VPNs de capa 3 basadas en MPLS

Ingeniería de tráfico - Curso 2014-15

Área de Ingeniería Telemática - Departamento de Automática

Universidad de Alcalá

José Manuel Giménez

Aplicaciones de MPLS

- Principales aplicaciones reales de MPLS:
  - Redes privadas virtuales (VPNs):
    - L3VPN: BGP/MPLS VPNs de capa 3.
    - L2VPN: VPNs de capa 2:
      - Transporte de capa 2 sobre MPLS: VPNs punto a punto.
      - VPLS: *Virtual Private LAN Service*: VPNs punto a multipunto.
  - Ingeniería de tráfico con MPLS (TE MPLS).
    - FRR: *Fast ReRoute*.
  - Calidad de servicio (QoS) con MPLS.

VPNs basadas en MPLS

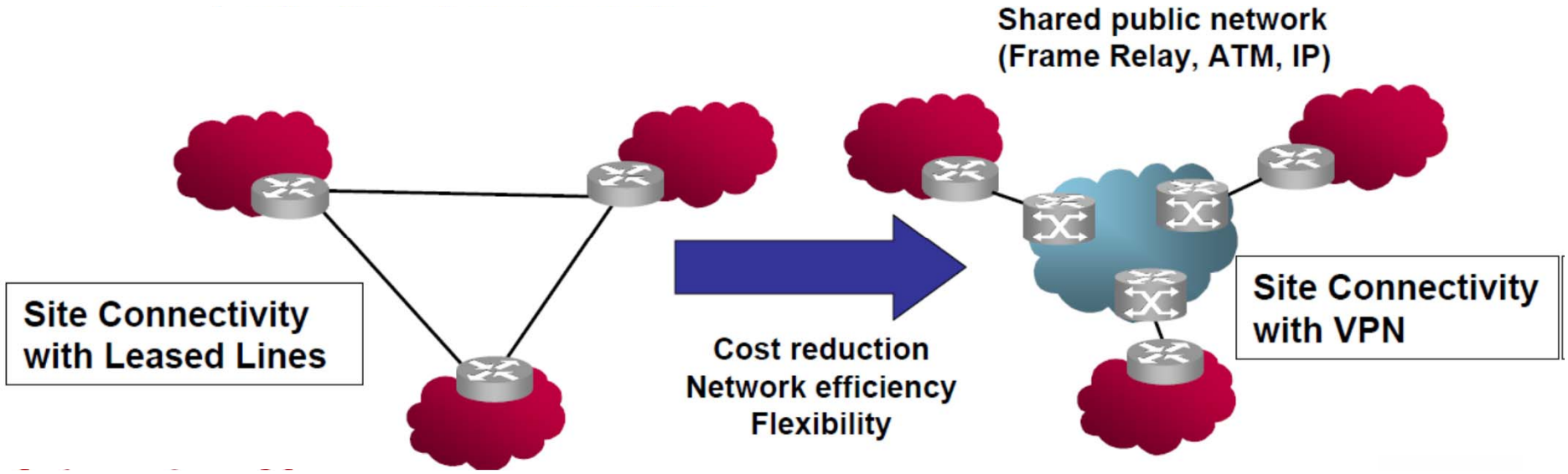
- Introducción a las VPNs:
  - Modo *overlay.*
  - Modo *peer.*
- MPLS VPNs:
  - Introducción.
  - VRFs.
  - Distribución de rutas restringida.
  - Modelos de conectividad VPN típicos.
  - Túneles MPLS.
  - Ejemplo.
  - Alternativas.
  - *Route Reflectors.*
  - Resumen.

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.

Introducción a las VPNs: modelo *overlay*

- Antecedentes. Modelos de VPNs:
  - Modelo *overlay*.
  - Modelo *peer*.
- Modelo *overlay*:
  - Modelo VPN más intuitivo: si se busca conectividad → Conectar las sedes mediante enlaces punto a punto entre ellas.
  - 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.

Introducción a las VPNs: modelo *overlay*

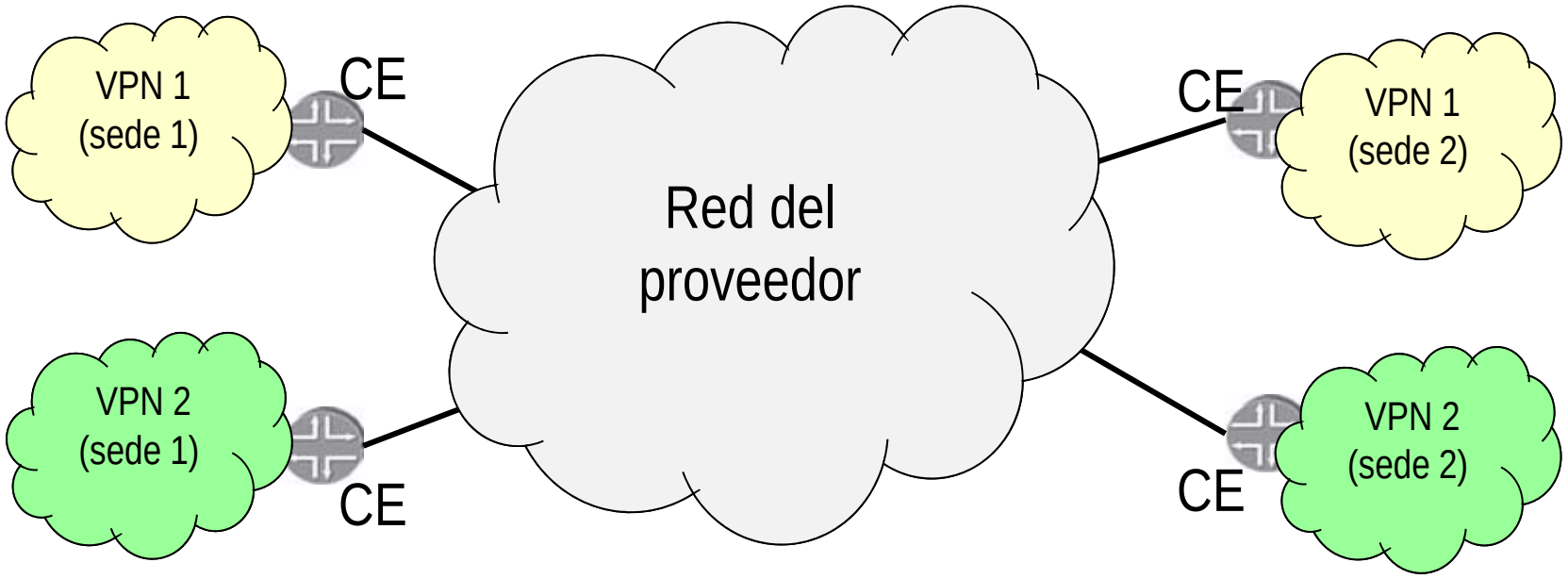
- Implementaciones del modelo *overlay*:
  - Capa 1: con conexiones del operador de capa 1: E1, STM-1… El cliente es responsable del resto de capas.
  - Capa 2: el operador proporciona conexiones de capa 2 (ATM, FR). El cliente es responsable del resto de capas.
  - Túneles IP (IP sobre IP). Tipos de túneles:
    - GRE (*Generic Router Encapsulation*):
      - Simple, rápido y permite QoS.
    - IPSec (*IP Security*):
      - Seguridad y autenticación, aunque no permite QoS al ocultar las cabeceras originales. Configuración compleja.

Introducción a las VPNs: modelo *overlay*

- La inteligencia está en los *routers* CE:
  - En la sede del cliente.
  - Requiere conocimientos por parte del cliente.
  - Si el cliente traspasa la gestión al operador, el operador debe gestionar muchos CE en "casa" del cliente → Problemas de escalabilidad.
- Cada vez que se añade una sede hay que:
  - Conectarla con el resto de sedes…
  - … y configurar el resto de sedes para conectarlas con la nueva.

  → Más problemas de escalabilidad.

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.

