASBR [MAH2008] [LOB2005].

Esta opción se utiliza principalmente cuando existen múltiples enlaces entre los ASBRs, con la necesidad de balancear carga para incrementar el ancho de banda disponible. A diferencia de los submodelos anteriores, aquí si se debe habilitar LDP entre los ASBRs ya que ahora los vecinos MP-eBGP no están directamente conectados [MAH2008].

La desventaja de este escenario, radica en la forma como los LSRs generan e insertan etiquetas para rutas estáticas. Esto varía significativamente si las interfaces que conectan los ASBRs son multiacceso o punto-punto [MAH2008].

Si son multiacceso, la ruta estática debe apuntar al siguiente salto y no a la interfaz de salida. De lo contrario, la etiqueta saliente será nula y todo el etiquetado local será nulo. El ASBR hará una búsqueda local de la IP y descartará el paquete. Si son punto-punto, no habrá problemas ya que el LSR local tendrá una etiqueta saliente sin importar como esté configurada la ruta estática [MAH2008].

Por un tema de seguridad, la única etiqueta que puede intercambiarse entre los ASBRs es la “Pop Label” de la dirección loopback respectiva (El significado de Pop Label se explica más adelante). El hecho de no habilitar un IGP entre los ASBRs puede solucionar el problema de seguridad al habilitar LDP entre ellos, ya que nunca insertarán internamente etiquetas aprendidas del otro ASBRs si es que no tienen rutas exactas en su tabla de enrutamiento. Incluso se podrían filtrar etiquetas entre los ASBRs. Sin embargo, la opción más segura es no habilitar IGP o LDP entre dos proveedores distintos [MAH2008].

3.1.3 Conexión MP-eBGP Multisalto entre RRs

Este modelo también esta descrito en el RFC 4364 como “Multi-hop eBGP redistribution of labeled VPN-IPv4 routes between source and destination ASs, with eBGP redistribution of labeled IPv4 routes from AS to neighboring AS” y en la documentación de Cisco figura como “Multi-Hop MP-eBGP entre RRs y eBGP entre ASBRs” [MAH2008].

Esta opción es considerada la más escalable comparada con las dos anteriores, ya que los ASBRs no tienen que aprender todos los prefijos VPNv4 pues la sesión MP-eBGP se establece entre los routers Route Reflector (RRs). Los ASBRs serán los encargados únicamente de intercambiar las direcciones del siguiente salto IPv4 juntos con sus etiquetas a través de eBGP. De esta manera se completa la creación de un LSP desde el PE de ingreso local hasta el PE de egreso remoto [MAH2008]. La figura 3-3 ilustra este modelo.

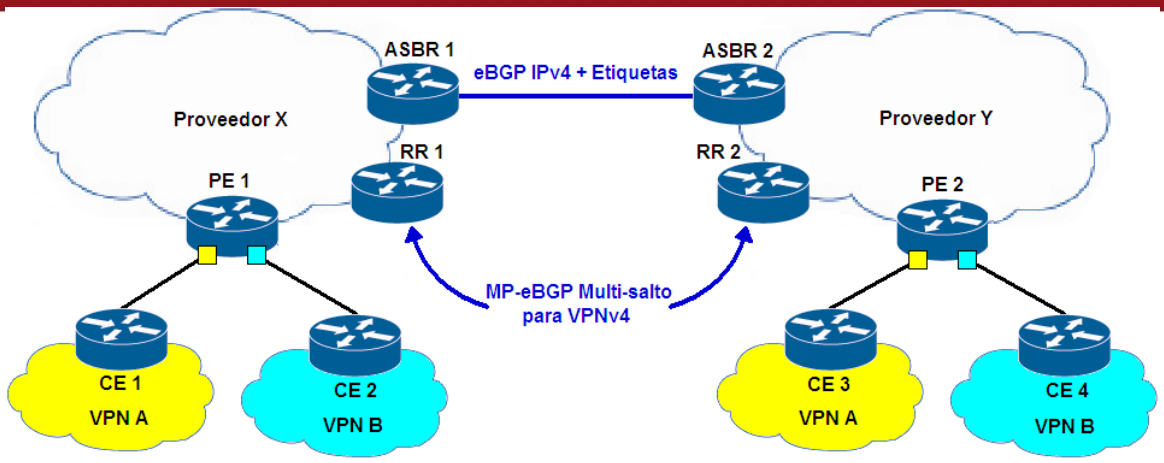

FIGURA 3-3 MODELO MULTIHOP MP-eBGP

Fuente: "Multihop MP-eBGP" [HAS2005]

Se debe habilitar la sesión eBGP en cada ASBR para permitir el intercambio de etiquetas MPLS junto con las rutas IPv4. Para la sesión MP-eBGP entre los RRs, se debe hacer que el siguiente salto no sea modificado cuando las rutas VPNv4 se intercambien entre los RRs, y los prefijos VPNv4 tampoco deben modificarse. Este es el único caso en el que el LSP no es partido y la etiqueta MPLS-VPN original es usada en todo el tramo, pues el siguiente salto en la ruta VPNv4 nunca cambia [MAH2008].

Debido a que cada AS puede alcanzar los siguientes saltos internos del AS vecino, la seguridad hace que ésta sea una alternativa viable cuando los AS se encuentran bajo una misma autoridad, como es el caso de un proveedor con AS en diferentes regiones del mundo [MAH2008]. Sin embargo, se puede incrementar la seguridad utilizando métodos de encriptación para que el tráfico esté cifrado.

3.1.4 Conexión con Proveedor de Tránsito sin VPNs:

Este modelo no figura en el documento RFC 4364. Sin embargo, es una opción también utilizada y figura en la documentación de Cisco como "Non-VPN Transit Provider" [ZHA2003], por lo que también será motivo de estudio.

En este caso, los proveedores VPN utilizan un tercer proveedor de tránsito, que no conoce las VPN pero si debe tener implementado MPLS [HAS2005]. Los dos AS "clientes", se conectan al AS "proveedor" de tránsito a través de los routers ASBR. La información VPNv4 entre los dos AS clientes se intercambia entre sus respectivos RRs utilizando MP-eBGP Multisalto. Se establece una sesión eBGP entre los ASBRs clientes y los ASBRs del proveedor de tránsito para poder transmitir las rutas a través del proveedor de tránsito [ZHA2003]. El modelo se muestra en la figura 3-4.

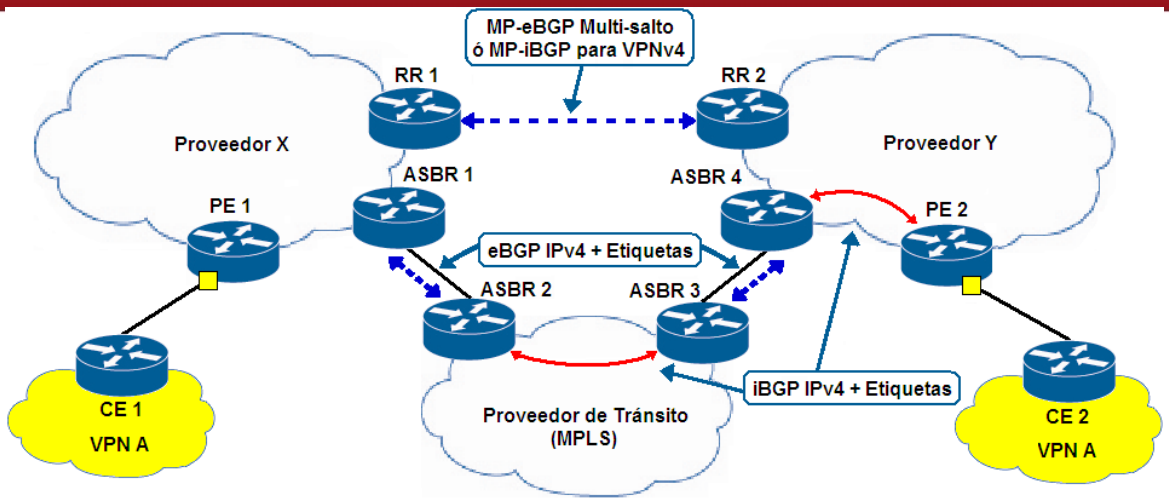

FIGURA 3-4 MODELO PROVEEDOR DE TRÁNSITO

Fuente: "Non-VPN transit provider" [HAS2005]

Los PE y RRs deben ser accesibles y tener etiquetas adecuadas entre los dos AS clientes. Es decir, el LSP debe ser extremo-extremo desde el PE local hasta el PE remoto. Los ASBRs clientes pueden intercambiar prefijos IPv4 y etiquetas con los ASBRs del AS proveedor [ZHA2003].

En el backbone de transito, se utiliza un IGP entre los ASBRs y se habilita iBGP para propagar las rutas externas. Se habilita también el intercambio de etiquetas IPv4 entre los dos vecinos iBGP. Los ASBRs son configurados con eBGP [ZHA2003] [LOB2005].

3.2 Parámetros de medición:

Hay parámetros comúnmente usados para evaluar el desempeño de una red. A continuación se hará una breve descripción de cada uno de estos, indicando que información relevante brindan.

- **Ancho de Banda:** Es la capacidad de transportar datos de una red. Indica la máxima cantidad de datos que puede pasar de un punto a otro por unidad de tiempo. Para el estudio que se realizará se medirá en términos de rendimiento, es decir, la cantidad real de datos que se puede enviar por unidad de tiempo. Por ejemplo, si una red Ethernet tiene una velocidad de 100 megabits por segundo, ese es el tope de rendimiento de la red, aunque normalmente es menor [KOZ2005].
- **Latencia:** Se refiere al tiempo de transferencia de datos en un canal de comunicación o red. Un aspecto importante de la latencia es cuánto tiempo pasa

desde que se hace una petición de datos hasta que los datos empiecen a llegar. La baja latencia es considerada mejor que la alta latencia [KOZ2005].

- **Jitter:** Este parámetro mide la variación de retardo entre paquetes. Cuando múltiples paquetes son enviados consecutivamente desde el origen hacia el destino separados 10 ms uno del otro, en condiciones ideales el destino debería recibir los paquetes separados 10 ms uno del otro. En condiciones reales, los retardos en la red causan que el retardo de llegada sea mayor o menor a 10 ms. Un valor positivo de jitter indica que los paquetes llegaron con más de 10 ms de separación. Los paquetes que llegan 12 ms después del anterior causan un jitter positivo de 2 ms, mientras que los paquetes que llegaron 8 ms después, causan un jitter negativo de 2 ms [CIS2006].
- **Uso del CPU:** Existen funciones críticas en los dispositivos de red, como el procesamiento de protocolos de enrutamiento y de conmutación de paquetes que requieren alto procesamiento. Estos procesos son llevados a cabo en la memoria y comparten el CPU. Si el uso del CPU es muy alto, es posible que una actualización de ruta no sea realizada o que un paquete sea descartado.
- **Tiempo de convergencia:** Es el tiempo que le toma a la red establecer las sesiones necesarias, intercambiar información y actualizar sus tablas de enrutamiento. Esto es importante para determinar cuánto demorará una red en recuperarse ante un corte o caída de uno o más enlaces.

3.3 Herramientas de Medición:

Para la medición de los parámetros mencionados se utilizarán las siguientes herramientas:

- **Iperf:** Desarrollado por NLANR / DAST, se utilizará para medir el ancho de banda y el Rendimiento (BW real / BW teórico) [SOU2012].
- **Estadísticas del router:** Se utilizarán los comandos que muestren el uso total del CPU del equipo durante un periodo de tiempo. El uso máximo es medido y registrado cada segundo, y el promedio de uso es calculado en un periodo de tiempo de alrededor de un minuto.
- **Analizador de protocolos:** Se utilizará el analizador *Wireshark*, que permite capturar y explorar el tráfico que se ejecuta en una red. Se usará para capturar los mensajes BGP que se intercambien y así determinar el tiempo de convergencia de cada red [WIR2012].

Capítulo 4

Implementación y Pruebas de Desempeño

4.1 Información preliminar:

Para realizar las implementaciones, se cuenta con 6 routers Cisco 2800 del laboratorio de redes de la Pontificia Universidad Católica del Perú, además de la herramienta de simulación de redes GNS3. Debido a que no es posible implementar la totalidad de la red con el número de equipos físicos con los que se cuenta, se determinó que los routers Cisco 2800 conformen las redes backbone de los proveedores VPN y los equipos de cliente sean simulados por computadora utilizando la herramienta GNS3.

El estudio de las diferentes opciones de Inter-AS VPN se basa principalmente en la forma en la que se establece la interconexión entre los proveedores, por lo que las mediciones se realizarán principalmente es estos enlaces, es decir, en los routers ASBR. Además, se realizarán mediciones extremo-extremo. La arquitectura de red interna de cada uno de los proveedores es transparente para este estudio, y se implementarán de tal forma que ambas sean simétricas.

La conexión entre proveedores será a través de un enlace serial, mientras que los enlaces entre los equipos de cada proveedor, así como los de proveedor con cliente, serán enlaces Fast-Ethernet. Finalmente, las conexiones entre proveedores y clientes

serán también enlaces FastEthernet. El ancho de banda teórico de extremo a extremo está definido por el enlace serial, al ser el enlace de menor capacidad, con un ancho de banda teórico de 2048 Kbps.

Se consideró simular un escenario de 20 clientes, cada uno de los cuales tiene una sede en cada extremo de la topología. El hecho de que el número máximo de clientes simulados sea 20 se debe a razones de configuración, ya que de aumentar significativamente este número las configuraciones serían demasiado extensas y poco prácticas para el propósito de la presente tesis (Ver Anexo 1). Al ser veinte clientes, se anunciarán veinte rutas desde cada lado. Se instalará 1 host real en cada extremo que se será asignado al cliente número 10. Otros nueve clientes serán simulados en una sola computadora utilizando el programa VPCS. Así, se simularán 10 de los 20 clientes configurados en la red con los que se probará la conectividad.

Se realizarán 3 pruebas en cada topología. La primera será con una conexión de extremo a extremo, la segunda se hará con diez conexiones y la tercera con veinte conexiones. Para simular las distintas conexiones se empleará el programa Traffic.

A continuación se describen las topologías implementadas y las pruebas hechas en cada una de ellas. Se muestran imágenes de los gestores de la red que permiten ver parte de las pruebas hechas. Los resultados consolidados se encuentran en un cuadro resumen al final de cada sección.

4.2 Implementación

4.2.1 Modelo 1: VRF-VRF

Para esta implementación, se han considerado 2 routers para cada proveedor. No se consideraron Route Reflectors ya que no forman parte de la conexión entre proveedores. Además, con el objetivo de simular múltiples clientes, se ha utilizado un solo CE en cada lado (que son los routers simulados por computadora) y en cada uno se configurarán todas las VPNs clientes (Mult- VRF CEs). La topología se muestra en la figura 4-1.

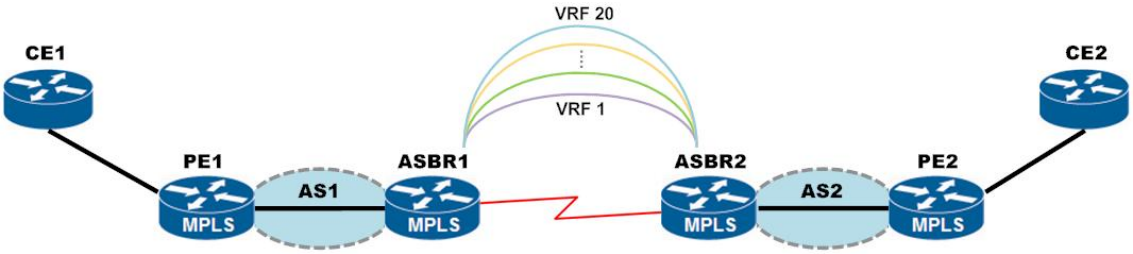

FIGURA 4-1 IMPLEMENTACIÓN MODELO 1

Fuente: “Elaboración Propia”

En primer lugar se verificó la conectividad y el desempeño con una única conexión.

Se logró conectividad entre los equipos finales de cliente, con un retardo promedio de 95 ms. Como ejemplo en la figura 4-2 se muestra el caso del Cliente 10.

