Ingeniería de tráfico

Aplicaciones MPLS: **VPN de capa 2 con MPLS (1ª parte).**

- Introducción. Definición. Tipos.
- L2VPN-MPLS.
  - Pseudocables. Conectividad con pseudocables.
  - Plano de reenvío.
    - Métodos y tipos de encapsulados. Operativa de reenvío.
    - Encapsulado Ethernet. Modos.
  - Plano de control. Soluciones LDP y BGP.
- Conclusiones. L2VPN vs L3VPN.
- Bibliografía.

Introducción.

- VPN de capa 2 con MPLS (L2VPN-MPLS).
  - Solución alternativa a las L3VPN-MPLS para extensión LAN vía WAN.
  - Otro factor de estímulo hacia la tecnología MPLS.
    - L3VPN-MPLS y L2VPN-MPLS estimulan la migración a MPLS por parte del proveedor.
    - En pos de una única tecnología (MPLS) y no múltiples (FR, ATM, MPLS) para **conectividad privada extensa** mediante soluciones L2VPN y L3VPN.
    - Conlleva a reducir costes de inversión/explotación → Abaratamiento de servicios para los clientes.
  - L2VPN-MPLS, **definición**.

    Procedimiento para interconectar sedes de un cliente (LAN) mediante transporte de PDU2 sobre infraestructura MPLS pública del proveedor.
    - Transporte de PDU2 privadas (ATM, FR, Ethernet, etc.) sobre red pública del proveedor.
    - Usualmente mediante topología *hub and spoke*, pero también *full mesh*.
    - Para todo tipo de tráfico (datos, voz, vídeo) → Requisitos QoS.

Introducción.

- Servicios Ethernet sobre MPLS.
  - Transporte de tramas Ethernet (privadas) entre sedes de un cliente sobre red MPLS (pública).
  - Presentan alta demanda dada la penetración Ethernet en redes corporativas, de manera nativa o por migración.
  - Solución "natural" para extender el uso de redes Ethernet.
    - Personal IT de empresas familiarizado con esta tecnología.
    - Más flexible que otras tecnologías en cuanto a tasas de acceso.
    - Equipamiento menos costoso en virtud del volumen de producción respecto a FR, ATM, etc.
  - Dos tipos de servicios posibles para extender Ethernet privada sobre MPLS público.
    - Servicio Ethernet punto a punto, usualmente denominado L2VPN.
    - Servicio Ethernet multipunto, denominado VPLS (*Virtual Private LAN Service*).

L2VPN-MPLS.

- Transporte de PDUs de capa 2 (PDU2) con MPLS.
  - Plano de control.
    - Se ocupa de la **lógica de control** L2VPN.
    - Dos enfoques/soluciones diferentes:
      - Mediante señalización LDP.
      - Mediante señalización BGP.
  - Plano de reenvío.
    - Se ocupa de la **lógica de transporte** L2VPN a través de la red MPLS del proveedor.
    - Mismo encapsulado PDU2/MPLS para ambas soluciones del plano de control (LDP o BGP).

L2VPN-MPLS.

- Transporte de PDUs de capa 2 con MPLS, definiciones.
  - **Pseudocable** (***PW***, ***P****seudo****W****ire*).
    - Denominación en el sentido de que la red del proveedor se hace "invisible" al cliente.
    - **Conexión lógica de capa 2 punto a punto bidireccional** sobre la red del proveedor para transporte de **partes esenciales** de PDU2 o tramas TDM.
      - Tramas Ethernet, PPP, FR, ATM, SDH, etc.
    - Identificado por una "etiqueta" (etiqueta de pseudocable).
    - Posible sobre redes MPLS y redes IP puras (p.e, mediante "tunelado" GRE o IPSec).

GRE (*Generic Routing Encapsulation*): protocolo para transporte de diferentes PDU3 mediante "tunelado" lógico a través de Internet. RFC 1701 y 1702.

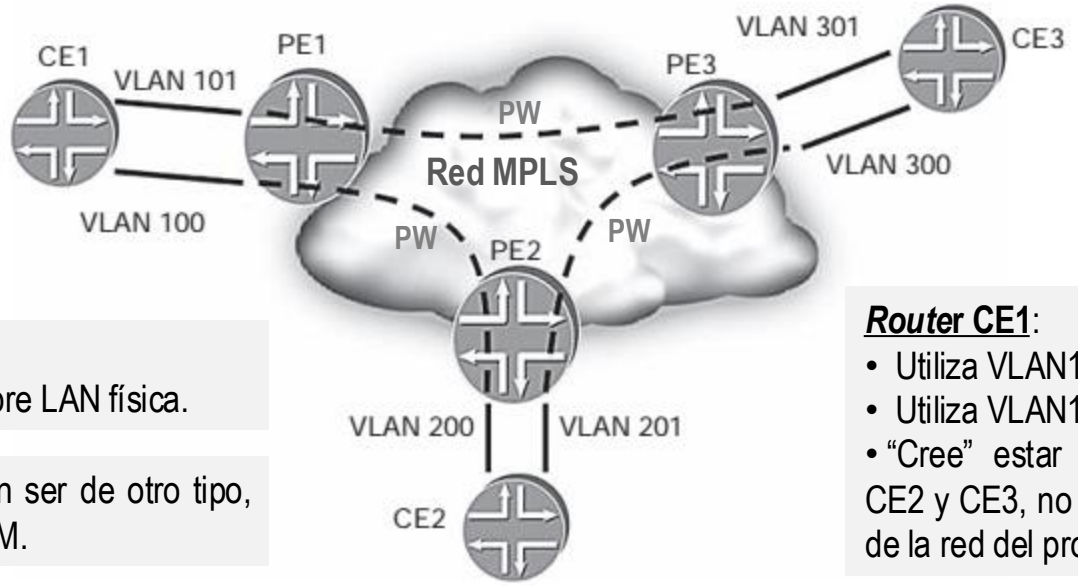
  - Pseudocable en el contexto MPLS.
    - Conexión lógica "directa" entre dos *routers* CE del cliente vía dos *routers* PE del proveedor.
    - Puerto "virtual" desde la perspectiva de la lógica de los *routers* PE.
  - **L2VPN - MPLS.**
    - Conjunto de PW que conectan *routers* CE de un cliente a través de *backbone* MPLS.
    - Topología de interconexión de servicio definida por el propio cliente (p.e, *hub-and-spoke* o *full-mesh*).

L2VPN-MPLS.

- En las redes de proveedores MPLS:
  - Los PW son “tunelados” a través de túneles MPLS (LSP).
  - Uno o varios PW pueden ser multiplexados en el mismo túnel MPLS (mismo LSP).
  - Dos etiquetas se requieren para el soporte de PW (encapsulado Martini).
    - 1ª etiqueta (la más alta) identifica el túnel MPLS (etiqueta de transporte/túnel).
    - 2ª etiqueta (la más baja) identifica el PW (etiqueta PW, etiqueta VPN).
- El *mapping* entre una PDU2 a ser transportada y un PW puede realizarse:
  - A partir del puerto/interfaz físico de conexión al *router* PE local (conexión local entre CE y PE), o...
  - A partir de información de cabecera de la PDU2.
  - En cualquier caso requiere **tablas de reenvío en los PE**, por puerto o por información de cabecera L2.
- Los PW requieren nuevas formas para especificar las FEC.
  - Porque los PW no transportan paquetes IP, sino “tramas” (PDU2 o tramas TDM).
  - **Para indicar a los puntos extremos de los PW cómo reenviar los datos que transporta.**
  - Cada tecnología “transportada” a través de un PW requiere su propia especificación FEC.
  - Solución: extensiones LDP para PW → Nuevos campos en Ms LDP para indicar el servicio emulado.

L2VPN-MPLS.

- Ejemplo de conectividad entre sedes de un cliente.
  - Cliente con tres sedes conectadas en modo *full mesh*.
  - Un PW establecido entre cada par de sedes (entre cada par de *routers* PE).
  - Los PE pertenecen al proveedor, los CE pertenecen al cliente.
  - Acceso Ethernet desde cada sede del cliente a la red MPLS del proveedor.
    - Circuitos de acceso (*CA, Attachment Circuits*) tipo VLAN entre proveedor (PE) y cada sede cliente (CE).



12

VLAN, *Virtual LAN*:
Configuración lógica sobre LAN física.

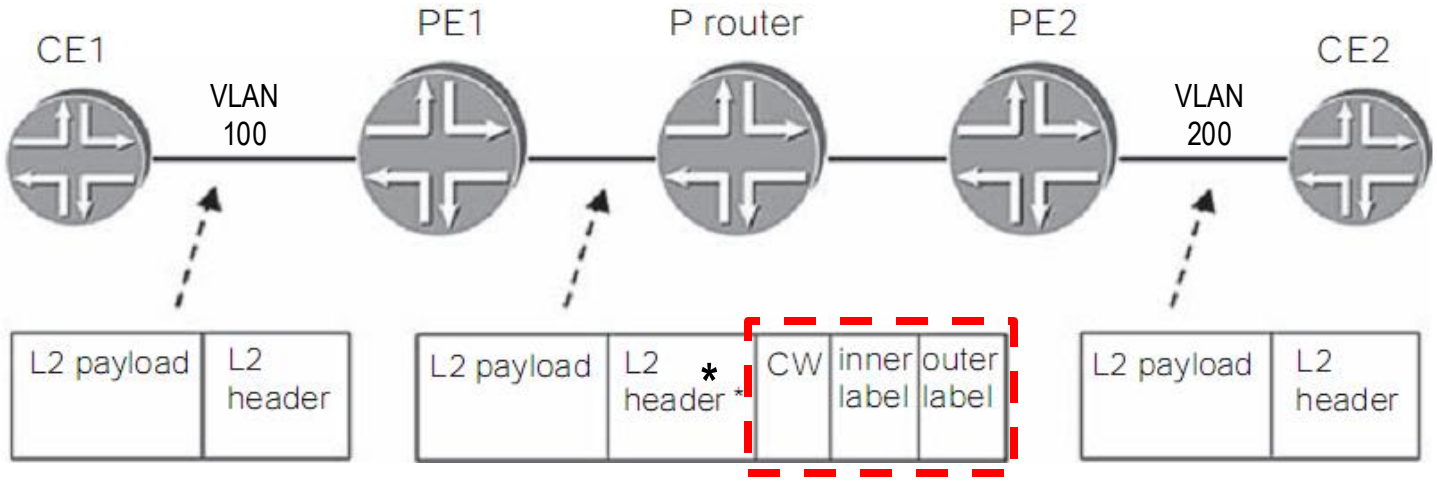
Los CA también podrían ser de otro tipo, ATM o FR, o incluso TDM.