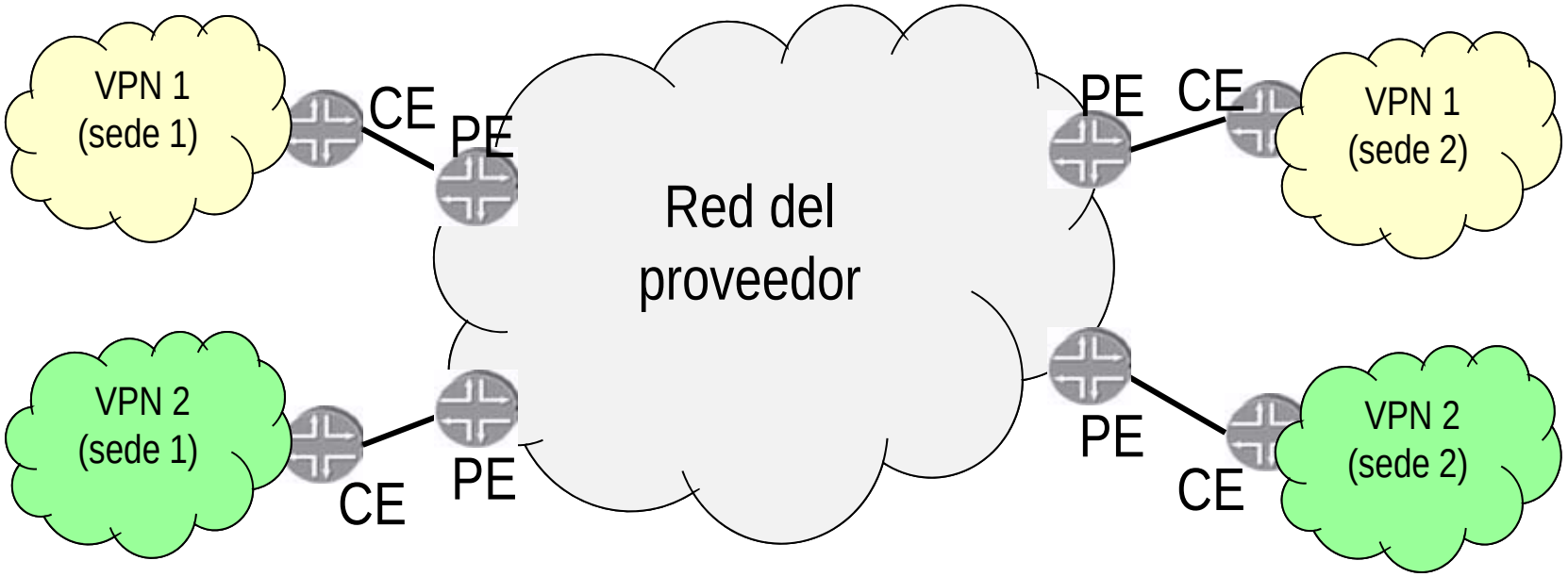
Introducción a las VPNs: modelo *peer*

- Los *routers* CE ya no se comunican sobre la red del operador, sino que se comunican con los routers PE:
  - PE: *Provider Edge*, *routers* frontera del proveedor.
  - No es necesaria la gran cantidad de *peerings* entre CE que requiere el modelo *overlay*.
  - Para el cliente, el encaminamiento se vuelve muy sencillo.
  - La inteligencia se traslada a los *routers* PE → PE-VPNs.

Introducción a las VPNs: modelo *peer*

- Pasar de CE-VPN a PE-VPN tiene las siguientes ventajas:
  - Añadir una sede a una VPN requiere únicamente cambios en el CE y su PE asociado (no del resto de sedes).
  - El número de dispositivos inteligentes que toman decisiones de encaminamiento no se incrementa necesariamente al añadir una nueva sede.
  - Encaminamiento simple desde el punto de vista del CE.
    - Cada CE anuncia al PE información de alcanzabilidad para los destinos de la sede a la cual pertenece CE.
    - Se asegura un encaminamiento óptimo entre CEs puesto que los protocolos de encaminamiento del proveedor aseguran el encaminamiento óptimo entre PEs.
  - Cada sede puede ejecutar diferentes protocolos de encaminamiento.

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.

Introducción a las VPNs: modelo *peer*

- Por tanto, el modelo *peer* es atractivo pero en los PE falta aislar el tráfico entre VPNs.
  - Se consigue haciendo que cada cliente tenga su PE virtual.
  - Cada PE virtual solo acepta rutas de la VPN a la que sirve.
    - Se consigue mediante el concepto de comunidades BGP.
- Consecuencias en el núcleo de la red:
  - Puesto que se basa en el reenvío IP:
    - Se impide el uso de direcciones IP privadas.
    - No se puede usar ruta por defecto porque no se pueden diferenciar las de distintos clientes.
    - Escalabilidad limitada porque todos los *routers* del núcleo (routers P, *Provider routers*) deben ser capaces de encaminar.
  - Solución: uso de túneles.

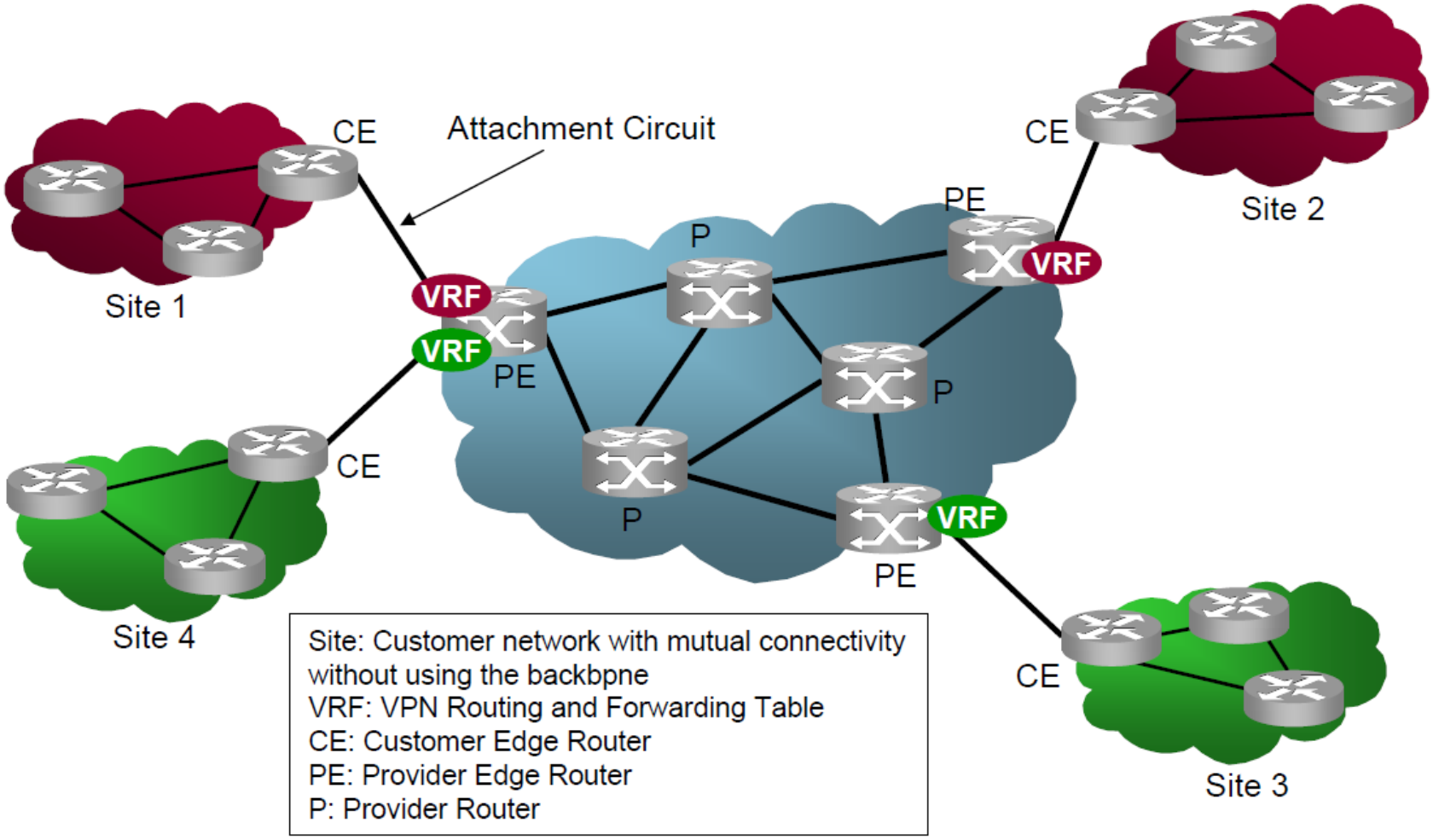
MPLS VPNs: introducción

- MPLS VPNs (BGP/MPLS VPNs) se basan en el modelo *peer*.
  - Encaminamiento sencillo para el cliente.
  - Fácil añadir nuevas sedes a una VPN.
  - MPLS provee los túneles para el núcleo de la red.
- Interconexión de sedes de cliente mediante transporte de PDUs de capa 3 sobre infraestructura MPLS de proveedor.
- Estandarizado en RFC 4364.
- Objetivos:
  - Aislamiento de tráfico entre diferentes VPNs.
  - Conectividad entre sedes de cliente.
  - Uso de direcciones privadas entre cada sede.

MPLS VPNs: VRFs

- Aislamiento de tráfico: un cliente de una VPN no debe poder enviar tráfico a otra VPN.
- Si se usa una tabla de reenvío única en un PE:
  - Dos sedes no pueden usar el mismo direccionamiento privado.
  - Un cliente puede enviar tráfico a la otra simplemente usando esa dirección destino.
  - 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: CV (ATM o FR) o VLANs.

MPLS VPNs: VRFs



- Todavía se puede enviar información entre VPNs.

MPLS VPNs: distribución de rutas restringida

- ¿Cómo restringir la distribución de rutas?
  - Ejecutar una instancia del protocolo de encaminamiento para cada VPN no es escalable → Solución descartada.
  - Transportar todas las rutas VPN con un único protocolo de encaminamiento en la red del proveedor y restringir la distribución de alcanzabilidad de VPN en los PEs → Solución escogida.
- Se emplea BGP como protocolo para transportar rutas VPN.

