Anexo IV: Artículo presentado en el Congreso 2015

VPNs (Virtual Private Networks)

Daniel Biga, Fernando Dufour, Ariel Serra, Carlos Peliza

Universidad Nacional de La Matanza, Florencio Varela 1903 (B1754JEC) -- San Justo, Buenos Aires, Argentina
infoingenieria@unlam.edu.ar

Abstract

La característica principal de las VPN (Virtual Private Network) es utilizar la infraestructura de las redes públicas y privadas compartidas para ofrecerle a un cliente las facilidades de una red privada. Esto permite a los usuarios beneficiarse de las prestaciones, la seguridad y la gestión de redes de alta performance a costos más accesibles. Las nuevas tecnologías permitieron implementar las VPNs basándolas en redes IP e IP/MPLS (MultiProtocol Label Switching), permitiendo minimizar inversiones y disponer de mayor velocidad de transmisión.

En nuestro trabajo hemos realizado una investigación sobre el estado del arte actual de esta tecnología, focalizándonos en sus principios y alternativas de funcionamiento, también hemos expuesto un ejemplo de un caso de implementación actual en Argentina que nos permite ver la importancia de esta tecnología para las comunicaciones actuales.

Key words: **MPLS, VPN, Servicios, Pseudowire**

9. Introducción

Las redes de transmisión de datos X.25, Frame Relay y modo de transferencia asíncrono (ATM) con sus mecanismos de circuitos virtuales fueron las primeras que permitieron la implementación de redes virtuales independientes para cada cliente, soportadas sobre una misma red con nodos y enlaces físicos compartidos provistos y operados por las compañías de telecomunicaciones.

Existen distintos puntos de vista respecto de si estas tecnologías deben ser consideradas o no VPNs, a los efectos de entender la lógica la evolución de estas últimas las incluiremos como tales y las consideraremos VPNs de primera generación.

Sin embargo las primeras VPNs que fueron reconocidas como tales son las que se establecían sobre las redes IP, destacándose entre ellas las que armaban los clientes entre ordenadores y servidores de VPN en entornos corporativos conocidas como VPNs de acceso remoto. Este tipo de VPN permite que empleados puedan acceder a la intranet de su empresa desde su casa o mientras viaja fuera de la oficina

Otro tipo de VPNs son las punto-a-punto, que permiten unir las oficinas geográficamente dispersas de una empresa.

En las VPN el proveedor proporciona la conectividad entre los sitios del cliente, y permite que sólo los dispositivos que pertenezcan a la misma VPN tengan visibilidad entre ellos. Ningún dispositivo no autorizado pueda acceder a la VPN.

A continuación detallaremos distintas formas de clasificar a las VPNs.

De acuerdo a la evolución histórica de las VPNs, podemos clasificarlas de la siguiente manera:

1ª Generación →Terminadas en el CE y basadas en líneas dedicadas que se alquilaban al proveedor.

2ª Generación →Terminadas en el CE a base de circuitos virtuales ATM/Frame Relay sobre una red de conmutación de paquetes del proveedor.

3ª Generación → Los proveedores ofrecen servicios para gestionar los routers del cliente usados en las terminaciones en el CE.

4ª Generación → VPNs de nivel 3 terminadas en el PE y basadas en IP/MPLS.

5ª Generación → VPNs de nivel 2 terminadas en el PE y basadas en IP/MPLS.

Existen distintos aspectos que permiten caracterizar a las VPNs y una VPN puede contener varias de estas características. En base a esta óptica se las puede clasificar por:

- Según el punto de terminación del túnel.
- Basadas en el CE (overlay)
- Basadas en el PE (peer-to-peer)

Según el tráfico de cliente transportado

- VPN de nivel 3
- VPN de nivel 2

Según el tipo de red del proveedor

IP, IP/MPLS, ATM, Frame Relay, SONET/SDH, red telefónica, etc.

Según la tecnología (protocolos) utilizados para la implementación de túneles

Túneles IPsec, L2TP, PPTP, MPLS-LSP, ATM-VP/VC, Frame Relay, SONET/SDH VT, PPP/Dial-up

Según el Número de redes conectadas

- Punto a punto: 2 sedes
- Multipunto: más de dos sedes

Para nuestro estudio la primera gran división a considerar es:

Customer Provisioned VPN (CPVPN)

Son túneles que interconectan siempre terminales de clientes entre sí (basadas en el CE) que generalmente son simples túneles que interconectan equipos de clientes y en donde la red sólo transporta paquetes IP convencionales.

Provider Provisioned VPN (PPVPN)

Son túneles que interconectan siempre equipos del Carrier y que permiten proveer los servicios definidos por el MEF.

Este es el tipo de túneles en que se focaliza nuestro estudio.

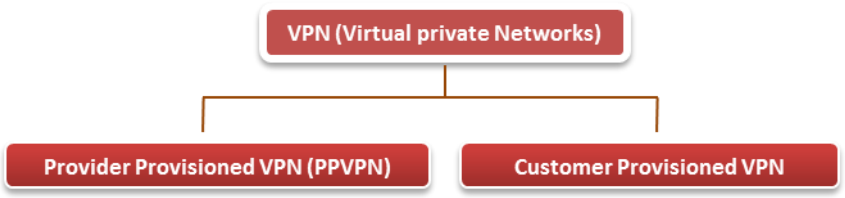

Fig. 2. Primera clasificación de las VPNs

Nos focalizaremos en las PPVPN que es al grupo al que pertenecen las L2VPN.

