



# VPNs sobre MPLS con Tecnología Cisco

# Presentación

- Ponente: Francisco Javier Nóvoa (Grupo Academia Postal)
  - En twitter: @fjnovoa\_
  - <http://ciscoetworkingspain.blogspot.com>
  - Responsable en Grupo Academia Postal del Programa Cisco Networking Academy
    - Cisco Academy: CCNA, CCNA Security, CCNP
    - Academy Support Center
    - Instructor Training Center
  - Responsable en Grupo Academia Postal del Programa VMware IT Academy



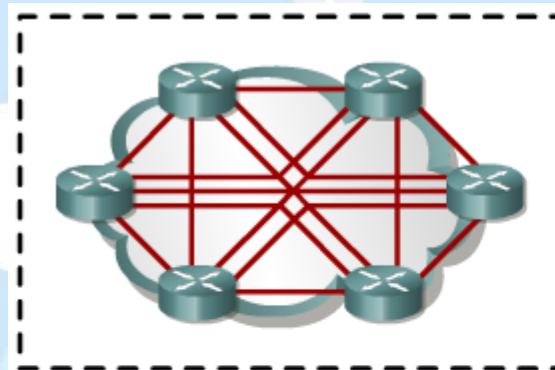
# Introducción a las Redes MPLS

# Introducción

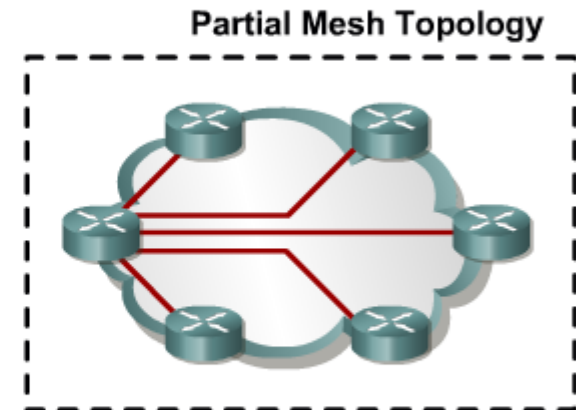
- MPLS es una tecnología orientada a que los proveedores de servicios puedan ofrecer nuevos productos de valor añadido utilizando la infraestructura de red existente.
- Cisco IOS MPLS permite fusionar la inteligencia del enrutamiento IP con el rendimiento de la conmutación.
- MPLS proporciona las siguientes ventajas:
  - VPNs escalables de extremo a extremo.
  - QoS de extremo a extremo
  - Aprovechamiento de las infraestructuras de red existentes
    - Es decir, permite proporcionar a los clientes servicios diferenciados de extremo a extremo escalables, manteniendo para el cliente una configuración, mantenimiento y provisión sencillas.
- En esta ponencia se abordarán:
  - Modelo conceptual de MPLS.
  - Arquitectura MPLS: Plano de control y plano de envío.
  - Etiquetado MPLS: Etiquetado de IP en MPLS.
  - Implementación de VPNs de MPLS.

# Modelo Conceptual de MPLS

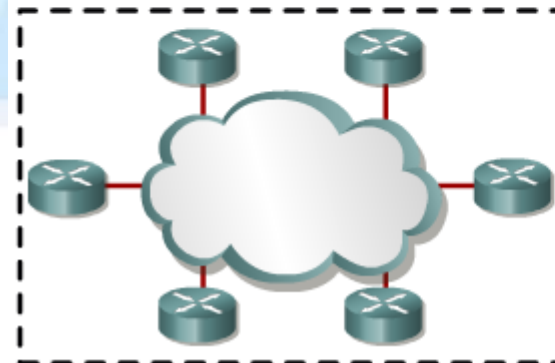
- Multiprotocol Label Switching (MPLS) es una nueva tecnología WAN emergente, cuya arquitectura está definida en el RFC 3031.
- Situación de partida: Topologías WAN.
  - Punto a punto
  - Multipunto:
    - Hub & Spoke
    - Partial mesh
    - Full mesh



Full Mesh Topology



Partial Mesh Topology



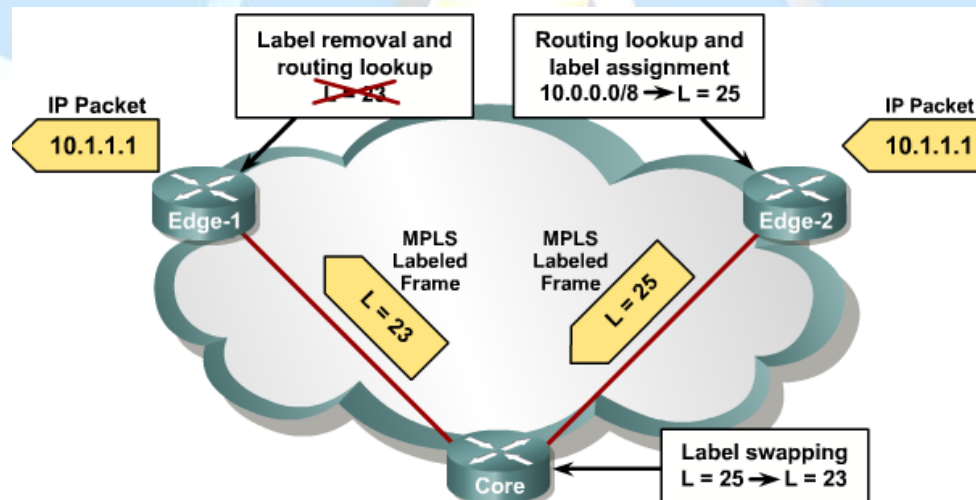
MPLS Topology

## Modelo Conceptual de MPLS

- La tecnología MPLS permite realizar tareas de enrutamiento óptimo entre diferentes ubicaciones de una misma organización, utilizando una sola conexión física o circuito virtual por ubicación al Proveedor de Servicios MPLS.
- MPLS se compone de una serie de tecnologías de capa 2 y capa 3 que le permiten enviar paquetes de cualquier protocolo de red utilizando etiquetas cortas y de tamaño fijo.
- En una WAN, MPLS proporciona las siguientes características:
  - Reduce el número de búsquedas en las tablas de enrutamiento
  - Proporciona un mecanismo de conmutación que asigna etiquetas a los paquetes. Estas etiquetas son utilizadas para enviar los paquetes.
    - Las etiquetas se asignan en los “bordes” de la red MPLS y se utilizan como único mecanismo de toma de decisiones de envío dentro de la red MPLS.
    - Habitualmente cada etiqueta es corresponde con una ruta IP (IP sobre MPLS).
    - Las etiquetas también se pueden corresponder con destinos como VPNs de capa 3 (MPLS VPN) o parámetros no IP, incluyendo información de capa 2 como podrían ser identificadores de circuito, interfaz saliente, etc.
    - MPLS proporciona soporte para el envío de otros protocolos además de TCP/IP.

# Modelo Conceptual de MPLS

- En el ejemplo se puede ver como MPLS proporciona enrutamiento rápido en redes grandes y complejas (como las de los proveedores de servicios).
  - Solamente realizan la búsqueda en la tabla de enrutamiento los routers “edge”.
  - Los routers del “core” de la red MPLS realizan el envío de paquetes basándose en las etiquetas MPLS.
  - El router Core no realiza ninguna búsqueda en la tabla de enrutamiento, toma la decisión utilizando las etiquetas y cambia dicha etiqueta (significado local).
- Los mecanismos de conmutación de los routers son un elemento clave del modelo conceptual de MPLS





