

# TUTORIAL TÉCNICO DEL VPLS

## Introducción técnica a los servicios Ethernet multi punto sobre MPLS

### Introducción

Las VPNs (redes privadas virtuales) han evolucionado de forma considerable desde su introducción a principios de los años ochenta, cuando fueron construidas usando líneas alquiladas dedicadas. Frame relay, introducido en los años 90, es actualmente la oferta VPN predominante a escala mundial.

Después de la introducción de MPLS (comunicación por etiquetas multiprotocolo) a finales de los noventa, se definieron nuevos tipos de VPN. La aceptación por los proveedores de servicio del MPLS como la tecnología de convergencia de red a elegir llevó a poner una gran atención en las VPNs basadas en MPLS, que ofrecen fácil suministro de servicios dentro de las redes de los proveedores de servicios, además de la entrega de servicios a los usuarios.

Los diferentes tipos de VPN basadas en MPLS pueden clasificarse de distintas formas. Una de las más sencillas es basar la clasificación en el servicio que se está ofreciendo al cliente. Usualmente es un servicio multipunto o punto-a-punto de capa 2 [1, 2] o capa 3. Esto da lugar a los siguientes tipos de VPN:

VPNs multipunto de capa 3 o VPNs IP (protocolo Internet); se denominan normalmente como VPRN (redes enrutadas privadas virtuales).

VPNs punto a punto de capa 2, que consisten básicamente en una colección de VLLs (líneas alquiladas virtuales) distintas o PWs (pseudowires).

VPNs multipunto de capa 2, o VPLSs (servicios LAN privados virtuales), como se indica en este artículo.

Las VPNs IP basadas en MPLS, introducidas hace algunos años, disfrutan actualmente de un crecimiento saludable. Los dos puntos fuertes de este servicio VPN son su naturaleza multipunto y su soporte de IP. Las VLLs, introducidas más recientemente, ofrecen una clara migración de las tradicionales VPNs de FR/ATM (frame relay/modo de transferencia asíncrona) a la red MPLS convergente sin sustituir equipo en las instalaciones del cliente y sin afectar a la experiencia de servicio del cliente.

Aunque los servicios VPLS sólo han sido introducidos de forma reciente, un gran número de operadores ya los están ofreciendo comercialmente. Como las VPNs IP basadas en MPLS, el VPLS es un servicio multipunto, pero a diferencia de las VPNs IP éste

puede transportar tráfico no-IP; también se beneficia de las bien conocidas ventajas de Ethernet. VPLS también se utiliza dentro de una red de proveedores de servicios para agregar servicios a suministrar a clientes de empresas y residenciales.

Este artículo se centra en los fundamentos de VPLS y H-VPLS (VPLS jerárquico) como se describen en los foros de normalización y ampliamente apoyados por los principales fabricantes; Alcatel es uno de los fundadores de VPLS y H-VPLS. Las soluciones e innovaciones de Alcatel son tema de otro artículo de este número de *Revista de Telecomunicaciones de Alcatel* [3].

### VPLS sobre MPLS: Descripción de la solución

VPLS, también conocido como TLS (servicio de LAN transparente) o servicio E-LAN, es una VPN multipunto de capa 2 que permite conectar múltiples sitios en un único dominio puenteado sobre una red MPLS/IP gestionada por el proveedor [4]. Todos los sitios del cliente en un caso de VPLS (es decir, un VPLS para una empresa particular) parecen estar en la misma LAN (red de área local), sin tener en cuenta sus localizaciones. VPLS utiliza una interfaz Ethernet con el cliente, simplificando la frontera LAN/WAN (red de área extensa) y permitiendo un aprovisionamiento rápido y flexible del servicio.

Una red con VPLS consta de CEs (bordes de cliente), PEs (bordes de proveedor) y de una red central MPLS:

El dispositivo CE es un router 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 (circuito de conexión). 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. Ya que el VPLS es un servicio Ethernet de capa 2, el PE debe ser capaz de conocer, puentear y replicar el MAC (control de acceso a los medios) 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 (protocolo de distribución de etiqueta) se utiliza para establecer estos túneles; alternativamente se puede utilizar RSVP-TE (protocolo de reserva de recurso – ingeniería de tráfico) 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 routers 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 (servicio de autenticación remota de marcación de entrada de usuario).