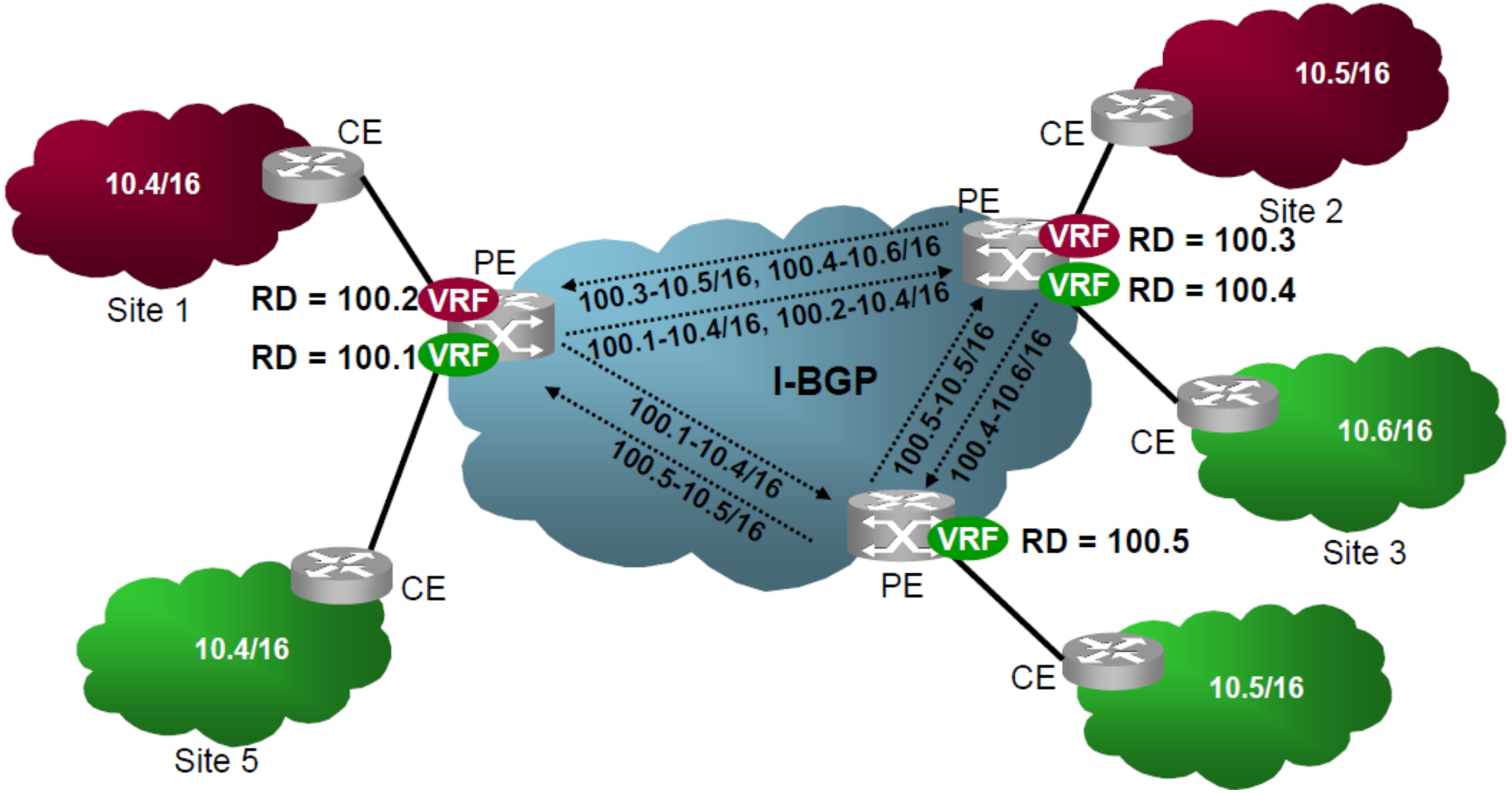
MPLS VPNs: distribución de rutas restringida

- Características de BGP que lo hacen adecuado para transportar rutas VPN:
  - Tiene soporte para filtrado de rutas usando el atributo “comunidad”.
  - Tiene soporte para un conjunto rico de atributos, permitiendo el control del punto de salida de encaminamiento preferido.
  - Puede transportar un número muy grande de rutas de clientes.
  - Puede intercambiar información entre *routers* que no están directamente conectados, permitiendo que el intercambio de rutas se haga entre *routers* PE únicamente.
  - Puede transportar información de etiquetas asociadas con rutas.
  - Soporta múltiples familias de direcciones.
  - Puede funcionar a través de varios operadores.

MPLS VPNs: distribución de rutas restringida

- Carencia de BGP para transportar rutas VPN:
  - Solo puede instalar y distribuir una ruta para un prefijo dado: problema para el mismo espacio de direcciones privadas que puedan emplear varias VPN.
    - SOLUCIÓN: Crear una nueva familia de direcciones VPN-IPv4, que consiste en añadir un identificador único (RD: *Route Distinguisher*) al prefijo IP. Así, para BGP no pueden existir dos prefijos iguales pese a que dos VPNs compartan un mismo direccionamiento privado.
    - Se hace uso de la característica BGP *Multiprotocol* (MP) → Por ese motivo, en el contexto de VPNs a veces se le llama MP-BGP.
- La dirección VPN-IP solo la conocen los *routers* 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 tiene porqué conocer dicho prefijo RD.

MPLS VPNs: distribución de rutas restringida

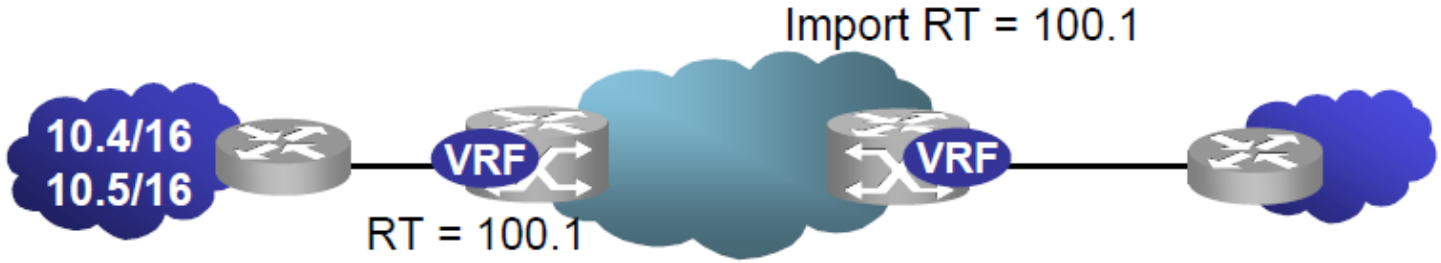


MPLS VPNs: distribución de rutas restringida

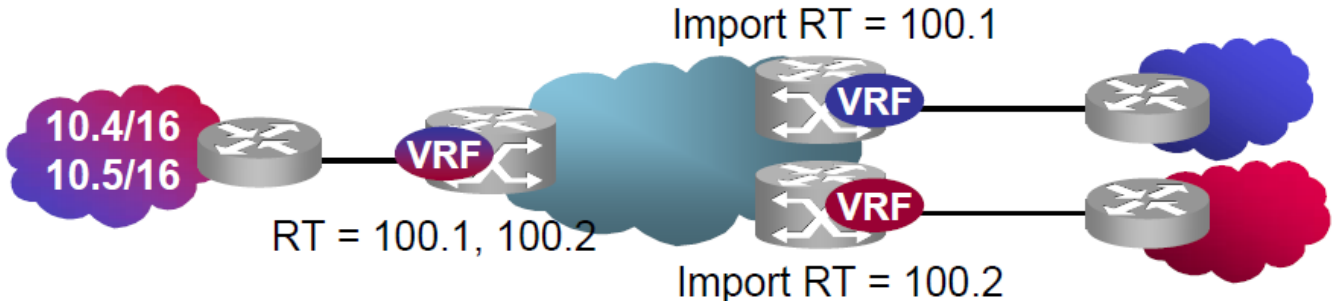
- ¿Cómo restringir la distribución de información de encaminamiento entre PEs?
  - SOLUCIÓN: Filtrado de rutas.
- El filtrado de rutas se hace usando la capacidad de BGP para marcar rutas asociándolas a una o más comunidades extendidas.
- La comunidad extendida usada para el filtrado de rutas se llama *Route Target* (RT).
- RT define la distribución de rutas restringida → Conectividad entre sedes VPN.
- Propiedades de RT:
  - Podemos asignar uno o más RTs a la misma ruta.
  - La asignación de RT a una ruta puede hacerse con cualquier granularidad:
    - El mismo RT para todas las rutas de una sede o diferentes RTs para cada ruta.
- El valor de RT se añade en el momento de exportar una ruta: *export-RT*.
- Para decidir en qué VRF instalar la ruta usamos *import-RT*:
  - Si coincide *import-RT* con *export-RT* en una VRF → Añadimos la ruta a dicha VRF.
    - Un ruta marcada con varias RTs se importa a una tabla VRF sólo si alguno de sus RTs corresponde con alguno de los RTs definidos para importación en la tabla VRF.

MPLS VPNs: distribución de rutas restringida

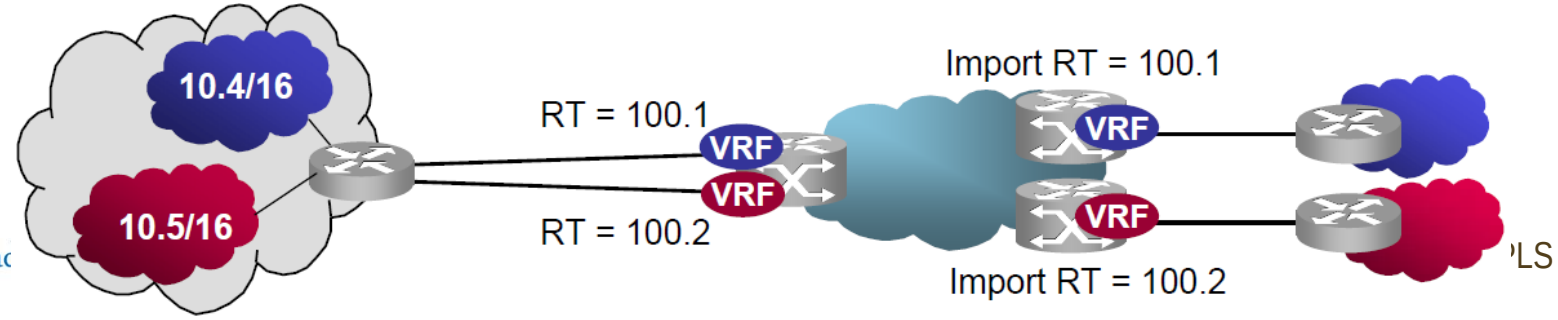
- PE configurado para asociar todas las rutas de una sede con un RT:



- PE configurado para asociar todas las rutas de una sede con múltiples RTs:

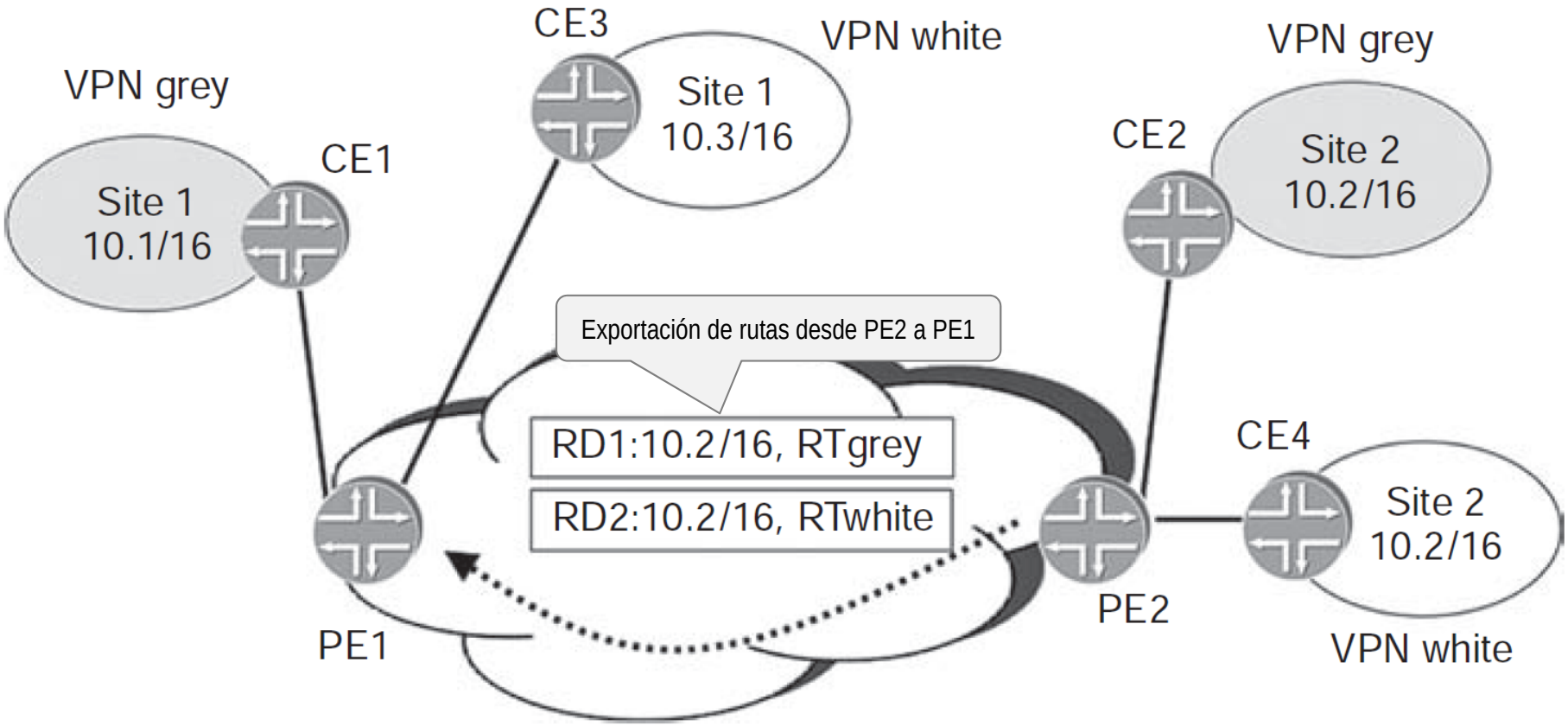


- CE se une a PE a través de dos circuitos, cada uno configurado con un RT diferente:



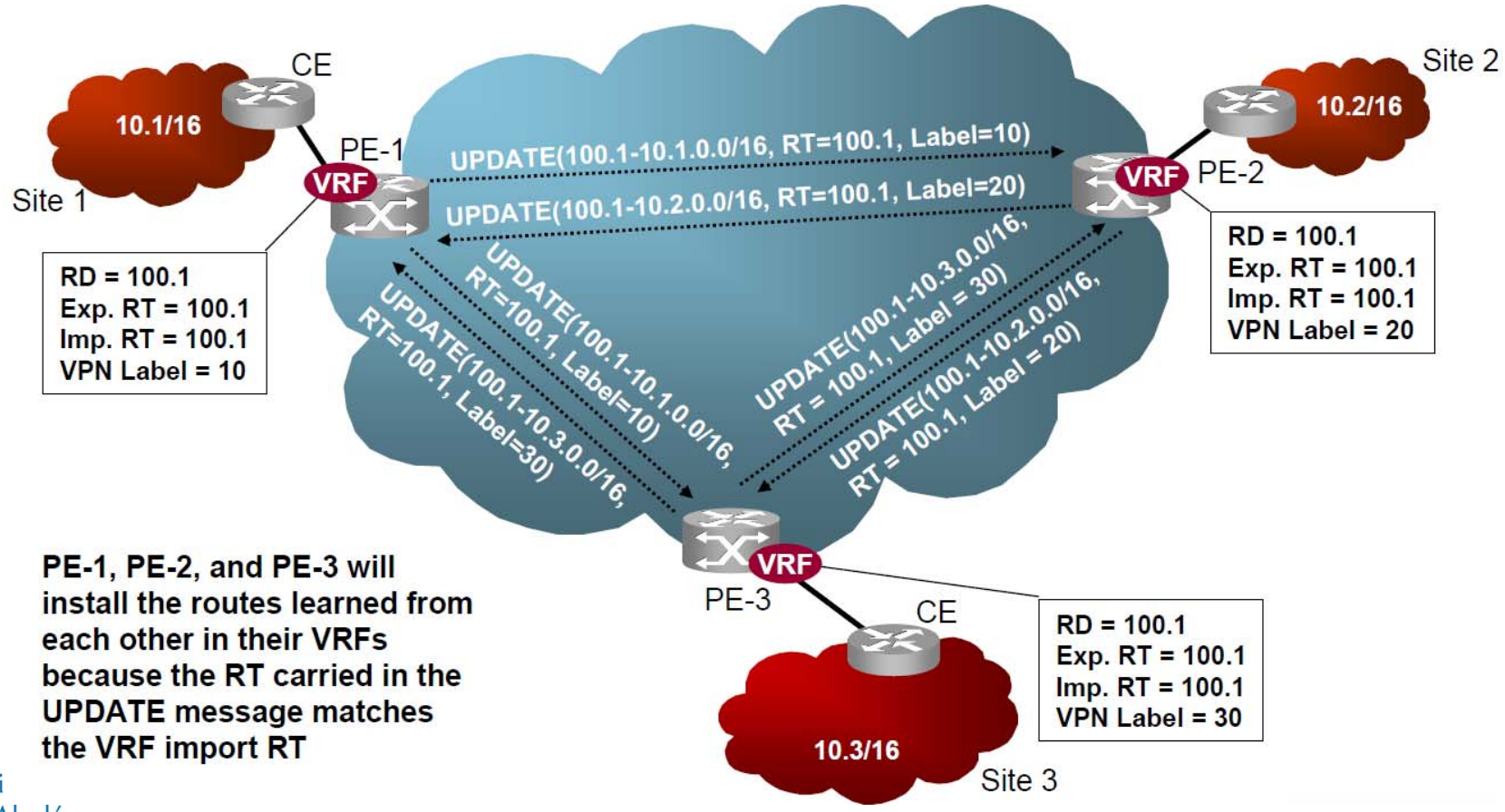
MPLS VPNs: distribución de rutas restringida

- Ejemplo:



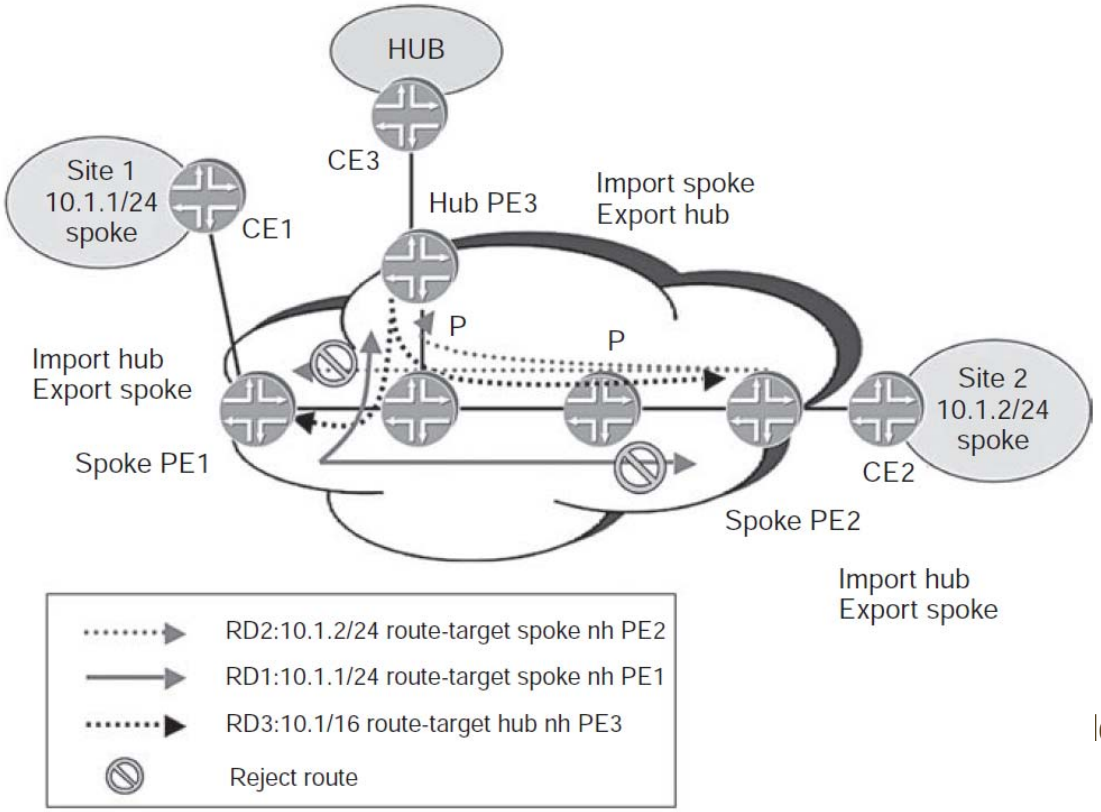
MPLS VPNs: modelos de conectividad VPN típicos

- *Full mesh*:
  - Todas las sedes se pueden comunicar con todas las demás directamente.
  - Se emplea un único RT para las políticas *import* y *export* en todas las sedes.