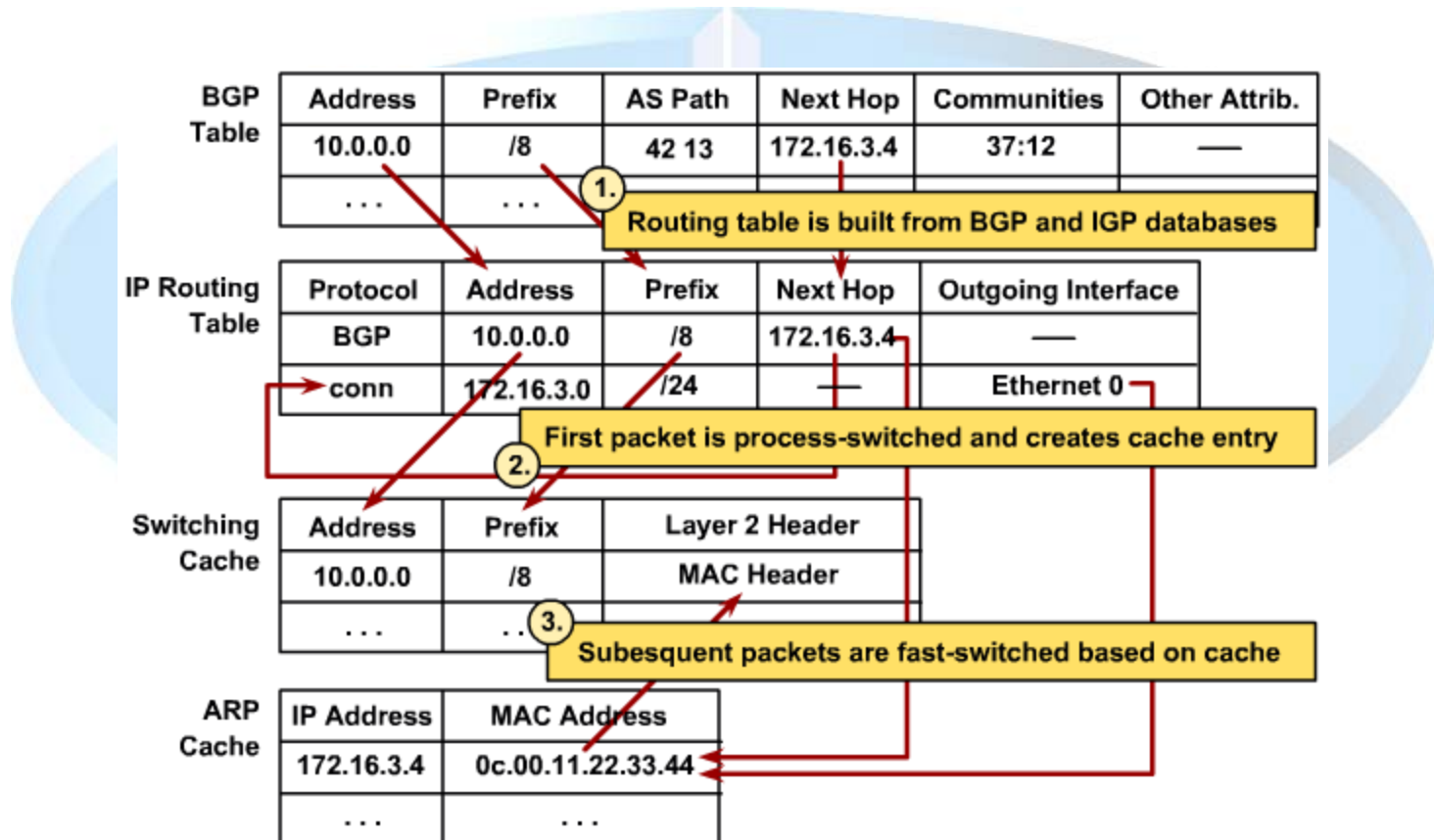
# Mecanismos de conmutación en el router

- Mecanismos de conmutación de paquetes con IOS:
  - Process switching: Proceso de conmutación clásico, realizando búsquedas en la tabla de enrutamiento.
    - Es un proceso lento
      - Búsqueda de la ruta en la tabla de enrutamiento (Memoria RAM)
      - Posibles búsquedas recursivas
      - Debe obtenerse la información de las cabeceras de capa dos y construir dichas cabeceras.
  - Fast switching: Proceso de conmutación basado en el uso de una caché para no reenrutar paquetes dirigidos a destinos recientes
    - El primer paquete de un flujo siempre se enruta mediante “process switching”
  - Cisco Express Forwarding: Se basa en el uso de la FIB para tomar decisiones de conmutación basadas en el prefijo IP. Conceptualmente, es una tabla de enrutamiento implementada en hardware.
    - La FIB mantiene almacenada también información del siguiente salto.
    - Se complementa con el contenido de la Tabla de Adyacencias.



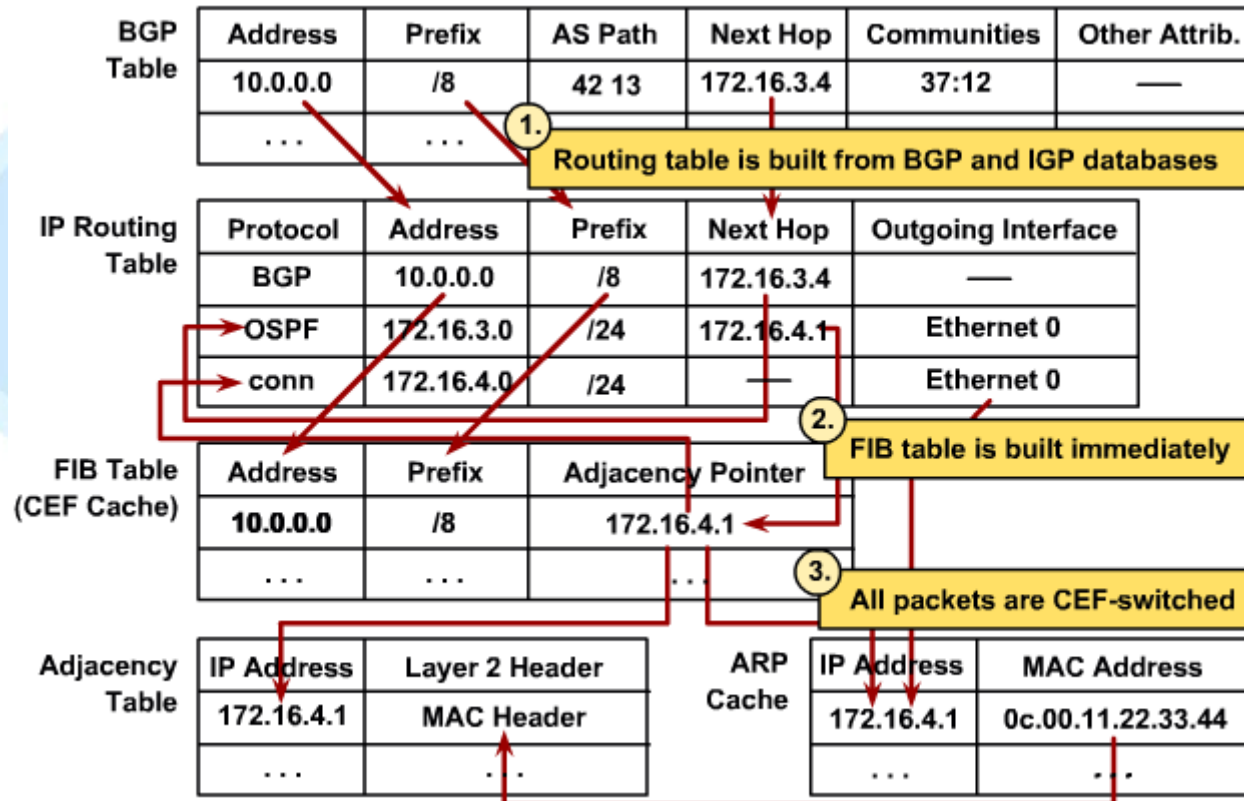
# Mecanismos de conmutación en el router

- Conmutación IP estándar. (Process Switching y Fast Switching).



# Mecanismos de conmutación en el router

- Arquitectura de conmutación de CEF



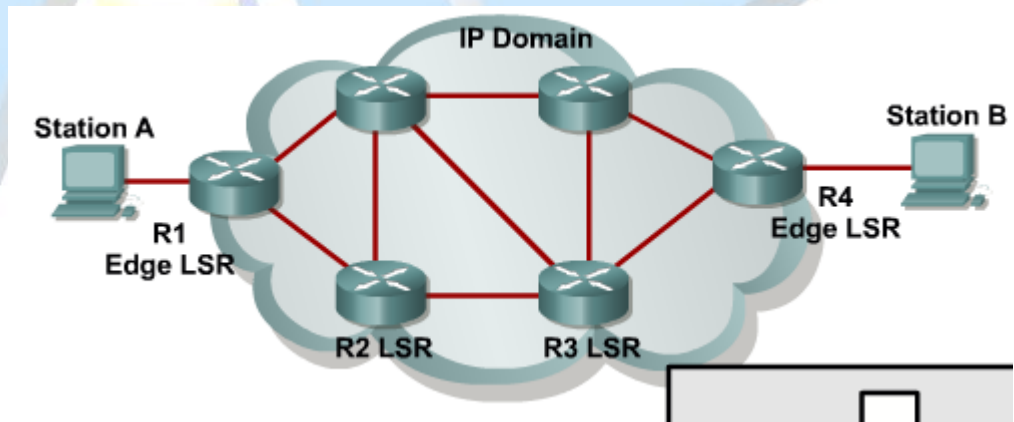
# Fundamentos de MPLS

- Tipos de routers:
  - Customer, Customer Edge.
  - Provider Edge (PE), Provider Core (P): Los routers P son “Label Switching Routers (LSR)” y Los routers PE se denominan “Edge Label Switching Routers (Edge LSR)”.
- Manejo de paquetes:
  - Cuando un paquete IP entra en un dominio MPLS, los Edge LSR convierten el paquete IP en un paquete MPLS añadiéndole una etiqueta.
  - Cuando un paquete MPLS deja el dominio, los Edge LSR eliminan la etiqueta volviendo el paquete a su estado anterior.
  - Dentro del dominio MPLS, los LSRs envían los paquetes basándose en las etiquetas de los mismos.