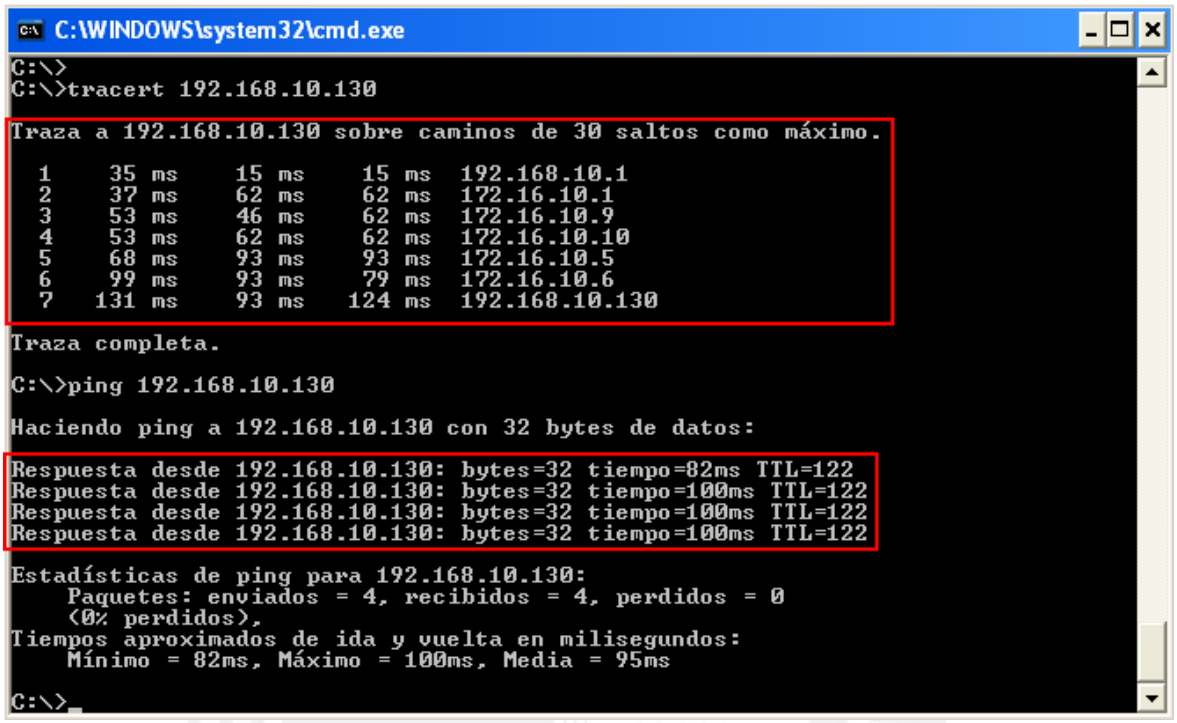

FIGURA 4-2 CONECTIVIDAD ENTRE SEDES A Y B (MODELO 1)

Fuente: “Elaboración Propia”

Posteriormente se midió el ancho de banda para este cliente con el enlace sin conexiones adicionales.

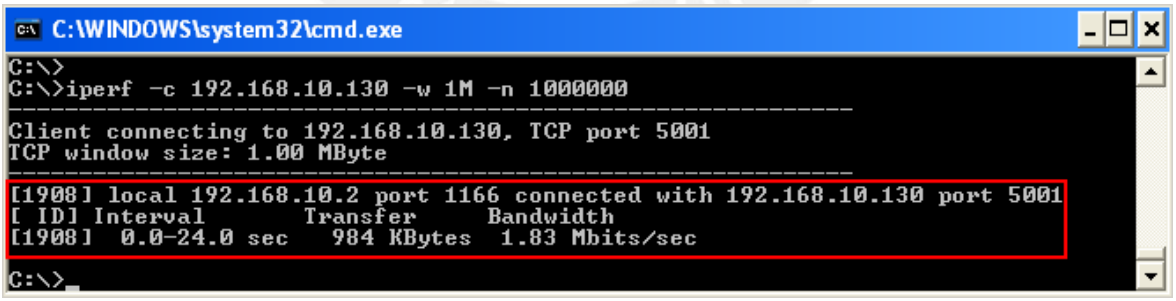

FIGURA 4-3 ANCHO DE BANDA CON 1 CONEXIÓN DESDE SEDE A (MODELO 1)

Fuente: “Elaboración Propia”

En la figura 4-3 se aprecia un ancho de banda para este cliente de 1.83 Mbps, que equivale a un rendimiento de 89.36%.

Para verificar que existe simetría en el enlace, se repitió la medición desde la Sede B, que se muestra en la figura 4-4.

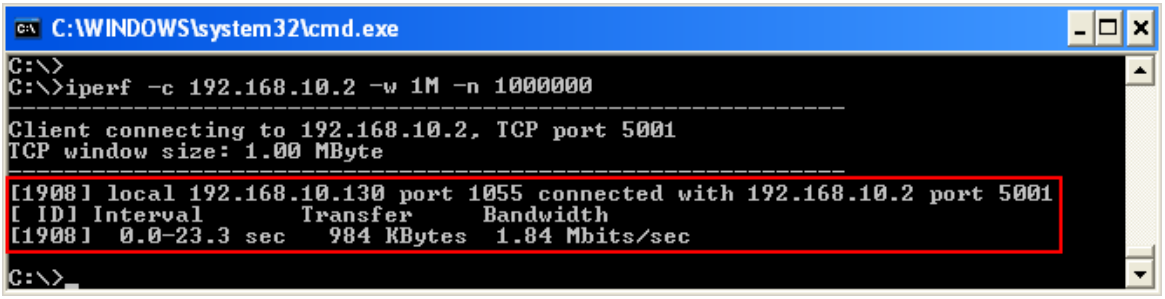

FIGURA 4-4 ANCHO DE BANDA CON 1 CONEXIÓN DESDE SEDE B (MODELO 1)

Fuente: "Elaboración Propia"

Para la prueba de utilización del CPU, se reinició la sesión BGP en los routers ASBR, y se observó un porcentaje de uso del CPU mayor al normal. La figura 4-5 muestra un valor máximo del 13% en el router ASBR2, mientras que la utilización normal del CPU oscila entre 1% y 3%.

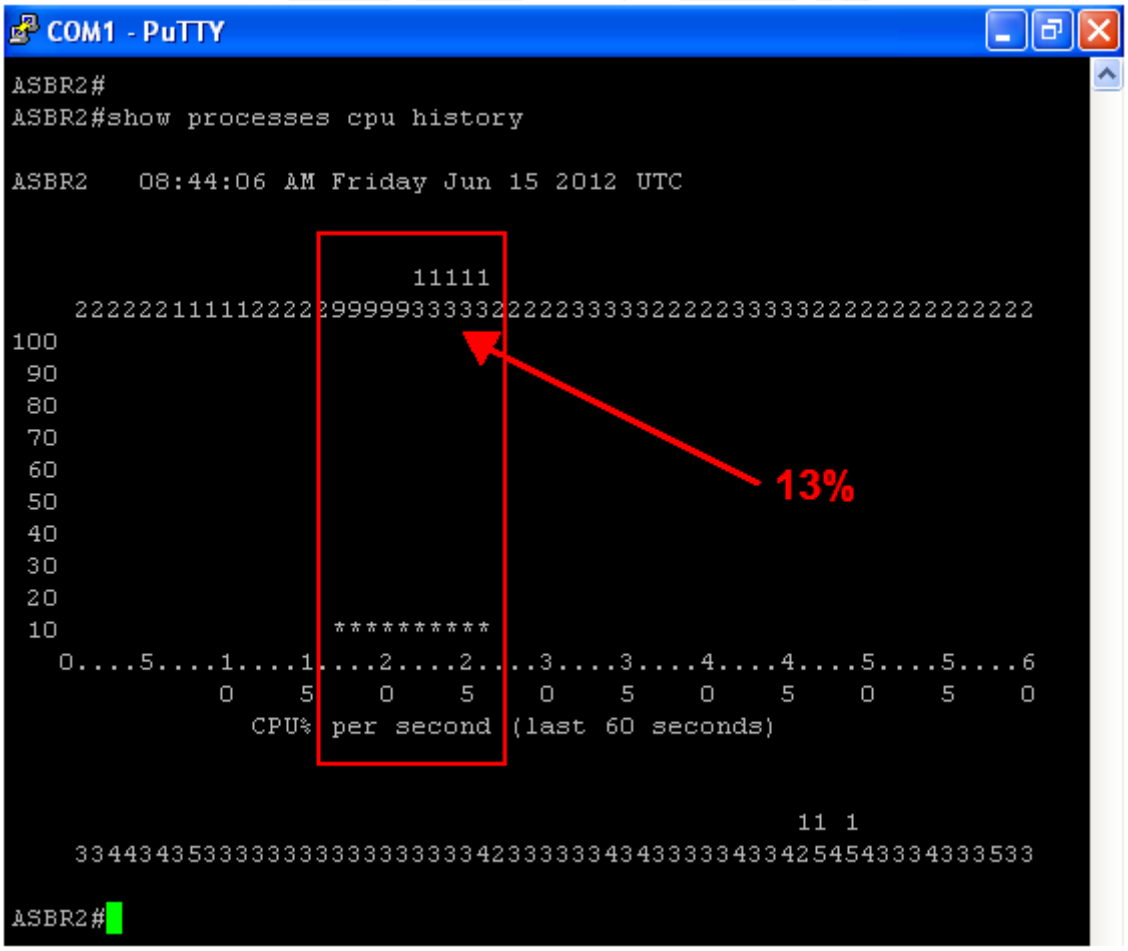

FIGURA 4-5 USO DEL CPU CON REINICIO BGP (MODELO 1)

Fuente: "Elaboración Propia"

Para las pruebas 2 y 3, se inyectó tráfico en la red de extremo a extremo. Con la ayuda del software generador de tráfico, se simularon 10 conexiones para la prueba 2, y 20 conexiones para la prueba 3. La figura 4-6 muestra como ejemplo la interfaz del generador Traffic durante la prueba 3 en el modelo 1.

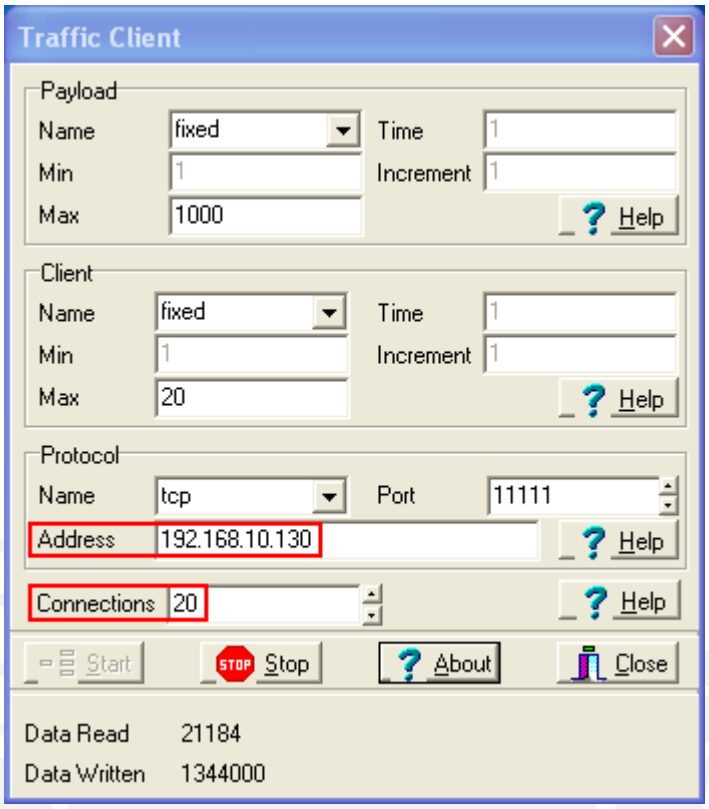

FIGURA 4-6 GENERADOR DE TRAFICO CON 20 CONEXIONES (MODELO 1)

Fuente: "Elaboración Propia"

La figura 4-7 muestra a continuación el comportamiento del CPU durante las tres pruebas realizadas.

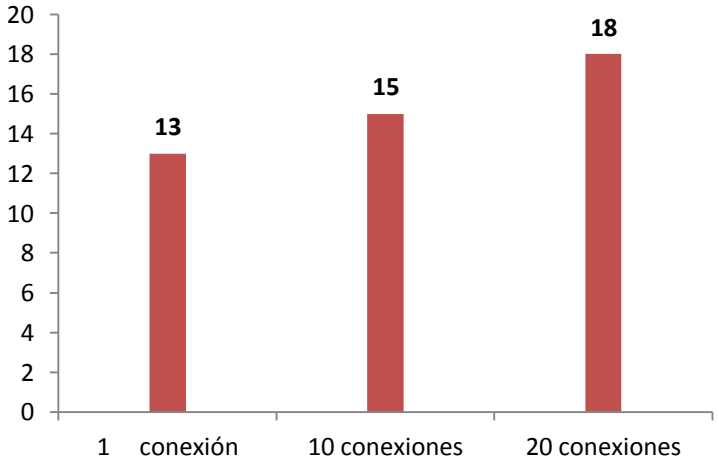

FIGURA 4-7 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 1

Fuente: "Elaboración Propia"

Para medir el tiempo de convergencia, se reinició la sesión BGP en el router ASBR1. En ese momento el sniffer conectado al router, que ya había iniciado la captura de tramas segundos antes, muestra las tramas BGP que anuncian las rutas. El primer mensaje BGP OPEN llega a los 22.57 segundos de iniciada la captura y anuncia la loopback 10.10.10.101 que identifica al router ASRB1. La figura 4-8 muestra dicha trama.

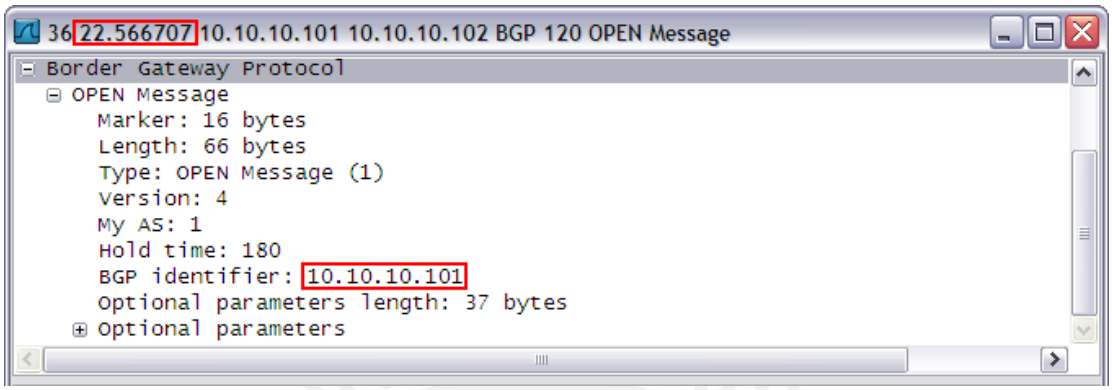

FIGURA 4-8 PRIMER MENSAJE BGP OPEN (MODELO 1)

Fuente: "Elaboración Propia"

De igual forma, el último mensaje BGP UPDATE llega a los 102.61 segundos de iniciada la captura. Anuncia la ruta para la Sede B del Cliente 2 y tiene una etiqueta asignada única con valor 76. La trama es mostrada en la figura 4-9.

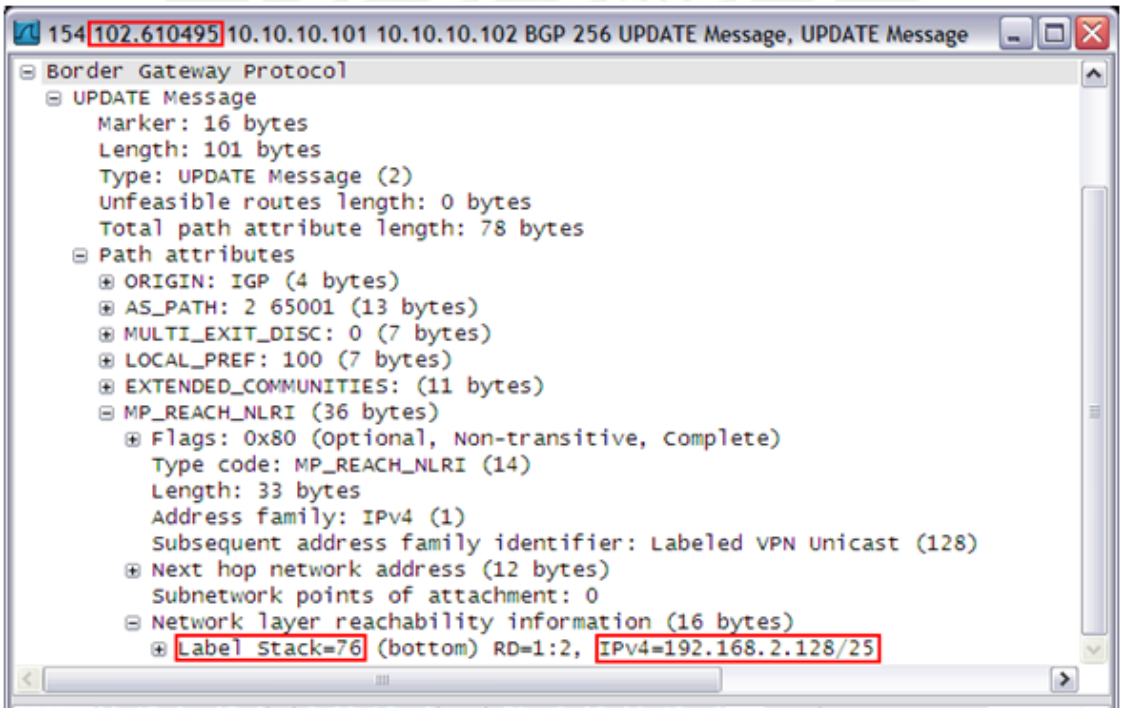

FIGURA 4-9 ÚLTIMO UPDATE BGP (MODELO 1)

Fuente: "Elaboración Propia"

De las pruebas anteriores, se obtiene que el tiempo total de convergencia de la sesión BGP en la red con veinte conexiones habilitadas es 80.04 segundos.

Una vez establecida la sesión y distribuidas todas la rutas, se puede apreciar que los ASBRs conocen ambas sedes de los clientes. En la figura 4-10 se muestra el caso del Cliente 7 (notar que hay una VRF configurada en el router para este cliente).

