

# **Tema 2-1: Redes privadas virtuales con MPLS**

# Objetivos

- ◆ Conocer el funcionamiento de las redes privadas virtuales en general y su implementación en MPLS (MPLS-VPN)
  - Comprender cómo se aísla el encaminamiento de los clientes con los **VRF** (*per-VPN Routing and Forwarding table*)
  - Comprender el uso de **BGP** para difundir rutas de los clientes
- ◆ Saber configurar (**provisionar**) las MPLS-VPN en la red del operador para dar servicio a los clientes
  - Comprender y saber aplicar los parámetros **RD** (*Route Distinguisher*) y **RT** (*Route Target*)

# Índice

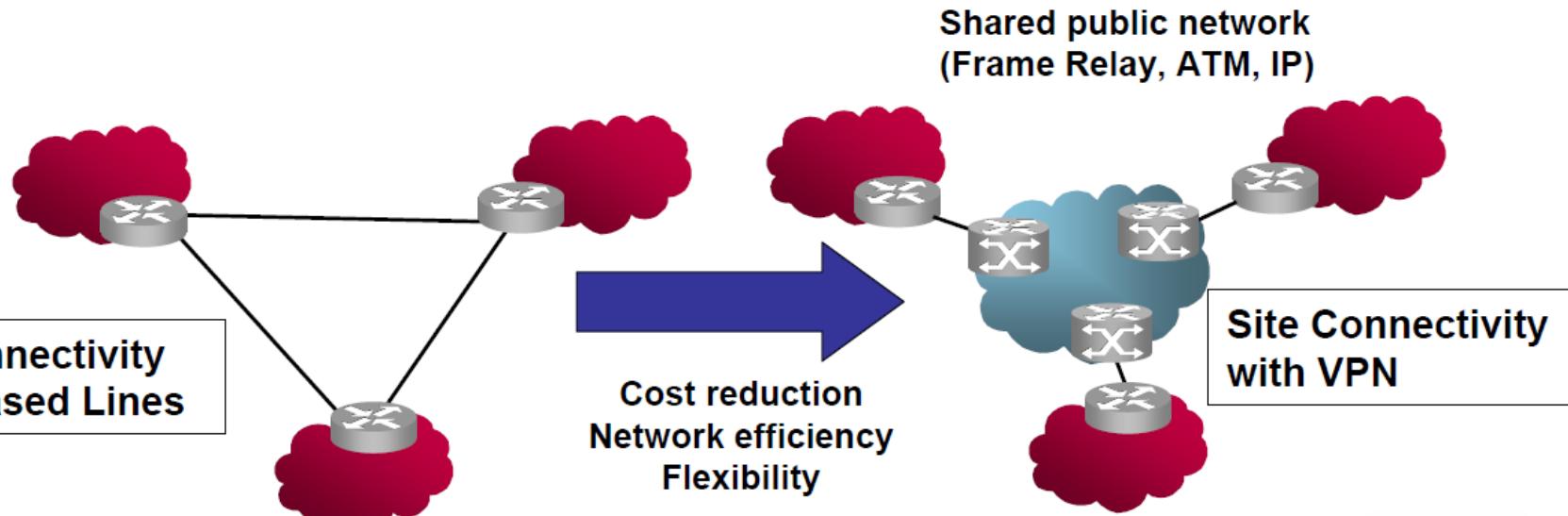
- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

# Introducción a las VPNs

- ◆ La posibilidad de crear VPNs es la mayor aplicación de MPLS
  - Las VPNs existían ya antes de MPLS.
  - La ventaja de emplear MPLS (y BGP) es la escalabilidad y simplicidad
- ◆ Las VPN de capa 3 basadas en MPLS (MPLS VPN) en realidad se llaman BGP/MPLS VPN.
  - Uso de MP-BGP para transportar las rutas BGP
    - MP-BGP: *MultiProtocol BGP*

# Introducción a las VPNs

- ◆ ¿Qué es una VPN?
  - Red: conjunto de sitios remotos.
  - Privada:
    - Acceso limitado a los miembros de la VPN.
    - Separación de direcciones y de rutas.
  - Virtual: conectividad emulada sobre una red pública.



# Introducción a las VPNs

- ◆ ¿Qué características desea el cliente?
  - En general, conseguir conectividad entre sedes de la manera más sencilla posible.
  - La conexión de las sedes dispersas debe tener las mismas garantías de privacidad y QoS que una red privada.
  - No debe requerir cambios en la manera en la que se configura la red del usuario.
    - Por ejemplo, debe permitir el direccionamiento privado que escoja el cliente.
  - Las operaciones que afecten a la conectividad deben ser sencillas.
    - Por ejemplo, añadir conectividad a una nueva sede, cambiar la conectividad entre sedes o incrementar el ancho de banda entre sedes no debe requerir muchos cambios.
  - No debe requerir protocolos de encaminamiento complejos en las sedes del cliente.

# Tipos de VPNs L3

- ◆ Hay dos modelos para implementar VPN
  - Overlay VPNs, el proveedor suministra enlaces punto a punto entre sedes de clientes
  - Peer to peer VPNs, el proveedor participa del encaminamiento del cliente (caso de MPLS)

# Introducción a las VPNs: modelo *overlay*

- ◆ Modelo VPN más intuitivo: si se busca conectividad → Conectar las sedes mediante enlaces punto a punto entre ellas.
- ◆ Habitualmente, conexiones configuradas a mano.
- ◆ El proveedor desconoce la estructura y direccionamiento de la red interna del cliente → Proporciona solo un servicio de transporte.
- ◆ La inteligencia y control de las VPNs está en los *routers* frontera del cliente (*CE routers*, *Customer Edge routers*).
  - A este tipo de VPNs se les llama CE-VPNs.

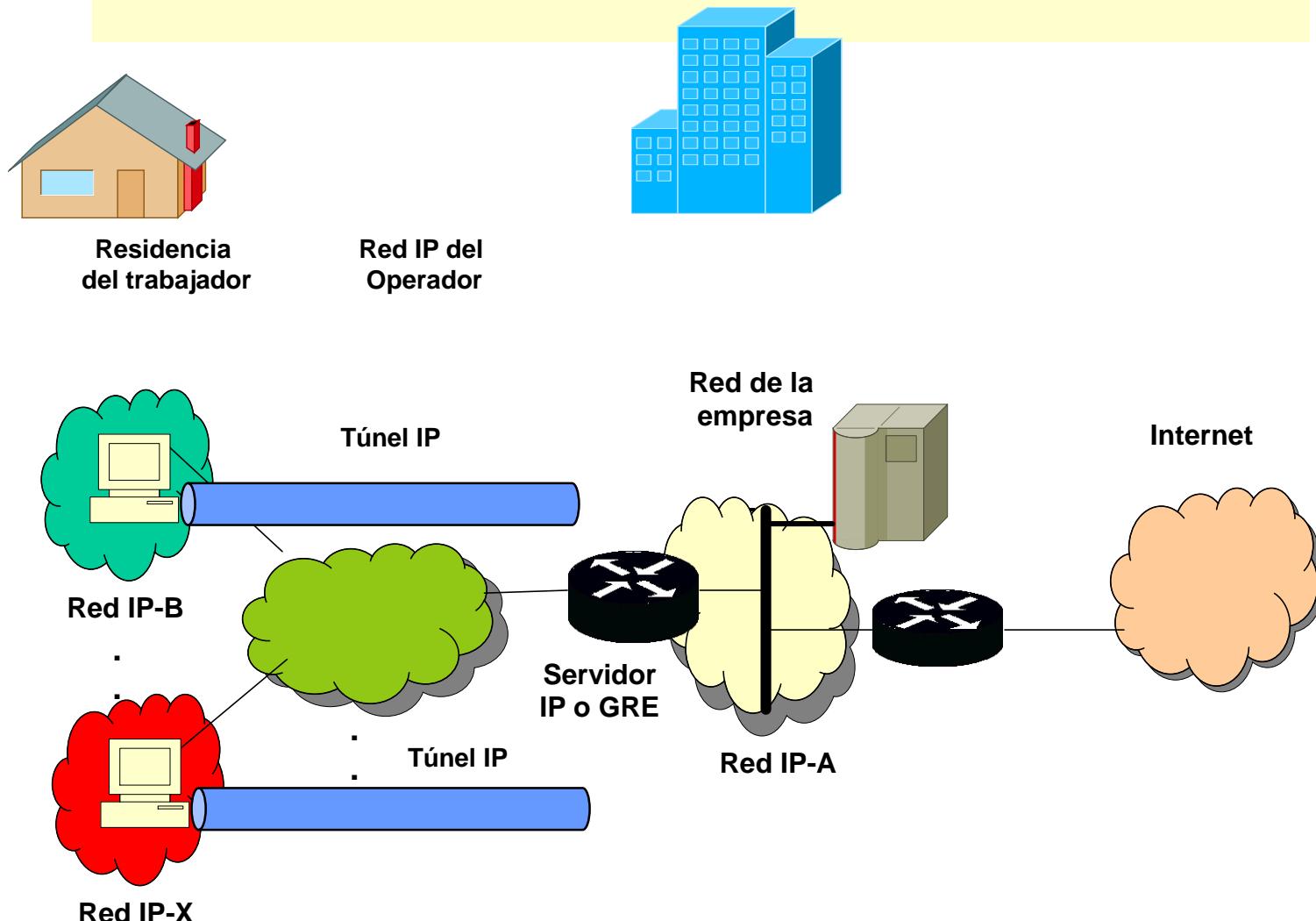
# Modelo Overlay

- ◆ Implementación de nivel 1
  - Con conexiones del operador de nivel 1, ISDN, E1, SDH
  - El cliente es responsable del resto de capas (X.25, FR, ATM, TCP/IP)
- ◆ Implementación de nivel 2
  - El operador suministra conexiones de nivel 2 (X.25, FR, ATM)
  - El cliente es responsable del resto de capas (TCP/IP)
  - La solución WAN tradicional
  - Con características implícitas de seguridad y cierto grado de QoS
    - FR, seguridad por los PVC, QoS por el CIR
    - ATM seguridad por los VPI/VCI, QoS implícita
- ◆ Conexiones configuradas a mano

# Modelo Overlay (Cont.)

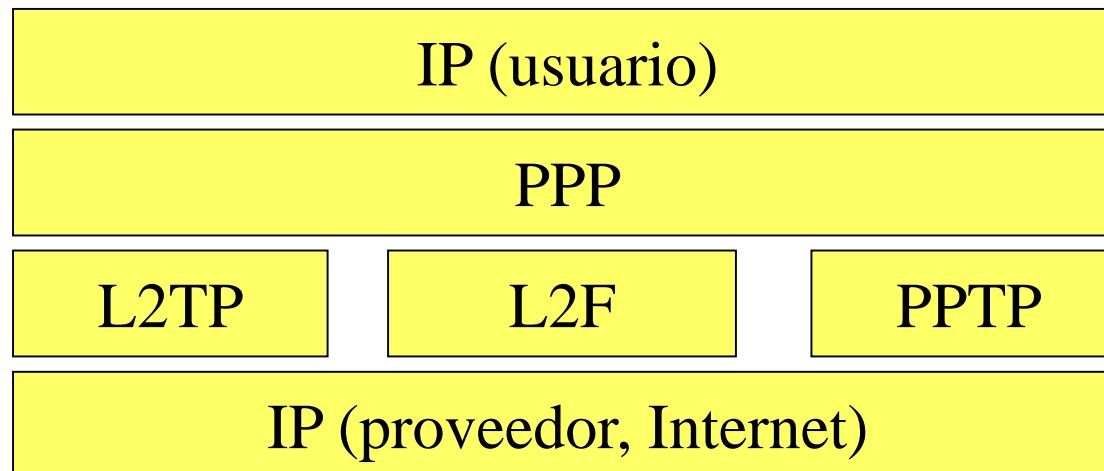
- ◆ Con IP tunneling (túneles IP sobre IP), crea una asociación permanente entre dos extremos, de modo que funcionalmente están conectados
  - Hay dos posibilidades
    - Generic Router Encapsulation (GRE), más simple y rápido
      - Permite QoS
    - IPSec, con seguridad y autenticación
      - No permite QoS, al ocultar las cabeceras originales
      - Configuración compleja
- ◆ Conexiones configuradas a mano
- ◆ Problemas de escalabilidad (en la configuración)