# Fundamentos de MPLS

## Ejemplo:

- A genera un paquete IP encapsulado en una trama Ethernet
  - La MAC de destino es la de la pasarela por defecto, que en este caso es un Edge LSR
- Utilizando la “Label Forwarding Information Base” → Envío de una trama MPLS hacia el siguiente destino LSR.
  - Dicho router también inserta una etiqueta entre las cabeceras de la capa 2 y la capa 3
- R2 LSR procesa la trama en función del valor de la etiqueta y el contenido de su LFIB.
- ...
- R4 elimina la etiqueta y envía una trama Ethernet estándar a la estación B
- Para enviar la información de A a B no se realiza ninguna tarea de enrutamiento dentro del dominio del SP



# Fundamentos de MPLS

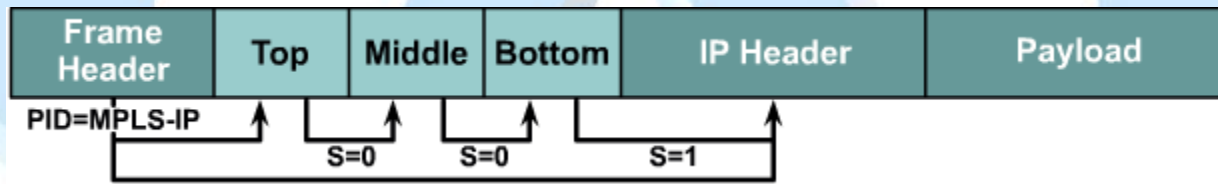
- Características:
  - MPLS funciona sobre cualquier medio físico y encapsulamiento de capa 2.
    - La mayor parte de tipos de encapsulamiento de capa dos utilizan el modo “trama” de MPLS (frame mode MPLS):
      - Insertan una etiqueta de 32 bits entre la cabecera de capa 2 y la de capa 3
    - Las etiquetas MPLS tienen un formato y campos específicos que proporcionan información al proceso de toma de decisiones.

Field	Description
20-bit label	The actual label. Values 0 to 15 are reserved.
3-bit experimental (EXP) field	Undefined in the RFC. Used by Cisco to define a class of service (CoS) (IP precedence).
1-bit bottom-of-stack indicator	MPLS allows multiple labels to be inserted. The bottom-of-stack bit determines if this label is the last label in the packet. If this bit is set (1), the setting indicates that this label is the last label.
8-bit Time to Live (TTL) field	Has the same purpose as the TTL field in the IP header.



# Fundamentos de MPLS

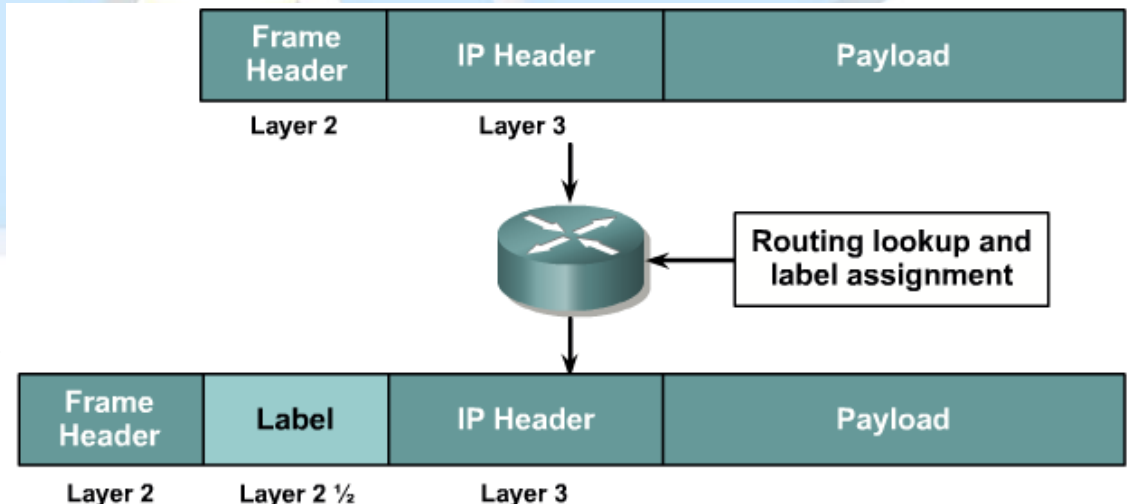
- Pila de Etiquetas:
  - En algunos casos, una etiqueta no contiene información acerca del protocolo de capa 3 que lleva el paquete.
    - La identidad del protocolo de capa de red debe ser inferible del valor de la etiqueta.
  - Los protocolos de capa 2 que tienen campos “Tipo” o “PID”, reciben nuevos valores que indican que el protocolo de capa 3 lleva una etiqueta MPLS.



- En algunos casos, un paquete solamente lleva una etiqueta. Sin embargo en muchos otros puede haber más de una:
  - MPLS VPNs: Se utiliza MP-BGP para propagar una segunda etiqueta que identifica a la VPN además de la etiqueta que se propaga por LDP para identificar la ruta.
  - MPLS TE: RSVP
  - MPLS VPNs combinadas con MPLS TE

# Fundamentos de MPLS

- Frame Mode MPLS. Operación de un router “edge” de entrada que recibe un paquete IP:
  - Se busca en la tabla de enrutamiento una interfaz de salida.
  - Asigna e inserta una etiqueta entre las cabeceras de la capa 2 y de la capa 3, si la interfaz de salida tiene MPLS activado y si la etiqueta “next-hop” para el destino existe. Además el router cambia el contenido del campo tipo, al correspondiente Ethertype.
  - Envía el paquete.
  - Se utilizará dicha etiqueta para alcanzar el destino.
- Frame Mode MPLS. Operación de un router “core” cuando recibe un paquete MPLS:
  - Envía el paquete por la interfaz adecuada en función de la etiqueta de entrada y cambia la etiqueta MPLS



