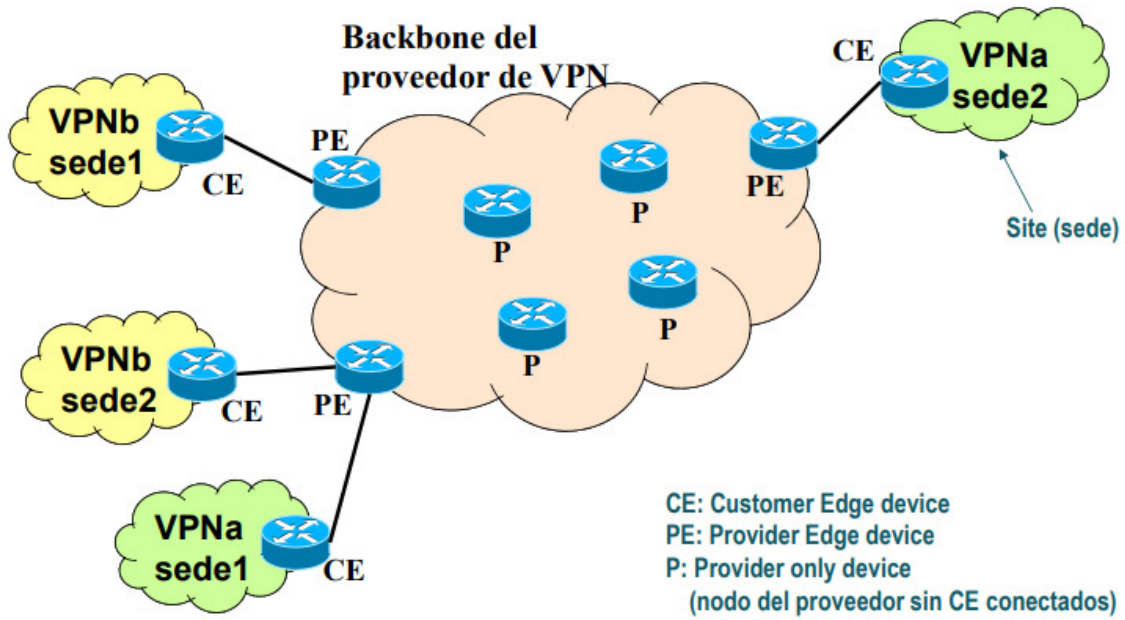
TEMA 1: APLICACIONES DE TECNOLOGÍA MPLS

1.REDES VIRTUALES DE NIVEL 2 Y NIVEL 3

El mayor potencial de MPLS está en la gran cantidad de aplicaciones en donde puede incluirse, entre ellas la creación de redes privadas virtuales de nivel 2 y 3, L2VPN y L3VPN.

El servicio de VPN se da en un escenario como el siguiente:



La VPN proporciona comunicación **PRIVADA** entre sedes que normalmente están separadas usando para ello una infraestructura **COMPARTIDA** con otras VPN o redes.

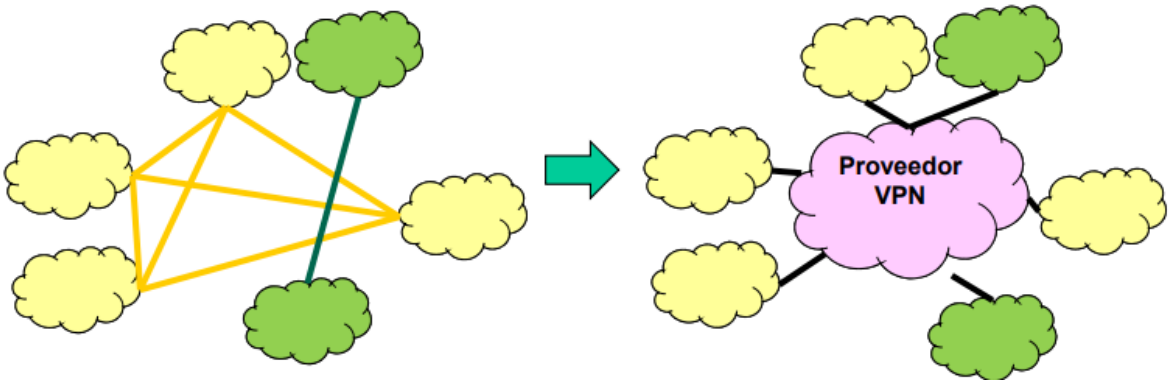
En los **enlaces de CE y PE** entre el backbone y las sedes de VPN se definen el servicio que se ofrece desde un punto de vista técnico, es decir, la seguridad, exclusividad…