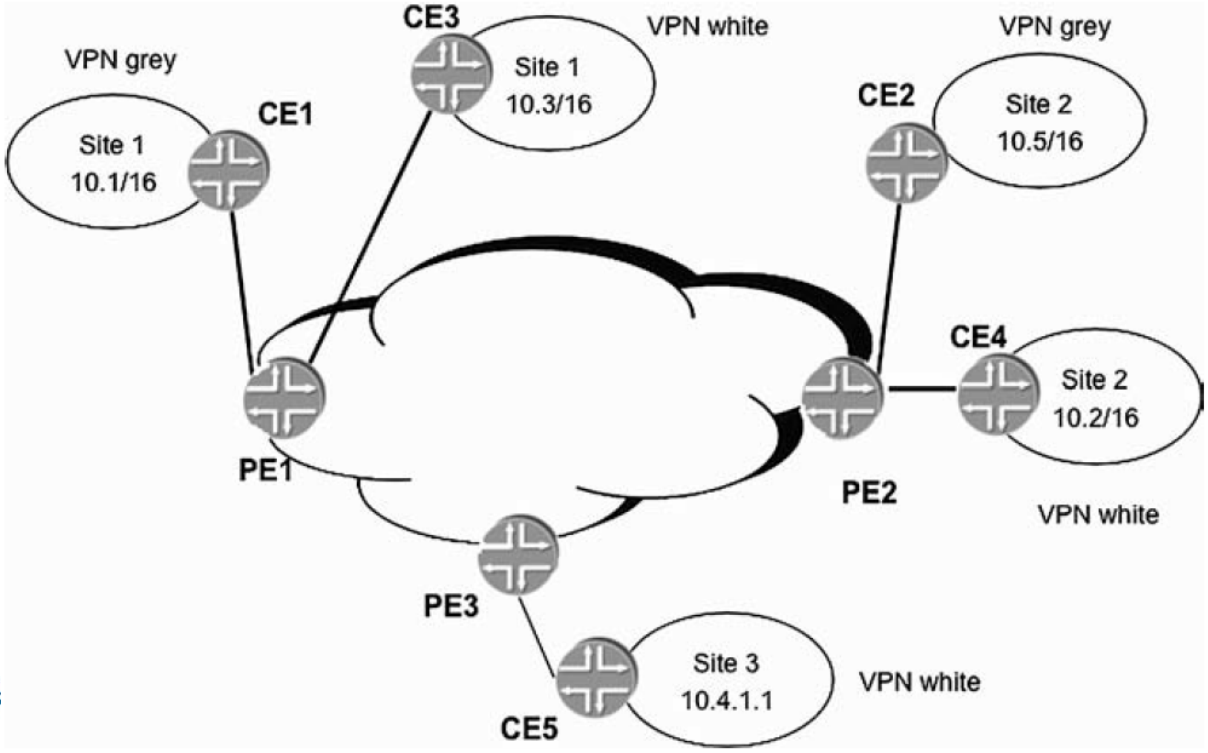
MPLS VPNs: modelos de conectividad VPN típicos

- *Hub and spoke:*
  - Las sedes se comunican indirectamente a través de una sede central (*hub*).
  - Dos RTs:
    - Para un *spoke* exportamos con *RT-spoke* e importamos solo con *RT-hub*.
    - Para el *hub* exportamos con *RT-hub* e importamos con *RT-spoke* (así aprende todas las rutas de los *spokes*).



MPLS VPNs: modelos de conectividad VPN típicos

- VPNs solapadas (extranet):
  - Se requiere acceder, por ejemplo, a una base de datos de la sede 3 desde cualquier VPN:
    - Para la sede 3 exportamos con *RTwhite* y *RTgrey*: así todas las sedes "verán" el recurso común.
    - La sede 3 debe importar a su vez los RT de todos los posibles solicitantes (para que pueda llegar el tráfico desde la sede 3 al solicitante).

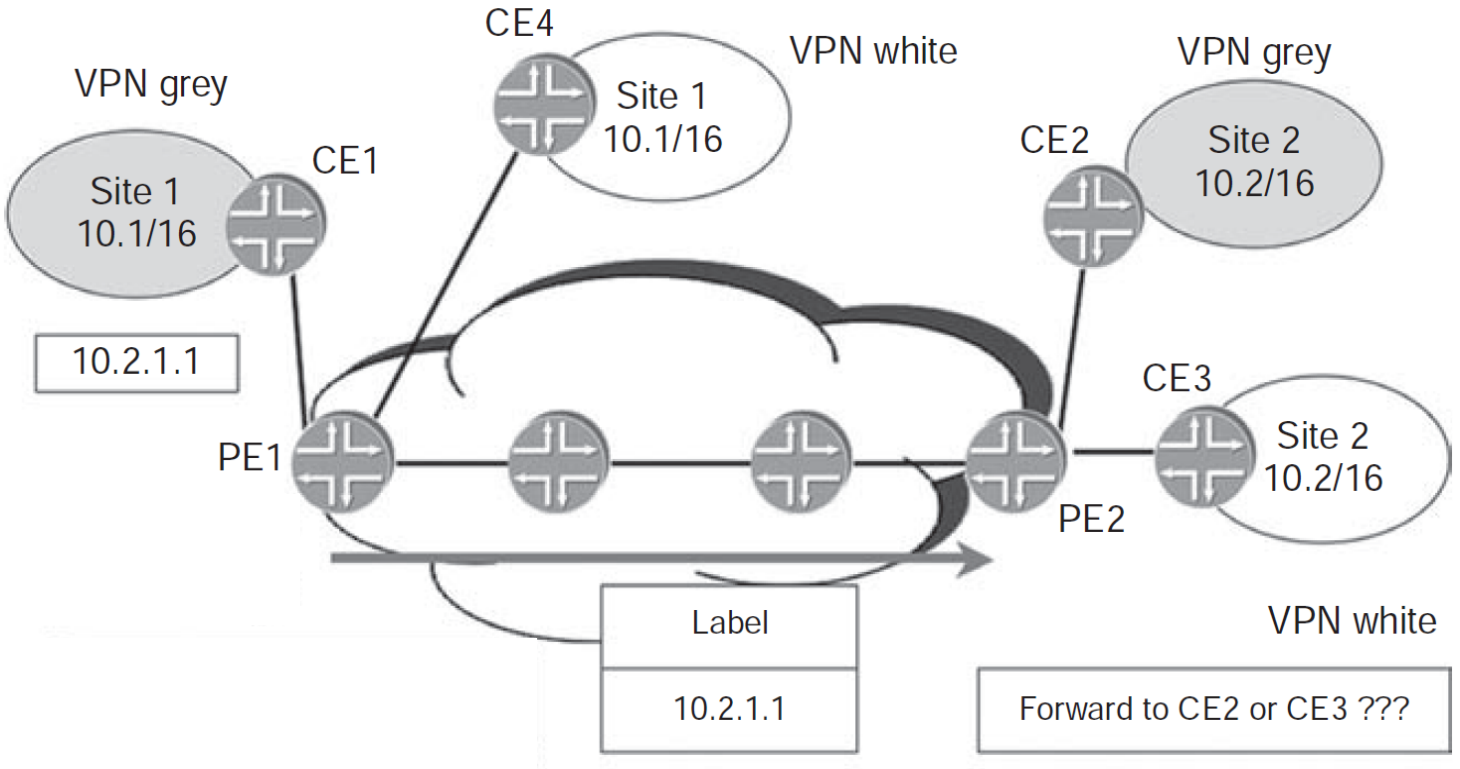


MPLS VPNs: túneles MPLS

- Las rutas VPN se distribuyen como prefijos VPN-IP entre PEs usando BGP.
- El siguiente salto de tal ruta es la dirección del PE anunciante: para alcanzar el destino el tráfico debe enviarse al PE anunciante.
- Deben utilizarse túneles entre PEs debido a:
  - Los *routers* P no tienen información de las rutas VPN.
  - La información de BGP es para direcciones VPN-IP, que no son directamente encaminables.

MPLS VPNs: túneles MPLS

- Problema: ¿a qué VPN pertenece un paquete que llega a PE2?



