# MPLS/VPN

## Multiprotocol Label Switching/Virtual Private Networks

# ¿Qué es una VPN?

- En general, una estructura de red que permite traficar información privada sobre una infraestructura de red pública
- El concepto de VPN no es nuevo
- VPNs basadas en MPLS: diseñadas para resolver muchos de los problemas de las que hoy llamaríamos “legacy VPNs”
- VPNs: uno de los motores para el despliegue de MPLS

# Evolución de las VPNs (1)

- Inicialmente:
  - Líneas Dial-up
  - Enlaces dedicados (enlaces privados con la TELCO o Proveedor de servicios)
- Ventajas:
  - Buena seguridad
  - Garantías respecto a la capacidad (100% comprometida)
- Desventajas:
  - Mala relación costo-eficiencia
  - Uso ineficiente de ancho de banda
- Alternativas: esquemas que permitan al proveedor realizar multiplexado estadístico. Más baratos y eficientes

# Evolución de las VPNs (2)

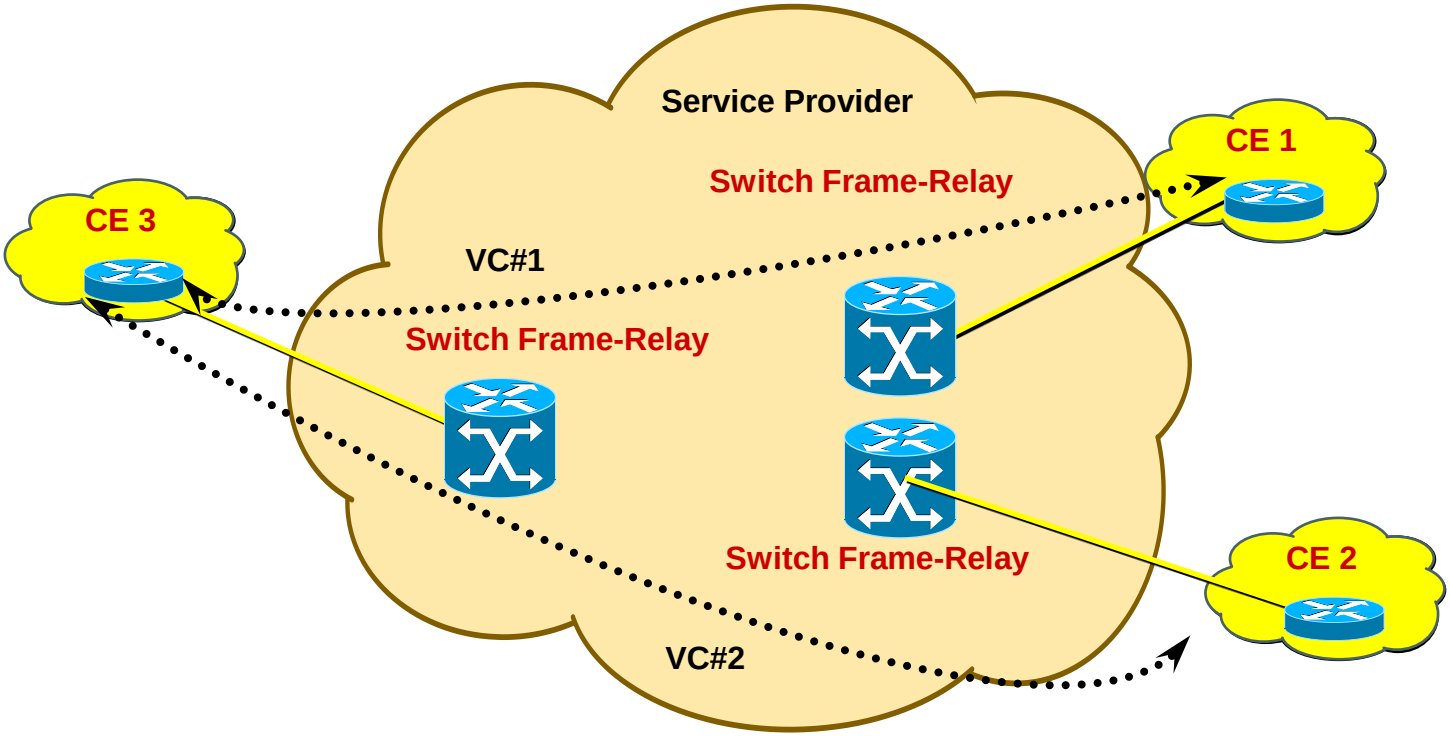
- Redes sobre tecnologías de circuitos virtuales: X.25, Frame-Relay, ATM
- Surgen dos paradigmas:

VPNs OVERLAY: emulación de línea dedicada, a través de un Circuito Virtual (VC)

- Tengo dos topologías, la que ve el proveedor (circuitos FR por ejemplo), y la que ve el cliente (por ejemplo IP)

VPNs Peer-to-Peer: intento de solucionar algunos problemas de las redes Overlay

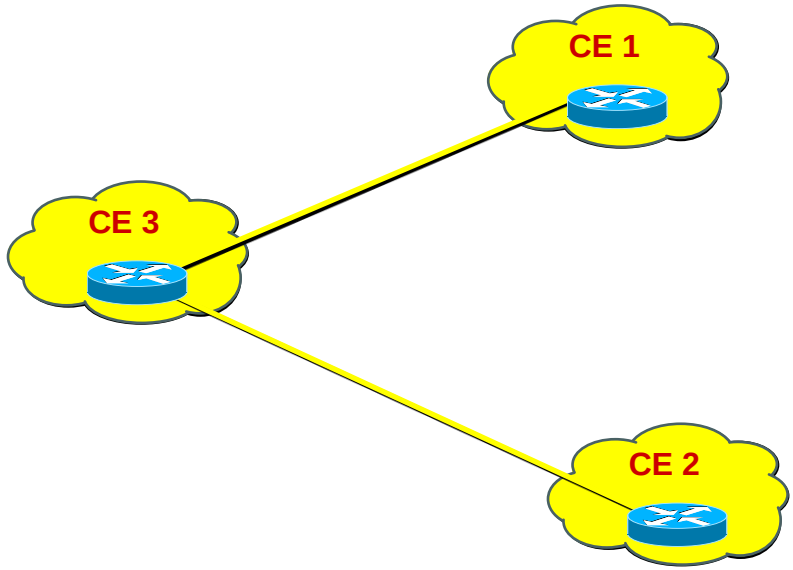
# VPNs OVERLAY (1)




**CE: enrutador del cliente**

# VPNs OVERLAY (2)

- El Proveedor de Servicios desconoce la estructura interna de red del cliente
- Enrutamiento IP en una VPN del tipo overlay: lo resuelve el cliente, es transparente para el Proveedor



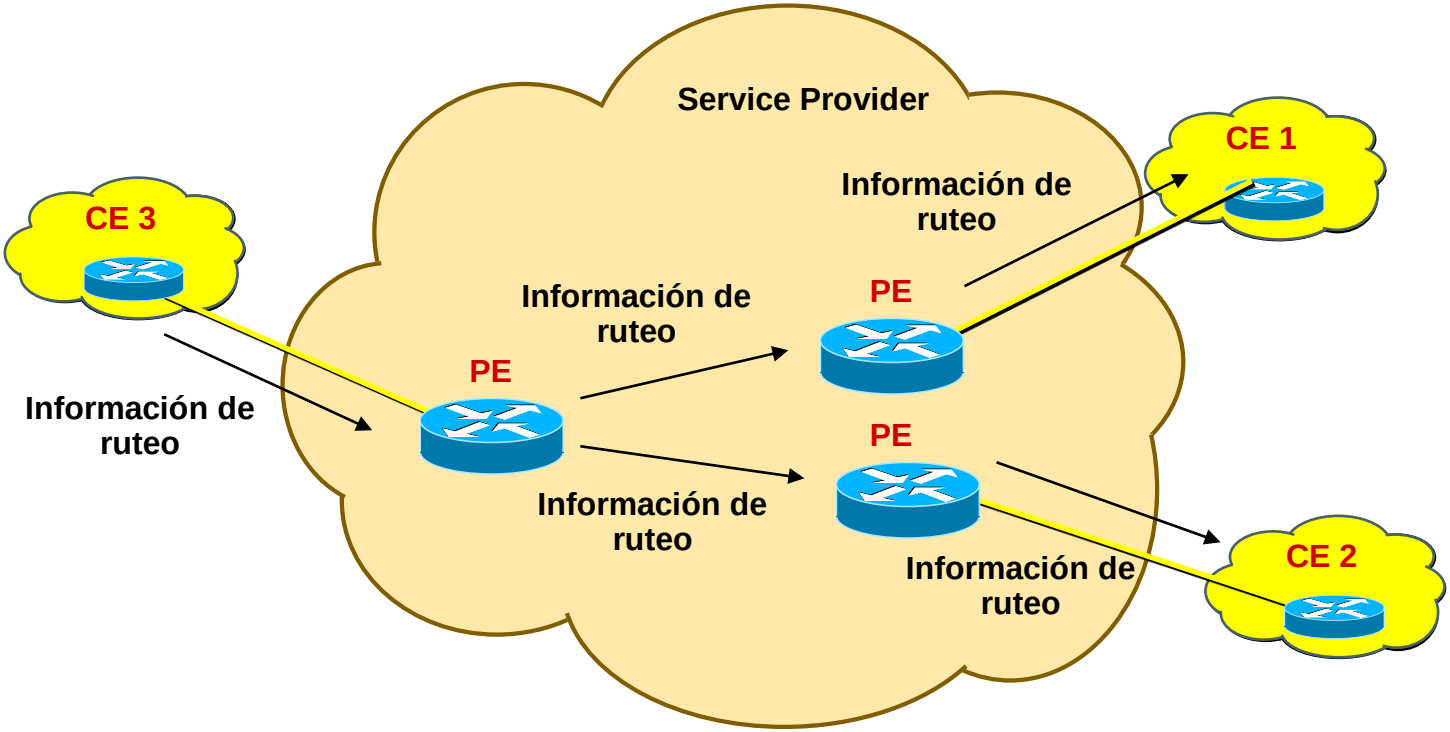
# VPNs OVERLAY (3)

- Ventajas:
  - Simples. Presentan clara separación entre entre el Proveedor y el cliente
  - Protocolos utilizados por el cliente no dependen del soporte del proveedor
- Desventajas:
  - Optimización del enrutamiento exige full mesh
  - Escalabilidad
  - Complica agregar nuevos sitios a la red
  - Mayores costos y complejidad para el proveedor
- Alternativas overlay: túneles IP-IP como GRE o IPSec

# VPNs Peer-to-Peer (1)

- En este modelo la red del proveedor intercambia información de ruteo directamente con los enrutadores del cliente
- Ventajas:
  - Ahora cada CE (enrutador del cliente) intercambia información con un único (o unos pocos) PE (enrutador del proveedor)
  - Cada PE solo debe conocer información de las VPNs que tiene conectadas
  - Ruteo óptimo entre CE
  - Más sencillo de dimensionar en ancho de banda
  - Se hace fácil agregar nuevos sitios a la VPN

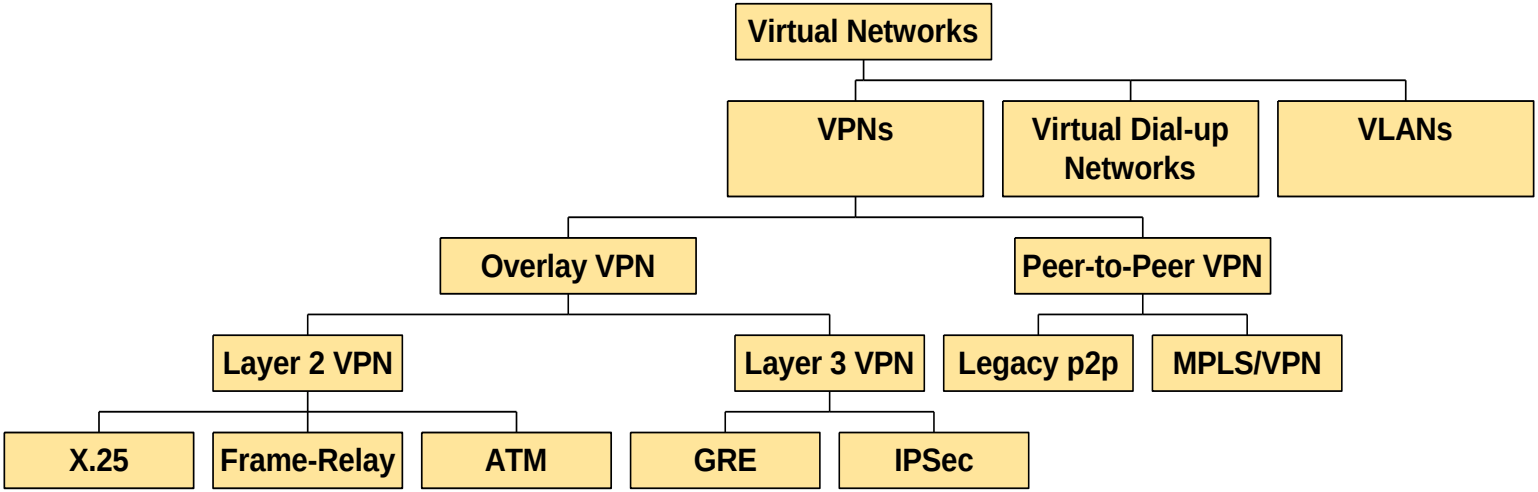
# VPNs Peer-to-Peer (2)