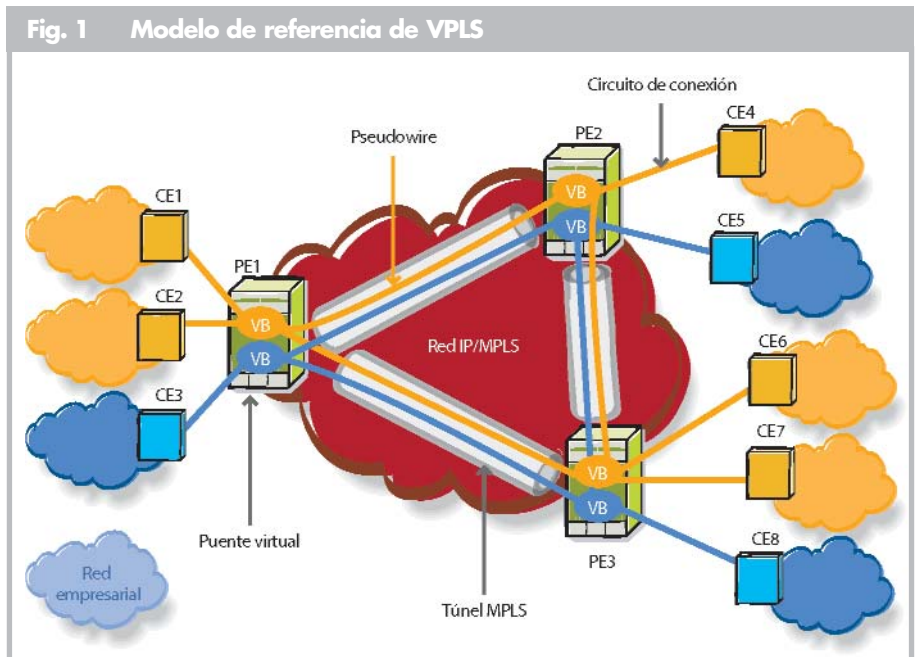
La tecnología pseudowire está normalizada por el IETF (grupo de tareas sobre ingeniería de Internet) PWE3 (Pseudo Wire Emulation Edge to Edge) Working Group [5]. Los PWs son conocidos históricamente como “túneles Martini”, y a las extensiones al protocolo LDP para permitir la señalización de PWs se las 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 (conexión virtual). 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:

cuando PE recibe una trama Ethernet con una dirección de fuente MAC desconocida, PE sabe en qué VC se envió.

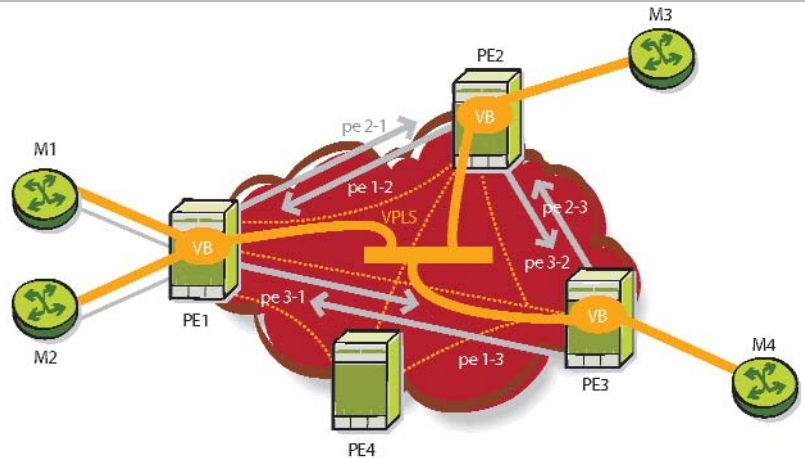
Los routers PE deben soportar todas las prestaciones “clásicas” Ethernet, como aprendizaje del MAC, replicación y envío de paquetes. Conocen las direcciones MAC de la fuente MAC del tráfico que llega a sus puertos de acceso y de red. Desde un punto de vista funcional, esto significa que los PEs deben implementar un puente por cada instancia VPLS, al que se le suele llamar VB (puente virtual), como se muestra en la *Figura 1*. La funcionalidad VB se lleva a cabo en el PE mediante una FIB (retransmisión de base de información) 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 routers 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 routers PE que participan en ese servicio hasta que responde la estación de destino y la dirección MAC es aprendida por los routers 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