Provider Provisioned VPN (PPVPN)

Las PPVPN son redes privadas virtuales en las que el proveedor es el responsable de crear y administrar los túneles para el tráfico privado entre los puntos de conexión de clientes.

En la actualidad las redes de los proveedores utilizan la tecnología MPLS que como sabemos, aprovecha el direccionamiento IP y el protocolo de ruteo OSPF, para el establecimiento de los caminos virtuales (Virtual Path).

Por este motivo los proveedores utilizan su infraestructura MPLS como medio de transporte para crear túneles entre los sitios privados. Creando de esta forma un nuevo tipo de servicio, y por ende un nuevo negocio utilizando su red de transporte existente.

Sobre la infraestructura de red MPLS de los Carriers se pueden implementar dos tipos de VPN, las L3VPN (4° generación de VPN) y las L2VPN (5° generación de VPN).

Sobre Las L2VPN nos explayaremos más adelante, pero a continuación haremos una breve mención sobre las L3VPN para que se entienda la diferencia entre ambas.

Las L3VPN también llamadas VPRNs (Virtual Private Routed Networks), permiten que la red sea vista como un súper-router dado que para implementar las VPNs se tienen en cuenta las tablas de ruteo de nivel 3 de cada cliente.

El cliente debe utilizar BGP (MP-BGP) como protocolo de ruteo dentro de la red del proveedor con el objeto de intercambiar la información de ruteo, lo que aumenta la complejidad del diseño y complica la puesta en práctica de este tipo de redes.

Los clientes se conectan con el router del proveedor de servicio, con el que intercambian tablas de rutas, esta información de ruteo es colocada en tablas de ruteo específicas para cada cliente en el router del proveedor (y es transportada con MP-BGP dentro de la red).

Las L3 VPN se puede utilizar para implementar VPNs en redes corporativas, no utilizándose normalmente en redes de servicios públicos debido a su complejidad. En las

redes de servicio público, se ha focalizado en las L2VPN situación que los libera de la complejidad del manejo de la numeración IP a través de las tablas de ruteo.

De las dos opciones la tecnología L2VPN presenta grandes ventajas sobre la L3VPN dado que es vista por los clientes como un switch de nivel 2, evitando las serias consideraciones de plan de numeración IP que tienen las L3VPN. Es por ello que las L2 VPN es la tecnología utilizada para la implementación de los servicios Metro Ethernet CE2.0.

10. L2 MPLS VPN

Las L2 MPLS VPN permiten la implementación de dos modelos de servicio, VPWS (Virtual Private Wire Service) que implica la implementación de un Pseudo Wire que emula conexiones punto a punto y VPLS (Virtual Private Lan Service) que emula un gran LAN Switch permitiendo conexiones punto a punto y multipunto.

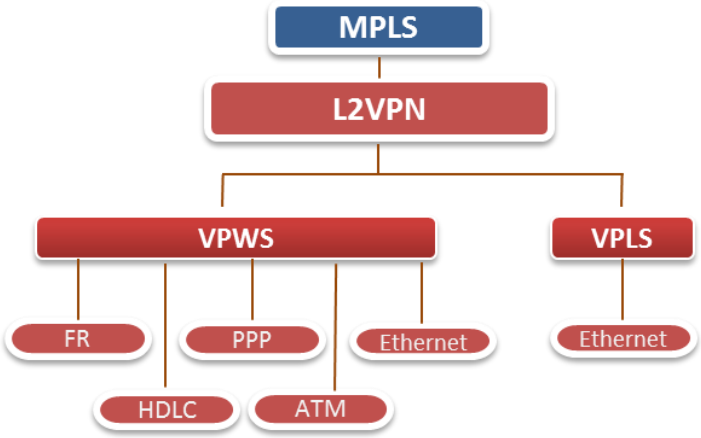

Fig. 2. Modelos L2VPN

Utilizando L2VPNs se logra conectividad en capa 2 entre los sitios, tunelizando las diferentes tecnologías en caminos LSP. De esta forma, se logra transportar una trama L2 entre dos sitios remotos. Desde el punto de vista del cliente, la red del proveedor simula ser una conexión directa (cable) entre los sitios. Las L2VPN son de tipo punto a punto. Los equipos frontera del cliente (Router Customer Edge, CE) mapean el tráfico a un circuito específico (Ethernet, ATM, Frame Relay, etc.) y lo envían al proveedor (Router Provider Edge, PE). El proveedor encapsula dicho tráfico en un LSP, y lo envía hacia el Router PE remoto asociado a dicha conexión. Para obtener conectividad entre varios sitios de una L2VPN, se debe configurar un esquema full-mesh entre los Routers PE. Para este tipo de aplicaciones se puede considerar la utilización de VPLS.

Las tramas del cliente se transmiten utilizando un stack de dos etiquetas MPLS. La etiqueta externa identifica al LSP entre los Routers PE, y la interna identifica a la VPN (Circuito L2) que se está interconectando. Este esquema permite que múltiples VPNs utilicen el mismo LSP de transporte. Debido a que la conexión a través del proveedor se realiza en capa 2, el esquema de ruteo del cliente se implementa en los equipos CE y no involucra al proveedor.

Existen dos variantes de VPNs de capa 2. La diferencia entre las mismas radica en el protocolo de señalización y control que utilizan. Dicho protocolo se utiliza para establecer

las sesiones entre Routers PE, y para negociar la etiqueta VPN a utilizar. Los esquemas son BGP L2VPN (Utiliza el protocolo BGP, draft-Kompella) y LDP L2VPN o LDP L2 Circuit (Utiliza el protocolo LDP, RFC 4447). Al utilizar el protocolo BGP se logra mayor escalabilidad y prestaciones como auto-descubrimiento de vecinos, pero el esquema se hace más complejo. Al utilizar el protocolo LDP, se logra un ambiente más sencillo, pero se debe configurar explícitamente cada vecino y como consecuencia se pierde escalabilidad.