***Router* CE1**:
- Utiliza VLAN100 para conectarse a CE2.
- Utiliza VLAN101 para conectarse a CE3.
- "Cree" estar conectado directamente con CE2 y CE3, no es consciente de la presencia de la red del proveedor.

Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

L2VPN-MPLS.

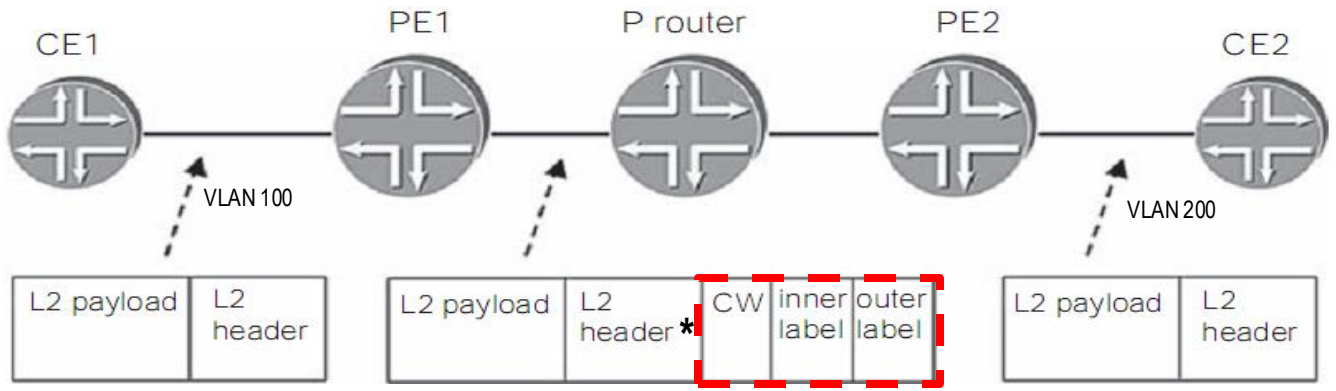
- Plano de reenvío, ejemplo.
  - La figura muestra:
    - Una sección de la red representada en la diapositiva nº 10 (accesos Ethernet).
    - El transporte de tramas L2 sobre el PW que conecta CE1 y CE2 vía PE1, red del proveedor (P) y PE2.
  - L2 header*: cabeceras de capa 2 a transportar sobre red MPLS según protocolo L2 utilizado.
  - Diapositivas siguientes → Operativa básica de los nodos CE, PE y P involucrados.



Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

L2VPN-MPLS.

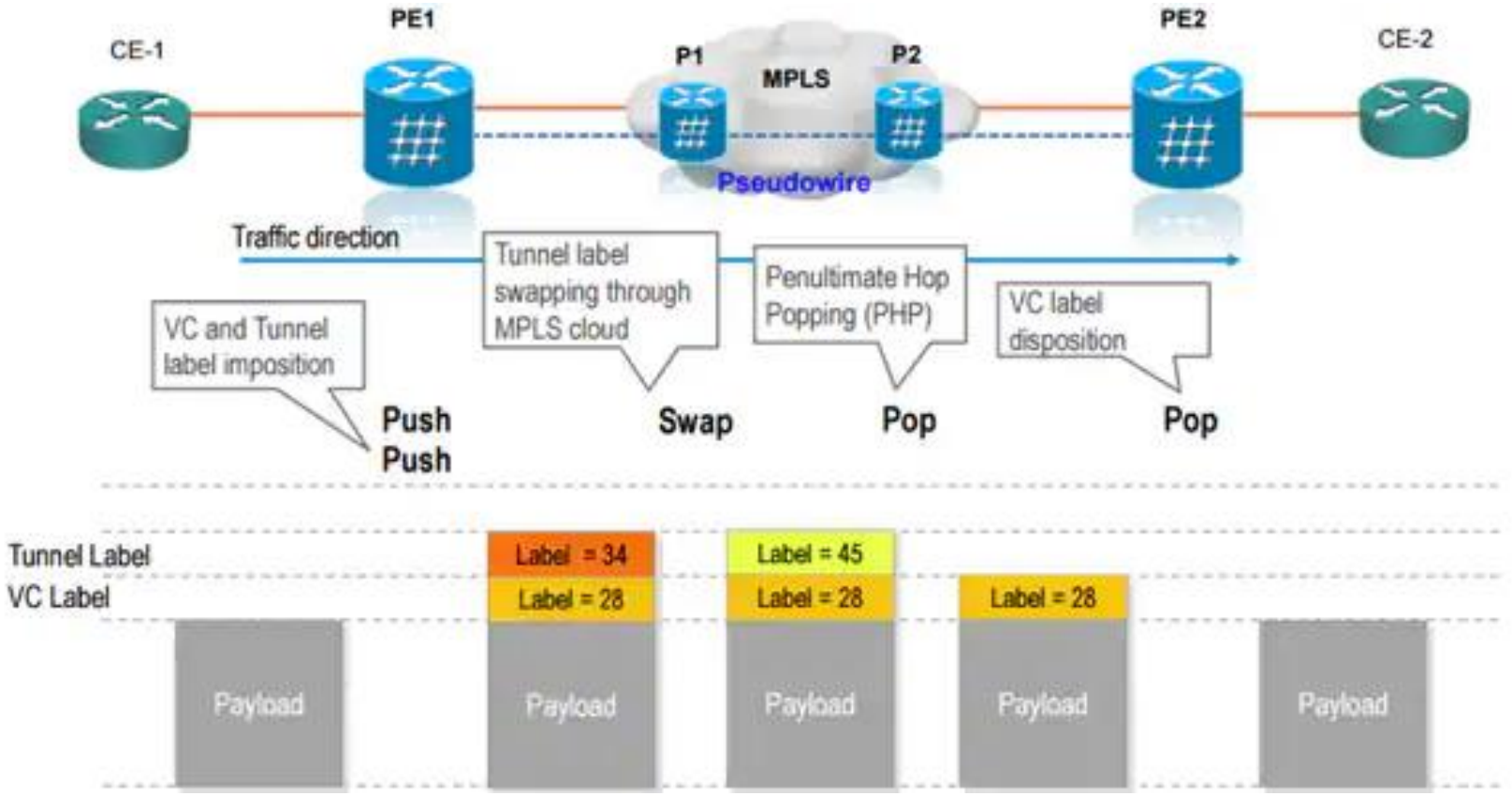
- Ejemplo de operativa básica L2VPN-MPLS
  - Trama L2 llega a PE1 vía enlace de acceso VLAN 100.
  - PE1 (PE de ingreso), para el reenvío:
    - Elimina **parte** de la trama L2 a no transportar al PE remoto (p.e, en tramas Ethernet campos "preámbulo" y FCS).
    - Añade, en ocasiones, campo ***Control Word* (*CW*)** de 4 octetos, que puede contener:
      - Nº de secuencia y *flags* relativos a campos de la cabecera L2 nativa (para no enviar la cabecera L2 completa).
    - Busca y añade la etiqueta VPN (***inner label***) que espera PE2 y que identifica la sede cliente conectada a CE2.
    - Determina cómo alcanzar PE2, qué túnel lógico de transporte escoger.
      - Para túnel MPLS determina la etiqueta de transporte (***outer label***) y la "apila" sobre la etiqueta VPN (***inner label***).



Hay varias formas posibles para establecer **túneles lógicos de transporte** entre dos PE a través de la red del proveedor.
• Para túneles MPLS mediante LSP, ídem a L3VPN-MPLS (con CR-LDP o RSVP-TE).
• Para túneles **no** MPLS según procedimiento con GRE o IPSec.
Un túnel de transporte **puede ser compartido** por diferentes tipos de tráfico: L3VPN, L2VPN y VPLS.

L2VPN-MPLS.

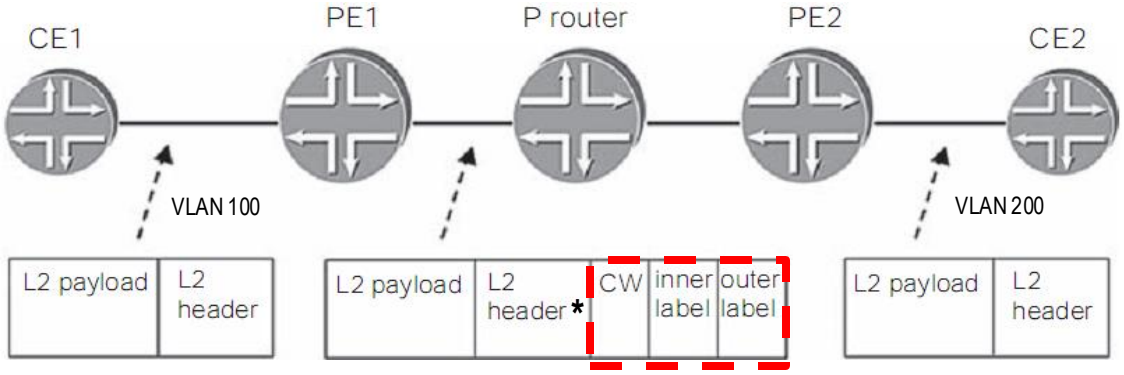
- Plano de reenvío, ejemplo 2.



Fuente de la figura: Cisco – MPLS L2VPN Pseudowire: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/213238-mpls-l2vpn-pseudowire.html

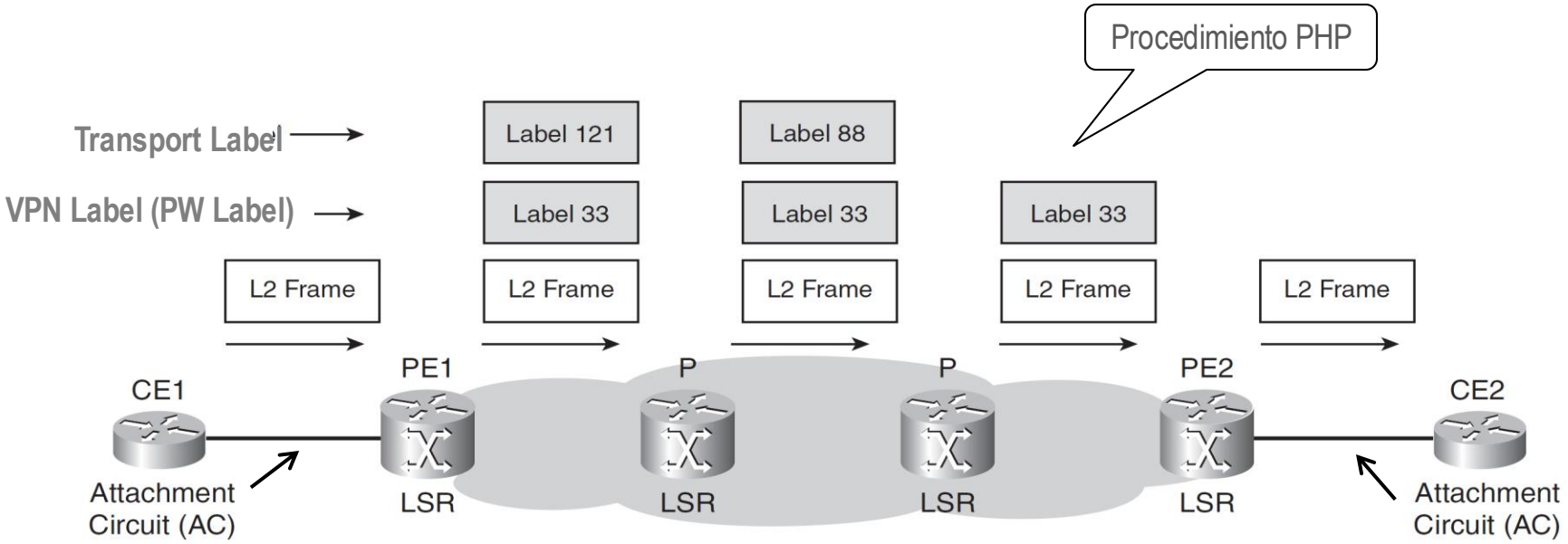
Ejemplo de operativa básica L2VPN-MPLS (II).