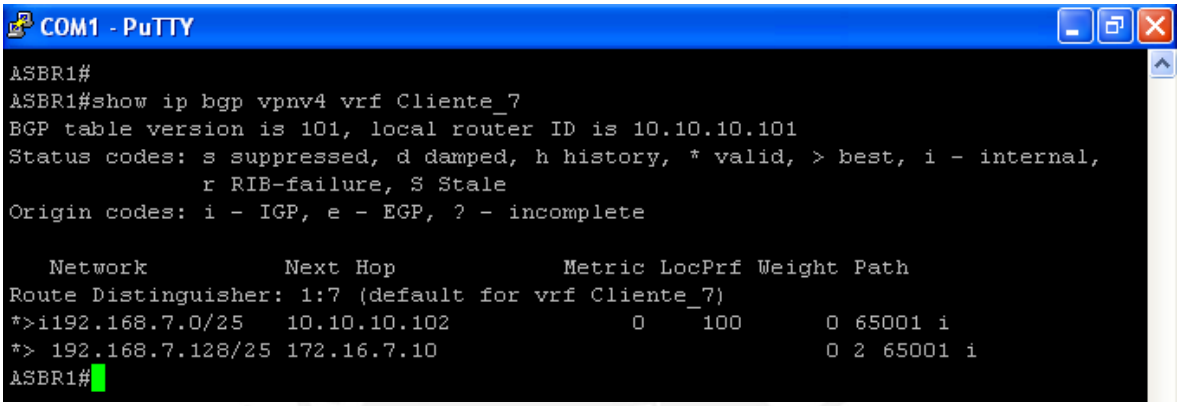

FIGURA 4-10 TABLA VRF DEL CLIENTE 7 (MODELO 1)

Fuente: "Elaboración Propia"

Luego se realizaron las mismas mediciones que en la prueba 1 en estas nuevas condiciones. La tabla 4-1 muestra los resultados luego de las 3 pruebas.

TABLA 4-1 RESULTADOS DE PRUEBAS MODELO 1

Fuente: "Elaboración Propia"

Modelo 1	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	95	8.55	89.36	13	16.42
Prueba 2	10	517	190.15	35.21	15	43.95
Prueba 3	20	1359	502.33	25.19	18	80.04

4.2.1.1. Análisis del etiquetado de paquetes

A continuación se analizará el etiquetado para el modelo 1. Se muestran las etiquetas en los routers que forman parte del LSP desde la sede A hacia la sede B para el caso el cliente 10. La figura 4-11 muestra las etiquetas VPNv4 y LDP en el router PE1 como 67 y 16, respectivamente. Además, se aprecia la etiqueta LDP de salida como "Pop Label". Esto se debe a que la etiqueta es retirada al salir del router porque el siguiente salto, el router ASBR, es un router de borde que ya no se basará en el etiquetado para enviar el paquete al AS vecino. Este proceso se denomina PHP (Penultimate Hop Popping).

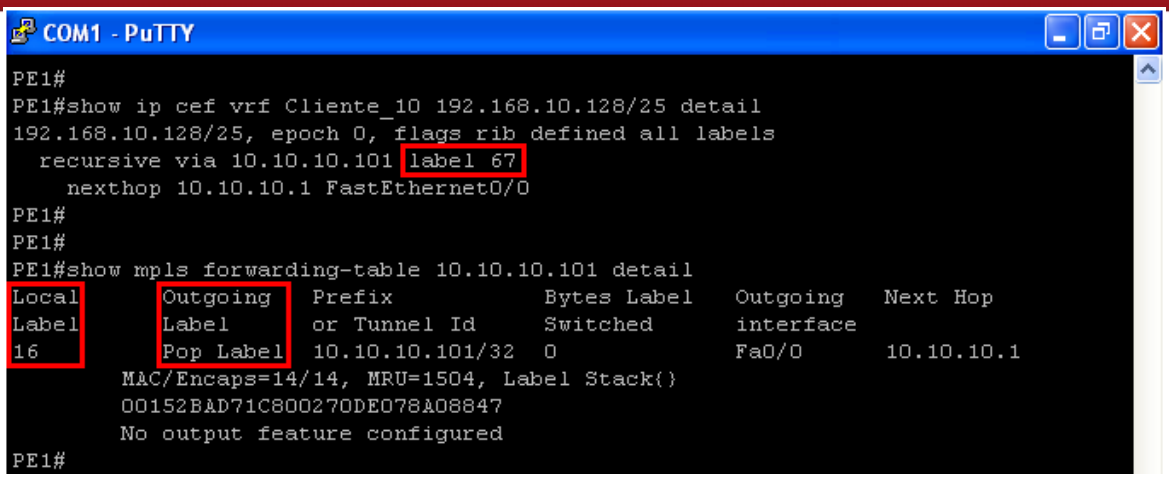

FIGURA 4-11 ETIQUETADO EN EL ROUTER PE1 (MODELO 1)

Fuente: "Elaboración Propia"

La figura 4-12 muestra que la etiqueta VPNv4 es retirada al salir del router ASBR1. Este router no cuenta con etiqueta LDP de salida para el LSP desde la sede A hacia la sede B ya que el siguiente salto corresponde al router ASBR2. Como se menciona en la descripción del modelo, entre los ASBRs no hay MPLS implementado y el enrutamiento se realiza basándose en la información de Capa 3.

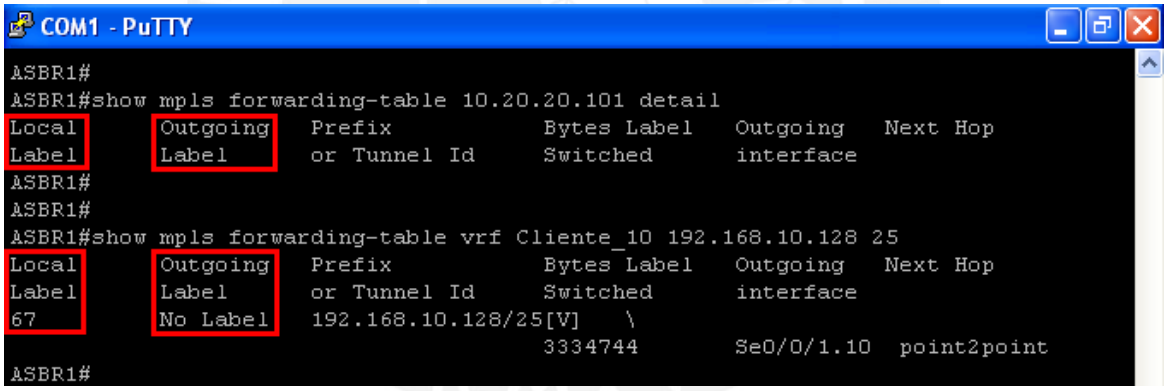

FIGURA 4-12 ETIQUETADO EN EL ROUTER ASBR1 (MODELO 1)

Fuente: "Elaboración Propia"

Al llegar al AS vecino, el router ASBR2 asigna nuevamente las etiquetas VPNv4 y LDP al paquete. También se aprecia el proceso PHP en este router, ya que la etiqueta LDP de salida figura como "Pop Label" porque el siguiente salto, el router PE2, es un router de borde. La figura 4-13 muestra dichas etiquetas.

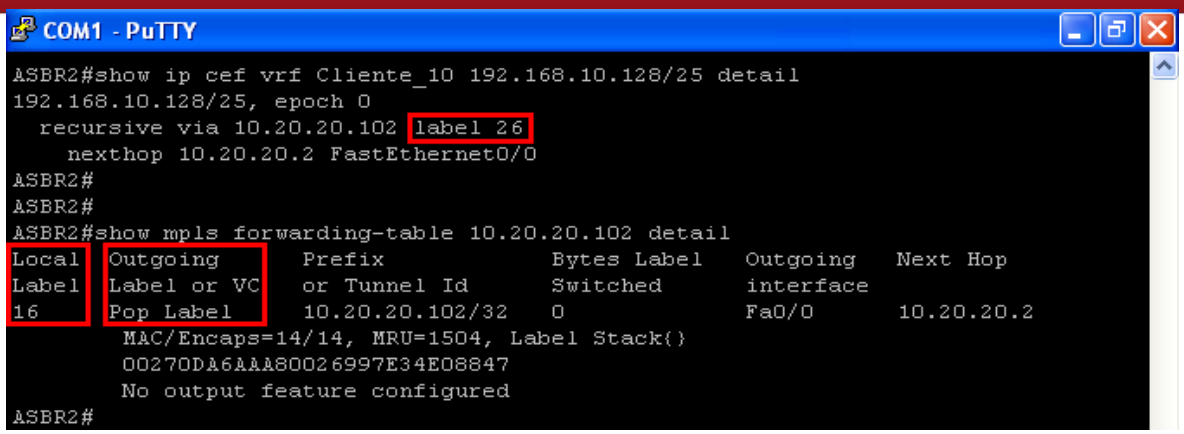

FIGURA 4-13 ETIQUETADO EN EL ROUTER ASBR2 (MODELO 1)

Fuente: “Elaboración Propia”

Al llegar al router PE2, las etiquetas son nuevamente retiradas para que el paquete sea enviado al router CE2 a través del enrutamiento IP. Esto se muestra en la figura 4-14.

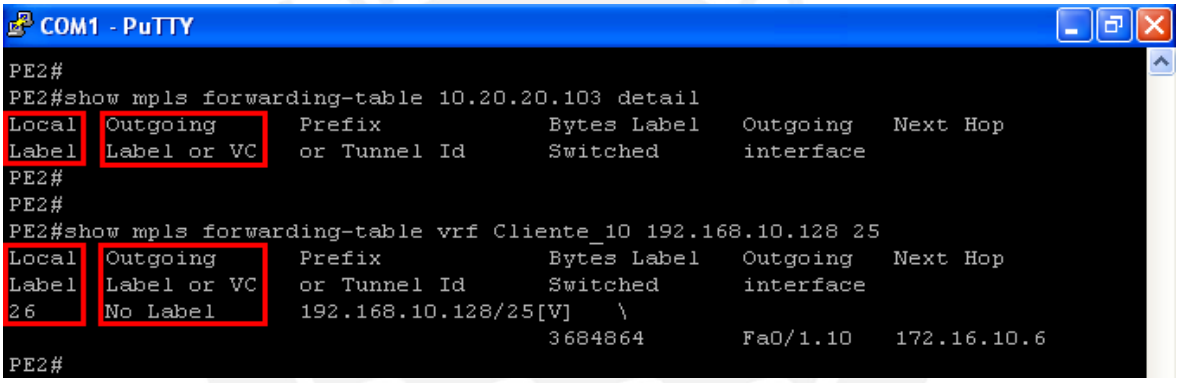

FIGURA 4-14 ETIQUETADO EN EL ROUTER PE2 (MODELO 1)

Fuente: “Elaboración Propia”

De esta forma se completa el etiquetado a lo largo de la red. Se debe notar que entre los proveedores no existe intercambio de etiquetas, ya que cada ASBR trata a su par como si fuera un CE. Tambien se debe tener en cuenta que en el caso de que el paquete vaya desde la sede B hacia la sede A, el etiquetado será diferente pues se tratan de LSPs distintos. La figura 4-15 resume el proceso.

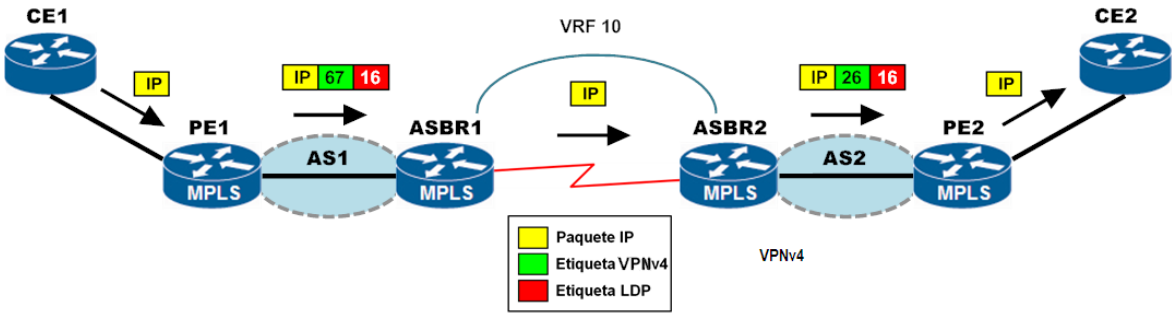

FIGURA 4-15 ETIQUETADO PARA EL CLIENTE 10 EN EL MODELO 1

Fuente: “Elaboración Propia”

4.2.2 Modelo 2: MP-eBGP

Para esta implementación, se han considerado 2 routers para cada proveedor. Al igual que en caso anterior, se simularon los routers CE por computadora, donde están configurados con Multi-VRF. Como se indica en la figura, ya no hay VRFs configuradas entre los proveedores. Ya que esta implementación cuenta con 3 submodelos, se realizaron las pruebas a cada uno de ellos. La figura 4-16 ilustra el modelo general.

2a – Next-hop-self

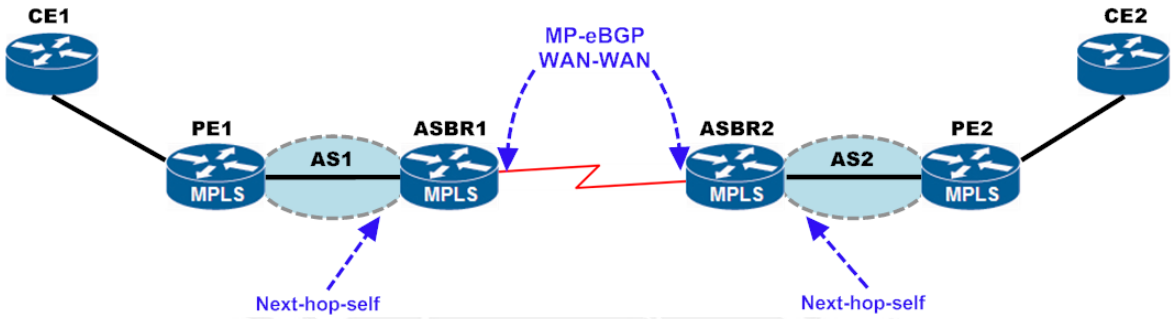

FIGURA 4-16 IMPLEMENTACIÓN MODELO 2A

Fuente: "Elaboración Propia"

La validación de conectividad inicial es similar para todos los casos. Se muestra la medición de la prueba 1 en la figura 4-17.

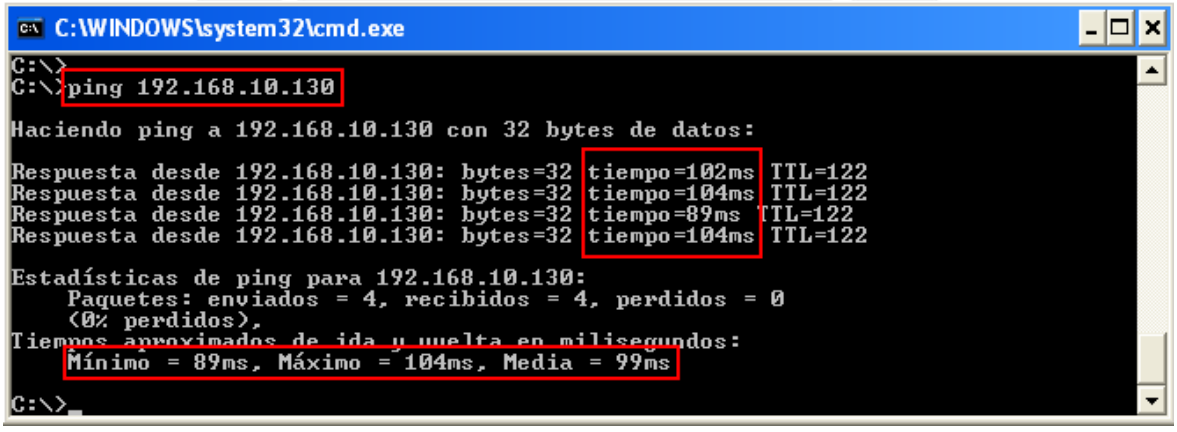

FIGURA 4-17 CONECTIVIDAD ENTRE SEDES (MODELO 2A)

Fuente: "Elaboración Propia"

El retardo es similar al del modelo 1 (valor medio de 99ms) cuando ambas redes se encuentran sin tráfico generado por otros clientes. Sin embargo, al hacer las pruebas con 10 y 20 conexiones cursando tráfico de extremo a extremo los resultados empiezan a variar, como se aprecia en la figura 4-18. El ancho de banda con 20 conexiones es de 723 Kbps, equivalente a un rendimiento de 35.32%.