**Fig. 2 Señalización pseudowire**

- PE1->PE2: para Svc-id 101 use pe 2-1 de etiqueta VC
- PE2->PE1: para Svc-id 101 use pe 1-2 de etiqueta VC
- PE1->PE3: para Svc-id 101 use pe 3-1 de etiqueta VC
- PE3->PE1: para Svc-id 101 use pe 1-3 de etiqueta VC
- PE3->PE2: para Svc-id 101 use pe 2-3 de etiqueta VC
- PE2->PE3: para Svc-id 101 use pe 3-2 de etiqueta VC



VPLS.

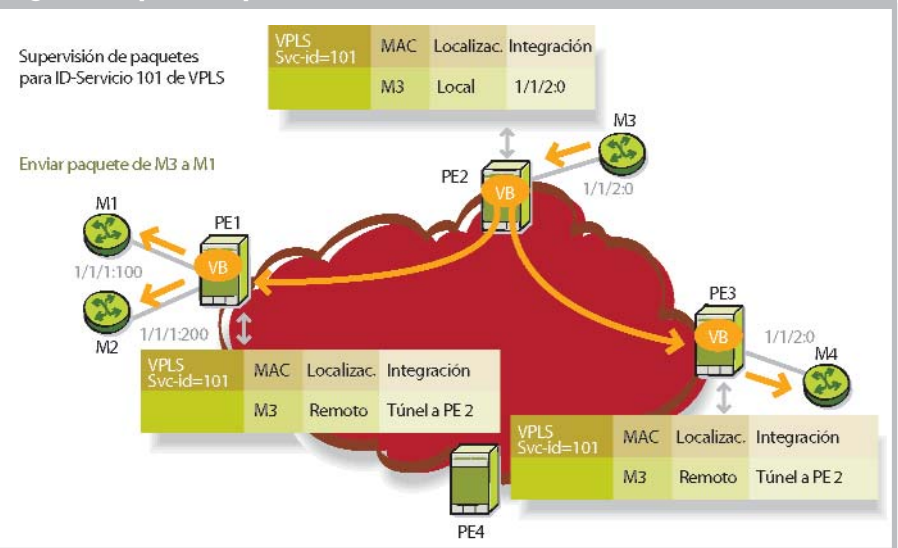
**¿Cómo funciona VPLS?**

Se da por sentado que hay una malla completa de túneles MPLS entre los cuatro PEs conectados a la red MPLS. Ha de 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 (ver Figura 2) han sido configurados en los PEs para pertenecer a una instancia VPLS concreta: Svc-id 101.

**Creación de los pseudowires**

Se necesita crear tres PWs, cada uno con un par de LSPs unidireccionales, o conexiones virtuales. Para señalar la etiqueta-VC entre PEs, cada PE inicia una sesión LDP 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 (p. ej., Svc-id 101). En el ejemplo de abajo, 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

**Fig. 3 Aprendizaje VPLS**



el encapsulado de paquetes”. De este modo se crea el primer PW.

**Aprendizaje del MAC y envío 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), según se muestra en la Figura 3:

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). El formato del paquete se muestra en la *Figura 4*.

PE1 conoce por el pe2-1 de la etiqueta VC que M3 está detrás de PE2 y almacena esta información en el FIB para Svc-id 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 Svc-id 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 (ver *Figura 5*):

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.

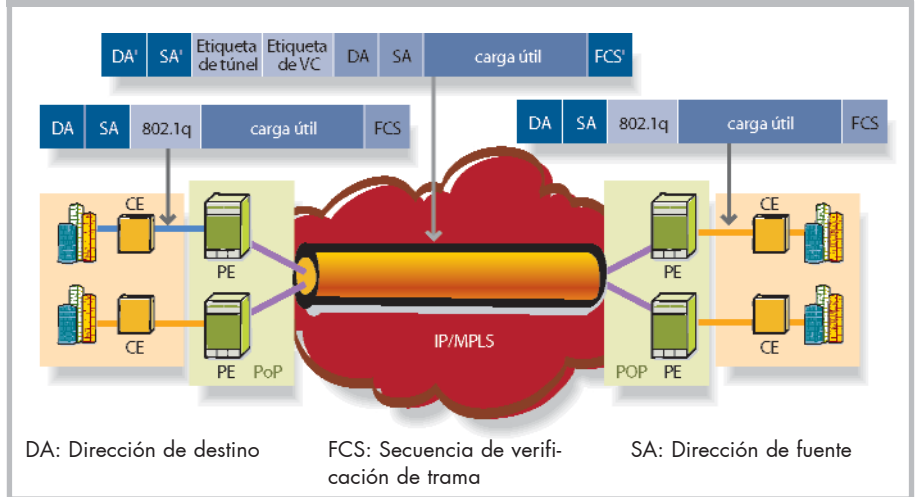
PE1 ya sabe que M3 se puede alcanzar vía PE2 y, por ello, solamente envía el paquete a PE2 usando la etiqueta VC pe1-2.