- PE2 recibe paquete transportado a través de los túneles lógicos que contienen la trama L2.
- PE2 (PE de egreso):
  - Examina valor de la etiqueta VPN* → Determina que la trama L2 que transporta el paquete debe ser enviada a CE2 a través del enlace de acceso VLAN 200.
  - Si el campo CW está presente (opcional) puede chequear el nº de secuencia.**
  - Regenera la trama L2.
    - Puede incluir la determinación de bits de control de cabecera L2 a partir del campo CW.
    - Reescribe el campo ID-VLAN a un valor 200 (trama L2 recibida contiene ID-VLAN = 100).
  - Reenvía trama L2 a CE2 a través del enlace de acceso VLAN 200.



*: Si el paquete llega vía túnel MPLS y no se utiliza el procedimiento PHP, primero elimina la etiqueta de transporte (*outer label*) para luego valorar la etiqueta VPN.
**: Si el paquete llega fuera de secuencia la lógica asociada puede determinar reordenarlo o descartarlo.

Ejemplo de operativa básica L2VPN-MPLS (III).



Procedimiento PHP (*Penultimate Hop Poping*) entre el último *router* P y el *router* PE de egreso (PE2).

Túnel de transporte establecido puede ser compartido por diferentes tipos de tráfico: L3VPN, L2VPN y VPLS.

Varias formas posibles para establecer **túneles de transporte** entre un par de *routers* PE a través de la red del proveedor:
- Para túneles MPLS mediante LSPs, ídem a L3VPN-MPLS (con CR-LDP o RSVP-TE).
- Para túneles **no** MPLS según procedimiento GRE o IPSec.

L2VPN-MPLS.

- Encapsulado Ethernet (PW-E).
  - Tipo de PW de mayor importancia/relevancia actual.
  - PE de ingreso **elimina** los campos “preámbulo” y FCS de la trama Ethernet.
  - PE de egreso **regenera** los campos “preámbulo” y FCS de la trama Ethernet.

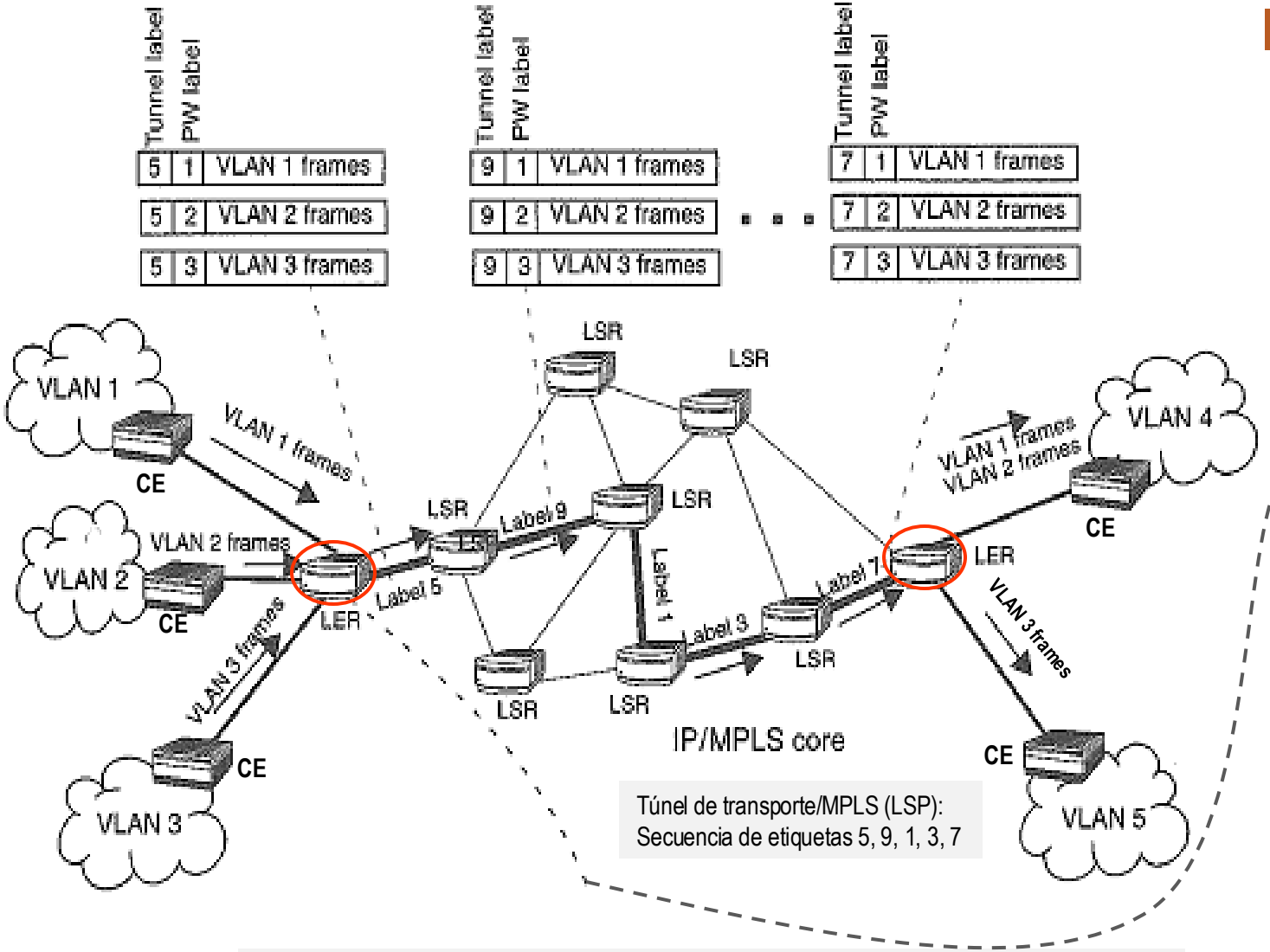
28

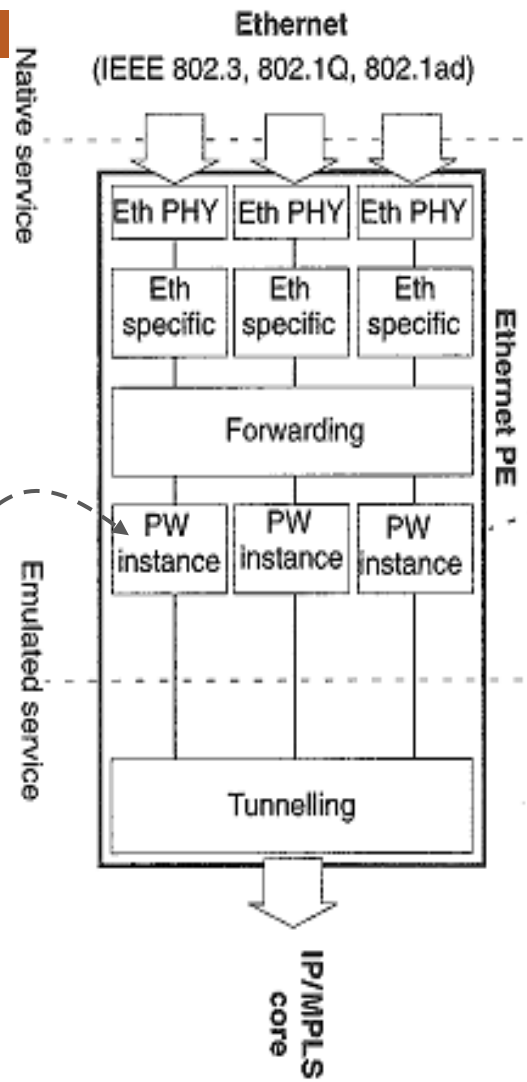
  - Campo CW (*Control Word*) opcional.
    - Menos útil que en ATM y FR.
    - Si se utiliza solo dispone del subcampo “nº de secuencia” de 16 bits, restantes 16 bits a “0”.

9

  - Dos modos especificados para el *mapping* a pseudocables.
    - Modo “por VLAN”.
      - Cada VLAN se “mapea” a un único PW.
      - Si una conexión Ethernet local CE - PE contiene múltiples VLAN, cada una es “mapeada” a un PW diferente para su transporte al correspondiente CE remoto.
    - Modo “por puerto”.
      - Cada puerto Ethernet completo (que puede contener o no múltiples VLAN) se “mapea” a un único PW.

Operación con pseudocables Ethernet (PW-E)





El *router* PE de ingreso actúa como un *bridge Ethernet* con puertos físicos y virtuales.
- Los puertos físicos se conectan a los *routers* CE vía interfaces *Ethernet* estandarizadas.
- Los puertos virtuales son los PW-E "tunelados" a través del *backbone* IP/MPLS.

En la figura:
Routers PE = LER, *Label Edge Router*.
Routers P = LSR, *Label Switching Router*.

Universidad de Alcalá

Fuente: F.J. Hens and J.M. Caballero. *TRIPLE PLAY, building the converged network for IP, VoIP and IPTV,* © John Wiley & Sons. Ltd 2008

L2VPN-MPLS.