# Modelo Overlay (Cont.)



# Modelo Overlay, usado en la VPN de la UAH

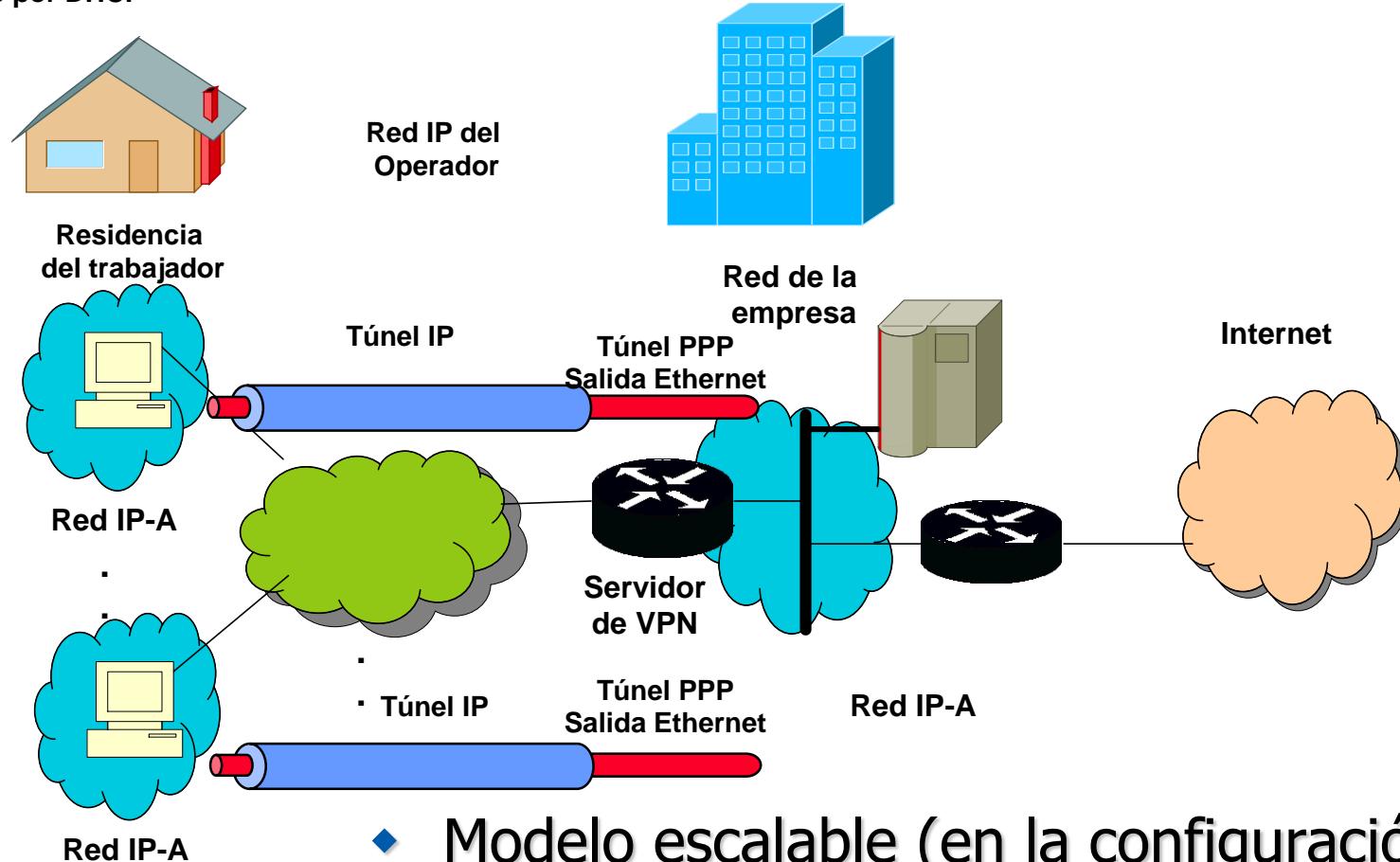
- ◆ Con envío de nivel 2
  - El tráfico IP del cliente se encapsula en tramas PPP sobre la red IP del proveedor
  - Se necesita una entidad y un protocolo para adaptar PPP a IP
    - Point to point Tunneling Protocol (PPTP), (Microsoft)
    - Layer 2 Forwarding Protocol (L2F), (Cisco)
    - Layer 2 Tunneling Protocol (L2TP), (estándar IETF)



# Modelo Overlay, usado en la VPN de la UAH

Parámetros:

Dir Servidor, usuario+clave  
Resto por DHCP



- ◆ Modelo escalable (en la configuración)

# Introducción a las VPNs: modelo *overlay*

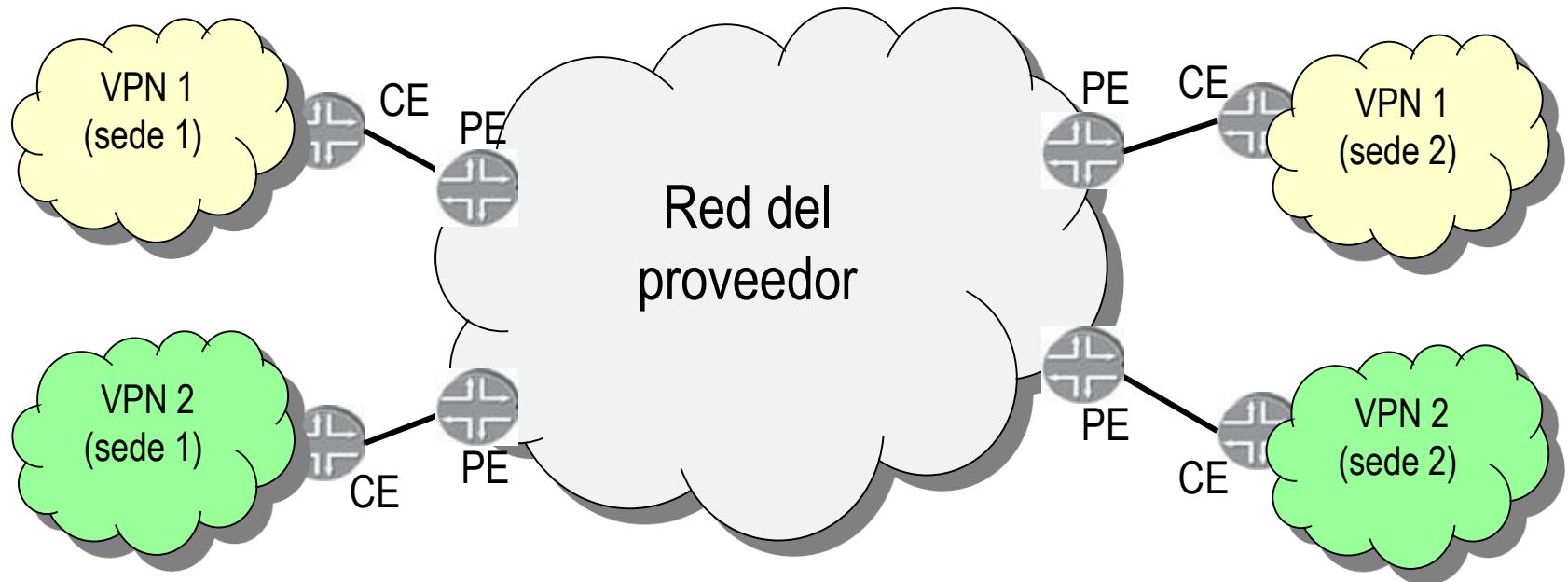


La inteligencia y el control de la VPN radica en los *routers* frontera del cliente (*routers CE*).  
CEs interconectados mediante una «malla» lógica para intercambiar información de encaminamiento.  
Requiere configuración manual.

# Introducción a las VPNs: modelo *peer*

- ◆ Los *routers CE* ya no se comunican sobre la red del operador, sino que se comunican con los routers PE (*Provider Edge*), *routers* frontera del proveedor
  - La inteligencia se traslada a los *routers PE* (controlados por el proveedor)
  - El encaminamiento entre sedes se hace de manera automática,
    - El cliente intercambia información de encaminamiento de forma transparente a través de la red del proveedor
- ◆ Cada cliente tiene un router virtual en cada PE
  - Routers del mismo cliente se comunican entre sí
  - Routers de distintos clientes no se comunican entre sí

# Introducción a las VPNs: modelo *peer*

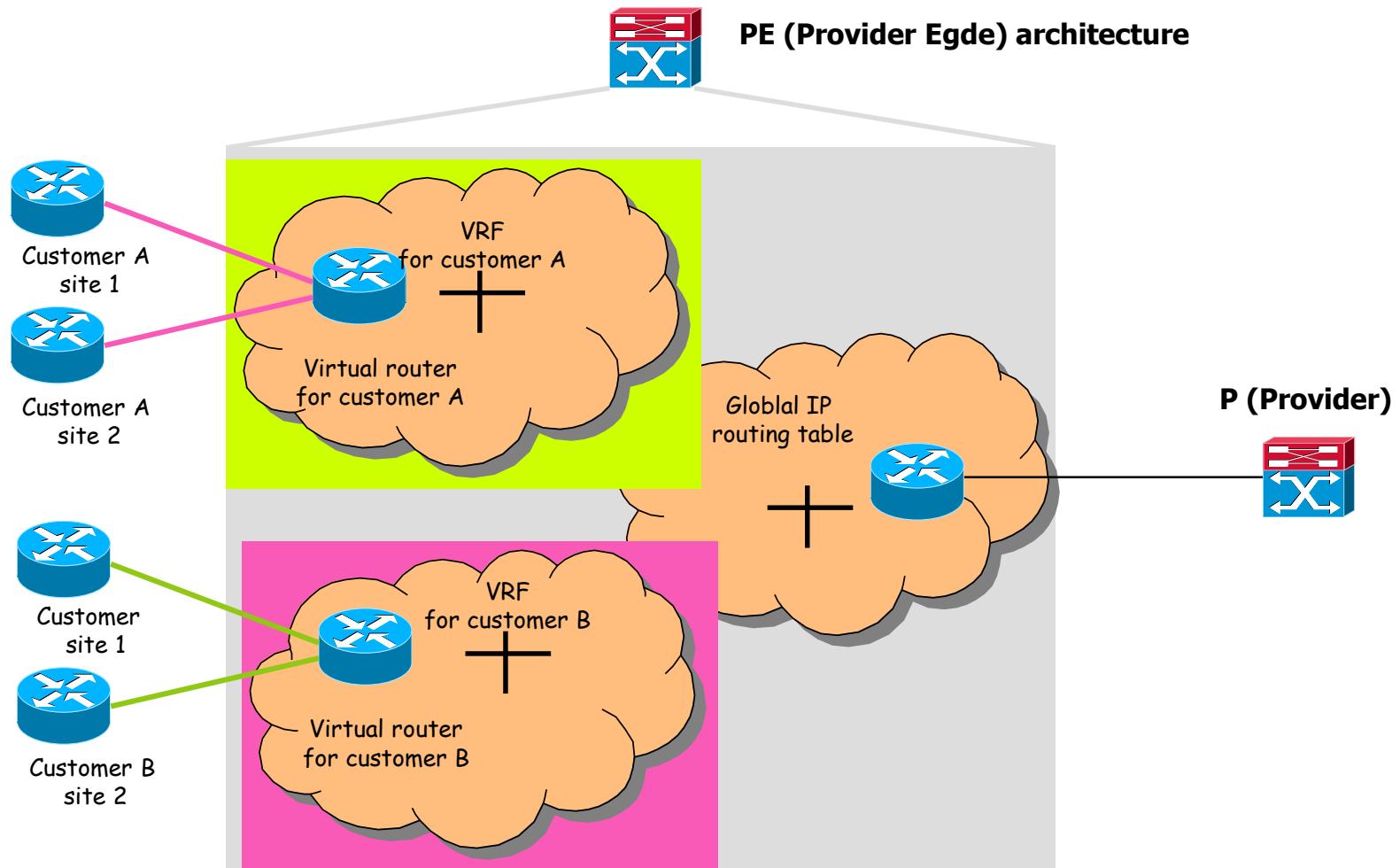


La gestión del encaminamiento entre sedes de un cliente se pasa al proveedor.  
La inteligencia se traslada a los *routers PE*, que intercambiar información de encaminamiento  
a través de la red del proveedor.  
Los *routers CE* interactúan sólo con los *routers PE*.