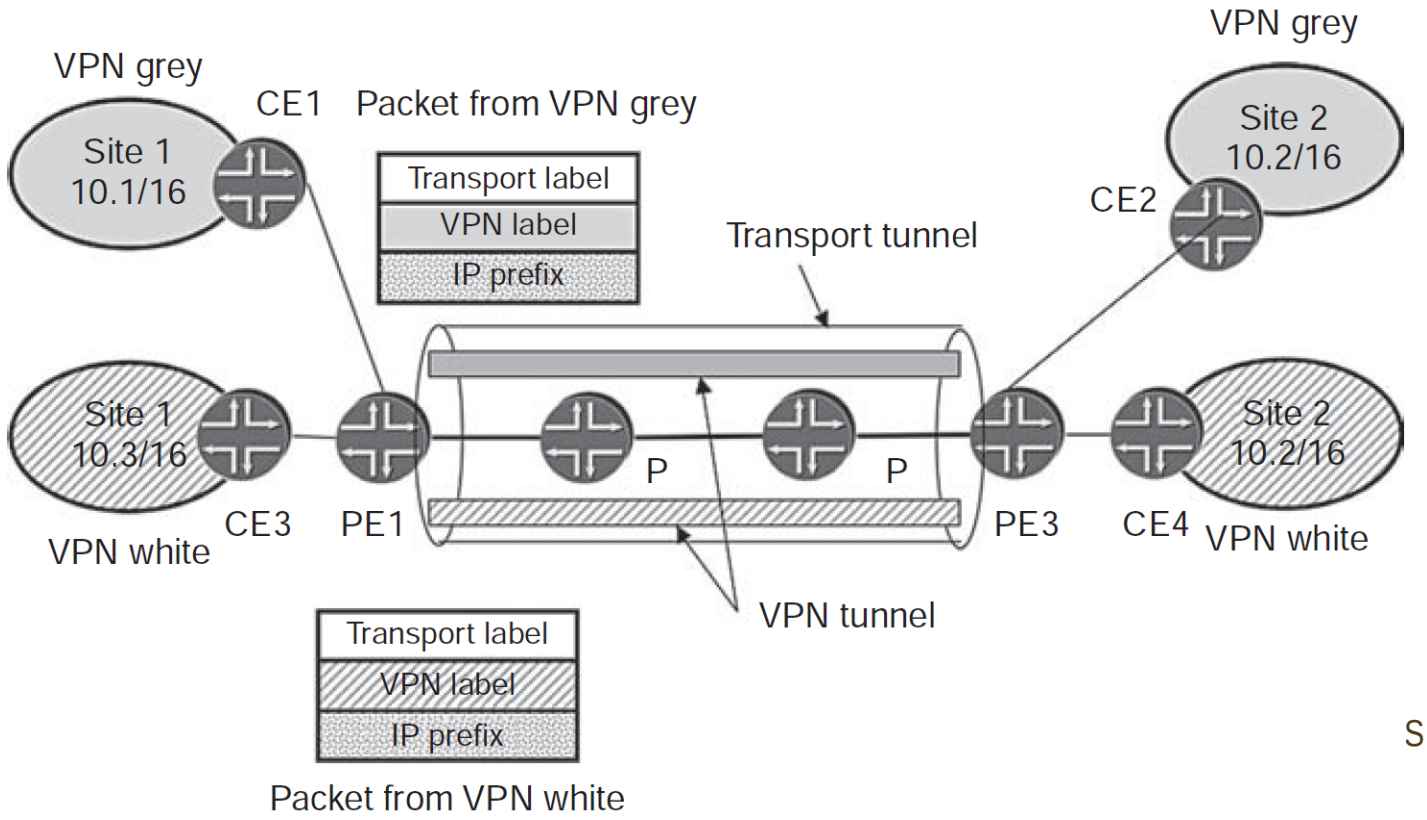
- SOLUCIÓN: Uso de un túnel entre PEs para cada VPN.

MPLS VPNs: túneles MPLS

- Para crear un túnel VPN con MPLS hay que asociar una etiqueta (etiqueta VPN) con una ruta VPN:
  - A la entrada del túnel se etiqueta el tráfico con la etiqueta VPN en el PE de entrada y se envía hacia el PE de salida.
  - A la salida del túnel, el PE de salida sabe a qué VPN enviar el tráfico en función de la etiqueta VPN.
- El uso de un túnel para cada VPN plantea problemas de escalabilidad si requiere que en el núcleo de la red los *routers* P mantengan el estado para cada VPN.
  - Se evita que cada *router* P mantenga el estado por VPN mediante las pilas de etiquetas → Jerarquía de túneles.

MPLS VPNs: túneles MPLS

- Se apilan dos etiquetas:
  - Etiqueta de túnel VPN (etiqueta VPN):
    - La utilizan los r*outers* PE de salida para conocer donde enviar los paquetes.
  - Etiqueta de túnel PE-PE (etiqueta de transporte):
    - La utilizan los *routers* P para el reenvío → Los *routers* P no necesitan ninguna información de los túneles VPN.

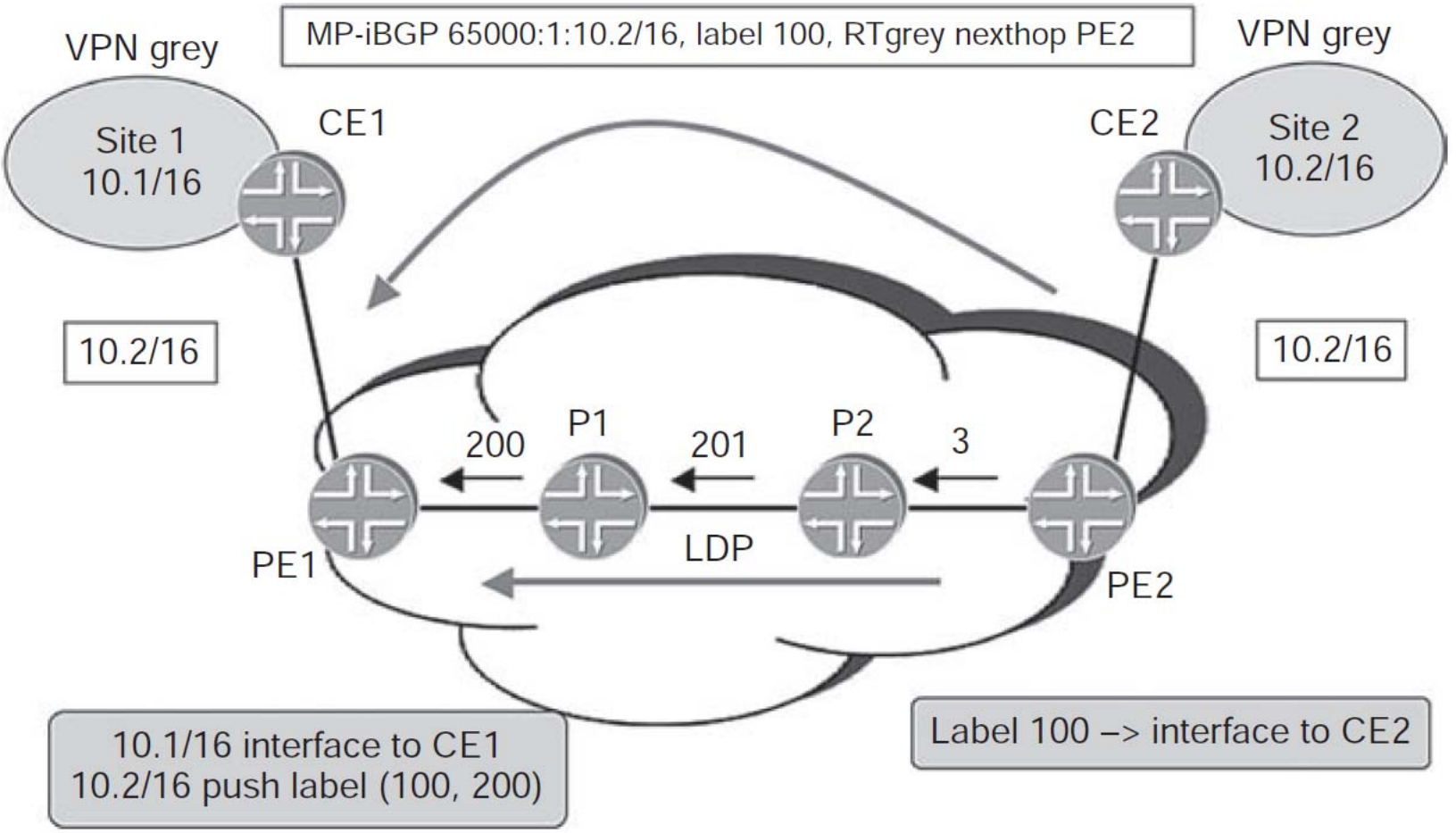


MPLS VPNs: túneles MPLS

- Políticas de reenvío en *routers* PE de salida:
  - Dos opciones:
    1. Búsqueda MPLS de la etiqueta VPN para determinar la VRF correspondiente, seguido de una búsqueda IP en esa VRF.
       - La etiqueta VPN indica la tabla correcta para la búsqueda.
    2. Búsqueda MPLS basada en la etiqueta VPN, en cuyo caso la etiqueta proporciona una interfaz de salida.
       - La etiqueta VPN indica la interfaz de salida.
  - El resultado es el mismo: el paquete IP se envía hacia la sede VPN correcta.
  - Se suelen poder configurar ambos modos.
  - ¿Y si se usa algún campo de la cabecera IP (por ej. *DiffServ*)?
    - Solo podemos usar la opción 1 cuando se requiere información del encabezado IP.