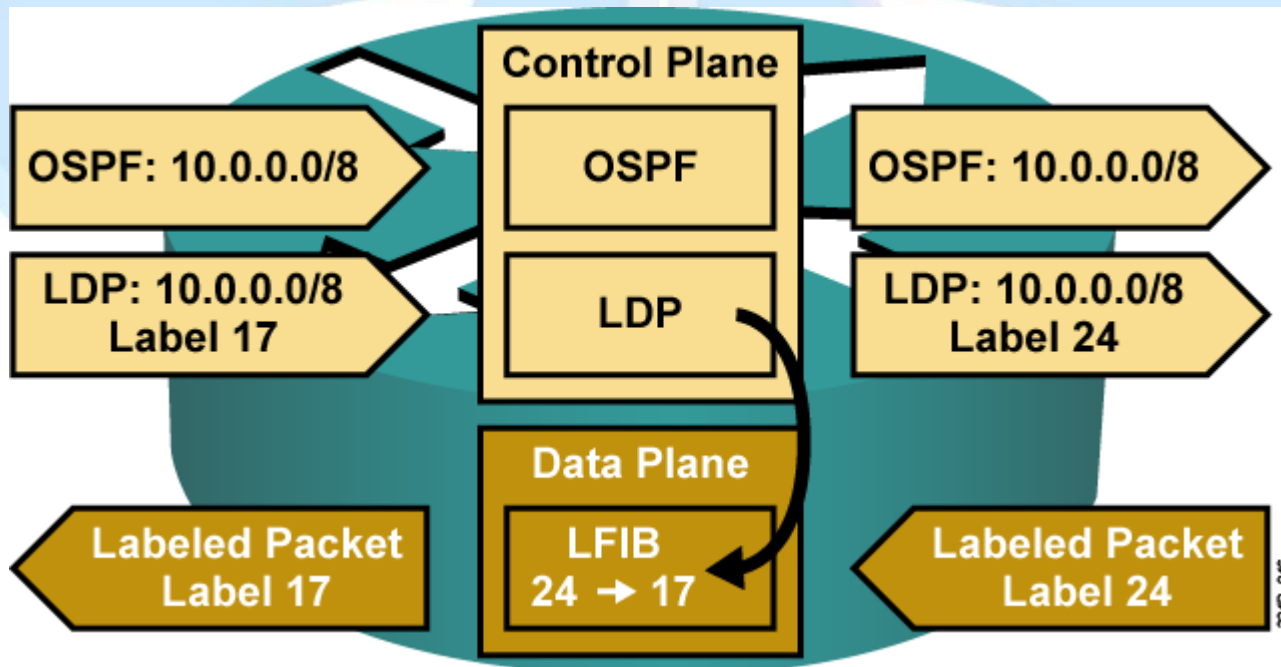


# Arquitectura MPLS

- MPLS divide la arquitectura de enrutamiento clásica en dos partes:
  - “Control plane”: Controla el intercambio de la información de enrutamiento y el intercambio de etiquetas entre dispositivos adyacentes.
    - Es dependiente del protocolo de enrutamiento utilizado: OSPF, IS-IS, RIP o BGP
    - Necesita un protocolo de intercambio de etiquetas: MPLS LDP, MP BGP (MPLS VNP), RSVP (MPLS TE) para reservar recursos.
  - “Data plane” o “Forwarding Plane”: Controla el envío de paquetes tanto basado en direcciones de destino como en etiquetas.
    - Es un motor de envío basado en etiquetas.
    - Es independiente de los protocolos de enrutamiento o de los protocolos de intercambio de etiquetas.
    - La tabla “Label Forwarding Information Base (LFIB)” almacena la información que el motor de envío utiliza para enviar los paquetes.
    - Los protocolos de intercambio de paquetes generan el contenido de la tabla LFIB.

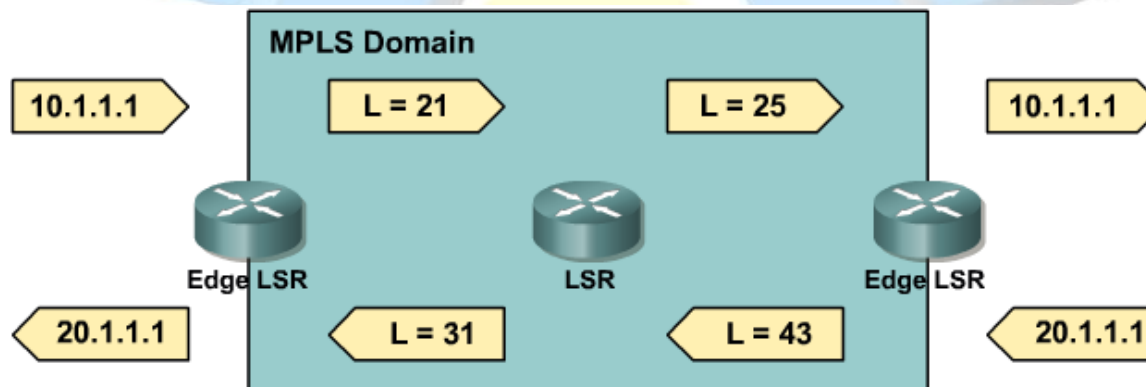
# Arquitectura MPLS

- Componentes del “Control Plane”:
  - El protocolo de enrutamiento de capa 3 se necesita para propagar la información de enrutamiento.
  - El mecanismo de intercambio de etiquetas es un mecanismo añadido que propaga las etiquetas que está usando el router para sus destinos conocidos.



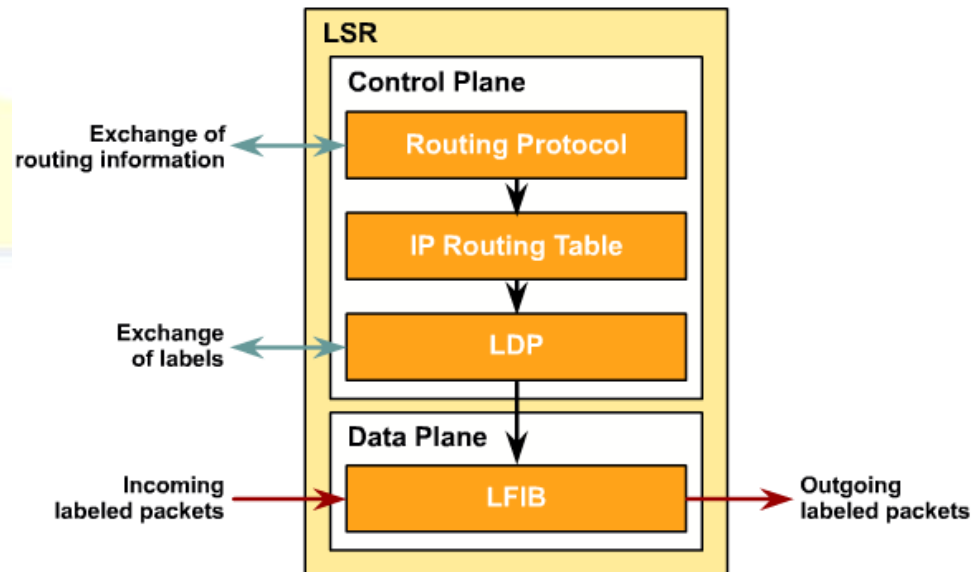
# Label Switch Routers

- LSR y Edge LSR envían paquetes tomando en base a la etiqueta MPLS. Habitualmente suelen realizar tareas tanto de enrutamiento IP como de conmutación basada en etiquetas.
  - LSR: Dispositivos que envían paquetes basándose fundamentalmente en etiquetas.
    - Todas sus interfaces tienen MPLS habilitado
  - Edge LSR: Dispositivo cuyo cometido principal es añadir y eliminar etiquetas.
    - Tienen 1 o más interfaces con MPLS activo y 1 o más interfaces con él inactivo
    - Son el límite de un dominio MPLS, que puede coincidir con el límite de un SA
    - Envían los paquetes basándose en el enrutamiento IP y en etiquetas, si la interfaz de salida tiene habilitado MPLS