# MPLS VPNs: VRFs

- ◆ Aislamiento de tráfico: un cliente de una VPN no debe poder enviar tráfico a otra VPN
- ◆ Para aislar tráfico entre cliente, **NO** se puede usar **una sola** tabla de reenvío en un PE ya que:
  - Dos clientes pueden usar el mismo direccionamiento privado (típicamente 10.0.0.0)
  - Distintos clientes podría comunicarse entre sí
- ◆ SOLUCIÓN: usar una tabla de encaminamiento y reenvío para cada VPN: **VRF** (*per-VPN Routing and Forwarding table*)
  - ¿Cómo saber qué VRF utilizar cuando llega un paquete IP de un cliente?
    - Asociar cada interfaz con una VRF
    - Uso de interfaces lógicos por escalabilidad. Ej: VLANs.

# PE (Provider Egde) architecture



# MPLS VPNs: VRFs

- ◆ En el PE hay dos tipos de tablas de encaminamiento
  - La tabla de rutas de la red MPLS, necesaria para acceder a todos los nodos del núcleo (Global routing table)
  - Una tabla por cada cliente con sede en ese PE (VRFs)

# Comparativa de VPNs: Ventajas

- ◆ Overlay VPNs
  - Bien conocido y fácil de implementar
  - Proveedor no participa en el encaminamiento del cliente
  - Aislamiento cliente-proveedor
- ◆ Peer to peer VPNs
  - Encaminamiento óptimo entre sedes del cliente
  - Fácil proveer una VPN adicional, no hay que crear nuevos enlaces
  - Creación de “circuitos virtuales” entre sedes, automática
  - Permite servicios avanzados (QoS, TE, FRR, etc.)
  - Migración sencilla
    - MPLS funciona sobre las infraestructuras de red existentes
    - Los clientes no tienen que cambiar sus routers (CE)

# Comparativa de VPNs: Inconvenientes

- ◆ Overlay VPNs
  - Creación de circuitos virtuales entre sedes y configuración de las rutas, **manuales**
  - Bajo rendimiento por las cabeceras adicionales
  - En topologías malladas, el añadir una nueva sede implica reconfigurar todos los equipos frontera
  - **No escala**
  - **Caros de configurar**
- ◆ Peers VPNs
  - Si grandes inconvenientes

# Diferencias de operación de VPNs

- ◆ Sólo consideramos el número circuitos virtuales a abrir manualmente
- ◆ Supuestos, N PEs mallados sobre núcleo ATM y K VPNs diferentes

Nuevo CV a abrir a mano		
Tipo/Incidencia	Peer to peer	Overlay
Alta o baja de sede	0	N
Alta o baja de VPN	0	$N(N-1)/2$
Alta o baja de PE	N	$[N(N-1)/2] K$

- ◆ La explicación es que MPLS utiliza los mismos circuitos virtuales, para las diferentes VPNs

# Índice

- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

# Funcionamiento de una VPN MPLS

- ◆ El principio en el que se basan las VPN MPLS es el apilar conexiones a dos niveles:
  - Conexión externa, se usa para llevar todo tráfico a la salida de la red MPLS
  - Conexión interior, se usa una conexión diferente por cliente, para no mezclar tráficos
- ◆ El tráfico de una sede se encapsula en el router frontera
  - Se identifica por el puerto de entrada, que pertenece a una VPN determinada y se envía por su conexión interior
  - En función del destino se manda también dentro de otra conexión exterior

# Funcionamiento de una VPN MPLS (Cont.)

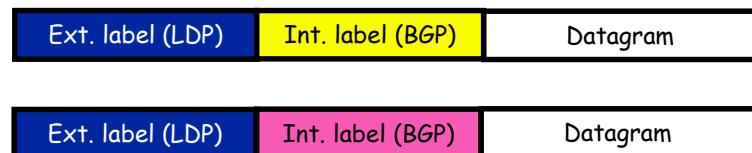
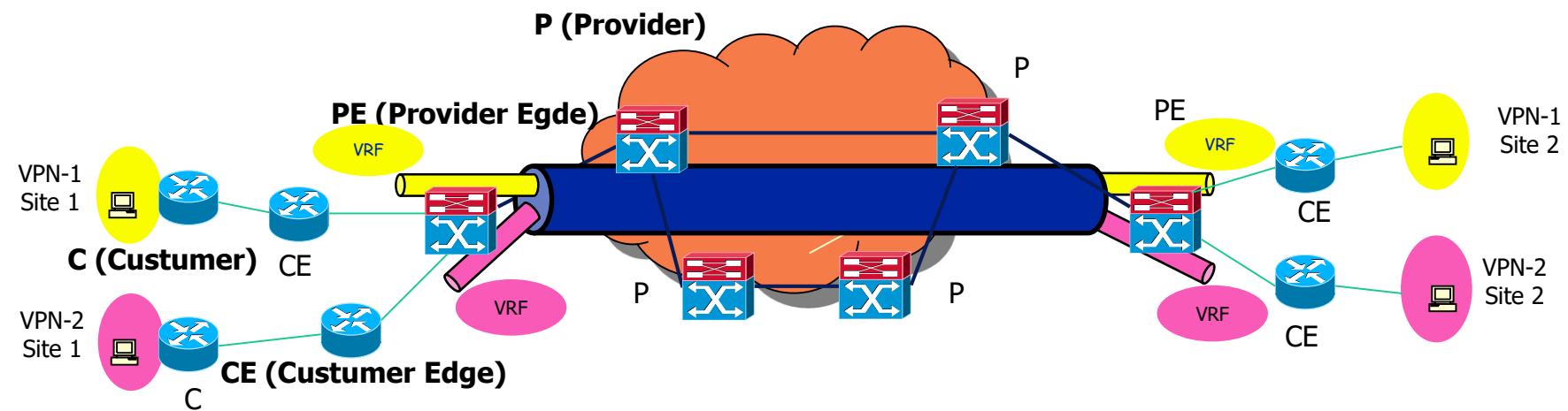
- ◆ El encaminamiento se hace en función del router e interfaz de entrada
- ◆ Esto no puede hacerse en las redes convencionales,
  - Entre por donde entre el paquete, sale por el mismo sitio
  - La “identidad” del router de entrada no viaja con el paquete (en MPLS es la etiqueta exterior)
- ◆ En VPN-MPLS la identidad de entrada del paquete se preserva
  - El router de entrada, etiqueta exterior
  - El interfaz dentro del router de entrada, etiqueta interior

# Topología VPN MPLS

 IP router

 IP/MPLS router  
ATM switch

MPLS Backbone



# Elementos de una VPN MPLS

- ◆ Routers internos MPLS (P routers)
  - Conocidos como *provider routers*
  - No mantiene ninguna tabla de rutas VPN, pero si la tabla de rutas de la red MPLS
  - Son routers LSR
  - Se conectan a los routers PE pero no a los routers de los clientes

# Elementos de una VPN MPLS (Cont.)

- ◆ Routers frontera MPLS (PE routers)
  - Conocidos como *provider edge routers*
  - Mantienen tablas de rutas VPN para las VPNs que son miembros
  - Son el interfaz con los P routers
  - Tiene una tabla de encaminamiento por cada VPN (cliente) y la tabla de rutas de la red MPLS
  - Encapsulan el tráfico para que se transmita sin que se mezcle

# Elementos de una VPN MPLS (Cont.)

- ◆ Routers frontera de clientes (CE routers)
  - Conocidos como *customer edge routers*
  - No son routers MPLS
  - Cada sitio debe acceder al PE por un solo CE
  - Los CE nunca se conecta directamente a los P routes
- ◆ Routers cliente (C routers)
  - Conocidos como *customer routers*
  - No soportan MPLS
  - Se conecta a los CE usando el encaminamiento IP normal

# Funcionamiento de una VPN MPLS (Cont.)

- ◆ El datagrama IP enviado por un CE al PE, se identifica como perteneciente a una VPN por el puerto de entrada
  - Se debe configurar a qué VRF (VPN) pertenece cada interfaz, comando
    - ip vrf forwarding VPN1
- ◆ Cada VPN tiene una tabla de encaminamiento virtual
  - Se denominada VRF (*per-VPN Routing and Forwarding table*)
  - Contiene las redes IP de esa VPN
  - Está presente en todos los PEs donde hay sedes de esa VPN
- ◆ El datagrama recibido con la dirección IP destino consulta su VRF, de donde se obtiene
  - La dirección IP de PE de salida para llegar a ese destino
  - La etiqueta de **interior** (BGP), con la que viajará el datagrama por la red MPLS
  - Esta etiqueta valdrá para saber en el PE de salida, a qué VPN pertenece el datagrama

# Funcionamiento de una VPN MPLS (Cont.)

- ◆ Posteriormente, se consulta la tabla de envío, necesaria para tomar el LSP que va al router PE de salida
  - De esta consulta se obtiene la **etiqueta exterior** (LDP o RSVP) y el interfaz de salida
- ◆ El router PE apila estas dos etiquetas y manda el mensaje por la red MPLS
- ◆ Los routers P examinan sólo la etiqueta exterior, llevando el tráfico al router PE de salida
- ◆ En el router PE de salida
  - Se eliminan las etiquetas, pero antes se toma la etiqueta de bajo nivel, que indica la VPN del datagrama
  - Se consulta con la dirección destino IP, la correspondiente VRF
  - Se retransmite (a nivel IP) para alcanzar el destino

# Índice

- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

# Distribución de rutas restringida con BGP

- ◆ Características de BGP que lo hacen adecuado para transportar rutas VPN:
  - Tiene soporte para filtrado de rutas usando **RT**
  - Puede intercambiar información **entre routers que no están directamente conectados**, permitiendo que el intercambio de rutas se haga entre *routers* PE únicamente
    - BGP abre una conexión TCP entre dos routers IP (sesión BGP)
    - Debe configurarse en cada PE a mano abrir esta sesión BGP
  - Puede transportar información de etiquetas (**Interior labels**) asociadas con rutas
  - Soporta múltiples familias de direcciones (**RD**)
  - Puede funcionar a través de varios operadores

# **RD, solape de direcciones**

- ◆ El direccionamiento de diferentes sedes de distintos clientes puede coincidir
  - No es recomendable (gestión, fusiones, etc)
  - Muy probable que suceda
- ◆ Problema al enviar el prefijo IP a otros PEs, no se puede distinguir
- ◆ La propagación de la ruta con BGP, se hace así:
  - Al llegar el prefijo IP, BGP lo compara con el resto de destinos que tiene
    - Si es nuevo, lo almacena en la VRF correspondiente
    - Pero si ya existe, se queda con sólo la ruta con menor coste, perdiéndose una ruta de cliente

# **RD, Solape de direcciones (Cont.)**

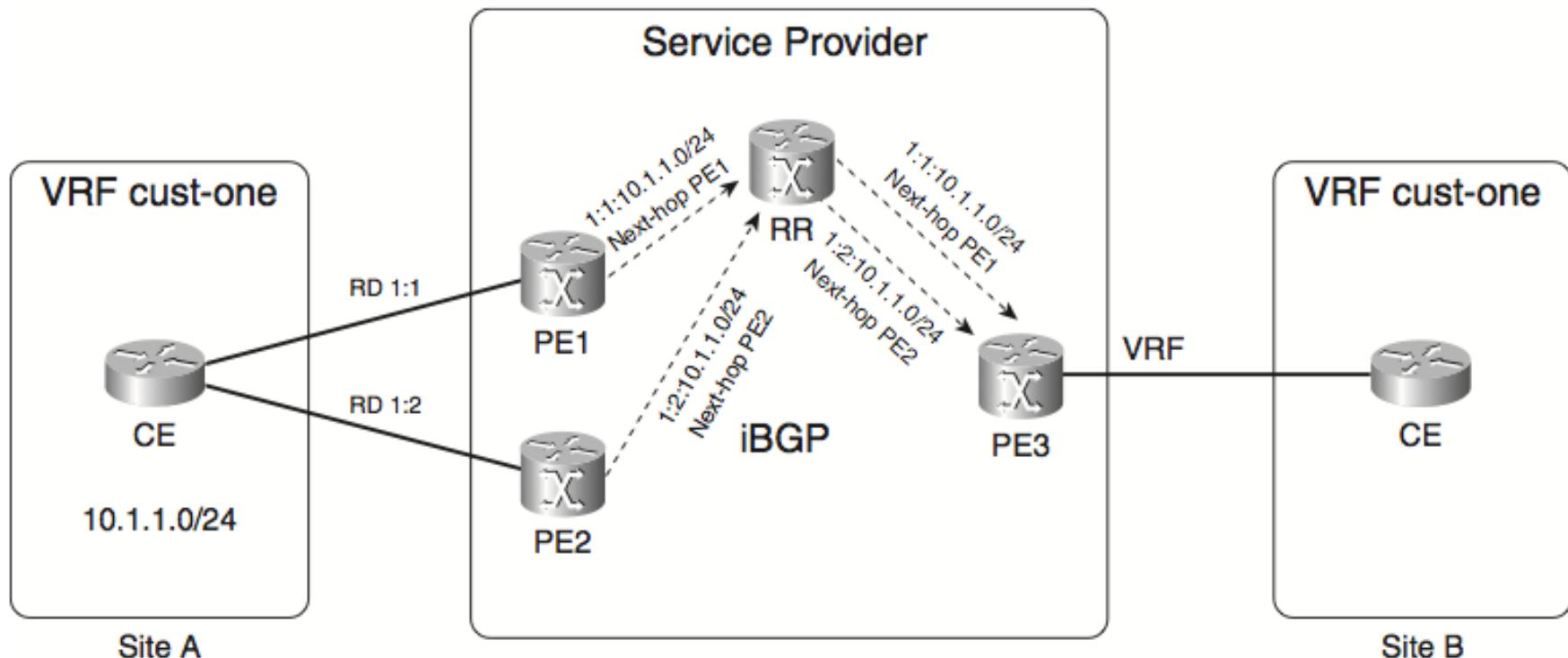
- ◆ Solución, extender la dirección:
  - Añade a la dirección de red IPv4 un prefijo de VPN
  - Es el llamado Router Distinguish (**RD**)
  - Cada VPN tiene un identificador diferente, RD distinto
  - Ahora la dirección de red de una sede es
    - $\text{VPNv4(96 bits)} = \text{IPv4(32 bits)} + \text{RD (64 bits)}$
- ◆ An extension of BGP, Multiprotocol BGP MP-BGP, is needed for VPNv4 route distribution, (RFC 4364)
- ◆ BGP soporta una nueva familia de direcciones

