Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

VPLS una Opción de Transporte Ethernet

Autora: Vanesa Hernández Hernández

Tutor: Dr. Félix Álvarez Paliza

Santa Clara

2011

"Año 53 de la Revolución”

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

VPLS una Opción de Transporte Ethernet

Autora: Vanesa Hernández Hernández

vanesa@uclv.edu.cu

Tutor: Dr. Félix Álvarez Paliza

fapaliza@uclv.edu.cu

Consultante: Tte. Yohansy Rodríguez Espino

Santa Clara

2011

"Año 53 de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

Firma del Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

"La obtención de un título o diploma representa para muchos, el término de sus estudios, pero para un revolucionario dicha formación significa una vida entera consagrada al estudio."

Fidel Castro Ruz.

DEDICATORIA

Quisiera dedicar este trabajo de diploma primeramente a mi madre, sin la cual no hubiese podido llegar hasta este punto tan importante en mi vida. A mi hermana, que con su ejemplo, ha sido la persona que me ha impulsado a llevar a cabo retos que le han dado un giro determinante a mi vida. A mi novio que gracias a su amor y cariño, he podido seguir adelante en los momentos más difíciles de mi vida. A mi familia en general que me han brindado el apoyo necesario y un amor incondicional para ser cada día una mejor persona y finalmente a todas aquellas personas que de una forma u otra han hecho posible la realización de este proyecto.

AGRADECIMIENTOS

Agradezco diariamente a mi madre Irma que ha sido el motor impulsor y la persona más importante en mi vida.

A mi hermana y alma gemela Marianela que es mi razón de ser y la luz que me guía día a día.

A mi novio Elier que me ha brindado un amor incondicional en todos estos años.

A mis amigos Heidy, Dayana, Beatriz, Araly y Ariagna que con sus consejos me han convertido en una mejor persona.

A mi tutor Paliza sin el cual no hubiese sido posible la realización de este proyecto.

A mis profesores de todos estos años que me han enseñado, entre muchas cosas, a crecer.

TAREA TÉCNICA

1. Hacer una revisión bibliográfica que permita conocer los trabajos relacionados con las redes MPLS, los servicios de *Carrier Ethernet* y en especial VPLS.
2. Actualizarse en los estándares emitidos por IETF (RFC) y UIT-T.
3. Organizar y estructurar la información disponible sobre VPLS.
4. Actualizarse en el empleo de la herramienta de modelación y simulación de redes OPNET.
5. Desarrollo de diferentes proyectos y escenarios para la interconexión de redes a fin de ofertar el servicio VPLS.
6. Evaluación experimental.
7. Informe Final.

Firma del Autor

Firma del Tutor

RESUMEN

El servicio de red LAN privado virtual (VPLS) es una tecnología emergente para incorporar la conexión transparente de redes LAN sobre la INTERNET. Este servicio aparece y se comporta desde el punto de vista de los usuarios como un simple puente Ethernet. Gracias a la combinación de la simplicidad de las redes LAN Ethernet con la escalabilidad y seguridad de las redes MPLS, VPLS constituye una alternativa viable para aquellas empresas que buscan una solución balanceada entre el costo y la efectividad de la red. Este proyecto persigue un objetivo general basado en la Valoración los cambios de los servicios VPLS derivadas de MPLS como una opción a considerar para la interconexión de redes.

El presente proyecto analiza los conceptos y los principios de funcionamiento de la tecnología VPLS y analiza las posibilidades técnicas que hoy posee nuestro país para implementar este servicio, se analizan las posibilidades que representan las herramientas de operación, administración y mantenimiento para ofertar calidad de servicio. Se propone además algunos escenarios de nuestro país donde la implementación de la tecnología VPLS acometería un cambio favorable en sus redes.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Ethernet se ha convertido en la tecnología más usada en el mundo para las redes LAN, con razones de datos que van desde 10 Mbps hasta 10 Gbps y se habla de alcanzar en los próximos años los 100 Gbps.

Ethernet ha resuelto la demanda de ancho de banda de forma flexible, pues cada nueva tecnología ha incorporado las anteriores. Simultáneamente fue convirtiéndose en un atractivo para los proveedores de servicio y comunidades de telecomunicaciones como una tecnología de transporte. Para estructurar mejor Ethernet como un servicio de transporte (*carrier-ethernet*) se creó el Fórum de redes metropolitanas Ethernet (Metro Ethernet Forum MEF), el cual ha impulsado diferentes aplicaciones y estándares.

El MEF definió tres tipos de servicio Ethernet los cuales fueron definidos en términos de Conexión Ethernet Virtual (EVC):

E-Line: constituye un EVC punto a punto

E-LAN: constituye un EVC multipunto a multipunto

E-Tree: constituye un EVC de ruteo multipunto

Mientras que E-Line provee un servicio de conexión a dos sitios de clientes exactamente, E-LAN y E-Tree permiten la conexión de múltiples clientes (multipunto). Todos estos servicios poseen definiciones estandarizadas como son las características de ancho de banda y servicio de multiplexación.

Hoy en día la mayoría de las empresas que utilizan servicios punto a punto ven la necesidad de migrar hacia la tecnología de los servicios multipunto para lograr mayor eficiencia en el desempeño de sus redes y de esta forma poder hacer un mejor uso de las nuevas

aplicaciones que han estado abriéndose paso. Ejemplo de estas aplicaciones son voz sobre IP (VoIP), mensaje instantáneo y herramientas de redes basadas en presentación y reconocimiento.

Este proyecto va a estar encaminado hacia la fundamentación del servicio E-LAN también llamado VPLS.

Desde la perspectiva del usuario el servicio que provee una red VPLS es visto como un conmutador Ethernet virtual conectando usuarios desde sitios remotos. El servicio VPLS resulta muy atractivo debido a que los clientes solo necesitan adquirir una única conexión a la red desde cada oficina.

VPLS es una tecnología en proceso de estandarización en el seno del **IETF** que permite crear una red privada virtual de Nivel 2 capaz de soportar múltiples sedes en el interior de un único dominio sobre una red IP/MPLS (*Multiprotocol Label Switching*) gestionada. Diseñada para proporcionar conectividad Ethernet entre cualquier extremo con altos niveles de granularidad y ancho de banda, su objetivo es superar las limitaciones de tecnologías anteriores, como ATM y FR, proporcionando un servicio WAN totalmente mallado e independiente de protocolos.

La clave que explica la creciente popularidad de esta tecnología radica en su naturaleza de Nivel 2, que como tal, no requiere que los usuarios compartan sus tablas de enrutamiento con el operador, algo que muchas de las compañías encuentran cada vez más atractivo. Además de que esta característica aporta un nivel de protección especialmente indicado para manejar documentos y datos fuertemente regulados por las normas generales y sectoriales. Esta tecnología es una alternativa efectiva en costes en entornos WAN, sobre todo para aquellas organizaciones que necesitan conexiones seguras de gran ancho de banda entre múltiples sedes, nacionales e internacionales. En definitiva, VPLS es una buena opción para las entidades públicas multisede e incluso multinacionales que deseen proporcionar conectividad de alta velocidad entre sus oficinas e instalaciones. La posibilidad de cambiar la velocidad de los puertos y la capacidad de incrementar o reducir el ancho de banda a medida que las necesidades cambian hacen que sea más fácil soportar las nuevas aplicaciones en tiempo real, como la videoconferencia, la colaboración y la VoIP. Y todo ello con la seguridad y confort que aporta Ethernet.

En el presente proyecto se tiene como objetivo general valorar los cambios de los servicios VPLS derivadas de MPLS como una opción a considerar para la interconexión de redes empresariales.

Y como objetivos específicos se proponen:

1. Analizar la evolución y despliegue que han tenido los servicios de redes LAN Privadas Virtuales (VPLS).
2. Determinar los escenarios y aplicaciones en los que mejor se utiliza VPLS.
3. Modelar y Simular diferentes escenarios en base al equipamiento desplegado por diferentes firmas en el mundo.

Con la puesta en práctica de este proyecto se pretende lograr algunos aportes significativos como contribuir a la interconexión de redes con servicios de banda ancha, una necesidad de nuestra sociedad. Tener una red con un mejor desempeño de la redes de las empresas, universidades, gobiernos, etc. Al lograr su interconexión mediante redes LAN privadas virtuales.

Dentro del impacto social del proyecto se pretende lograr que los usuarios de las redes LAN puedan interconectarse con calidad de servicio y diversidad en sectores priorizados del país y como impacto económico se pretende que la oferta de servicio VPLS permitirá ampliar las ofertas de ETECSA a un mayor número de usuarios de banda ancha.

Organización del informe

El trabajo de investigación cuenta con la siguiente estructura:

1. En la introducción se dejará definida la importancia, actualidad y necesidad del tema que se aborda.
2. Capítulo I: Evolución de los servicios VPLS, nuevos estándares, aplicaciones etc.
3. Capítulo II: Análisis de escenarios de aplicaciones, fundamentación de los modelos acordes a la realidad cubana.

4. Capítulo III: Análisis de resultados de las simulaciones y propuesta de alternativas económicas para ofertar los servicios de banda ancha.
5. Conclusiones
6. Recomendaciones
7. Referencias Bibliográficas
8. Anexos
9. GLOSARIO Y/O SIGLARIO

CAPÍTULO 1. EVOLUCIÓN DE LOS SERVICIOS VPLS

1.1 Introducción a las Redes de Transporte Ethernet (*Carrier Ethernet*)

A finales de los 90 se vio la necesidad de ofrecer nuevos servicios de transporte que fueran más baratos, rápidos y flexibles que las líneas arrendadas tradicionales o los servicios de acceso FR, este nuevo servicio fue basado en Ethernet.

Para las redes de transporte, implementando Ethernet como una tecnología de nivel 2, existen dos direcciones fundamentales:

La primera dirección y más significativa es usando un mecanismo de transporte de datos sobre Ethernet como MPLS. La segunda dirección se refiere a la tecnología resultante de las extensiones de los puentes empleados en redes Ethernet, con componentes de envío (*forwarding)* y/o plano de control para las direcciones necesarias de las redes de transporte/agregación.(Chinea)

El Forum Ethernet Metropolitano (MEF) ha definido al transporte Ethertnet (*Carrier Ethernet*) como el servicio predominante entre todas las clases de transporte (*Carrier-Class*), definidos por cinco atributos esenciales que distinguen al mismo de la familia Ethernet para LANs. El transporte Ethernet esencialmente enriquece el Ethernet tradicional, optimizado para la implementación en redes de área local (LAN) ahora extendido a redes de acceso, redes de área metropolitana (MAN) e incluso más allá, a rede de área global (WAN). Además provee al usuario final de un servicio robusto, con un desarrollo determinístico y con gran fiabilidad.

1.2 Atributos de Transporte-Ethernet

Los cinco atributos que esencialmente definen el transporte Ethernet son:(Chinea)

- Servicio estandarizado
- Escalabilidad
- Fiabilidad
- Calidad de servicio
- Servicio de gestión

Los mismos proveen la capacidad necesaria adicional para usar a Ethernet de igual forma a como lo hacían sus anteriores proveedores de servicio como es el caso de ATM y *Frame Relay*.

1.2.1 Servicio Estandarizado

Este atributo esencialmente habilita un proveedor de servicio para que sea capaz de entregar información de un terminal tanto en forma de paquetes como TDM tradicional a un servicio multipunto en un modo eficiente y determinado sobre una plataforma de servicio estandarizado. Este servicio fortalece la multitud de aplicaciones clientes que están emergiendo a través de la voz, video y datos(Chinea). Este atributo está definido por los siguientes componentes específicos:

• Ubicuidad: *Carrier Ethernet* habilita un proveedor de servicios Ethernet siempre presente a través de equipos estandarizados, independiente de la infraestructura por debajo de aplicación (Media) y Transporte.

• Servicios Ethernet: *Carrier Ethernet* soporta dos tipos de servicios: Servicios Ethernet punto a punto (Referidos a Ethernet Line o E-Line) y multipunto a multipunto (Referidos a Ethernet LAN o E-LAN).

• Servicios de Emulacion de Circuitos (CES): *Carrier Ethernet* es capaz de transportar no solo servicios basados en Ethernet sino otros servicios como TDM, necesitando emular ciertas características para este tipo de aplicaciones como son la señalización y la sincronización.

• Fragmentacion y Calidad de Servicio: Los servicios soportados por *Carrier Ethernet* proveen una amplia selección de opciones de fragmentación del ancho de banda y Calidad de Servicio.

Esto es vital en el funcionamiento de una red donde coexisten múltiples usuarios con aplicaciones de diferentes requerimientos en cuanto a capacidad de ancho de banda y a prioridad en el servicio.

• Convergencia en el Transporte: Soporta la convergencia de los servicio de voz, datos y video sobre un único transporte (Ethernet) y simplifica grandemente la administración, la entrega y adición de tales servicios. Básicamente todos los servicios y aplicaciones de una empresa ahora se soportan sobre un simple túnel Ethernet.

1.2.2 Escalabilidad

Una diferencia fundamental entre una red LAN y una de proveedor de servicio es el alcance. En un proveedor de servicios existen cientos de usuarios más y consecuentemente muchas más conexiones que en una red basada en simples aplicaciones Ethernet, puesto que esta cubre un área geográfica mayor. La solución de Transporte Ethernet puede tener un alcance de varias dimensiones simultáneamente.(Chinea):

• Usuarios/Terminales: Una red de proveedor de servicios soporta cientos de miles de terminales y millones de usuarios Ethernet en una óptima configuración. Especialmente este soporta la entrega de millones de servicios Ethernet con una apropiada (QoS) calidad de servicio.

• Alcance Geográfico: Los servicios entregados pueden abarcar redes de acceso, metropolitanas y más allá, cubriendo grandes distancias geográficas y sobre una variedad de infraestructuras incluyendo Ethernet, WiFi, WiMax, TDM, SONET/SDH, y muchas más.

• Aplicación: Crece el surgimiento de aplicaciones soportadas sobre un terminal de negocios, de información y entretenimiento, todo bajo el beneficio de la convergencia de la vos, el video y los datos.

• Ancho de Banda: El incremento del ancho de banda desde 1Mbits/s hasta 10GBits/s con intervalo de crecimiento de 1MBits/s, habilita aún más la solución tanto para el proveedor de servicio como para el usuario final(Chinea).

1.2.3 Fiabilidad

Como los servicios de Transporte Ethernet están diseñados para soportar aplicaciones críticas a gran escala, el habilitar la detección de fallas, rápidamente y en el nodo remoto, ya sea en la infraestructura física o en la capa de servicios Ethernet, se hace esencial. Los siguientes aspectos son direccionados por *Carrier Ethernet*.(Chinea):

• Servicio de Recuperación (*Resiliency*): El impacto de una falla es localizado y no afecta a otros clientes o aplicaciones. La correlación de múltiples errores serán identificados rápidamente. Además el proceso de solución y recuperación de fallas será rápido y usa herramientas que minimizaran los gastos operacionales para el proveedor de servicios y cualquier impacto adverso en los usuarios finales.

• Protección (*Protection*): *Carrier Ethernet* provee un nivel de servicio de protección *end-to-end* que contiene protección contra cualquier falla dentro de la infraestructura desarrollada en la entrega de los servicios. Esto significa que *Carrier Ethernet* protege cualquier falla en el camino de los servicios *end-to-end.*

• Recuperación (*Restoration*): *Carrier Ethernet* provee Similar recuperación a SONET/SDH que tienen un tiempo de recuperación por debajo de los 50 ms, para la implementación de redes de conmutación de vos. Para el tratamiento de las aplicaciones de vos y video es un requisito indispensable que *Carrier Ethernet* implemente recuperaciones igual que las de SDH, quedando obsoleta la implementación de STP en grandes redes de proveedor de servicios, y surgiendo nuevas variantes como RPR, RRPP, entre otras(Chinea).

1.2.4 Calidad de Servicio

Proveer calidad de servicio para Transporte Ethernet es algo muy necesario para ser considerado como el sustituto de ATM y *Frame Relay* y últimamente como un mecanismo de convergencia en la entrega de todos los servicios. Proveer QoS para los servicios de Transporte Ethernet, comprende los siguientes aspectos.(Chinea) (Jitter):

• Desempeño de Acuerdo al Nivel de Servicio (SLA): Es la capacidad de proveer una rigurosa clasificación de los niveles de servicios necesarios para proveerle a un terminal de servicios críticos como vos video y datos sobre una infraestructura de Ethernet convergente.

• Parámetros SLA: La configuración de estos parámetros permite a un Proveedor de servicios actualmente definir los SLA específicos para cada servicio comercial.

• Suministros de SLA: La calidad de servicio provee un duro desempeño basado en garantizar los elementos típicos que definen la QoS de una red tales como, la perdida de paquetes, la demora en los paquetes y variación de la demora de los paquetes (Jitter)(Chinea).

1.2.5 Servicio de Gestión

La gestión de un gran número de clientes instalados sobre un área geográfica amplia, requiere de proveedores de servicios que tengan una capacidad sofisticada para instalar, solucionar y actualizar los servicios Ethernet rápidamente(Chinea).

1.3 Tecnologías de Transporte-Ethernet

Este epígrafe hace un breve resumen de las tecnologías de agregación o acceso de Transporte Ethernet.

• IEEE 802.1Q: *Virtual LANs* (VLANs): 802.1Q provee tramas Ethernet marcadas con identificadores de VLANs. Este provee los mecanismos que Habilitan múltiples puentes de red para compartir transparentemente el mismo medio físico el cual mantiene el aislamiento entre las redes.

• IEEE 802.1Q-IN-802.1Q (Q-IN-Q): Q-in-Q habilita el almacenamiento de VLANS que soportan la incorporación de múltiples VLAN marcadas en la misma trama Ethernet creando una jerarquía. Q-in-Q es iniciado como una implementación propietaria para sobrepasar el límite de empleo de 4094 VLANs impuesto por 802.1Q.

• IEEE 802.1AD (PB): 802.1 ad estandariza la arquitectura de protocolos de puentes para permitir las tramas Ethernet con múltiples VLAN marcadas. Además define las etiquetas para las VLANs clientes (C-VLAN) y de servicio (S-VLAN) e introduce en la trama una

dirección MAC para el cliente y provee además un espacio al proveedor de direcciones MAC para el protocolo de control de capa 2. 802.1ad provee una instancia separada para el servicio de MAC del puente a múltiples clientes independientes de una red de puenteado de área local adicionando o removiendo las S-VLANs.

• IEEE 802.1AH (PBB): 802.1ah define los protocolos del puente y una arquitectura para la interconexión de redes de puentes de proveedores (PBNs). 802.1ah permite a un proveedor soportar hasta 2 expo 24 (16 millones) instancias de servicio, superando las 2 expo 12 (4000) instancias de servicio que se pueden emplear en una PBN. En la frontera de una red de PBB (PBBN), la trama Ethernet es asociada a una instancia de servicio basada en la S-VLAN en el encabezado de la trama. El encapsulado de la cabecera MAC de una PBB de la trama del cliente incluye la cabecera MAC del cliente (C-MAC). La cabecera de un PBB está compuesta por la dirección MAC destino y fuente (B-MAC), un *BackBone* VLAN ID (B-VID) para separar el dominio de emisión en el *BackBone*, un identificador de instancias de servicio de 24 bits (I-SID) en una instancia de servicio marcada (I-Tag).

Servicios de Líneas Virtuales Privadas (VPLS): VPLS es una tecnología de Red Privada Virtual de capa dos (L2 VPN) multipunto que habilita múltiples sitios para ser conectados sobre un dominio de emisión Ethernet emulado a través de una red IP/MPLS. VPLS desarrolla una extensión lógica de los servicios privados de cables virtuales (VPWS) basados en la RFC4447. Una VPWS Ethernet provee un servicios punto a punto (P2P) basados en Ethernet L2 VPN. Una VPLS puede ser definida como un grupo de instancias de conmutación virtual que están interconectados formando un simple dominio de puentes lógicos. Un VSI es similar a las funciones de puente definidas en 802.1q, donde una trama es conmutada basada en la dirección MAC destino y asociada a una L2 VPN(Chinea).

1.4 Introducción a las Redes VPLS

VPLS es una tecnología L2VPN de multipunto que permite que múltiples sedes sean conectadas sobre un dominio de emisión Ethernet simulado. Una gran importancia de VPLS es que entrega una conectividad de nivel 2 multipunto sobre arquitectura de redes de nivel 3. VPLS evolucionó como una extensión lógica de EoMPLS la cual fue perfeccionada para permitir Ethernet punto a punto basada en los servicios de L2VPN. Como un nivel básico VPLS puede ser definida como un grupo de VSI que están interconectados usando

circuitos EoMPLS en una topología de malla completa simples. Un VSI es similar a la función de puenteado encontrada en 802.1Q(2003)(Gómez 2007).

VPLS, también conocido como TLS o servicio E-LAN, es una VPN multipunto de capa2 que permite conectar múltiples sitios en un único dominio puenteado sobre una red MPLS/IP gestionada por el proveedor. Todos los sitios del cliente en un caso de VPLS (es decir, un VPLS para una empresa particular) parecen estar en la misma LAN, sin tener en cuenta sus localizaciones. VPLS utiliza una interfaz Ethernet con el cliente, simplificando la frontera LAN/WAN y permitiendo un aprovisionamiento rápido y flexible del servicio(J. Witters 2004)(Reyes 2007).