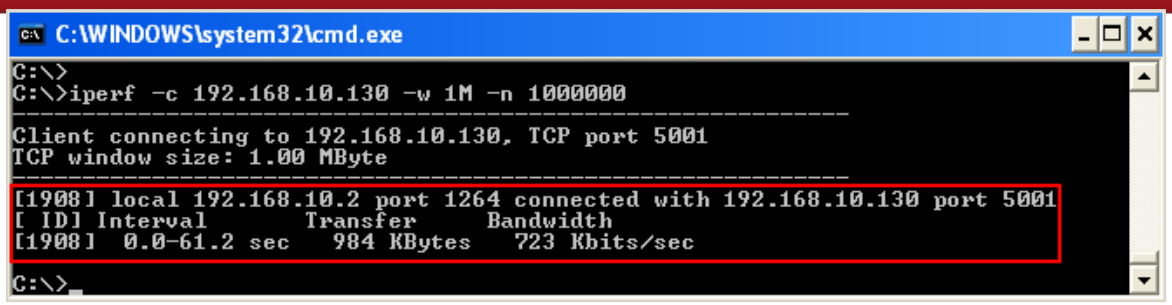

FIGURA 4-18 ANCHO DE BANDA CON 20 CONEXIONES DESDE SEDE A (MODELO 2A)

Fuente: “Elaboración Propia”

La figura 4-19 muestra que también hay una diferencia en la utilización del CPU al reiniciar la sesión BGP.

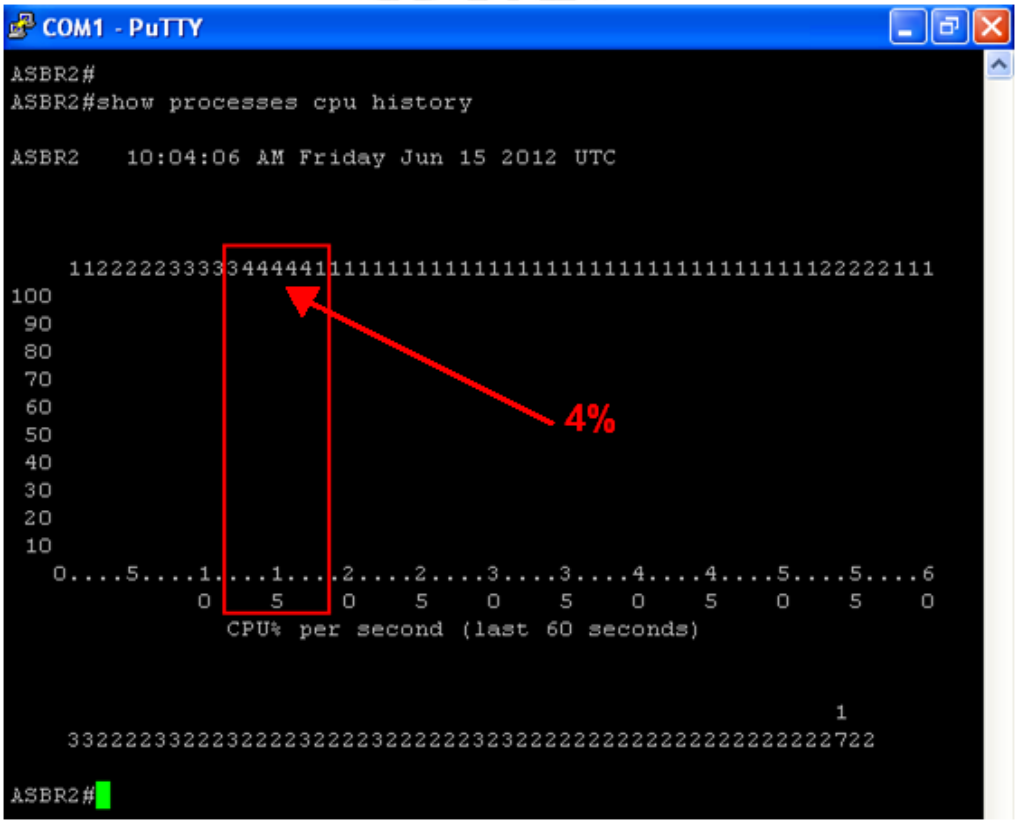

FIGURA 4-19 USO DEL CPU DEL ROUTER ASBR2 CON 20 CONEXIONES (MODELO 2A)

Fuente: “Elaboración Propia”

Para el escenario con 20 conexiones, la utilización del CPU del router no sobrepasa el 4%. La figura 4-20 muestra el comportamiento del CPU durante las 3 pruebas.

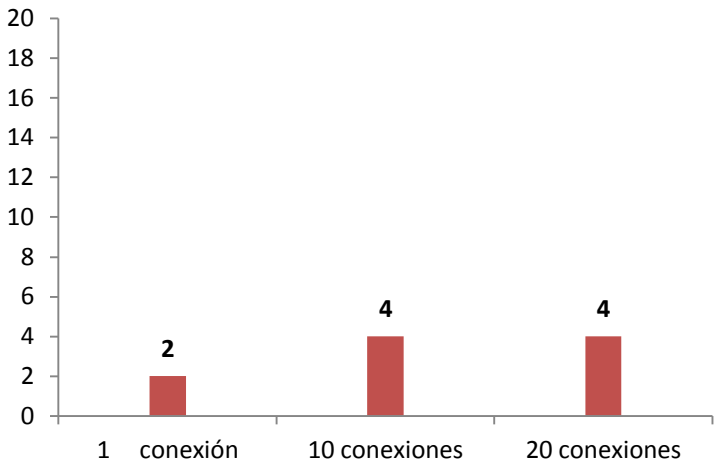

FIGURA 4-20 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 2A

Fuente: "Elaboración Propia"

Además, es importante notar la ausencia de VRFs en los routers ASBR. Como se mencionó en la descripción del modelo, no se necesitan configurar VRFs en la interconexión entre proveedores ya que el intercambio de etiquetas se realiza a través de Multi Protocol BGP. La figura 4-20 muestra la tabla BGP en el router ASBR2.

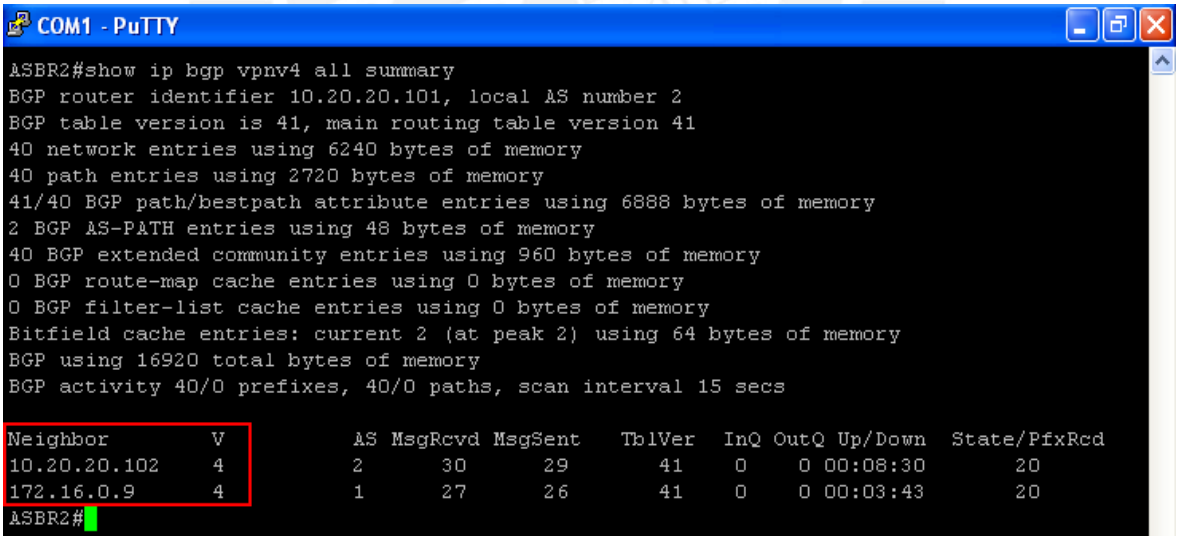

FIGURA 4-21 TABLA VRF EN EL ROUTER ASBR2 (MODELO 2A)

Fuente: "Elaboración Propia"

Los vecinos BGP de cada ASBR son la dirección loopback del PE interno conectado, y la dirección WAN del ASBR remoto.

Las tres pruebas sobre la red (con 1, 10 y 20 conexiones transmitiendo tráfico) arrojaron los resultados mostrados en la tabla 4-2.

TABLA 4-2 RESULTADOS DE PRUEBAS MODELO 2A

Fuente: "Elaboración Propia"

Modelo 2a	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	99	7.23	93.75	2	2.84
Prueba 2	10	320	124.71	52.73	4	36.06
Prueba 3	20	1883	208.09	35.32	4	64.85

2b – Redistribute connected

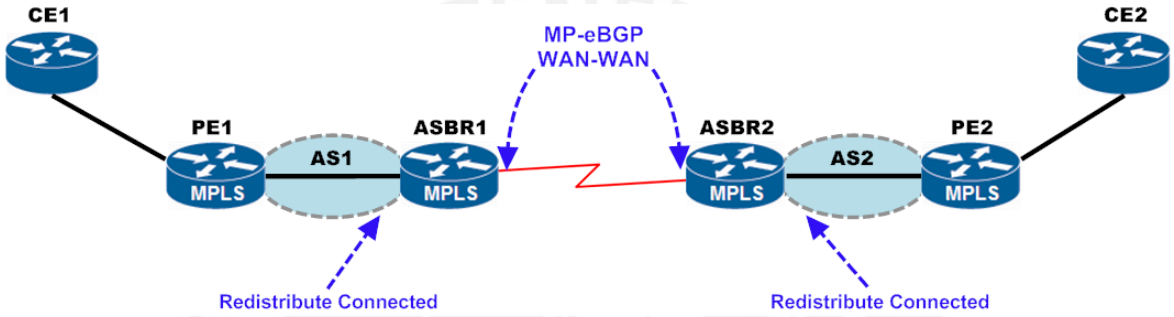

FIGURA 4-22 IMPLEMENTACIÓN MODELO 2B

Fuente: "Elaboración Propia"

Este submodelo presentó valores comparables con los anteriores en cuanto a retardo y jitter. Sin embargo, el ancho de banda disponible es mayor aún cuando se realiza la prueba de mayor stress (tráfico generado simulando 20 conexiones), con un valor de 928 Kbps, que equivale a un rendimiento de 45.33%. Esto se aprecia en la figura 4-23.

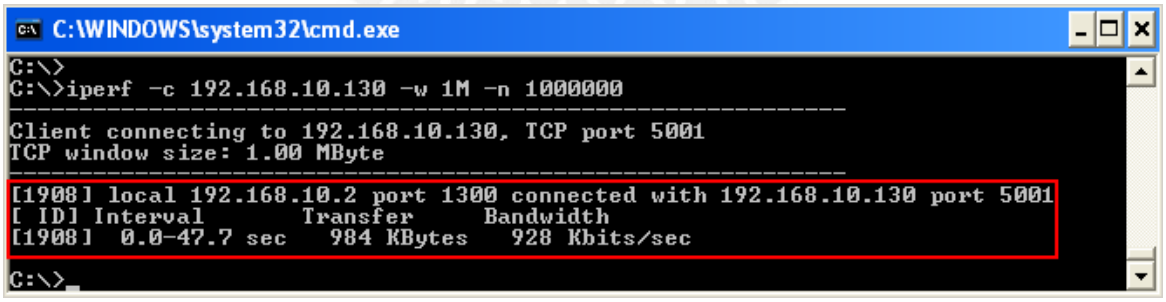

FIGURA 4-23 ANCHO DE BANDA CON 20 CONEXIONES DESDE SEDE A (MODELO 2B)

Fuente: "Elaboración Propia"

La medición del tiempo de convergencia arrojó mejores resultados que el primer submodelo. La figura 4-24 muestra la primera trama BGP OPEN durante la tercera medición, y anuncia la dirección 10.20.20.101 que identifica al router ASBR2 dentro de la sesión BGP.

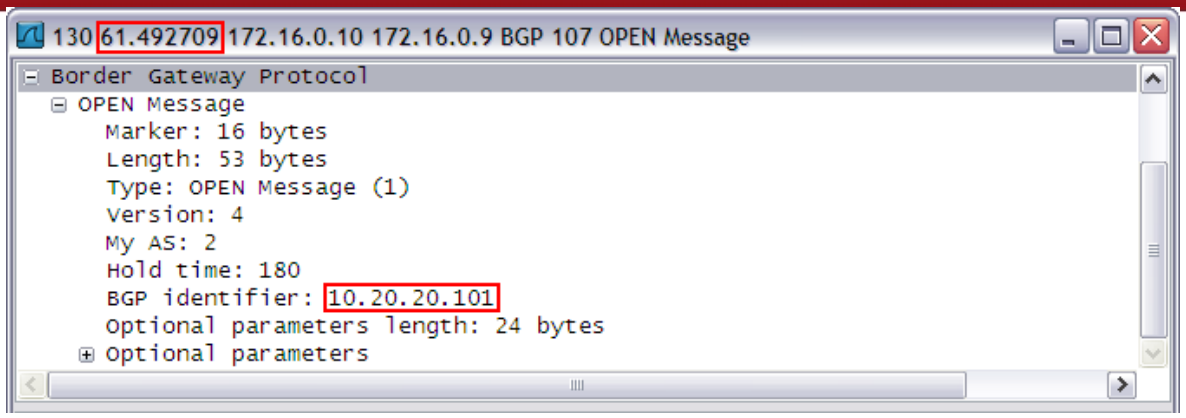

FIGURA 4-24 PRIMER MENSAJE BGP OPEN (MODELO 2B)

Fuente: “Elaboración Propia”

La figura 4-25 muestra la ultima trama BGP UPDATE, la cual anuncia la ruta de la sede B del cliente 18.

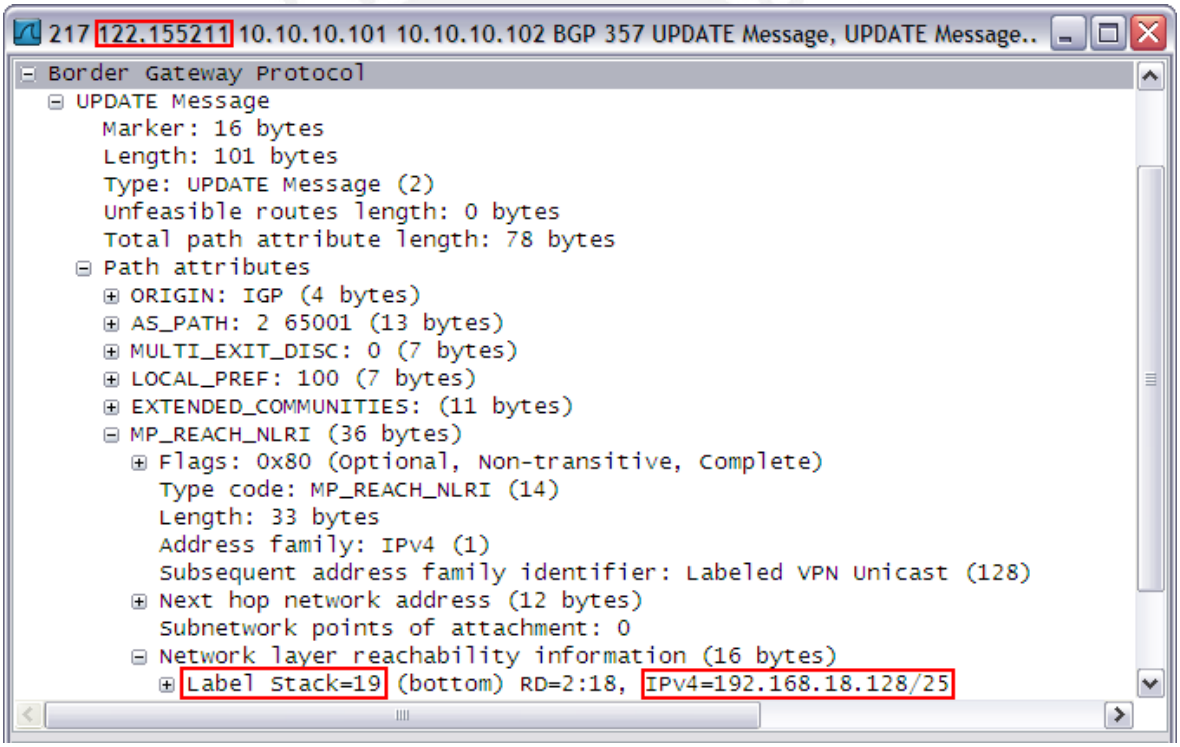

FIGURA 4-25 ULTIMO UPDATE BGP (MODELO 2B)

Fuente: “Elaboración Propia”

El uso del CPU para este caso fue similar al del primer submodelo. La figura 4-26 muestra el comportamiento del CPU durante las 3 pruebas.

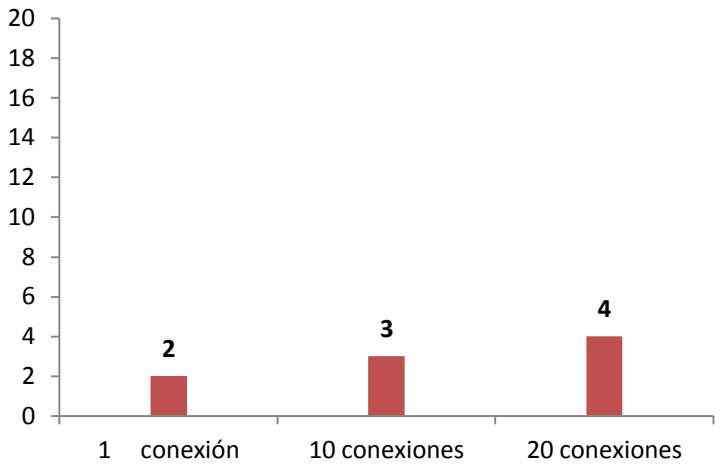

FIGURA 4-26 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 2B

Fuente: "Elaboración Propia"

La tabla 4-3 muestra los resultados de todas las pruebas realizadas en el submodelo 2b.