# **RD, Solape de direcciones (Cont.)**

- ◆ La dirección VPN-IP solo la conocen los PE
  - Antes de anunciar una ruta VPN de un cliente en BGP, el PE añade el RD → Ruta VPN-IP
  - Cuando un PE recibe una dirección VPN-IP → Le quita el RD y queda solo la dirección IP
- ◆ El cliente no sabe el prefijo RD
- ◆ Lo habitual es que cada cliente tenga un RD para todas sus sedes, configurado en el VRF
  - No implica que se aisla el tráfico entre clientes por el RD, (se hace por RT)
  - Un cliente puede necesitar más de un RD, ejemplo siguiente diapositiva, sedes con doble conexión

# Sedes con doble conexión (dual homed)

Figure 7-16 Usage of Multiple RDs



# RT, distribución de rutas restringida

- ◆ ¿Cómo aislar las rutas de clientes diferentes entre PEs?
  - SOLUCIÓN: Filtrado de rutas
- ◆ El filtrado de rutas BGP se hace con *Route Target* (RT)
- ◆ El valor de RT se añade en el momento de exportar una ruta: *RT export*
- ◆ Para decidir en qué VRF instalar la ruta usamos *RT import*.
  - Si coincide *RT import* con *RT export* en una VRF → **añadimos** la ruta a dicha VRF (en caso contrario, se tira)
  - Los valores de RT son configurados por el administrador, son 64 bits que se suelen codificar con dos números de 32 bits, eg 62001:94 si significado especial

# RT, distribución de rutas restringida

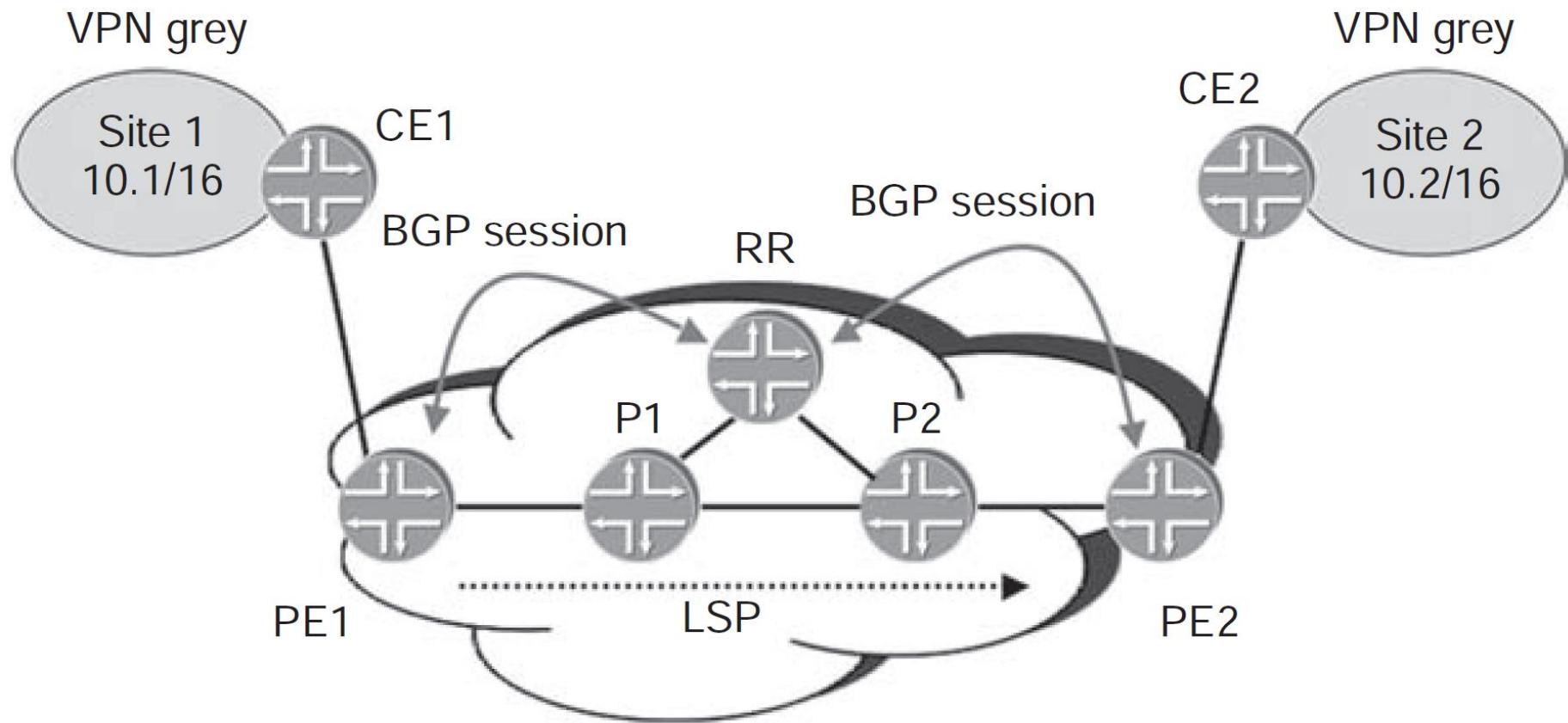
- ◆ Un PE exporta para cada VPN que tiene configurada:
  - El/los prefijo/s IP local/es
  - Selecciona la etiqueta interior con la que identifica el tráfico de cada cliente local, que le enviarán el resto de sedes
- ◆ Estas etiquetas interiores pueden ser diferentes en cada sentido de transmisión

# **RR *route reflectors* BGP**

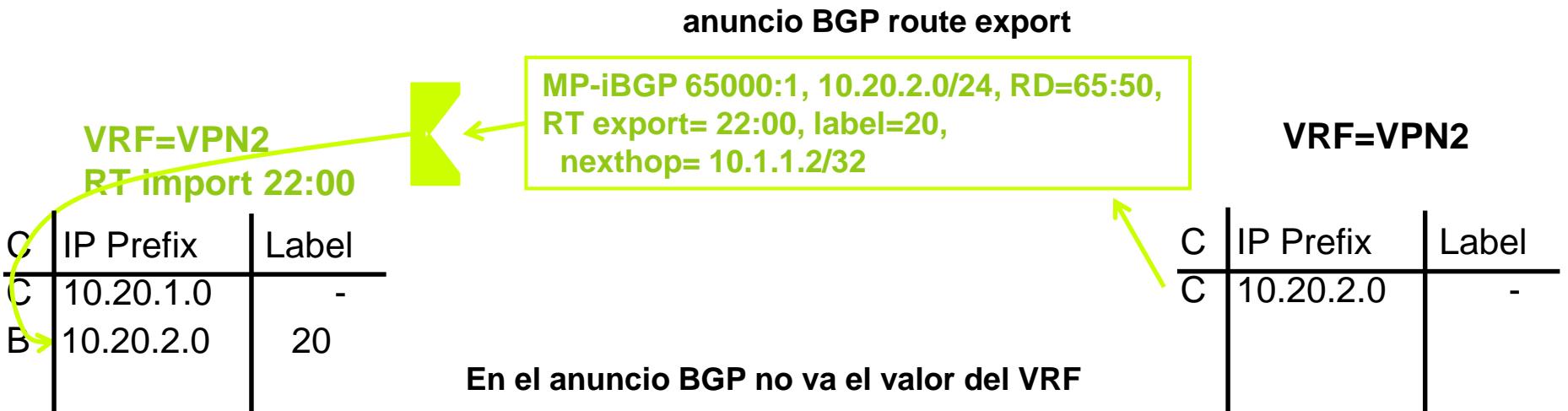
- ◆ El problema de establecer sesiones BGP entre todos los PEs es que se debe hacer a mano y no escala (es una malla)
- ◆ Los RR permiten:
  - Reducir el número de sesiones BGP
    - Un PE solo necesita hacerse una sesión a un RR, no siendo necesario hacerse *sesiones* de otros PEs
    - RR actuará como intermediario en la comunicación de rutas VPN entre PEs.
    - Cada PE mantiene un número constante de *sesiones*, independientemente del número de PEs en la red
    - Cambia la conectividad BGP a estrella, punto central el RR
  - Facilidad en la configuración
    - Añadir un nuevo PE solo implica establecer una nueva sesión BGP con el RR (no múltiples sesiones a/desde el nuevo PE)
- ◆ Los datos no se envía a través de los RR

# MPLS VPNs: *route reflectors*

- ◆ Ejemplo:



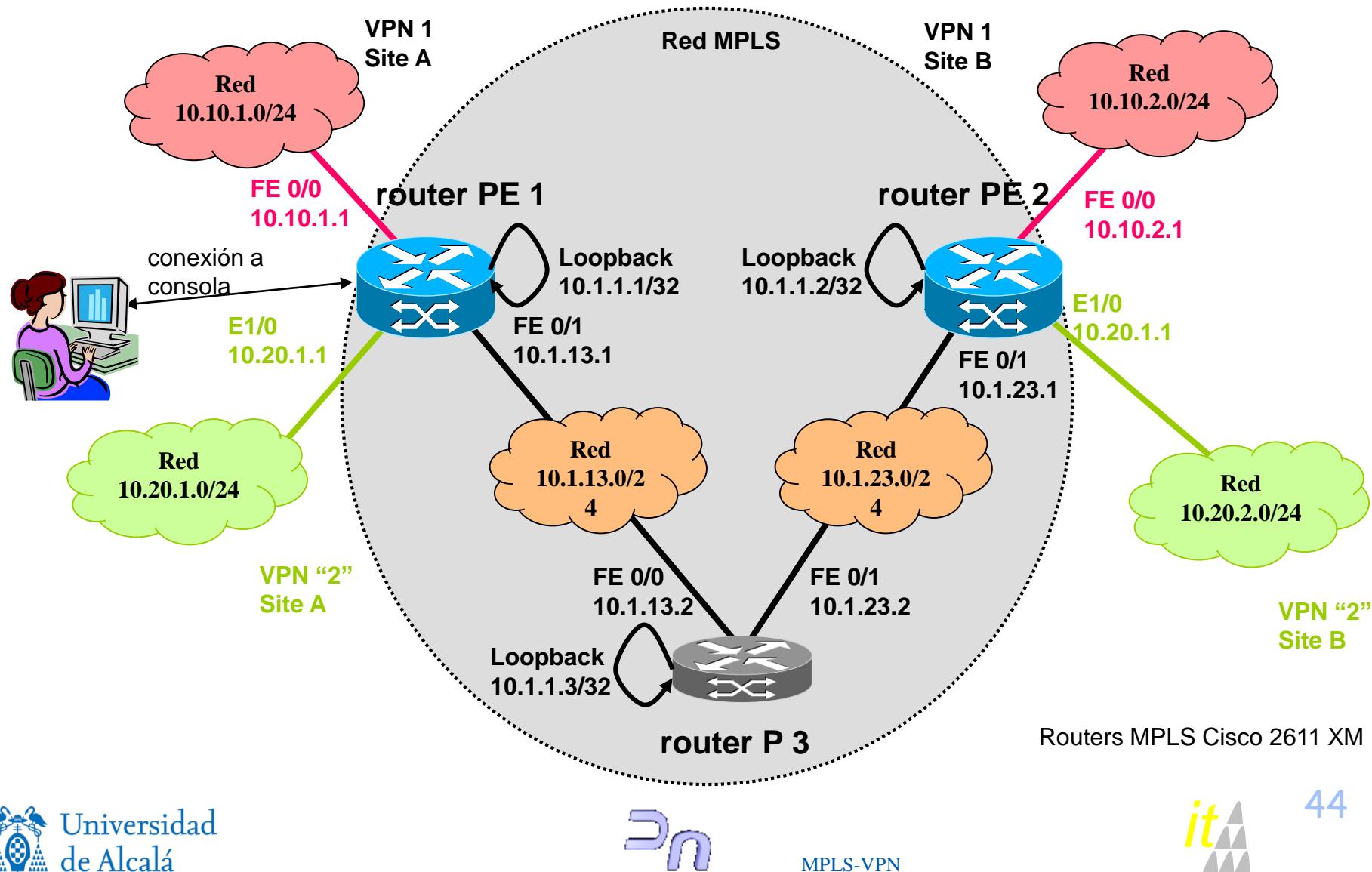
# BGP Intercambio información PEs



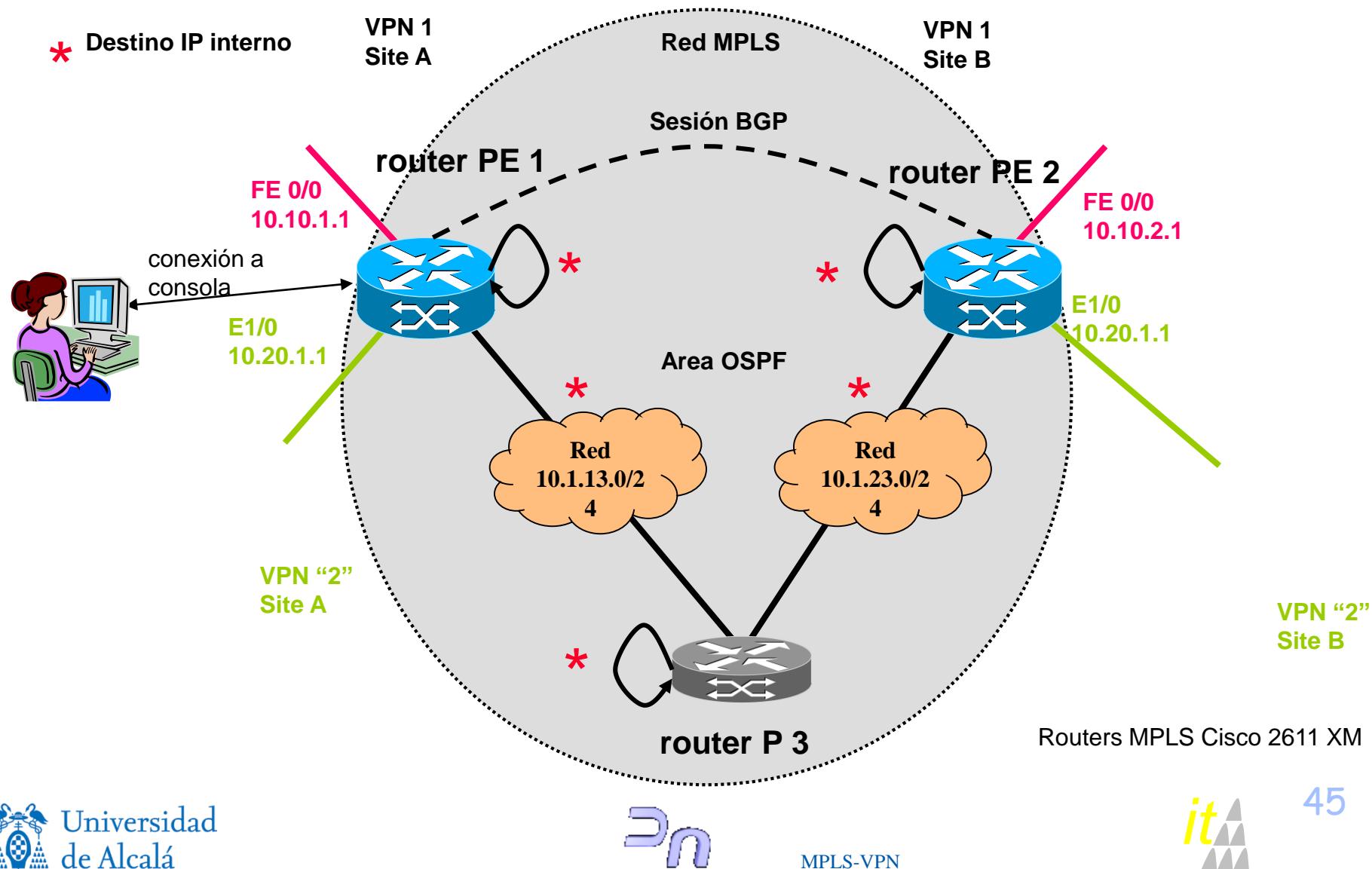
# Índice

- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

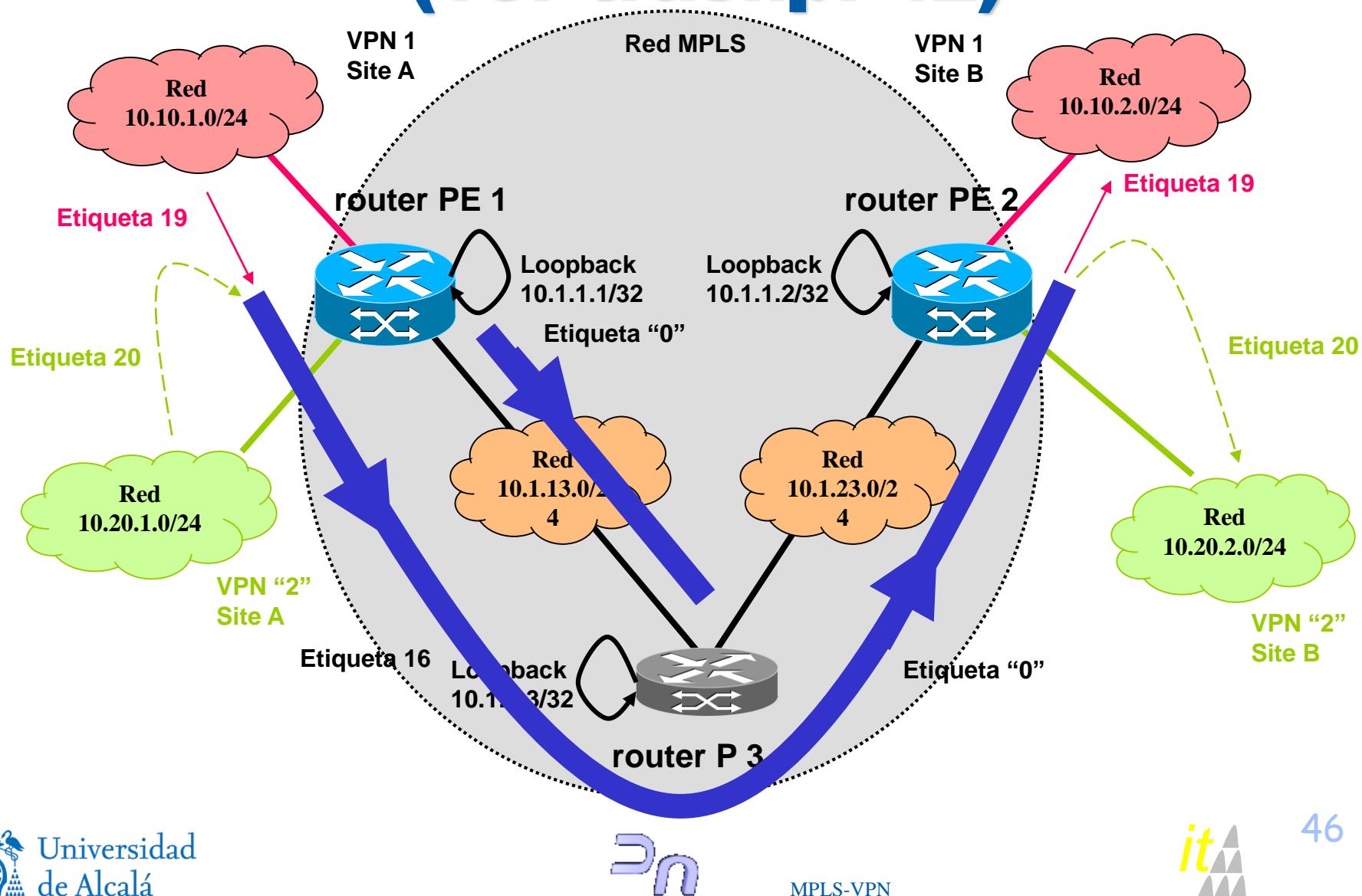
# Ejemplo de VPN, topología lógica



# Topología de encaminamiento



# Caminos etiquetados de ida (ver trasnp. 42)



# Router 1: Tablas de rutas generales

router\_1#sh ip route

Codes: **C** - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, **O** - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks

C 10.1.13.0/24 is directly connected, FastEthernet0/1

O 10.1.1.2/32 [110/3] via 10.1.13.2, 00:04:03, FastEthernet0/1

O 10.1.1.3/32 [110/2] via 10.1.13.2, 00:04:03, FastEthernet0/1

C 10.1.1.1/32 is directly connected, Loopback0

O 10.1.23.0/24 [110/2] via 10.1.13.2, 00:04:03, FastEthernet0/1

# Router 1: Tablas de las VPNs

```
router_1#sh ip route vrf VPN1
```

Routing Table: VPN1

Codes: **C - connected**, S - static, R - RIP, M - mobile, **B - BGP**

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 2 subnets

**C** 10.10.1.0 is directly connected, FastEthernet0/0

**B** **10.10.2.0 [200/0] via 10.1.1.2, 00:04:06**

```
router_1#sh ip route vrf VPN2
```

Routing Table: VPN2

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 2 subnets

**B** 10.20.2.0 [200/0] via 10.1.1.2, 00:04:09

**C** 10.20.1.0 is directly connected, Ethernet1/0

# Router 1: Tablas de envío

```
router_1#sh ip bgp vpnv4 vrf VPN1 labels
      Network          Next Hop          In label/Out label
Route Distinguisher: 65001:30 (VPN1)
  10.10.1.0/24      0.0.0.0          19/aggregate (VPN1)
→ 10.10.2.0/24      10.1.1.2          nolabel/19
```

```
router_1#sh ip bgp vpnv4 vrf VPN2 labels
      Network          Next Hop          In label/Out label
Route Distinguisher: 65001:40 (VPN2)
  10.20.1.0/24      0.0.0.0          20/aggregate (VPN2)
  10.20.2.0/24      10.1.1.2          nolabel/20
```

```
router_1#sh mpls forwarding-table
Local  Outgoing      Prefix          Bytes tag   Outgoing      Next Hop
tag    tag or VC    or Tunnel Id  switched   interface
16     0             10.1.23.0/24  0           Fa0/1        10.1.13.2
17     16            10.1.1.2/32  0           Fa0/1        10.1.13.2
18     0             10.1.1.3/32  0           Fa0/1        10.1.13.2
19     Aggregate     10.10.1.0/24 [V] 648
20     Aggregate     10.20.1.0/24 [V] 0
```

# Router 1: Comprobaciones

```
router_1#traceroute 10.1.1.2
```

Tracing the route to 10.1.1.2

```
1 10.1.13.2 [MPLS: Label 16 Exp 0] 4 msec 0 msec 4 msec  
2 10.1.23.1 4 msec * 0 msec
```

```
router_1#traceroute 10.1.1.3
```

Tracing the route to 10.1.1.3

```
1 10.1.13.2 0 msec * 0 msec
```

```
router_1#traceroute vrf VPN1 10.10.2.1
```

Tracing the route to 10.10.2.1

```
1 10.1.13.2 [MPLS: Labels 16/19 Exp 0] 4 msec 4 msec 4 msec  
2 10.10.2.1 0 msec * 0 msec
```

```
router_1#traceroute vrf VPN2 10.20.2.1
```