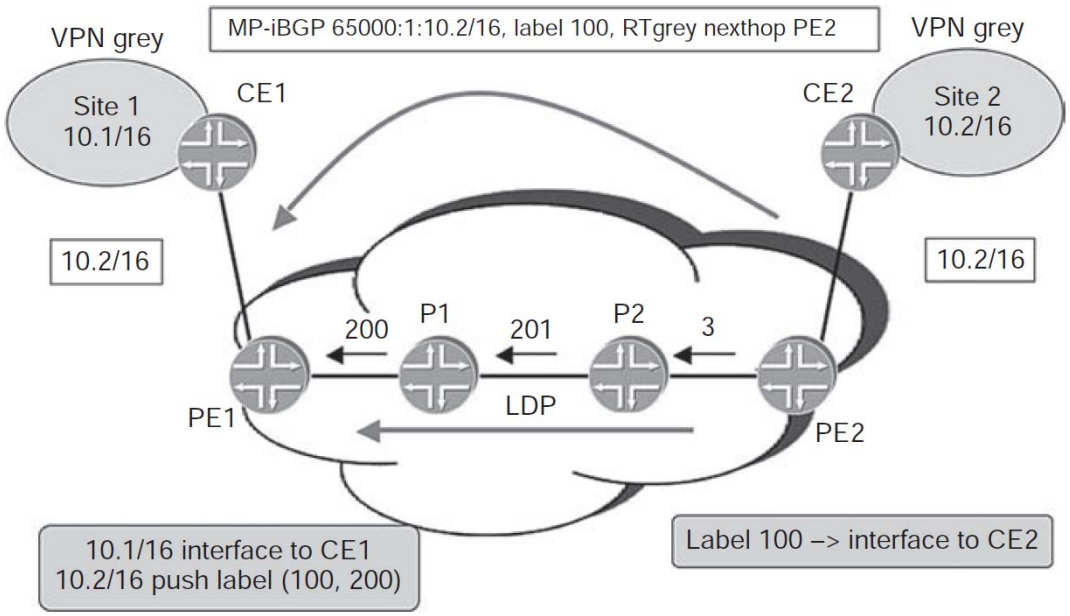
MPLS VPNs: ejemplo

- Establecimiento del camino PE2→PE1, envío de paquetes PE1→PE2.



MPLS VPNs: ejemplo

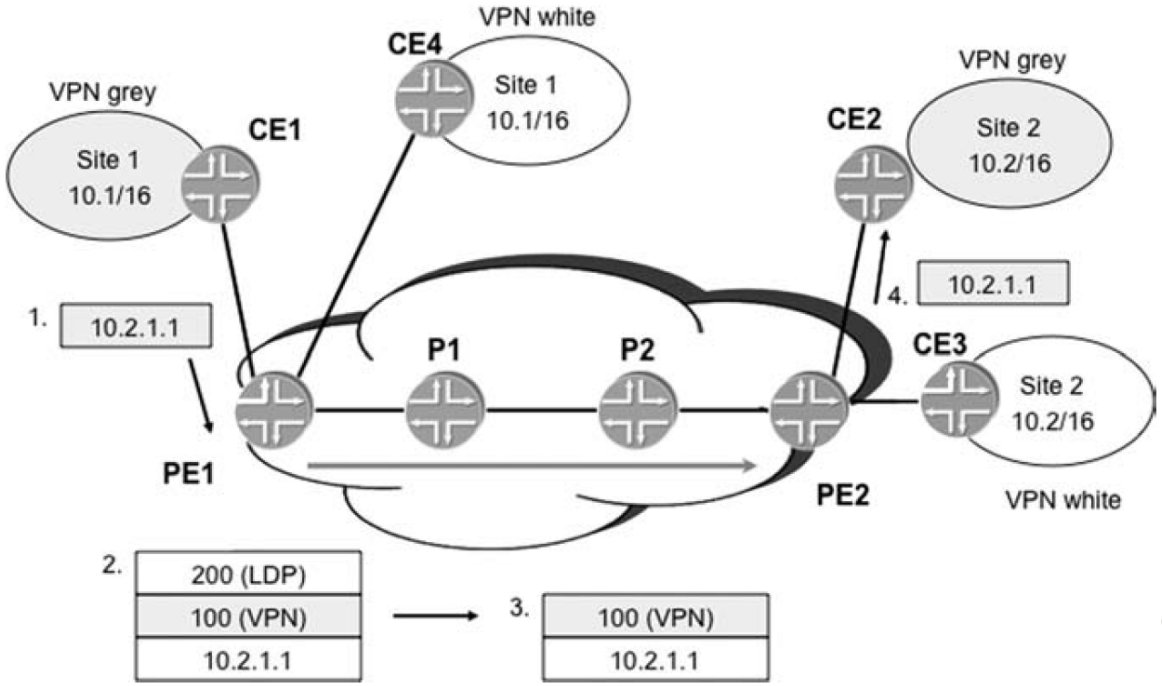
- Establecimiento del camino:
  1. Asumimos que PE2 recibe un anuncio de ruta 10.2.0.0/16 de CE2.
  2. PE2 añade un RD (65000:1) a la ruta y le asigna una etiqueta VPN (100) a este prefijo. PE2 exporta la ruta etiquetada con MP-BGP con el RT “grey”.
  3. PE2 crea la asociación en la tabla de reenvío para la etiqueta VPN 100 con la interfaz de salida con CE2.
  4. PE1 recibe el anuncio de MP-BGP para la ruta VPN-IP 65000:1:10.2.0.0/16 con siguiente salto PE2 y etiqueta 100.
  5. Conforme al RT, PE1 instala la ruta 10.2.0.0./16 en el VRF del cliente “grey”, quitando el RD, con etiqueta 100 y siguiente salto PE2. Hace falta un túnel MPLS entre PE1 y PE2 que se puede crear, por ejemplo, con LDP (etiqueta 200). Para 10.2.0.0/10 PE1 añadirá la pila de etiquetas (100,200).
  6. PE1 anuncia la ruta a CE1.



MPLS VPNs: ejemplo

- Envío de paquetes:

1. PE1 recibe un paquete de CE con destino 10.2.1.1.
2. Basándose en la interfaz en la que se recibe el paquete, la búsqueda de ruta se hace en la VRF del cliente “grey”. Se le añade la pila de etiquetas (100,200) y se envía hacia PE2.
3. El paquete llega a PE2 con una única etiqueta (la etiqueta VPN (100)). La etiqueta de transporte ha sido eliminada un salto antes (PHP).
4. PE2 tiene información de que los paquetes con etiqueta VPN 100 deben enviarse a CE2.



MPLS VPNs: alternativas

- Alternativas al uso de túneles MPLS:
  - Los túneles MPLS son la manera más natural de reenviar tráfico etiquetado (etiqueta VPN) hacia un destino.
  - Si se está migrando a MPLS, el operador no quiere usar MPLS o se usan redes que no soportan MPLS para el transporte, hay otras alternativas para transportar tráfico etiquetado (con la etiqueta VPN, que puede considerarse MPLS en sí misma).
  - Extensiones para transportar tráfico MPLS en:
    - IPSec
      - *Architecture for the Use of PE-PE IPsec Tunnels in BGP/MPLS IP VPNs* (*draft IETF: http://tools.ietf.org/html/draft-ietf-l3vpn-ipsec-2547-05*).
    - GRE:
      - *RFC4023: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*.
    - Túneles L2TPv3.
      - *RFC4817: Encapsulation of MPLS over Layer 2 Tunneling Protocol Version 3*.

MPLS VPNs: *route reflectors*

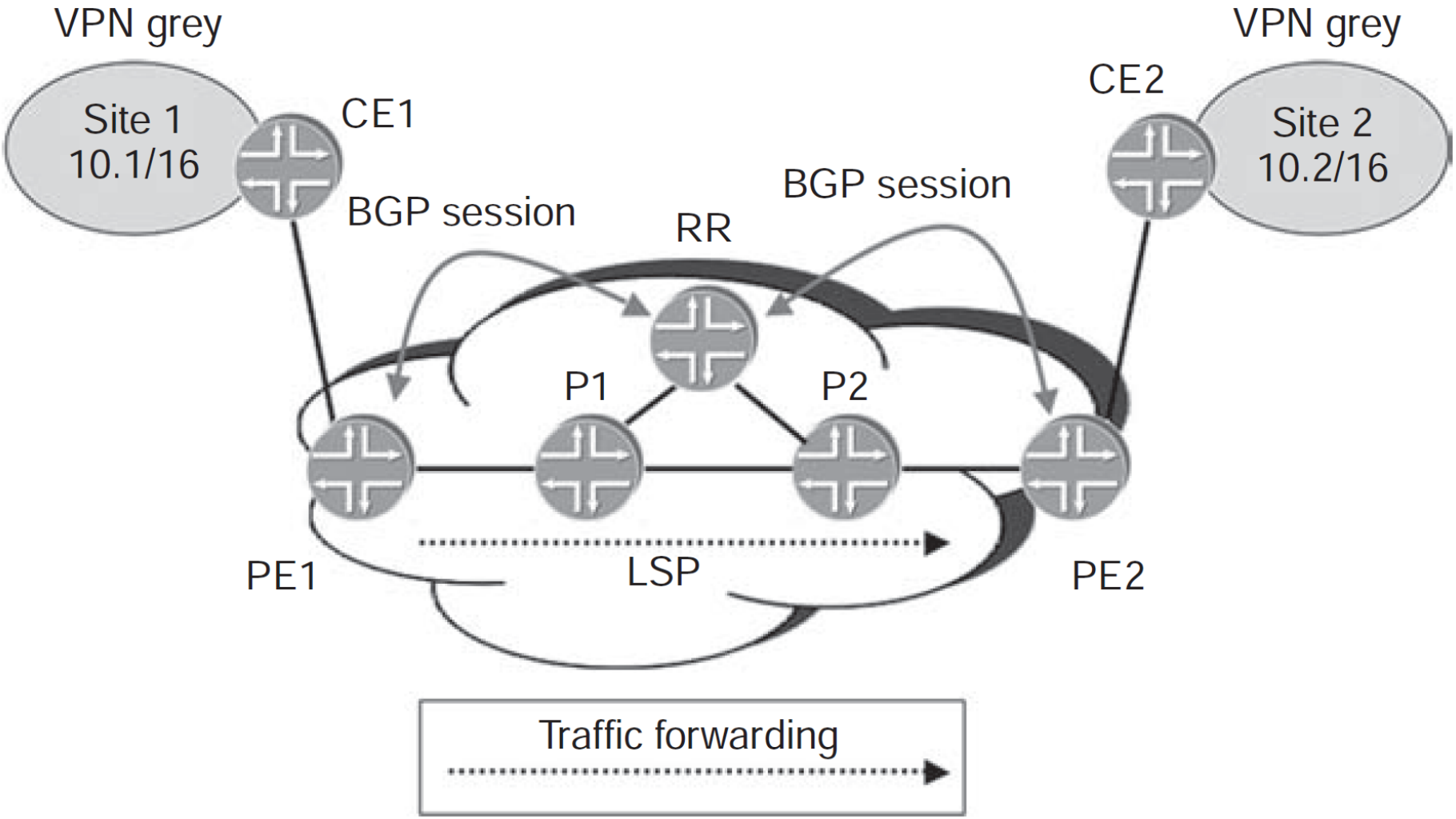
- RR: Route Reflector.
- Los RR permiten:
  - Reducir el número de *peerings* BGP.
    - Un PE solo necesita hacerse *peer* de un RR, no siendo necesario hacerse *peer* de otros PEs.
    - RR actuará como intermediario en la comunicación de rutas VPN entre PEs.
    - Cada PE mantiene un número constante de *peerings*, independientemente del número de PEs en la red.
  - 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).