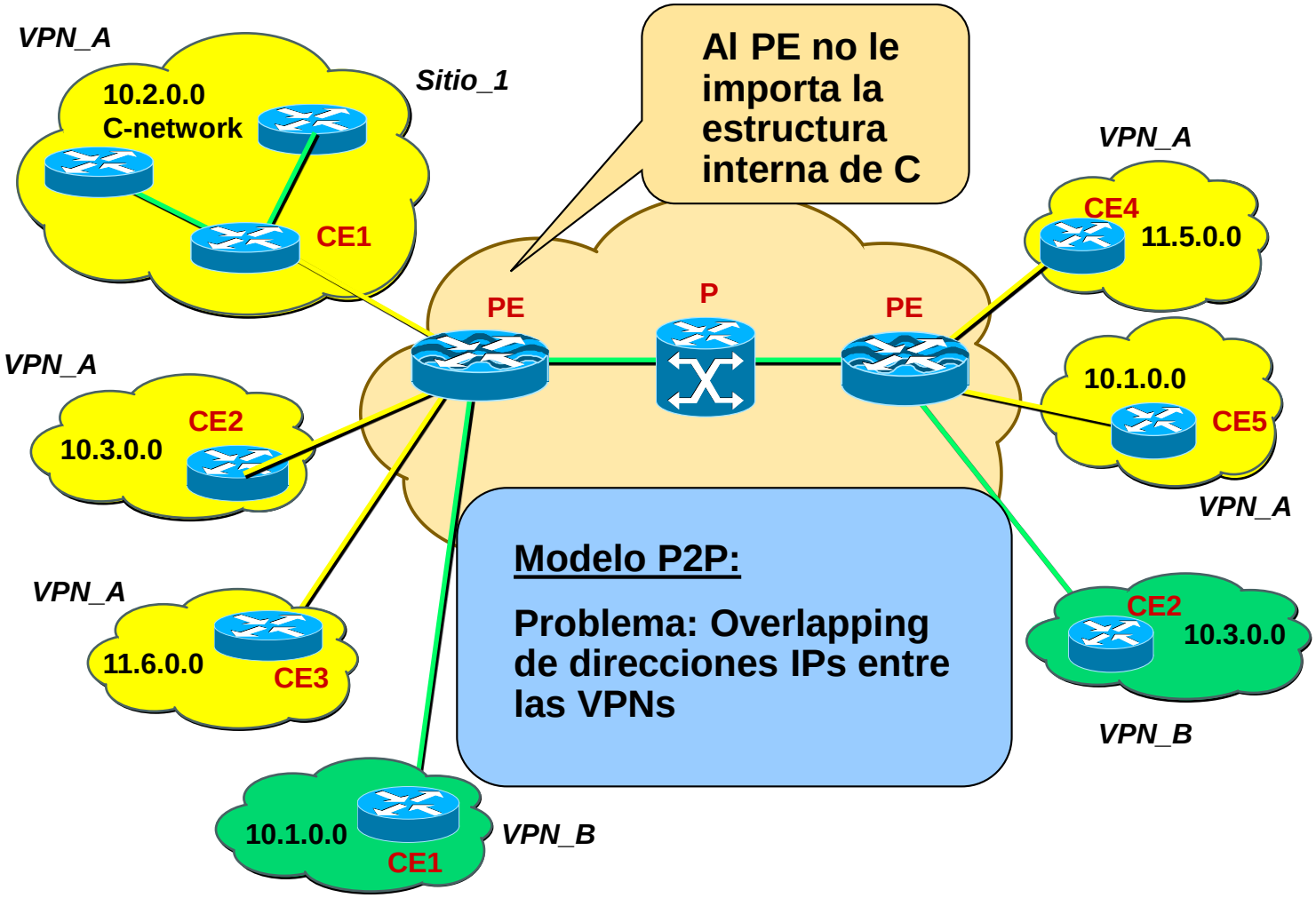
# VPNs Peer-to-Peer (3)

- Desventajas de las primeras VPNs Peer to peer:
  - Un único espacio de direccionamiento IP, es decir no se pueden duplicar IPs (RFC 1918). El proveedor debe tener un plan de numeración IP para las VPN de los clientes
  - Perdemos la seguridad y aislación que aparecía en las lineas dedicadas y el modelo overlay
  - Puede estar limitada la elección de protocolos enrutados
- Solución: VPNs basadas en MPLS
  - Combina los beneficios y sencillez de las redes Peer-to-Peer con las garantías de las redes overlay
  - No exige un único espacio de direccionamiento IP

# Clasificación de VPNs



# Ejemplo de SP y sus clientes (1)



# Ejemplo de SP y sus clientes (2)

- Problemas de las primeras VPNs overlay:
  - No puedo tener dos clientes que utilicen las mismas direcciones
  - Tengo que impedir que equipos de una VPN puedan enviar paquetes a otras VPNs
  - Tengo que impedir que una VPN conozca rutas de otras VPNs
- Estos problemas hicieron que no se popularizaran, para el cliente obligaban a renumerar, para el proveedor implicaba configuraciones complejas

# 2 problemas a resolver

- Mantener (y propagar) información de ruteo separada para cada VPN
- Mantener los paquetes dentro de cada VPN
- Ambas de forma escalable y sin configuraciones complejas para el proveedor

# Solución con MPLS y BGP

- Describiremos la solución de la RFC 2547 Bis

  Actualizada en RFC 4364
- Esta solución es exclusivamente para IP
- Tendremos tablas de enrutamiento independientes para cada VPN
  - Cada cliente perteneciente a una VPN tendrá acceso sólo al conjunto de rutas contenidas en esas tablas
  - La información de estas tablas se propagará utilizando extensiones a BGP
- Utilizaremos etiquetas MPLS para separar el tráfico de las distintas VPNs

# Terminología MPLS-VPN (1)

- Provider Network (P-Network):

  Red del proveedor

- Customer Network (C-Network):

  Red bajo control del cliente

- Enrutador PE:

  Provider Edge router. Enrutador de borde del proveedor. Equipo del proveedor que tiene clientes conectados. Procesan todo lo referente a VPNs

- **Enrutador P:**

  Provider (core) router. Enrutador interno (sin clientes conectados), no conocen las VPNs

# Terminología MPLS-VPN (2)

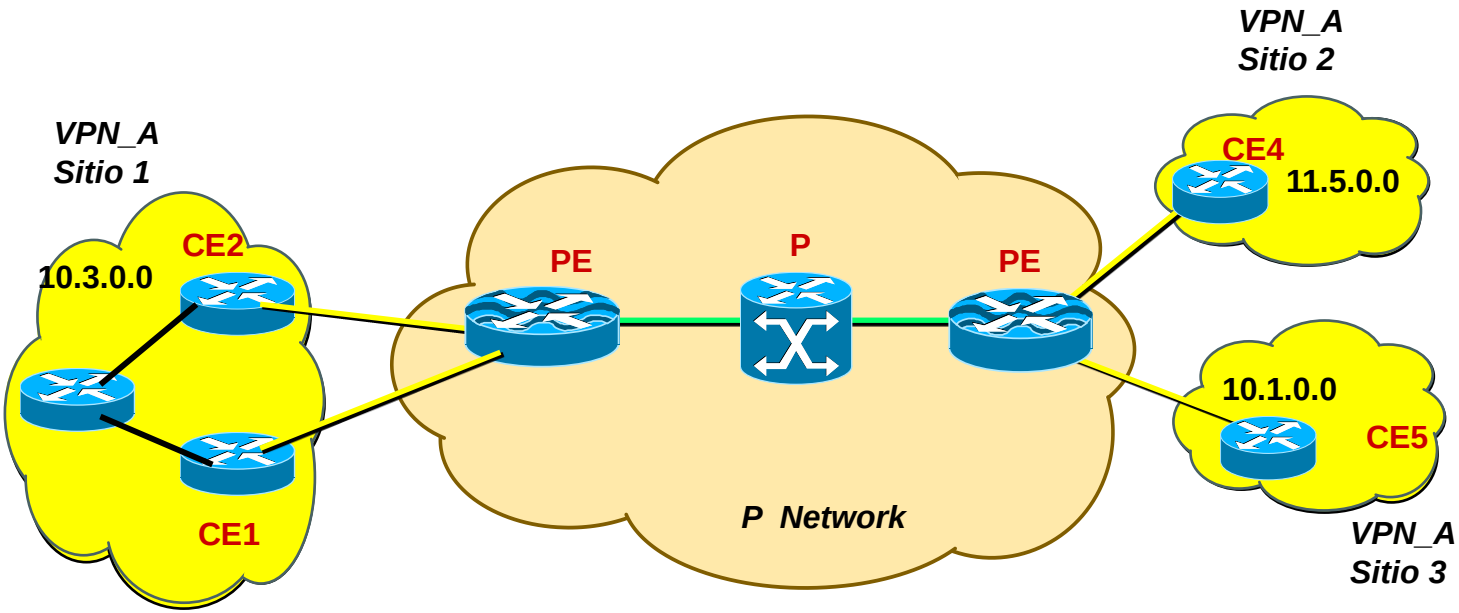
- Enrutador CE:

  Customer Edge router. Equipo que conecta el cliente a los routers PE. No precisa conocer MPLS

- Sitio:

  Conjunto de redes de un cliente que se conecta a la red del proveedor a través de uno o más links CE/PE

# Ejemplo

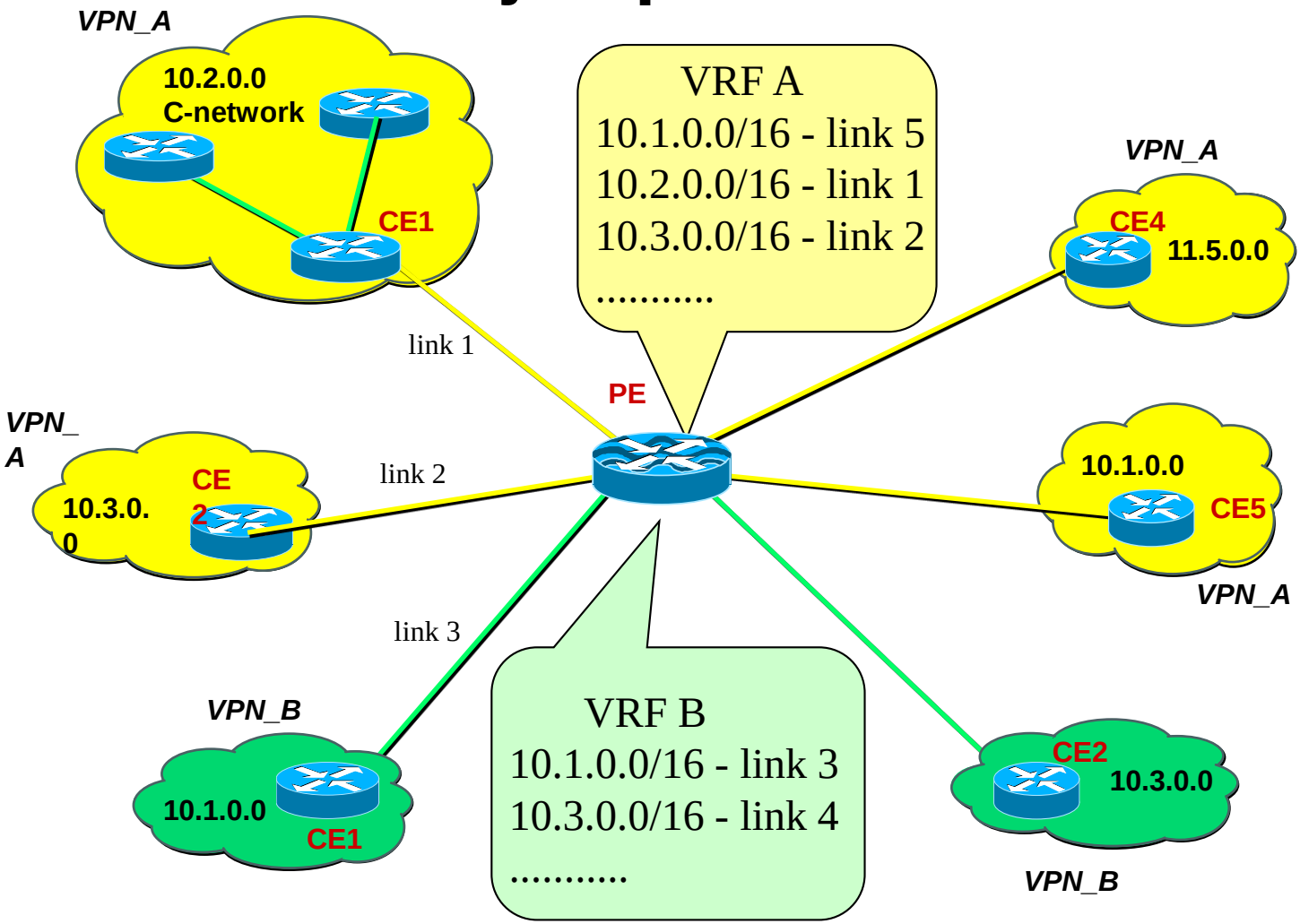

VPN_A
Sitio 1
CE2
10.3.0.0
CE1
PE
P
PE
P Network
VPN_A
Sitio 2
CE4
11.5.0.0
10.1.0.0
CE5
VPN_A
Sitio 3