1.4.1 Estructura de una Red VPLS

Una red con VPLS consta de CEs, PEs y de una red central MPLS:

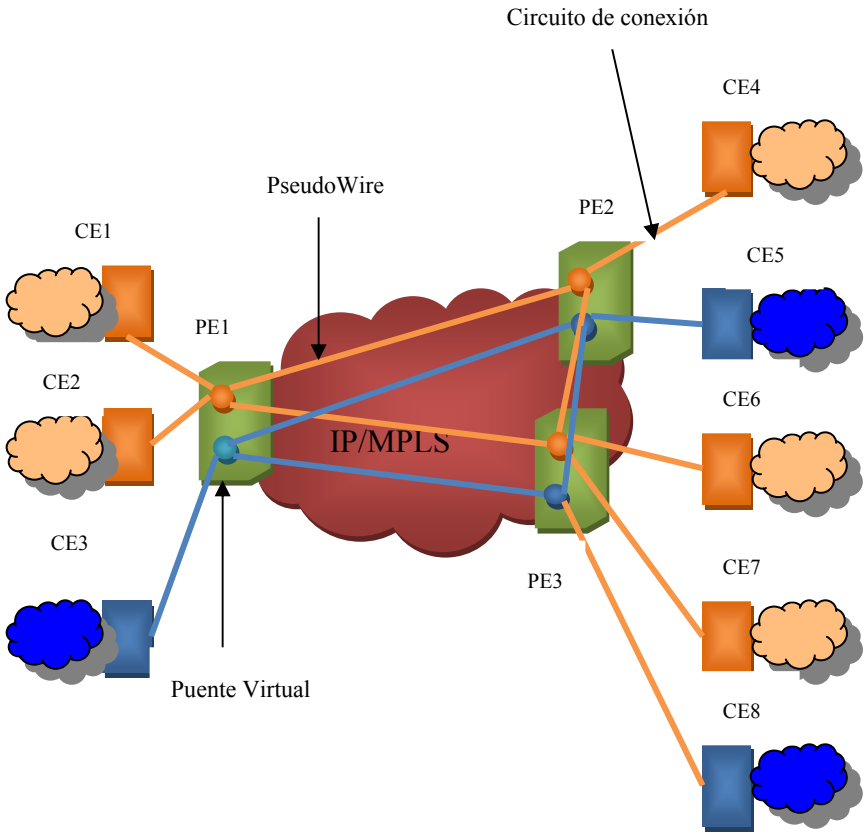


Figura 1.1) Modelo de referencia de VPLS

El dispositivo CE es un ruter o conmutador situado en las instalaciones del cliente; puede pertenecer y gestionarse por el cliente o por el proveedor de servicios. Se conecta al PE mediante un AC. En el caso de VPLS, se asume que Ethernet es la interfaz entre CE y PE. El dispositivo PE es donde reside toda la inteligencia de VPN, donde el VPLS comienza y termina y donde se establecen todos los túneles necesarios para conectar con todos los otros PEs. (Reyes2007). Ya que el VPLS es un servicio Ethernet de capa2, el PE debe ser capaz de conocer, puentear y replicar el MAC en base a VPLSs. La red central MPLS/IP interconecta los PEs; no participa realmente en la funcionalidad de VPN. El tráfico se conmuta simplemente basándose en etiquetas MPLS. La base de cualquier servicio VPN multipunto (VPN IP o VPLS) es una malla completa de túneles MPLS (LSPs – trayectos conmutados por etiquetas, también llamados túneles externos) que se establecen entre todos los PEs que participan en el servicio VPN. LDP se utiliza para establecer estos túneles; alternativamente se puede utilizar RSVP-TE o una combinación de LDP y RSVP-TE. Las VPNs multipunto pueden crearse encima de esta malla completa, ocultando la complejidad de la VPN desde los ruters centrales. Para cada instancia VPLS se crea una malla completa de túneles internos, llamados *pseudowires*, entre todos los PEs que participan en la instancia VPLS. Un mecanismo de auto-detección localiza todos los PEs que participan en la instancia VPLS. Este mecanismo no se ha incluido en las especificaciones previas, de esta forma el proveedor de servicio puede configurar el PE con las identidades de todos los otros PEs en un VPLS concreto, o puede seleccionar el mecanismo de auto-detección que prefiera, por ejemplo, RADIUS. (Gómez 2007). Cuando un PE recibe una trama Ethernet con una dirección de fuente MAC desconocida, PE sabe en qué VC se envió. Los routers PE deben soportar todas las prestaciones “clásicas” Ethernet, como aprendizaje del MAC, replicación y envío de paquetes. Desde un punto de vista funcional, esto significa que los PEs deben implementar un puente por cada instancia VPLS, al que se le suele llamar VB. La funcionalidad VB se lleva a cabo en el PE mediante una FIB para cada supuesto de VPLS; esta FIB se popula con todas las direcciones MAC aprendidas. Todo el tráfico se conmuta en base a las direcciones MAC y se reenvía entre todos los ruters PE participantes, usando túneles LSP. Los paquetes desconocidos (es decir, las direcciones de destino MAC que no han sido aprendidas) se replican y reenvían en todos los LSPs a todos los ruters PE

que participan en ese servicio hasta que responde la estación de destino y la dirección MAC es aprendida por los ruters PE asociados con dicho servicio.

Para evitar bucles de reenvío se usa la regla llamada "*Split Horizon* (partir el horizonte)". En el contexto VPLS, esta regla implica básicamente que un PE nunca debe enviar un paquete a un PW si ese paquete se ha recibido de un PW. Esto asegura que el tráfico no pueda formar un bucle sobre la red de *backbone* usando PWs. El hecho de que haya siempre una malla completa de PWs entre los dispositivos PE asegura que cada paquete emitido alcanzará su destino dentro del VPLS(J. Witters 2004)(Reyes 2007)(Gómez 2007).

1.5 Tecnología Pseudo-Wire

La tecnología pseudo-hilo está normalizada por el IETF (grupo de tareas sobre ingeniería de Internet) PWE Grupo de trabajo. Los PWs son conocidos históricamente como "túneles Martini", y a las extensiones al protocolo LDP para permitir la señalización de PWs se las denomina frecuentemente "señalización Martini". Un PW consta de un par de LSPs unidireccionales punto-a-punto de un solo salto en direcciones opuestas, cada uno identificado por una etiqueta PW, también llamada VC. Las etiquetas PW se intercambian entre un par de PEs usando el mencionado protocolo de señalización LDP. El identificador VPLS se intercambia con las etiquetas, así ambos PWs pueden enlazarse y asociarse a una instancia VPLS particular. A observar que este intercambio de etiquetas PW tiene que darse entre cada pareja de PEs participantes en una instancia VPLS concreta, y que las etiquetas PW tienen solamente un significado local entre cada una de esas parejas. La creación de PWs con una pareja de LSPs permite a un PE participar en el aprendizaje del MAC(J. Witters 2004)

PWE3 es un mecanismo que emula los atributos esenciales de servicios tales como ATM, *Frame Relay* o Ethernet sobre una red conmutada de paquetes (*Packet Switched Network, PSN*). Las funciones requeridas de los PWs incluyen encapsulación de los paquetes que arriban a la puerta de ingreso, y el transporte de estos a través de un trayecto o túnel, y otras operaciones para emular el comportamiento del servicio tan fielmente como sea posible. Para la perspectiva del cliente, el PW es percibido como un enlace o circuito no compartido(Reyes 2007).

1.5.1 Tipos de Señalización para el establecimiento de los Pseudo-Wire

Existen 2 modos de señalización para el establecimiento de un túnel PW: LDP y MPBGP Cuando el protocolo LDP es usado para la señalización, el TLV del estándar LDP es extendido para portar la información VPLS. Dos tipos de TLV FEC son añadidos: tipo128 y tipo129. La secuencia de distribución de etiquetas durante el establecimiento del PWs adopta el modo descendente no solicitado (*downstream unsolicited, DU)* y la retención de etiquetas adopta el modo liberal de retención de etiquetas. Las conexiones LDP usadas para intercambiar señalización VC deben ser configuradas al modo remoto(Reyes 2007).
En la figura que es mostrada a continuación, ilustra un procedimiento característico de establecimiento y liberación del PW con el modo de señalización LDP. Cuando el PE1 es configurado con un VSI y PE2 es especificado como su par, una etiqueta será distribuida para la sesión y un mensaje será enviado al PE2 (*mapping message*), si la sesión entre PE1 y PE2 ha sido establecida. Con la recepción del mensaje, PE2 chequeará si el mismo VSI ha sido configurado localmente. Si el VSI fue configurado localmente con el mismo VSI ID y tipo de encapsulación, esto indica que los
VSIs en los dos PEs están en la misma VPN. El PW será establecido para PE2. Lo mismo sucede con PE1 después de recibir el mensaje de mapeo de PE2.
Cuando PE1 no necesita enviar por más tiempo paquetes hacia PE2 (por ejemplo, el cliente remueve la designación de PE2 como su par), este enviará un mensaje *withdraw*,
PE2 liberará el PW y retornará un mensaje *release*. PE1 liberará la etiqueta y desconectará el PW después de recibir el mensaje(Reyes 2007).
Cuando se utiliza la señalización LDP se le llama VPLS Martini.

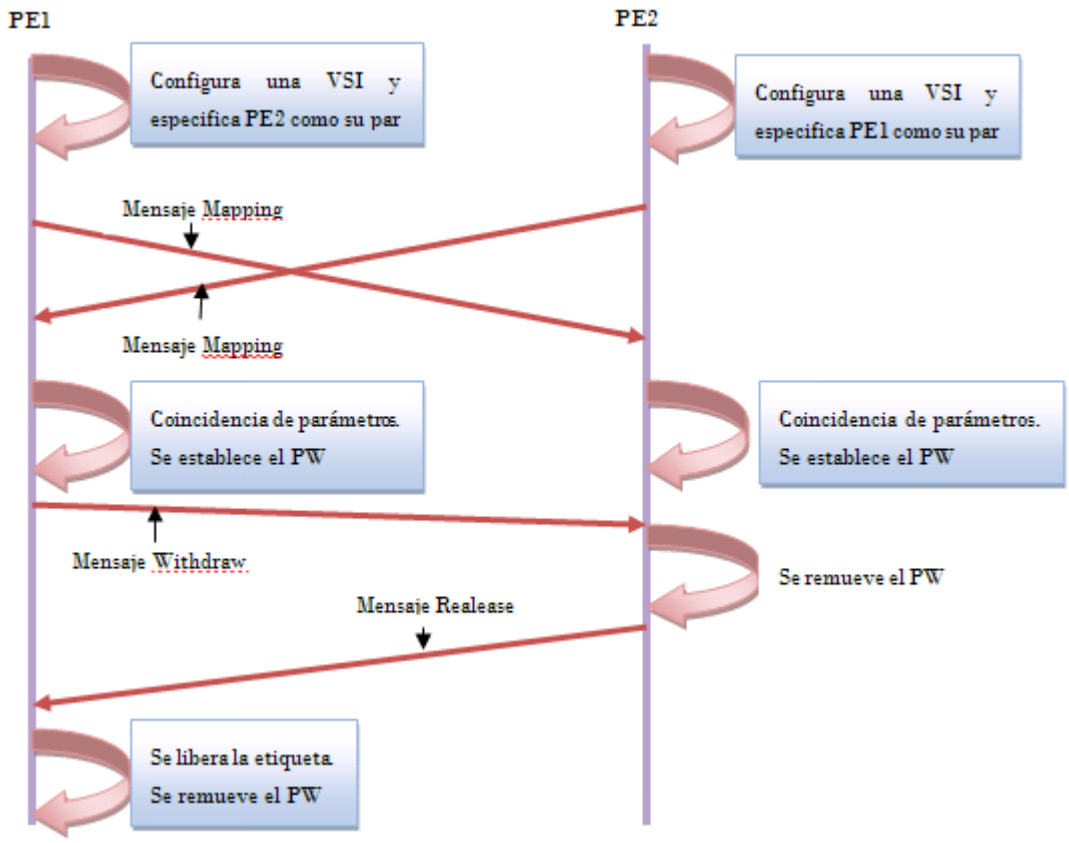


Figura 1.2) Procedimiento de establecimiento/liberación de un PW con LDP

Cuando el Protocolo de Borde Multiprotocolo es usado para la señalización, la extensión de BGP (RFC 2283) es usada para transmitir la información de los miembros VPLS. Los atributos MP-*reach* y MP-*unreach* transmiten la información de la etiqueta VPLS y los atributos de la comunidad extendida trasmiten la información de los parámetros de interface. La membresía VPN es determinada por el RD (*Route Distinguish*) y el *VPN-TARGET* que son transmitidos en el atributo de comunidad extendida.(Reyes 2007)(Gómez 2007).

La figura que es mostrada a continuación, ilustra un procedimiento característico de establecimiento y liberación del PW con el modo de señalización BGP. Cuando el PE1 es configurado con un VSI y tiene una sesión BGP establecida al PE2 y la familia de direcciones VPLS es habilitada en esta sesión, una etiqueta será distribuida a la sesión BGP y un mensaje *update* que porta el atributo MP-REACH será enviado al PE2. Con la

recepción del mensaje *update*, PE2 chequeará si el mismo VSI ha sido localmente configurado. Si el mismo VSI ha sido configurado localmente y el *VPNTARGET* coincide, esto indica que los VSIs en los dos PEs están en la misma VPN. El PW será establecido para PE2. Lo mismo sucede con PE1 después de recibir el mensaje *update* de PE2. Cuando PE1 no necesita enviar por más tiempo paquetes hacia PE2 (por ejemplo, el cliente remueve la designación de PE2 como su par), este enviará un mensaje *update* que porta el atributo *MP-UNREACH* mientras desconecta el PW y libera la etiqueta al mismo tiempo. PE2 liberará el PW después de recibir el mensaje *update* del PE1.

Cuando se utiliza la señalización BGP se le llama VPLS Kompella.

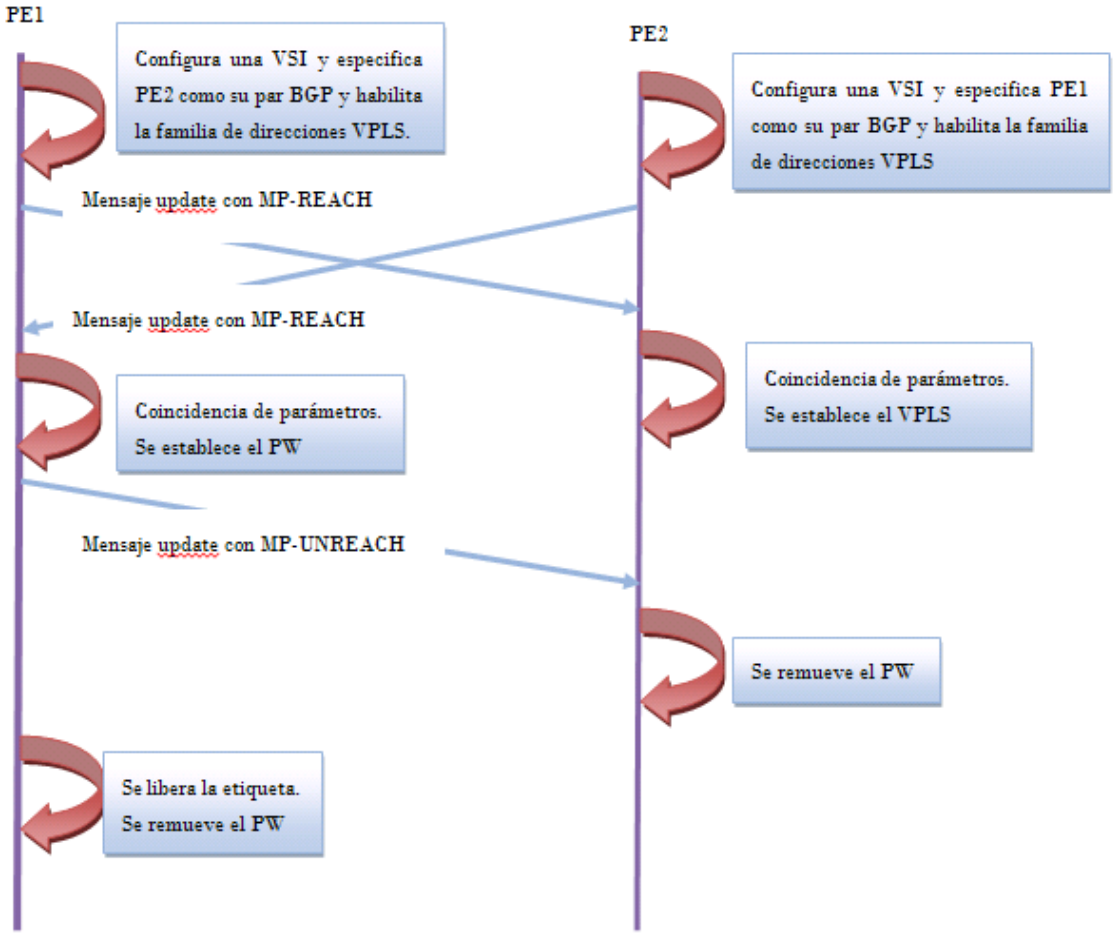


Figura 1.3) Procedimiento de establecimiento/liberación de un PW con BGP

1.5.2 Comparación entre los modos de Señalización LDP y BGP para el establecimiento de los Pseudo-Wire

El protocolo LDP es muy simple y tiene bajos requerimientos para los PEs, pero no provee a los miembros de la VPN mecanismo de autodescubrimiento y la membresía debe ser configurada manualmente. Al contrario el modo BGP tiene altos requerimientos para los PEs y sí posee mecanismo de autodescubrimiento.

En el modo LDP una etiqueta es distribuida a cada PE solamente cuando es necesario, mientras un bloque de etiquetas es distribuido a cada PE en el modo BGP y resulta en un cierto gasto de etiquetas.

Un PW debe ser configurado por cada PE para conectar el nuevo PE cuando un nuevo PE es añadido en el modo LDP, mientras en el modo BGP solo es necesario configurar el nuevo PE, a condición que el número de PEs no puede exceder el tamaño del bloque de etiquetas.

En el modo LDP debe asegurarse de que la instancia VPLS configurada para todos los miembros de la VPN usen el mismo VSI ID mientras el *VPN TARGET* es usado para identificar las relaciones VPN y el mismo espacio *VPN TARGET* es requerido en el modo BGP.

Como conclusión es importante destacar que el modo BGP es conveniente para el núcleo de grandes redes donde los PEs corren el protocolo BGP y tienen requerimientos de inter-AS. El modo LDP es aplicable cuando existen pocos sitios VPLS y raramente tienen requerimientos de inter-AS, especialmente cuando los PEs no corren el protocolo BGP. Cuando la red VPLS es grande (con numerosos nodos y extensión geográfica), el HVPLS combina estos dos modos: El núcleo adopta el modo BGP y el acceso adopta el modo LDP(Reyes 2007).

1.6 Funcionamiento Básico de una Red VPLS

En este epígrafe se dará una breve descripción del funcionamiento básico de una red VPLS donde se tomará como referencia la figura 1.4. Primeramente debe existir una malla completa de túneles MPLS conectada a la red MPLS. Debe crearse una instancia VPLS identificada por Svc-id 101 (identificador de servicio 101) entre PE1, PE2 y PE3; PE4 no participa en la instancia VPLS considerada. Se considera que esta configuración se

determinó usando un mecanismo de auto-detección no especificado. M1, M2, M3 y M4 son estaciones finales en distintas localizaciones del cliente y sus ACs a sus respectivos dispositivos PE han sido configurados en los PEs para pertenecer a una instancia VPLS concreta: Svc-id 101(J. Witters 2004).

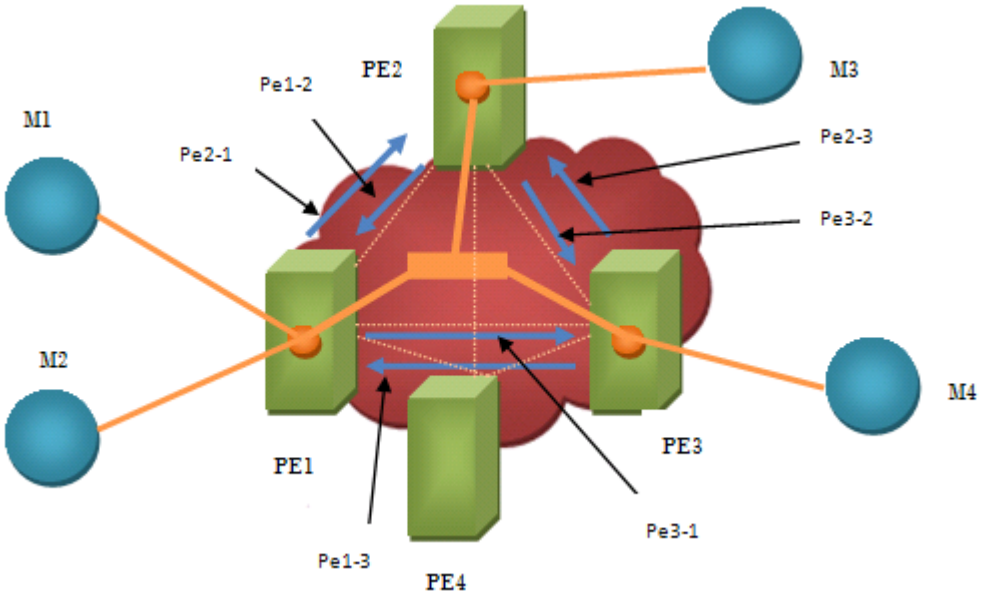


Figura 1.4) Funcionamiento de una red VPLS

1.6.1 Establecimiento de los Pseudo-Wire

Se necesita crear tres PWs, cada uno con un par de LSPs unidireccionales, o conexiones virtuales. Para señalizar la etiqueta-VC entre PEs, cada PE inicia una sesión que tiene como objetivo el PE par y le comunica qué etiqueta VC usar cuando envía paquetes al VPLS en cuestión. La instancia VPLS específica se identifica en el intercambio de señalización usando un identificador de servicio. Para la creación del primer pseudo-cable PE1 indica a PE2: "si tienes tráfico que enviarme por Svc-id 101, usa el pe2-1 de la etiqueta VC en el encapsulado de paquetes". A su vez, PE2 indica a PE1: "si tienes tráfico que enviarme por Svc-id 101, usa la etiqueta pe1-2 de la etiqueta VC en el encapsulado de paquetes"(Reyes 2007).