- Transporte de capa 2 sobre MPLS, **plano de control**.
  - Plano de control: medio por el cual los *routers* PE se comunican para autodescubrimiento y señalización VPN.
  - Dos enfoques para señalización relativa a pseudocables:
    - Señalización basada en LDP.
    - Señalización basada en BGP.
    - Ambos enfoques presentan características comunes y diferentes.
  - Características **comunes** para LDP y BGP.
    - Asumen PWs punto a punto bidireccionales.
    - Permiten señalizar las características del PW (p.e, valor de la MTU).
    - Proveen notificación de etiquetas VPN.
      - Procedimiento que habilita a los PE de ingreso para conocer el valor de las etiquetas VPN (etiquetas interiores) que “esperan” los correspondientes PE de egreso.
    - Proveen medios a los PE para:
      - Detectar la consistencia o no de la configuración de ambos extremos de un PW.
      - Indicar a los PE remotos problemas de conectividad (p.e, enlace a un CE fuera de servicio).

L2VPN-MPLS.

- ¿Qué servicio VPN elegir sobre MPLS, **L2VPN** o **L3VPN**? Depende de varios factores:
  - Protocolo a ser transportado.
  - Grado de implicación de cliente y proveedor en el *routing* del tráfico.
  - Disponibilidad actual de *routers* para funciones PE.
    - Soporte simultáneo de ambos tipos de servicios, L2VPN y L3VPN.
    - Soporte también para servicios VPLS (*Virtual Private LAN Service*).
  - Disponibilidad actual de proveedores: muchos proveedores ofrecen ambos servicios.

- L2VPN vs L3VPN.

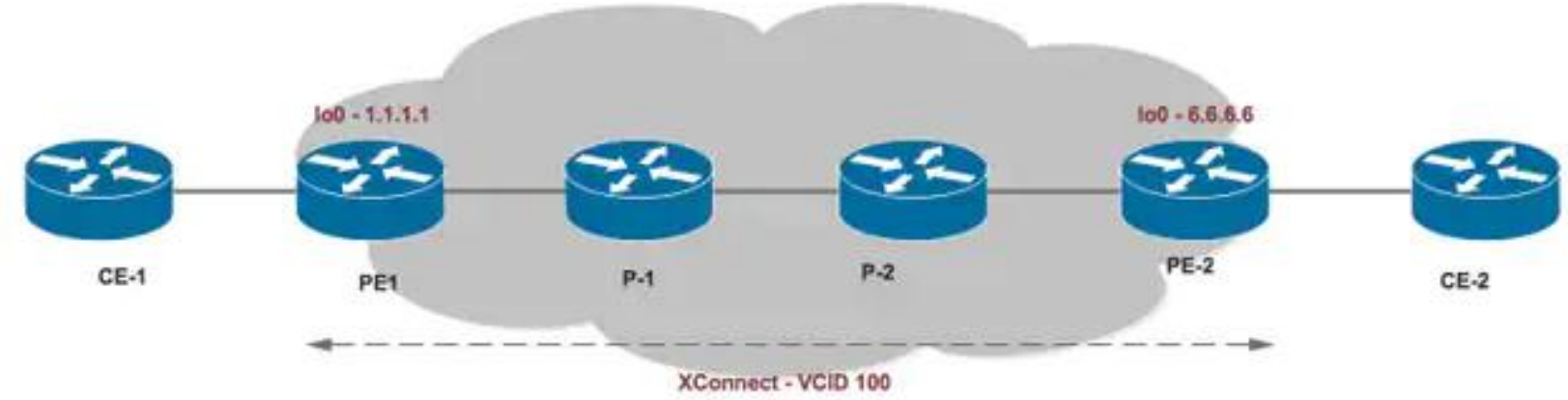
	L2VPN	L3VPN
Nº de conexiones entre CE y PE	Múltiples conexiones (físicas o lógicas) entre cada CE y su correspondiente PE local, una por cada CE remoto con el que se pretenda conexión.	Sólo una conexión entre cada CE y su correspondiente PE local. Cada PE es responsable del *routing* del tráfico hacia el CE de egreso apropiado.
Interacción para *routing* entre cliente y proveedor	No	Si CE y PE tienen que intercambiar información de *routing*.
Protocolo de capa 3 entre las sedes del cliente.	Cualquier protocolo de capa 3 (excepto para L2.5VPN). La red del proveedor sólo se ocupa de transportar las PDU2, no es consciente del protocolo de capa 3.	Se requiere IP. Excluye transporte de protocolos de capa 3 que no sea IP (p.e. IPX, SNA, Apple Talk).

Bibliografía.

- I. Minei and J. Lucek:
  - "*MPLS-Enabled Applications*". John Wiley & Sons, 3rd Ed, 2011.
- L. De Ghein:
  - "*MPLS Fundamentals*". Cisco Press, 2007.
- V. Alwayn:
  - "*Advanced MPLS Design and Implementation*". Cisco Press, 2001.
- F.J. Hens and J.M. Caballero.
  - *"TRIPLE PLAY, building the converged network for IP, VoIP and IPTV"* . John Wiley & Sons, 2008.

PseudowirePacket Analysis

- Topology



  - Ping from PE1 to PE2
    - R1#ping mpls pseudowire 6.6.6.6 100

Overview


```
4 0.203148      1.1.1.1          127.0.0.1          MPLS E…   130 MPLS Echo Request
```

```
Frame 2: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
Ethernet II, Src: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06), Dst: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 0, TTL: 255
MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 1, TTL: 1
PW Associated Channel Header
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
Multiprotocol Label Switching Echo
```

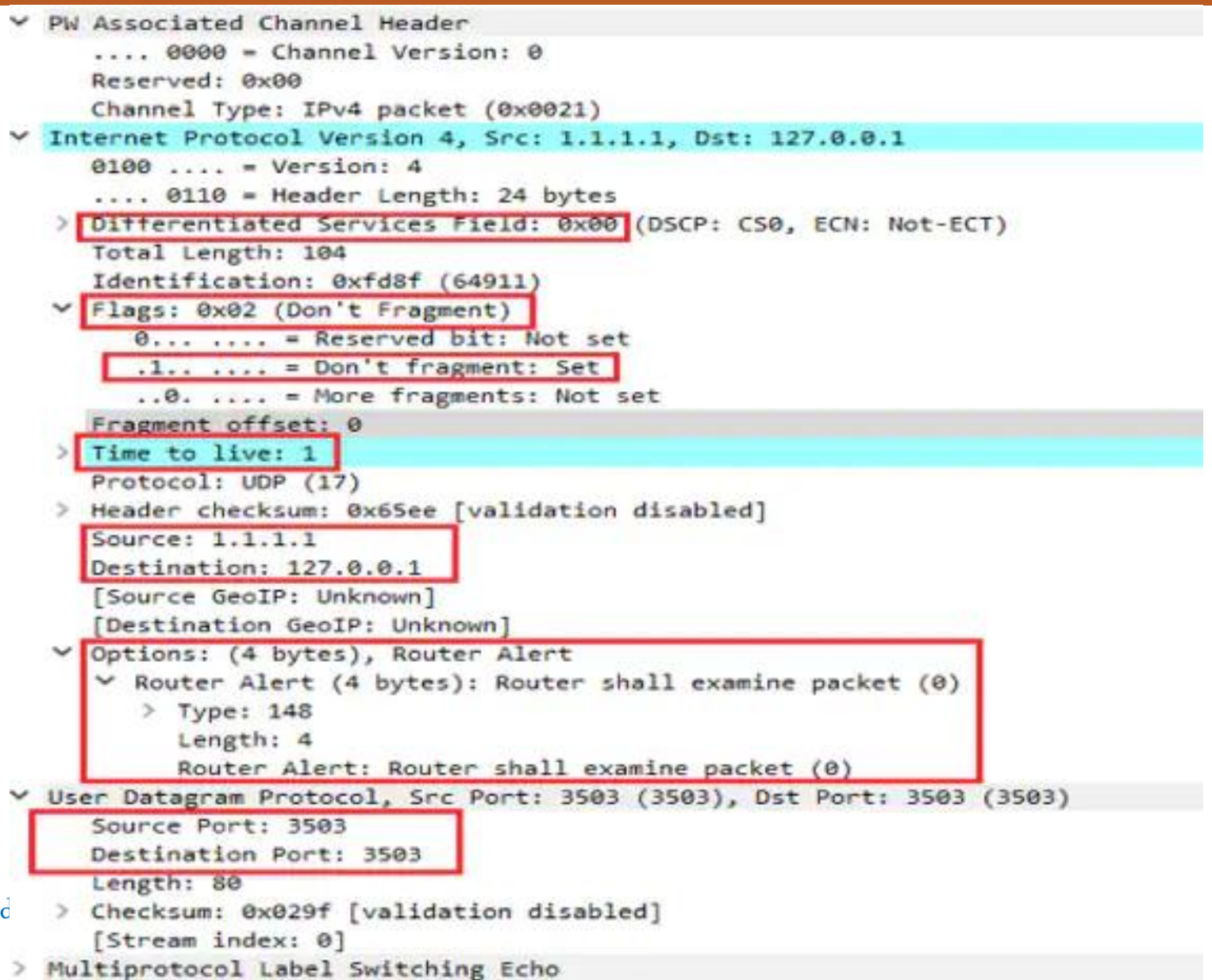
Transport label

VPN label

Layer 2/Labels


```
> Frame 4: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
v Ethernet II, Src: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06), Dst: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Destination: ca:04:13:5c:00:06 (ca:04:13:5c:00:06)
  > Source: ca:01:1b:c0:00:06 (ca:01:1b:c0:00:06)
    Type: MPLS label switched packet (0x8847)
v MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 0, TTL: 255
    0000 0000 0000 0001 1000 .... .... .... = MPLS Label: 24
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
v MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 1, TTL: 1
    0000 0000 0000 0001 1100 .... .... .... = MPLS Label: 28
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 0000 0001 = MPLS TTL: 1
v PW Associated Channel Header
    .... 0000 = Channel Version: 0
    Reserved: 0x00
    Channel Type: IPv4 packet (0x0021)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 3503 (3503), Dst Port: 3503 (3503)
> Multiprotocol Label Switching Echo
```

Layer 3/Layer 4



MPLS payload


```
Multiprotocol Label Switching Echo
    Version: 1
  > Global Flags: 0x0000
    Message Type: MPLS Echo Request (1)
    Reply Mode: Reply via an IPv4/IPv6 UDP packet (2)
    Return Code: No return code (0)
    Return Subcode: 0
    Sender's Handle: 0xc7735d85
    Sequence Number: 284
    Timestamp Sent: Feb  3, 2017 10:41:23.998999000 UTC
    Timestamp Received: Jan  1, 1970 00:00:00.000000000 UTC
  v Vendor Private
      Type: Vendor Private (64512)
      Length: 12
      Vendor Id: ciscoSystems (9)
      Value: 0001000400000004
  v Target FEC Stack
      Type: Target FEC Stack (1)
      Length: 20
    v FEC Element 1: FEC 128 Pseudowire (new)
        Type: FEC 128 Pseudowire (new) (10)
        Length: 14
        Sender's PE Address: 1.1.1.1
        Remote PE Address: 6.6.6.6
        VC ID: 100
        Encapsulation: Ethernet (5)
        MBZ: 0x0000
        Padding: 0000
```



Ingeniería de tráfico

Aplicaciones MPLS: **VPN de capa 2 con MPLS (2ª parte) (MPLS-VPLS)**.