TABLA 4-3 RESULTADOS DE PRUEBAS MODELO 2B

Fuente: "Elaboración Propia"

Modelo 2b	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	101	10.95	93.75	2	2.75
Prueba 2	10	377	95.69	59.57	3	36.98
Prueba 3	20	1869	197.28	45.33	4	60.66

2c – eBGP entre ASBRs y MP-eBGP entre RRs

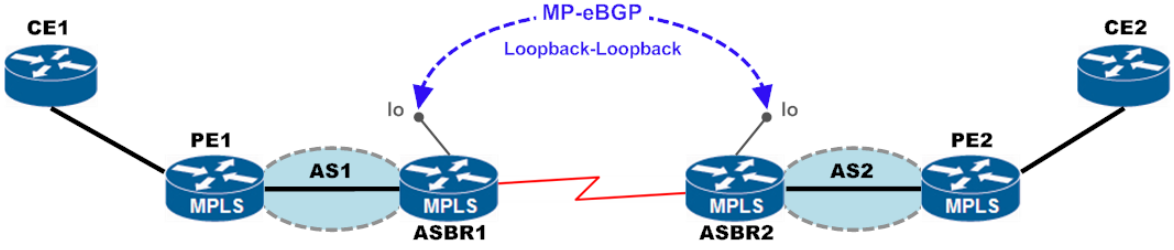

FIGURA 4-27 IMPLEMENTACION MODELO 2C

Fuente: "Elaboración Propia"

Este último submodelo, presentó resultados más distantes de los submodelos previos. La figura 4-28 muestra la medición de los tiempos de respuesta, donde se aprecia un retardo promedio menor que en los casos anteriores para la prueba con 20 conexiones.

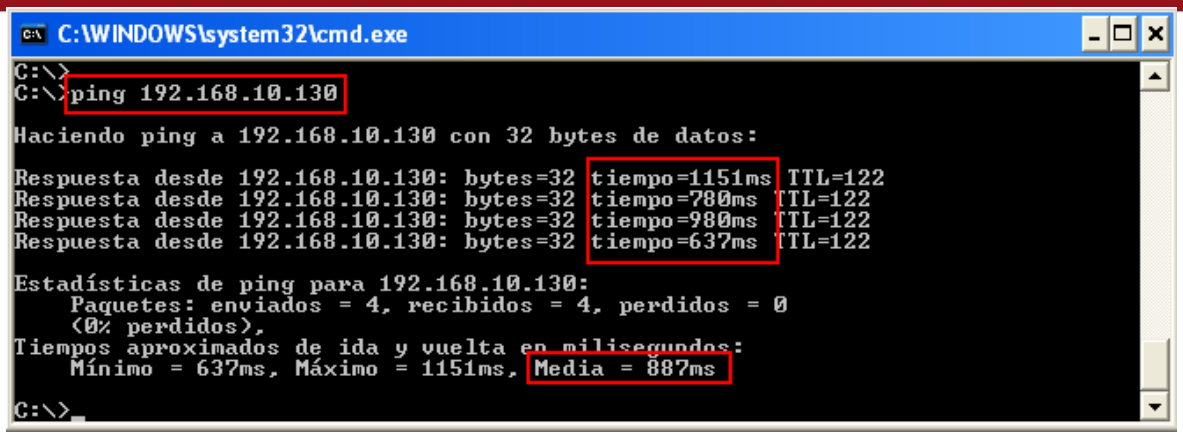

FIGURA 4-28 CONECTIVIDAD ENTRE SEDES MODELO 2C

Fuente: "Elaboración Propia"

También se muestran las pruebas de la medición del tiempo de convergencia de la sesión BGP. La figura 4-29 muestra el primer mensaje BGP OPEN que anuncia la dirección 10.20.20.101 como identificativo del router ASBR2 dentro de la sesión BGP.

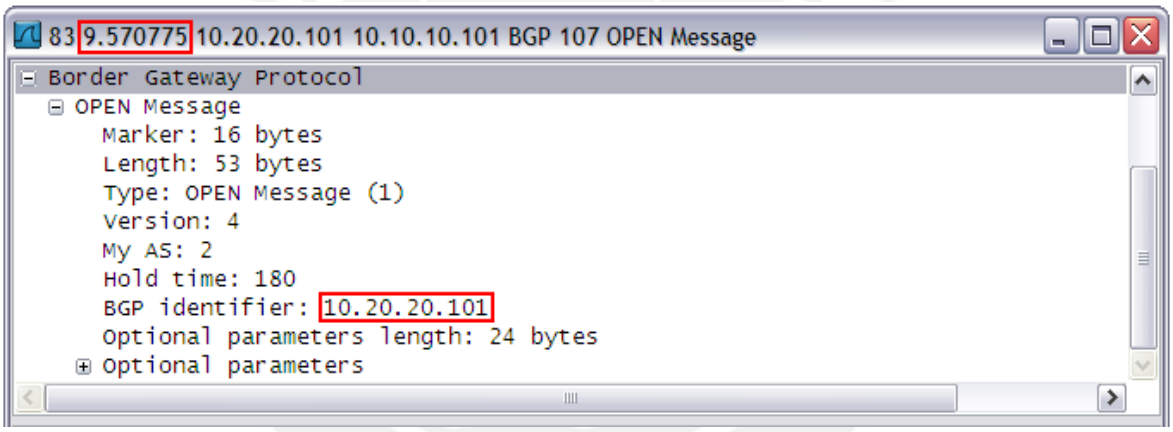

FIGURA 4-29 PRIMER MENSAJE BGP OPEN (MODELO 2C)

Fuente: "Elaboración Propia"

La figura 4-30 muestra la trama del último UPDATE BGP que anuncia la ruta de la sede B del cliente número 20. Con esta trama se termina el proceso de convergencia BGP.

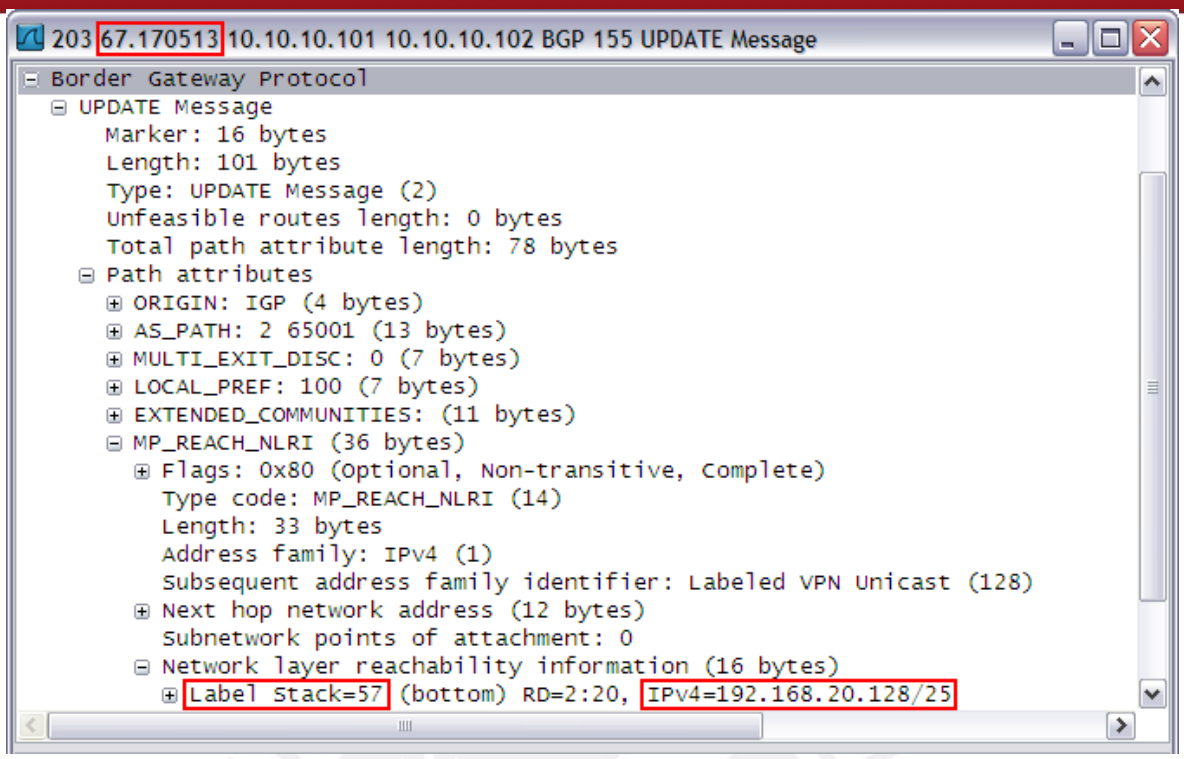

FIGURA 4-30 ULTIMO UPDATE BGP (MODELO 2C)

Fuente: “Elaboración Propia”

La figura 4-31 muestra un porcentaje de uso del CPU del 5%, el cual se repite en las 3 pruebas. El tiempo de convergencia con 20 conexiones es 57.60 segundos.

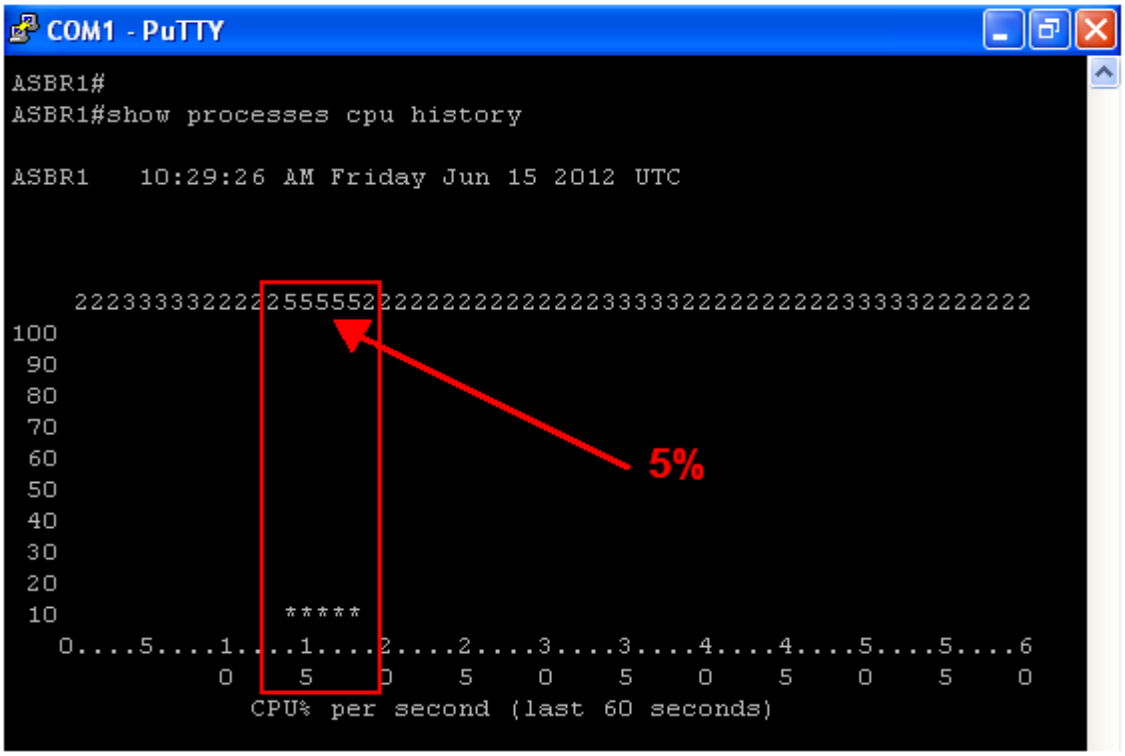

FIGURA 4-31 USO DEL CPU (MODELO 2C)

Fuente: “Elaboración Propia”

En la figura 4-32 se muestran los valores del uso del CPU durante las 3 pruebas realizadas en este modelo.

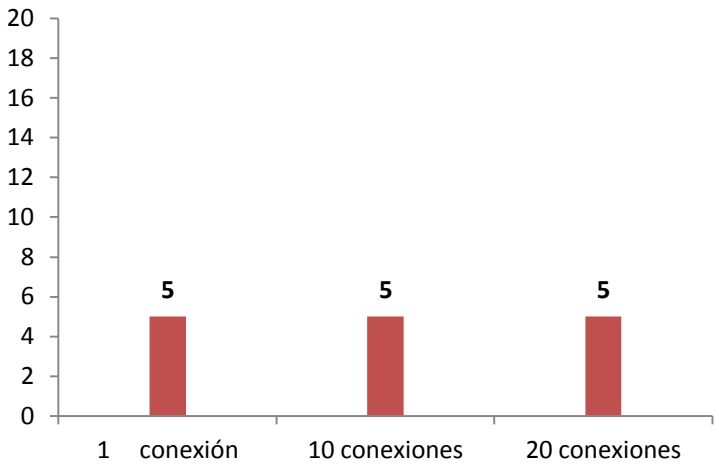

FIGURA 4-32 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 2C

Fuente: "Elaboración Propia"

Los resultados de las pruebas para ese submodelo se muestran en la tabla 4-4.

TABLA 4-4 RESULTADOS DE PRUEBAS MODELO 2C

Fuente: "Elaboración Propia"

Modelo 2c	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	109	6.02	92.29	5	1.95
Prueba 2	10	231	130.73	62.01	5	28.01
Prueba 3	20	887	225.31	36.53	5	57.60

4.2.3 Modelo 3: MP-eBGP Multisalto entre Route Reflectors

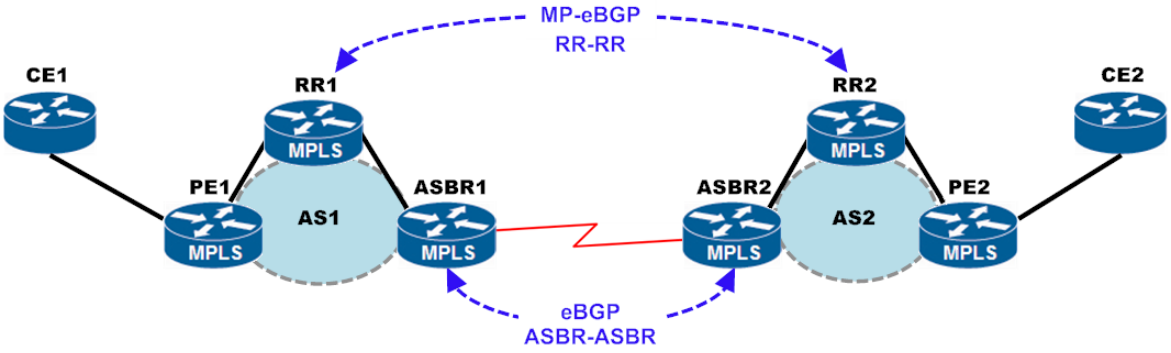

FIGURA 4-33 IMPLEMENTACION DEL MODELO 2C

Fuente: "Elaboración Propia"

Para esta implementación, se han considerado 3 routers para cada proveedor, ya que se agregan los Route Reflectors. La sesión MP-eBGP se establece entre estos dos routers, como se ve en la figura 4-33. Por ello, esta vez el procesamiento de la CPU se medirá en estos routers. Los CE continúan configurados con Multi- VRF.

En la figura 4-34 se ve la ruta que sigue el paquete esta nueva topología.

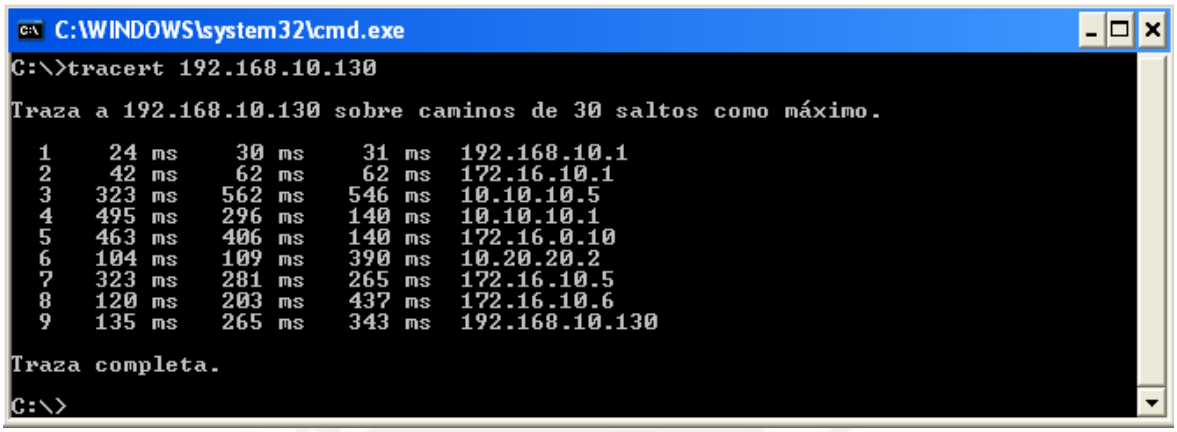

FIGURA 4-34 RUTA DESDE SEDE A HASTA SEDE B (MODELO 3)

Fuente: “Elaboración Propia”

El ancho de banda medido con una sola conexión fue menor a los casos previos. Sin embargo, presentó menos variación conforme se aumentó el número de conexiones, como se aprecia en la figura 4-35. El ancho de banda en el caso más crítico es de 873 Kbps, que es equivalente a un rendimiento de 47.53%.