Tracing the route to 10.20.2.1

```
1 10.1.13.2 [MPLS: Labels 16/20 Exp 0] 4 msec 4 msec 4 msec  
2 10.20.2.1 4 msec * 0 msec
```

# Router 2: Tablas de envío

```
router_2>sh ip bgp vpnv4 vrf VPN1 labels
      Network          Next Hop          In label/Out label
Route Distinguisher: 65001:30 (VPN1)
  10.10.1.0/24      10.1.1.1        nolabel/19
  10.10.2.0/24      0.0.0.0         19/aggregate (VPN1)
```

```
router_2>sh ip bgp vpnv4 vrf VPN2 labels
      Network          Next Hop          In label/Out label
Route Distinguisher: 65001:40 (VPN2)
  10.20.1.0/24      10.1.1.1        nolabel/20
  10.20.2.0/24      0.0.0.0         20/aggregate (VPN2)
```

```
router_2>sh mpls forwarding-table
tag
Local Outgoing Prefix           Bytes tag   Outgoing   Next Hop
  tag or VC   or Tunnel Id    switched interface
16    0          10.1.1.3/32     0          Fa0/1      10.1.23.2
  17    0            10.1.13.0/24   0          Fa0/1      10.1.23.2
  18    17           10.1.1.1/32     0          Fa0/1      10.1.23.2
  19    Aggregate    10.10.62.0/24 [V]
gggregate 10.20.2.0/24[V]      528
```

# Router 2: Comprobaciones

```
router_2>traceroute 10.1.1.1
```

```
Tracing the route to 10.1.1.1
```

```
1 10.1.23.2 [MPLS: Label 17 Exp 0] 4 msec 4 msec 4 msec
```

```
2 10.1.13.1 4 msec * 4 msec
```

```
router_2>traceroute 10.1.1.3
```

```
Tracing the route to 10.1.1.3
```

```
1 10.1.23.2 4 msec * 0 msec
```

```
router_2>traceroute vrf VPN1 10.10.1.1
```

```
Tracing the route to 10.10.1.1
```

```
1 10.1.23.2 [MPLS: Labels 17/19 Exp 0] 4 msec 4 msec 0 msec
```

```
2 10.10.1.1 4 msec * 0 msec
```

```
router_2>traceroute vrf VPN2 10.20.1.1
```

```
Tracing the route to 10.20.1.1
```

```
1 10.1.23.2 [MPLS: Labels 17/20 Exp 0] 0 msec 4 msec 4 msec
```

```
2 10.20.1.1 4 msec * 4 msec
```

# Router 3: Tablas de envío

```
router_3>sh mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes switched	Outgoing interface	Next Hop
16	Pop tag	10.1.1.2/32	24881	Fa0/1	10.1.23.1
17	Pop tag	10.1.1.1/32	4867	Fa0/0	10.1.13.1