# VRF
# (virtual routing and forwarding)

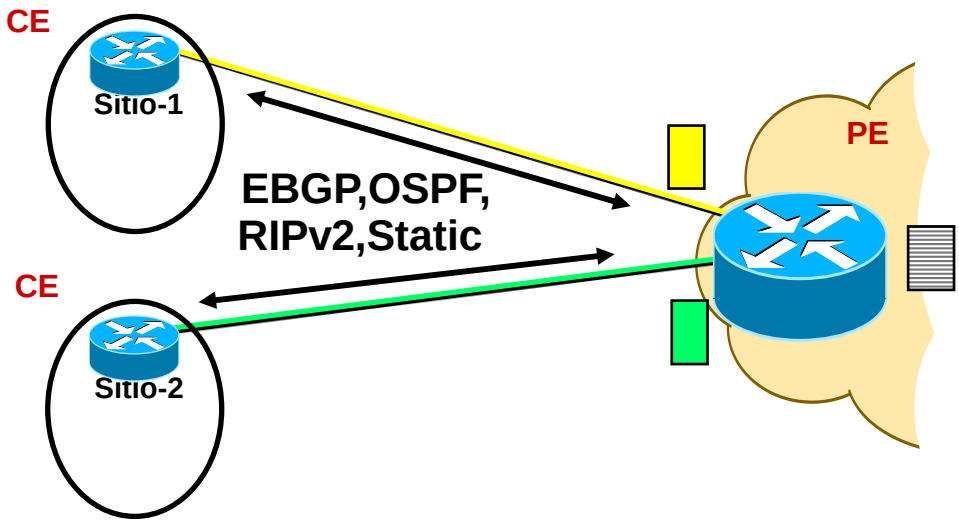
- Objetivo: destinar recursos exclusivos para un conjunto de rutas e interfases

  Por ejemplo, todos los puntos de una vpn
- Cada enrutador PE debe ser capaz de mantener una tabla de rutas PARA CADA CLIENTE
- A estas tablas se les llama VRF(VPN Routing and Forwarding o Virtual Routing and Forwarding)
- Por lo tanto, cada enrutador PE tendrá tantas tablas de rutas como clientes, más una tabla global
- Cada VRF consiste en una tabla de ruteo, su correspondiente tabla de forwarding y un conjunto de interfases que usan dicha tabla de forwarding

# Ejemplo


VPN_A
10.2.0.0
C-network
CE1
VRF A
10.1.0.0/16 - link 5
10.2.0.0/16 - link 1
10.3.0.0/16 - link 2
.....
VPN_A
CE4
11.5.0.0
link 1
PE
VPN_
A
CE
2
10.3.0.
0
link 2
10.1.0.0
CE5
VPN_A
link 3
VPN_B
10.1.0.0
CE1
VRF B
10.1.0.0/16 - link 3
10.3.0.0/16 - link 4
.....
CE2
10.3.0.0
VPN_B

# Enrutamiento proveedor - cliente




- PE y CE intercambian información de ruteo a través de ruteo “clásico”:

  EBGP, OSPF, RIPv2, rutas estáticas

- CE no sabe que hace tránsito en una red MPLS para alcanzar otros CEs

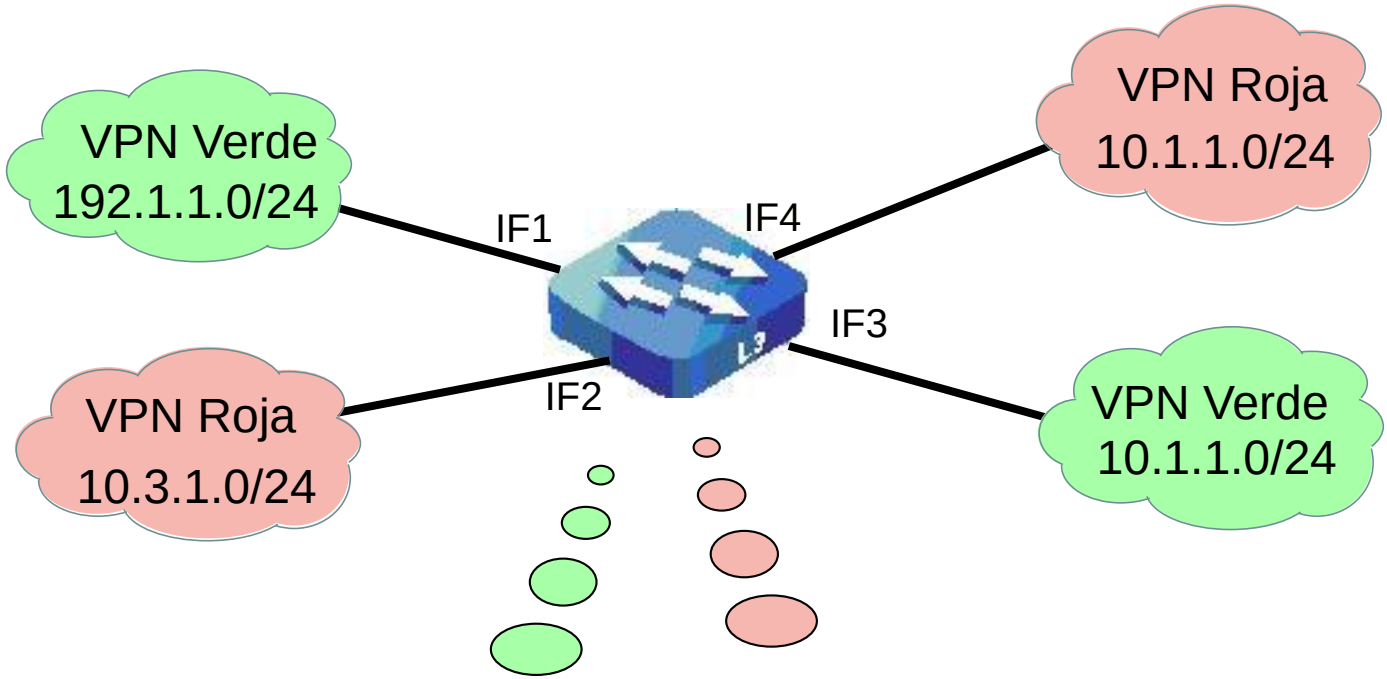
# Extensiones a los protocolos

- Cambios solamente en la red del proveedor
- En general, simple extensión a la configuración usual de los protocolos
- Detalles de redistribución, especialmente en protocolos complejos como OSPF

# Interconexión de sitios

- Si tuviéramos todos los puntos del cliente conectados al mismo router PE, el problema estaría resuelto
  - No escala
- Podemos interconectar enrutadores por múltiples interfaces o subinterfaces (p. ej. vlans), una por VRF
  - No escala

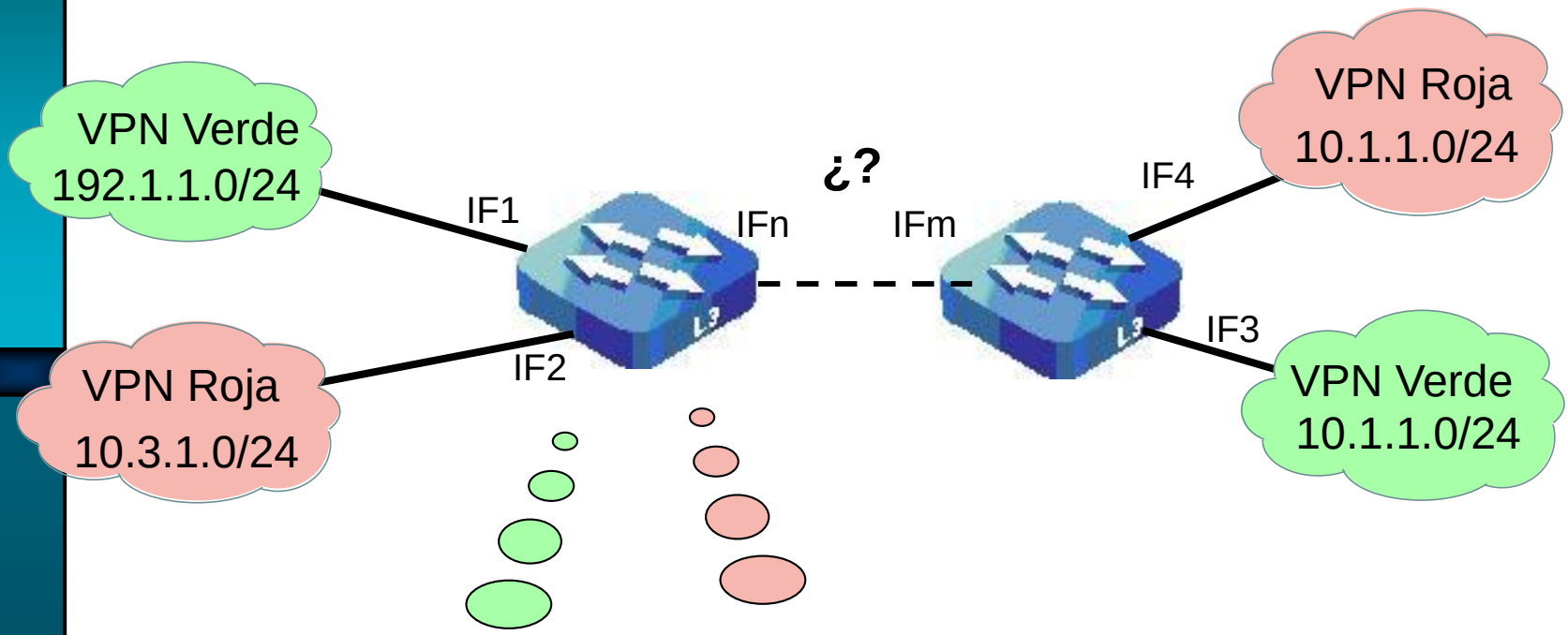
# VRFs en un solo enrutador




| Destino | salida |
|---|---|
| 10.1.1.0/24 | IF3 |
| 192.1.1.0/24 | IF1 |

| Destino | salida |
|---|---|
| 10.1.1.0/24 | IF4 |
| 10.3.1.0/24 | IF2 |

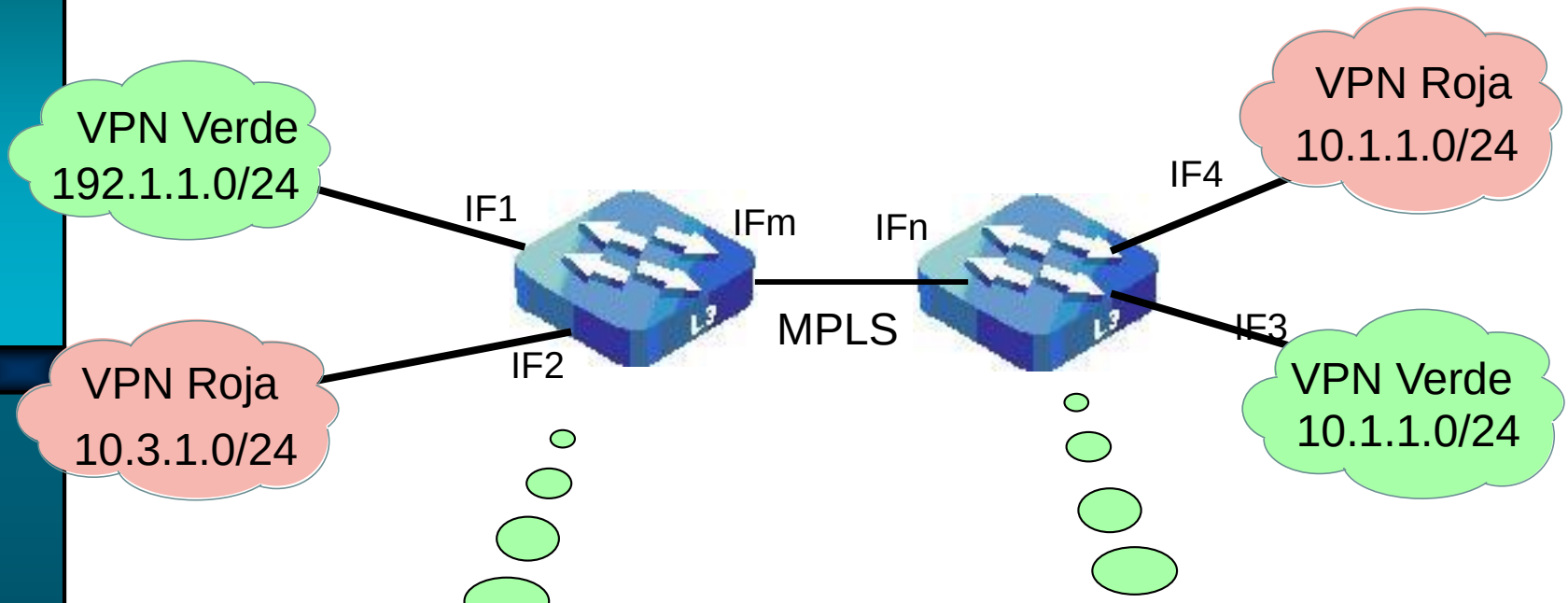
# Dos enrutadores




| Destino | salida |
|---|---|
| 10.1.1.0/24 | ? |
| 192.1.1.0/24 | IF1 |

| Destino | salida |
|---|---|
| 10.1.1.0/24 | IF4 |
| 10.3.1.0/24 | ? |

# VRFs en múltiples enrutadores




| Destino/etiq. | salida | etiqueta |
|---|---|---|
| 10.1.1.0/24 | IFm | X |
| 192.1.1.0/24 | IF1 | - |
| Y | IF1 | - |

| Destino/etiq. | salida | etiqueta |
|---|---|---|
| 10.1.1.0/24 | IF3 | - |
| X | IF3 | - |
| 192.1.1.0/24 | IFn | Y |