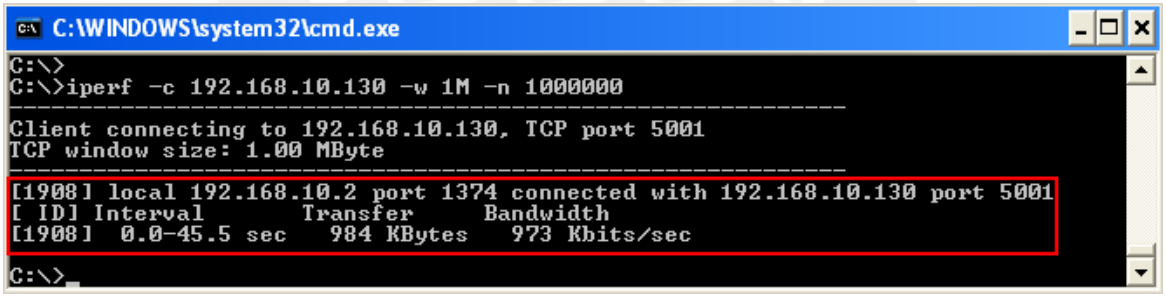

FIGURA 4-35 ANCHO DE BANDA CON 20 CONEXIONES (MODELO 3)

Fuente: “Elaboración Propia”

Además, el sniffer muestra que ahora las rutas son intercambiadas entre los Route Reflectors. Como ejemplo la figura 4-36 muestra una trama enviada desde el Route Reflector 1 hacia el Route Reflector 2 anunciando la ruta de la sede A del cliente 6.

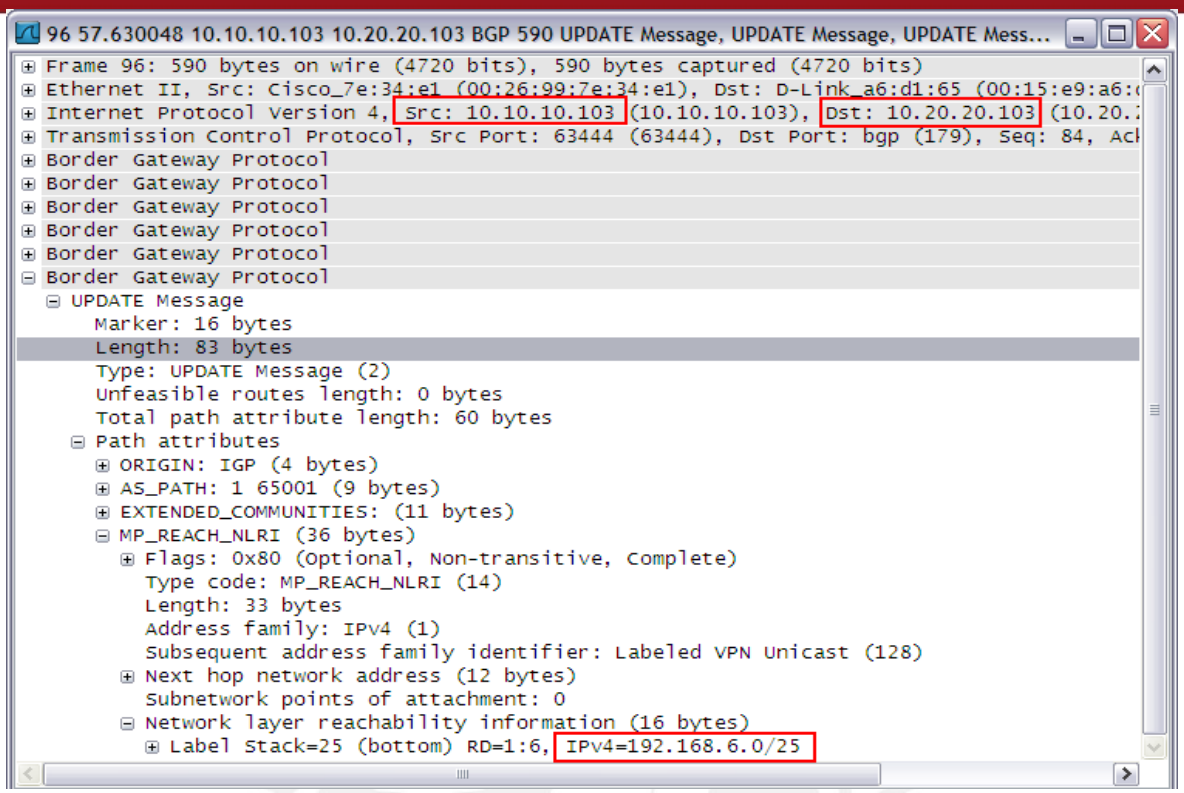

FIGURA 4-36 INTERCAMBIO DE RUTAS ENTRE RRs (MODELO 3)

Fuente: “Elaboración Propia”

En cuanto al uso del CPU, no se observa mayor variación cuando se reinicia la sesión BGP, como se aprecia en la figura 4-37.

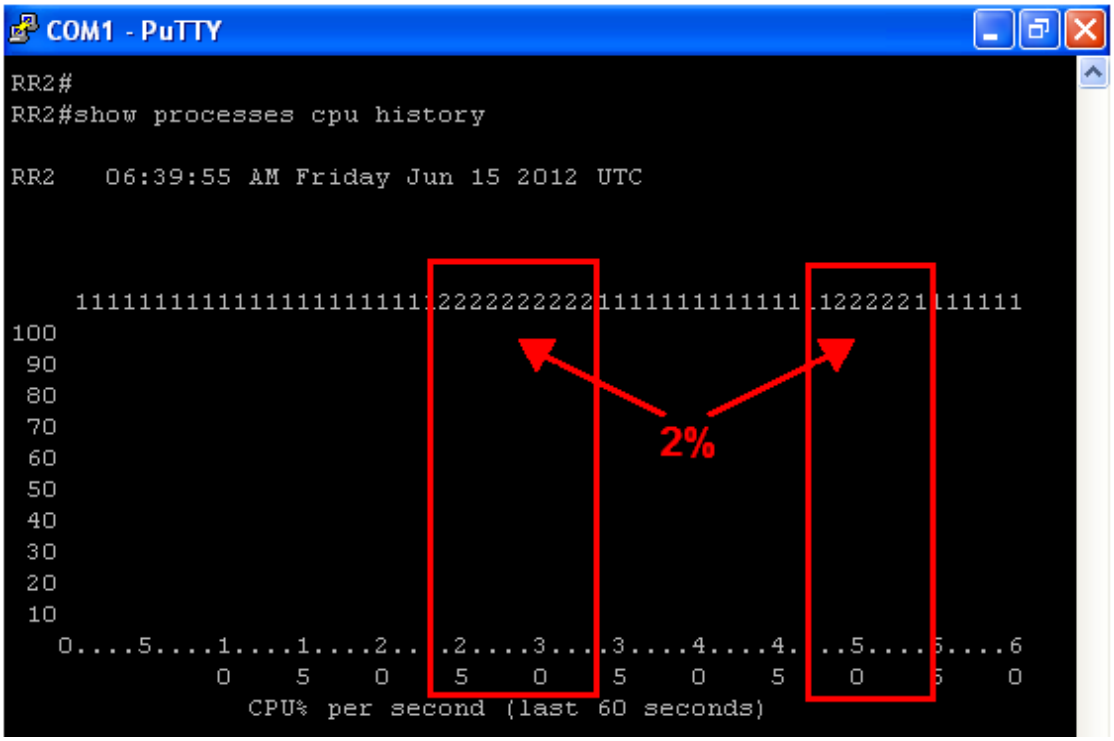

FIGURA 4-37 USO DE CPU (MODELO 3)

Fuente: “Elaboración Propia”

El uso del CPU se mantuvo constante durante las 3 pruebas, como se muestra en la figura 4-38.

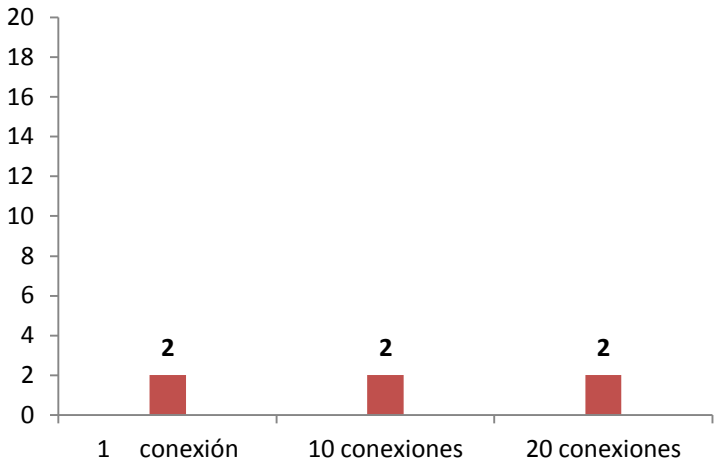

FIGURA 4-38 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 3

Fuente: "Elaboración Propia"

Los resultados completos para este modelo se muestran en la tabla 4-5.

TABLA 4-5 RESULTADOS DE PRUEBAS MODELO 3

Fuente: "Elaboración Propia"

Modelo 3	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	99	10.15	89.84	2	0.62
Prueba 2	10	275	39.01	68.36	2	18.97
Prueba 3	20	628	234.91	47.53	2	41.46

4.2.4 Modelo 4: Proveedor de Tránsito sin VPNs

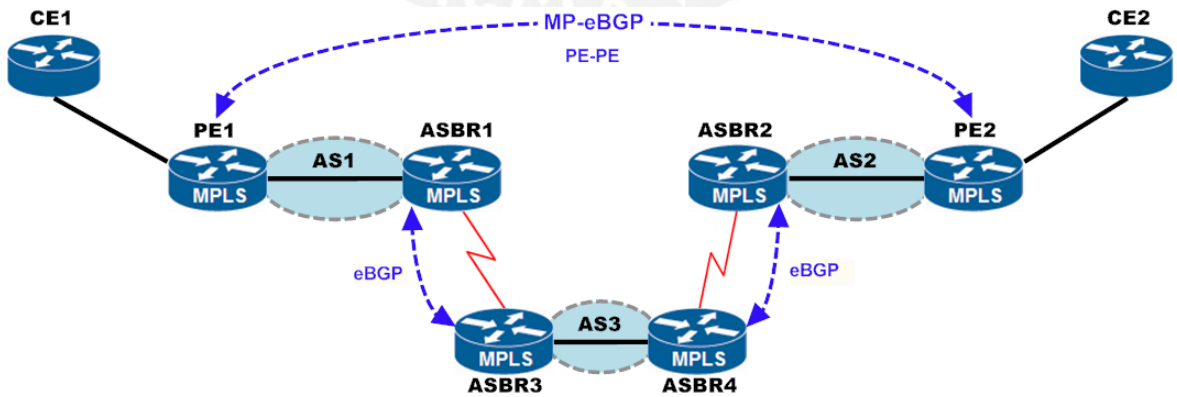

FIGURA 4-39 IMPLEMENTACION DEL MODELO 4

Fuente: "Elaboración Propia"

Esta última implementación incluye un tercer sistema autónomo, y la sesión BGP se establece entre los Route Reflectors de los proveedores VPN. Se determinó que la tarea de RRs también la realizen los routers PE debido a que no se disponen de routers suficientes para implementar la topología tal cual muestra el modelo. Sin embargo, la implementación es válida para fines de prueba ya que no se consume la totalidad de los recursos de los routers PE. Además, la medición del CPU se hizo en los routers PE ya que son los que intercambian las rutas a través de MP-eBGP. La primera prueba de conectividad muestra tiempos de respuesta elevados, como se aprecia en la figura 4-40.

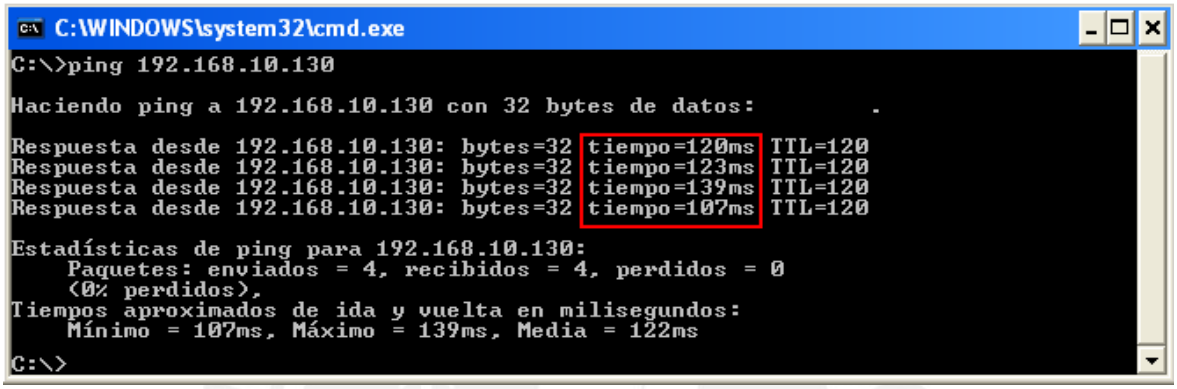

FIGURA 4-40 CONECTIVIDAD DE EXTREMO A EXTREMO (MODELO 4)

Fuente: “Elaboración Propia”

Al reiniciar la sesión BGP, se observa un pico de 10% de uso del CPU. Esta medición corresponde a la prueba sin tráfico. La figura 4-41 muestra este valor en el Router PE1.

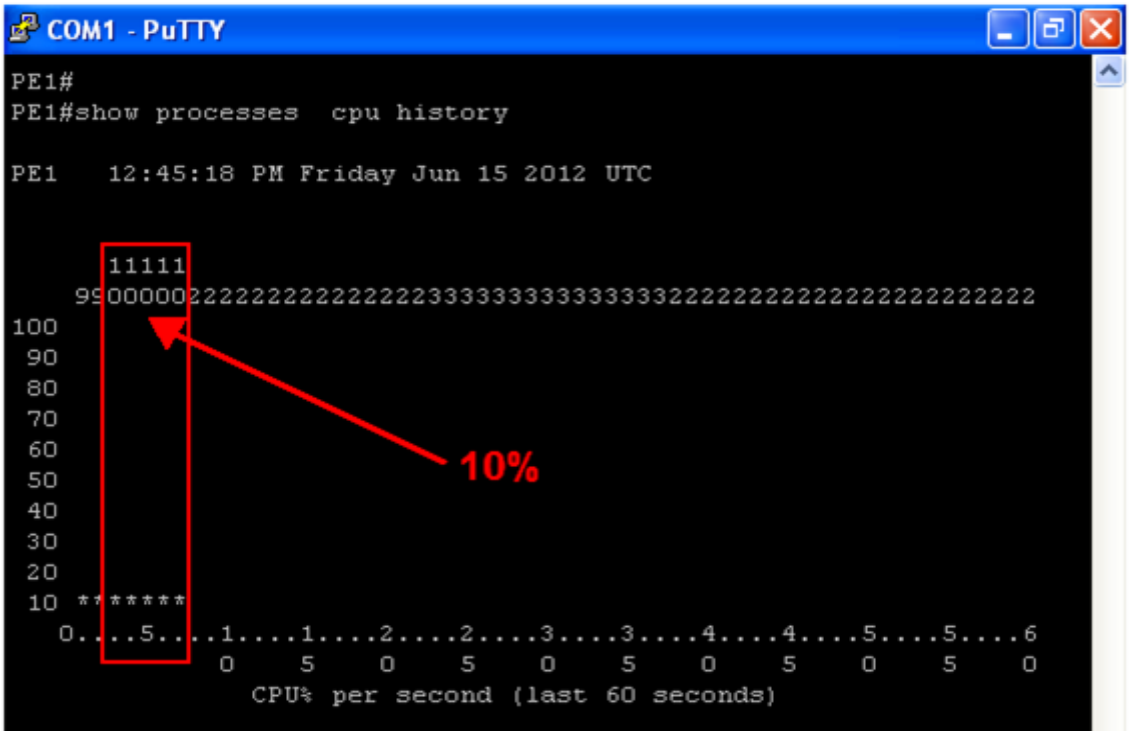

FIGURA 4-41 USO DEL CPU (MODELO 4)

Fuente: “Elaboración Propia”

La figura 4-42 muestra una trama con rutas que son intercambiadas entre los routers PE. Como ejemplo se aprecia la ruta 192.168.6.0/25 (Sede A del Cliente 6) siendo anunciada desde el PE1 hacia el PE2.