1.6.2 Aprendizaje de MAC y envio de paquetes

Una vez que creada la instancia VPLS con Svc-id 101, pueden enviarse los primeros paquetes y comienza el aprendizaje del MAC. Se supone que M3 está

enviando un paquete al PE2 destinado a M1 (M3 y M1 quedan identificados por una sola dirección MAC). PE2 recibe el paquete y reconoce (desde la dirección MAC de la fuente) que ese M3 se puede alcanzar en el puerto local 1/1/2:0; almacena esta información en el FIB para Svc-id 101.PE2 no conoce todavía el M1 de la dirección MAC de destino, así que inunda el paquete a PE1 con el pe2-1 de la etiqueta VC (en el túnel externo MPLS correspondiente) y a PE3 con el pe2-3 de la etiqueta VC (en el túnel externo MPLS correspondiente). PE1 conoce por el pe2-1 de la etiqueta VC que M3 está detrás de PE2 y almacena esta información en el FIB para Svcid 101. PE3 sabe por el pe2-3 de la etiqueta VC que M3 está detrás de PE2 y almacena esta información en el FIB para Svcid 101. PE1 retira el pe2-1 de la etiqueta, no conoce el M1 de destino e inunda el paquete a los puertos 1/1/1:100 y 1/1/1:200; PE1 no inunda el paquete a PE3 debido a la regla *Split-Horizon*. PE3 retira el pe2-3 de la etiqueta, no conoce el M1 de destino y envía el paquete al puerto 1/1/2:0; PE3 no inunda el paquete a PE1 debido a la regla del *Split-Horizon*.

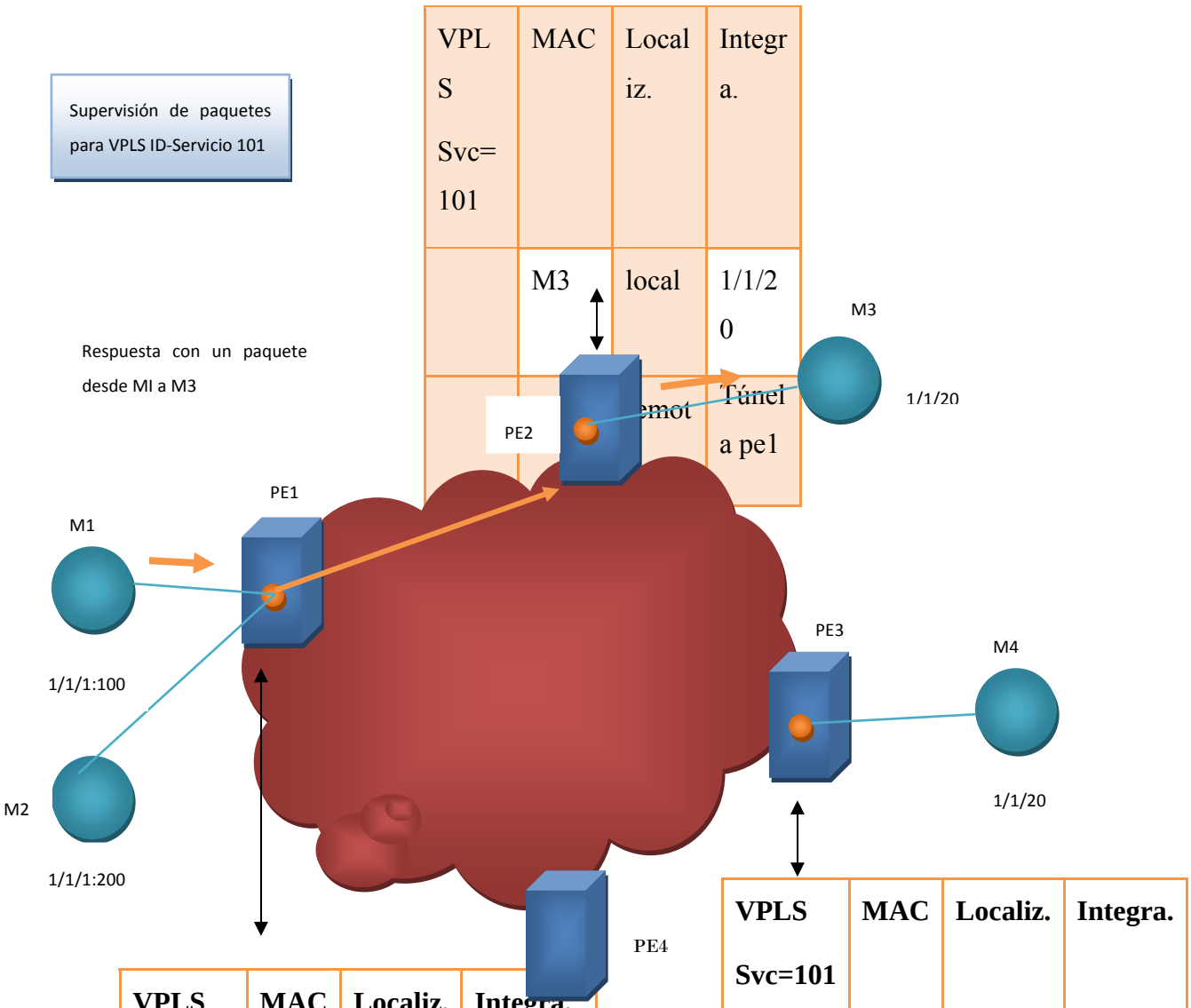
M1 recibe el paquete.

Cuando M1 recibe el paquete de M3, responde con un paquete a M3:

PE1 recibe el paquete de M1, reconoce que M1 está en el puerto local 1/1/1:100 y almacena esta información en el FIB para Svc-id 101. PE1 ya sabe que M3 se puede alcanzar vía PE2 y, por ello, solamente envía el paquete aPE2 usando la etiqueta VC pe1-2. PE2 recibe el paquete para M3 y sabe que M3 es accesible por el puerto 1/1/2:0.

M3 recibe el paquete.

El aprendizaje de direcciones MAC remotas necesita de un mecanismo de envejecimiento para remover las entradas relacionadas con etiquetas VC que no se han usado en mucho tiempo. Después que un paquete es recibido, el temporizador de envejecimiento (*aging timer*) correspondiente a las direcciones fuente será reiniciado. De igual forma, todas las direcciones MAC aprendidas en la VSI local deben ser *aged*(Reyes 2007).



- VB: Puente Virtual

Figura 1.6) aprendizaje MAC y envío de paquetes

1.7 VPLS Jerárquico

Tanto el modo BGP o el modo LDP de señalización para el VPLS, el establecimiento de una malla completa es un concepto básico para evitar la ocurrencia de lazos. Pero la existencia de una malla completa dificulta la escalabilidad de la red VPLS, por la gran cantidad de PWs que se establecen. Supongamos que existen 100 sitios, entonces deben ser establecidas 4950 sesiones LDP entre estos. Para dar solución a este problema se introduce el concepto HVPLS.

Otro problema que resuelve este modelo es la cantidad de direcciones MAC que tienen que aprender los ruters PE. A medida que crece el número de sitios, el número de direcciones MAC aumenta, y dado que estas no tienen una estructura jerárquica, como las direcciones IP, no pueden ser agrupadas para reducir las tablas de los ruters PE. *H-VPLS* permite "ocultar" al núcleo VPLS las direcciones MAC de los clientes.

Otra ventaja de esta arquitectura, es que permite la posibilidad de concentrar la inteligencia y complejidad de los ruters PE VPLS, en los puntos de presencia del proveedor (*POP*) y utilizar dispositivos más simples de cara al cliente, lo que repercute en una reducción en los costos, mayor facilidad y rapidez en el crecimiento del servicio.

La arquitectura H-VPLS se construye sobre la base de la solución VPLS, ampliándola para proporcionar distintas ventajas operacionales y de escala. Es especialmente útil en despliegues a gran escala con un gran número de PEs y/o MTU. El dispositivo MTU es frecuentemente referenciado como U_PE, con el PE del núcleo como un N-PE. Los proveedores de servicio instalan MTUs en edificios compartidos para dar servicio a distintas empresas radicadas en ellos; cada empresa puede, potencialmente, pertenecer a diferentes VPN VPLS(Reyes 2007)(Witters, De Clercq 2004).

Basados en el concepto general de *H-VPLS,* cada fabricante ha desarrollado de de forma muy particular la manera de implementarlo en sus equipamientos. A continuación citaremos algunos despliegues de *H-VPLS* de distintos fabricantes líderes del mercado.

HVPLS de HUAWEY

HUAWEI separa en sus arquitecturas los dos dominios, el núcleo y la frontera, basándose en el empleo de dos nuevos dispositivos que se muestran en la figura 1.7.

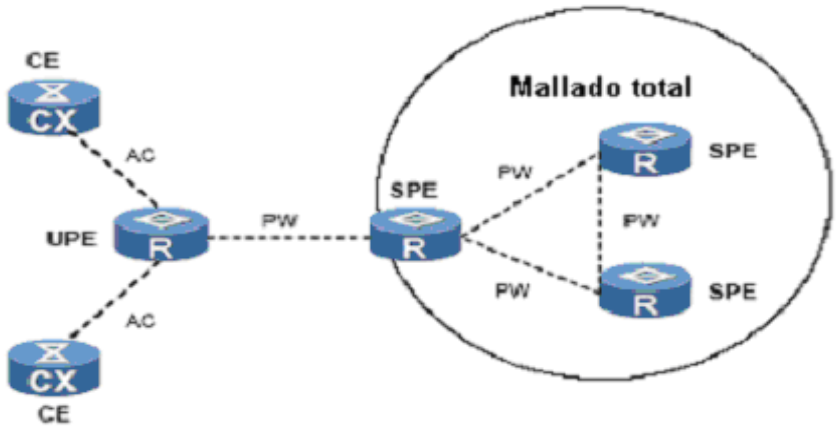


Figura 1.7) Modelo HVPLS de HUAWEY.

En esta figura, a los dispositivos de cara a la red se les denomina SPE o ruters PE de capa superior, mientras que los que se encuentran enlazados directamente con los ruters CE del cliente, y a través de un PW con el SPE, son los ruters UPE o ruters PE de capa inferior, es decir, estos últimos son los dispositivos de agregación de usuario, que soportan la asignación de ruta y la encapsulación MPLS. Los UPE se conectan con múltiples ruters CE y funcionan de puente, además con el empleo de estos, la carga en el SPE puede aliviarse. (2006)

HVPLS de CISCO.

Por otro lado, analizando la estructura que emplea otro de los fabricantes líderes del mercado, *CISCO*, como se observa en la figura 1.8, utiliza otra manera de denominarlos.

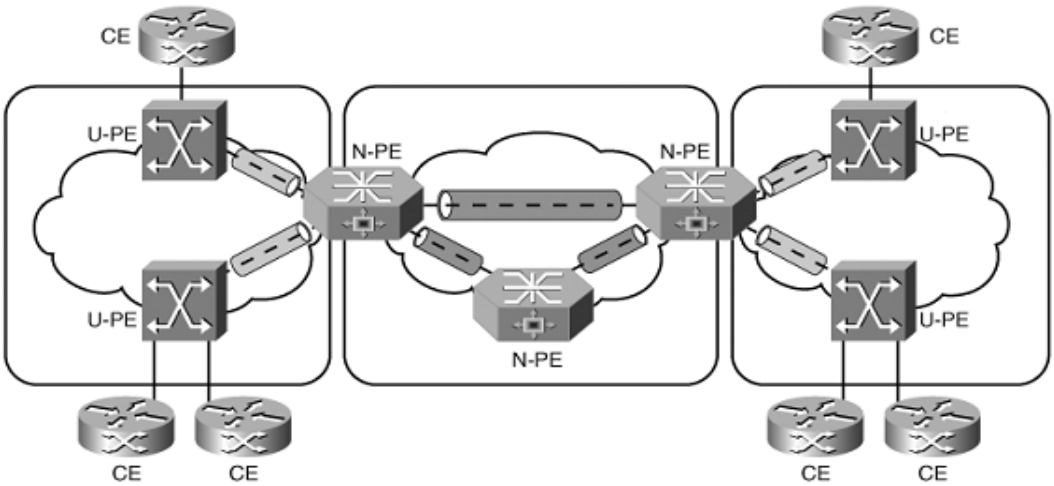


Figura 1.8) Modelo HVPLS de CISCO.

En este despliegue H-VPLS, el ruter PE de cara a la red del proveedor se le denomina NPE, y el dispositivo de cara al usuario o cliente, es el UPE. Es importante aclarar que este fabricante, se basa en dos proyectos, el primero de ellos *draft-khandekar-ppvpn-hvpls-mpls-00* descrito por Sunil Khandekar (Alcaltel) y el otro proyecto *draft-sajassi-vpls-architectures* de autoría Ali Sajassi (Cisco), ambos proyectos están recogidos en el proyecto de la IETF, *VPLS LDP*, que describe una arquitectura VPLS que consiste en una red MPLS extremo a extremo o también en una arquitectura que combine MPLS en el núcleo y Ethernet en la frontera.(Luo W. 2005)(Marc L. 2006)

En el primero de los casos, es decir, MPLS extremo a extremo, el dispositivo de frontera (UPE) debe soportar la imposición y extracción de etiquetas MPLS, señalización LDP, y suficientes recursos como CPU y memoria, mientras que el dispositivo (NPE) debe soportar conmutación lógica VPLS e imposición y extracción de etiquetas MPLS.

En el segundo de los casos, donde se combina MPLS y Ethernet, los dispositivos de frontera pueden ser conmutadores Ethernet estándares que empleen IEEE 802.1q etiquetas VLAN para poder separar las VPN, con esta solución se incurriría en menos gastos de los dispositivos de fronteras. (Martinez D. 2007)

1.8 Conclusiones Parciales del Capítulo

Aunque los servicios de capa 2 basados en MPLS, como VLL y VPLS, son relativamente nuevos, los proveedores de servicio ya los ofrecen en todo el mundo. Su éxito inicial se puede atribuir al hecho de que utilizan MPLS en la red del proveedor de servicios combinado con FR/ATM y Ethernet como traspaso a la empresa para VLL y Ethernet para VPLS.

Los servicios de capa 2 basados en MPLS ofrecen a los clientes de empresa lo que necesitan exactamente para la conectividad entre sucursales: transparencia de protocolo, ancho de banda escalable y granular a partir de 64 kbit/s y hasta 1 Gbit/s, rápida activación y suministro de servicios y una frontera de LAN/WAN simplificada. VPLS también permite a los proveedores de servicios suministrar una oferta de servicios VPN escalable que puede combinarse con el acceso a Internet en una infraestructura consolidada IP/MPLS, reduciendo así los gastos de explotación. VPLS ha recibido ya el apoyo generalizado de la industria, tanto de fabricantes como de proveedores de servicios.

VPLS tiene importantes ventajas tanto para los proveedores de servicios como para los clientes. Los proveedores de servicios se benefician porque pueden generar ingresos adicionales, ofreciendo un servicio Ethernet con el ancho de banda flexible y sofisticados acuerdos de nivel de servicio (SLA). VPLS es también más sencillo y más económico de operar que un servicio tradicional. Los clientes se benefician porque pueden conectar todos sus sitios a una VPN Ethernet que proporciona una velocidad segura.

CAPÍTULO 2. VPLS, ANÁLISIS DE ESCENARIOS DE APLICACIÓN

2.1 Implementación de Servicios VPLS

Existen dos direcciones importantes a la hora de la implementación del servicio VPLS que ha sido discutido a manos del IETF, las cuales la mayoría de los vendedores está teniendo en cuenta las circunstancias para una perspectiva de ejecución. La primera es "draft Kompella" y la segunda es "draft Lasserre-Vkompella". Cada uno de estos modelos puede ser descrito por dos características fundamentales que son el auto descubrimiento y la señalización.

2.1.1 Auto- Descubrimiento

El auto descubrimiento es absolutamente crítico para habilitar proveedores de servicios para mantener bajos los costos de operación. A fin de comprender el auto-descubrimiento, se asume que un nuevo PE es sumado por el proveedor de servicios. Una sesión de BGP sencilla es establecida entre el nuevo PE y un ruter reflector. El nuevo PE es unido entonces a un dominio VPLS (por ejemplo, una nueva sucursal está abierta y necesite la conectividad) cuando la instancia VPLS es configurada en ese PE, y uno o más puertos de guarnición de cliente en ese PE estén asociados con esa instancia VPLS. Una vez que esto ocurre, el PE anuncia que es parte del dominio VPLS por la vía del reflector de ruta a otros PE que están unidos en esa instancia VPLS. Ahora todos los PE son "conscientes" del nuevo PE y ahora tienen toda la información que necesitan para establecer un túnel LSP con el nuevo PE de forma automática. Debido a que con draft Lasserre-Vkompella no está

especificado el auto-descubrimiento pues el proveedor de servicio debe conocer específicamente cuáles PE forman parte de la instancia VPLS.

Para cada instancia VPLS presente en un PE, el proveedor de servicio deberá tener la configuración del PE con las direcciones de los demás PE que son parte de la instancia VPLS. Existe un número de vías para que esta información sea almacenada, ya sea en una base de datos LDAP o en un sistema de aprovisionamiento, pero todos estos mecanismos son operacionalmente intensivos y están sujetos al error humano. Es interesante notar que este mismo asunto del autodescubrimiento se ha dirigido muchas veces en el pasado y en la mayor parte de los casos finalmente apuntaban hacia BGP. {Capuano, 2003 #11}(Martínez 2007).

2.1.2 Señalización

El modelo de VPLS sustentado draft Kompella aboga por BGP para la señalización. Alternativamente el modelo VPLS propuesto por draft Lasserre-Vkompella define LDP como un mecanismo de señalización. Existen dos argumentos en contra del uso de BGP para la señalización que se refieren específicamente primero a que BGP es muy complejo de usar y segundo que requiere de pre-bloques a la hora de la distribución de etiquetas. Sin embargo estos argumentos son algo triviales. Ya que muchos proveedores están ahora desplegando VPNs que usan BGP y mientras que la distribución de pre-bloque es requerida, la pre-definición de tamaños de bloque no tiene ningún impacto en los recursos hasta que las etiquetas reales dentro del bloque sean asignadas o configuradas (Reyes 2007).

Por otra parte los argumentos en contra de la señalización LDP si son significativos. En primer lugar debido a que draft Lasserre-Vkompella no define el autodescubrimiento, cada vez que un PE se une a un dominio VPLS, el proveedor de servicios debe buscar manualmente los otros PE que son parte del dominio VPLS. Una vez esta información es lograda, deben construir entonces una malla completa de sesiones LDP entre ese PE y cada dos PE que sean parte del dominio VPLS. Estos tremendos gastos generales de una malla completa de las sesiones de LDP son requeridas porque LDP no tiene la ventaja de la arquitectura del ruter reflector de BGP. Para un proveedor de servicios que ofrece el servicio VPLS para sólo unas cuantas empresas con un número muy pequeño de sitios en

cada empresa, la carga de LDP no llega a ser perceptible. Sin embargo, la carga se convierte en más y más significativo con el crecimiento del servicio. En segundo lugar, la operación con las sesione LDP se convierte en un desafío aún más perceptible, cuando un proveedor de servicios opta por autenticar las sesiones de señalización LDP por la vía de MD5. Con una malla completa de sesiones LDP, las llaves MD5 necesitan ser configuradas en uno u otro fin en cada sesión LDP.

En tercer lugar, si la instancia VPLS cubre sistemas autónomos múltiples, el mundialmente conocido identificador de circuitos virtuales de 32 bits usado por la señalización LDP requiere una operación manual intensiva en la coordinación entre sistemas autónomos, en otras palabras si una instancia VPLS cubre 3 sistemas autónomos los tres proveedores de servicio necesitarían usar el mismo identificador de circuitos virtuales para ese VPLS y finalmente si *draft Lasserre-Vkompella* alguna vez especifica BGP para el autodescubrimiento entonces requeriría de la sincronización de BPG y LDP. Incluso si las sesiones LDP ya existen entre los PEs, aún se necesitaría BGP para comunicar cuales PEs necesitan el establecimiento de los túneles LSP.{Capuano, 2003 #11}

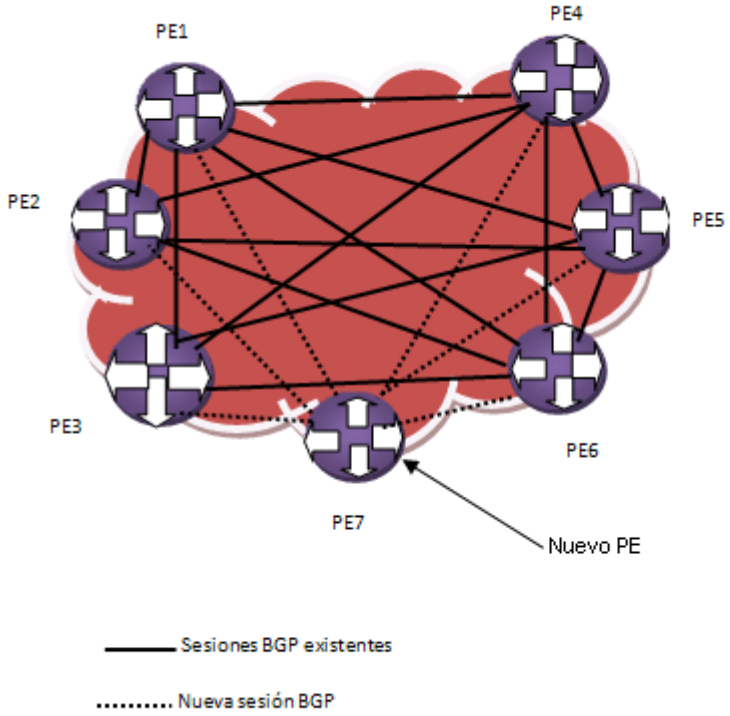


Figura 2.1) Usando LDP se necesita establecer una malla completa de sesiones LDP cuando se agrega un nuevo PE.

En contraste con este acercamiento de usar BGP para la señalización como fue propuesto por draft Kompella, cuando un PE es añadido, sólo una sesión de BGP entre él y el ruter reflector necesita ser establecida. Si la sesión va a ser autenticada con MD5, entonces loas únicas llaves que deben ser establecidas son las de los dos puntos extremos de esa sesión BGP. Cuando una nueva instancia VPLS es configurada en ese PE, este anuncia entonces su disponibilidad por la vía del ruter reflector.