PE2 recibe el paquete para M3 y sabe que M3 es accesible por el puerto 1/1/2:0. M3 recibe el paquete.

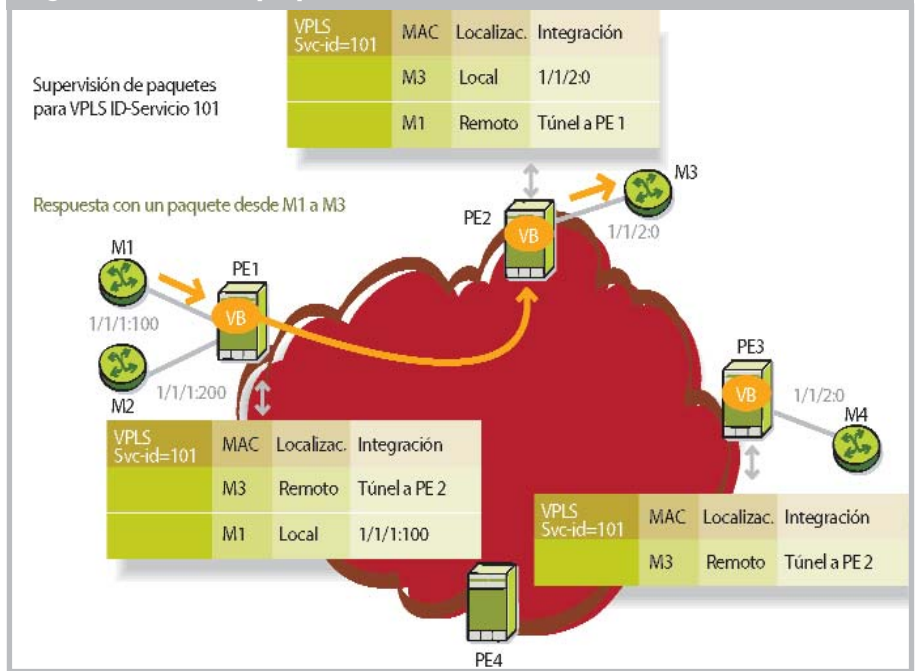
### VPLS jerárquico

La arquitectura H-VPLS se construye sobre la base de la solución VPLS, ampliándola para proporcionar distintas ventajas operacionales y de escala [4]. Es