Usando estas tecnologías, el cliente puede tercerizar el transporte de circuitos manteniendo el control del ruteo, utilizando el protocolo de capa 3 que desee. Por otro lado, el proveedor puede utilizar la infraestructura IP/MPLS existente para brindar un nuevo servicio de valor agregado, y utilizar el mismo LSP de transporte para todos los servicios entre Routers PE.

11. Componentes de una red VPLS

Como se ha visto, las nuevas tecnologías de implementación de VPNs trabajan sobre MPLS y a consecuencia de ello, los routers MPLS agregan funciones para el armado de las VPNs, y se los denomina con nuevos nombres. Lo que en una red MPLS se llama LER (Label Edge Router) pasa a llamarse PE y los LSR (Label Switching Router) pasan a llamarse P.

Las empresas públicas que participan en una VPN basada en VPLS se presentan como un LAN Switch de tamaño nacional, independiente para cada cliente que toma servicios sobre sus puertas.

En VPLS, no se pueden producir bucles de información, conocidos como LOOPS: Los PE están conectados en forma full mesh por lo que una trama recibida por un PE (entrante) se envía a otro PE (saliente por una conexión virtual directa. El uso de una configuración full mesh junto con el Split Horizon garantiza un dominio de broadcast, libre de bucles.

A continuación mostramos la arquitectura de una red IP/MPLS que permite implementar VPNs.

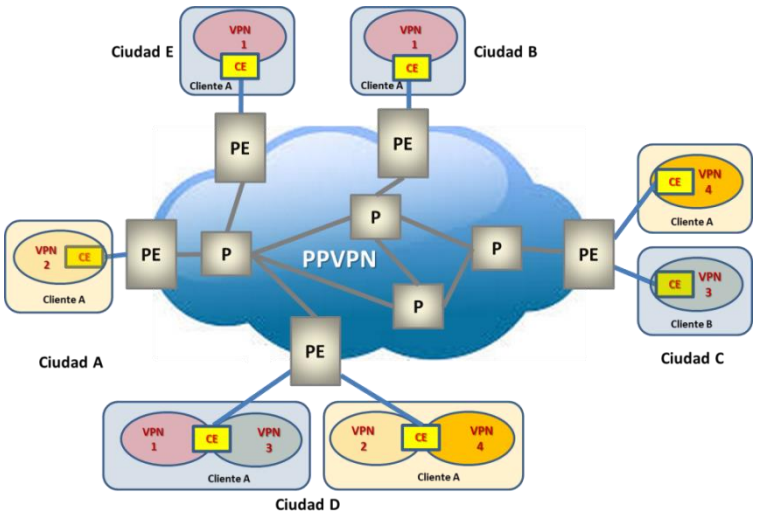

Fig. 3. Arquitectura de L2VPN

Dispositivos de cliente (C): Un dispositivo que está dentro de la red del cliente y no está conectado directamente a la red del proveedor de servicios. Dispositivos de C no son conscientes de la VPN.

CE (Customer Edge): Dispositivo borde de cliente Edge: Un dispositivo en el borde de la red del cliente que proporciona acceso a la PPVPN. Puede ser provisto y gestionado por el cliente o provisto y gestionado por el proveedor dela red, siendo de responsabilidad del proveedor o del cliente según el caso. Se conecta al PE a través del Attachment Circuit (AC). En el caso de VPLS, se asume que la interface entre PE y CE es Ethernet. En el caso de VPWS la interface puede ser FR, ATM, PPP, HDLC ó Ethernet.

PE (Provider Edge): Dispositivo de borde de proveedor: Un PE es un dispositivo o conjunto de dispositivos, en el borde de la red de los proveedores al que se conecta las redes de los clientes a través de dispositivos de CE. La unión del PE y el CE se realiza a través del AC y es el punto de entrada del cliente a la VPN. Los PEs son los elementos claves de las VPNs pues los túneles entre los distintos PE son los que conforman las VPNs. Es también el dispositivo donde residen las funciones las funciones necesarias para las decisiones de forwarding y switching (que siempre se realizan al ingreso de la red L2VPN)

Attachment Circuit (AC): Es el circuito físico que une un CE a un PE. Un AC puede ser, por ejemplo, un DLCI de Frame Relay, un VPI / VCI de ATM, un puerto Ethernet, una VLAN, o un LSP MPLS. Uno o varios ACs pueden pertenecer a la misma VFI.

P (Provider): Es un dispositivo de proveedor que opera dentro de la red del proveedor y no interactúa directamente con el punto final de cliente. Proporcionan enrutamiento de los túneles en la PPVPNs.

Pseudowire (PW): (PWE3) es un mecanismo que emula el funcionamiento de interconexión de un servicio (por ejemplo un circuito TDM, Frame relay o ATM) sobre una red de paquetes.

Hasta ahora hemos mencionado los componentes que tiene una L2 VPN, ahora nos concentraremos en los components propios de una VPLS.

Virtual Bridge instance: Reside dentro de un PE (puede tener distintos nombres según el proveedor), Un Virtual Bridge Instance pertenece a una sola VPLS El VB realiza las funciones standard de bridging de un Lanswitch. Al igual que un Lanswitch, se encarga del forwarding basaado en la MAC addresses y VLAN tags.