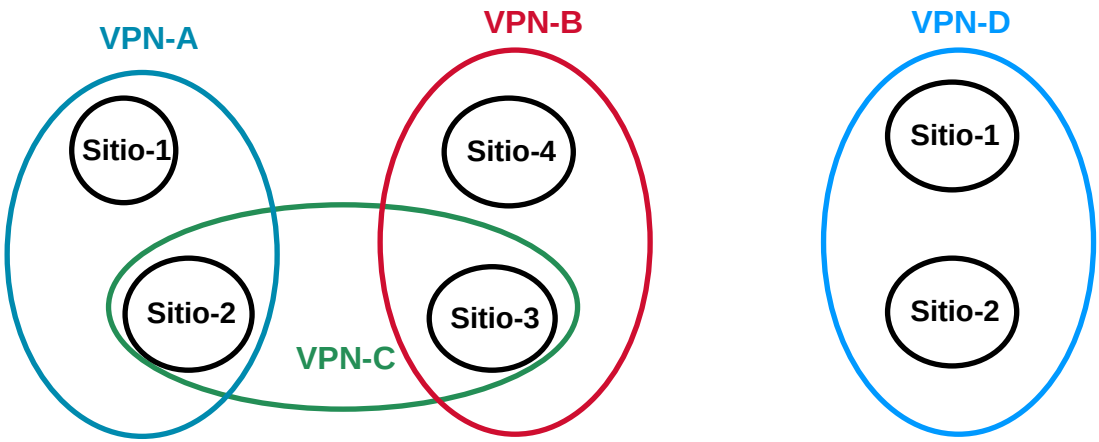
# Solución de MPLS VPNs

- Distribución de información de ruteo: BGP
  - Veremos que me permite, en una misma sesión, llevar información de todas las VRFs
- Separación de tráfico: MPLS
  - Me permite mantener aislados los paquetes de cada “VPN”

# Modelo de conexión MPLS/VPN (1)

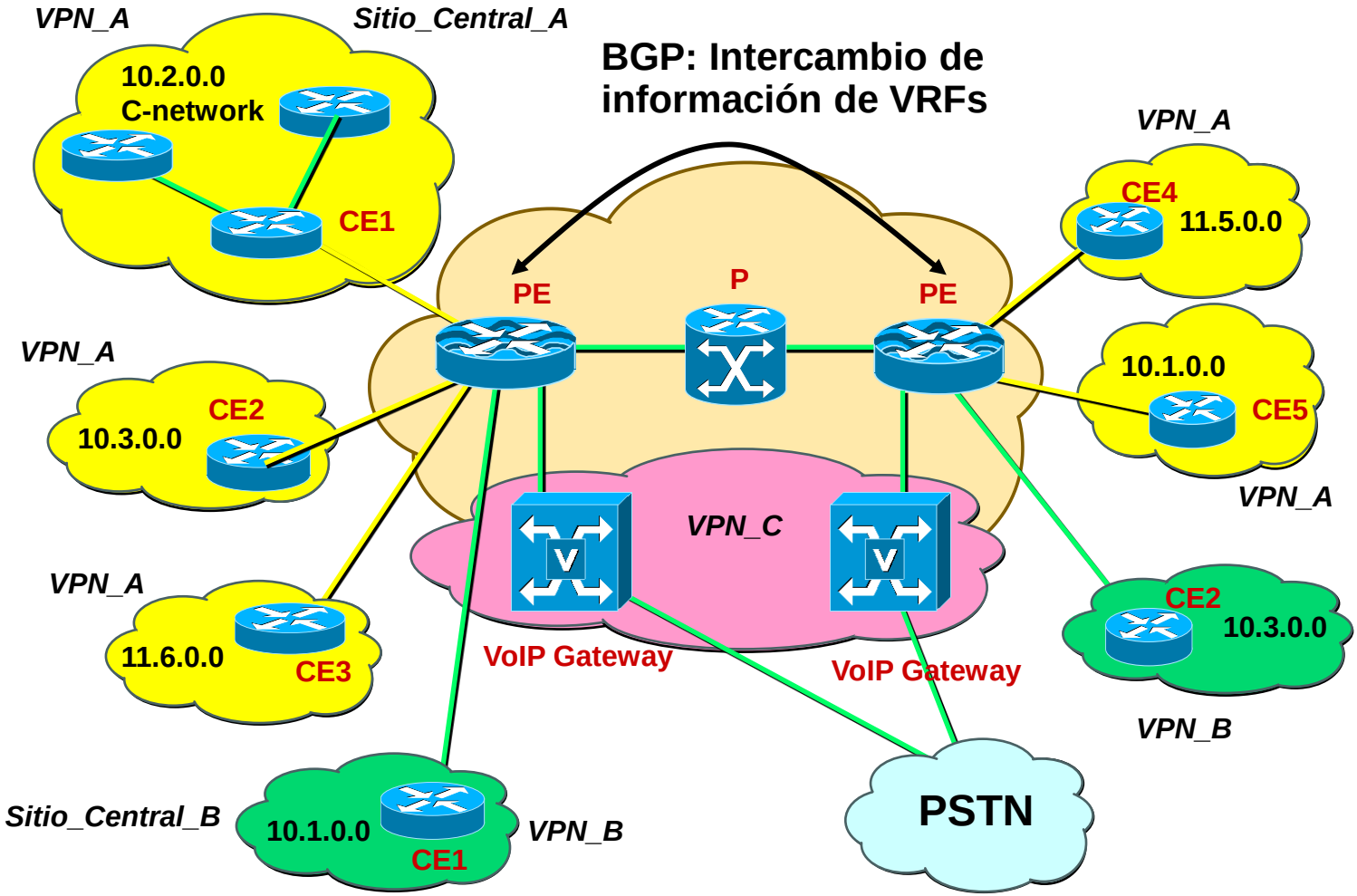
- Una VPN es una colección de “Sitios” que comparten información común de ruteo. Una VPN debe verse como una comunidad o grupo cerrado de usuarios
- Un “Sitio” puede pertenecer a más de una VPN
- Cada “Sitio” estará asociado a una VRF

# Modelo de conexión MPLS/VPN (2)




- Por ejemplo, dos empresas que tienen cada una su VPN, pero desean interconectar algún recurso común, pueden hacerlo
- Si dos o más VPNs tienen un sitio en común, el espacio de direccionamiento SÍ debe ser único para esas VPNs !!

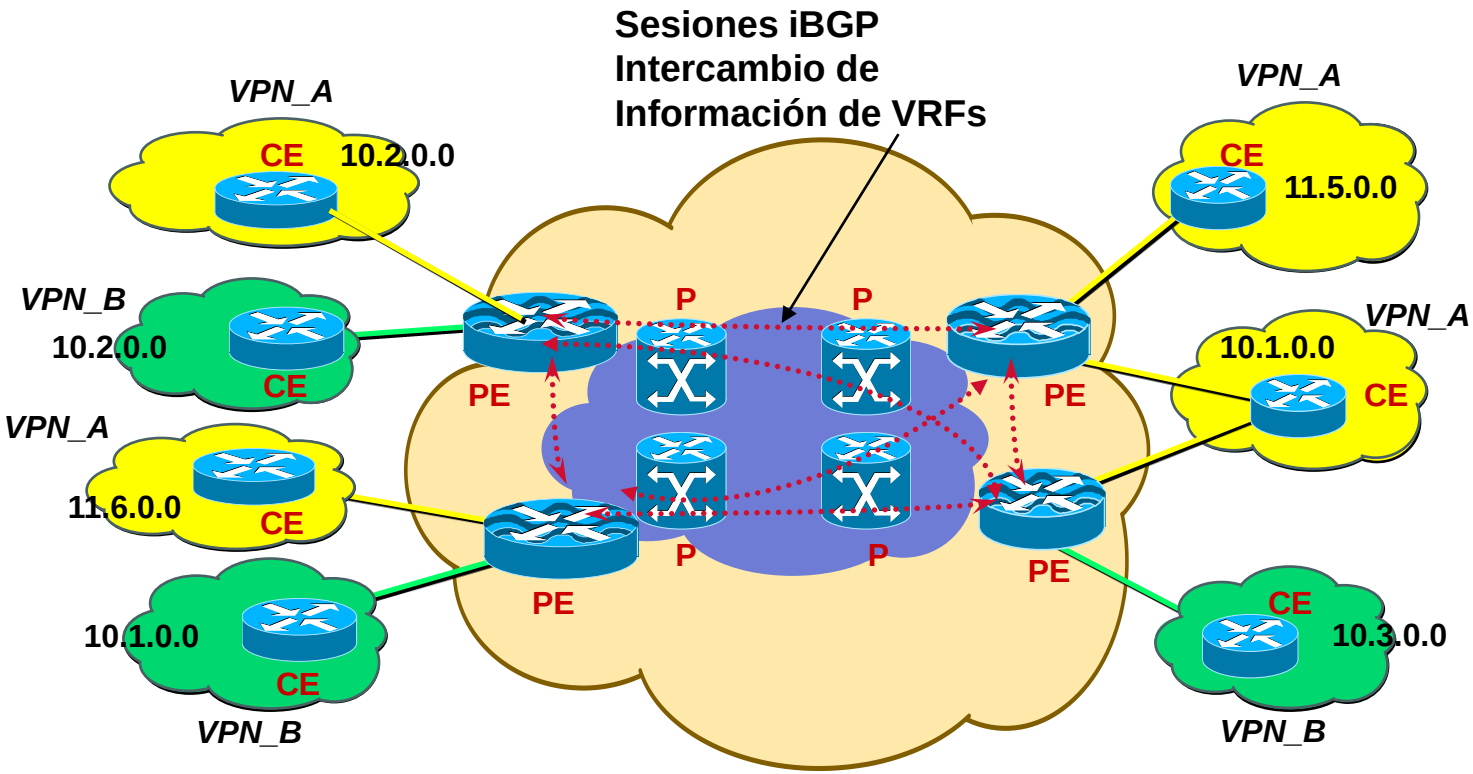
# Modelo de conexión MPLS/VPN (3)



# Funcionamiento de MPLS/VPN

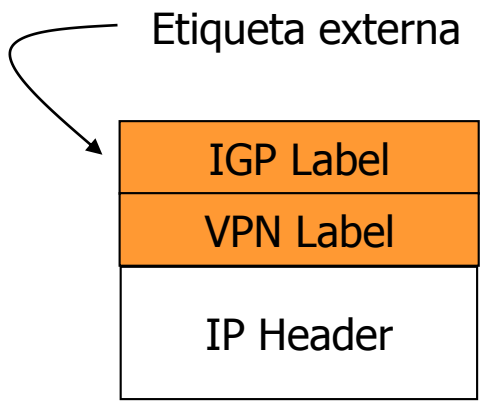
- La red del proveedor debe estar corriendo MPLS entre sus nodos, con algún método de propagación de etiquetas (ej. LDP)
  - Como lo que hemos visto hasta ahora
- Tendremos algún protocolo de enrutamiento interno para intercambiar rutas IP entre los nodos de esta red, de forma que todos los enrutadores sean alcanzables
- Utilizaremos BGP interno para intercambiar las rutas de las distintas VRFs
  - Lo veremos en un rato