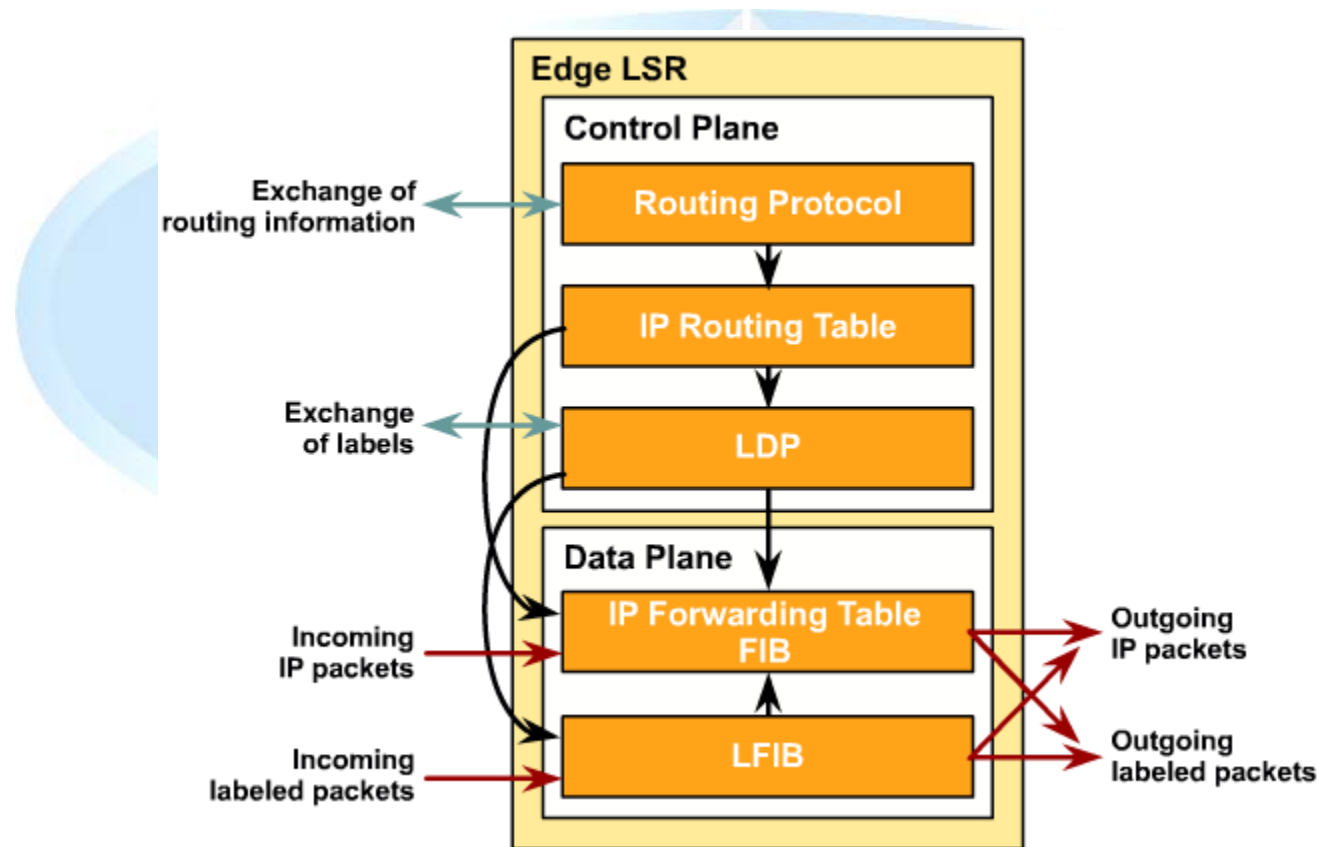
# Arquitectura de Componentes de un LSR

- Todos los LSRs:
  - Intercambian información de enrutamiento (Control Plane).
  - Intercambian etiquetas (Control Plane).
  - Envían paquetes (Data Plane).
    - En Frame Mode MPLS, los paquetes se envían en base a una etiqueta de 32 bits.
- Arquitectura de Componentes de un LSR.
  - Protocolo de enrutamiento.
  - Protocolo de intercambio de etiquetas
  - El LDP puebla la tabla LFIB.



# Arquitectura de Componentes de un LSR

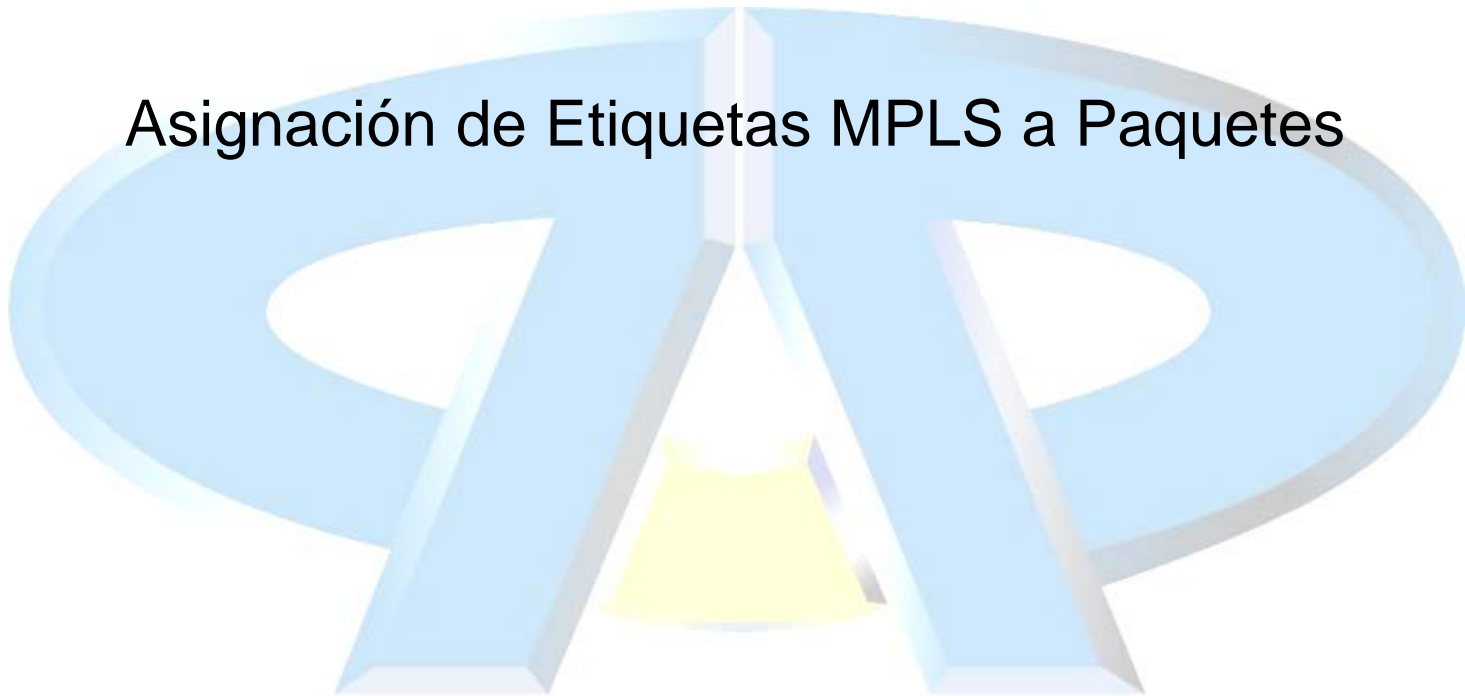
- Arquitectura de Componentes de un Edge LSR:



## Arquitectura de Componentes de un LSR

- Arquitectura de Componentes de un Edge LSR: Existen varias posibles combinaciones de envío y etiquetado de paquetes:
  - Enviar un paquete IP en base a la IP de destino y enviarlo como un paquete IP.
  - Enviar un paquete IP en base a la IP de destino y enviarlo como un paquete etiquetado.
  - Enviar un paquete etiquetado en base a su etiqueta, cambiar su etiqueta y enviarlo como un paquete etiquetado.
  - Enviar un paquete etiquetado en base a su etiqueta, eliminar su etiqueta y enviarlo como un paquete IP
- Escenarios posibles si la red no está debidamente configurada:
  - Un paquete etiquetado será eliminado si su etiqueta no existe en la tabla LFIB, incluso aunque su dirección IP de destino exista en la tabla FIB.
  - Un paquete IP será eliminado si su destino no se encuentra en la FIB, aunque exista una etiqueta para enviarlo hacia su destino.

## Asignación de Etiquetas MPLS a Paquetes





# Colocación de la Etiqueta en un entorno Frame Mode MPLS

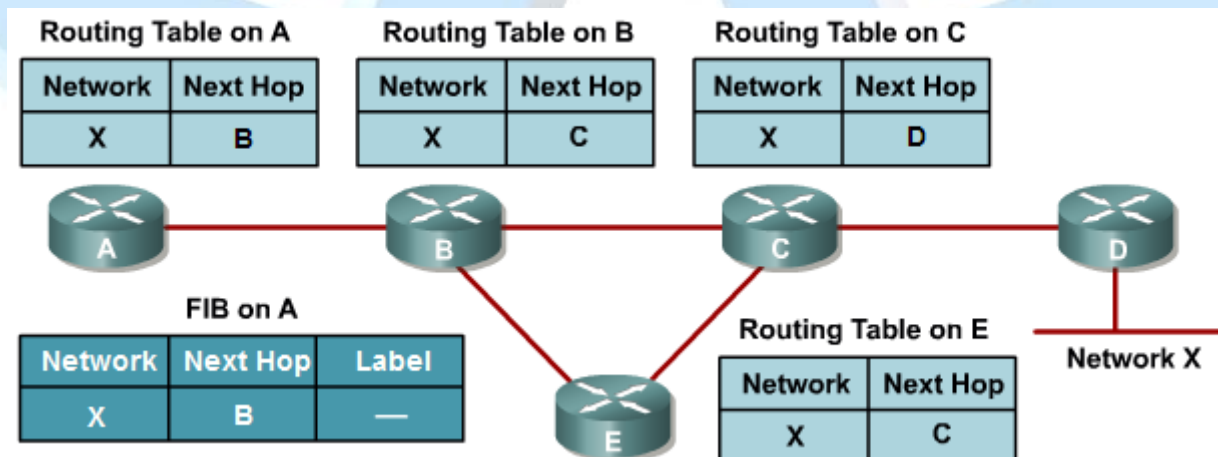
- Pasos para la colocación de una etiqueta y su distribución en una red con enrutamiento IP unicast y MPLS.
  1. Los routers intercambian información de sus rutas utilizando protocolos de enrutamiento IGP (OSPF, EIGRP...)
  2. Cada router genera sus etiquetas locales.
    - Se crea una etiqueta local única para cada ruta IP que se encuentra en la tabla de enrutamiento
    - Se almacena dicha información en la Label Information Base (LIB).
  3. Las etiquetas locales se publican a los routers vecinos adyacentes, donde estas etiquetas pasarán a ser “next-hop labels” para la ruta en cuestión
    - Se almacenan en la FIB y en la LFIB).
    - La publicación y aprendizaje de estas etiquetas habilita la conmutación en MPLS en todo el dominio
  4. Cada LSR construye su LIB, LFIB y FIB en base a las etiquetas recibidas
- La manipulación y uso de etiquetas se lleva a cabo en la red del proveedor, de forma completamente transparente para el cliente