VPLS Service ID (VPLS SID): Es un término que utilizamos para identificar el conjunto de todos los VB que conformarían el VPLS para un cliente y que se ve como un súper bridge (a nivel de toda la red). Soporta el Multipoint briging entre todos los ACs y VCs. Es un dominio de broadcast como en todo switch está separado de los otros dominios de broadcast de las otras VPLS SID, Cada VPLS SID se comporta en el súper bridge como una VLAN se comporta en un Lanswitch.

12. El Pseudo Wire (PW)

Pseudowire (PW) es un mecanismo para emular varios servicios de redes o de telecomunicaciones a través de redes de conmutación de paquetes que utilizan Ethernet, IP, o MPLS. Los servicios emulados pueden incluir servicios como Frame Relay, Ethernet, ATM, TDM o SDH. Tal como se define en el RFC 3985, un Pseudowire ofrece el mínimo de

funcionalidad necesaria para emular una conexión física punto a punto con la calidad requerida por las características de cada servicio que emula.

Un PW consiste en un circuito emulado Punto a Punto, para lograr esto, se requieren un par de LSP (MPLS) en direcciones opuestas. Dentro de cada LSP se ubican VC identificados por una etiqueta del PW (PW label). La etiqueta del PW se mantiene extremo a extremo dentro de la red MPLS entre los dos PE.

Para la conexión de los PE se pueden usar targeted LDP (para el caso que usemos señalización LDP).

Pseudowire Emulation Edge to Edge (PWE3), específica la forma en que se encapsula, transporta, controla y gestionan los servicios emulados sobre los PW.

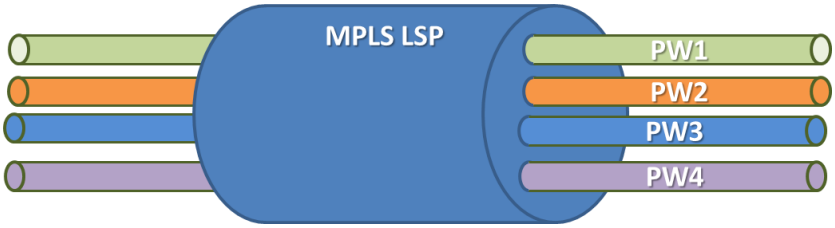

Fig. 4. Pseudo Wire

13. Virtual Private LAN service (VPLS)

VPLS es un PPVPN de Capa 2 (L2VPN), que emula una LAN tradicional. VPLS permite que los segmentos remotos de LAN de un cliente se vean como una sola LAN, con una cobertura interurbana.

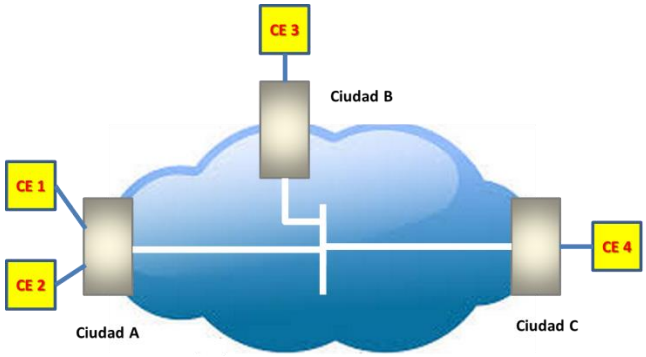

Fig. 5. Modelo 1 VPLS

En el siguiente caso el proveedor de red emula un gran Self Learnig Bridge (que podría ser visto como un Súper Bridge), que aprende las MAC origen, conmuta en función de la MAC destino y deja pasar las tramas broadcast / multicast / unknown.

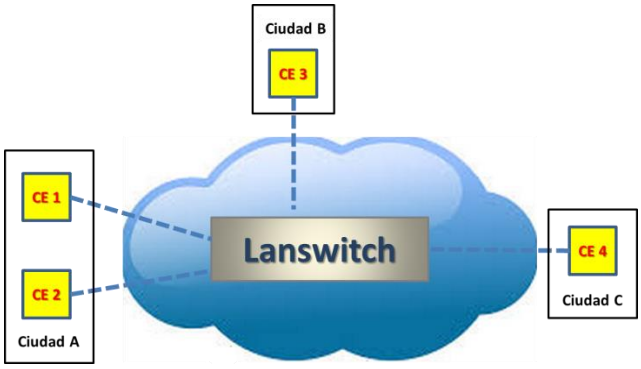

Fig. 6. Modelo 2 VPLS

Las VPLS también son conocidas como TLS (Transparent LAN Service) y como ELAN service.

VPLS se basa en VLLs tradicionales. Soporta comunicaciones multipunto a multipunto.

La inteligencia del servicio reside en los equipos PE, la red MPLS desconoce el contenido de los túneles que transporta y por lo tanto, para ella son túneles como los de cualquier otro cliente.

14. Arquitectura de la red VPLS

En una configuración simple todos los sitios de cliente que se conectan a los PEs de la red pertenecen a una sola instancia VPLS.

Los equipos de un cliente se conectan a uno de los Virtual Bridges (VB) que cada PE tiene creados para él, y todos los VB creados para un cliente se conectan Full Mesh entre sí a través de Pseudo Wires.

Los PE tendrán configurados tantos VB como clientes distintos tenga conectados.

Los clientes se conectan a una VB a partir de una interface o una VLAN (en caso de existir).

Es importante resaltar que existirán tantas redes de VBs independientes como servicios VPLS tenga implementados el proveedor. Por otro lado los PEs solo tendrán VB de un VPLS en los Pes que tenga a este cliente conectado.