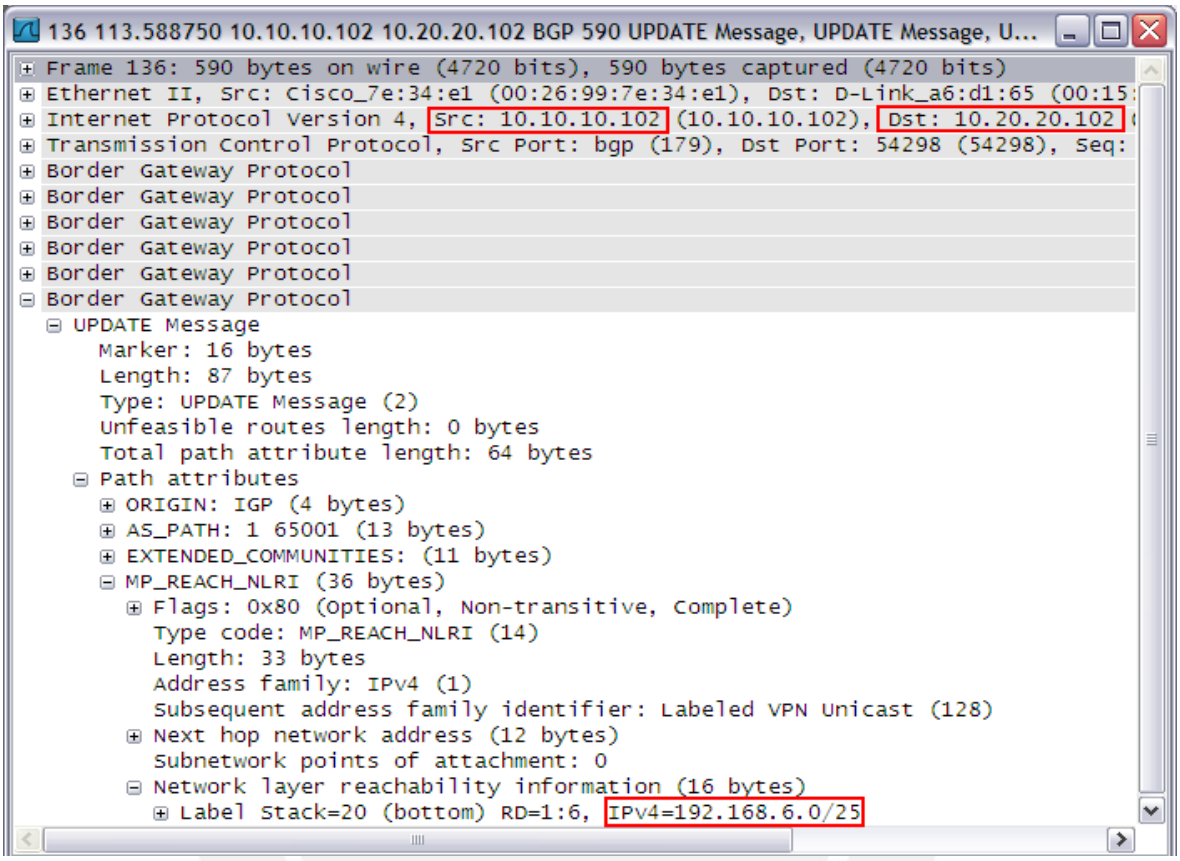

FIGURA 4-42 INTERCAMBIO DE RUTAS ENTRE PEs (MODELO 4)

Fuente: “Elaboración Propia”

En cuanto al uso del CPU, se obtuvieron valores altos en comparación con los casos anteriores, como se puede observar en la figura 4-43.

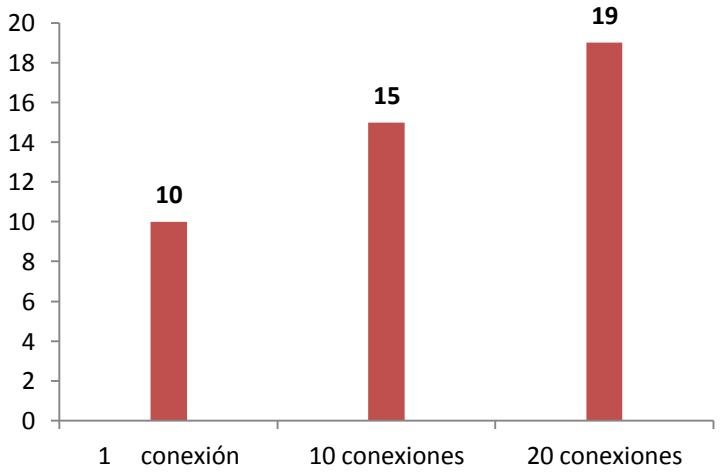

FIGURA 4-43 USO DEL CPU VERSUS NÚMERO DE CONEXIONES PARA EL MODELO 4

Fuente: “Elaboración Propia”

Los resultados de las pruebas hechas para este modelo se muestran en la tabla 4-6.

TABLA 4-6 RESULTADOS DE PRUEBAS MODELO 4

Fuente: “Elaboración Propia”

Modelo 4	# Conexiones	Retardo Medio (ms)	Jitter (ms)	Rendimiento (%)	Uso CPU (%)	Tiempo de Convergencia (s)
Prueba 1	1	122	13.15	92.77	10	1.48
Prueba 2	10	418	254.06	62.99	15	25.50
Prueba 3	20	772	258.91	36.42	19	52.60

4.2.5 Resultados de la Implementación y Pruebas:

De acuerdo a los resultados obtenidos en la sección anterior, los valores de retardo, jitter y ancho de banda disponible resultaron relativamente comparables para todas las implementaciones. Sin embargo, el modelo 3 marca una clara diferencia en cuanto al procesamiento en los routers, ya que el uso del CPU se mantuvo en 2% y los tiempos de convergencia no sobrepasaron los 15 segundos, incluso en el escenario con mayor tráfico.

Otro punto a tomar en cuenta es la escalabilidad que brinda esta implementación. Ya que son los Route Reflectors los encargados de intercambiar la información de rutas de las VPNs, la configuración entre los routers ASBR se hace menos engorrosa, lo que hace más factible el incremento de clientes en el enlace. No es necesario modificar la configuración en la conexión entre proveedores cada vez que se agreguen clientes, lo cual la convierte en una solución muy escalable.

Por tanto, el modelo escogido para la elaboración de la propuesta técnica es el Modelo de Implementación 3: “Multi Protocol eBGP Multisalto entre Route Reflectors. Dicha propuesta será desarrollada en la siguiente parte.

Capítulo 5

Propuesta Técnica

En este capítulo se elaborará la propuesta de implementación de una Multi-AS MPLS-VPN, para la cual utilizaremos el modelo de implementación 3, estudiado previamente.

5.1 Escenario de Implementación

El escenario que se tomará para elaborar la propuesta de la presente tesis consta de los siguientes elementos:

- **Cliente:** Empresa de cualquier rubro, que será la que contrate la Red Privada Virtual que comunique 2 de sus sedes que se encuentran en dos países distintos y fronterizos.
- **Proveedor 1:** Proveedor de servicios de Telecomunicaciones que opera en el país de origen del Cliente, y que es contratado por éste para llevar a cabo la implementación de la VPN.
- **Proveedor 2:** Proveedor de servicios de Telecomunicaciones que opera en el país donde se ubica la sucursal del Cliente, y que es contratado por el Proveedor 1 para proveer el tramo VPN dentro del país donde opera hasta la sucursal.

Cada proveedor cuenta con una red Backbone MPLS que se encuentra distribuida a lo largo de los territorios de los países donde operan. La topología interna de cada Backbone es transparente para los alcances de este estudio.

Se ha tomado el caso de operadores dentro de países fronterizos para poder implementar una solución con dos Sistemas Autónomos. Una VPN que abarque zonas geográficas más grandes posiblemente requiera atravesar más de 2 Sistemas Autónomos.

5.2 Recursos Técnicos

5.2.1 Routers

En cuanto a los equipos de proveedor, se asume que cada uno cuenta con un backbone MPLS, por lo que no es necesaria la adquisición de nuevos equipos para la implementación de la VPN. Lo que si se deberá determinar es los equipos de borde en cada backbone que harán las veces de ASBRs y PEs, así como los equipos que funcionarán como Route Reflectors.

En cuanto a los equipos de cliente, se debe confirmar si este cuenta con routers para conectarse a cada backbone. Como se describió en los capítulos previos, no es necesario que los routers soporten MPLS. De no contar con ellos, se acordará con el cliente si la adquisición del router será a cuenta suya o será parte del servicio de implementación de la VPN.

5.2.2 Protocolos y Métodos a Emplearse

La configuración abarcará el establecimiento de la sesión MP-eBGP entre RRs, la conectividad de ASBRs, y la configuración de VRFs en los PEs, Para ese propósito se utilizarán los siguientes protocolos:

- eBGP para la comunicación entre los routers de borde ASBR.
- MP-eBGP para la comunicación entre los Route Reflectors RR.
- eBGP e instalación de rutas VRF en los equipos PE.
- iBGP para distribuir las rutas externas en el backbone.

En caso de que el cliente también contrate el servicio de configuración de sus routers, se emplearán los siguientes protocolos:

- OSPF como protocolo de enrutamiento interno debido a su configuración sencilla y escalabilidad. Una alternativa similar es el protocolo IS-IS.
- eBGP para anunciar las rutas hacia los proveedores.
- iBGP para aprender las rutas que los proveedores le anuncien.

5.2.3 Enlaces

Se deben implementar enlaces físicos que interconecten las redes de proveedores y la del cliente. Los enlaces son los siguientes:

- Para la conexión entre Proveedores, se empleará un enlace serial.
- Para las conexiones entre el Cliente y cada Proveedor, se emplearán enlaces Fast-Ethernet.

5.2.4 Plan de Direccionamiento IP

Al ser una VPN, las direcciones IP utilizadas serán privadas. La tabla 5-1 muestra los rangos utilizados en esta propuesta.

TABLA 5-1 DIRECCIONAMIENTO IP

Fuente: "Elaboración Propia"

RANGO	MASCARA	CLASE	USO
172.16.0.0	255.255.255.252	B	Conexión PE-CE Sede Principal
172.16.0.4	255.255.255.252	B	Conexión ASBR-ASBR
172.16.0.8	255.255.255.252	B	Conexión PE-CE Sucursal
192.168.0.0	255.255.0.0	C	Red LAN de Cliente

Topología de la Red Propuesta

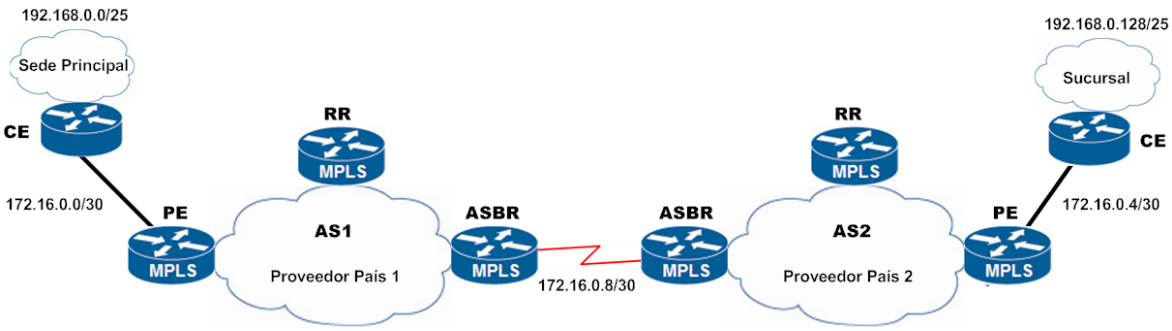

FIGURA 5-1 TOPOLOGÍA PROPUESTA

Fuente: "Elaboración Propia"

Como se observa en la figura 5-1, las direcciones propuestas son privadas ya que forman parte de una red que no interactúa directamente con ninguna otra. Las direcciones con los rangos 172.16.0.0, 172.16.0.4 y 172.16.0.8 son utilizadas para las redes WAN, mientras que el rango 192.168.0.0 se ha dividido entre las dos sedes del cliente.

5.3 Plan de Trabajo

A continuación de describen los distintos puntos a tomar en cuenta para llevar a cabo la implementación de la propuesta de VPN.

5.3.1 Etapas del Proyecto

Provisión

Cada proveedor determinará los nodos que se utilizarán en su red para realizar la implementación. Este trabajo supone la búsqueda de puertos libres, definición de los parámetros a utilizar y los servicios que se brindarán por el enlace.

Capacitación del Personal

Se capacitará técnicamente al personal encargado de realizar la implementación de la VPN, de acuerdo a los recursos de red que cada proveedor a asignado para el proyecto.

Implementación en los Proveedores

La configuración en el backbone de cada proveedor estará a cargo de dos equipos, uno para cada backbone. Cada equipo estará formado por dos personas que determinarán los routers que formarán los nodos de la red MPLS-VPN, es decir, los PE, ASBR y RR.

Una vez determinados los equipos, se deberán establecer tanto los PEs y ASBRs como clientes del Route Reflector. Posteriormente se configurarán las VRF en los PEs.

Conectividad entre Proveedores

Se hará el tendido del enlace físico respectivo entre ambos backbones. La conexión se realizará a través de un enlace serial, como se mencionó previamente.

Se establecerá conectividad entre las interfaces físicas de los ASBRs, usando el protocolo eBGP. Una vez logrado, se procederá a establecer la sesión Multi Protocol BGP entre los Route Reflectors.

Implementación en el Cliente

Se realizará el tendido de cableado desde backbones hasta las sedes del cliente. Si es que el cliente así lo haya contratado, se realizará la configuración de los routers CE. Se configurarán los enlaces que conectarán cada sede con el backbone de cada proveedor y se anunciarán las rutas internas deseadas.

Validación de Operatividad y Monitoreo

Finalmente, se verificará la conectividad de extremo a extremo, corroborando el correcto funcionamiento de la MPLS-VPN. Habrá un período de monitoreo de 4 semanas para detectar y corregir posibles fallos que se pudieran presentar.

5.3.2 Desarrollo del Proyecto

Las etapas descritas previamente se realizarán de acuerdo a la tabla 5-2:

TABLA 5-2 TIEMPOS ESTIMADOS DEL PROYECTO

Fuente: “Información Corporativa” [MAY2012]

ETAPA	DURACIÓN
Provisión	1 Semana
Capacitación del Personal	1 Semana
Implementación en los Proveedores	2 Días
Conectividad entre Proveedores	3 Días
Implementación en el Cliente	3 Días
Validación de Operatividad y Monitoreo	2 Semanas
TOTAL	36 Días

5.4 Aspectos Económicos

A continuación se detallan los costos involucrados en la implementación propuesta.

Personal: Teniendo en cuenta que son dos equipos de 2 personas cada uno los que tienen a cargo a implementación, se detalla el costo de la mano de obra calificada considerando un precio de hora-hombre de USD 50. Además, el cableado se hará en grupos de 2 personas, con un precio de hora-hombre de USD 30.

Equipos de Cliente: En caso el cliente no tenga router, se incluirá en el proyecto la adquisición de un router por cada sede. Para este caso, se asumió que el cliente cuenta con 2 sedes por lo que se cotizarán 2 routers. El equipo considerado para este proyecto es el router Cisco 880. Sin embargo, también se pueden considerar alternativas en otras

marcas que soporten los protocolos mencionados en el punto 5.2.2 y que además cuenten con 2 interfaces Fast Ethernet como mínimo.

La tabla 5-3 resume los costos implicados en la propuesta.

TABLA 5-3 COSTOS DE IMPLEMENTACION DEL PROYECTO

Fuente: "Información Corporativa" [MAY2012]

ETAPA	DURACIÓN	HORAS	# PERSONAS	PRECIO HORA/ HOMBRE	COSTO USD
Provisión	1 Semana	40	2	50	4,000
Capacitación de Personal	1 Semana	40	4	50	8,000
Implementación en los Proveedores	2 Días	16	4	50	3,200
Conectividad entre Proveedores					
Configuración	1 Día	8	2	50	800
Cableado	2 Días	16	2	25	800
Implementación en el Cliente					
Configuración	1 Día	8	2	50	800
Cableado	2 Días	16	2	25	800
Validación de Conectividad y Monitoreo	2 Semanas	80	2	25	4,000
TOTAL					**22,400**

El costo total de la propuesta está estimado en USD 22,400. El precio del servicio de instalación para el cliente será de **USD 25,000**. Adicionalmente se cotizan los routers de cliente y el servicio de soporte de 1 año por cada sede. El servicio de soporte será gratuito durante el primer año. La tabla 5-4 describe dicha cotización.

TABLA 5-4 COSTOS DE EQUIPOS Y SOPORTE

Fuente: "Información Corporativa" [MAY2012]

CONCEPTO	COSTO UNITARIO	CANTIDAD	COSTO USD
Router Cisco 880 Series	391	2	782
Soporte y Mantenimiento (Anual)	21600	2	43,200

El costo del personal que realizará el soporte y mantenimiento de los servicios se ha estimado de la siguiente manera: Un técnico por cada sede, con un promedio de 8 horas semanales de asistencia ante incidencias que presente el cliente, lo que resulta en un promedio de 384 horas de soporte anuales. Adicionalmente, se incluyen como costos fijos la capacitación constante del personal y el mantenimiento de herramientas y equipos como los que se brinda el servicio. La tabla 5-5 muestra esta estimación.