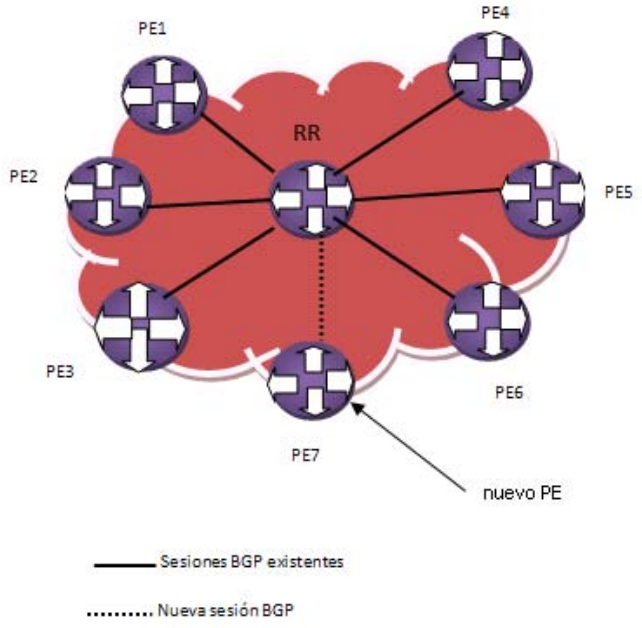


Figura 2.2) Las sesiones BGP solo necesitan ser establecidas entre el nuevo PE y un ruter reflector.

2.2 Factores decisivos para lograr un buen servicio VPLS.

Una vez que una empresa apuesta por VPLS, ha de tener en cuenta cinco factores importantes a la hora de elegir oferta.

1. **Cobertura geográfica.** Algunas versiones de VPLS están disponibles internacionalmente, mientras que otras se limitan a determinadas áreas geográficas o metropolitanas, antes de firmar con un proveedor de VPLS, es preciso asegurarse de que dispone de la cobertura geográfica necesaria no sólo hoy, sino durante los próximos cinco años.
2. **Incremento de la velocidad y granularidad.** Casi todos los proveedores de VPLS ofrecen la opción de incrementar la velocidad de los puertos y la granularidad. Por regla general, la mayoría proporcionan al menos tres tamaños de puertos en múltiples servicios Ethernet (10, 100 y 1 Gbps) y un número creciente ofrece -o planea hacerlo- puertos de 10 Gbps para dar servicio a sedes con grandes requerimientos de conectividad.
3. **Tipo de servicio.** La mayoría de operadores proporcionan diferentes tipos de servicios que pueden utilizarse en diferentes aplicaciones y tipo de tráfico a través de la red VPLS. Algunos, por ejemplo, permiten a sus usuarios priorizar el tráfico en función de cuatro clases de servicio: *Real Time Data* para aplicaciones avanzadas como *VoIP*; *Priority Data* para datos de misión crítica y aplicaciones de vídeo;

Business Data para datos transaccionales y aplicaciones basadas en peticiones; y *Basic Data* para aplicaciones menos sensibles a la calidad de servicio.

4. **Soporte de aplicación.** El simple acceso a una única sede se puede solventar con EPL en lugar de VPLS. Donde alcanza su valor VPLS es en el caso de aquellas empresas que necesitan rápida conectividad multisede para manejar aplicaciones como conectividad entre centros de datos, recuperación frente a desastres, *VoIP*, redes de área de almacenamiento e incluso aplicaciones de planificación de recursos empresariales y gestión de relación con los clientes.
5. **SLA.** Los SLA difieren enormemente entre operadores y pocos se acercan a lo habitualmente ofrecido en servicios *ATM/Frame Relay*. Las herramientas para monitorizar y gestionar SLA mejorarán mucho en breve, sin embargo, lo que restará importancia a este problema.

2.3 El Protocolo de Elasticidad y Balance de Tráfico (RTBP) en VPLS

Las actuales implementaciones de VPLS no proveen un acceso flexible y el protocolo STP que sí necesita de esta característica pues lo hace con demoras de reconfiguración considerables. En este epígrafe se describirá un nuevo protocolo RTBP que provee flexibilidad y balance en la carga de las redes VPLS. El protocolo maneja automáticamente fallas y restablecimientos de enlaces, redistribuyendo la carga entre los enlaces activos restantes. El protocolo es simple de desplegar: solo los nodos de acceso para VPLS requieren un software de modificación. El protocolo ha sido implementado en muchas pruebas llevadas a cabo y ha arrojado resultados muy favorables para las redes como el bajo tiempo de reconfiguración, por lo que se ha decidido incluir este protocolo en nuestro estudio para futuras implementaciones en nuestro país.

El protocolo de RTBP fue diseñado para prepararse para una recuperación rápida en caso de un enlace fallido. Los nodos PE que manejan cada sitio de cliente mantienen la huella de otros posibles nodos, implementando un tipo de protocolo llamado *keep-aliv*e. El equilibrio de carga es logrado basándose en las direcciones fuentes de las tramas. Se asume que el CE que une el sitio a la WAN es un conmutador Ethernet.

Un ruter PE corre el protocolo RTBP en sus interfaces de acceso (interfaces LAN), comportándose como un puente de aprendizaje.

• Si la dirección de destino de la trama es conocida la trama es remitida como en un puente

tradicional.

• Si la dirección de destino de la estructura es desconocida, en la emisión se ejecuta la función de *Hash* basada en las direcciones de fuente para decidir si este PE esta actuando como el servidor de RTBP para esta dirección fuente especifica. Si es así, se comporta nuevamente como un puente tradicional y envía la trama. De otro modo la trama es descartada (debe existir otro PE actuando como el servidor de RTBP para esta Dirección fuente específica).

La función de *Hash* es ejecutada en la dirección de fuente para garantizar que todas las tramas de información vienen de la misma fuente a un destino localizado en otro sitio. De otra manera, los caminos y las entradas correspondientes en las tablas de envío pueden exponer comportamiento de oscilación.

Con cada corrida de PE el protocolo lanza un mensaje de RTBP *HELLO* por todas sus interfaces LAN cada T segundos. El mensaje incluye:

• un ID de PE único (la dirección de retroceso de lazo, y valores administrados, etc.)

• un ID de interfaz único, la dirección MAC, solo en caso de que el PE tenga varias interfaces al mismo VPLS.

Las tramas RTBP *HELLO* no son ni enviadas ni reconocidas por los PE.

Cuando un PE recibe una trama RTBP *HELLO* con un nuevo ID un PE servidor del mismo sitio de cliente es hallado y el PE se prepara para balancear la carga de tráfico entre ellos. La duración de la función Hash es entonces dividido en (R +1) zonas donde R es el número de los PE servidores conocidos en el sitio.{J.M. Arco, #3}

2.3.1 Implementación de Protocolos

Se ha implementado el protocolo RTBP en un simulador que tiene una entidad VPLS (cliente A) con dos sitios (sitio1 y sitio2), el sitio 1 es *multi-homing*. Los PEs son PC con posibilidades de implementar el servicio VPLS y se han utilizado enlaces Ethernet a 100Mbps.

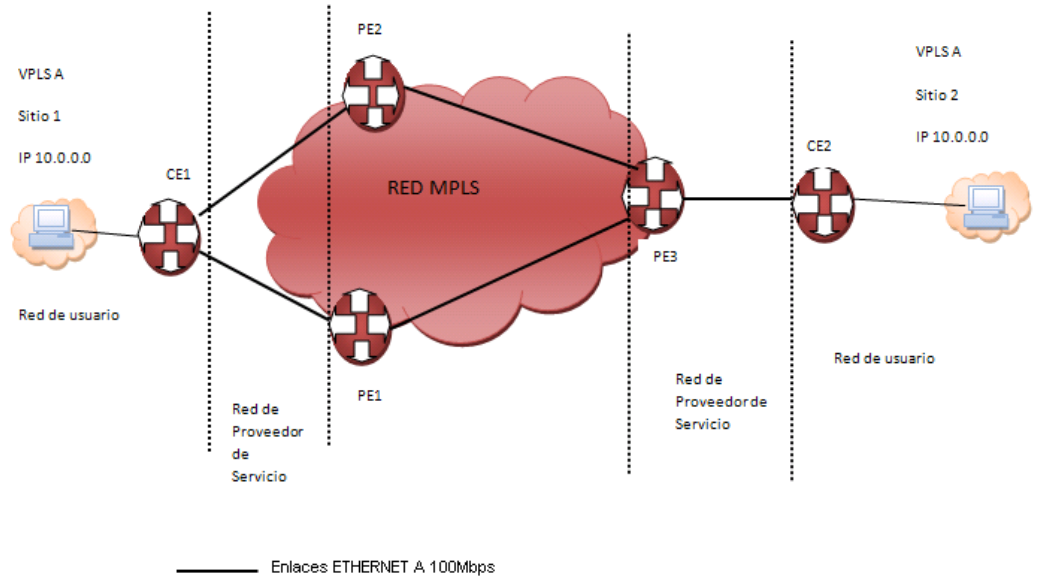


Figura 2.3) Implementación del protocolo RTBP

El protocolo procede de la siguiente manera:

Cuando una trama Ethernet llega al PE de entrada o PE1 se envía a la entidad Ethernet por un driver Ethernet y posteriormente estas tramas son enviadas a la entidad VPLS. El PE tiene la funcionalidad de puente y aprende las direcciones MAC de fuente y busca una interfaz de salida en la tabla de direcciones MAC, en este mismo momento el protocolo realiza un hash para decidir la interfaz de salida. Las tramas luego son encapsuladas en un mensaje MPLS con dos niveles y finalmente son enviadas a la entidad Ethernet y se realiza una cola para la transición en la red MPLS.{J.M. Arco, #3}

2.4 Escenarios de Aplicación para VPLS

En este epígrafe se va a describir dos escenarios de aplicación para VPLS de un ruter PE, en los cuales se podrá comprobar las posibilidades del ruter para implementar dos de las características del servicio VPLS que son: la funcionalidad y la escalabilidad de VPLS. En ambos escenarios se requiere de un probador que pueda simular la topología de una red de MPLS de proveedor de servicios y soporte el ruteo necesario y la señalización de protocolos. El probador debe también ser capaz de emular el tráfico de los clientes de VPLS generando múltiples VLAN de nivel 2 o cadenas de Ethernet nativo, y de esta forma

que conduzca a medidas en tiempo real de ejecución en este tráfico. Finalmente, el probador debe proporcionar una buena vía para detectar el escape de VPN inspeccionando las etiqueta de pila y verificando exactitud del envió. En ambos escenarios descritos debajo, el dispositivo en prueba (DUT), es un ruter PE habilitado.

2.4.1 Probando la Funcionalidad de VPLS

Esta prueba mide las capacidades funcionales básicas del ruter PE, habilitado específicamente para ser capaz de:

- ✓ Preparar una malla completa de conexiones virtuales sobre el pre-establecimiento de los túneles LSP.
- ✓ Aprendizaje de direcciones MAC.
- ✓ Correcto encapsulamiento y envío del tráfico de VPLS conteniendo las direcciones MAC de destino conocidas y desconocidas.(marzo 2003 #1}

La prueba exige dos puertos de prueba. En primer lugar, la topología de prueba está preparada, con un puerto de prueba configurado como un dispositivo CE local anexado al dispositivo bajo prueba por la vía de enlace punto a punto, y un segundo puerto de prueba usado para anunciar un simulado de la red de proveedor comprendiendo una malla de proveedor y un ruter (PE), con los dispositivos de CE configurados detrás de los ruters PE para simular sitios VPN remotos en la VPLS. La base de información de envío de cada dispositivo CE simulado es poblada con un conjunto de direcciones MAC para simular estaciones finales de cliente de VPLS. Una malla completa de túneles entrantes y salientes es preparada entre el dispositivo bajo prueba y todos los ruters PE. La configuración de esta prueba es ilustrada en la figura 2.6. El próximo paquete contiene direcciones MAC fuente desde los sitios remotos de la VPN simulada y son enviados desde el segundo puerto de pruebas del dispositivo bajo prueba, este dispositivo debe aprender las direcciones — es decir, crear entradas en su base de información de envío para cada una. Las tramas Ethernet de capa 2(VLAN marcadas o no, en dependencia de las necesidades de la prueba) pueden ahora enviarse desde el sitio de la VPN remota local en el primer puerto de prueba a direcciones en los sitios remotos de la VPN en el segundo puerto de prueba para verificar la habilidad del dispositivo bajo prueba para encapsular y enviar el tráfico con el túnel

correcto y los niveles VC LSP. Dos pilas de nivel de tráfico se envían en la dirección contraria del segundo puerto de prueba a direcciones en la VPN local adjunta en el primer puerto de prueba para verificar que el dispositivo bajo prueba pueda echar etiquetas e insertar las correctas VLAN marcada con etiqueta de información, si es requerido. Finalmente, el tráfico contenido en las direcciones MAC de destino desconocidas son enviadas desde el primer puerto de prueba para verificar las capacidades del dispositivo de duplicar e inundar.

Las estadísticas son tomadas durante cada uno de estos pasos para relatar el número de tramas de información perdidas, niveles de tramas pérdidas, tramas con etiqueta de VLAN incorrecta y entradas perdidas o incorrectas en la base de información de envío del dispositivo bajo prueba. {, Marzo 2003 #1}

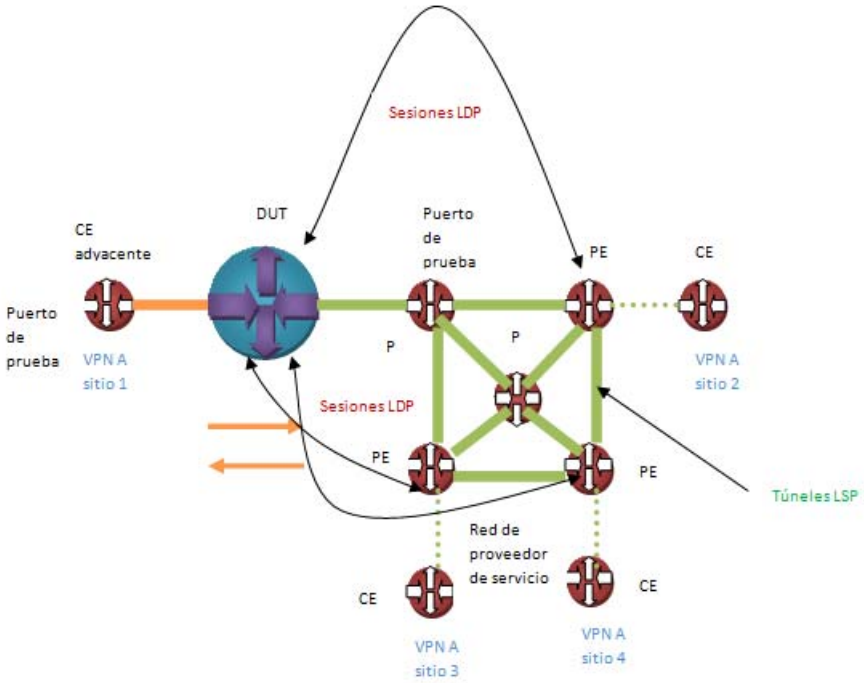


Figura 2.6) Funcionalidad de VPLS

2.4.2 Probando la Escalabilidad de VPLS

Esta prueba toma como punto de partida el primer escenario para determinar cuántas VPN puede establecer y mantener un ruter, también se prueba la capacidad de co0municación entre las VPN en condiciones extremas. A fin de simular el número máximo de VPN requeridas, el probador debe tener la habilidad para soportar múltiples sub interfaces en una interfaz física simple. La preparación de la topología de prueba es como se ilustra en la figura 2.7. Las Sub-interfaces en el primer puerto de prueba son simuladas por separado de las VPN locales conectadas vía punto a punto. Como Después de verificar que el dispositivo bajo prueba puede remitir exactamente el tráfico entre los sitios de cliente para una VPN, la estrategia de esta prueba es mantener preparando más y más VPN, como sigue:

- sub interfaces adicionales en el primer puerto de prueba son configurado para simular nuevos clientes de VPN locales.
- La topología del segundo puerto de prueba es expandido para añadir un sitio VPN remoto para cada nuevo VPN de cliente en el primer puerto de prueba.
- una malla completa de túnel LSP son establecidas para cada nueva VPN.
- El tráfico se envía desde cada nuevo dispositivo CE en el segundo puerto de prueba para el dispositivo bajo prueba, así nuevas bases de información de envío VPLS pueden ser creadas y pobladas.{, marzo 2003 #1}

La prueba continúa aumentando el número de VPN por el mismo incremento hasta que el número máximo de VPN es alcanzado. A cada iteración, el tráfico es enviado en ambas direcciones y son tomadas medidas para verificar la correcta encapsulación del nivel de pila, y el correcto envió de túneles LSP y sub interfaces.

Este escenario es particularmente importante porque ello responde la pregunta crítica para los fabricantes de equipo de red y proveedores de servicios: Bajo condiciones extremas de internet puede un ruter PE habilitado preparar sesiones de T-LDP y VC LSP, Aprender direcciones MAC, duplicar tramas, y encapsular y enviar tráfico de cliente sin escape de VPN.{, Marzo 2003 #1}

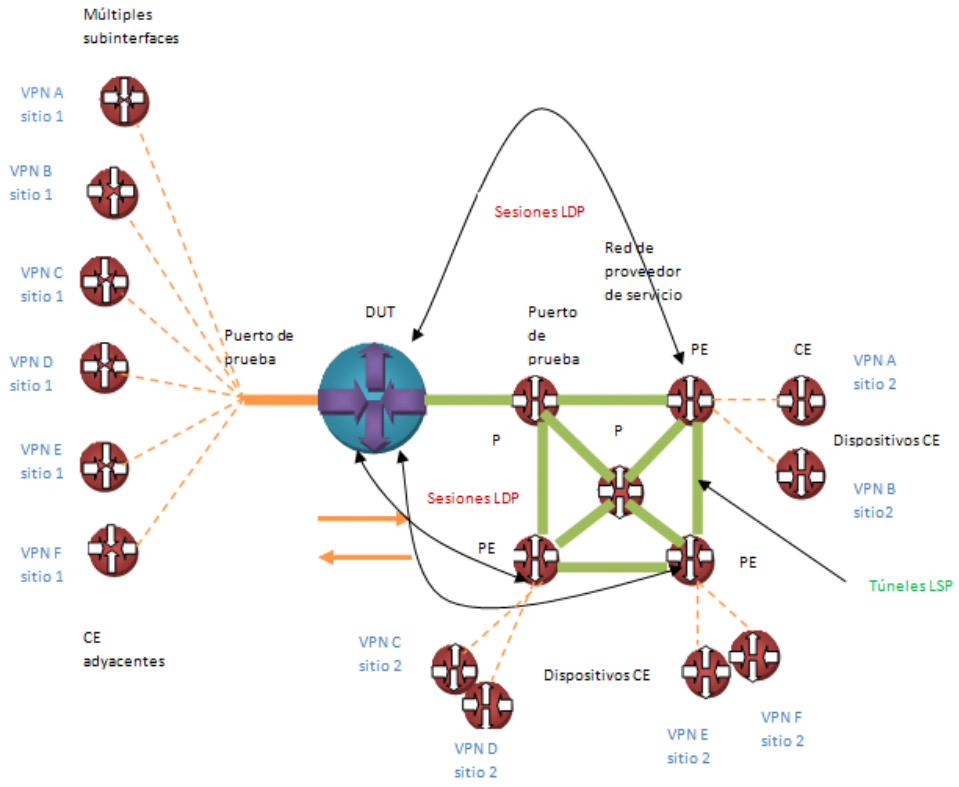


Figura 2.7) Probando la escalabilidad de VPLS

2.5 Características que debe cumplir el Router PE

Las funciones del ruter de frontera del proveedor, en VPLS, hay que dividirlas en 2 secciones, uno referido a las funciones del Plano de Control y otro referido a las funciones del Plano de Datos.{González, 2007 #8}

- ✓ **Funciones del Plano de Datos del ruter PE en VPLS.**

Las funciones del Plano de Datos son las siguientes:

1. Encapsulado: Cuando el ruter PE recibe una trama Ethernet desde un ruter CE, el PE la envía a la red del proveedor después de la encapsulación.
2. Envío**:** El modo de enviar paquetes depende de la interfaz que se reciben los

paquetes y de la dirección MAC destino de los paquetes.

- ✓ **Funciones del Plano de Control del ruter en VPLS.**

En la sección anterior, se mencionan las funciones del plano de envío para VPLS. Ahora nos centramos en los mecanismos del plano de control. Hay dos aspectos que se deben considerar: {González, 2007 #8}

1. Descubrimiento de Miembros.
2. Mecanismo de Señalización.

2.6 Posibles Escenarios de Aplicación para VPLS en Cuba

Con el estudio se han identificado tres sectores de la vida social del país que por los requerimientos de sus redes podrían constituir clientes potenciales de este servicio:

Escenario #1: Sector de la salud

El sector de la salud está tomando ventaja de las nuevas tecnologías para modernizar la forma en que sus servicios son ofrecidos. La investigación y el estudio sobre el bienestar de los individuos precisan hoy más que nunca de datos de alta calidad y de resultados que tengan como base estudios interdisciplinarios, teniendo en cuenta que la salud y el bienestar humanos son la base y la razón de ser de todos los esfuerzos del desarrollo. El logro de la meta "Salud Para Todos" depende en gran medida del aporte y acceso a la información misma.

Actualmente el Sistema Nacional de Salud de Cuba cuenta con una poderosa red telemática (INFOMED) y una de las más grandes del país con aproximadamente unos 400 enlaces conectados a nivel nacional, entre ellos 57 hospitales, 152 policlínicos y 9 bancos de sangre. Recientemente se benefició con la conexión de un enlace de 155 Mb/s a su nodo

principal. Esta intranet contribuye al mejoramiento de la atención clínica, la docencia, la investigación y la gestión de salud.