El siguiente esquema nos permite visualizar lo explicado.

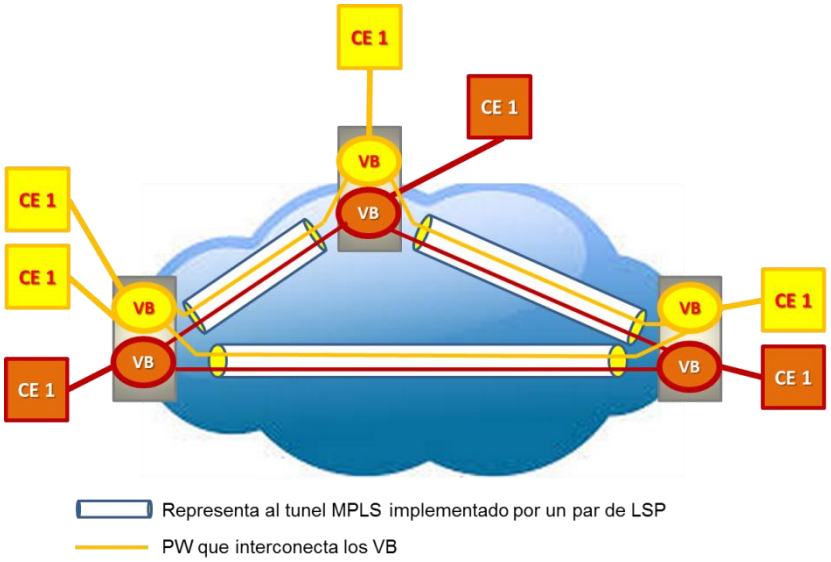

Fig. 7. Modelo 3 VPLS

15. Forma de operación de VPLS

Como dijimos los equipos a los que se conectan los clientes se son los PE, y en una red VPLS los PE deben estar interconectados Full Mesh.

Esta conexión se realiza a través de PWs, que utilizan un par de LSPs (recordar que los LSP en MPLS son unidireccionales, y los PWs son full dúplex).

Los Virtual Bridges de cada VPLS service se interconectan con con PW solo asignados a ese servicio, en la Fig, 6 se ve que los VB amarillos se interconectan con los PW amarillos, y los VB rojos se interconectan con los PW rojos (se han utilizado colores para una mejor visualización).

15.1. Aprendizaje de las MAC y fordwarding

Cuando un VB de una VPLS recibe una trama del CE de un cliente, al igual que un Self Learning Bridge (no olvidemos que lo está emulando) aprende la MAC origen del CE, lo almacena en la tabla de MAC del VB del VPLS del cliente (anotando en que puerta esa MAC se encuentra ubicada)

Luego analiza la MAC destino y pueden ocurrir dos cosas. La primera es que la MAC destino no se encuentre en la tabla de MAC del VB o que sea una dirección de broadcast, en este caso la trama recibida se envía a todos los VB asociados (a través de la malla de PW) que residen en los PE remotos. La segunda es que encuentre la MAC destino en el VB, en este caso sólo envía la trama al VB destino a través del PW que lo asocia.

Cuando los VB de este servicio VPLS ubicados en los PE remotos reciban las tramas, lo primero que harán es anotar en su tabla MAC, la MAC origen (SA) de la trama (anotando como ubicación de la misma el PW por el que le llegó).

Respecto de la dirección destino en caso que sea una MAC unicast la entrega a la puerta correspondiente, y en caso que sea un broadcast se lo envía a todas las puertas de cliente que ese VB tenga.

Es importante mencionar que siempre que llegue una MAC destino unicast, la misma existirá en el VB destino, pues el hecho que llegue unicast implica que la MAC fue encontrada en el VB origen y por lo tanto aprendida por señalización (LDP o BGP).