MPLS VPNs: *route reflectors*

- Para conservar recursos CPU en PE y RR es deseable que los PE solo reciban actualizaciones de rutas VPN que les afecten (no todas las rutas).
- El RR maneja la actualización de todas las VPNs que tienen rutas en el RR.
- No es necesario que el tráfico de datos se reenvíe a través del RR → Ayuda a conservar recursos del RR.

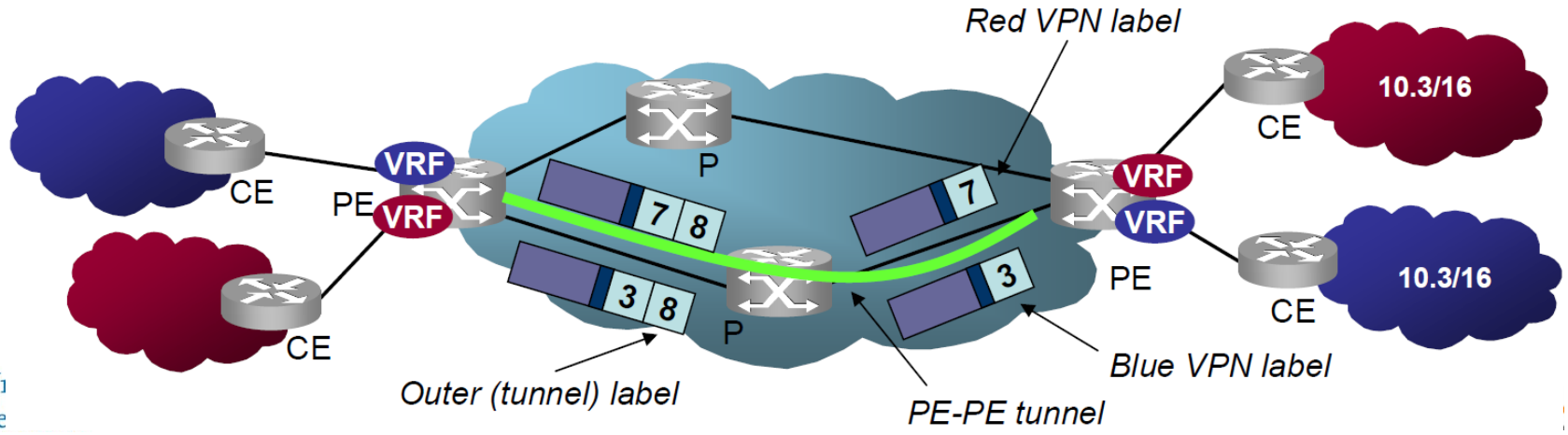
MPLS VPNs: *route reflectors*

- Ejemplo:



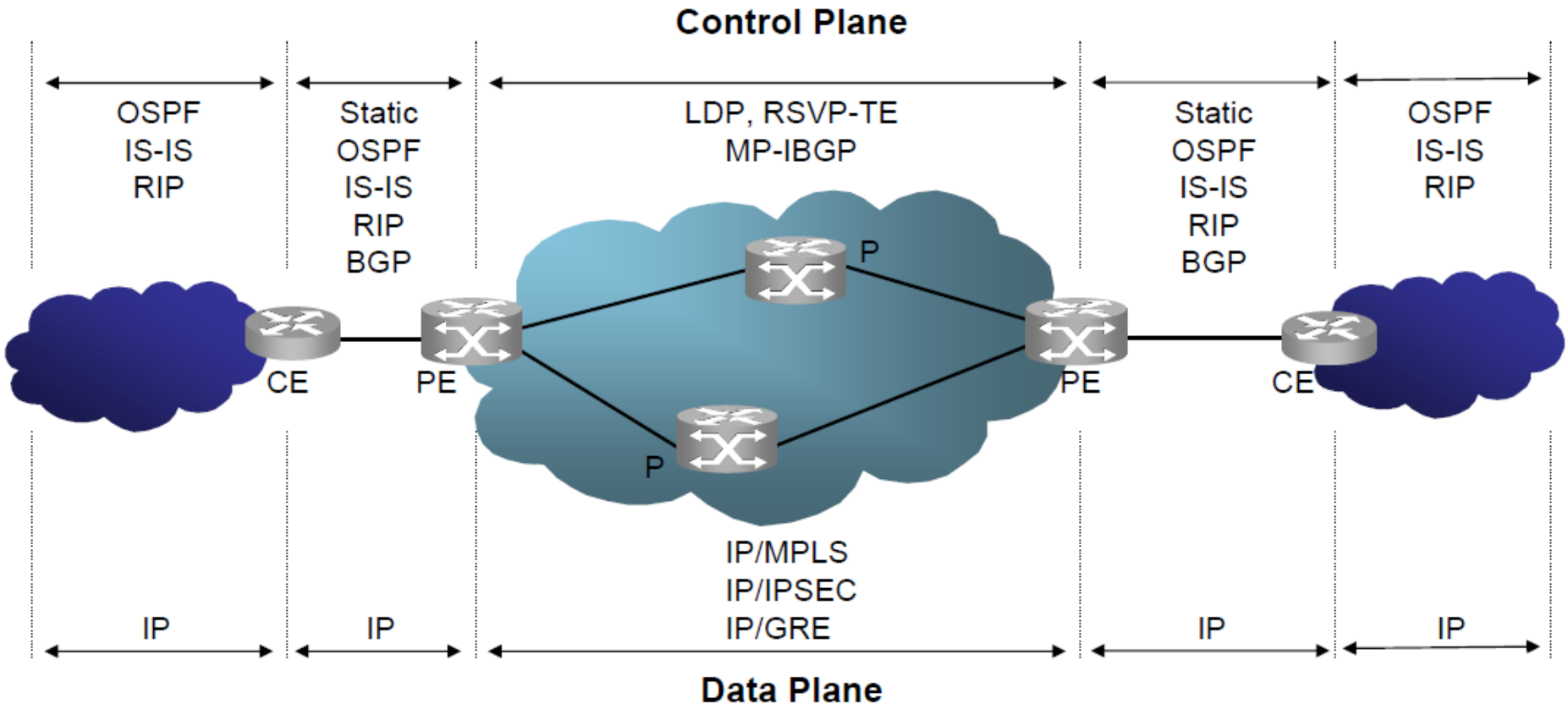
MPLS VPNs: resumen

- BGP proporciona un mecanismo automático de distribución de etiquetas VPN junto con rutas VPN-IP.
- La etiqueta VPN permite a los *routers* PE:
  - Introducir convenientemente tráfico VPN en el núcleo de red del proveedor (PE de ingreso).
  - Demultiplexar tráfico VPN que le llegue desde el núcleo de red del proveedor (PE de egreso).
- La información de túnel VPN está "oculta" a los *routers* P.
- Múltiples túneles VPN se transportan en un único túnel PE-PE.



MPLS VPNs: resumen

- Protocolos usados:



MPLS VPNs: resumen

- Beneficios de la solución BGP/MPLS VPV (MPLS L3VPN).
  - Se basa en protocolos y tecnologías ya desarrolladas, solo requiere extensiones a protocolos ya existentes.
  - Posibilita al cliente VPN deshacerse de las tareas de encaminamiento y descargar éstas en el proveedor de servicio .
  - Habilita al proveedor de servicio para ofrecer a los clientes servicios de valor añadido.
  - Los túneles PE-PE MPLS permiten transportar tráfico de múltiples VPNs y aplicaciones.
  - "Ocultando" la información VPN al núcleo de red (*routers* P) se simplifica éste y se trasladan las tareas más complejas a la frontera (*routers* PE)
    - Solución escalable ante crecientes demandas de servicio, sólo añadiendo más *routers* PE.
  - Por otra parte, la utilización de túneles MPLS habilita:
    - Reenvío de tráfico VPN a través del núcleo de red (*routers* P), no siendo éste consciente del direccionado VPN.
    - Identificar el tráfico de cada VPN en los puntos de egreso de la red del proveedor (*routers* PE).

Bibliografía

- I. Minei y 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.