Requerimientos del servicio:

- Llamadas de voz inter-clínica, telemedicina, monitoreo de enfermos, captura de datos de pacientes en línea y en general e-mail/ navegación Internet para la superación y actualización del personal médico.
- Mantener reglas de confiabilidad estricta, indisponibilidad para compartir información de ruteo.
- Conexión simple para todas las aplicaciones en cada sitio.
- Videoconferencias.
- Sistemas de gestión de imágenes médicas (DIMCO).

Fundamentos para la selección del servicio

- Indisposición de no compartir información de ruteo.
- Desempeño de garantías de acuerdos de niveles de servicio (SLA).
- Soporte de conectividad multipunto.

Escenario #2 – Sector de Educación.

La irrupción de la informática y las nuevas tecnologías en las universidades cubanas está revolucionando radicalmente el quehacer científico y estudiantil. Grandes redes, con cientos de computadoras conectadas entre sí, ponen en el monitor de la computadora libros, materiales de consulta diversos, las actividades de la FEU o el horario del comedor, y hasta las preguntas de "la tarea" que dejó el profesor en su última conferencia.

No se trata de un empeño aislado de determinadas universidades. El Ministerio de Educación Superior (MES), cuenta hoy con 65 centros junto a las 3 150 sedes universitarias que imparten clases en los 169 municipios, dispersos por cada rincón de la geografía cubana.{Dávalos, 2006 #13} El futuro: enlazarlos a través de una poderosa red nacional.

Actualmente el MES trabaja en lograr estructurar una gran red universitaria a nivel nacional, que conectaría a todas las universidades y centros de investigación.

REDUNIV, como se llamaría la magna extranet, también posibilitaría, entre otras cosas, la impartición de postgrados a distancia, o que un profesor de la Universidad de La Habana aclarara una duda a un alumno de Santiago de Cuba, o uno de Cienfuegos les impartiera clases on-line a sus alumnos en Matanzas.

Requerimientos del servicio:

- Conectividad multipunto.
- Soporte Multiprotocolo (No solo IP)
- Alta disponibilidad.
- Videoconferencias.
- Videostreamings.

Fundamentos para la selección del servicio

- Multiprotocolo para soporte de aplicaciones no solo IP.
- *Dual-Homing* de centros de datos para minimizar los tiempos de caídas del servicio e incrementar la disponibilidad.
- Soporte de conectividad multipunto

Escenario #3: Sector de Administración Pública

Los departamentos de la Administración Pública son descentralizados para localizar al cuerpo administrativo más cerca del pueblo al que sirven con oficinas locales, oficinas regionales y sedes nacionales. Las pérdidas de servicio repercuten en la productividad que el público espera y aísla las oficinas. Con el uso del servicio VPLS se producirá una mejoría significativa en el acceso a la información administrativa por parte de los ciudadanos, ya sea información de carácter general o de interés particular asociada a tramitaciones y gestiones en curso, lo que conllevará a reducciones apreciables en la necesidad de desplazamientos de los interesados para realizar gestiones administrativas, y mayores posibilidades y simplificación en la presentación de solicitudes y reclamaciones.

Requerimientos del servicio:

- Conectividad multipunto.
- Soporte Multiprotocolo (No solo IP)

- Alta disponibilidad
- Posibilidad de retener el control de ruteo.
- Transparencia del servicio para acomodar datos encriptados del cliente.

Fundamentos para la selección del servicio:

- Multiprotocolo para soporte de aplicaciones no solo IP.
- *Dual-Homing* de centros de datos para minimizar los tiempos de caídas del servicio e incrementar la disponibilidad.
- La conmutación Ethernet no requiere compartir información de ruteo.
- La conmutación Ethernet es transparente a los protocolos de encriptación utilizados por el cliente.

2.7 Conclusiones Parciales del Capítulo

El estudio de los escenarios de aplicación para el servicio VPLS nos permite dar un resultado definitivo de los sitios donde mejor se desempeña el servicio y para los cuales resulta más efectivo. A pesar de que la implementación usando señalización mediante el protocolo de distribución de etiquetas resulta más complicada que utilizando BGP, no es recomendable abandonar su uso pues en determinados escenarios resulta muy efectivo a la hora de realizar el mallado completo. Es importante antes de implementar el servicio estudiar de manera detallada las necesidades de cada empresa, como el tipo de enlace, etc. Para que se pueda escoger el escenario más adecuado para esa empresa en particular y de esta forma poder tener el 100 % de efectividad del servicio.

Con los escenarios de aplicación estudiados en este capítulo nos hemos podido percatar de las grandes potencialidades que presenta el servicio VPLS como son su escalabilidad y funcionalidad, para cada una de ellas con sus características específicas. Tener en cuenta las capacidades del ruter PE a la hora de habilitarlo para poder implementar el servicio es sumamente importante, pues de este dispositivo depende prácticamente casi toda la funcionalidad de la red. En nuestro país hay muchas empresas que por sus características, el implemento del servicio VPLS, contribuiría a un cambio radical en su red, logrando

eficiencia, calidad en el servicio, velocidad y un importante beneficio en su ancho de banda disponible, por lo que sería un gran acierto pensar en la posibilidad de migrar hacia las redes LAN privadas virtuales.

CAPÍTULO 3. ANÁLISIS DE RESULTADOS

3.1 Introducción

En este capítulo se llevaron a cabo una serie de simulaciones para ver de manera práctica, las potencialidades del servicio a implementar. A pesar de que las redes escogidas no son específicamente redes VPLS, se escogieron dos redes que por sus características de configuración son muy similares a este servicio que hoy nos ocupa. Aun así en epígrafes posteriores se dará una explicación de cómo configurar VPLS sobre una red MPLS.

3.2 Configurando VPLS sobre una red MPLS

BGP o LDP pueden ser usados para autodescubrimiento y señalización de VPLS. El método para configurar VPLS difiere en dependencia del protocolo usado, BGP o LDP.

3.2.1 VPLS basado en BGP

BGP en una red VPLS es configurado en el ruter de proveedor de servicio (P) y en el ruter de borde de proveedor de servicio (PE). La configuración de BGP consiste en tres pasos fundamentales: {González, 2007 #8}

- Crear un túnel LSP entre los ruters PE.
- Configurar IGP en los ruters PE y P.
- Configurar una sesión IBGP entre los ruters PE.

Creación de los túneles LSP entre los ruters PE:

Un túnel LSP son conexiones punto a punto establecidas entre los ruters PE que agrega y transfiere tráfico a usuarios individuales. Antes de crear un túnel LSP primero es necesario habilitar MPLS en todas las interfaces de los ruters. Los LSP pueden ser configurados

dinámicos o estáticos usando diferentes protocolos para la señalización. Para VPLS los ruters PE deben tener una malla completa de túneles LSP dinámicos.

Configurando un IGP en los ruters P y PE:

Para trabajar apropiadamente con VPLS, los ruters P y PE deben estar habilitados para intercambiar información de ruteo. Esto implica que se deba configurar IGP o rutas estáticas entre estos ruters. Si se ha configurado LSP dinámicos o estáticos para crear túneles LSP es necesario configurar OSPF como el IGP.

3.2.2 VPLS basado en LDP

VPLS basado en LDP usa LDP como el protocolo para el autodescubrimiento y la señalización. Los ruters PE deben tener módulos de nivel 2 y 3. Los ruters de borde de clientes (CE) deben estar conectados al módulo de nivel 2 del ruter PE. El procedimiento para la creación de un túnel LSP entre los ruters PE y para configurar un IGP en los ruters P y PE es el mismo que para VPLS basado en BGP. {González, 2007 #8}

3.3 Escenario 1: VPN basado con túneles IP

Esta red se escogió debido a su similitud con el servicio VPLS, ya que los túneles IP pueden ser usados para varios propósitos, como por ejemplo la construcción de VPNs entre diferentes sitios de una empresa sobre la red de INTERNET, esto significa que pueden conectar dos sitios con una dirección IP privada sobre una red pública. Las interfaces de los túneles son capacitadas para ejecutar el ruteo de protocolos.

3.3.1 Estructura de la Red simulada

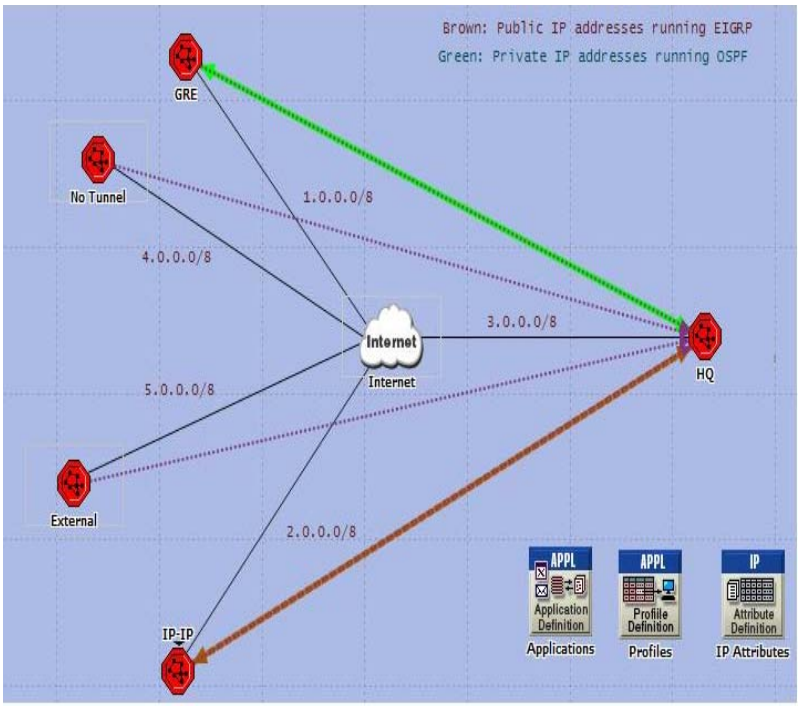


Figura 3.1) red VPN con túneles IP.

El escenario consiste en una red de empresa con varios sitios:

HQ: Este sitio usa internamente direcciones IP privadas y es conectado a INTERNET por una interfaz con una dirección IP pública.

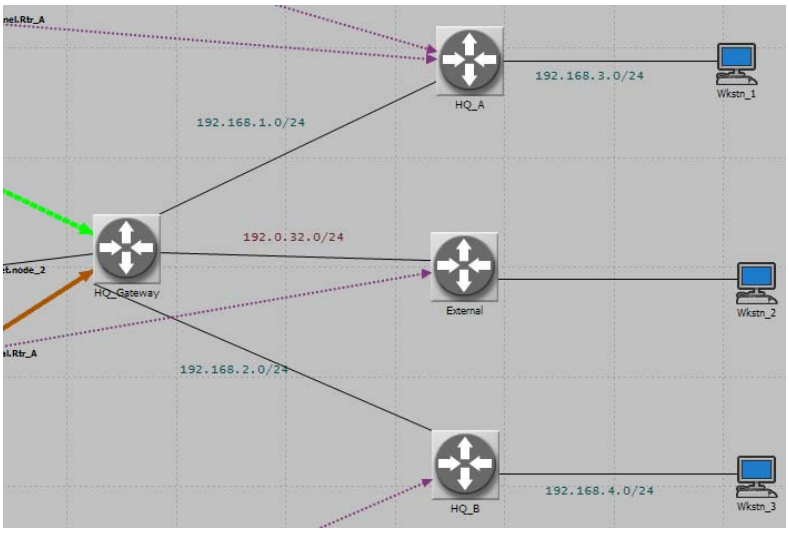


Figura 3.2) Estructura interna del sitio HQ.

GRE: Este es un sitio VPN remoto, su configuración es similar a la de HQ, es conectada al *gateway* HQ mediante un túnel GRE.

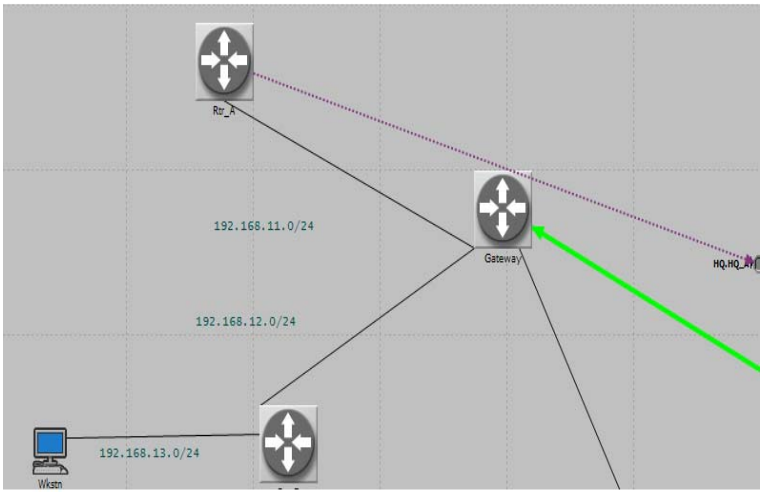


Figura 3.3) Estructura interna del sitio GRE

IP-IP: Este es otro sitio VPN remoto que se conecta al Gateway mediante túneles IP-IP.

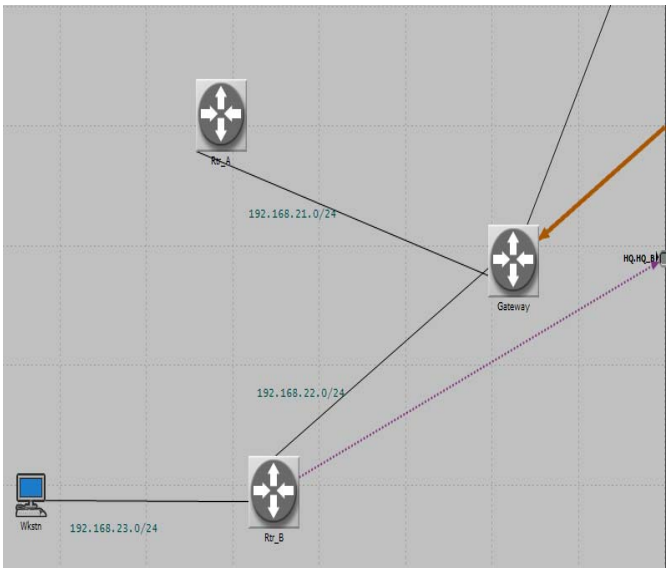


Figura 3.4) estructura interna de la red IP-IP

NO TUNEL: Este sitio usa internamente direcciones IP privadas pero no tiene modo de comunicarse al sitio HQ.

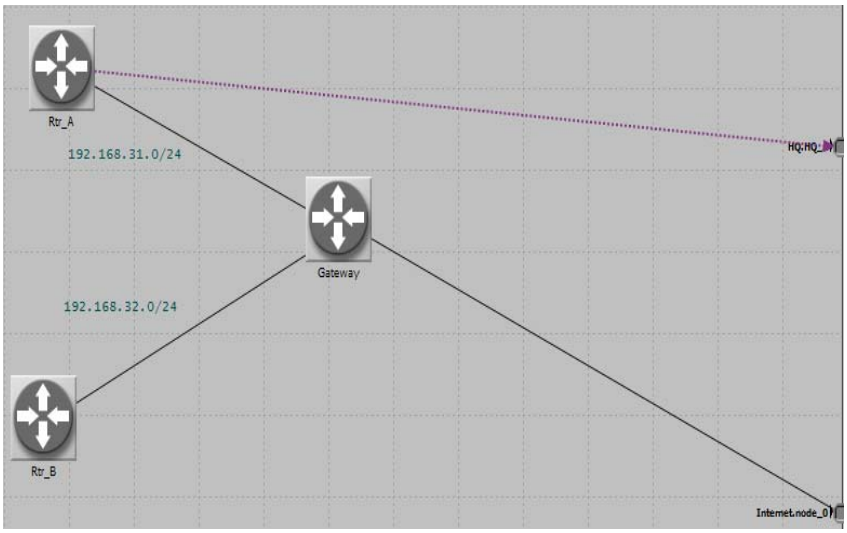


Figura 3.5) Estructura interna del sitio NO TUNEL

EXTERNAL: Este sitio tiene una dirección IP pública por lo que puede comunicarse con el nodo *external* en el sitio HQ.

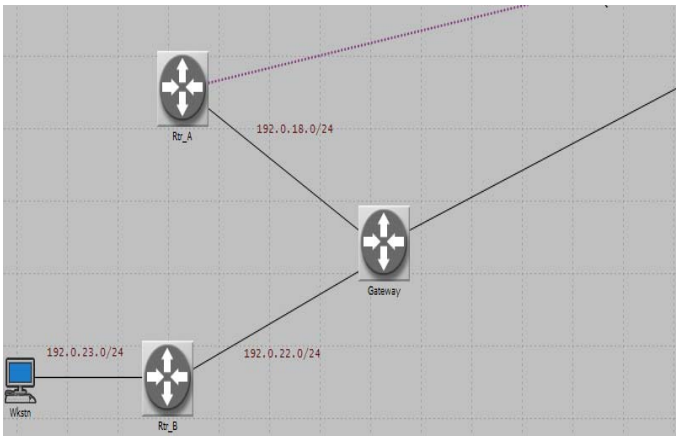


Figura 3.6) estructura interna del sitio external.

INTERNET: La INTERNET consiste en múltiples ruters. Uno de los nodos falla durante la simulación, esto se realizó para examinar el efecto de fallo y recuperación de túneles.

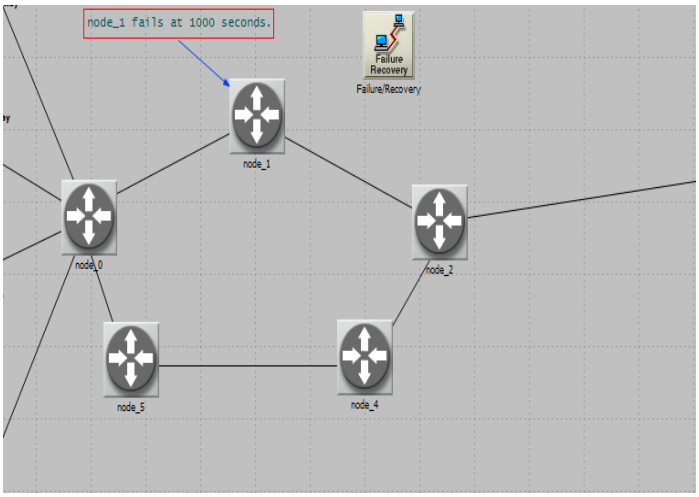


Figura 3.7) Red VPN con túneles IP.

A esta red se le configuraron dos aplicaciones que a nuestro entender resultaban importantes para este tipo de escenario en particular:

- Voz.
- Videoconferencia.

Las simulaciones arrojaron resultados favorables y no favorables de acuerdo a los servicios que brindaba la red, éstos resultados podemos analizarlos en las siguientes gráficas:

Servicio de voz

En este servicio se evaluaron diferentes características como el jitter, la variación de la demora de paquetes, el tráfico enviado y recibido, entre otros y de acuerdo a los resultados obtenidos nos dimos cuenta de que este servicio en particular carga la red pero de una manera que no llega a afectar el buen funcionamiento de la misma.

La figura que aparece a continuación muestra el jitter que caracteriza a esta red. El jitter representa la variación que va teniendo el retardo en el tiempo, pues los paquetes van sufriendo un retardo variable y mientras menor sea este parámetro mejor se va a comportar la red. Es apreciable como a los pocos segundos de iniciada la simulación aparece el jitter con un valor entre 0.014 y 0.016 segundos, a partir de ese valor comienza a aumentar de forma rápida hasta llegar a un valor pico que está entre los 0.018 y 0.020 segundos. A partir de este punto y hasta algunos minutos después de iniciada la simulación comienza a disminuir el jitter hasta llegar a un valor mínimo que está entre los 0.002 y 0.004 segundos,

el cual se mantiene con este valor constante hasta terminada la simulación. El hecho de que en la mayor parte de la simulación este parámetro se halla mantenido constante y con un valor bajo resulta de buen agrado para el buen funcionamiento de la red.

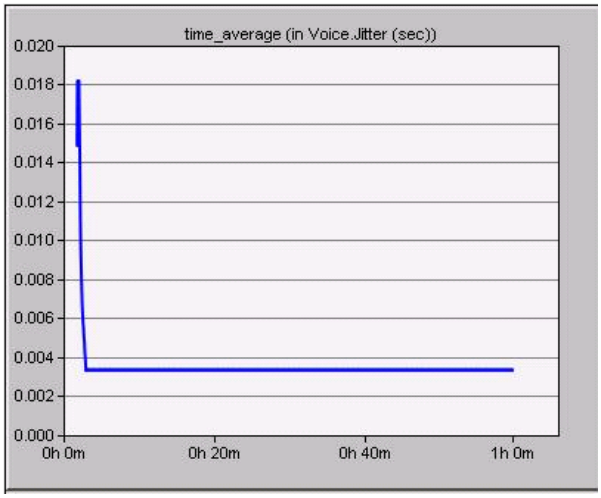


Figura 3.8) Jitter de la red (seg.)

El valor del MOS es otro de los parámetros evaluados en el servicio de voz y su gráfica aparece a continuación.

Como es apreciable en la gráfica, después de transcurridos unos instantes de la simulación es que aparece este parámetro con valor de 3, a partir de este momento y en los próximos segundos comienza a disminuir de manera drástica hasta llegar a un valor de poco más de 1. Desde este instante y hasta la culminación de la simulación este parámetro mantiene este valor. Este parámetro da en una medida la calidad de servicio en la red, y en este caso no resulta muy favorable este parámetro pues la mayor parte de la simulación se mantiene con un valor bajo.

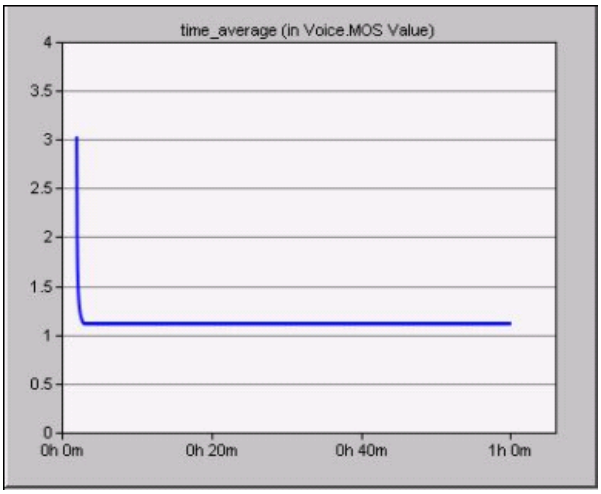


Figura 3.9) Valor del MOS.