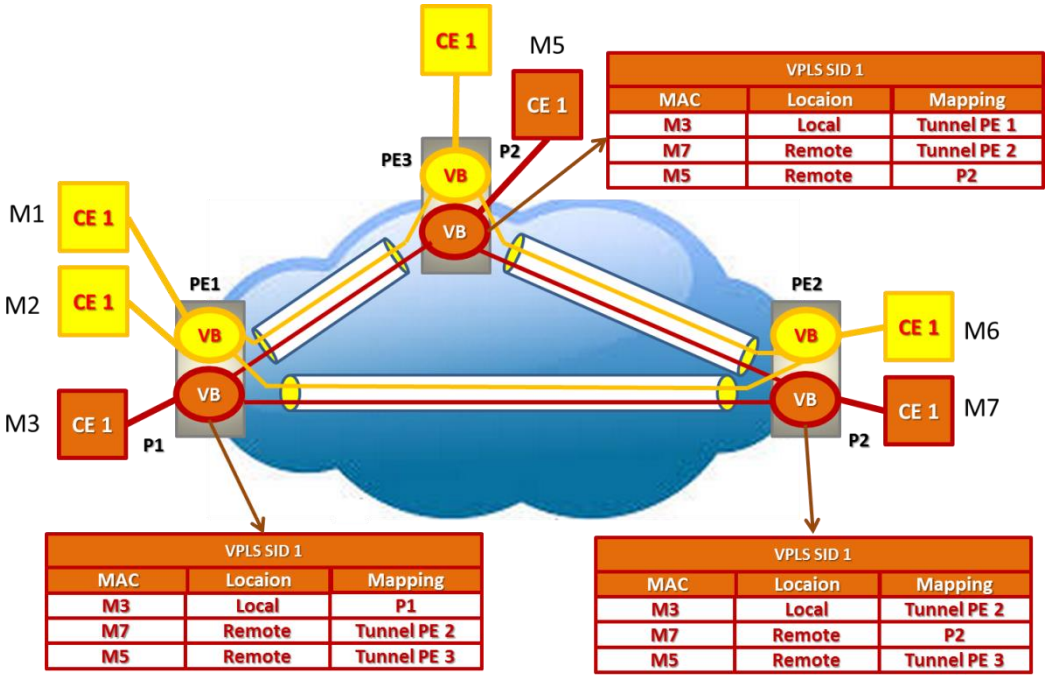

Fig. 8. Aprendizaje en VPLS

15.2. Los bucles en VPLS

Para evitar bucle o loops, los VB implementan Split Horizon. No existe la posibilidad de la existencia de loops dentro de la red pues todos los VB están conectados full mesh.

El problema de los loops en las redes de LAN Switches es abordado por las normas STP, RST y MSP protocol.

Sin embargo puede ocurrir que el cliente (dado su topología externa a la red, requiera del uso de mecanismos para evitar loops (tal sería el caso de redes de clientes que se conectan a dos PE, pero que también tienen uniones externas entre sí).

Por ello VPLS tiene dos formas dee funcionamiento a este respecto, que son:

VPLS Transparen Mode, que transporta los BPDUs generados por el cliente en forma transparente (solo le agrega las etiquetas de PW y VP para su transporte), hacinédoselo llegar a todos los AC (excepto por el que lo recibió) en donde haya Pes de este servicio VPLS.

VPLS Participation Mode, los VB también generan BPDUs dentro del core, el Bridge ID que se utiliza utiliza es la prioridad que le otorguemos al VB más MAC address que cada hardware PE tiene asignada de fábrica. El Port ID será el Virtual Channel port.

16. Virtual Pseudo Wire Service (VPWS)

En el caso de VPWS, el proveedor emula un circuito entre dos puntos de clientes, lo hace a través de un Pseudowire que atraviesa su red.

Esta tecnología ha sido desarrollada como una alternativa de mercado para los servicios de FR y ATM debido a que se presenta servicios similares. También es utilizada para inter-operar con estas tecnologías legacy. De esta forma el proveedor logra importantes ahorros dado que no requiere de redes específicas para cada servicio. También permite el transporte de los protocolos FR, ATM, HDLC y PPP, lo cual se muestra en la siguiente figura.

Fig. 9. Modelo de transporte en VPWS

17. Señalización y autodescubrimiento en L2 MPLS VPN

En las redes L2VPN, se deben atender dos problemas a saber:

Auto-Discovery: Consiste en lograr que los múltiples VB residentes en los PEs que pertenecen a las distintas VPLS, se encuentren entre ellos.

Señalización: Es la forma en que se establecen los túneles y que se distribuyen las etiquetas entre los PEs.

En L2 MPLS VPN, se pueden utilizar dos protocolos, ambas utilizan una cabecera MPLS estándar para encapsular datos.

Los protocolos que se utilizan, que pueden ser:

Basado en BGP: Que realiza ambas funciones, Auto-Discovery y Señalización.

Basados en LDP: Que solo realiza la función de Señalización.

En la siguiente tabla vemos las RFCs que tratan el tema:

VPLS Implementation Model	Discovery	Signaling
RFC 4761 (BGP-based VPLS)	BGP	BGP
RFC 4762 (LDP-based VPLS)	None	LDP

Fig. 10. RFCs VPLS

18. Señalización en L2 MPLS VPN basada en BGP

Se basa en un borrador de la especificación escrito por Kireeti Kompella, de Juniper Networks.

Utiliza el Border Gateway Protocol (BGP) como el mecanismo para routers PE para comunicarse entre sí acerca de sus conexiones con los clientes.

Cada router se conecta a una nube central, usando BGP. Esto significa que cuando se agregan (por lo general a los nuevos routers) nuevos clientes, los routers existentes se comunicarán entre sí, a través de BGP, y añadirán automáticamente los nuevos clientes con el servicio.

19. Señalización en L2 MPLS VPN basada en LDP

El segundo tipo se basa en un borrador de la especificación de Luca Martini de Cisco Systems. Este método también se conoce como un circuito de capa 2.

Utiliza el protocolo de distribución de etiquetas (LDP) para el establecimiento de la comunicación entre routers PE. En este caso, todos los routers de habla LDP, intercambiarán FECs y establecerán LSP con cualquier otro enrutador de habla LDP en la red (o el otro router PE, en el caso de que LDP sea tunelizado en RSVP-TE), que difiere de la metodología basada en BGP.

El estilo basado en LDP de L2 VPN define nuevos TLV y parámetros para la LDP para ayudar en la señalización de las VPNs.

20. Ejemplo de caso real

Uno de los más desafiantes proyectos en redes de datos, de la actualidad nacional es proveer de una solución eficiente para el acceso a los nodos de radio de telefonía celular.

La adopción de los sistemas de tercera generación (3G) de telefonía móvil incluyen las operaciones de oferta de datos. La proporción de volumen de tráfico de datos y de voz cambia completamente respecto al escenario de la generación anterior (2G).

En especial para la red de acceso, denominado Backhaul, donde se cursa todo tráfico de datos y de voz desde los nodos de radio (BTS/NODO B) hasta sus controladores (BSC/RNC).