# Colocación de la Etiqueta en un entorno Frame Mode MPLS

- Las siguientes estructuras de datos contienen la siguiente información:
  - LIB (control plane): Es la base de datos que utiliza “Label Distribution Protocol”.
    - En esta base de datos es donde se realiza la asignación para cada prefijo IP de una etiqueta con significado local que se mapea a la “next-hop label” recibida de un vecino “downstream”
  - LFIB (data plane): Es la base de datos que se utiliza para etiquetar los paquetes y enviar los paquetes etiquetados.
    - Las etiquetas locales, publicadas a los vecinos (upstream), se mapean a las “next-hop labels”, recibidas desde los routers vecinos (downstream).
  - FIB (data plane): Es la base de datos que se utiliza para enviar los paquetes no etiquetados
    - Un paquete a enviar se etiqueta si existe una “etiqueta next-hop” disponible para dicho prefijo. Si no existe, no se etiqueta.

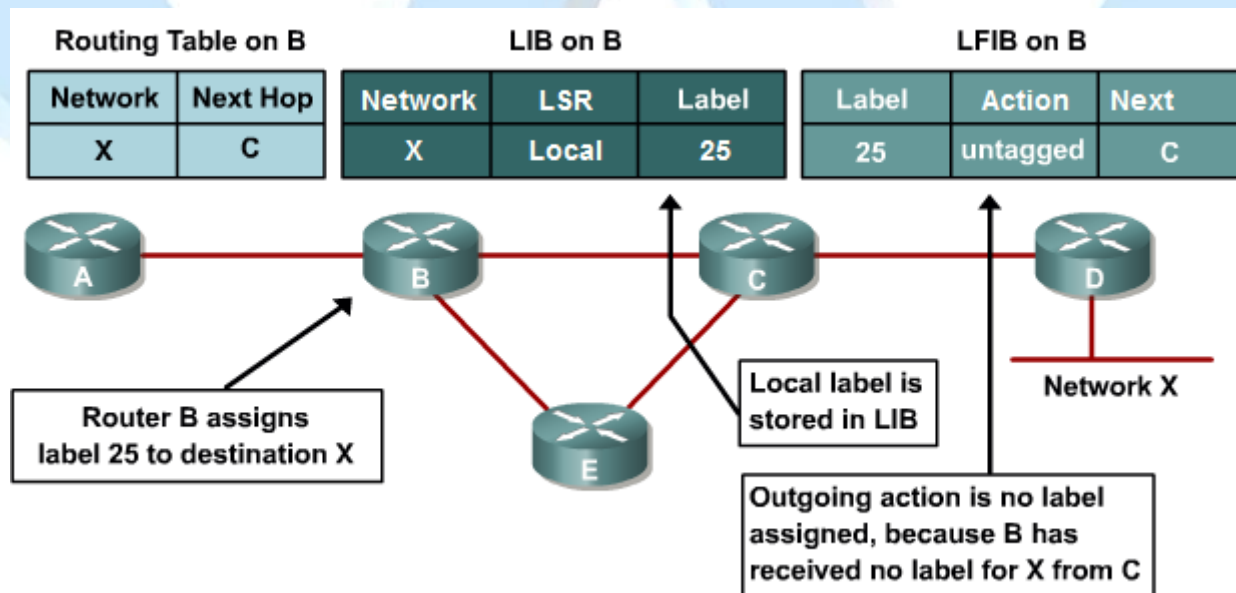
# Colocación de la Etiqueta en un entorno Frame Mode MPLS

- Asignación de etiquetas: Los routers aprenden las rutas mediante protocolos de enrutamiento IGP.
  - Si para una ruta determinada, no existe una “next-hop label”, los paquetes se envían utilizando enrutamiento convencional, como paquetes no etiquetados.
  - Los routers generan etiquetas locales para las rutas (asynchronous allocation of labels), pero no le sirven para enviar los paquetes utilizando esa información.
    - Las etiquetas desde la 0 a la 15 están reservadas.



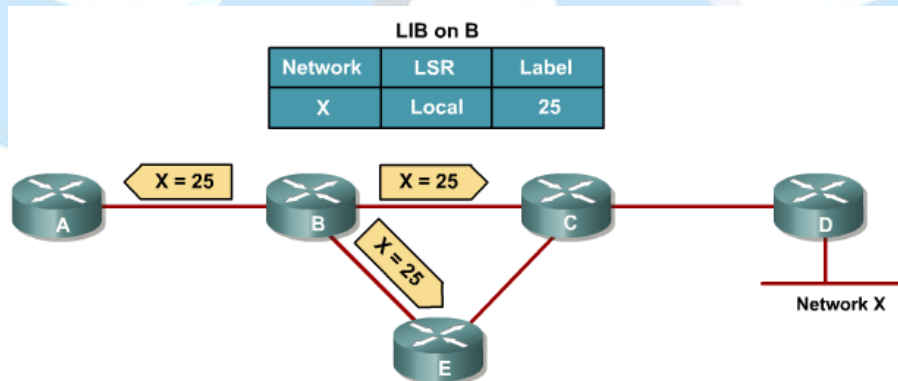
# Colocación de la Etiqueta en un entorno Frame Mode MPLS

- Configuración LIB y LFIB.
  - Cuando se asigna una etiqueta a un prefijo IP, dicha etiqueta se almacena en dos tablas: LIB y LFIB.
  - El router utiliza la tabla LIB para mantener el mapeo entre el prefijo IP, la etiqueta asignada y el router que la asigna (en este caso el propio router).
  - La tabla LFIB se modifica para contener la etiqueta local mapeada a la acción de envío.



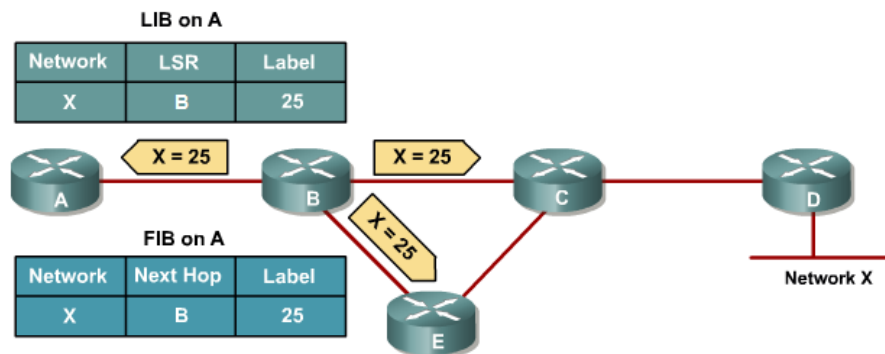
# Distribución de Etiquetas y Publicación

- El Protocolo de Distribución de Etiquetas (LDP) permite intercambiar las etiquetas MPLS y almacenarlas en la LIB.
  - Esta ubicado en el “control plane”
- Ejemplo: El router B ha asignado la etiqueta 25 a la ruta X, por lo que propaga dicha etiqueta a todos los vecinos.
  - Los vecinos usarán esa etiqueta como next-hop label.
  - B almacena dicha etiqueta en su propia LIB, como ruta local.