# Funcionamiento de MPLS/VPN (2)



# Separación de tráfico: Stack de etiquetas

- Para el forwarding, 2 etiquetas MPLS
- La etiqueta externa nos lleva de un PE a otro
- La etiqueta interna separa las VPNs
- La externa (IGP) se obtiene por el protocolo de enrutamiento interior (p. ej. OSPF + LDP)
- VPN Label por MP-BGP



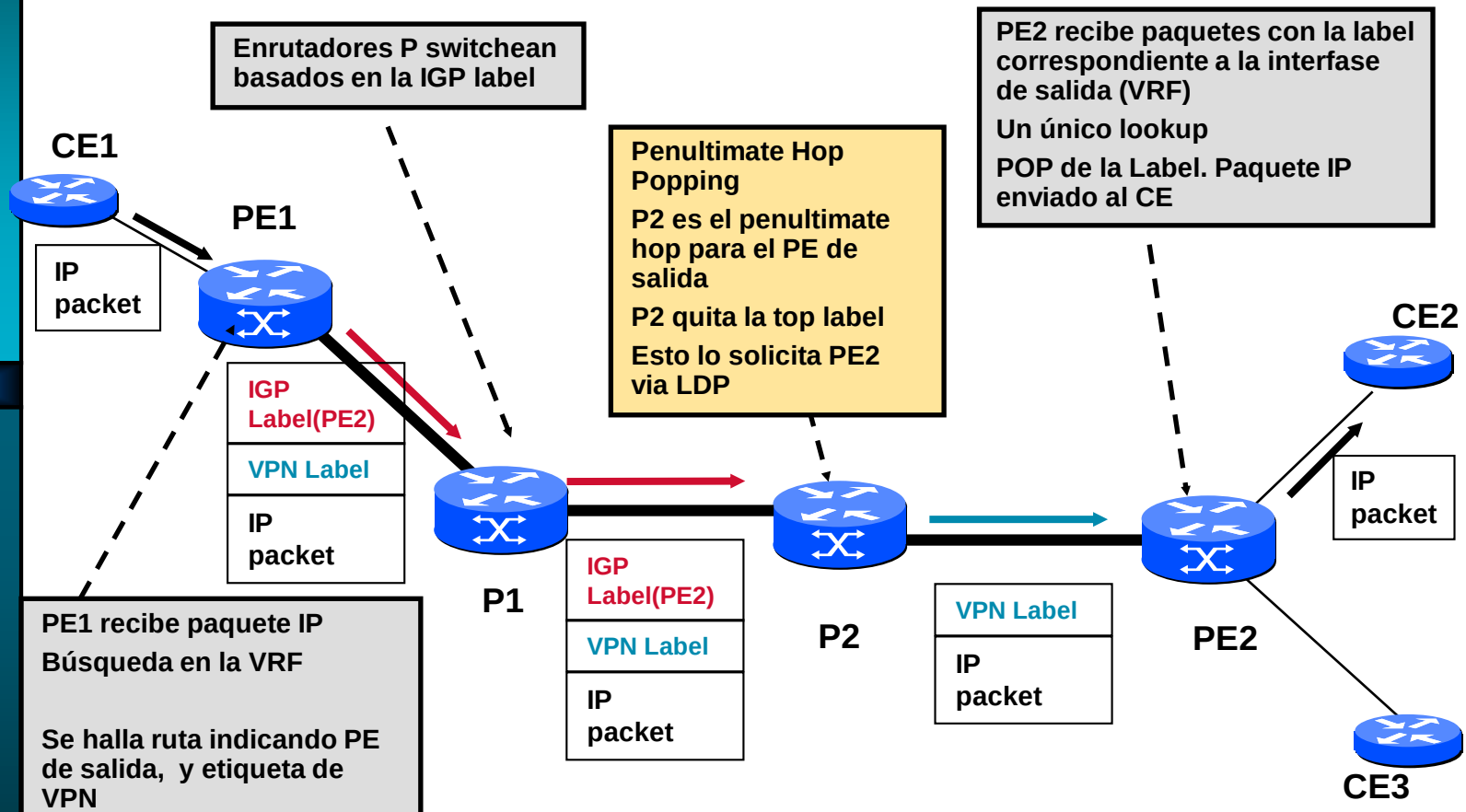
# MPLS Forwarding (1)

- Los routers PE y P deben tener etiquetas (aprendidas por LDP) correspondientes a los demás routers PE
  - estrictamente, a la IP del peer BGP
- Stack de etiquetas: usado para hacer el encaminamiento de paquetes
  - Etiqueta exterior: indica el enrutador PE al que está conectado el destino
  - Etiqueta de segundo nivel: la utiliza el PE destino para saber a que VPN pertenece el paquete

# MPLS Forwarding (2)

- Enrutador PE de ingreso agrega ambas etiquetas
- Nodos MPLS (P) hacen el forwarding basados en la etiqueta exterior
- El router PE de egreso encaminará el paquete basado en la segunda etiqueta, la cual indica la VPN y la interfase de salida

# MPLS Forwarding (3)



# Distribución de etiquetas y rutas de VPN

- Se distribuyen mediante extensiones a BGP (BGP Multiprotocolo)
- Todos los PE deben estar interconectados por iBGP
- Se pueden utilizar las técnicas que vimos para escalar BGP (route reflectors, confederaciones)

# Unicidad de las direcciones

- BGP siempre anuncia una ruta por destino
- ¿Qué pasa si dos clientes usan la misma red?
  - BGP anunciará sólo una ruta: PROBLEMA !!!
- Se define un nuevo espacio de direcciones, VPNv4, a partir de un atributo Route Distinguisher (RD):

  RD : Route distinguisher (64 bits) +

  IPv4 (32 bits)

# Route Distinguisher

- RD se configura para cada VRF en cada PE
  - No tiene por qué ser el mismo en todos los PE, aunque es más fácil que si lo sea
- Lo importante es que RD:IP sea único en toda la red

# Formato del Route Distinguisher

- 2 campos:

  Tipo: 2 bytes

  Valor: 6 bytes

- A su vez, según el tipo la codificación del valor:

  –Tipo 0: AS:n°

  –Tipo 1: IP:n°

  –Tipo 2: AS:n° (con AS de 32 bits)

  El n° es asignado administrativamente

# Extensiones de BGP usadas para las VPNs

- **Comunidades extendidas (Extended Community):**
  - Atributo BGP, similar a las comunidades
  - 8 bytes
  - 1 o 2 bytes: tipo. El valor se codifica de acuerdo al tipo
  - Route-Origin: 64 bits que identifican el enrutador que originó la ruta
  - Route-Target: 64 bits que identifican las VRFs que deben recibir la ruta
    - Se usará para importación y exportación de rutas

# Route Target

- RT (Route Target), es un atributo que indica a qué VRF pertenece la ruta

  Es el “color” de la VPN

- También es un valor de 64 bits

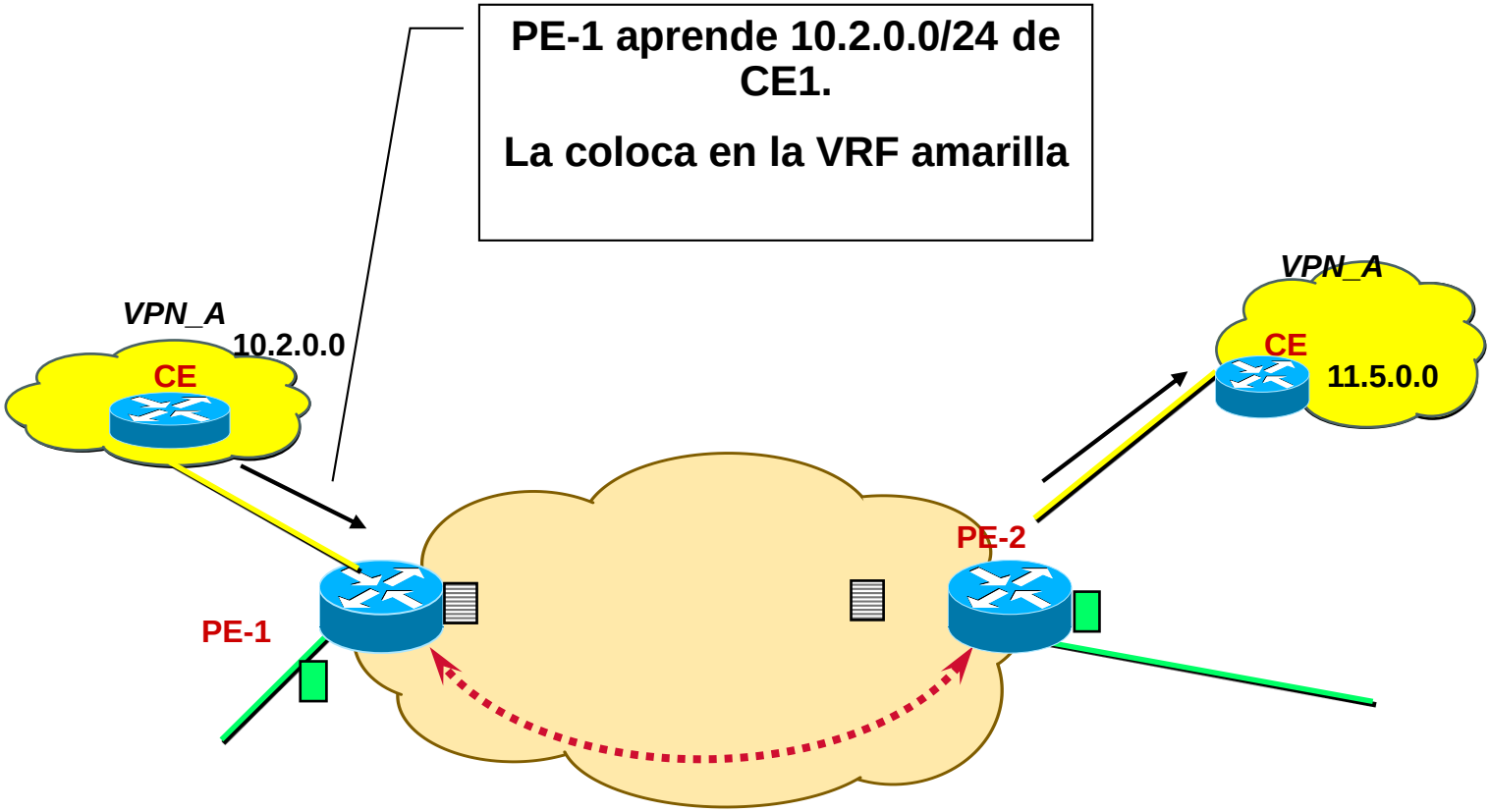
  También se recomienda poner el número de AS en los primeros 16 bits (o una IP pública en los primeros 32 bits)

- En el caso más sencillo, es simplemente un identificador de la VPN

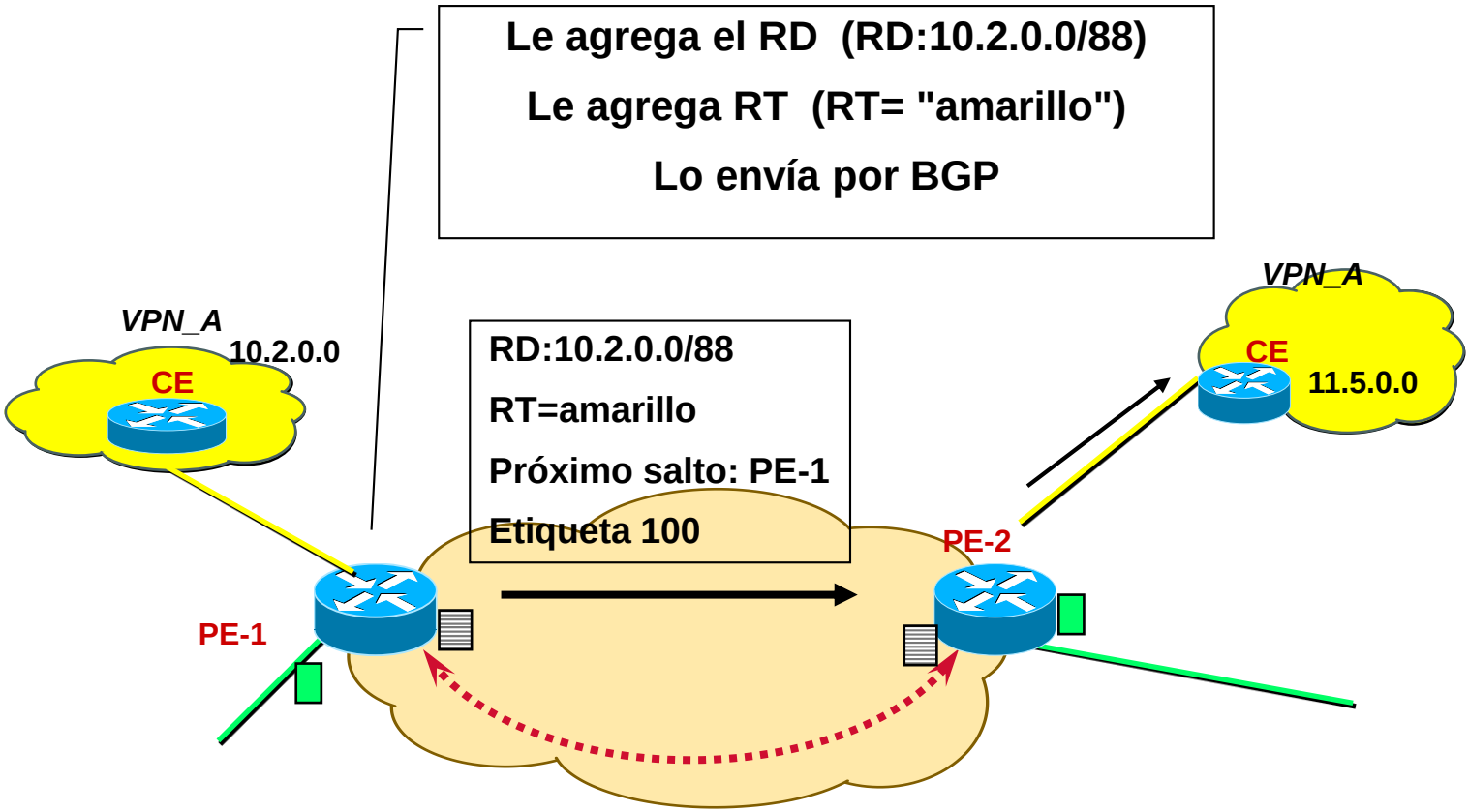
# Route Target (cont.)