El Backhaul hasta hace muy poco tiempo estaba basado solo en PDH/SDH lo cual es un escenario pensado únicamente para el tráfico de voz pero no lo es para tráfico de datos, en estas condiciones el Backhaul se puede volver en el cuello de botella para el crecimiento de oferta de BAM (Banda Ancha Móvil), necesitando altas inversiones en estructuras TDM no evolutivas y de mayores costes. Es por ello que se está realizando la transformación del Backhaul hacia una estructura Ethernet que soporte cursar tanto el tráfico de voz como el de datos, manteniendo los requerimientos de disponibilidad y seguridad en la entrega de estos tráficos característicos de operaciones móviles.

Esta evolución del Backhaul basada en una red de paquetes se alinea con la estrategia de evolución de red móvil hacia una estructura "all-over IP" (3GPP) desde la tercera generación.

Las operadoras están aprovechando la capilaridad de su red Metroethernet existente y buscan generar una solución más eficiente usando MPLS.

El modelo de Red del punto de vista lógico se basa en la utilización de PWE3 sobre MPLS (caso particular de VPN MPLS Capa 2) para el transporte del tráfico móvil a través de una red de paquetes.

La figura siguiente ilustra el modelo de red planificado, desde el punto de vista lógico, para los casos donde haya red Metro Ethernet y el acceso esté basado en puertos Ethernet:

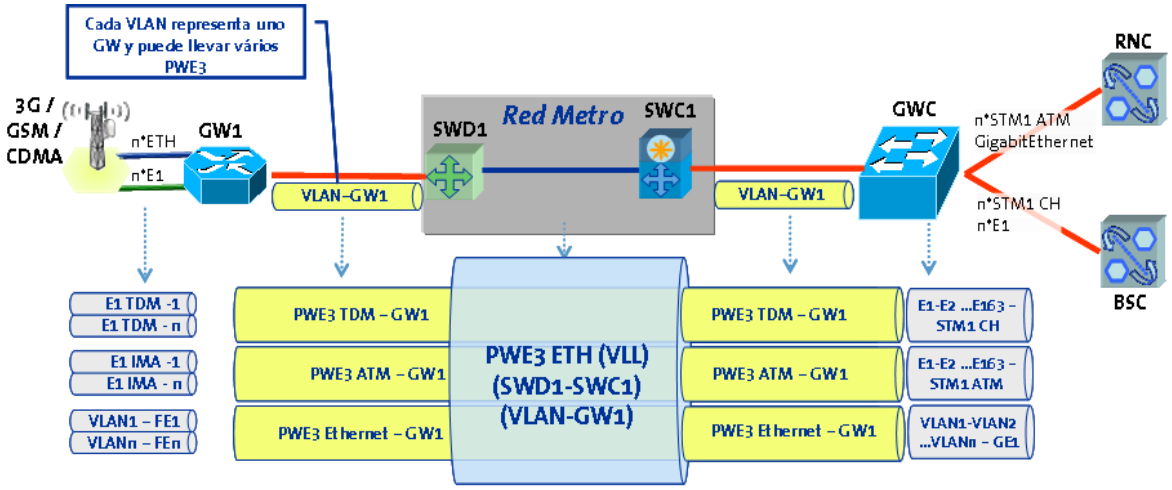

Fig. 11. Modelo de red

Conforme podemos observar en la figura, que los PWE3 son establecidos entre el GW de acceso (GWT o GWD) y el GWC sobre MPLS a través del uso de LDP. Los gateways son capaces de establecer PWE3 TDM (CESoPSN), PWE3 ATM y PWE3 ETH, los 3 tipos de tráficos actualmente encontrados en una red móvil.

Los GWT establecen los PWE3 correspondientes al tipo de tráfico recibido y una VLAN transporta el tráfico hasta el GWD donde es establecida una VLL que lo transporta hasta el GWC donde la VLL y los PWE3 son desmontados y el tráfico es entregado a las controladoras (BSC /RNC). La adopción de tal modelo (con desarrollo de VLLs entre los GWD y GWC) ya contempla un posible desarrollo de otros servicios, por eso son adoptadas las VLL para separación del tráfico de otros servicios.

En la implementación real, las exigencias de un rápido despliegue del Backhaul con costos bajos hicieron que muchas operadoras se volcaran a la compra de equipos chinos para GWT, GWD y GWC, dentro de los cuales, es un proveedor destacado Huawei.

A continuación se muestra el esquema general que se utiliza actualmente en el AMBA (Área Múltiple Buenos Aires) por una importante operadora y los principios de funcionamiento:

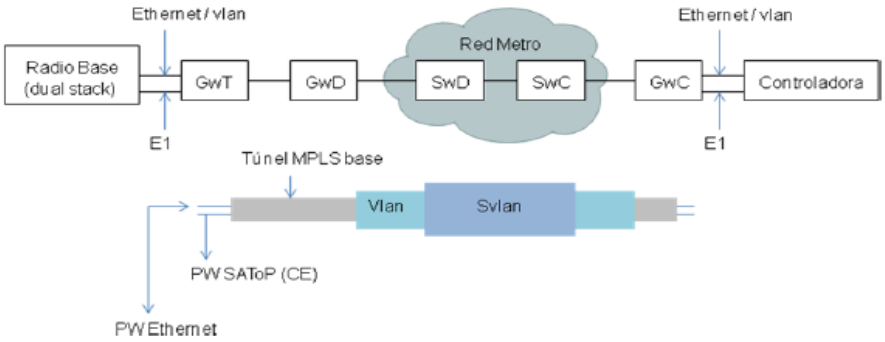

Fig. 12. Esquema general

Entre el GwT (modelo PTN 910, de Huawei) y el GwC (NE 40E de Huawei) se levanta un túnel (estático) base MPLS.