## Distribución de Etiquetas y Publicación

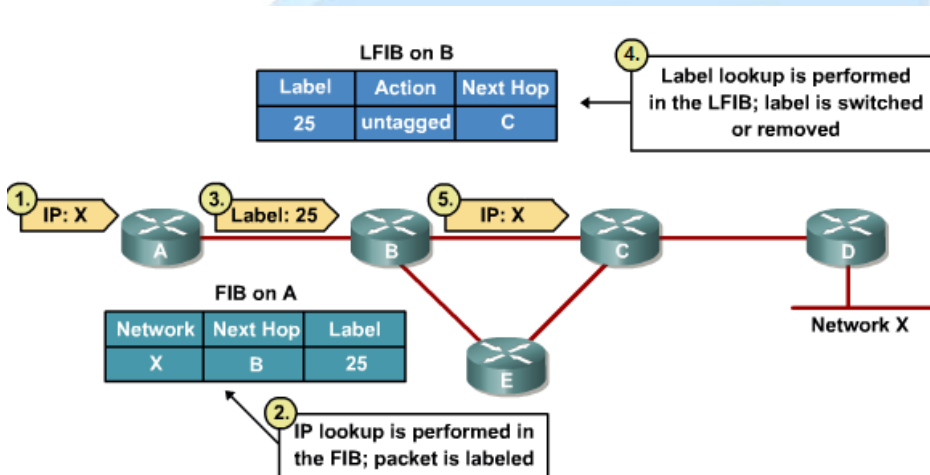
- Ejemplo: Después de recibir la actualización LDP del router B, los routers A, C y E añaden la nueva información a sus tablas LIB, LFIB y FIB
  - La etiqueta 25, recibida desde el LSR B, se almacena en la tabla LIB (control plane) como una etiqueta para la red X, lo que en el router A habilita la funcionalidad de Edge LSR.
    - Los paquetes entrantes destinados a la red X se envían como paquetes etiquetados
  - La etiqueta 25 se vincula a la entrada de envío IP de la tabla FIB correspondiente a la red X
  - En la tabla LFIB se elimina la acción “untagged” y se establece que los paquetes entrantes destinados a la red X se etiqueten con el valor “25”.





# Distribución de Etiquetas y Publicación

- Propagación de paquetes provisional a través de una red MPLS:
  - Envío de un paquete a través de una red MPLS que todavía no ha convergido.
  - ¿Qué sucede cuando llega un paquete destinado a una red X y dicha red no tiene etiqueta en todos los routers del dominio MPLS?



- Llega un paquete IP no etiquetado a A.
- El paquete se envía utilizando la información de la tabla FIB, en la que se ha asociado una etiqueta a la entrada X
- El paquete se envía al next-hop router, B.
- B elimina la etiqueta debido a que todavía no ha recibido su una “next-hop-label” para esa red.
- Envía el paquete IP estándar

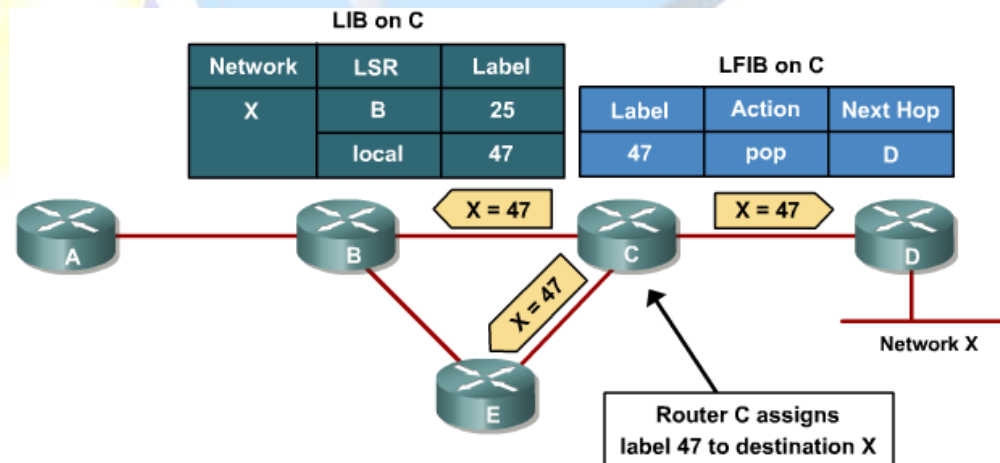


# Distribución de Etiquetas y Publicación

## Cuestiones avanzadas de asignación de etiquetas. Penultimate Hop Popping.

- Todos los routers MPLS realizan las mismas acciones que se han comentado para A y B en los ejemplos anteriores, lo que permite crear un “label switch path” entre A y D.
- En este caso el router D publica su etiqueta para la red X.
  - Como la red X está directamente conectada al router D, en su publicación envía una etiqueta “implicit null”.
  - Esta etiqueta indica que esta red está directamente conectada a dicho router y por lo tanto debe recibir los paquetes ya sin etiqueta, por lo que en este caso C, enviará a D el paquete IP.

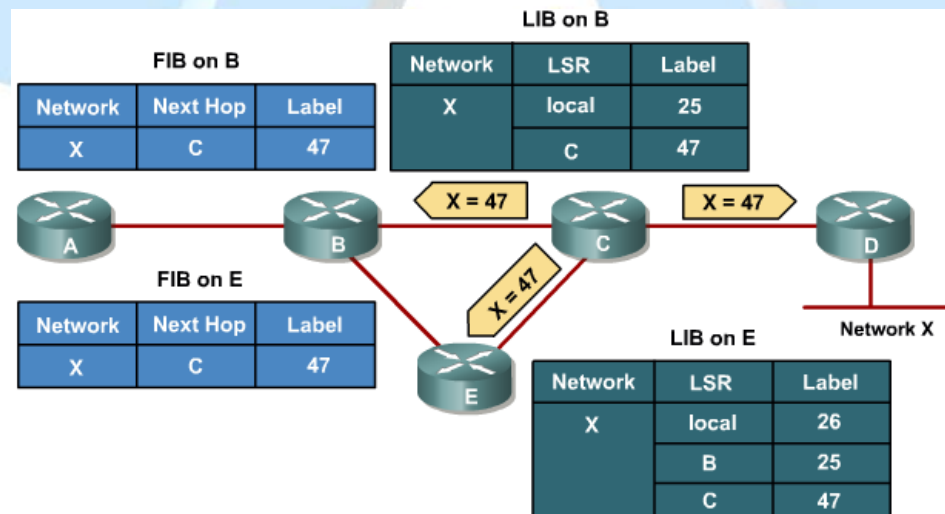
Este comportamiento se denomina **Penultimate Hop Popping**.



# Distribución de Etiquetas y Publicación

## Recepción de etiquetas

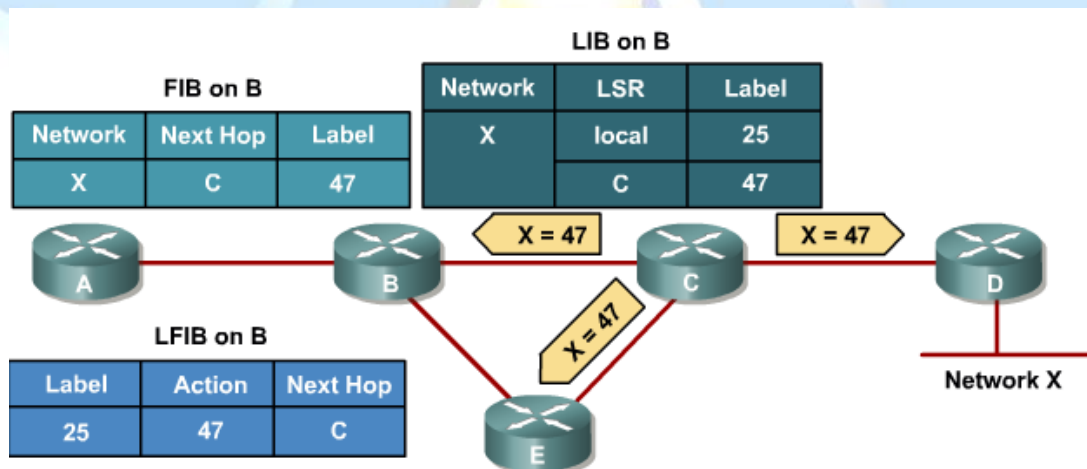
- Actualización de la tabla de etiquetas (LIB) y la tabla de envío FIB.
- Ejemplo: By E
  - B puede mapear la entrada para la red X de su tabla FIB, que tiene asociada la etiqueta local 25, con la etiqueta publicada por su next-hop downstream hacia la red X, que es el router C, y que se corresponde con la etiqueta 47.
  - En el ejemplo, E ha asignado la etiqueta 26 a la red X y ha recibido para la misma red las etiquetas 25 desde el router B y 47 desde el router C