```
router_3>exit
```

# Índice

- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

# Servicios avanzados de VPN

- ◆ Además del servicio básico de conectividad, cabe plantearse otros servicios
  - QoS
  - Ingeniería de tráfico para controlar el envío del mismo
  - Comunicación punto a multipunto
  - Fiabilidad
  - Conexión entre sedes de diferentes operadores
  - Herramientas de auto comprobación

# VPNs complejas

- ◆ Por conectividad (comunicaciones permitidas en la topología)
  - Simple, todas las sedes participan en una única VPN
  - Solapadas, pudiendo participar una sede en más de una VPN
  - En estrella, todas las sedes se comunican con la central pero no entre sí
  - En estrella redundante (con dos puntos centrales)
  - Hub and Spoke, se permite el intercambio de tráfico, a través de la central entre las sedes remotas
  - VPN de gestión, para gestionar todos los PEs y Ces
  - Con doble conexión para más fiabilidad

# Índice

- ◆ Tipos de VPN de nivel 3
- ◆ Funcionamiento de VPN MPLS
- ◆ Distribución de rutas restringida (RD,RT)
- ◆ Ejemplo de VPN
- ◆ VPN avanzadas
- ◆ Modelos de conectividad VPN típicos.

# Descubrimiento de rutas: RT

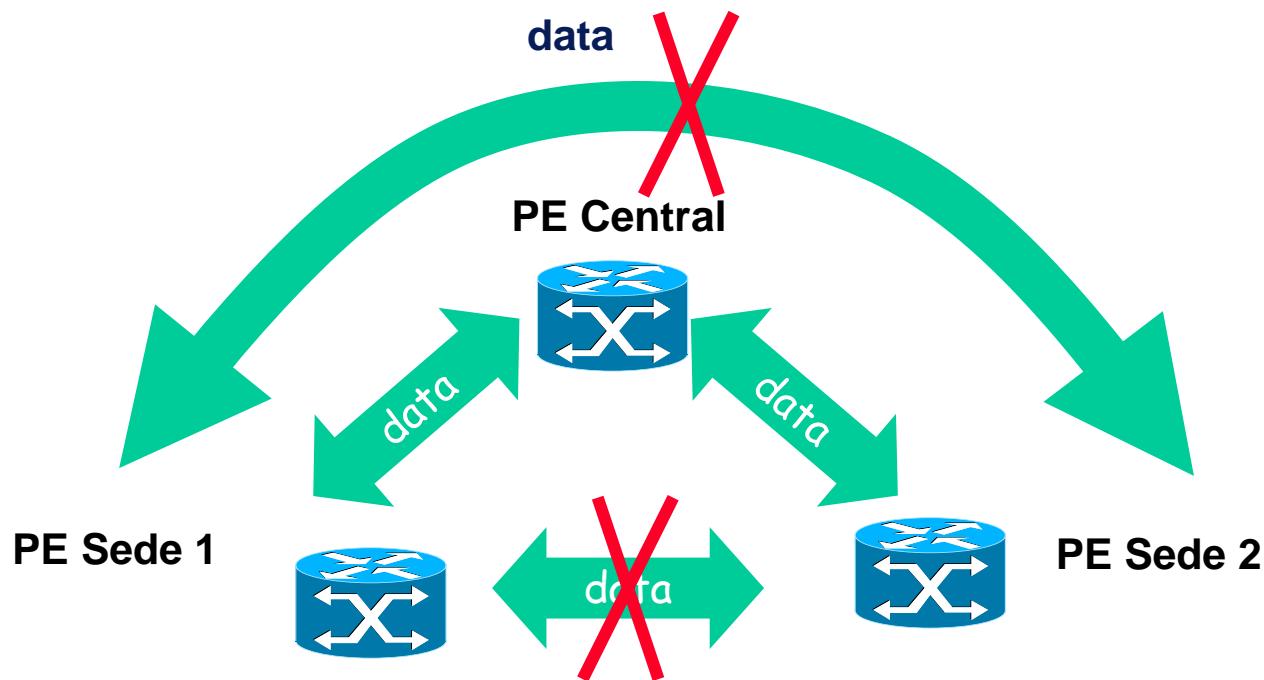
- ◆ Veremos los casos típicos, malla, estrella y hub & spoke
- ◆ Cada prefijo de sede VPNv4 es enviado por BGP con un valor de RT Export, el receptor
  - ◆ Almacena la ruta si coincide RT Export con RT Import
- ◆ Las cada cliente tiene al menos unos valores de RT para comunicar las sedes y aislarlas de las demás
- ◆ El RT puede ser visto como el identificador del cliente

# Descubrimiento de rutas: RT

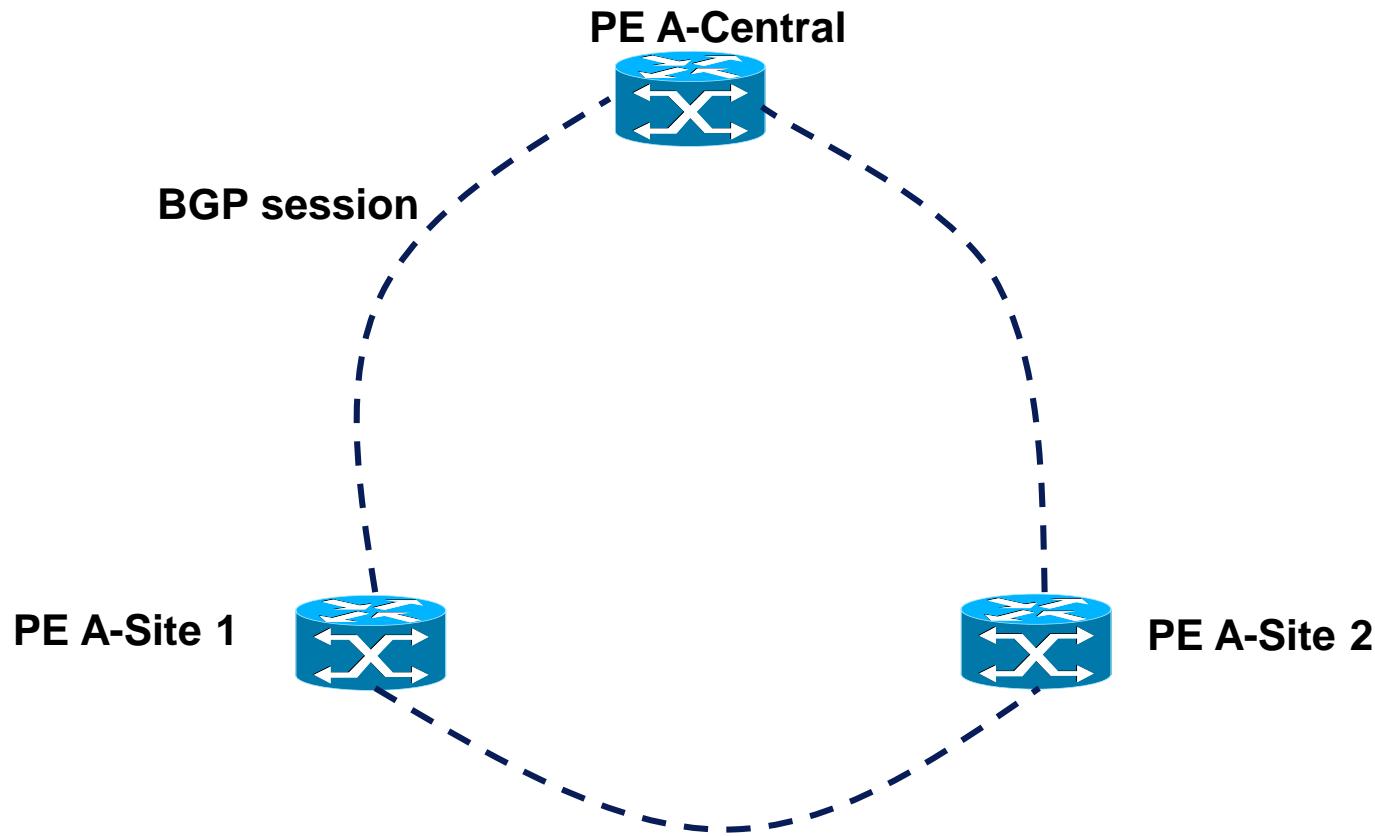
- ◆ Recordar que el administrador debe configurar
  - Los interfaces de las sedes, con sus prefijos
  - Asociar los interfaces a una VRF
  - En las VRF el
    - ◆ RT Export, que usa para las rutas que exportan
    - ◆ RT Import, para las rutas que reciben
  - El RD, uno por VRF (cliente)

# Star VPN service

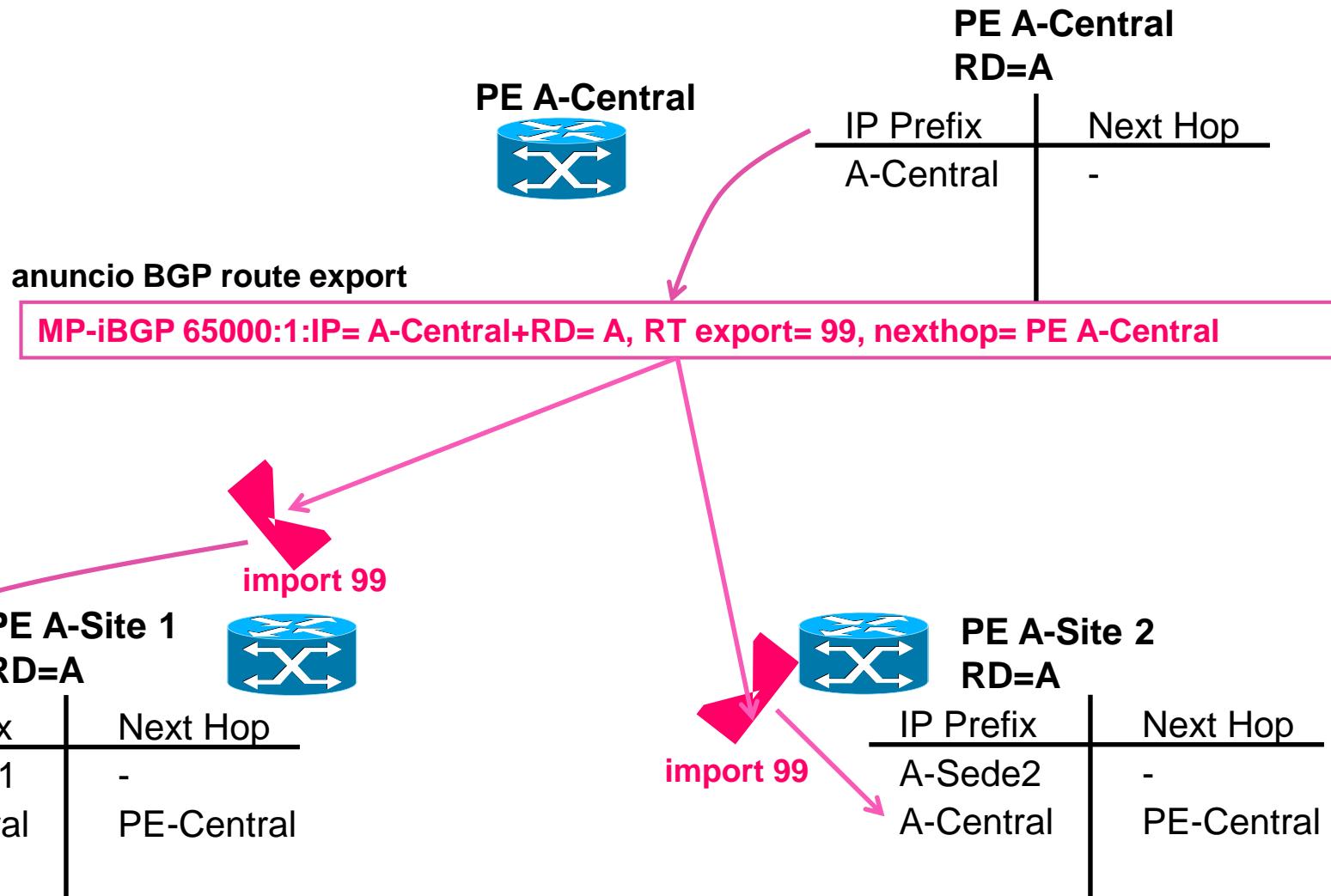
- La figura muestra la conectividad a nivel de usuario final, no de MPLS



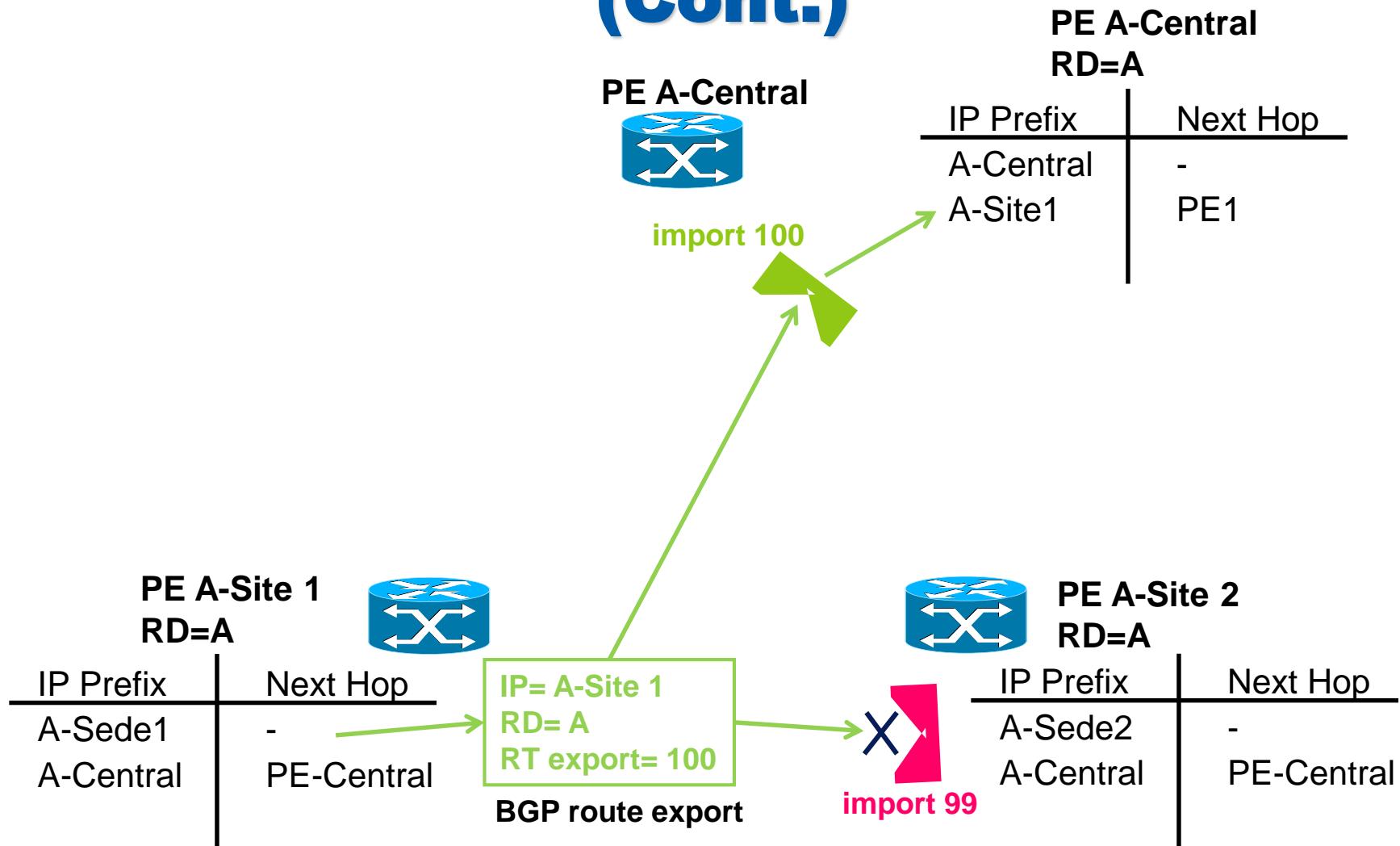
# Star VPN service: BGP topology



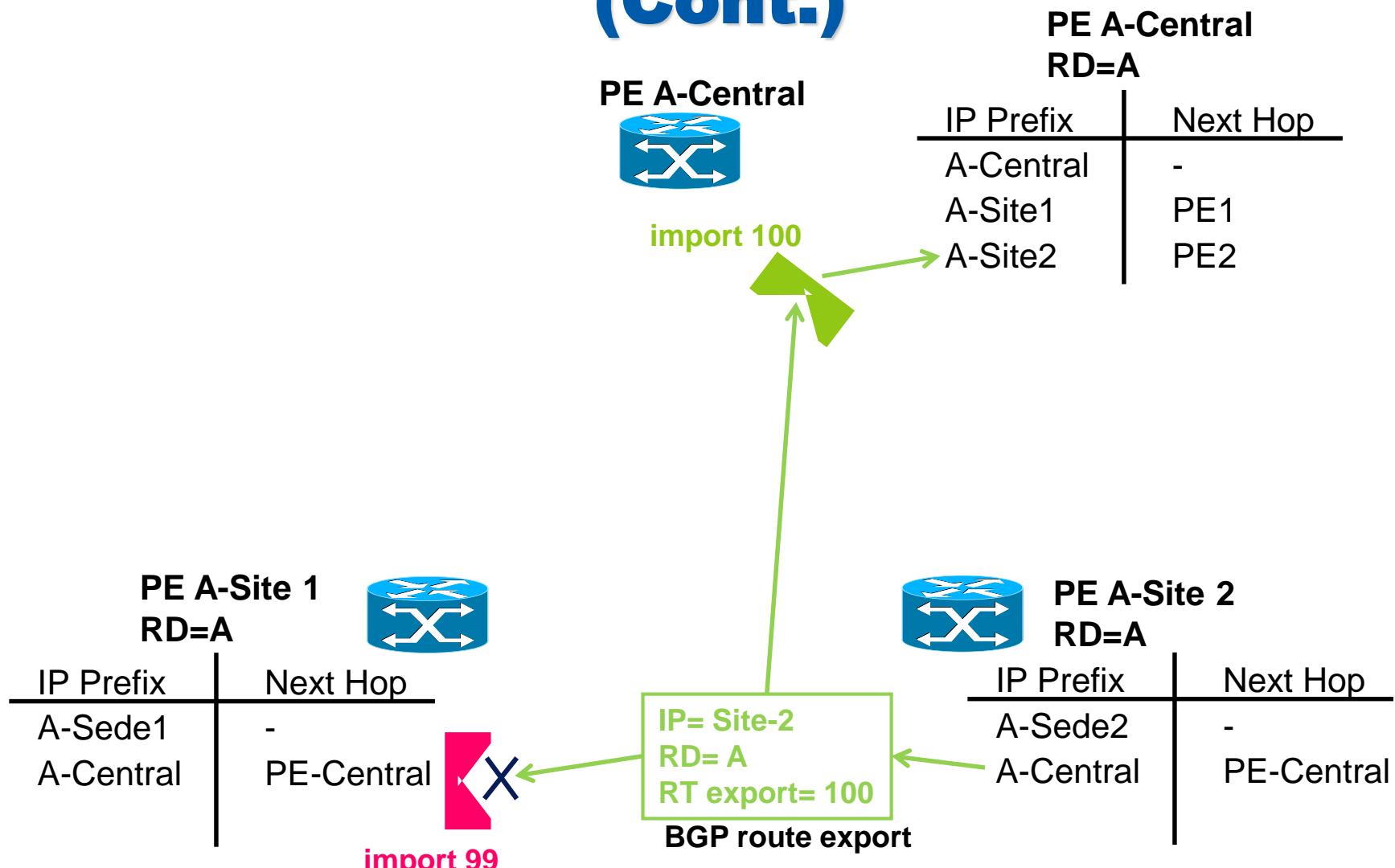