La figura que es mostrada a continuación representa el valor del retardo de los paquetes de extremo a extremo. Este parámetro debe mantenerse por debajo de un cierto nivel para minimizar dos efectos indeseables importantes que son la pérdida por interactividad y el eco. En las simulaciones realizadas este parámetro no aparece hasta los primeros instantes de la simulación, con un valor aproximado que está entre 0.5 y 1 segundos. En los próximos segundos de transcurrida la simulación el retardo comienza a aumentar rápidamente hasta llegar a un valor de 4 segundos, un instante de tiempo después disminuye hasta un valor aproximado que está entre 3.5 y 4 segundos, valor que se mantiene constante hasta la culminación de la simulación. Para el servicio de voz, este retardo no afecta en gran medida el funcionamiento de la red, pues sus valores están por debajo de los límites para minimizar los efectos indeseables mencionados anteriormente.

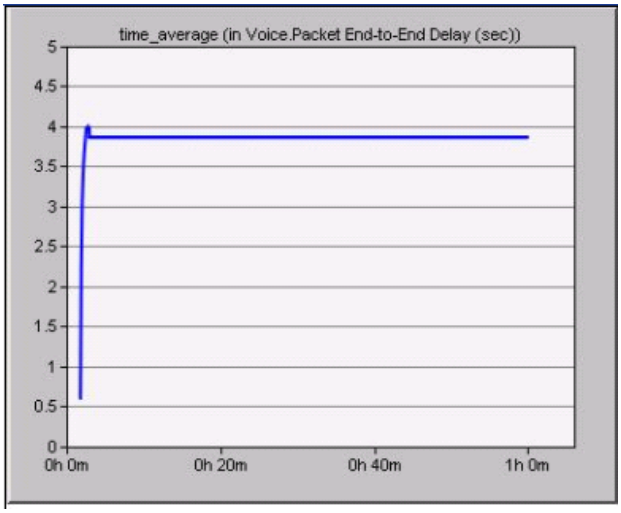


Figura 3.10) Retardo de los paquetes de extremo a extremo.

El tráfico recibido es otro de los parámetros evaluados en las simulaciones para el servicio de voz. Este parámetro viene expresado tanto en paquetes/segundos como en bytes/segundos Las gráficas que a continuación se muestran especifican las simulaciones de estos parámetros. En ambas gráficas es evidente que en los primeros instantes de iniciada la simulación se dispara el tráfico recibido hasta un valor máximo de aproximadamente 700 bytes/segundos que va a corresponder con un recibo de casi 70 paquetes/segundos este pico en el tráfico recibido se debe a un comportamiento característico de la red donde hace un establecimiento del canal de entrada. Posteriormente es evidente como el tráfico recibido va disminuyendo paulatinamente hasta el final de la simulación.

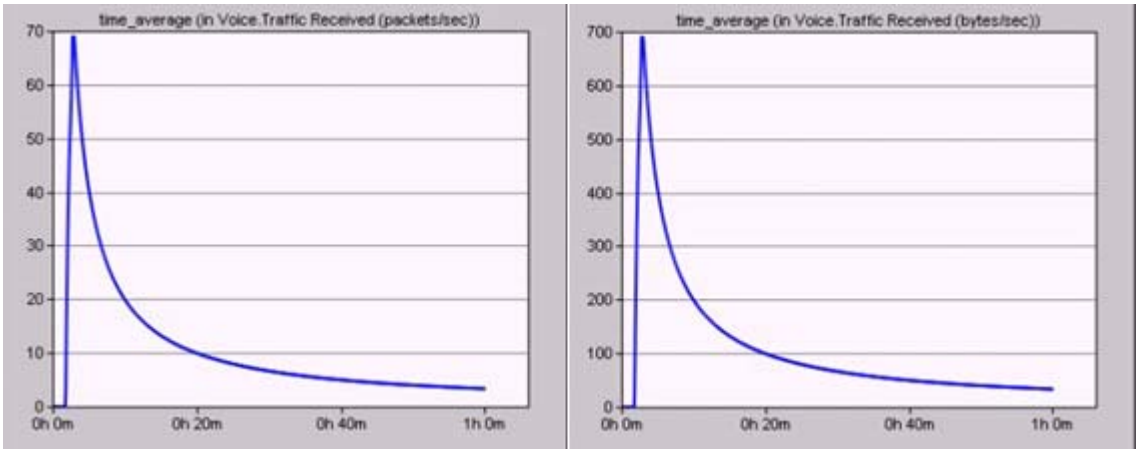


Figura 3.11) Tráfico recibido.

El tráfico enviado es otro de los parámetros evaluados para el servicio de voz. Este parámetro como el anterior también viene expresado tanto en bytes/segundos como en paquetes/segundos y su comportamiento es muy similar al del tráfico recibido. Segundos después de iniciada la simulación, el tráfico enviado se dispara hasta un valor máximo de poco más de 3000 bytes/segundos lo que equivale a poco más de 300 paquetes/segundos, como se había explicado anteriormente este comportamiento se debe al establecimiento del canal de salida. Segundos después el tráfico enviado disminuye paulatinamente hasta el final de la simulación.

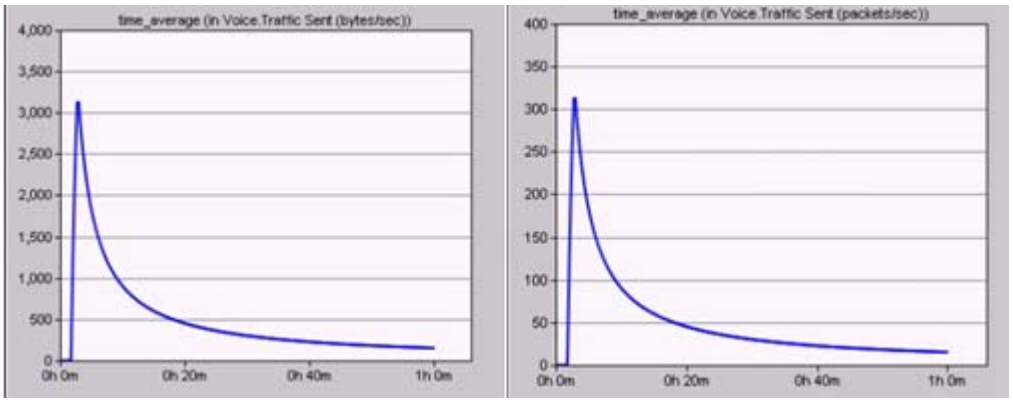


Figura 3.12) Tráfico enviado.

Servicio de videoconferencia

Videoconferencia fue otro de los servicios habilitados en la red. Este servicio en casos donde no este habilitado el equipamiento necesario para ofrecer este servicio le proporcionar a la red una mayor carga y provocar altos retardos lo que afectaría el óptimo funcionamiento de la red. En este caso en particular dentro de este servicio fueron evaluados varios aspectos como el tráfico enviado y recibido y algunos retardos.

La siguiente figura muestra el retardo que presentan los paquetes de extremo a extremo. Este retardo aparece segundos después de iniciada la simulación y con un valor de aproximadamente 0.11 segundos, este retardo incrementa rápidamente hasta llegar a un valor máximo de aproximadamente 0.27 segundos, este valor pico no llega a afectar el buen funcionamiento de la red pues es un valor relativamente bajo y solo se mantiene pocos segundos durante la simulación pues rápidamente disminuye hasta valores muy bajos e incluso a partir de los 20 minutos de transcurrida la simulación este retardo se iguala a cero, manteniéndose así hasta finalizada la simulación.

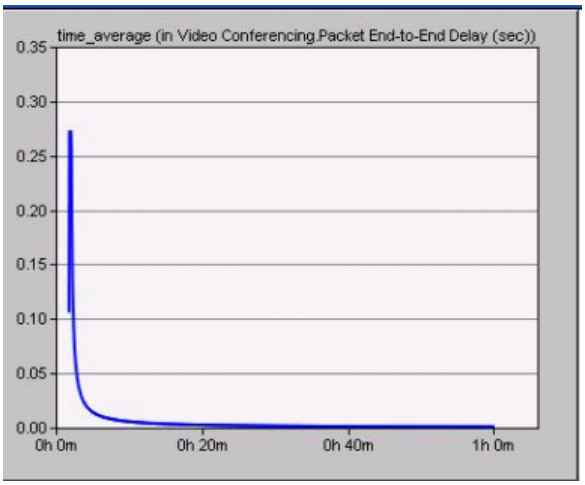


Figura 3.13) Retardo de los paquetes de extremo a extremo.

La siguiente figura muestra el tráfico recibido dado en bytes/segundos y en paquetes/segundos. Este parámetro en el servicio de videoconferencia va aumentando rápidamente a medida que transcurre la simulación y hasta llegar a un valor aproximado de 1600000 bytes/segundos que corresponde a 45 paquetes/segundos, a partir de este valor continua aumentando pero de forma poco pronunciada hasta llegar a un valor máximo, en los instante finales de la simulación, de aproximadamente 2000000 bytes/segundos que va a corresponder a 58 paquetes/segundos aproximadamente.

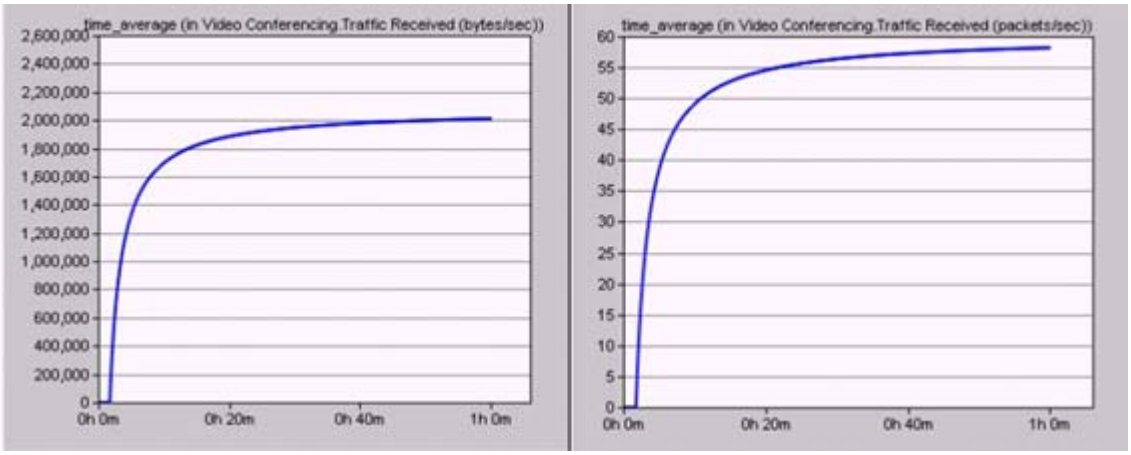


Figura 3.14) Tráfico recibido.

El tráfico enviado es otro de los parámetros evaluados en esta simulación y es dado al igual que el tráfico enviado en bytes/segundos y paquetes/segundos, el comportamiento de este parámetro es muy similar al del tráfico recibido pero con valores mayores. En este caso el

rápido aumento se detiene en un valor de aproximadamente 3000000 bytes/segundos que equivale a un valor aproximado de 80 paquetes/segundos, a partir de estos valores y hasta culminada la simulación el aumento se mantiene de forma poco agresiva y hasta llegar a un valor de aproximadamente 4000000 bytes/segundos y 118 paquetes/segundos respectivamente.

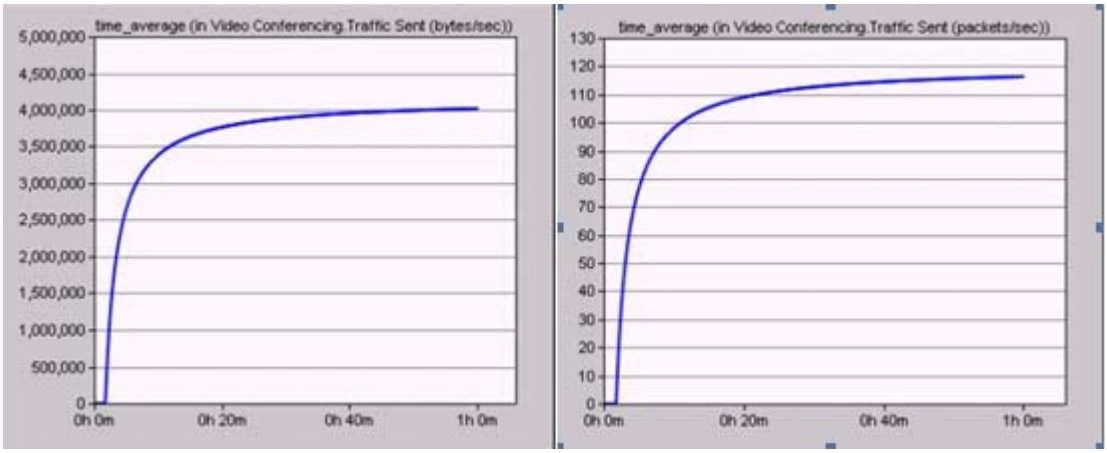


Figura 3.15) Tráfico enviado.

3.3.2 Elementos de la Red

En el epígrafe anterior se pudo observar los resultados que arrojaron las simulaciones del funcionamiento de la red en general para los servicios implementados. En este epígrafe se escogieron dos dispositivos específicos de la red para verificar como había sido su comportamiento durante la simulación, los dispositivos escogidos fueron la estación de trabajo del sitio External y el Gateway del sitio Gre.

- **Estación de trabajo del sitio external**

En esta estación de trabajo fueron evaluados algunos aspectos como la utilización el rendimiento y el retardo en la cola de cola tanto en el canal de entrada como de salida. La figura mostrada a continuación represente el retardo en la cola de los canales de entrada y salida. Es importante que en un determinado tiempo los paquetes vayan saliendo de la cola, pues un alto retardo en las colas puede resultar fatal para la red, debido a que puede dar lugar a una congestión. En ambos casos este retardo se comporta de manera similar y con valores lo suficientemente bajos como para no ocasionar problemas en el adecuado funcionamiento de la red.

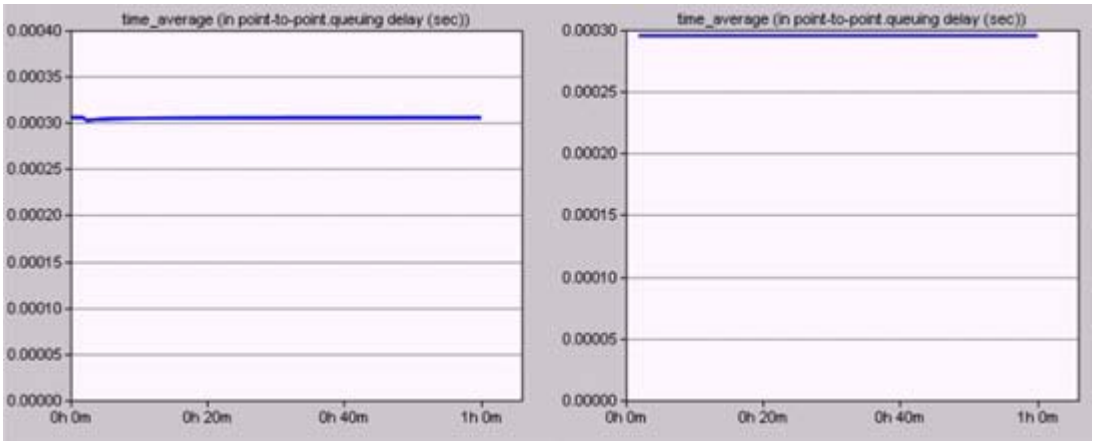


Figura 3.15) Retardo en la cola.

La utilización de entrada y salida fue otro de los parámetros evaluados en la simulación para esta estación de trabajo. La primera gráfica representa la utilización del canal de entrada, la cual alcanza un valor máximo de 0.30 y queda en este instante de tiempo establecido el canal de entrada , este parámetro generalmente se valora en por ciento y no es favorable para la red que alcance altos valores pues podría producir posibles congestiones en la misma. En el caso de la segunda gráfica la cual representa la utilización del canal de salida, donde es evidente un valor por encima de 1 por lo que este canal está siendo más utilizado que el de entrada. En ambas gráficas la utilización luego del establecimiento del canal la utilización va disminuyendo y estableciéndose una buena utilización hasta terminada la simulación.

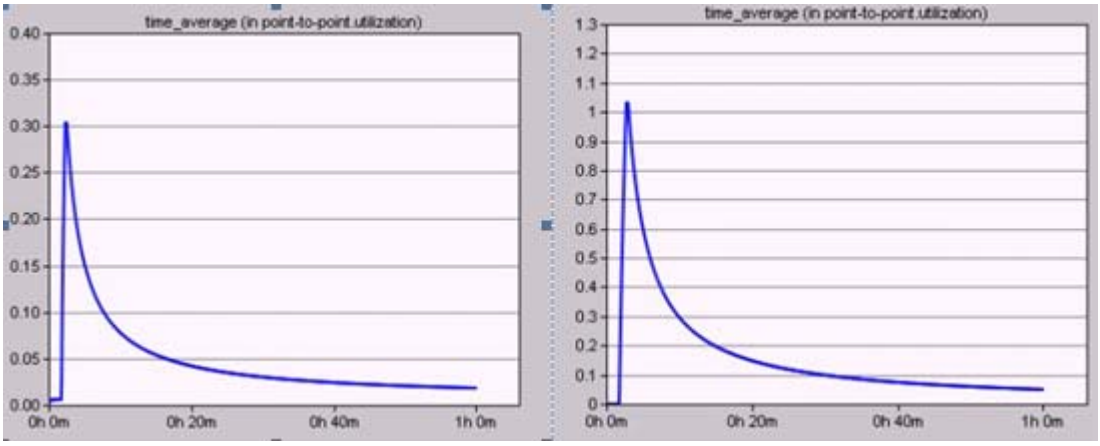


Figura 3.16) Utilización del canal.

El rendimiento es un parámetro importante que da una medida de la cantidad de paquetes de información en el tiempo de operación de la red. En este caso en particular tenemos el rendimiento en el canal de entrada dado en bits/segundos y paquetes/segundos. Es evidente como en los primeros instantes de la simulación aparece un máximo en un valor de poco más de 4500 bits/segundos lo que equivale a poco más de 10 paquetes/segundos, a partir de ese momento el rendimiento comienza a disminuir de manera descendente hasta el final de la simulación.

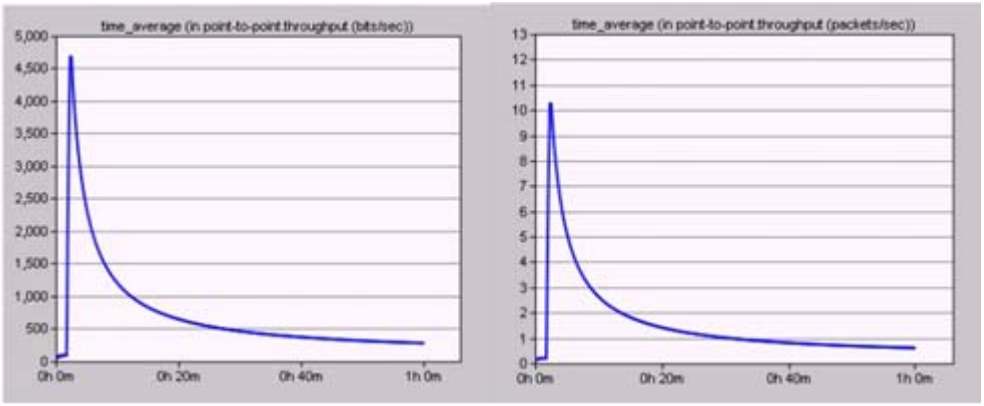


Figura 3.17) Rendimiento del canal de entrada.

Para la estación de trabajo que se está analizando en este momento, el rendimiento de salida es mucho mayor que el de entrada, esto es apreciable en la siguiente figura donde aparece un valor máximo de 16000 bits/segundos que equivalen a 35 paquetes/segundos. Al igual que sucede en el rendimiento del canal de entrada hay una disminución descendente hasta culminada la simulación.

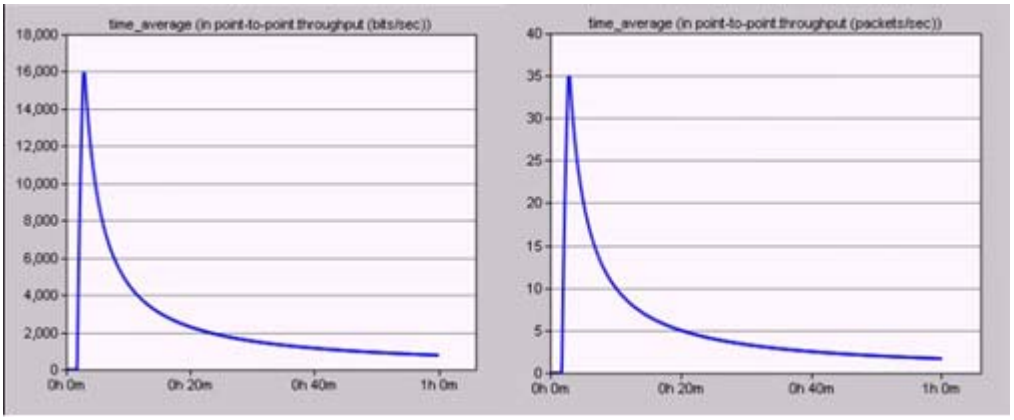


Figura 3.18) Rendimiento del canal de salida.

- **Gateway del sitio Gre**

Las simulaciones realizadas a este dispositivo en particular evaluaron diferentes parámetros como retardos y distintos tipos de tráfico.