- En general, en cada VRF (en cada PE), indico uno (o más) route target para importar y uno (o más) para exportar
- Al exportar las rutas, se "estampan" con los RT indicados
- Al recibirlas, se revisa si alguno de los RT coincide con los RT importados por alguna VRF

# Ejemplo de funcionamiento
# Aprendizaje de rutas



# Ejemplo de funcionamiento
# Aprendizaje de rutas



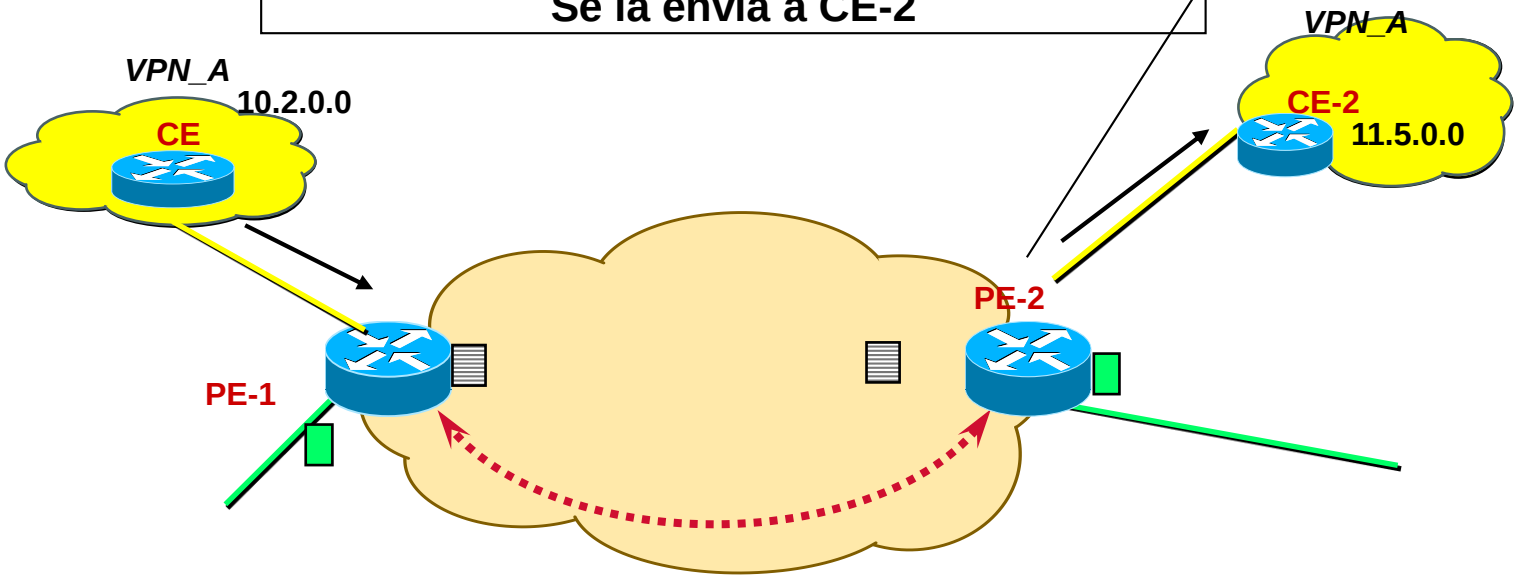
# Ejemplo de funcionamiento
# Aprendizaje de rutas

**PE-2 elige mejor ruta a RD:10.2.0.0/88**

**Quita el RD (10.2.0.0/24)**

**Verifica el RT, pone ruta en tablas que importen "amarillo“ con la etiqueta indicada**

**Se la envía a CE-2**



# Resumiendo: plano de control

- Se definen VRFs en los distintos enrutadores
- Se asocian las interfases a las VRFs
- El enrutador PE aprende rutas del cliente mediante protocolos standard (o estáticas)
- Las rutas así aprendidas se propagan internamente por BGP utilizando direcciones VPNv4. Para indicar la VRF, se utiliza el route-target. Se envía además una etiqueta
- Las rutas aprendidas por BGP se agregan en la tabla y envían a los clientes

# Resumiendo: plano de datos

- De acuerdo a la interfaz de entrada, se elige la VRF a utilizar para los paquetes
  - O la tabla global
- Si la tabla de la VRF indica que es un destino remoto, se arma el stack de etiquetas
  - Etiqueta interna: la etiqueta propagada por BGP
  - Etiqueta externa: la etiqueta IGP correspondiente al next-hop de BGP

# Topologías

- Si en todas las VRFs de una VPN importamos y exportamos el mismo route-target, obtenemos una estructura plana (interconexión directa todos con todos)
- Definiendo con qué Route Target se exporta cada ruta, y qué Route Targets se importan en cada VRF, puedo definir topologías que se adapten a mis requerimientos

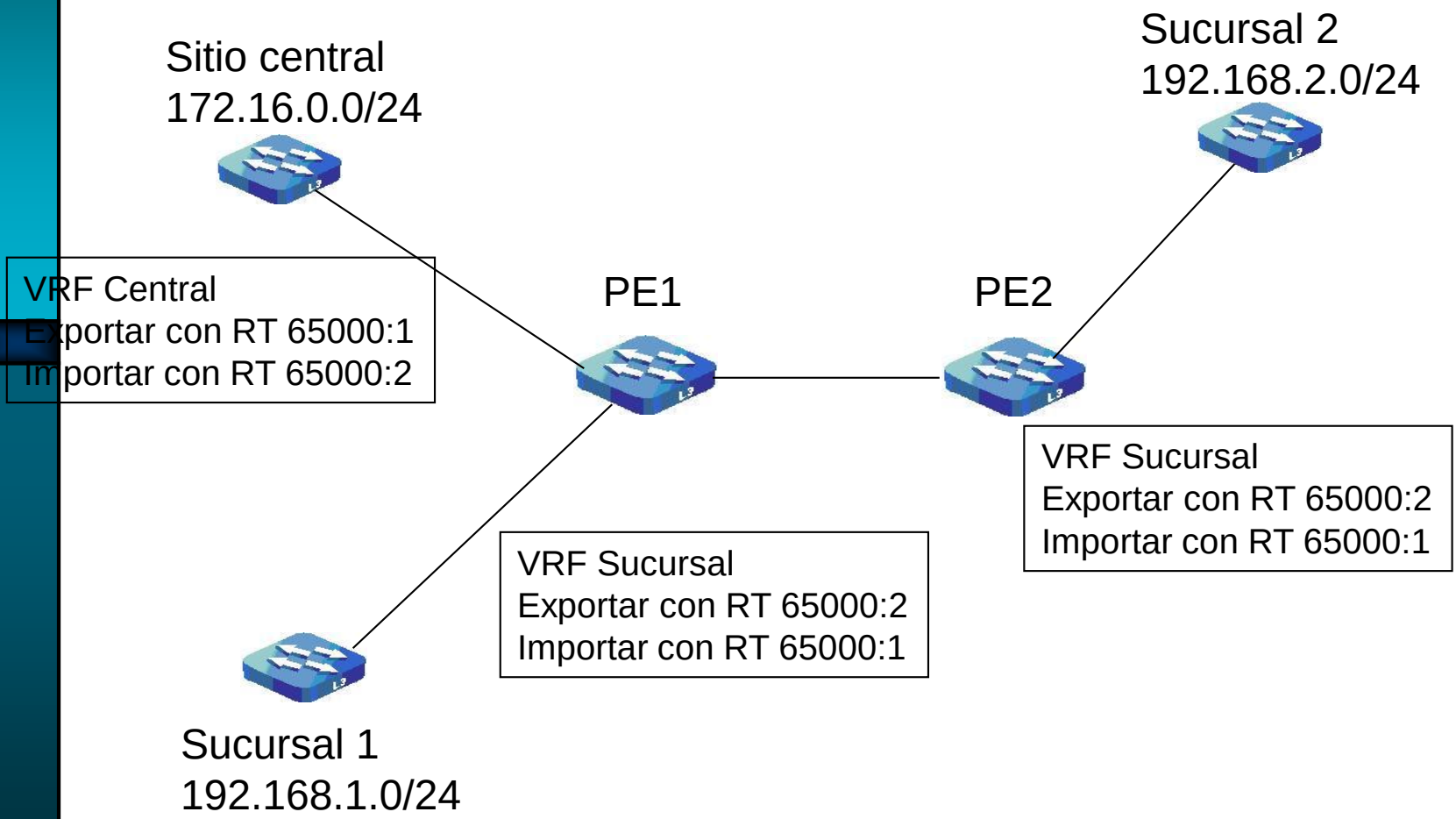
# Ejemplo:
# Sitio central y sitios remotos

- Requerimiento: interconexión de un sitio remoto a sucursales
- NO debe permitirse tráfico entre los sitios remotos
- Puede resolverse de mas de una manera
- Posible solución: 2 Route Targets

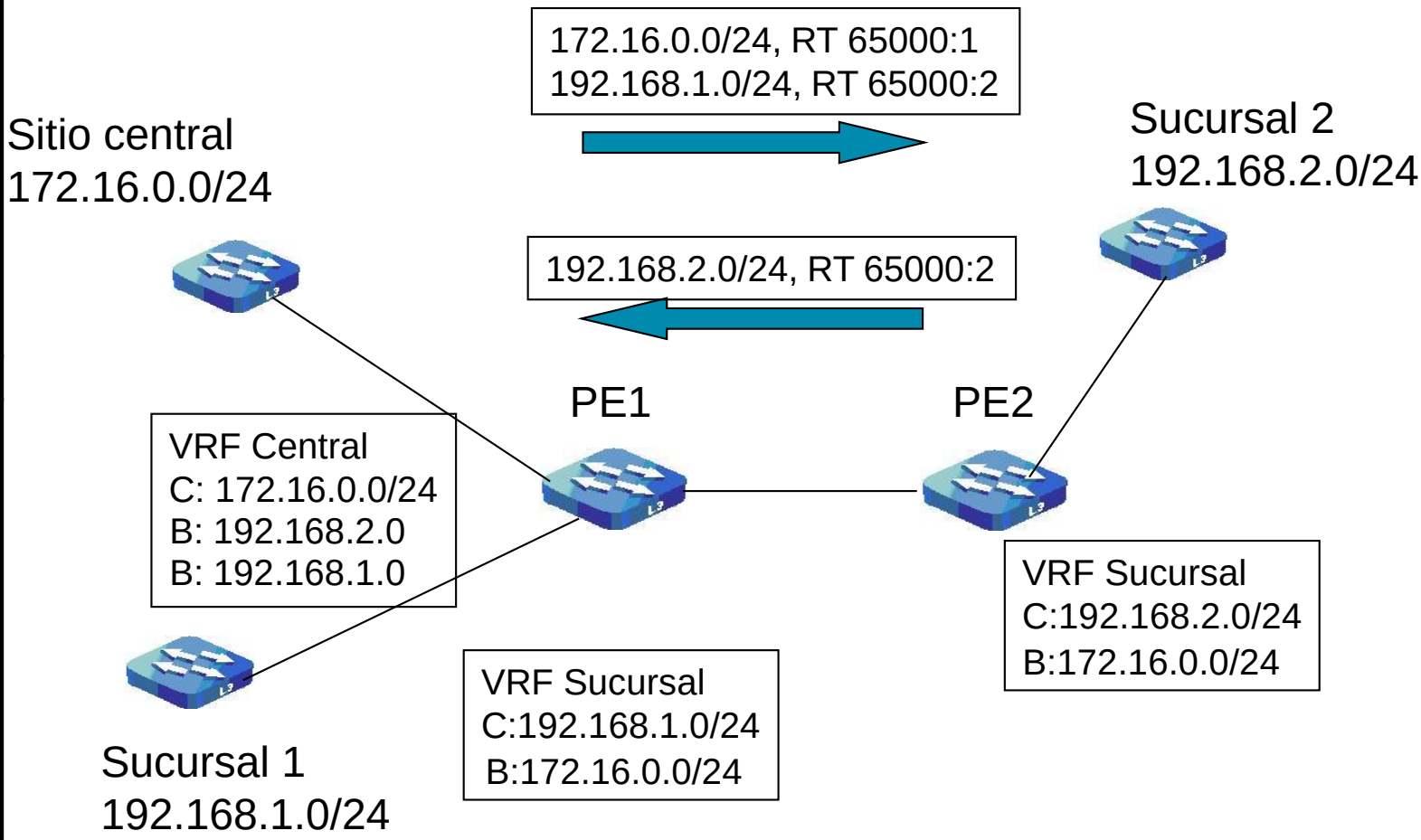
  RT “central”: 65000:1

  RT “sucursales”: 65000:2
- VRF sitio central importa rutas con RT “sucursales”
- VRF sucursales importan rutas con RT “central”