El backbone está predefinido por el operador de la VPN y es el encargado de gestionar el tráfico y proporcionar estabilidad.

El nombre de VPN viene de Virtual Private Network, pero ¿Y esos adjetivos?

- PRIVADA: Por la comunicación limitada entre las sedes.
- VIRTUAL: Por el uso de la infraestructura compartida

A pesar de que como hemos visto el backbone sea común entre las distintas VPN que puedan conformarlo, debemos ver una topología de VPN de la siguiente forma:

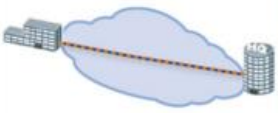


Tipos de VPN

Podemos clasificar las VPN en función a tres criterios:

- Según quien la proporciona: Proporcionada por la misma entidad o por una externa
- Tecnología: plano de usuario (túneles), plano de control (Señalización MP-BGP) y plano de datos (seguridad y gestión)
- Según el nivel: Nivel 3 (IP), Nivel 2 (Ethernet), Nivel 1 (pseudocables, es decir, un camino de routers que actúa como si fuese un único cable)

Topologías según el nivel

NIVEL 1	NIVEL 2		NIVEL 3
E-Line (P2P) PWE3	E-LAN (MP2MP) VPLS	E-Tree (RMP) VPLS with Multicast Optimization (P2MP LSP)	IP-VPN IP/MPLS
			
Cell-site backhaul Residential multi-play backhaul	Collaboration, Multi-site connectivity, corporate networking, VoIP, photo imaging, hosted applications.	Streaming video, broadcast TV Multimedia Content Delivery Streaming financial data	Internet Access Corporate VPN

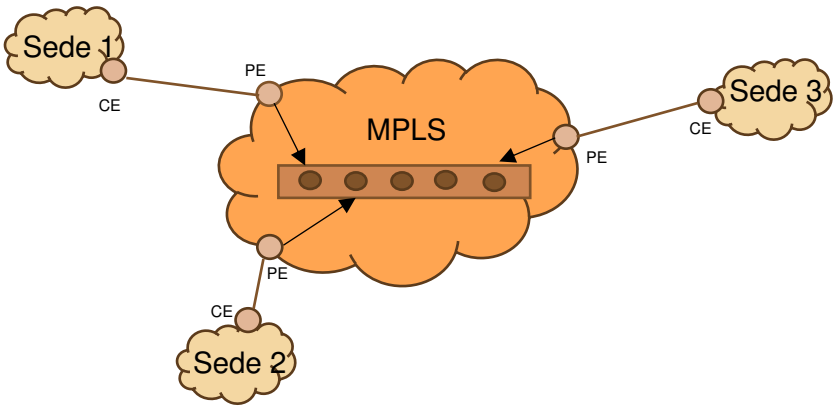
NOTA: Siempre debe haber nodos de conmutación, independientemente del nivel

VPN nivel 2 vs VPN nivel 3

La VPN de nivel 2 (VPLS) da conectividad entre las sedes como si se conectasen mediante una LAN (es decir, como si hubiese un switch).

Los equipos PE están conectados entre si mediante pseudocables, los cuales usan túneles, posiblemente creados mediante MPLS con LDP.

Los PE **aprenden** las direcciones MAC y les asocian puertos (lógicos) como los switches.