- Introducción. Definición. Utilización. Comparativa con L2VPN.
- Mecanismo de operación. Tipos de CE.
- Mecanismo de operación en el plano de reenvío. Ejemplo.
- Tablas de reenvío. Lógica de los PE.
- Conclusiones.

VPLS: introducción.

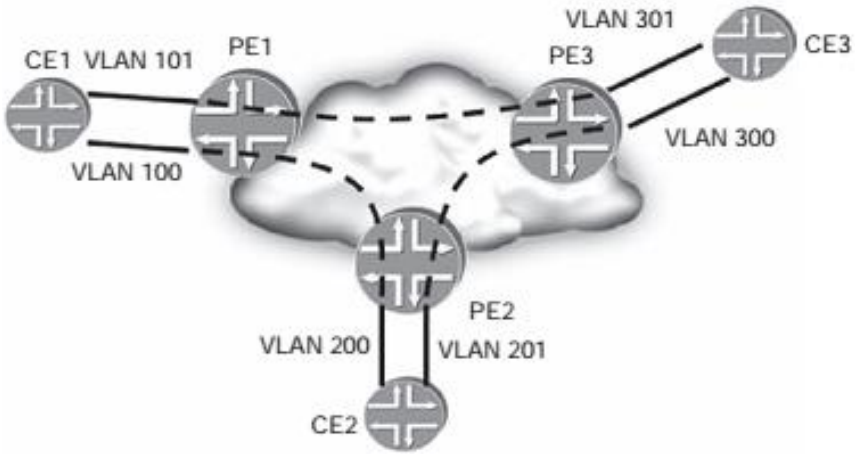
- Factibilidad de las L3VPN y L2VPN.
  - **Sí** para grandes empresas, **suelen disponer de personal técnico apropiado**.
    - L3VPN: cliente se tiene que ocupar del *routing* entre CE y PE con procedimientos estáticos o dinámicos (protocolos de *routing*).
    - L2VPN: cliente debe conformar una red *overlay* con conexiones punto a punto sobre la red del proveedor (pseudocables) y ejecutar un protocolo de *routing* sobre ésta.
    - L2VPN suele requerir personal con mayor nivel de capacitación que L3VPN.
  - **No** para PYMES, **no suelen disponer de personal técnico apropiado**.

VPLS: definición y utilización.

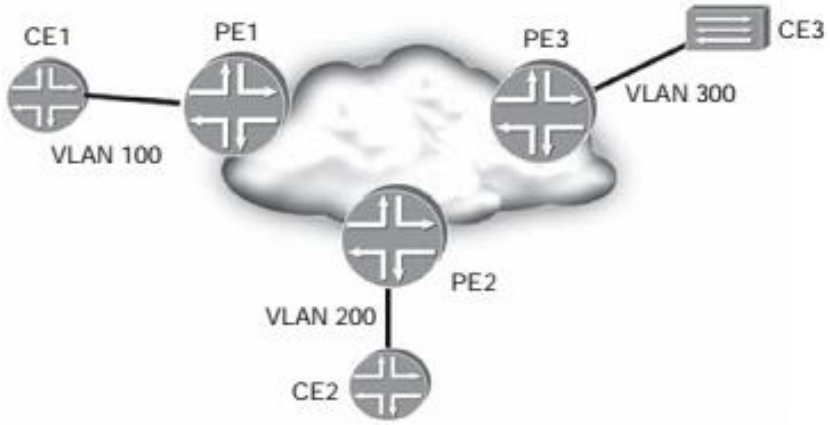
- ***VPLS, Virtual Private LAN Service.***
  - Otro tipo de:
    - Extensión LAN sobre WAN para conectar sedes de un cliente.
    - VPN de capa 2 que admite cualquier protocolo de capa 3.
  - Solución más apropiada para PYMES, requiere personal técnico menos capacitado que las soluciones L2VPN y L3VPN.
  - Especificada en:
    - RFC 4761: *VPLS Using **BGP** for Auto-Discovery and Signaling.*
    - RFC 4762: *VPLS Using **LDP** Signaling.*
  - Definición:
    - Servicio de conexión **multipunto** extendido sobre la red del proveedor (MPLS o IP) .
    - Permite **compartir dominios de difusión Ethernet** entre sitios geográficamente dispersos y conectados a través de **pseudocables** mediante topología ***full mesh.***
    - Reenvío basado en **direcciones de capa 2** (direcciones físicas, direcciones MAC).

VPLS: comparativa con L2VPN.

- VPLS vs L2VPN.



Servicio de conectividad L2VPN.
Servicio punto a punto, para conectividad *full mesh* requiere múltiples interfaces entre cada sede cliente (CE) y proveedor (PE).

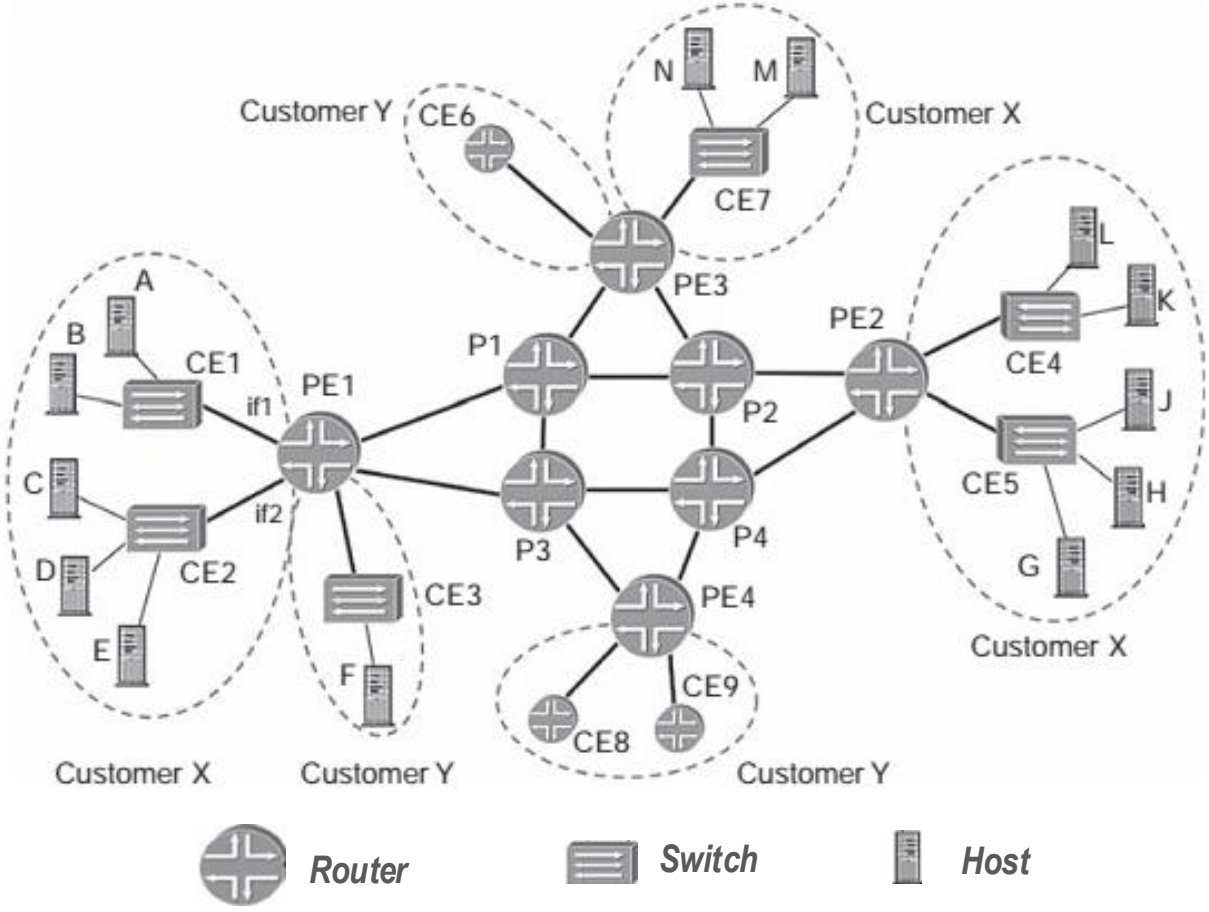


Servicio de conectividad VPLS.
Servicio multipunto, para conectividad *full mesh* requiere sólo una interfaz entre cada sede cliente (CE) y proveedor (PE).

Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

VPLS: mecanismo de operación.

- VPLS, ejemplo genérico.



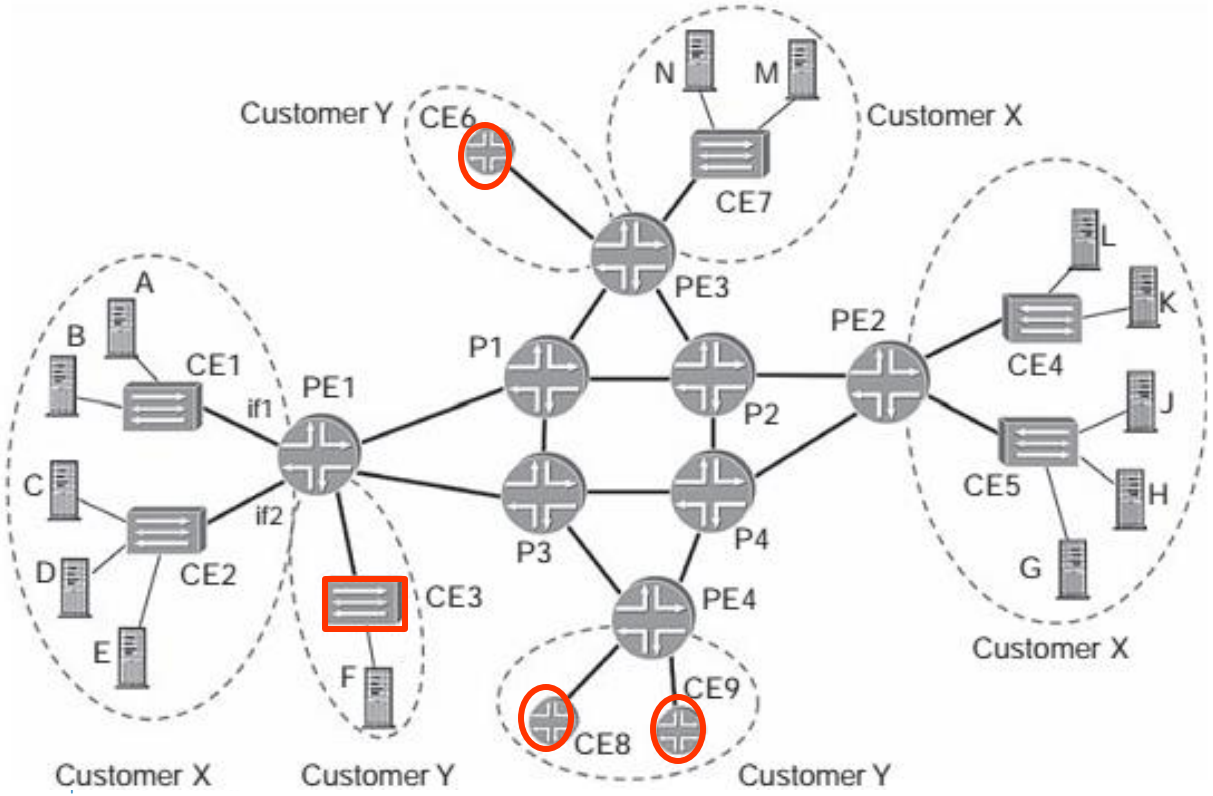
Red del proveedor.
Routers frontera: PE1, PE2, PE3, PE4
Routers del núcleo: P1, P2, P3, P4