El túnel MPLS que se levanta entre los extremos es un túnel estático, es decir no se utiliza ningún protocolo de distribución de etiquetas (LDP) ya que estas se configuran a mano en los extremos. La falta de manejo de LDP se debe a una limitación técnica de los GwT estas limitaciones son propias de soluciones de compromiso para bajas costos.

En el túnel se transportan los PWs, un PW Ethernet y un PW SAToP (Structure-Agnostic TDM over Packet) producto de la emulación de circuitos realizada para transportar la trama E1 a través de la red Metro (se levanta un PW SAToP por cada E1).

En el GwD (PTN 950/ NE 40E X3, ambos de Huawei) el túnel se encapsula en una VLAN. En el SwD, en la red Metro, se agrega un segundo tag (sVLAN), con el que se transporta el tráfico hasta el SwC, equipo donde se retira dicho sVLAN.

En el GwC, se retira la VLAN, se termina el túnel base y los PWs son convertidos en las respectivas tramas Ethernet y E1 que luego son entregadas a la frontera con la red móvil.

Los proveedores ya están ofreciendo equipos económicos con capacidad de armar túneles de manera dinámica con la utilización de LDP, con estos equipos se espera mejorar la confiabilidad de la red de Backhaul.

21. Conclusiones

Las redes L2 MPLS VPN es la tecnología que están ofreciendo en la actualidad los Carriers de todo el mundo en la actualidad para servicios internos y redes corporativas. El motivo es que es el reemplazo natural de los servicios legados provisto a través de la infraestructura MPLS, también permite el transporte de estos servicios y la interconexión con estas redes residuales.

Adicionalmente con el servicio VPLS pueden ofrecer servicio de conmutación de nivel 2 a múltiples clientes y a nivel nacional como si fuese un Lanswitch de alcance nacional, donde cada servicio VPLS se comporta como una VLAN, separando entornos de broadcast. En este escenario la red del proveedor se independiza de la numeración IP del cliente dado que conmuta a nivel 2.

22. Futuras líneas de investigación

La solución adecuada para cada problemática es dependiente de la dimensión de la red que hay que diseñar como así también de las prestaciones que pretendemos de ella. Por ello y dada la gran variedad de combinaciones tecnológicas posibles para dar solución en particular y la cantidad de casos existentes en el mercado, hemos puesto nuestro foco en las necesidades y dimensiones del mercado Argentino.

Con esta información desarrollaremos una futura línea de investigación en la que nos focalizaremos en la determinación de las mejores prácticas y prospectivas para los próximos 3 años en el mercado Argentino.

23. Referencias

https://datatracker.ietf.org/wg/l2vpn/charter/l2vpn-charter.html
https://datatracker.ietf.org/wg/pwe3/charter/

Sam Halabi (2003). *Metro Ethernet*. Cisco Press. Indianapolis.ISBN: 1-58705-096-X.

J. Guichard and I. Pepelnjak (2000). *MPLS and VPN Architectures*, Cisco Press. Indianapolis. ISBN: 1-58705-002-1.

Bruce S. Davie, Paul Doolan,Yakov Rekhter (May 1998). *Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies*. ISBN-13: 978-1558605053 ISBN-10: 1558605053. First edition

Wei Luo, Carlos Pignataro,Dmitry Bokotey,Anthony Chan (February 2005) *Layer 2 VPN Architectures*. Cisco Press. Indianapolis. ISBN: 1-58705-168-0.

Bruce S. and Davie, Yakov Rekhter (June 2, 2000) *MPLS: Technology and Applications*. ISBN-13: 978-1558606562. ISBN-10: 1558606564. First Edition.

24. Definiciones

E-LAN - Servicio E-LAN definido por MEF utilizado para crear VPN L2 multipunto y un servicio de LAN transparente; constituye los cimientos de las redes IPTV y de multidifusión.

E-Line - Servicio E-Line definido por MEF utilizado para crear líneas privadas Ethernet, líneas privadas virtuales y acceso Ethernet a Internet.

E-Tree - Servicios de árbol privado Ethernet (EP-Tree) definido por MEF y árbol privado virtual Ethernet (EVP-Tree). Proporcionan la separación del tráfico entre usuarios,

permitiendo que el tráfico de una “hoja” llegue a una de varias “raíces”, pero que nunca se transmita a otras “hojas”.

EVC - Circuito virtual Ethernet definido por MEF.

Certificado de referencia


Cuarto Congreso Argentino de la Interacción-Persona Computadora, Telecomunicaciones, Informática e Información Científica (IPCTIIC)

Fourth Argentine Conference on Human-Computer Interaction, Telecommunications, Informatics and Scientific Information (HCITISI)

Certificate

PAPER PRESENTACION

IPCTIIC 2015 :: HCITISI 2015
Huerta Grande – Córdoba, Argentina
November 16 – 17, 2015

Virtual Private Networks

Fernando Javier Dufour
DNI 27.178.618

Universidad Nacional de La Matanza
Buenos Aires, Argentina

ALAIPO & AInCI

[i] Entrevista con Diario TI en septiembre de 2013, Kevin Vachon, Director General de Operaciones del MEF (http://webcache.googleusercontent.com/search?q=cache:wM-ALHBVR9kJ:diarioti.com/los-servicios-los-equipos-de-red-y-los-programas-de-certificacion-profesional-del-mef-ganan-popularidad-en-todo-el-mundo/76153+&cd=1&hl=es-419&ct=clnk&gl=ar&client=firefox-a)