Desde el punto de vista del servicio, los CE se conectan a la boca del conmutador. Cuando necesita conocerse una dirección MAC, el conmutador manda un broadcast. Este comportamiento también lo tiene la propia VPLS. En las interfaces CE-PE no hay etiquetado, es el proveedor el único que usa MPLS.

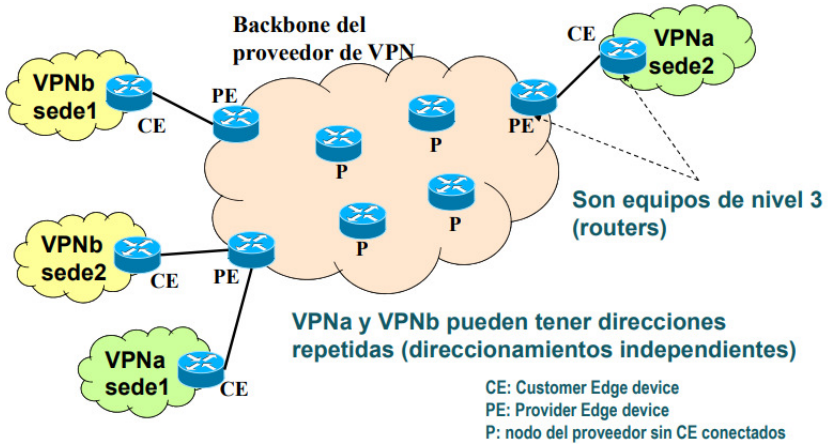
La VPN de nivel 3 (IP-VPN) da conectividad entre las sedes mediante un servicio de nivel 3, como si de un router se tratase. En este caso, los PE también se conectan mediante túneles posiblemente creados mediante MPLS con LDP.

En cambio, al contrario que en el nivel 2, los routers se **intercambian** información de encaminamiento de nivel 3 (entre los CE y los PE). Cabe destacar que los router P no tienen información de encaminamiento de las VPN.

2. FUNDAMENTOS DE VPN NIVEL 3

Estas VPN también se conocen como BGP/MPLS IP VPNs.

Tienen la siguiente distribución:



Debemos tener cuidado, como veremos después, los prefijos de las sedes no pueden solaparse unos con otros (hablando de la misma VPN), ya que habría problemas en las comunicaciones. En los siguientes puntos veremos cómo evitar este problema.

Información de encaminamiento

CE

Los router CE son los encargados de encaminamiento de la VPN para su sede.

- Sede Local: Aprendido por el **IGP propio** de esa sede.
- Sedes remotas de la VPN: Aprendidos del PE directamente conectado a esa sede por el protocolo correspondiente, entre los que podemos encontrar **OSPF, BGP…**

PE

Los router PE son los encargados del encaminamiento de la VPN, pero siempre de forma separada para cada VPN. Para ello intercambian información de encaminamiento mediante BGP.

- Locales: Aprendidas por los CE correspondientes mediante **OSPF, BGP…**
- Remotos: Aprendidos de los PE remotos. Obligatoriamente se hace con **MP-iBGP**

El encaminamiento del núcleo de red IP se hace con el **IGP propio** del operador.

Es importante remarcar que cada PE mantendrá unas tablas de rutas (VRF) distinta para cada conexión VPN, manteniendo así la información de encaminamiento de cada VPN separada.

P

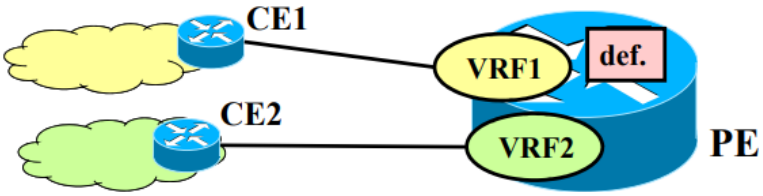
Son los routers internos de la red y se encargan del encaminamiento del núcleo mediante el IGP designado por el operador. Estos routers no tienen información de la VPN, algo que aumenta la estabilidad de la red. Esto se consigue mediante el uso de túneles en el plano de datos entre los PE.