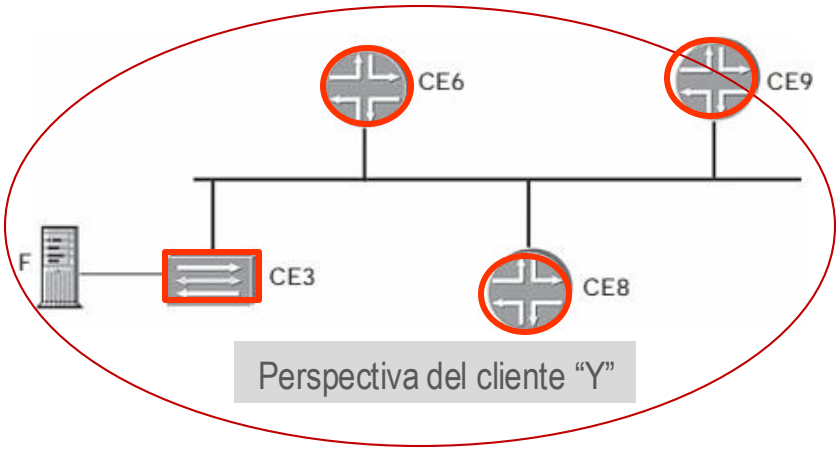
- Dos clientes VPLS, cliente "X" y cliente "Y".
- Cada cliente con tres sedes.
- Tipo de dispositivo para la funcionalidad CE según nº de *hosts* en cada sede.
  - En sedes "X": *switches Ethernet.*
  - En sedes "Y": *routers y switch Ethernet.*
- Cada CE requiere **sólo una conexión Ethernet** al *router* PE del proveedor, consecuencia del servicio multipunto VPLS.
- Los PE de ingreso reenvían PDU2 (tramas) en base a **direcciones MAC** destino.

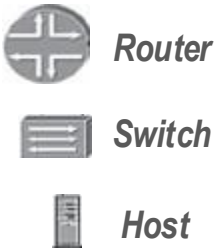
Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

VPLS: mecanismo de operación.

- Mecanismo de operación VPLS.
  - Permite lo básico de toda VPN: conectividad entre sedes remotas de un cliente compartiendo la red del proveedor y con aislamiento de tráfico entre diferentes VPN .
  - Cada cliente percibe la red como una simple LAN de uso exclusivo.
  - P.e, la perspectiva del **cliente "Y"** es la que refleja la figura de la derecha.



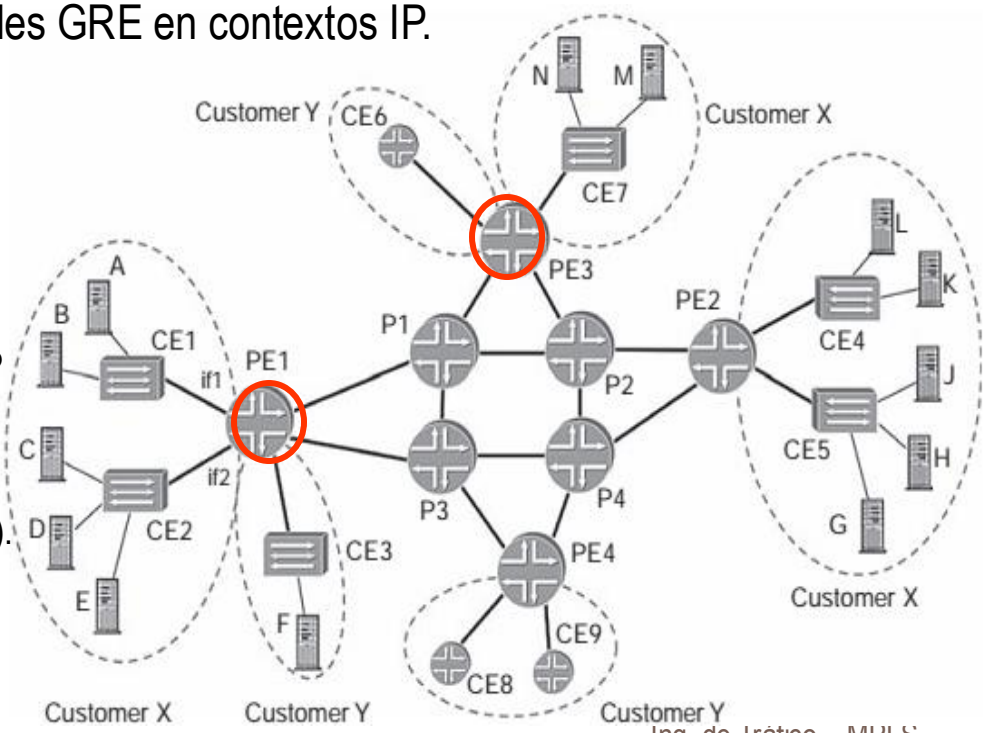




VPLS: mecanismo de operación.

- Mecanismo de operación VPLS (II).
  - Requiere pseudocables (PW) que conecten en modo ***full mesh*** los PE de cada VPLS.
    - Cada VPLS con sus propios PW.
    - PE de egreso identifica la VPLS a la que pertenece una trama - PDU2 según **etiqueta de PW**.
  - Requiere túneles de transporte entre los PE de ingreso y egreso para el tráfico VPLS vía PW.
    - Mediante LSP en contextos MPLS (túneles MPLS) y señalización CR-LDP o RSVP-TE.
    - Otras alternativas mediante túneles IPSec o túneles GRE en contextos IP.

- Ejemplo.
  - Para conectividad entre PE1 y PE3 se requieren dos PW:
    - Un PW para tráfico VPLS del cliente "X".
    - Un PW para tráfico VPLS del cliente "Y".
  - ¿Cómo procede PE1 para enviar a PE3 tráfico del cliente "X"?
    - Identifica la etiqueta de PW según VPLS que corresponda.
    - Añade la **etiqueta de PW** a la trama Ethernet.
    - Añade la 1ª **etiqueta de transporte** MPLS (LSP, túnel de transporte).



VPLS: mecanismo de operación.

- Mecanismo de operación VPLS (III).
  - ¿Cómo conoce cada PE los otros PE miembros de la misma VPLS con los que debe establecer pseudocables?
    - Mediante procedimiento similar al utilizado en las L2VPN: **señalización LDP o BGP**.
  - Reenvío de tramas Ethernet por los *routers* PE†:
    - A partir de la dirección MAC destino que porta cada trama.
    - *Host* destino puede ser alcanzado vía PE remoto o vía otro puerto del mismo PE origen.
    - Si *host* destino se alcanza vía PE remoto → PE de ingreso reenvía la trama por el PW apropiado (requiere conocer cuál es el PE de egreso).
  - Los PE utilizan "auto aprendizaje" de direcciones MAC.
    - Para conocer a qué *router* PE está asociada determinada dirección MAC.
    - Observan la dirección MAC origen de toda trama recibida por cada puerto local o no local (PW).
    - Para cada **nueva** direc. MAC origen crean una entrada en la tabla de reenvío de tramas que gestiona.
    - Resultado: los PE no requieren mecanismo explícito para notificar/aprender las direcciones MAC.

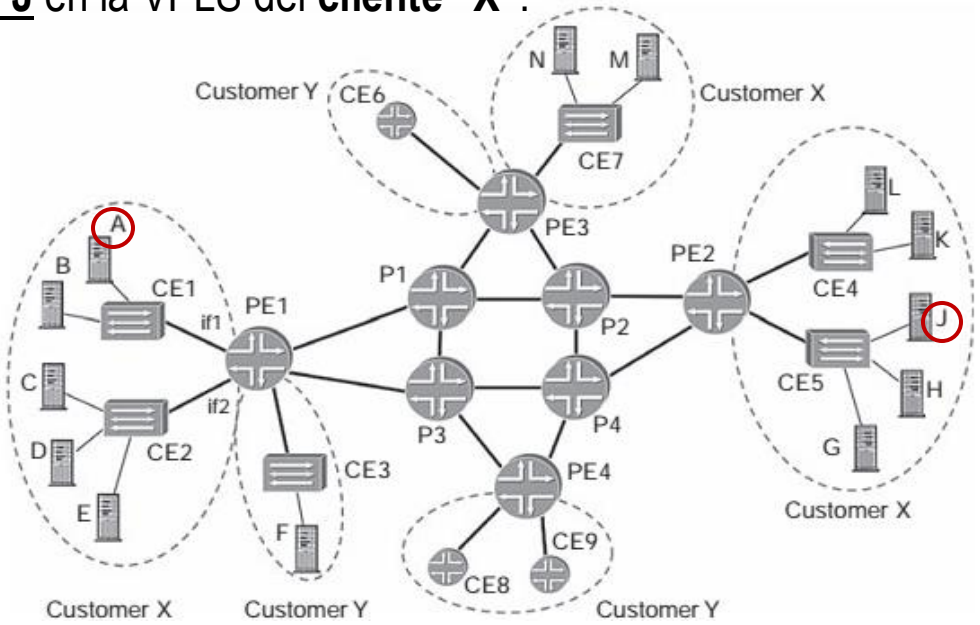
† En L2VPN, el PE de ingreso seleccionaba el PE de egreso basándose en el identificador de la VLAN de la trama entrante.