**Fig. 4 Formato de paquete VPLS**



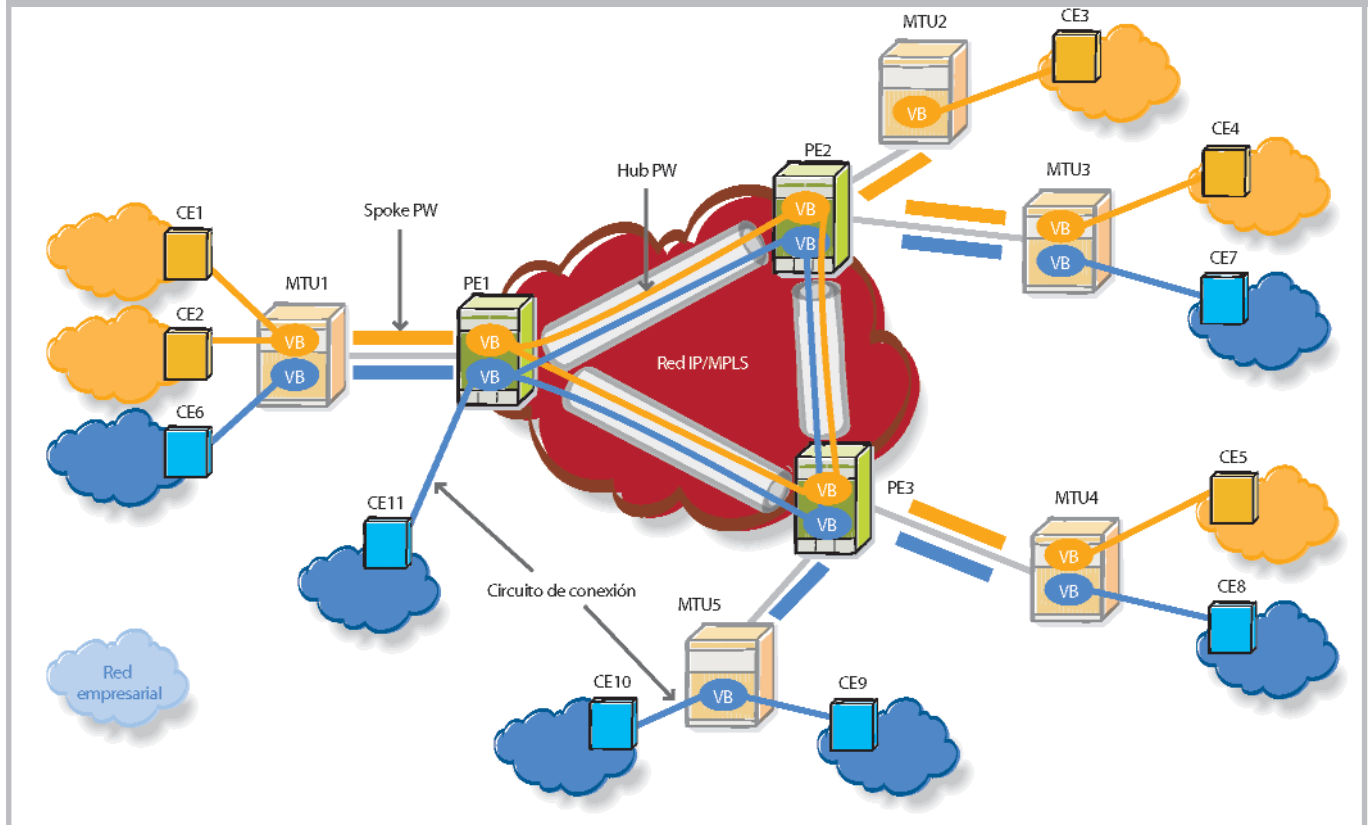
**Fig. 5 Envío de paquete VPLS**



especialmente útil en despliegues a gran escala con un gran número de PEs y/o MTU (unidades multiusuario).

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. Los proveedores del servicio necesitan entonces agregar tráfico MTU hacia el dispositivo PE en la central principal o PoP (punto de presencia), según se muestra en la *Figura 6*. Una MTU tradicional es un dispositivo Ethernet que soporta todas las funciones de

Fig. 6 Modelo de referencia de H-VPLS



conmutación de la capa 2, incluyendo las funciones normales de derivación de aprendizaje y replicación en todos sus puertos; está dedicada normalmente a una empresa. Para compartir los recursos WAN de forma eficaz entre los clientes existe la posibilidad de ampliar la funcionalidad VPLS a los MTUs. En este caso, los MTUs actúan como dispositivos PE, llevando a un gran número de PEs participantes en el VPLS. Una red con numerosos MTUs/PEs, nos llevaría a limitaciones en la escalabilidad en términos del número de PWs a mantener, paquetes a replicar y direcciones MAC a mantener.

Las ventajas del escalamiento del H-VPLS se obtienen introduciendo la jerarquía, eliminando así la necesidad de una malla total de LSPs y de PWs entre todos los dispositivos participantes. La jerarquía se alcanza aumentando la malla principal del VPLS base del PE al PWs de PE (llamados *hub PWs*) con PWs de acceso (llamados *spoke PWs*) para formar un modelo VPLS jerárquico de dos niveles, como se muestra en la **Figura 6**.

Los spoke PWs se crean entre los MTUs y los routers PE. H-VPLS ofrecen la flexibilidad de utilizar distintos tipos de conexión para la implementación del spoke PW: o una conexión etiquetada IEEE 802.1Q, o un LSP

MPLS con señalización LDP.