La forma de que los PE distingan los túneles de VPN es con el uso de etiquetas. Por tanto, los paquetes tendrán 2 etiquetas, una para MPLS y otra para el túnel.

TABLAS DE REENVÍO

Como hemos visto antes, las tablas de reenvío de los PE están separadas, por lo que tendrán su propia tabla por defecto y luego las VRFs para las conexiones de las VPNs. Esta separación es para evitar la confusión de sitios VPN y sitios No VPN.

Por otro lado, la existencia de VRF separadas para cada VPN facilita el aislamiento de estas, ya que así será imposible acceder al trafico de una VPN externa.



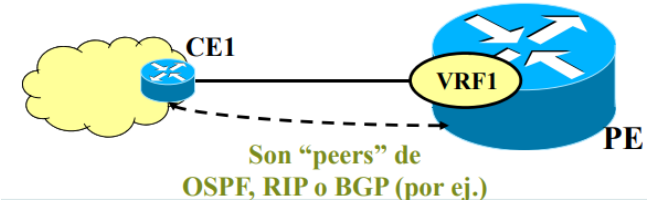
NOTA: Las VRF son tablas que se almacenan **EXCLUSIVAMENTE** en los PE, los CE no tienen VRF

INTERCAMBIO DE INFORMACIÓN CE-PE

El PE instala en la VRF las rutas de la VPN que aprende a través del CE. Este aprendizaje puede ser o mediante la configuración estática del PE o mediante protocolo de encaminamiento CE-PE, como, por ejemplo, OSPF, RIP o BGP

Una vez en el PE se le asignan etiquetas MPLS a las rutas. Varias posibilidades:

- Una etiqueta para toda la VRF
- Una ruta para cada ruta de la VRF
- Una etiqueta para cada grupo de rutas de la VRF

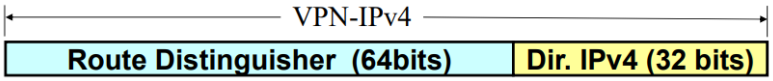


Po otro lado, los PE usan BGP entre ellos para intercambiar la información de encaminamiento de las VPN. En esta información encontramos:

- Prefijos aprendidos del CE (envío al resto de PE) junto a la etiqueta MPLS.
- NEXT-HOP, el cual es él mismo, indicando que es el PE que exporta esos prefijos.
- Route Ditinguisher (RD): Debido a que las VPN pueden usar prefijos IP iguales, para evitar problemas de comunicación se les coloca un prefijo de 8 octetos el cual creará rutas distintas para prefijos de IPv4 iguales.

Route Distinguisher – 8 bytes		
Type 0	100:1	Tipo (2 B) + Nº SA (2 B) + Id (4 B)
Type 1	192.168.19.1:1	Tipo (2 B) + Dir. IP (4 B) + Id (2 B)
Type 2	65538:10	Tipo (2 B) + Nº SA (4 B) + Id (2 B)

La aparición de los RD se crea una nueva familia de direcciones denominada VPN-IPv4 (VPNv4), formadas como se indica en la figura por 12 octetos. Esta información es transportada por extensiones del protocolo BGP como MP-iBGP

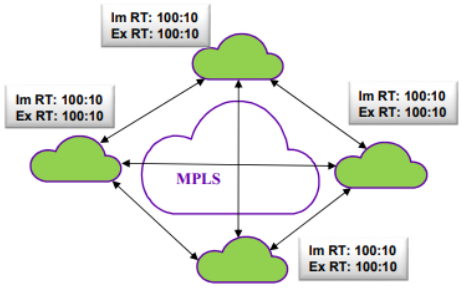


Router Target (RT)

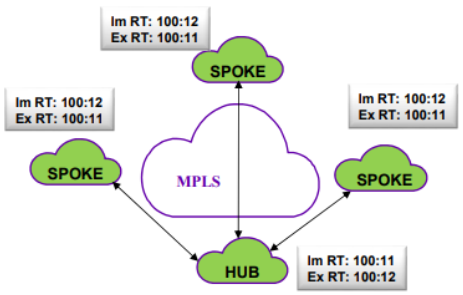
Las VRF solo pueden tener un RD, en cambio puede tener varios valores de RT en cada uno de sus tipos, exportación e importación.