VPLS: tipos de CE.

- Tipos de dispositivos CE y efecto en los *routers* PE.
  - Los PE necesitan:
    - Aprender las direcciones MAC de los *hosts* alcanzables a su través.
    - Una entrada en la tabla de reenvío para cada dirección MAC individual.
  - Las direcciones MAC no tienen una estructura jerárquica, no pueden ser resumidas.
    - Para evitar problemas de escalabilidad hay que limitar el tamaño de las tablas de reenvío.
  - **CE con *switches***.
    - Los PE tienen que aprender las direcciones MAC de **todos** los *hosts* conectados a los *switches.*
    - Solución recomendable para sedes con pocos *hosts*.
  - **CE con *routers***.
    - "Ocultan" las direcciones MAC de los *hosts*.
    - Los PE tienen que aprender solo las direcciones MAC de los CE locales conectados.
    - Solución recomendable para sedes con muchos *hosts*.

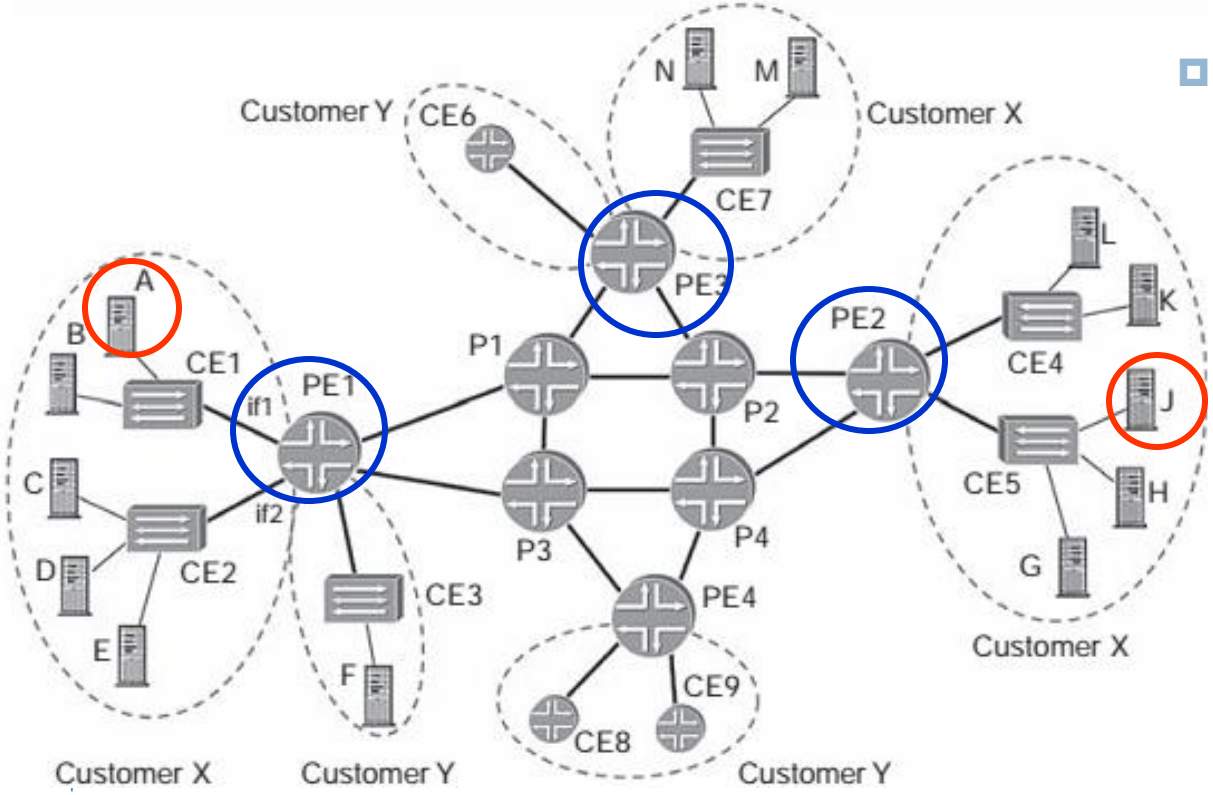
VPLS: plano de reenvío.

- Mecanismos en el plano de reenvío VPLS.
  - Requerimientos.
    - Todos los PE de una VPLS tienen que estar conectados mediante PWs con topología ***full mesh***.
    - Cada PE debe gestionar una ***Frame Forwarding Table*** **(FFT)** por cada VPLS.
    - Cada PE debe aplicar la regla ***split horizon*** → **No reenvío de tramas entre PW de la misma VPLS.**
      - Permite no tener que ejecutar en los PE algoritmos para evitar la formación de bucles.
      - Cada VPLS es un dominio de difusión Ethernet.
  - Ejemplo.
    - Envío de tramas *unicast* desde el *host* **A** al *host* **J** en la VPLS del **cliente "X"**.
      - Dirección MAC del *host* A = MAC A.
      - Dirección MAC del *host* J = MAC J.
    - Ver a continuación.



VPLS: plano de reenvío.

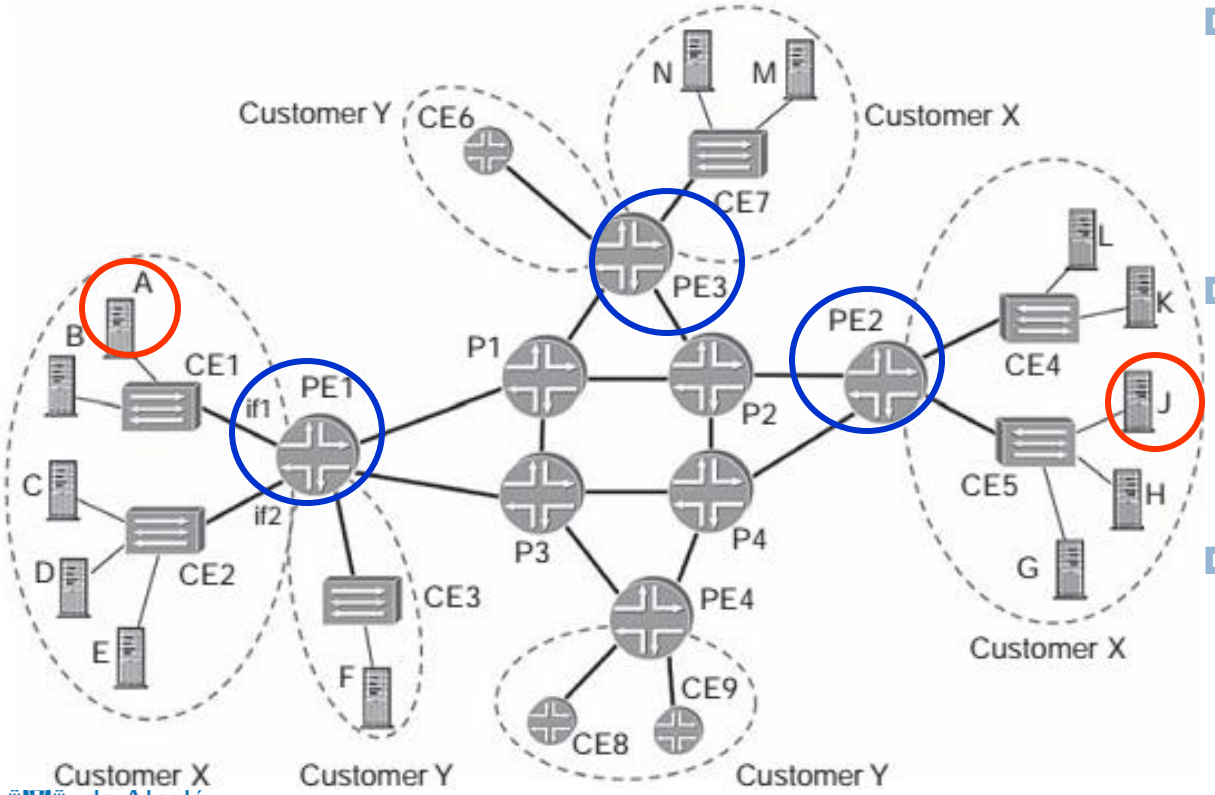
- Ejemplo de reenvío *unicast*.
  - Inicio del proceso, **A** envía trama con MAC_fuente=A y MAC_destino=J.
  - Supuesto: tabla de reenvío VPLS-X en PE1 no tiene aún entrada para el *host* J.
  - PE1 reenvía la trama por todos sus puertos excepto por el que la recibió (inundación).
    - Puerto local hacia CE2 (**if2**) y pseudocables hacia PE2 y PE3.



- PE2 y PE3:
  - Identifican la trama como perteneciente a la VPLS-X a partir del PW por donde arribe.
  - Buscan en sus respectivas FFT-X y no encuentran entrada para la MAC J, por lo que retransmiten mediante inundación:
    - PE2 por los dos puertos locales hacia CE4 y CE5, no a otros PE (regla ***split horizon***).
    - PE3 por el puerto local hacia CE7, no al puerto local hacia CE6 (VPLS-Y) ni a otros PE (regla ***split horizon***).

VPLS: plano de reenvío.

- Ejemplo de reenvío *unicast* (II).
  - **Aprendizaje**: con la recepción de una trama cada PE actualiza la FFT correspondiente si es necesario. En consecuencia:
    - PE1, PE2 y PE3 añaden una entrada a sus FFT-X cuando reciben la trama con MAC_fuente=A.
      - Entrada en la FFT-X que identifica el puerto a través del cual el PE puede alcanzar el *host* A.



- PE1.
  - Añade asociación "MAC A – CE1(if1)".

MAC address	Next hop
A	if1

- PE2.
  - Añade asociación "MAC A – PW_PE1".