# Star service: Route distribution



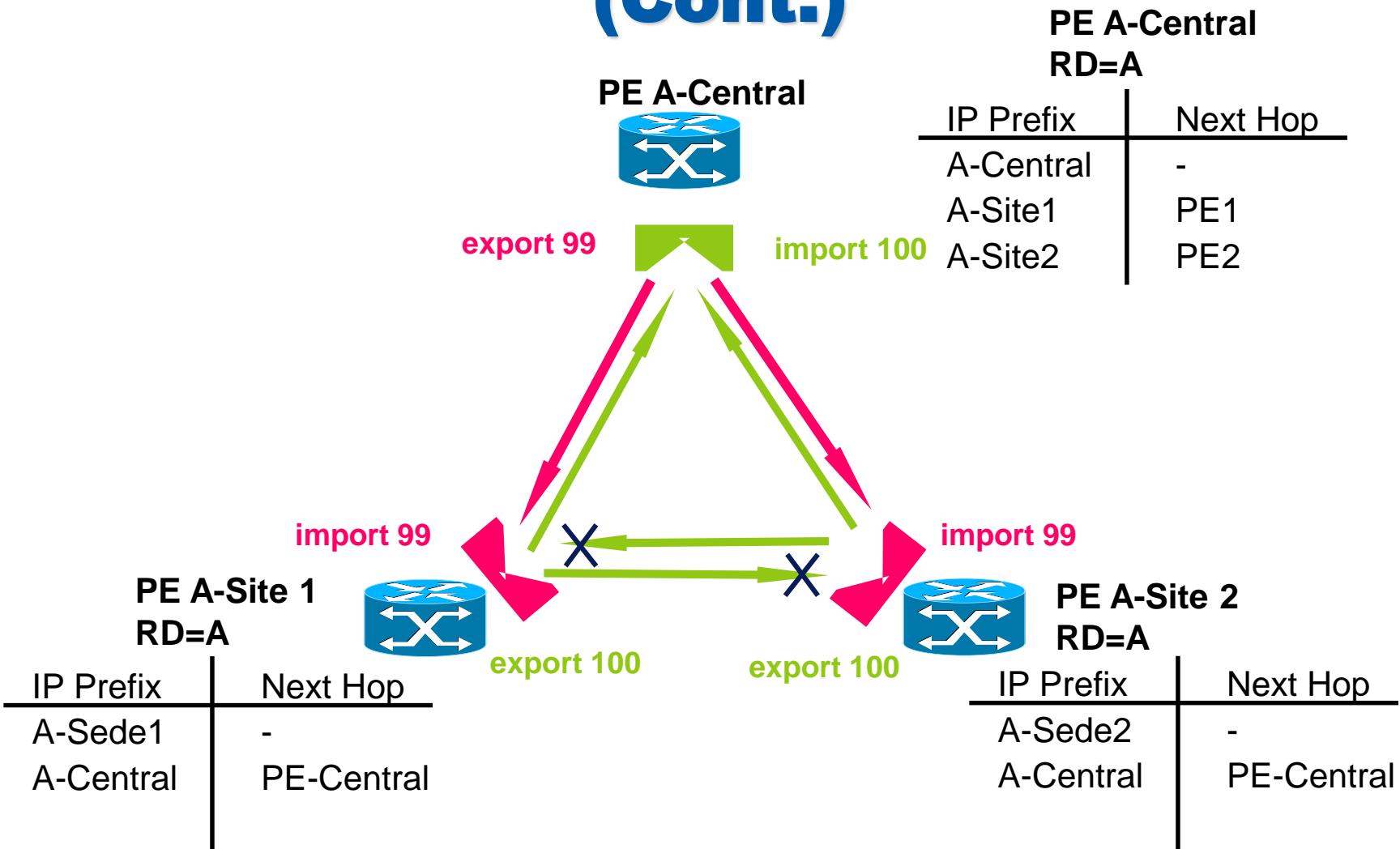
# Star service: Route distribution (Cont.)



# Star service: Route distribution (Cont.)

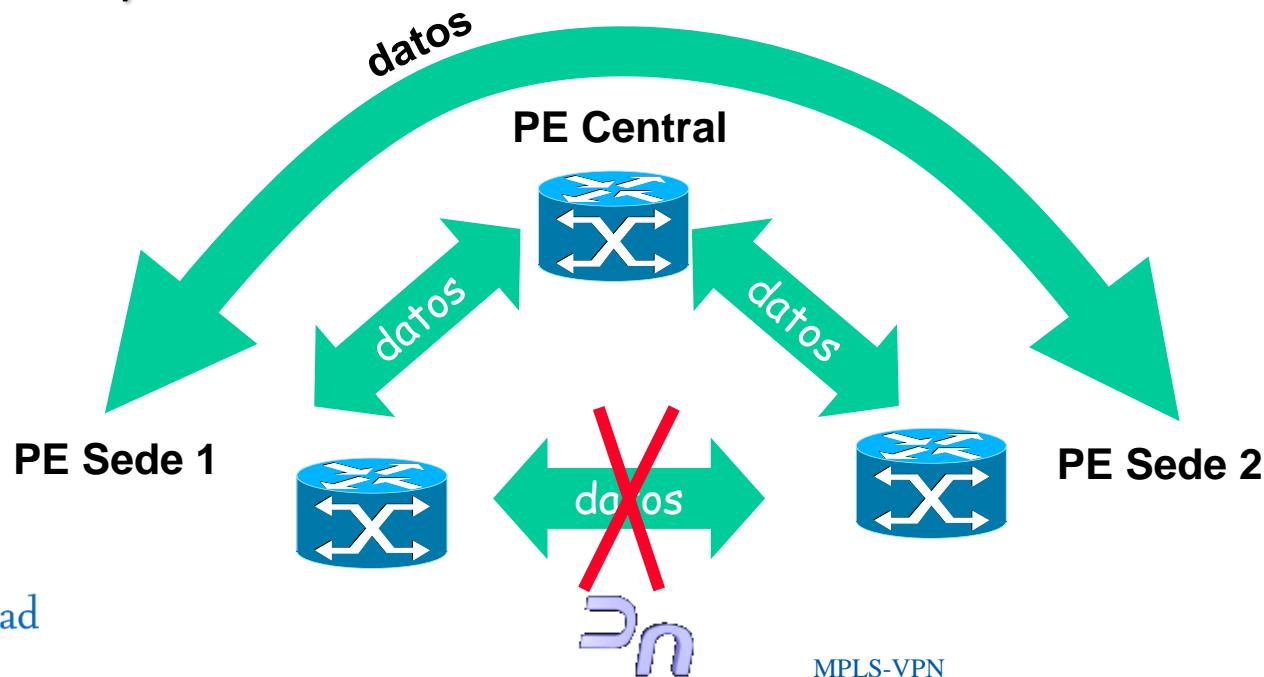


# Star service: Route distribution (Cont.)

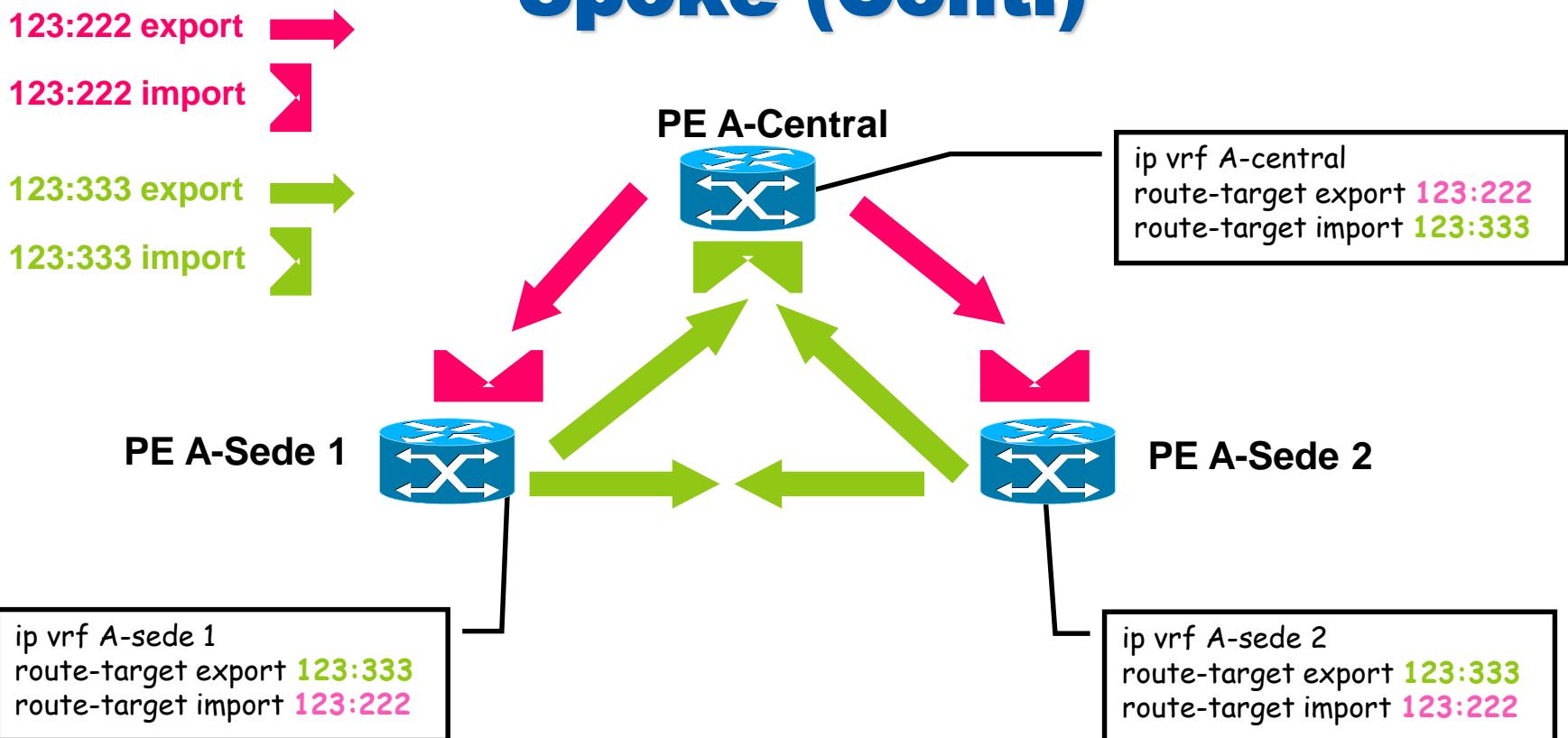


# Servicio de VPN Hub and Spoke

- ◆ Se quiere una VPN en la que las comunicaciones pasen por una sede central
  - Con las VPN sencillas no es posible ya que todos los PEs están comunicados
- ◆ La figura muestra la conectividad a nivel de usuario final, no de MPLS



# Servicio de VPN Hub and Spoke (Cont.)



# Servicio de VPN Hub and Spoke (Cont.)

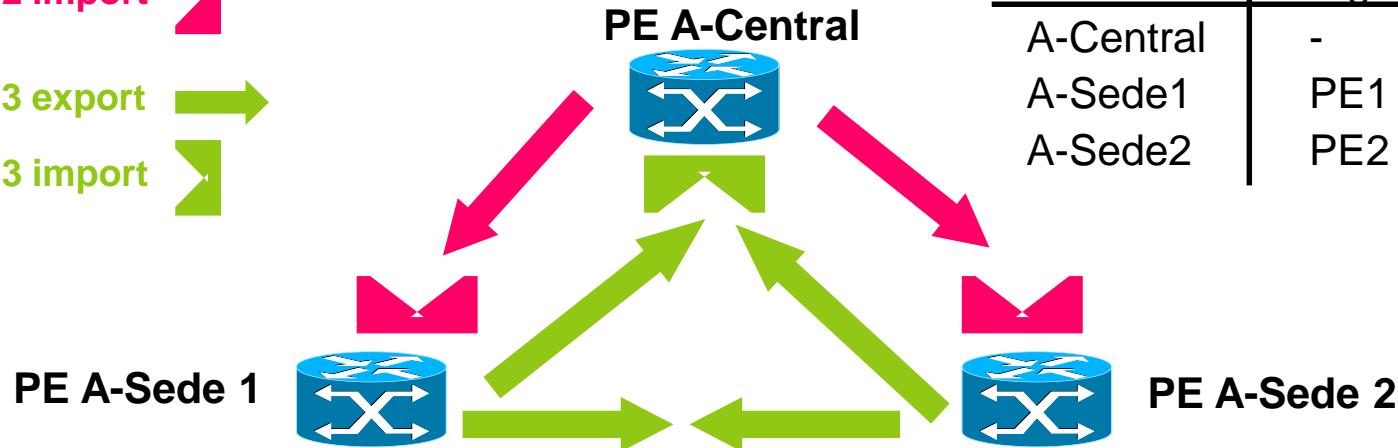
- ◆ Retransmisión de rutas BGP dentro de un operador
  - Se hacen por iBGP (internal BGP)
  - Sólo se transmiten las rutas locales a una VRF (de un PE), con el/los atributo/s RT Export de la/s VRF/s
  - Las rutas aprendidas (de otros PEs), no se reenvía
- ◆ En la tabla VRF hay dos tipos de entradas
  - Locales, aprendidas por el nombre de la VPN (configurado en la VRF y en el interfaz)
  - Remotas, introducidas por BGP

# Servicio de VPN Hub and Spoke (Cont.)

- ◆ En el ejemplo, la Central no propaga las rutas de las sedes
- ◆ Para que las sedes se comunique a través de la central hay varias opciones, basadas en una ruta que exporta la Central para que sea importada por las otras sedes, opciones:
  - Que sea la ruta por defecto
  - Que sea una ruta estática que englobe a las redes IP de las sedes
  - Lo mismo de punto anterior, pero en varias rutas
- ◆ Para convertir esta configuración al servicio de VPN en estrella, no se exporta la ruta anterior

# Servicio de VPN Hub and Spoke (Cont.)

123:222 export →  
 123:222 import ↘  
 123:333 export →  
 123:333 import ↘



Destino	Sig. Salto
A-Central	-
A-Sede1	PE1
A-Sede2	PE2

Destino	Sig. Salto
A-Sede1	-
A-Central	PE-Central
default	PE-Central

Destino	Sig. Salto
A-Sede2	-
A-Central	PE-Central
Default	PE-Central

# Referencias

- ◆ I. Minei, J. Lucek, "MPLS-Enabled Applications", **Capítulo 7**, John Wiley & ons, 3rd, 2011
- ◆ **De Ghein**, "MPLS Fundamentals", **Capítulo 7**, Cisco Press, 2007.
- ◆ V. Alwayn, "Advanced MPLS Design and Implementation", Cisco Press, 2001.