Las PE se mandan sus valores de RT de exportación mediante mensajes UPDATE. El PE que recibe el UPDATE comprueba si en su lista de RT de importación existe algún valor igual al recibido en los de exportación. En el caso de que al menos uno coincida (la intersección sea no nula) se instalarán las rutas en la VRF.

Podemos encontrar las redes configuradas de las siguientes dos formas:



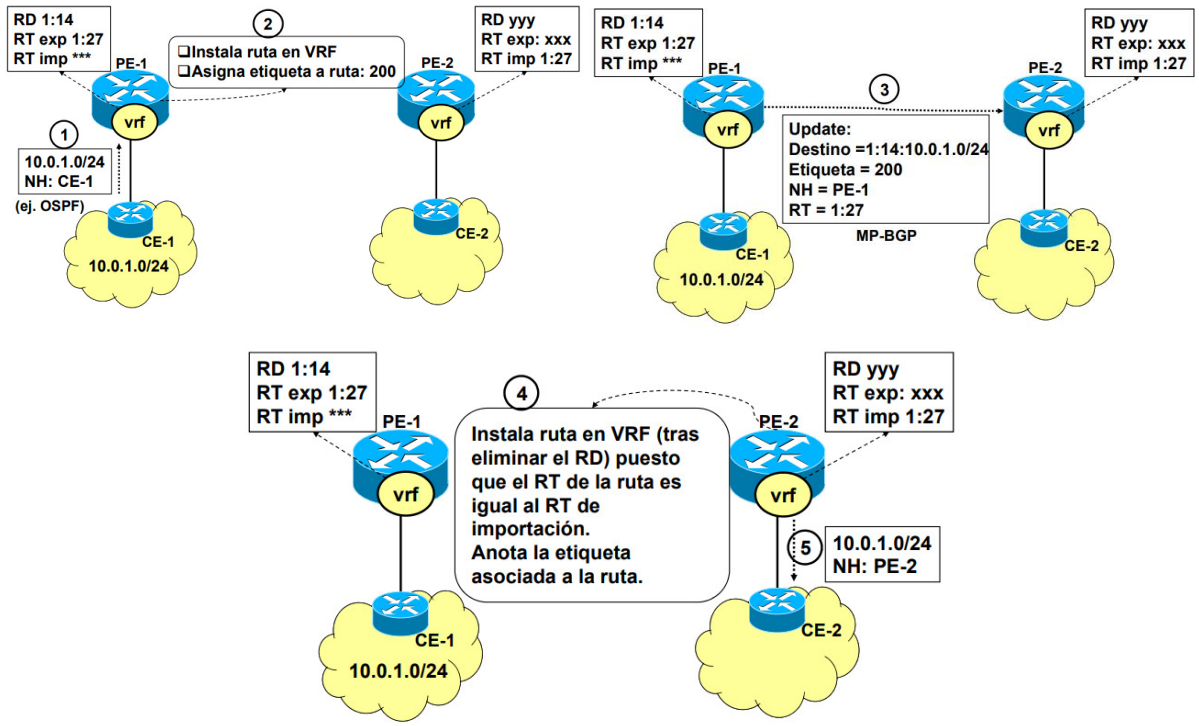
❑ VPN "Full-Meshed"
(mallada, any-to-any)
Todos los sitios de la VPN pueden enviar y recibir tráfico entre ellos, pero con nadie más