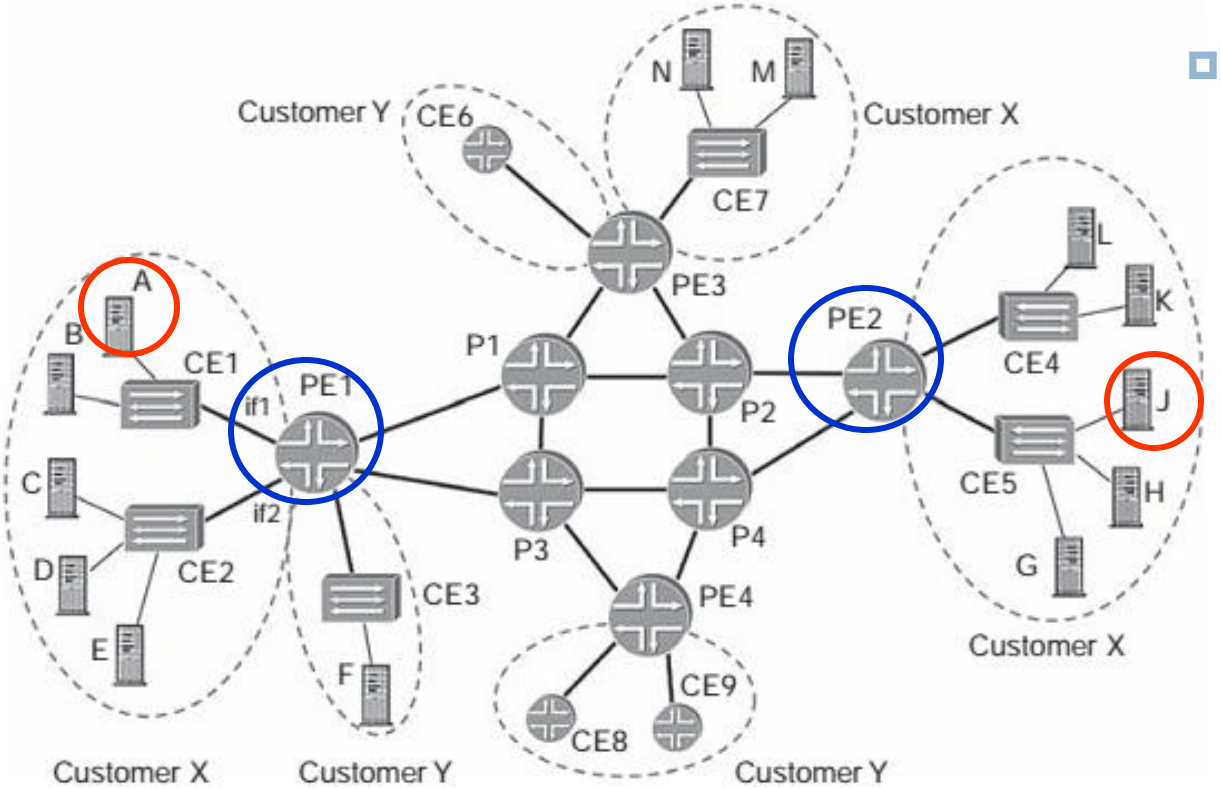
MAC address	Next hop
A	PW_PE1

- PE3.
  - Añade asociación "MAC A – PW_PE1"

MAC address	Next hop
A	PW_PE1

VPLS: plano de reenvío.

- Ejemplo de reenvío *unicast* (III).
  - ***Host* J** envía trama al ***host* A** (p.e, como respuesta a la trama antes recibida).
  - PE2 tiene en su FFT-X la entrada que apunta al *host* A a través del pseudocable PW_PE1.
    - No requiere inundación (aprendizaje previo), reenvía la trama solo por el pseudocable PW_PE1.



- PE1.
  - Recibe trama con destino A y origen J, "aprende" cómo alcanzar el *host* J y añade entrada a su FFT-X.

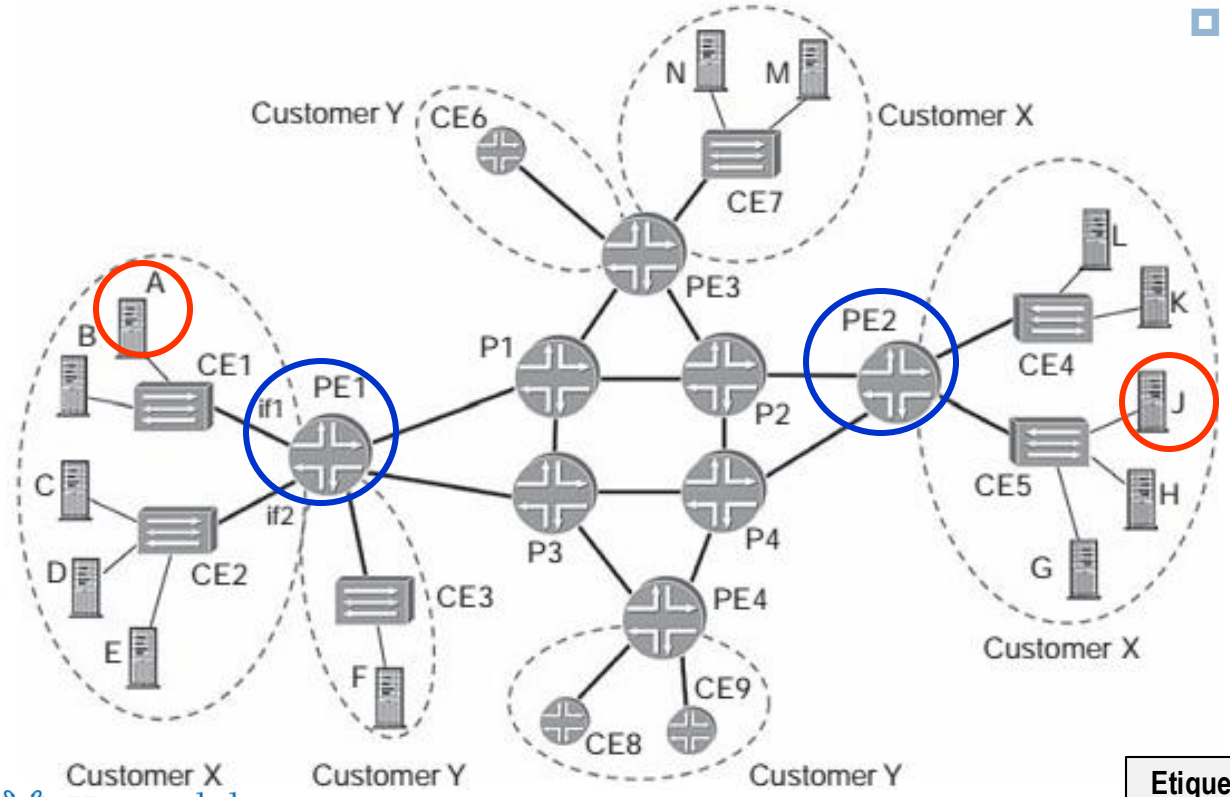
MAC address	Next hop
J	PW_PE2

  - Reenvía la trama hacia el *host* A vía "if1" y CE1 a partir de la entrada que ya tiene en su FFT-X para el *host* A.

MAC address	Next hop
A	if1

VPLS: plano de reenvío.

- Ejemplo de reenvío *unicast* (IV).
  - Como resultado del primer envío de tramas entre los *hosts* A y J se produce el "aprendizaje" indicado → Las FFT-X en PE1 y PE2 disponen ya de entradas para los *hosts* A y J.
    - Siguientes tramas entre los *hosts* A o J no requiere reenvío con "inundación".



- FFT-X de **PE1** al cabo de un tiempo.

MAC address	Next hop
A	if1
B	if1
C	if2
D	if2
E	if2
G	PW: 200, T: 410
H	PW: 200, T: 410
J	PW: 200, T: 410
K	PW: 200, T: 410
L	PW: 200, T: 410
M	PW: 300, T: 235
N	PW: 300, T: 235

Etiqueta de pseudocable (*inner label*)

Etiqueta de transporte/túnel (*outer label*)

VPLS: tablas de reenvío.

- Contenido y gestión de las **tablas FFT** en cada PE.
  - Entradas para accesos locales (CE).
    - Dirección MAC – puerto (interfaz).
  - Entradas para accesos remotos (PE).
    - Dirección MAC - etiqueta de PW - etiqueta de transporte.
  - Se actualizan mediante auto aprendizaje, no por mecanismo alguno de señalización explícita para traducción/notificación de direcciones MAC.
  - Para limitar el crecimiento indiscriminado de su tamaño, se eliminan entradas no utilizadas durante cierto tiempo.

VPLS: lógica en los PE.

- Cada PE cuando recibe una trama Ethernet procede de la siguiente manera:
  - Busca en la FFT que corresponda **según puerto por donde arribe** la trama (cada PE gestiona una FFT por cada VPLS).
  - Si encuentra entrada coincidente:
    - Para acceso remoto → Añade a la trama las **etiquetas** de PW y de transporte, y la reenvía por el puerto que corresponda para alcanzar el PE remoto.
    - Para acceso local → Retransmite la trama **sin etiquetar** por el puerto local que corresponda.
  - Si no encuentra entrada coincidente → Retrasmite la trama mediante inundación.
    - Retransmite por "todos" los puertos excepto por donde recibió la trama.

- Túneles para el soporte de PW entre *routers* PE.
  - Túneles de transporte **tipo LSP** para el caso de proveedor MPLS.
  - Otras alternativas para túneles de transporte para proveedor IP: tipo IPSec o tipo GRE.
  - Un túnel de transporte puede ser compartido por diferentes PW y diferentes servicios.

GRE (*Generic Routing Encapsulation*): protocolo para transporte de diferentes PDU_3 mediante "tunelado" lógico a través de Internet. RFC 1701 y 1702.

VPLS: conclusiones.

- VPLS, conclusiones.
  - Proveen servicio Ethernet multipunto. Desde una perspectiva de alto nivel:
    - *Backbone* MPLS del proveedor **emula un gran *switch* Ethernet** que conecta los CE de las diferentes sedes de un cliente.
  - *Mapping* a PW mediante inundación o según aprendizaje previo de direcciones MAC.
    - Tablas de reenvío en los PE por direcciones MAC, puertos y etiquetas (de PW y de transporte).
  - Plano de reenvío.
    - Extremo emisor del PW → Encapsulado de las PDU2 mediante etiquetados de **PW** y de **transporte**.
    - Extremo receptor del PW → Des encapsulado, eliminación de etiquetas y reenvió de las PDU2.
  - Plano de control/señalización VPN.
    - Para PW: LDP o BGP, ídem a los procedimientos utilizados en L2VPN.
    - Para el transporte (LSP): CR-LDP o RSVP-TE.
  - Solución flexible, fiable y eficiente, pero **no escalable a medida que crece el nº de clientes**.
    - Consecuencia de la topología ***full mesh*** para los PW de una VPLS.
      - Nº total de PW para "N" *routers* PE = **N(N-1)/2** → P.e, si N = 60, 1770 PW.
    - Excesiva replicación de paquetes y excesiva señalización VPN mediante LDP o BGP.

VPLS y TE con MPLS: bibliografía.

- I. Minei and J. Lucek:
  - "*MPLS-Enabled Applications*". John Wiley & Sons, 3rd Ed, 2011.
- H. Jonathan Chao and Xiaolei Guo:
  - *Quality of Serice Control in High-Speed Networks*. 2002 John Wiley & Sons, Inc.
- L. De Ghein:
  - "*MPLS Fundamentals*". Cisco Press, 2007.
- V. Alwayn:
  - "*Advanced MPLS Design and Implementation*". Cisco Press, 2001.