La figura que se muestra a continuación representa la variación en el retardo, como se había explicado anteriormente este parámetro se debe a que algunos paquetes lleguen más rápidos que otros comportándose de forma indeseable para la red. Este parámetro durante los primeros 10 minutos de la simulación va aumentando rápidamente pero con algunas pequeñas variaciones, a partir de este instante de tiempo y hasta terminada la hora de simulación, los valores de este parámetro comienzan a variar en un constante sube y baja, manteniéndose siempre los máximos valores por debajo de los 2 segundos y los mínimos por encima de 1.8 segundos.

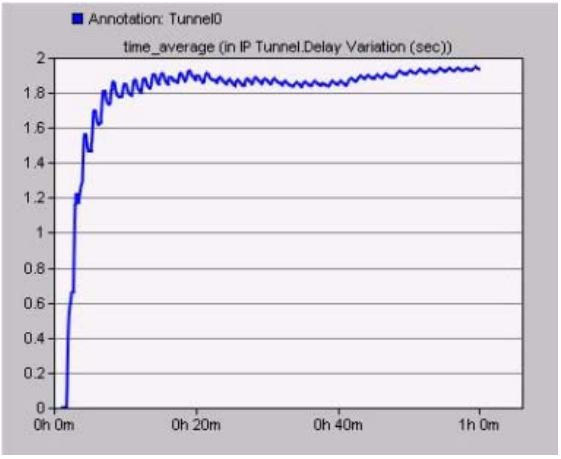


Figura 3.19) Variación del retardo.

En este dispositivo el tráfico recibido se mantiene en una constante variación durante toda la simulación, alcanzando un máximo de casi 550000 bits /segundos, este valor se alcanza cuando transcurren casi 35 minutos de la simulación. Casi finalizada la simulación disminuye un poco el tráfico recibido dando un valor de 500000 bits/segundos equivalentes a 60 paquetes/segundos.

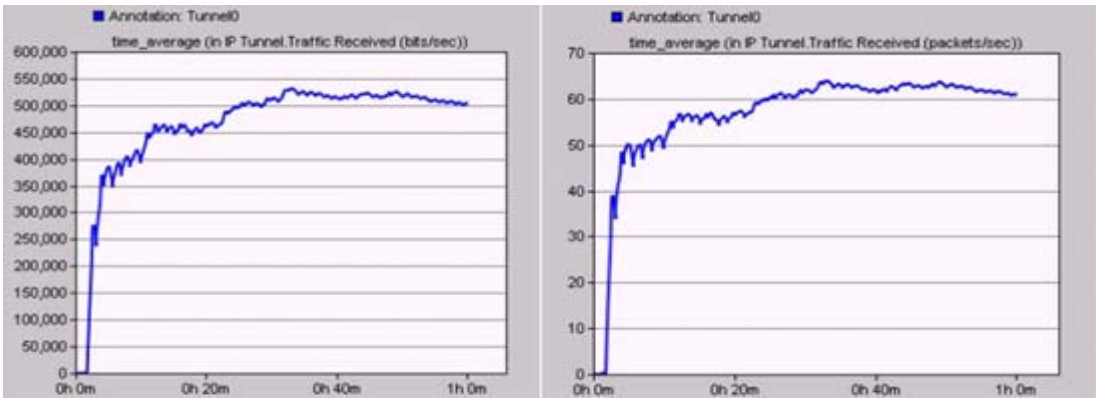


Figura 3.20) Tráfico recibido.

El tráfico enviado se comportó de manera similar al tráfico recibido pero con valores mayores. Se mantuvo variando constantemente aunque en pequeñas escalas, y llegó a alcanzar un valor máximo de poco más de 1000000 de bits/segundos que equivale a más de 160 paquetes/segundos.

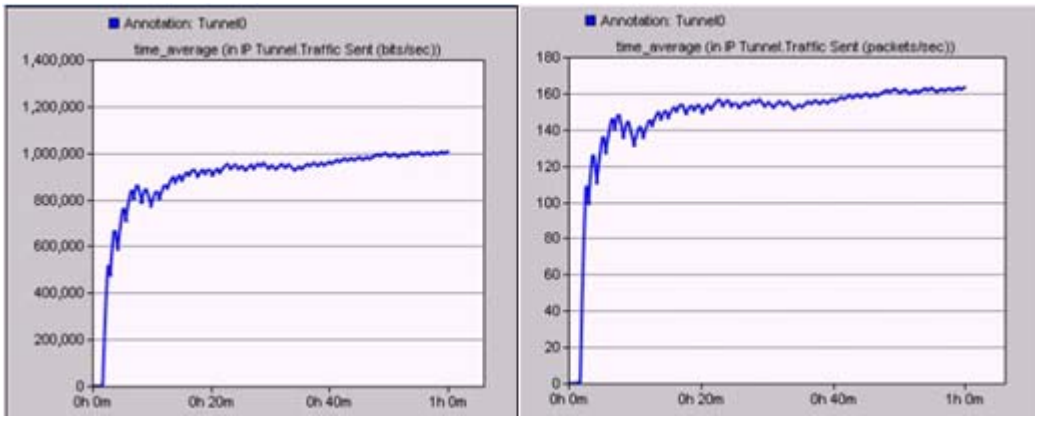


Figura 3.21) Tráfico enviado.

La figura que se muestra a continuación representa el tráfico perdido en el Gateway. Es apreciable como para este dispositivo no hay paquetes perdidos lo que resulta muy favorable para esta red, pues para los servicios que se estaban evaluando era importante que no hubiera pérdida de paquetes para no afectar la comunicación de voz y videoconferencia.

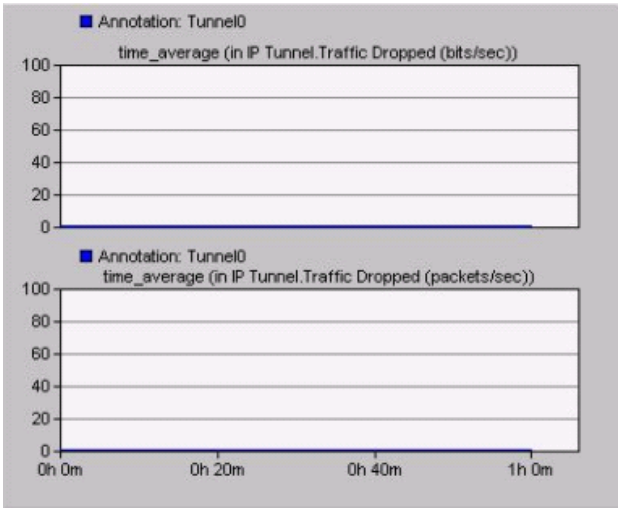


Figura 3.21) Tráfico perdido.

3.4 Escenario 2: Red MPLS-VPN-BGP

Esta red fue escogida por su similitud con las redes VPLS pues en esta red está presente el protocolo BGP y hace un uso fundamental de las VPN. Este escenario ilustra el uso de las VPN para la comunicación entre múltiples sitios diferentes.

3.4.1 Estructura de la Red

Dos redes de empresa han sido configuradas como empresa A y empresa B.

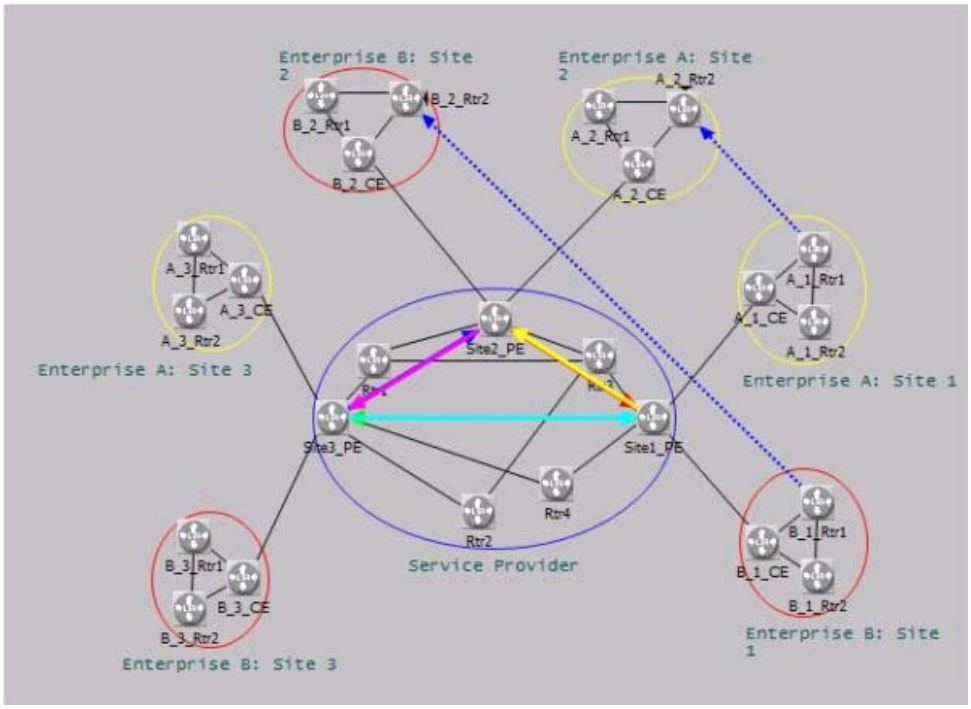


Figura 3.21) Red MPLS-VPN-BGP.

La empresa A usa una VPN llamada VPN amarilla y la empresa B usa una VPN llamada VPN roja, para comunicarse entre diferentes sitios. Túneles LSP han sido configurados entre todos los PE en la red. El protocolo BGP es configurado entre todos los PE y son vecinos BPG. Las rutas entre los PE son divididas usando BGP y son vecinos BGP entre sí. Todos los sitios de la empresa A son configurados para usar la VPN amarilla y todos los sitios de la empresa B son configurados para usar la VPN roja.

Las simulaciones fueros realizadas para analizar el desempeño de las VPN en general y ver como se comportaban ante diferentes parámetros.

La figura que se muestra a continuación representa la demora de las VPN amarilla y roja, en este caso la demora se comporta igual para ambas VPN, aumentando desde el inicio de la simulación y hasta poco después de los primeros 5 minutos de simulación, con este aumento alcanza un valor máximo entre 2 y 2.5 micro segundos, a partir de este instante de tiempo y hasta terminada la simulación esta demora se mantiene constante y con ese mismo valor.

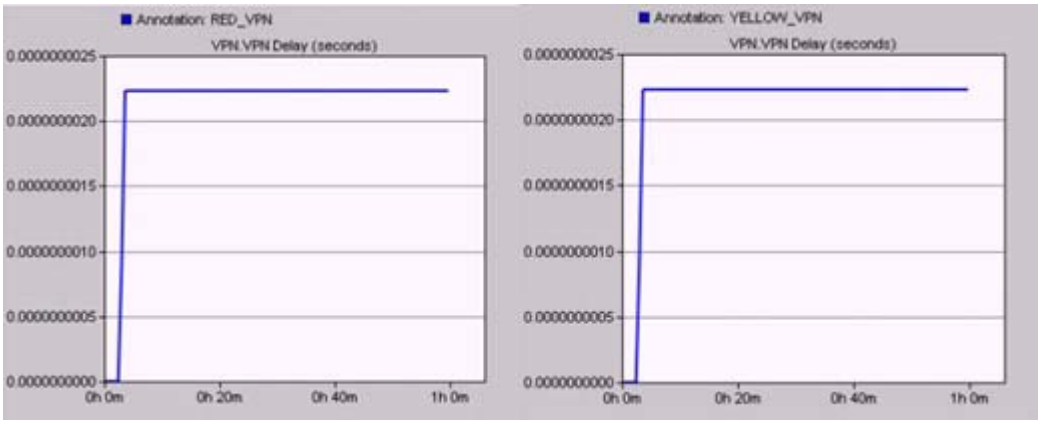


Figura 3.22) Demora en las VPN.

La figura que se muestra a continuación representa el rendimiento de la VPN roja, una vez iniciada la simulación este parámetro de comporta variando constantemente hasta que finaliza la simulación y alcanza unos valoras entre 45000000 y 55000000 de bits/segundos correspondiente a valores entre 80 y 120 paquetes/segundo.

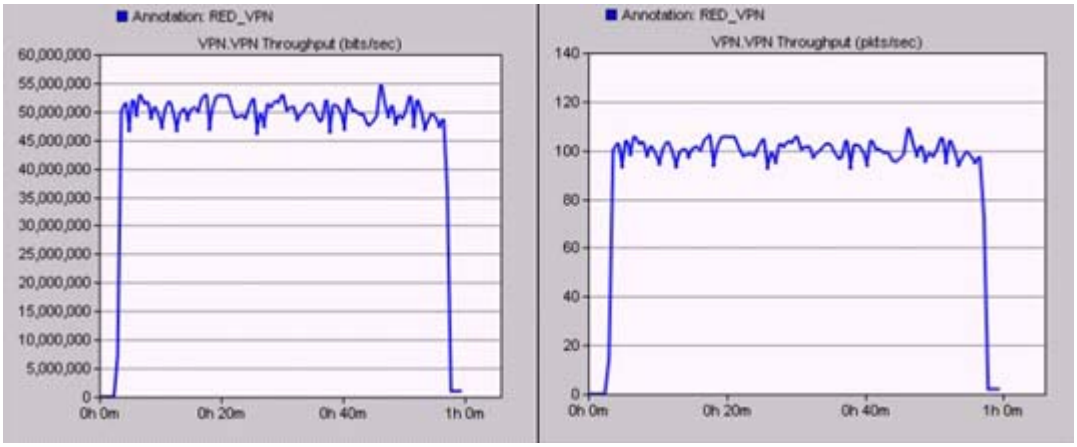


Figura 3.23) Rendimiento de la VPN roja.

El comportamiento de la VPN amarilla con respecto al rendimiento, es muy similar al de la VPN roja, su valor máximo y mínimo están al igual que en la VPN roja entre 45000000 y 55000000 de bits/segundo, en este caso lo que cambia un poco son las variaciones en los valores intermedios durante la simulación.

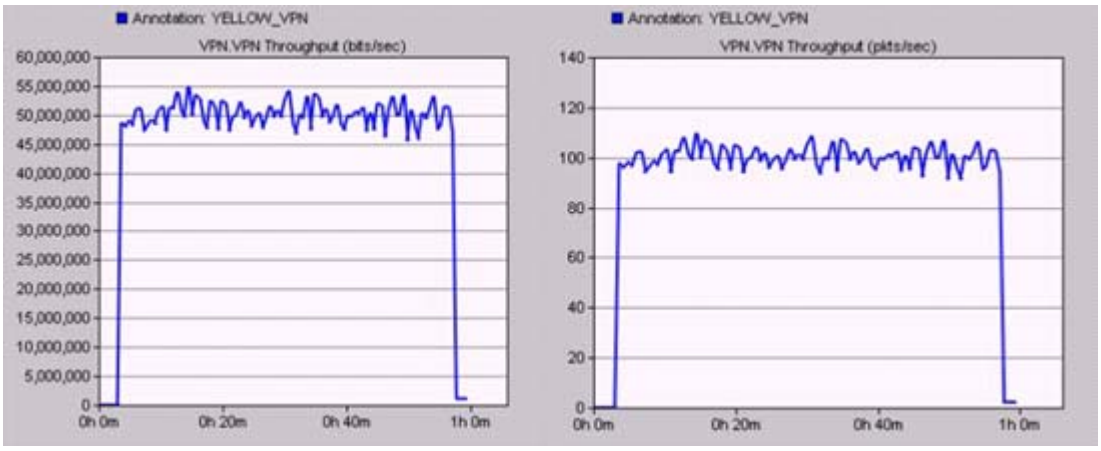


Figura 3.24) Rendimiento de la VPN amarilla.

La carga en una VPN es un parámetro de gran importancia para analizar el buen funcionamiento de la misma. En el caso de VPN roja, representada en la figura que se muestra a continuación, la carga se comporta de manera variable durante toda la simulación con valoras entre 45000000 y 55000000 de bits/segundos que equivalen a valores entre 80 y 120 paquetes/segundo.

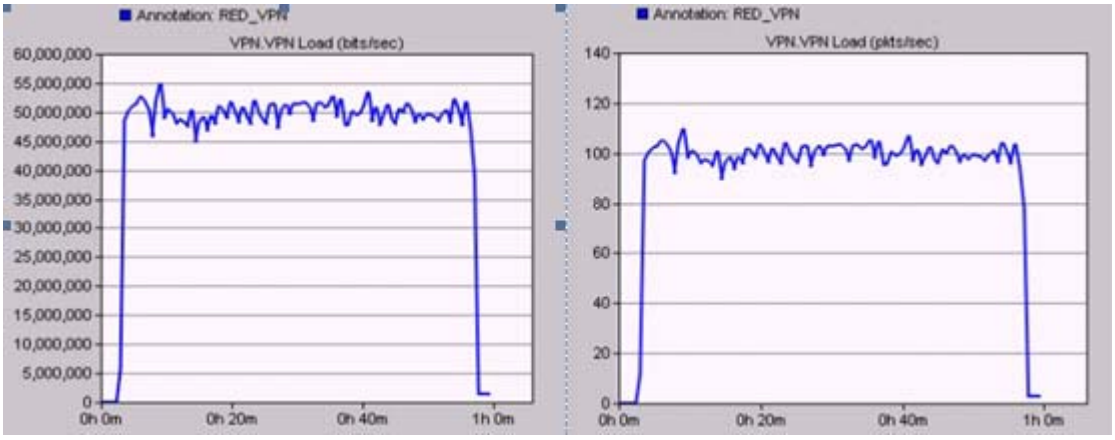


Figura 3.24) Carga de la VPN roja.

En el caso de la VPN amarilla la carga se comporta de manera similar al de la VPN roja, ya que se mantiene variando constantemente pero siempre entre los mismos valores que oscilan entre 45000000 y 55000000 de bits/segundo.

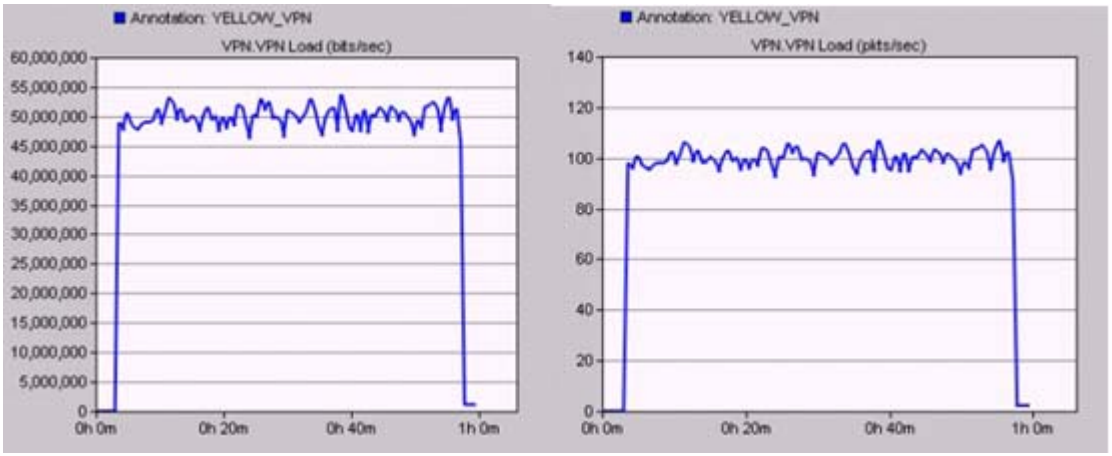


Figura 3.25) Carga de la VPN amarilla.

3.5 Conclusiones del Capítulo

Luego de la realización de las simulaciones se considera que el empleo de esta solución tecnológica aporta importantes beneficios. Para entornos tanto de pequeñas como medianas empresas, actualmente VPLS se considera como la mejor solución, permitiendo a estas no realizar grandes cambios tecnológicos en sus redes locales.

Gracias al simulador OPNET MODELER 14.0 pudimos realizar las simulaciones presentadas anteriormente, a pesar de que las redes escogidas no fueron precisamente VPLS si guardaban una estrecha similitud con la misma. En el caso de la segunda red su diferencia más importante con el servicio VPLS radica en la forma en que se comunican los ruter PE y CE, ya que a diferencia de MPLS-BGP-VPN, en VPLS el dispositivo CE no necesita intercambiar información de enrutamiento con el ruter PE.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Este trabajo se ha profundizado en uno de los servicios actuales de transporte Ethernet, ofreciendo un servicio multipunto-a- multipunto que puede cubrir una o más áreas metropolitanas y proporcionar conectividad entre múltiples sitios como si estos estuviesen conectados a la misma LAN Ethernet (Servicio Privado Virtual de LAN, VPLS). VPLS usa una infraestructura de proveedor de servicios IP/MPLS, que proporciona la escalabilidad necesaria. El uso de los protocolos de ruteo y procedimientos IP/MPLS en lugar del protocolo STP y las etiquetas MPLS en lugar de identificadores de VLAN dentro de la infraestructura de proveedor de servicios, da como resultado un mejoramiento significativo en la escalabilidad del servicio VPLS.
2. Sin embargo, hemos concluido que no todas las implementaciones de VPLS dan iguales beneficios. Para desplegar VPLS con la eficiencia operacional óptima, los proveedores de servicios deben considerar seriamente usar Protocolos de Ruteo de Borde (BGP) para autodescubrimiento y señalización, como se especifica en draft Kompella.
3. VPLS constituye un servicio ampliamente demandado por las actuales estructuras empresariales debido a las ventajas que ofrece en cuanto a seguridad, fiabilidad, escalabilidad y costos. VPLS comparado con otros tipos de servicios de transporte Ethernet, es superior en cuanto al número de sitios cubiertos, velocidad, costos y niveles de seguridad.

4. Es también la mejor opción para organizaciones preocupadas por la seguridad, dado que no necesitan compartir sus tablas de enrutamiento con el operador.
5. Con la consolidación de centros de datos, las aplicaciones que mejor se ajustan a VPLS son las que requieren conectividad multisede en tiempo real para soportar aplicaciones como telefonía IP, videoconferencia e incluso servicios de continuidad de negocio y recuperación de desastres.
6. Además se presentan algunos elementos prácticos necesarios para conocer el conjunto de protocolos del servicio y orientar su introducción en una red de datos.