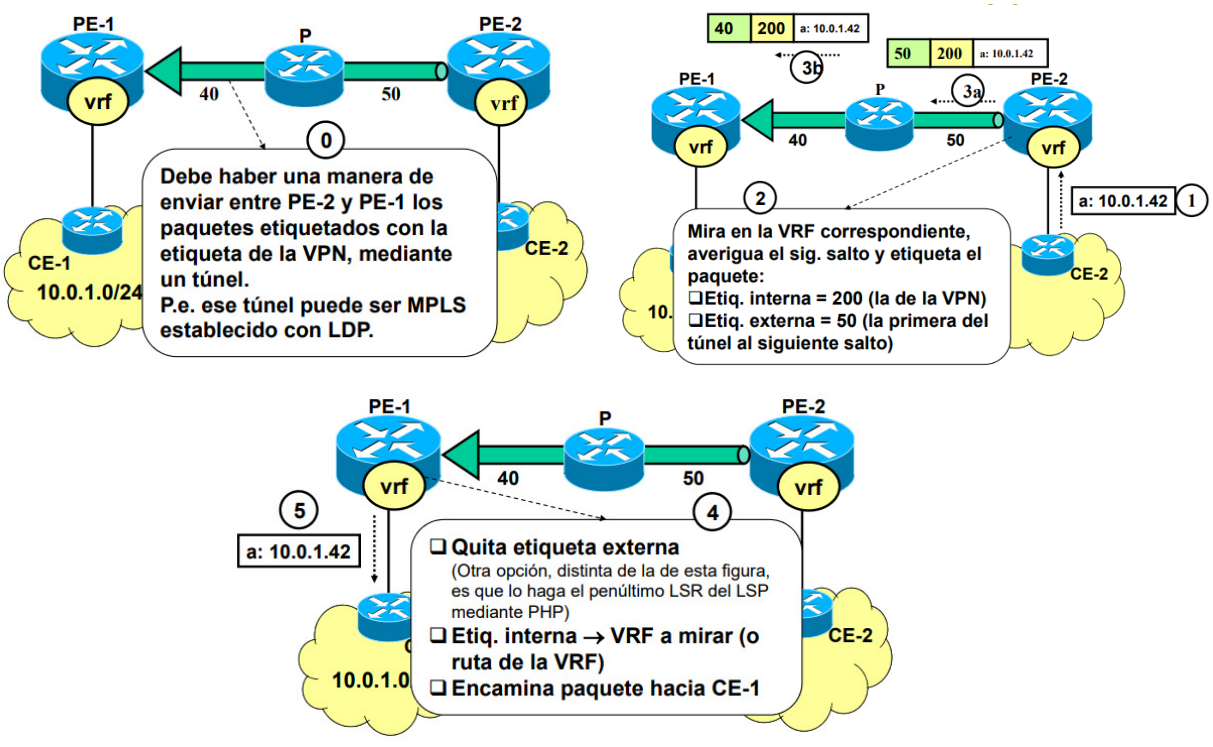
❑ VPN "Hub and Spoke"
(en estrella)
Todos los sitios pueden enviar al Hub. El Hub puede enviar a todos los sitios. Dos "spokes" no pueden comunicarse directamente.

Resumen del establecimiento de comunicación

PLANO DE CONTROL



PLANO DE USUARIO

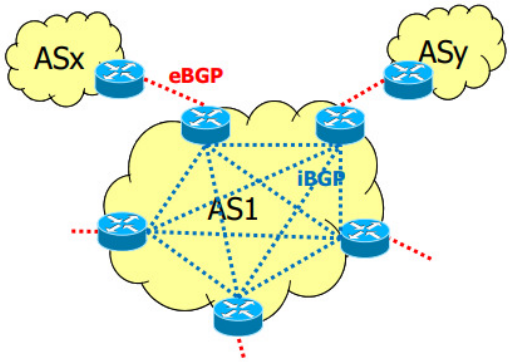


BGP Route Refelctors

Un route reflector es un router que envía actualizaciones a routers clientes.

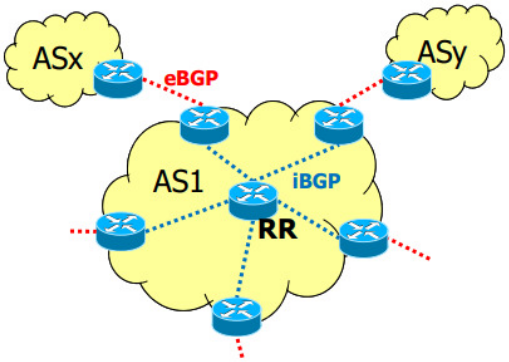
Cuando un cliente envía una actualización al route reflector, es enviado a su vez o reflectado a otros clientes. El route reflector es el único router que es configurado en un grupo de routers con varios clientes.