TABLA 5-5 COSTOS DEL SERVICIO DE SOPORTE Y MANTENIMIENTO

Fuente: "Elaboración Propia"

CONCEPTO	HORAS POR SEDE	# PERSONAS POR SEDE	PRECIO HORA/ HOMBRE	SEDES	COSTO USD
Soporte y Mantenimiento (Anual)	384	1	20	2	15,360
Costos Fijos Adicionales (Anual)	-	-	-	-	7,200

5.5 Análisis de rentabilidad

En base a la información económica presentada en el apartado anterior, se analizó la rentabilidad del proyecto a 5 años de realizada la implementación de la solución. Como ya se mencionó, el primer año de soporte será gratuito y posteriormente se cobrará por el soporte 4 años más. El soporte completo es de 5 años debido a que ese es el tiempo de vida para equipos de transmisión de datos según lo determinado por la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT.

En la tabla 5-6 se muestra el flujo de caja correspondiente al servicio MPLS-VPN que se propone. Este análisis toma en cuenta el punto de vista del proveedor de servicios, ya que el proyecto consiste en ofrecer una solución MPLS-VPN. Se ha considerado una tasa de costo de oportunidad (TCO) de 10%. Se puede apreciar en el campo del *Flujo Acumulado* que el proyecto es rentable a partir del tercer año desde la implementación.

TABLA 5-6 FLUJO DE CAJA DEL PROYECTO

Fuente: "Elaboración Propia"

CONCEPTO\AÑO	0	1	2	3	4	5
EGRESOS						
2 Routers	782.00					
Personal de provisión	4000.00					
Capacitación de personal	8000.00					
Pago al personal de instalación	10400.00					
Pago al personal de soporte y mantenimiento		15360.00	15360.00	15360.00	15360.00	15360.00
Costos Fijos Adicionales		7200.00	7200.00	7200.00	7200.00	7200.00
TOTAL EGRESOS	23182.00	22560.00	22560.00	22560.00	22560.00	22560.00
INGRESOS						
Servicio total de instalación		25000.00				
Servicio de soporte y mantenimiento			43200.00	43200.00	43200.00	43200.00
TOTAL INGRESOS	**0.00**	**25000.00**	**43200.00**	**43200.00**	**43200.00**	**43200.00**
FLUJO NETO	**-23182.00**	**2440.00**	**20640.00**	**20640.00**	**20640.00**	**20640.00**
FLUJO AL AÑO CERO	**-23182.00**	**2218.18**	**17057.85**	**15507.14**	**14097.40**	**12815.82**
FLUJO ACUMULADO	**-23182.00**	**-20963.82**	**-3905.97**	**11601.17**	**25698.57**	**38514.38**

VAN	**USD 38,514.38**
TIR	**51.18%**

TCO	**10.00%**

En la figura 5-2 se observa el punto de equilibrio del proyecto basado en el servicio de soporte y mantenimiento que se brindará en las sedes del cliente. El cruce entre los costos de personal y el precio del servicio por año se encuentra en 0.5 unidades de servicio. Esto quiere decir que con tan sólo brindar el mantenimiento en una sede es suficiente para cubrir con los costos operativos.

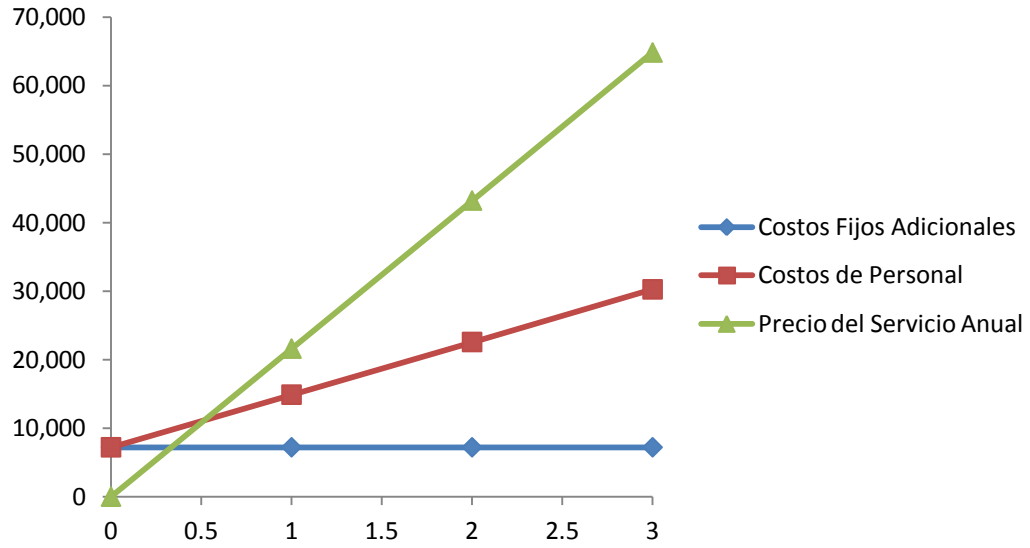

FIGURA 5-2 PUNTO DE EQUILIBRIO

Fuente: "Elaboración Propia"

Adicionalmente, la figura 5-3 muestra el flujo de caja de cada año con respecto al año cero. La inversión inicial es de USD 23,182.00, la cual es recuperada en el primer año en el momento del pago por parte del cliente por la instalación del servicio.

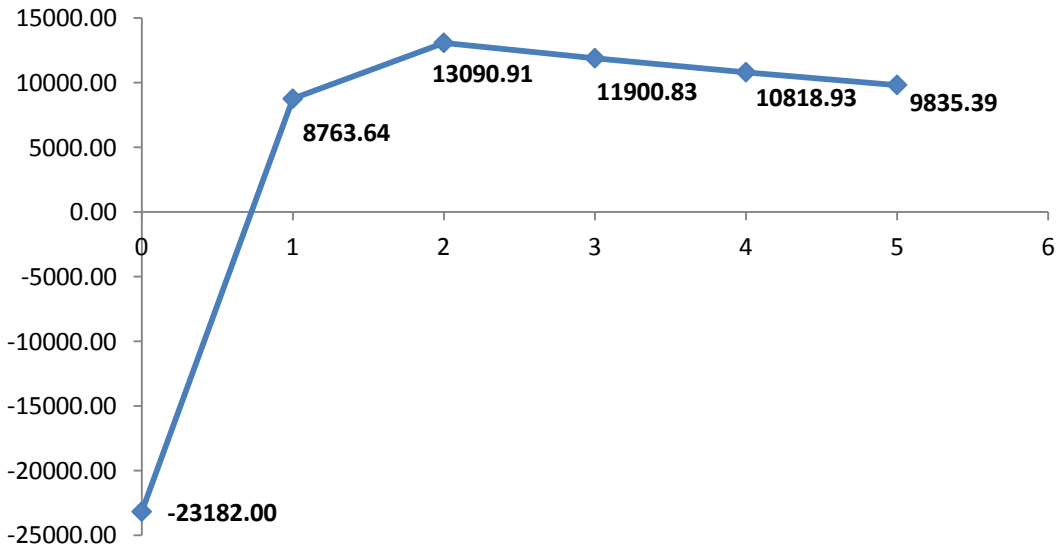

FIGURA 5-3 FLUJO DE CAJA RESPECTO AL AÑO CERO

Fuente: "Elaboración Propia"

5.6 Beneficios de la Propuesta

El modelo de implementación 3 es el más adecuado para poder comunicar entidades con sus sucursales remotas. Esta elección se basa en las pruebas realizadas en el capítulo 4, donde se observó que presentaba valores de retardo entre 99 ms para el caso del enlace sin tráfico, y 628 ms en el caso con 20 conexiones generando tráfico simultáneamente. En cuanto al ancho de banda, se obtuvo un rendimiento de 89.84% sin tráfico y de 47.53% con alto tráfico. Estos valores son comparables a los obtenidos en los demás modelos. Sin embargo, este modelo mostró gran capacidad para el procesamiento de información, al no utilizar más del 2% del CPU durante las 3 pruebas. Esto es de suma importancia teniendo en cuenta el incremento constante de clientes que buscan contratar un servicio VPN.

El hecho de emplear Route Reflectors reduce el consumo de recursos en la red, lo que permite un mejor procesamiento de los datos que se transmiten en ella. Esto incrementa aún más la escalabilidad de este tipo de soluciones, y permite que la red soporte diferentes tipos de servicio como voz, video y acceso a Internet. Además, el corto tiempo de convergencia obtenido en esta solución, que tuvo un valor máximo de 41.46 ms en el caso más crítico, permite afirmar que en caso de existir eventos que puedan hacer que una sesión BGP caiga, ésta se recuperará rápidamente, reduciendo así el tiempo de indisponibilidad de servicio hacia los clientes.

Conclusiones

- Se realizó un estudio detallado de la arquitectura MPLS y su uso principal en las implementaciones de redes privadas virtuales. Se planteó la necesidad de contar con un modelo que garantice el buen desempeño de una red VPN, y que pueda soportar incrementos futuros. Se logró identificar al modelo de implementación *"Multi Protocol eBGP Multisalto entre Route Reflectors"* como el más adecuado. Se pudo identificar que es el que mejores prestaciones presenta, ya que empleó sólo el 2% del CPU, además de tener tiempos de convergencia menores a 60 segundos y valores de retardo no mayores a 628 ms en el caso más crítico. Se verificó también que ofrece un uso efectivo del ancho de banda, con un rendimiento máximo de extremo a extremo de 1.840 Mbps, que representa el 89.84% respecto a los 2.048 Mbps teóricos que presenta la red.

- Se realizó la propuesta técnica en la cual se describe el escenario general al que se enfrenta un proveedor de servicio para brindar servicios VPN a grandes distancias. Se logró elaborar un plan de trabajo que permita lograr la conectividad de extremo a extremo y aprovechar los beneficios que este tipo de redes ofrece.

- El costo del proyecto va acorde a las características del mercado, se ha tomando en cuenta los precios del mercado actual, ajustando la propuesta a la situación de nuestro país. La inversión inicial se recupera en el primer año del proyecto, el cual es rentable a partir del tercer año. Al final de los 5 años servicio, se obtuvo un Valor Actual Neto de USD 38,514.38 y una Tasa Interna de Retorno de 51.18%.

Recomendaciones

- Es posible aumentar la seguridad de la información de cada VPN si se combina con protocolos de encriptación de datos como IPSec, el cual es también utilizado para implementar túneles VPN. Dicha encriptación se aplicará en los equipos de borde (PEs y ASBRs), que son la interfaz de comunicaciones con otras redes.

Trabajos Futuros

- De acuerdo a los servicios que cada cliente utilice a través de la VPN, implementar políticas de Calidad de Servicio (QoS) que permitan mejorar el flujo diferenciado del tráfico que se transmite por la red. Estas políticas varían de cliente a cliente y responden a una necesidad de priorizar tráfico que se considere relevante.

Bibliografía

[ARG2010] ARGUEDAS PORRAS Hellen, GONZÁLEZ QUESADA Erick.
Alajuela: Mayo 2010.
Manual de Comandos Para Enrutamiento. [Presentación Power Point].
URL: http://es.scribd.com/doc/54969097/33/Laboratorio-Frame-Relay-%E2%80%93-Punto-a-Punto
Última fecha de consulta: 15 de Mayo 2012.

[CIS2006] CISCO SYSTEMS.
Configuring Cisco IP SLAs UDP Jitter Operation. [Material de Enseñanza].
URL:http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6602/prod_white_paper0900aecd804fb392.pdf
Última fecha de consulta: 02 de Junio 2012.

[FEL2008] FELE Bostjan, Network Consulting Engineer Advanced Services WWSP WIMAX Practice.
Connecting Enterprises Over Service Provider Netwoks [Presentación PDF].
CISCO EXPO 2008.
URL:http://www.cisco.com/web/SI/ciscoexpo08/presentations/Povezovanje_uporabni_kih_omre_ponudnikov_storitev_Fele.pdf
Última fecha de consulta: 31 de Mayo 2012.

[GAR2009] GARCIA GIRON, Giancarlo.
Tesis de Grado: *Propuesta de Migración de la Red NGN de una Operadora Implementada en IP hacia MPLS.*
Pontificia Universidad Católica del Perú, Perú. 2009.

[GHE2006] GHEIN Luc De.
MPLS Fundamentals. Editor: Cisco Press. Estados Unidos: 2006.

[GON2010] GONZÁLEZ PIÑONES Francisco.
Comentario del 24 de Octubre de 2010, a *Point to Point / Multipoint*.
URL:http://redesfran-cisco.blogspot.com/2010/10/frame-relay-point-to-point-multipoint.html
Última fecha de consulta: 31 de Mayo 2012.

[HAS2005] HAAS Herbert.
MPLS Inter – AS VPN, Interconnecting MPLS Networks [Presentación PDF].
URL: http://www.perihel.at/2/basics/36-MPLS-02-VPN-Inter-AS.pdf
Última fecha de consulta: 05 de Mayo 2012.

[HUA2012] HUAWEI Technologies Co.
A Brief Study a Inter-AS MPLS VPN. Información Técnica.
URL: http://www.huawei.com/products/datacomm/catalog.do?id=1495
Última fecha de consulta: 08 de Junio 2012.

[INT2008] INTERNETWORK EXPERT INC.
CCIE Service Provider Lab Workbook Volume I, Version 1.0. [Presentación PDF]
URL: http://s3.www.ine.com/downloads/IEWB-SP-VOL1-Sample.pdf
Última fecha de consulta: 01 de Junio 2012.

[JAI2008] JAIN Shivlu.
Case Study: MP - eBGP (Option B). [Presentación PDF] del 22 de Agosto de 2008.
URL:https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/2764-102-1-7482/Case%20Study-MB-eBGP(OptionB).pdf
Última fecha de consulta: 01 de Junio 2012.

[JAI2010] JAIN Shivlu.
Comentario del 04 de Octubre de 2010 a Back to Back Vrf Inter-AS Option A.
Back to Back
URL: http://www.mplsvpn.info/2010/10/back-to-back-vrf-inter-as-option.html
Última fecha de consulta: 01 de Junio 2012.

[KAL2010] KALSARIA Prakash.
Comentario del 29 de Mayo de 2010 a Back to Back VRF {Option A}-INTER- AS.
CCIE SP LAB.
URL: http://prakashkalsaria.wordpress.com/tag/inter-as/
Última fecha de consulta: 25 de Mayo 2012.

[KOZ2005] KOZIEROK Charles.
Comentario del 20 de setiembre de 2005 a The TCP / IP Guide.
Performance Measurements: Speed, Bandwidth, Throughput and Latency.
URL:http://www.tcpipguide.com/free/t_PerformanceMeasurementsSpeedBandwidthThroughputand.htm
Última fecha de consulta: 03 de Junio 2012.

[LAV2010] LAVADO Gianpietro.
MPLS-Multiprotocol Label Switching. Versión 1.0 Modo de Compatibilidad
[Presentación Power Point] 2010.
Última fecha de consulta: 07 de Mayo 2012.

[LIM2004] LIMARI RAMIREZ, Víctor Humberto.
Tesis de Grado: *Protocolos de Seguridad para Redes Privadas Virtuales (VPN).*
Universidad Austral de Chile Valdivia, Chile. 2004
URL: http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/doc/bmfcil732p.pdf
Última fecha de consulta: 14 de Abril 2012.

[LOB2005] LOBO Lancy, LANKSHMAN Umesh.
MPLS Configuration on Cisco IOS Software. Editor: Cisco Press. Capítulo VII, *Inter-Provider VPNs*
Estados Unidos 2005.

[MAY2012] MAYORISTA DE TELECOMUNICACIONES
Información Corporativa – Junio 2012

[MAH2008] MAHMOUD Mohammed.
Comentario del 25 de Diciembre de 2008 a Inter - AS MPLS VPN - The Whole Story.
URL:http://www.networkers-online.com/blog/2008/12/inter-as-mpls-vpn-the-whole-story-updated-dec-2008/
Última fecha de consulta: 28 de Mayo 2012.

[MOR2006] MORALES BIBILDOX, Luis.
Tesis de Grado: *Investigación de Redes VPN con Tecnología MPLS*. Universidad de las Américas Puebla, México. 2006.
URL: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/
Última fecha de consulta: 07 de Mayo 2012.

[PAC2012] Packetlayer.
Comentario del 18 de Marzo de 2012 a Inter Service Provider Back to Back VRF.
URL: http://packetlayer.wordpress.com/2012/03/18/inter-service-provider-back-to-back-vrf/
Última fecha de consulta: 25 de Mayo 2012.

[PAR2011] PÁRAMO DíAZ Harold André.
Comentario del 3 de Junio de 2011 a *Definiciones y Configuración Frame Relay*.
URL: http://networkingtools.blogspot.com/2011/06/frame-relay.html
Última fecha de consulta: 06 de Junio 2012.

[PEP2002] PEPELNJAK Iván, GUICHARD Jim.
MPLS and VPN Architectures. Editor: Cisco Press, Estados Unidos 2002.

[SOU2012] SOUNDFORGE.NET
Iperf.
URL: http://iperf.sourceforge.net/
Última fecha de consulta: 09 de Mayo 2012.

[WIR2012] Wireshark Foundation
About Wireshark.
URL: http://www.wireshark.org/about.html
Última fecha de consulta: 14 de Mayo 2012.

[ZHA2003] ZHANG Randy, BARTELL Micah.
BGP Design and Implementation. Editor: Cisco Press.
Estados Unidos 2003.

Anexos

Anexo 1: Configuraciones de los routers que conforman las topologías Multi AS MPLS-VPN.

Se presentan las configuraciones realizadas en cada uno de los routers que conforman las redes de los cuatro modelos de implementación.