Recomendaciones

1. Recomendamos realizar un estudio de mercado y establecimiento de tarifas de los posibles clientes para este servicio, de manera tal que la inversión pueda ser recuperada en un tiempo razonable y aún así resulte atractiva para los usuarios.
2. Sería recomendable además incluir el estudio de la tecnología VPLS como parte de la formación teórica de los estudiantes de pregrado y postgrado en Telecomunicaciones y Electrónica, a fin de lograr una mejor preparación de los graduados con respecto a esta tecnología.

REFERENCIAS BIBLIOGRÁFICAS

1. (2003)."La alternativa VPLS. ″Carrier Ethernet." Revista Network World.
2. (2003)."MPLS. Virtual Private LAN Services." Revista Cisco IOS.
3. (2003). "Testing edge service VPLS over MPLS." White Paper.
4. (2008). "Curso de VoIP." ETECSA.
5. (2010). "100Gb Ethernet transport." IEEE Comuication magazine.
6. (2010). "Carrier Ethernet for mobile backhaul." IEEE Comuication magazine.
7. (2007).”BGP. Border Gateway Protocol”. Artículo curso de Ruteo IP y Tecnologías de Transporte. Instituto de Ingeniería Eléctrica, Universidad de la República.
8. (2006). “An Interview with Marc Lasserre, Architect of VPLS”. VPLS.ORG.
9. (2006). “VPLS Standards”. VPLS.ORG.
10. (2006). “BACKBONE MULTISERVICIO IP-MPLS”. Presentación en Power Point. ETECSA.
11. (2006).”VRP Operation Manual”. VRP 5.30. Huawei Technologies.
12. (2006). “Virtual Private LAN Service Architectures and Operation”. White Paper Cisco.
13. (2010). “What is Carrier Ethernet?” http://metroethernetforum.org/page_loader.php?p_id=140
14. Adnaloy, A. (2003) “Redes Privadas Virtuales: Modalidades de actualidad y recomendaciones para su implementación con el empleo de MPLS”. Tesis de Maestría en Telemática del Instituto Superior Politécnico José Antonio Echeverría.

15. Andersson L, P. Dolan, N. Feldman. “LDP Specification”. RFC 3036. IETF. http://www.ietf.org/rfc/rfc3036.txt
16. Arco, J. M., Carral, J. A., García, A., "RTB" Universidad de Alcala.
17. Benítez, A. Fonseca, C. (2007). “VPLS, una opción segura para las Redes Corporativas en Cuba”. Revista Telem@tica. Cujae.
18. Bradner, S. (1999). "RFC 2544."
19. Caro, L. F. (octubre 2009). "Improving resourse utilization in carrier ethernmet tecnologies". España, Universidad de Girona. **master:** 88.
20. Castro, F. (2006). "Discurso pronunciado por Fidel en ocasión al aniversario 47 de su entrada en Pinar del Rio en el acto por la culminación de los grupos electrógenos en esa provincia.
21. Cheung, D. (2009)“Carrier Ethernet Services with MPLS,”
22. Chinea, E. C. "Implementación de los servicios de carrier ethernet sobre un núcleo MPLS" Universidad Central Martha Abreu de las Villas. **Ingeniero**.
23. Dàvalos, G. (2006). "Cuba es una gran universidad."
24. Chinea, E. "Implementación de los servicios de carrier ethernet sobre un nucleo MPLS" Universidad Central de las Villas. Ingeniero.
25. Christophe, D. 92003). "MPLS-VPN Implementation Transition Approaches
26. Gómez, E. (2003). "diseño de un modelo virtual de las funciones de la capa de enlace WLAN en el IEEE 802.11e."
27. Gómez, J. (2007). "MPLS conceptos generales MPLS/VPN capa 2 y 3."
28. J. Witters, G. V. K., J. De Clercq, S. Khandekar (2004). "Claves para desplegar con éxitpo el VPLS." Revista de telecomunicaciones de Alcatel.
29. J. Witters, J. d. C., S. Khandekar (2004). "Tutorial técnico de VPLS " revista de telecomunicaciones de Alcatel.
30. Kompella, V. Rekhter, Y. (2007). ""irtual Private LAN Service using BGP".
31. Marc, L. Vach, K. (2007). “Virtual Private LAN Service Using LDP”. Internet Draft Document. IETF.draft-eietf-l2vpn-vpls-ldp-09.txt.
32. Luo, W. Carlos, P. (2005) “Layer 2 VPN Architectures”, Cisco.
33. Mark, L. (2006)”Comparing, Designing, and Deploying VPNs”. Cisco Press, ISBN: 1-58705-179-6.
34. Martínez, D. (2007). "Análisis comparativo de VPN BGP/MPLS y VPLS para su implementación en redes cubanas."
35. Martini, L. (2006). “Pseudowire Setup and Maintenance Using LDP" RFC 4447,
36. Miguel, F. (2007) “Estado del arte de las Redes de Telecomunicaciones en Cuba y de la tecnología MPLS”. Tesis de Diplomado en Telemática. Instituto Superior Politécnico José Antonio Echevarría.

37. “Redefining the Virtual Private Network”. Check Point Software Technologies Ltd. http://www.checkpoint.com/products/downloads/vpnredef.pdf

38. Reyes, A. G. (2007). "Contribución a las redes privadas virtuales sobre MPLS" santa Clara, Universidad central Martha Abreu de las Villas. **Ingeniero**.

39. Rossenhoevel, C. (septiembre 2008). "Carrier Ethernet sevices the future."

40. Xiaoming He, Mingying Zhu, Qingxin Chu. 2006). "Transporting Metro Ethernet Services over Metropolitan Area Networks" IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing - Vol 2 - Workshops.

ANEXOS

Anexo I Enrutadores HUAWEY

Quidway AR28-09.

El AR28-09 es un router de acceso de frontera, que al igual que todo los dispositivos de la Serie Quidway **AR28-09/1X de** este fabricante, posee una arquitectura modular.

Especificaciones del Producto.

Funciones	**Características**
Interfaces	1 Puerto Consola. 1 Puerto AUX. 1 Interfaz Serial. 1 Interfaz Fast Ethernet.
Slots	1 MIM: Multifunction Interface Module. 2 SIC: Smart Interface Card.

Procesador	MPC8241 200 MHz.
SDRAM	128MB
Flash	32 MB
Rendimiento(Performance)	70Kpps
Alimentación	100 VAC a 240 VAC; 50/60 Hz
Consumo	50W

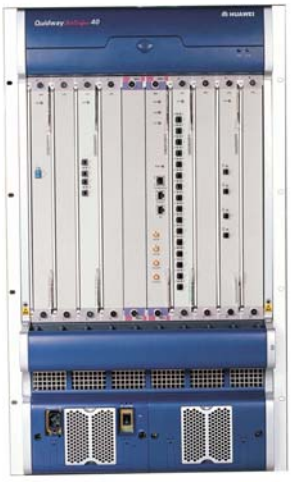
Principales características.

Funciones	**Características**
Protocolos	ENLACE: PPP y MP, ISDN, SLIP, HDLC, Frame Relay(FR), ATM, X.25. RED: DHCP, OSPF, IPX, VLAN, BGP, RIP-1/RIP-2, IS-IS.
Soporta MPLS	BGP/MPLS VPN MPLS L2VPN
Seguridad	AAA, RADIUS/HWTACACS, ACL, IPSec, IKE, PKI.

QoS	Soporta políticas de tráfico (CAR/LR). Soporta (GTS) Shaping Traffic. Soporta gestión de congestión (PQ/CQ/WFQ/CBQ). Soporta (WRED).

http://www.huawei.com/products/datacomm/

Quidway NetEngine(NE) 40-08.



El NE 40-08 forma parte de la serie NE40 USR *(Universal Switching Router)* desarrollada por Huawei Technologies Co. El NE40 Series USR esta orientado a utilizarse en las redes de frontera de los backbones de transporte, el núcleo y las capas de convergencia de las redes metropolitanas y redes de industrias y empresas.

El NE40 Series USR incorpora la vigorosa capacidad de procesamiento de servicios IP de los routers y la capacidad de conmutación de bajo costo de Ethernet de los conmutadores Ethernet capa 3. Este tiene opciones para trabajar como un potente enrutador de núcleo central o como un conmutador Ethernet de capa 3. Debido a ello, este equipo es una opción adecuada para utilizar en nuevas redes metropolitanas.

Es un router de la 5ta generación, con chipsets NP, escalable, configurable y flexible que proporciona servicios IP-v4 e IP-v6, MPLS, VPLS, Gigabit Ethernet, 10/100 Ethernet, que permite el soporte de múltiples servicios de datos, voz, video y del creciente tráfico IP.

Los componentes del NE40-08 son redundantes, los conmutadores, las unidades de control, fuentes de energía, unidades control del enfriamiento e interfaces de línea; de manera que puedan ser reemplazadas sin interrupción del servicio.

Las tarjetas del NE40 Series USR están clasificadas en SRU *(Switch and Routing Unit)* y LC *(Line Card)*. Las tarjetas LCs incluyen LPU *(Line Processing Unit)* y LPUF *(Flexible Card Line Processing Unit)*. El NE40-8 tiene dos SRUs para una redundancia 1+1. Cuando un SRU falla, el servicio será automáticamente conmutado al otro SRU.

Las LPUs implementan la interconexión y el reenvío de datos con otros dispositivos. El NE40 Series USR permite la utilización de las LPUs siguientes: Ethernet, POS, cPOS (POS canalizado), ATM, RPR *(Resilient Packet Ring)* y E1.

Resumiendo, es un equipo de pequeñas dimensiones, poco costoso y de muchas prestaciones.

Especificaciones.

Funciones	**Características**
Ranuras(Slots)	8
Rendimiento(Performance)	48 Mpps
Capacidad de Conmutación	64 Gbps
Capacidad de Backplane	128 Gbps
Tipos de Interfaces	OC-48c/STM-16c POS GE OC-12c/STM-4c POS FE OC-3c/STM-1c POS E3 OC-48/STM-16 cPOS T3 OC-3/STM-1 cPOS E1/cE1 OC-48c/STM-16c RPR OC-12c/STM-4c ATM OC-3c/STM-1c ATM
Número de VRF soportado para IPv4.	1024 VRF x 1024 rutas.
Número de VRF soportado para IPv6.	1024 VRF x 1024 rutas.
Alimentación	DC：-42 ~ -60V AC：100V ~ 240V

Consumo Máx.	<1000W

Principales características del Producto.

Funciones	**Características**
Pila doble (dual stacks)	IPv4 Rutas Estáticas, RIP, OSPF, IS-IS y BGP4 IPv6 Rutas Estáticas, BGP4+, RIPng, OSPFv3 y ISISv6
Capa 2	Protocolos LAN: Ethernet II, Ethernet SNAP, Ethernet SAP, 802.3z, 802.3ae Protocolos WAN: PPP, MP, HDLC, POS, ATM Envío VLAN Capa 2, VLAN Trunk, L2QoS, RSTP, MSTP, VPLS, HVPLS y 1483B
MPLS VPN	Soporta L2/L3 MPLS VPN y VPLS, puede utilizarse como router del backbone(P) o como router de frontera(PE). Soporta MPLS TE y TE FRR

Multicast	Soporta (IGMP) Internet Group Management Protocol. Soporta (PIM-DM) Protocol Independent Multicast-Dense Mode. Soporta (PIM-SM) Protocol Independent Multicast-Sparse Mode. Soporta (MSDP) Multicast Source Discovery Protocol. Soporta (MBGP) Multi-protocol Border Gateway Protocol. Soporta (PIM-SSM) PIM Source Specific Multicast.
QoS	Cada tarjeta de línea tiene 2K de cola. Soporta avanzadas tecnologías como CBQ, LLS/NLS y PBS. Soporta política de tráfico bi-direccional CAR. Soporta WRED y SA-RED. Soporta prioridad de descarte con 8 niveles.
Confiabilidad	Soporta (TE FRR) MPLS TE Fast Rerouting. Soporta (VPN FRR) VPN Fast Rerouting. Soporta (IP FRR) IP Fast Rerouting. Soporta (VRRP) Virtual Route Redundant Protocol. Soporta (EVRRP) BFD Enhanced Virtual Route Redundant Protocol. Soporta (GR) Graceful Restart. Soporta (NSF) Nonstop Forwarding. Soporta (IGP FC) IGP Fast Convergence.

Anexo II Conmutadores enrutadores Alcatel

Alcatel 7670

El 7670 es una plataforma de conmutación y enrutamiento escalable, configurable y flexible que proporciona servicios IP, MPLS, ATM, TDM, Frame Relay, Gigabit Ethernet, 10/100 Ethernet, que permite el soporte de múltiples servicios de datos, voz, video y del creciente tráfico IP.

Los componentes del sistema 7670 son redundantes, los conmutadores, las unidades de control, fuentes de energía, unidades control del enfriamiento e interfaces de línea; de manera que puedan ser reemplazadas sin interrupción del servicio.

En su configuración simple tiene 14 ranuras para tarjetas y soporta una capacidad de conmutación de 56 Gbps con redundancia 1+1, escalable en pasos de 14 Gbps hasta 450 Gbps añadiendo bastidores separados para la conmutación, los periféricos y servicios.

Configuración simple	**Máxima capacidad**
✓ 224 puertos OC-3/STM-1/DS3 o	1760 puertos OC-3/STM-1/DS3 o
✓ 56 puertos OC-12/STM-4 o	440 puertos OC-12/STM-4 o

- ✓ 14 puertos OC-48/STM-16 o 56 puertos GigE
- ✓ 124 puertos OC-48/STM-16 o 440 puertos GigE
  31 puertos OC192/STM-64

En su configuración de múltiples bastidores incluye:

- ✓ Bastidor de conmutación: hasta 450 Gbps de capacidad de conmutación en incrementos de 14 Gbps y con redundancia 1+1.
- ✓ Bastidor de periféricos: tiene 14 ranuras con capacidad de 3,4 Gbps para interfaces que van desde DS3 hasta OC-48/STM-16, incluyendo GigE.
- ✓ Bastidor de periféricos de alta velocidad: tiene 16 ranuras con capacidad de 14 Gbps para interfaces desde OC-48/STM-16 hasta OC-192/STM-64 y 10 GigE. Para una alta disponibilidad puede estar formado por cuatro sub-bastidores con 4 ranuras cada uno que posibilitan evitar que un fallo afecte a gran número de interfaces. Los sub-bastidores han sido diseñados para soportar OC-768/STM-256.
- ✓ El bastidor de extensión de servicios: con capacidad de 2,4 Gbps soporta un amplio rango de interfaces de datos de baja velocidad, que incluyen: E1/T1/E3/T3 ATM, Frame Relay, IP, multimedia, voz y de emulación de circuitos. Puede ser usado como un sistema independiente para soportar agregación de interfaces a OC-12/STM-4 y conmutación de conexiones de usuarios.

Soporta conexiones SVC/PVC punto a punto y multipunto, conexiones S-PVC punto a punto; con las categorías de servicio ATM: CBR, Rt-VBR, Nrt-VBR, ABR y UBR, para garantizar la calidad de servicio y mapeo de QoS a las Clases de Servicio (***CoS, Class of Service***) de IP. Permite soportar el tráfico ATM sobre caminos construidos en un núcleo MPLS conforme a las especificaciones del Foro ATM.

Soporta aplicaciones de voz sobre ATM utilizando troncos sobre AAL1 con interfaces STM-1, E3 y E1 que incluyen canceladores de eco. El soporte de voz en troncos utilizando AAL2 con interfaces STM-1 y procesamiento avanzado de las señales de voz incluyen: 248

llamadas por conexión, supresión de silencios, generación del ruido de fondo, codificación

conforme a la G.711, compresión ADPCM a 32 Kbps según la G.726 y cancelación de eco.

Alcatel 7470 y 7270

El 7470 es catalogado por Alcatel como una plataforma multiservicio y el 7270 como concentrador multiservicio, para soportar múltiples aplicaciones en ATM e IP/MPLS. Soportan Frame Relay, IP, emulación de circuitos, X.25 y servicios LAN transparente; con posibilidades de brindar calidad de servicio. Es posible interconectar usuarios Frame Relay con usuarios ATM a través de la capacidad de interfuncionamiento de servicios conforme al FRF.8. Soportan conexiones SVC, PVC y S-PVC, punto a punto y punto multipunto. Los módulos de multiplexación inversa permiten una mejor escalabilidad de los servicios sobre ATM al permitir formar flujos agregados con varias interfaces E1 que posibilitan incrementar la velocidad de los enlaces cuando se requiere.

La redundancia de las funciones de control y conmutación se puede configurar la protección de las interfaces que manejan el tráfico agregado de los usuarios en configuraciones 1+1 con conmutación automática en caso de fallos, la redundancia permite el cambio o actualización de tarjetas sin interrupción del servicio.

El 7270 está compuesto por un solo bastidor en dos configuraciones posibles, que incluyen 6 u 8 ranuras para alojar tarjetas de control e interfaces y con una capacidad de conmutación de 800 Mbps. El máximo de conexiones es de 32000 y la interfaz con mayor velocidad es OC-3/STM-1. En una configuración redundante dos de las ranuras son ocupadas por la tarjeta de control y conmutación y el resto queda disponible a interfaces.

El 7470 comienza por un simple bastidor con 12 ranuras de tarjetas y capacidad de conmutación de 1,6 Gbps, se pueden añadir bastidores sin interrupción del servicio para formar un sistema con 96 ranuras de tarjetas y capacidad de conmutación de 12,8 Gbps en incrementos de 800 Mbps. El máximo de conexiones es de 64000 y la interfaz con mayor velocidad es OC-12/STM-4. En la configuración simple 1 o 2 de las ranuras, si se desea redundancia, son usadas en las tarjetas de control. El sistema múltiple se forma por bastidores conmutadores y bastidores de periféricos iguales a los del sistema simple que posibilitan usar las 12 ranuras para tarjetas de interfaces de múltiples tipos de servicio y se interconectan con los conmutadores por cables de fibra óptica.

Los servicios IP se soportan mediante la Tarjeta de Servicios IP (***ISC, IP Service Card***), que permite la creación de VPN sobre la red ATM con soporte de calidad de servicio. El soporte de IP/MPLS en las nuevas versiones de la ISC asegura la evolución del sistema hacia redes IP/MPLS. La ISC permite la creación de 128 entidades de ruteo que permiten la interconexión IP con interfaces físicas, como por ejemplo la tarjeta de cuatro puertos Ethernet 10/100, para el soporte de servicios IP sobre ATM.

La gestión de los elementos y de la red (de todos los conmutadores Alcatel descritos en este anexo) es posible de forma centralizada desde el Gestor de Red 5620 de Alcatel, que incluye: gestión de fallas, configuración, desempeño y funciones de seguridad. Además soportan gestión por SNMP.

SIGLARIO

A	
AC	Circuitos de Acceso
ATM	Modo de Transferencia Asincrónico
B	
Backbone	Dorsal de la red.
BGP	Protocolo de Pasarela de Borde
C	
C-VLAN	VLAN de cliente
CE	Router de Frontera del Cliente
CPU	Unidad de Procesamiento Central
E	

EoMPLS	Ethernet sobre MPLS
E-LINE	Ethernet LINE
E-LAN	Ethernet LAN
E-TREE	Ethernet tree
ETECSA	Empresa de Telecomunicaciones de Cuba
Ethernet	Arquitectura de red de conmutación de paquetes
F	
FEC	Clase Equivalente de Envío
FIB	Base de Información de Envío
FR	Conmutación de Tramas
H	
H-VPLS	VPLS Jerárquico
I	
IETF	Grupo Especial sobre Ingeniería de Internet
IS-IS	Sistema Intermedio - Sistema Intermedio
ISP	Proveedor de Servicios de Internet
L	

L2VPN	Red Privada Virtual de Capa2
L3VPN	Red Privada Virtual de Capa3
LAN	Red de Área Local
LDP	Protocolo de Distribución de Etiquetas
LER	Router de Frontera de Etiquetas
LFIB	Base de Información de Envío de Etiquetas
LIB	Base de Información de Etiqueta
LSP	Trayecto Conmutado de Etiquetas
LSR	Enrutador Conmutador de Etiquetas
M	
MAC address	Dirección MAC
MPLS	Conmutación de Etiqueta de Multiprotocolo
MTU	Unidad de Máxima Transferencia
O	
OAM	Gestión y Operación
OSPF	Primer Trayecto Abierto más Corto
P	

P	Proveedor.(Router de núcleo en contexto VPN)
P2MP	Punto a Multipunto
P2P	Punto a Punto
PE	Frontera del Proveedor.(Router de frontera en contexto VPN)
POP	Punto de Presencia
PSTN	Redes Telefónicas Públicas Conmutadas
PW	Seudo conexión
Q	
QoS	Calidad de Servicio
R	
RADIUS	Servicio de autenticación remota.
RR	Reflectores de Ruta
RT	Ruta Objetivo.
RTBP	Protocolo de Elasticidad y Balance de Tráfico
S	
SDH	Jerarquía Digital Síncrona.
SLA	Acuerdo de Niveles de Servicio

SP	Proveedor de Servicio.
STP	Protocolo de Expansión de Árbol
T	
TDM	Multiplex por División de Tiempo
TLS	Servicio LAN Transparente
TE	Ingeniería de Tráfico.
V	
VC	Circuito Virtual.
VCID	Identificador de Circuito Virtual (usado por LDP)
VLAN	Red Virtual de Área Local
VoIP	Voz sobre IP.
VP	Trayecto Virtual.
VPI/VCI	Identificador de Camino Virtual/ Identificador de Canal Virtual.
VPLS	Servicios LAN Privados Virtuales.
VPN	Red Privada Virtual.
VRF	Instancia de Enrutamiento y Envío VPN.
VRP	Plataforma de los equipos Huawei

VSI	Instancia de Conmutación Virtual
W	
WAN	Red de Área Amplia.