Para este propósito existe una configuración de red sin usar RR, el problema es que demanda gran cantidad de recursos y es menos eficientes. Ambas configuraciones son:



Malla de sesiones iBGP

- N*(N-1)/2 sesiones
- Mucha configuración al añadir un nuevo ASBR
- Un ASBR que recibe una ruta de un par iBGP no reenvía esa ruta a otros pares iBGP

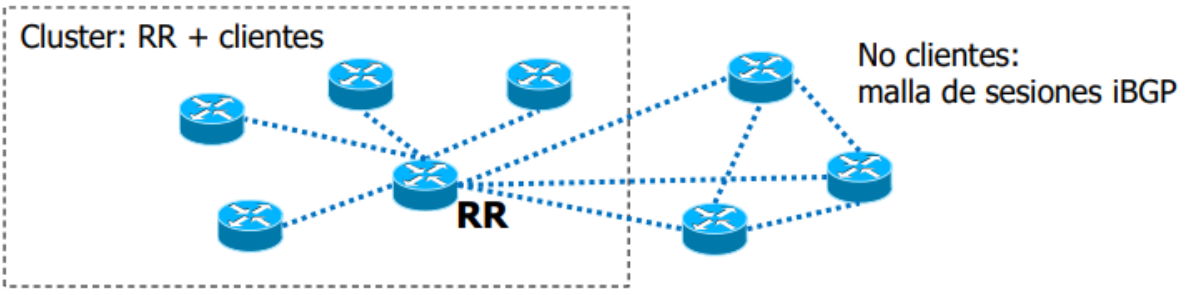


Route Reflector

- Mejora escalabilidad:
  - Menor número de sesiones: todos con el RR
  - Menor configuración al añadir un nuevo ASBR
- El RR reenvía ("reflects") rutas iBGP recibidas de pares iBGP a otros pares iBGP

Un cliente es un router que recibe actualizaciones de rutas de un route reflector que este a su vez ha aprendido de otro cliente. Por tanto, tanto el cliente como el route reflector forman una unidad que comparte información.

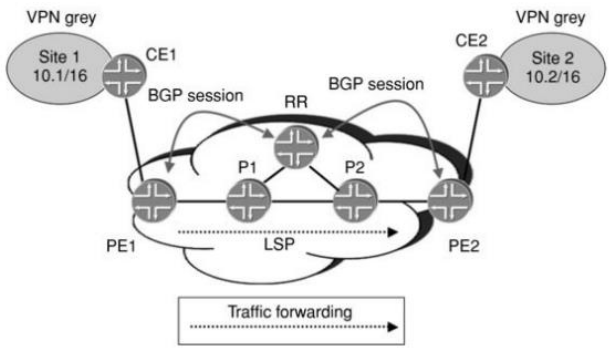
Esta unidad es denominada cluster. Debe tener como mínimo un RR, pero pude tener más. Realmente los RR se suelen desplegar por parejas para dar alta disponibilidad mediante la redundancia.



Como vemos en la figura, pueden existir router no clientes en una misma red donde tenemos un cluster, por tanto, el RR debe actuar de distinta forma para los clientes y para los no clientes:

Si un RR recibe una actualización iBGP:

- De un no cliente: Se la reenvía a los clientes. A los no clientes no se la reenvían, ya que será el mismo no cliente que ah mandado la actualización al RR el que se lo mandará al resto.
- De un cliente: Se la envía al resto de clientes y a los no clientes.



Los RR pueden aplicarse también en las VPN, en cambio, en este caso dedicarán toda su capacidad a la señalización en el plano de control, nada de reenviar tráfico en el plano de datos.

Los RR podrían tener que aceptar rutas iBGP para los RT, por ello podrían tener información de encaminamiento de todas las VPNs de la red.