H-VPLS ofrece también distintas ventajas operacionales centralizando en los routers PE del PoP las funciones principales (p. ej., auto-detección del punto final VPLS, participando en un backbone enrutado, manteniendo una malla completa de túneles LSPs y múltiples mallas totales de PWs). Esto hace posible utilizar dispositivos MTU de bajo costo y mantenimiento, reduciendo así el desembolso de capital total y de los gastos de explotación ya que, normalmente, hay un número mayor de dispositivos MTU que de routers PE. Otra ventaja operacional ofrecida por H-VPLS es el aprovisionamiento centralizado con pocos elementos a intervenir para reactivar el servicio de un cliente. Añadir un nuevo dispositivo de MTU requiere alguna configuración del router PE local, pero no requiere señalización *alguna* con otros routers PE o dispositivos MTU, simplificando de manera importante el proceso de aprovisionamiento.

En H-VPLS, un CE se conecta a una MTU mediante un circuito de conexión. Un AC de un cliente específico se asocia (por configuración) con un puente virtual dedicado a ese cliente dentro de la MTU considerada

<sup>1</sup> Cuando una dirección MAC no se ha utilizado durante un determinado tiempo se borra de la tabla; a esto se le conoce como "aging".

(ver *Figura 6*). Un AC puede ser un puerto físico o lógico etiquetado de VLAN (LAN virtual). En el escenario básico, una MTU tiene un canal de ida a un PE. Este canal de ida consta de un spoke PW para cada VPLS servido por la MTU. Los extremos de este spoke PW son una MTU y un PE. Los spoke PWs se pueden implementar usando PWs MPLS de LDP señalizado, si MTU permite MPLS. Alternativamente, pueden implementarse usando P-VLAN (VLAN de proveedor) por lo que cada VLAN en el canal de ida MTU-PE de una red de agregación Ethernet identifica un spoke PW. En la *Figura 6*, el canal de ida entre MTU1 y PE1 transporta dos PWs, ya que MTU1 tiene dos clientes VPLS conectados. Como MTU tiene solo un PW por VPLS, su operación es sencilla:

Las tramas Ethernet con direcciones MAC aprendidas se conmutan consecuentemente dentro del VPLS. Las tramas con direcciones MAC difundidas o desconocidas recibidas del PW se replican y envían a todos los dispositivos CE conectados dentro del VPLS.

Las tramas con direcciones MAC difundidas o desconocidas recibidas desde un dispositivo CE se envían por el PW al PE y a todos los restantes dispositivos conectados al CE dentro del VPLS.

Las direcciones MAC desconocidas se aprenden y aged<sup>1</sup> dentro del VPLS (tanto las tramas que provienen del PW como las de dispositivos CE).

El dispositivo PE necesita implementar un VB por cada VPLS servido por los MTUs conectados al PE; los spoke PWs son vistos como ACs de diferentes clientes. Como tal, un spoke PW particular se asocia con VB PE

dedicado a la instancia VPLS considerada. En la red central, PE tiene una malla de conexión completa de PWs a todos los otros PEs que sirven el VPLS (como en el escenario normal de VPLS). Estos PWs centrales se llaman hub PWs. Desde un punto de vista del nivel del plano de control y del plano de datos, la operación de los PE es la misma que en el escenario VPLS básico.