# Ejemplo:
# Sitio central y sitios remotos



# Ejemplo:
# Sitio central y sitios remotos



# BGP como protocolo PE-CE

- No es necesario configurar la redistribución

  Pero es necesario configurar explícitamente los vecinos

- Se utiliza BGP externo
- Podemos utilizar números de AS privados en el cliente

  Con cuidado, podemos utilizar el mismo número de AS en todos los sitios

  Debemos indicar, al configurar el vecino, que haga “as-override”, para que elimine el AS# remoto

  Si existe la posibilidad de loops, usar “SOO” (site of origin)

# OSPF entre PE-CE

- En muchos equipos, limitación en cantidad

  P. ej. Cisco, en muchas plataformas no más de 28 procesos

- El backbone MPLS se comporta como un área de jerarquía superior a la del área 0

  No es un área “0” real, entre enrutadores PE no se habla OSPF

  Si hay un área 0 en el cliente, el área 0 debe estar conectada directamente al backbone MPLS

- El tipo de ruta OSPF (inter/intra área, externa) se lleva utilizando comunidades extendidas

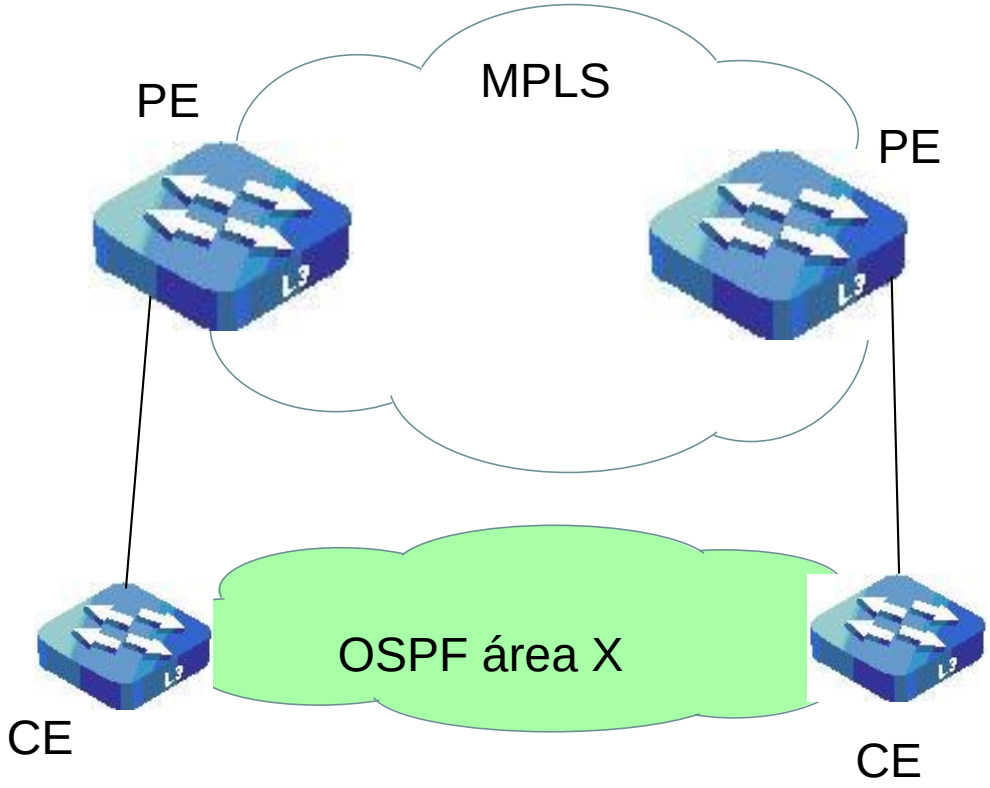
# OSPF entre PE-CE (cont.)

- El backbone MPLS envía hacia el router CE LSAs de tipo summary y externas

  Summary si eran summary o inter-área, externas si eran externas

- Se setea un bit en el campo opciones, para evitar loops en topologías complejas

# Conectividad OSPF fuera del backbone



# Conectividad OSPF fuera del backbone

- Las rutas dentro del área X serán intra-área
- Las rutas recibidas por MP-BGP se redistribuirán como inter-área o externas
- Los enrutadores preferirán el camino por fuera del backbone MPLS
- Solución: “sham links”

  Me ofrece conectividad virtual, en el área X, entre los enrutadores PE

  Podrán propagar anuncios tipo 1 y 2
- Debemos asegurarnos que el costo del link “sham” sea menor

# Convergencia del enrutamiento

- 2 componentes
  - Convergencia del protocolo interno del proveedor
  - Convergencia del enrutamiento entre los sitios “cliente” (MP-BGP)
- Podemos también tener una componente en convergencia en capa 2
- El protocolo interno converge en el mismo tiempo que si no estuviera MPLS
  - Se pueden cambiar los tiempos de OSPF

# Convergencia de las rutas de cliente

- Anuncio de las rutas desde el cliente al proveedor
- Propagación en el backbone por MP-BGP
- Importación en las VRF adecuadas
- Anuncio a otros sitios del cliente

# Convergencia de MP-BGP

- El principal tiempo que se agrega frente a una situación sin MPLS, es el tiempo de propagación en BGP
  - Los anuncios no se envían inmediatamente por defecto
  - Se acumulan tiempos en los reflectores
  - Puede cambiarse con
  - *neighbor advertisement-interval <seg>*

# VPNs “Capa 2”

# Agenda:

- Introducción
- Protocolos Soportados
- Ejemplo de Tunelización: Ethernet
- Ejemplo de Servicio: VPLS

# VPNs “capa 2”: Introducción

- Permite a Proveedores que ofrecen servicios de Capa 2 (o incluso capa 1) seguir ofreciéndolos sobre un backbone MPLS
- Consiste básicamente en una tunelización sobre una red MPLS
- Es la forma de dar una solución integrada de todos los servicios no IP sobre MPLS
- Pueden encontrarlo con distintos nombres según el fabricante
- Hay alternativas que no utilizan MPLS

# L2VPN

- Permite integrar los servicios de L2 con las ventajas de MPLS: Ingeniería de tráfico, QoS
- Proceso estándar abierto en el IETF
- Varios grupos de trabajo en el IETF
  - –Encapsulación: Pseudo Wire Emulation Edge to Edge (pwe3)
  - –Señalización: varias propuestas
    - » Se impuso utilizar sesiones LDP dirigidas

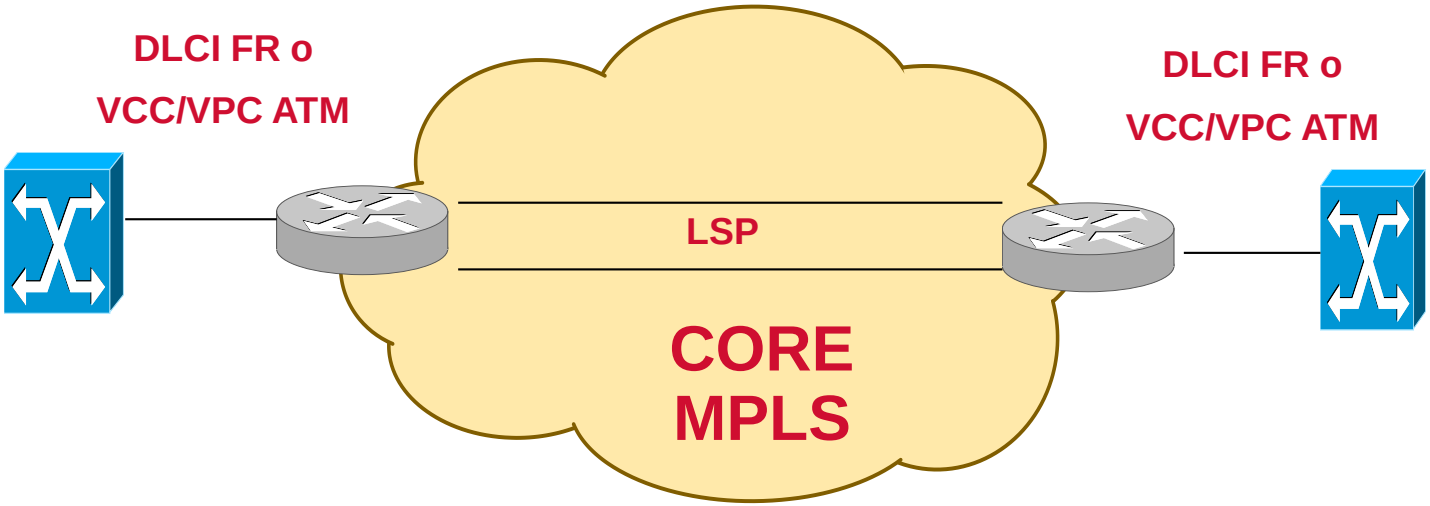
# Pseudo cables (pseudo wires)

- La idea es emular un "cable" de la tecnología adecuada
- En general se utiliza un stack de etiquetas adecuado para mantener multiplexación y jerarquía de direccionamiento
  - Típicamente, una etiqueta para llegar al PE destino, y otra para indicar lo que se transporta y por donde enviarlo
- Pueden utilizarse otros transportes para los túneles
  - Por ejemplo, L2TPv3, túneles sobre IP ....

# Señalización

- Se da a dos niveles:
  - Señalización en MPLS para la formación de los LSPs. Se ha adoptado una extensión de LDP (basada en los drafts de Martini), hay propuestas para utilizar BGP-MP (Kompella drafts)
  - Tunelización de la señalización de los protocolos a transportar

# Ejemplo de L2VPN



# L2VPN

- **Protocolos Soportados:**
  - Ethernet over MPLS
  - ATM AAL5 over MPLS
  - Frame Relay over MPLS
  - ATM Cell Relay over MPLS
  - PPP over MPLS
  - HDLC over MPLS
  - Circuit Emulation over MPLS

# Ejemplo: Pseudo Cable Ethernet

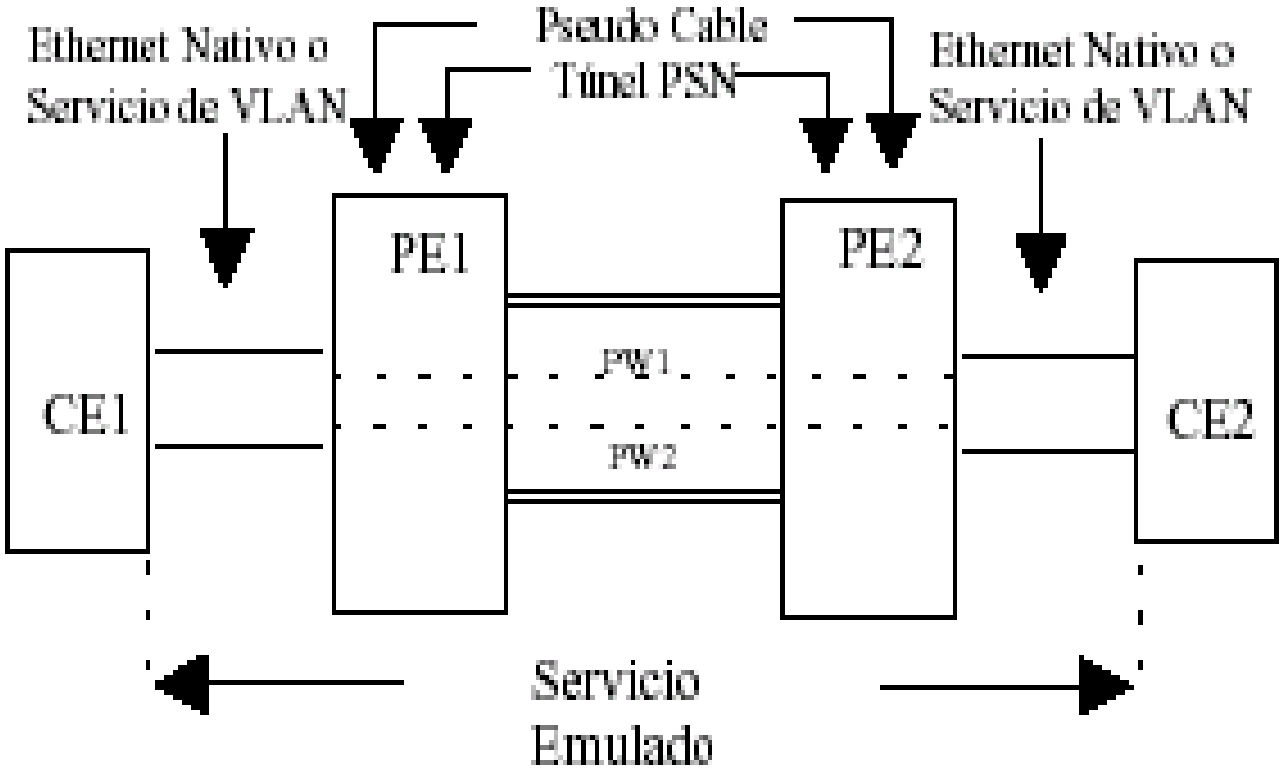
- LSP con stack de etiquetas de profundidad 2:

  Etiqueta externa (PSN): Etiqueta del LSP negociada por LDP “estándar”

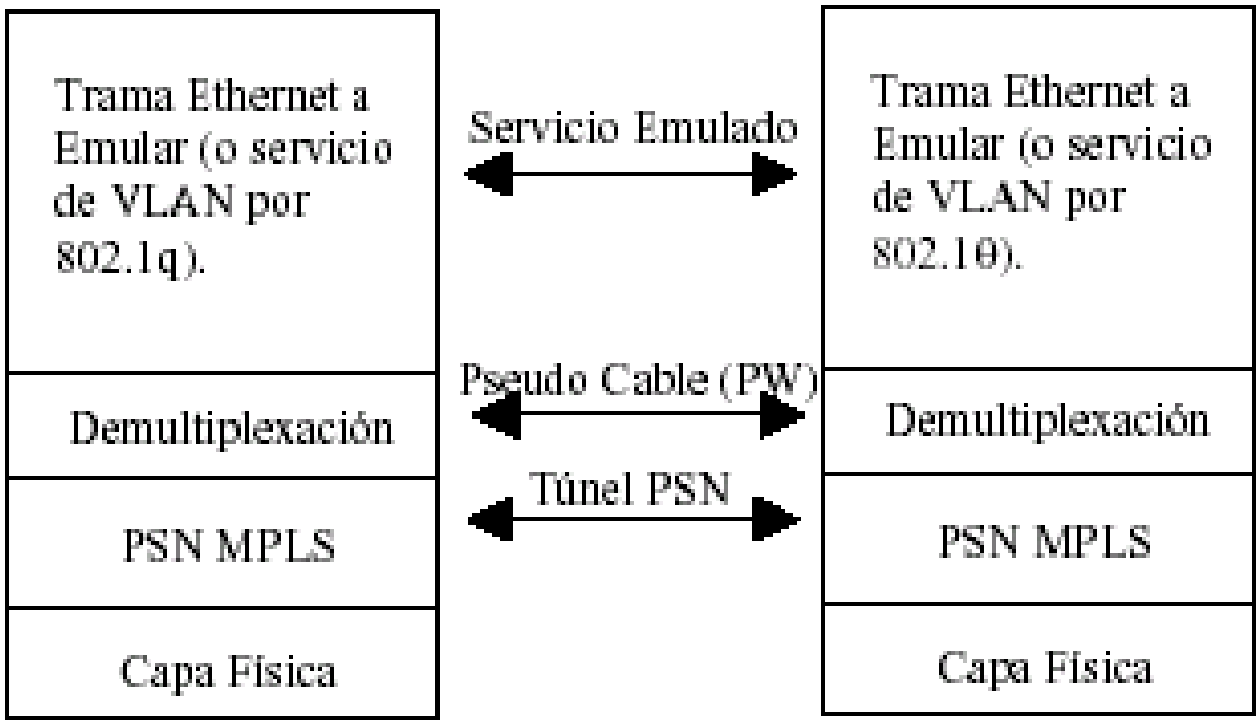
  Etiqueta interna (PW): identificador del servicio negociada por LDP con un nuevo tipo de FEC

- La red MPLS (equipos P) sólo ven el LSP entre el PE de entrada y el de salida (etiqueta externa)

# Pseudo Cable Ethernet:



# Pseudo Cable Ethernet:



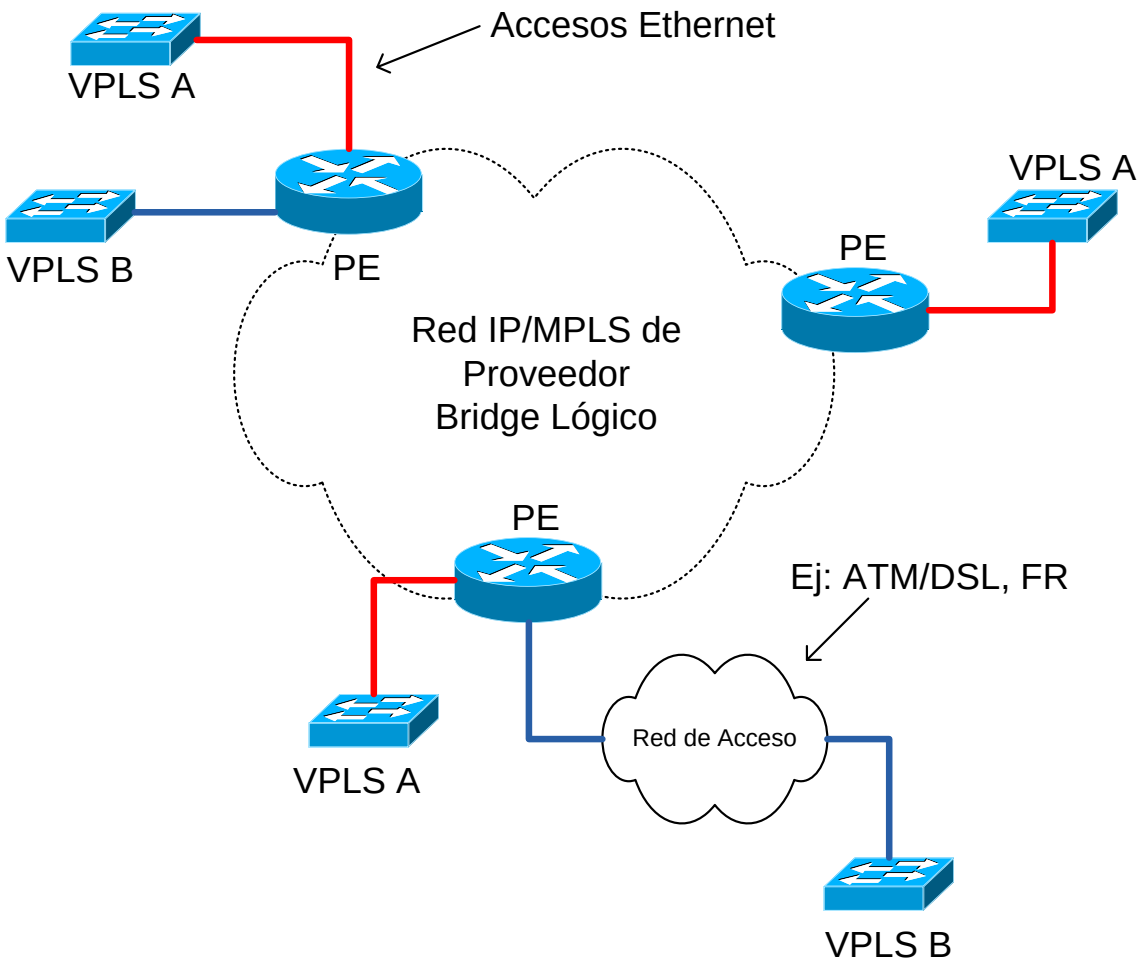
# VPLS: Virtual Private LAN Service

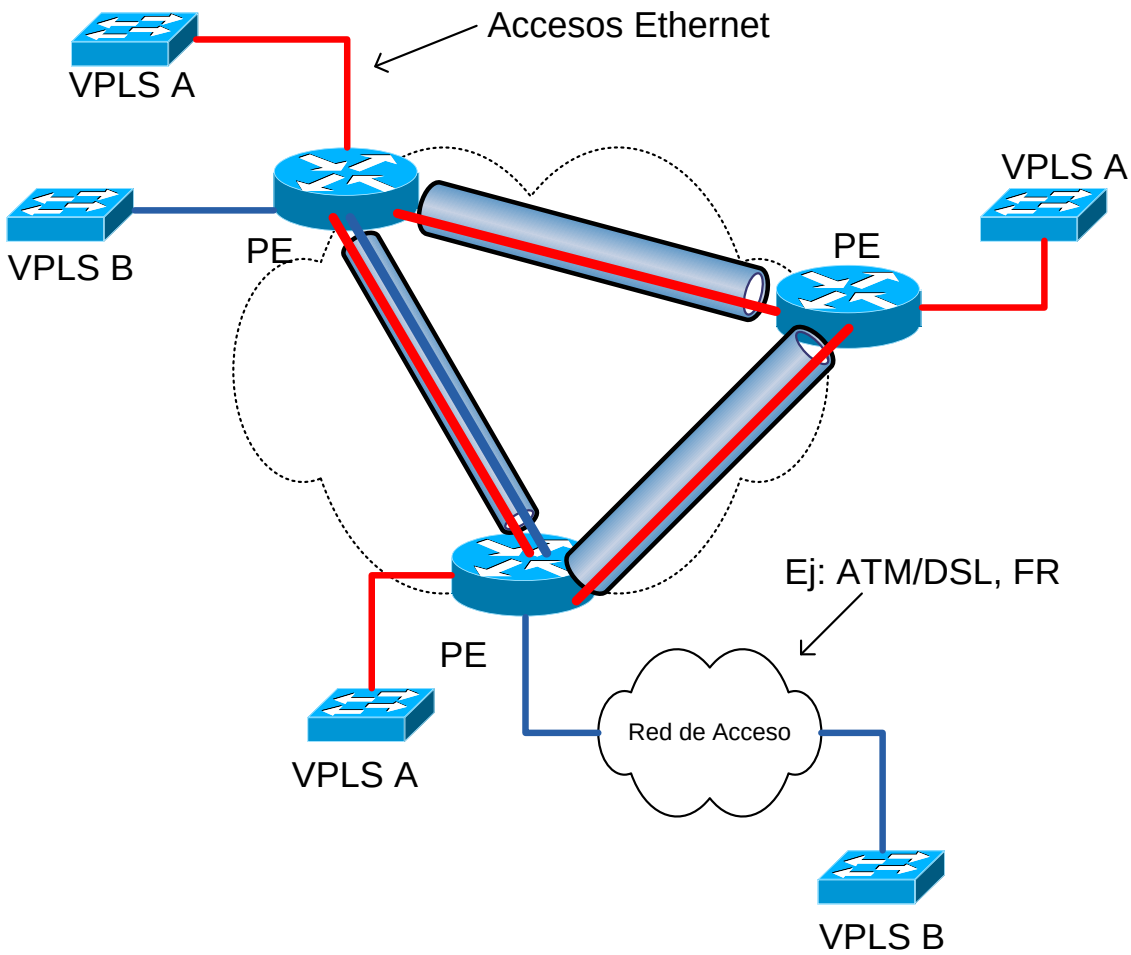
- Consiste en Emular una LAN sobre un dominio MPLS
  - La idea es que se parezca a un switch
- Problema similar al resuelto por LANE o RFC 1483
- Utiliza PW Ethernet sobre MPLS
- El principal problema a resolver es la traslación MAC destino <-> PE destino

# VPLS

- En el formato básico de una VPLS, tendremos una malla de LSPs (pseudowires) entre los enrutadores PE con puntos en la VPLS
- Cada enrutador PE funcionará como un switch transparente para esa VPLS
  - Las bocas del switch serán tanto las bocas físicas que interconectan a puntos del cliente, como las bocas lógicas correspondientes a los LSPs con los demás enrutadores PE
- Evitar loops: no se retransmite lo recibido por un LSP

# VPLS


Accesos Ethernet
VPLS A
VPLS B
PE
Red IP/MPLS de
Proveedor
Bridge Lógico
VPLS A
PE
PE
Ej: ATM/DSL, FR
Red de Acceso
VPLS A
VPLS B


Accesos Ethernet
VPLS A
VPLS B
PE
PE
VPLS A
PE
Ej: ATM/DSL, FR
Red de Acceso
VPLS A
VPLS B