### El servicio inter-metropolitano

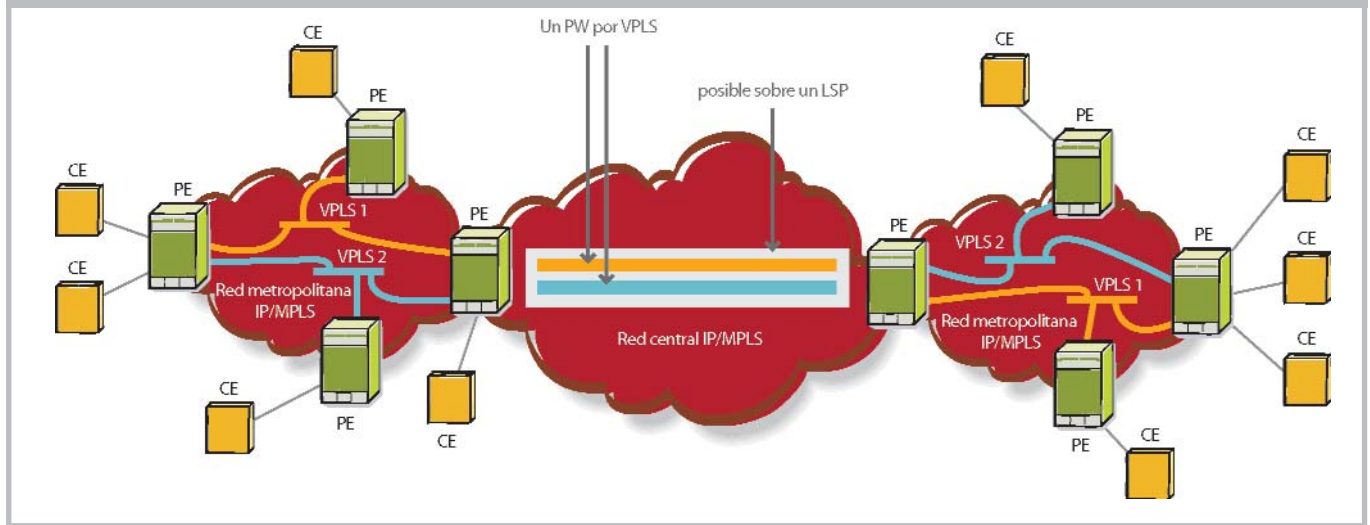
H-VPLS permite que los servicios VPLS se extiendan por múltiples redes metropolitanas, como se muestra en la *Figura 7*. Se utiliza una conexión spoke para conectar cada servicio VPLS entre dos áreas metropolitanas. En su forma más simple, podría ser un LSP de túnel. Un conjunto de etiquetas PW de ingreso y egreso se intercambian entre los dispositivos PE de borde para crear un PW por cada instancia de servicio VPLS a transportar sobre este LSP. Los routers PE en cada extremo tratan este PW inter-metropolitano como una conexión spoke virtual para el servicio VPLS, de la misma manera que tratan las conexiones PE-MTU. Esta arquitectura reduce al mínimo la tara de señalización y evita una malla total de VCs y LSPs entre las dos redes metropolitanas.

### Conclusión

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

Fig. 7 H-VPLS usado como servicio intermetropolitano



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.

Alcatel soporta VPLS y H-VPLS en una amplia gama de productos que incluyen productos ópticos y datos, complementados por una potente gestión de red y servicios.

**Referencias**

- 1 Grupo de trabajo IETF L2VPN: <http://www.ietf.org/html.charters/l2vpn-charter.html>.
- 2 L. Andersson, E. Rosen: "Marco para Redes Privadas Virtuales capa -2", Marco IETF L2VPN, trabajo en curso, <http://www.ietf.org/internet-drafts/draft-ietf-l2vpn-l2-framework-05.txt>.
- 3 J. Witters, G. van Kersen, J. De Clercq, S. Khandekar: "Claves para desplegar con éxito el VPLS", Revista de Telecomunicaciones de Alcatel, 4º trimestre de 2004, págs. 439-443 (este número).
- 4 M. Lasserre, V. Kompella: "Servicios LAN privados virtuales sobre MPLS", trabajo en progreso, <http://www.ietf.org/internet-drafts/draft-ietf-l2vpn-vpls-ldp-03.txt>.
- 5 Grupo de trabajo IETF PWE3: <http://www.ietf.org/html.charters/pwe3-charter.html>.

Alcatel mantiene un centro de recursos VPLS para aquellos interesados en conocer más sobre los aspectos técnicos y de negocio de este emergente servicio. Para más información visite [www.alcatel.com/vpls](http://www.alcatel.com/vpls).



**Johan Witters** is Solutions Manager for Data Networking solutions in the Alcatel Fixed Communications Group, Antwerp, Belgium. (Johan.witters@alcatel.be)



**Sunil Khandekar** is Director of Product Management within Alcatel's IP Division, Mountain View, California, USA. (Sunil.Khandekar@alcatel.com)



**Jeremy De Clercq** is working on managed home networking in the Alcatel Research & Innovation Division, Antwerp, Belgium. He also actively participates in VPN standardization activities at the IETF and ITU-T. He is a Regular Member of the Alcatel Technical Academy. (Jeremy.De\_Clercq@alcatel.be)