# Introducción de información en la tabla LFIB

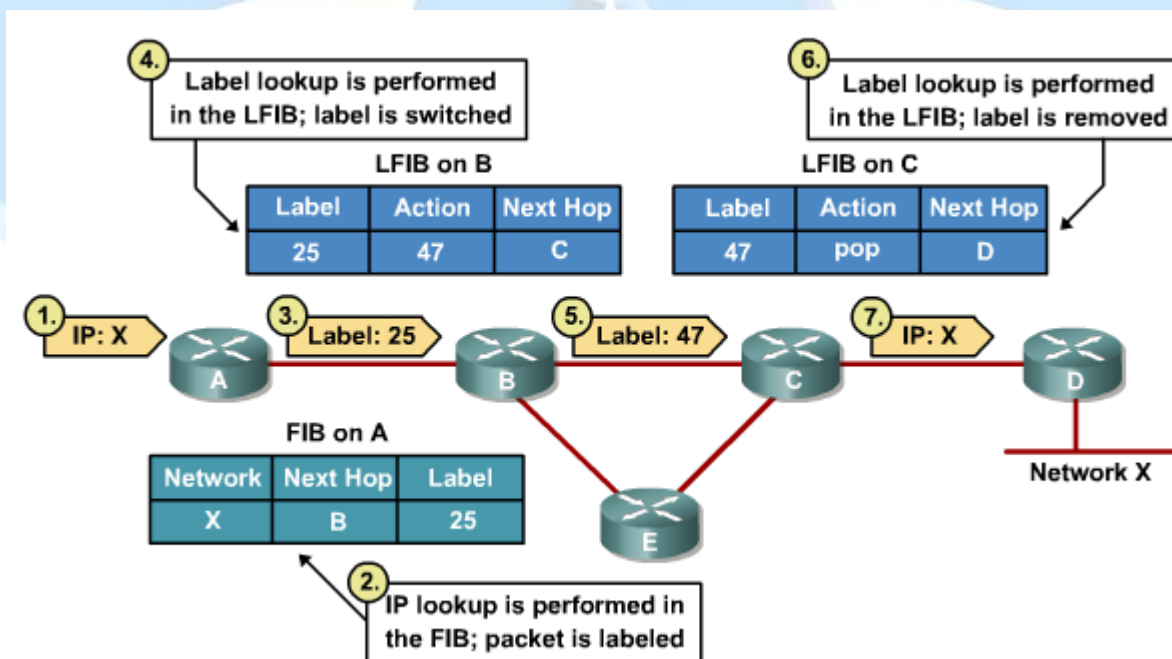
## Introducción de información en la tabla LFIB

- En MPLS, los protocolos de enrutamiento introducen la información en las tablas de enrutamiento y LDP propaga las etiquetas.
- Cada router determina cuál es la mejor ruta hacia su destino utilizando la información de las tablas de enrutamiento.
- En la tabla LFIB, se establece para cada ruta, la etiqueta propia, la etiqueta de “next-hop” y la acción a llevar a cabo.
  - La acción puede ser: cambiar la etiqueta, añadir una etiqueta o eliminar etiqueta



# Propagación de Paquetes en una Red MPLS

- Si a un LSR llega un paquete IP este se enviará utilizando la información de la tabla FIB, bien como paquete IP (no tiene next-hop label) o bien como paquete etiquetado.
- Si un LSR recibe un paquete etiquetado lo envía utilizando el contenido de la tabla LFIB, bien como paquete etiquetado o bien como paquete IP.
- Ejemplo:

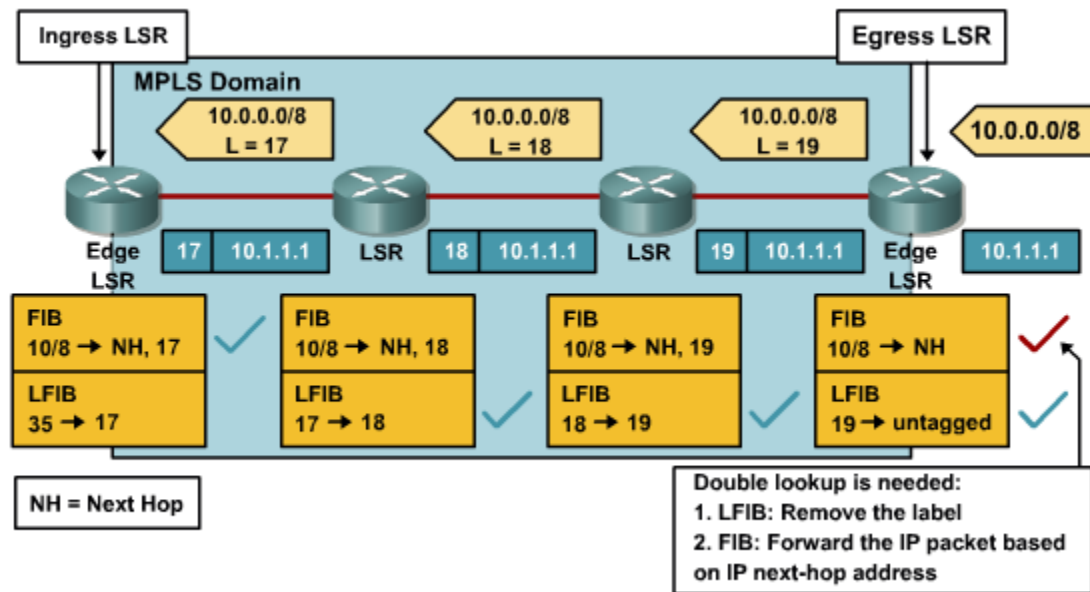


## Penultimate Hop Popping

- Mediante PHP, un LSR elimina la etiqueta externa de un paquete MPLS etiquetado antes de pasárselo al router Edge LSR adyacente.
  - PHP ha de ser implementado con cuidado en las redes que ofrecen ciertos servicios de QoS.
  - Los Edge routers no usan PHP.
- Sin PHP los Edge LSR realizan como mínimo dos búsquedas de etiqueta:
  - Etiqueta externa: Indica que el paquete estaba destinado a que su etiqueta se elimine en dicho router.
  - Etiqueta interna: Esta etiqueta identifica que instancia de Virtual Routing/Forwarding usar, y por lo tanto, provoca la consiguiente búsqueda en la tabla de enrutamiento.
- PHP reduce la carga de CPU de los Edge LSR distribuyendo el trabajo entre los vecinos.
- PHP mejora el rendimiento de MPLS, eliminando las búsqueda de rutas en los LSR de salida y reduciendo la búsqueda de etiquetas.
- Cuando el “downstream” router se da cuenta de que es el nodo final del camino conmutado, distribuye una etiqueta *imp-null* (valor 3), para indicarle al router anterior que en lugar de conmutar la etiqueta debe eliminarla.

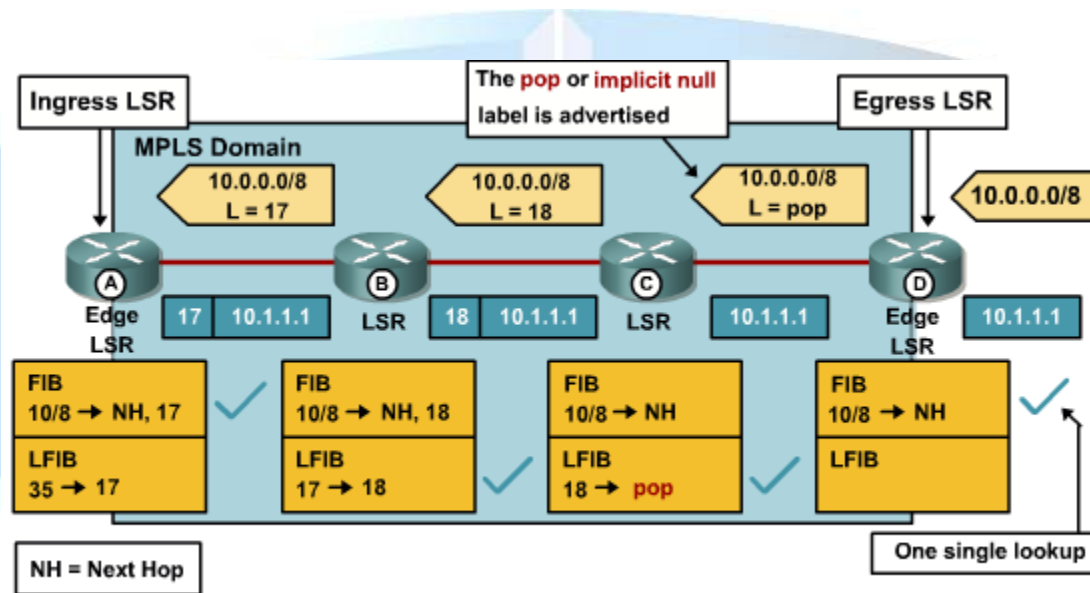
# Penultimate Hop Popping

- MPLS sin PHP




# Penultimate Hop Popping

- MPLS con PHP







# Configuración de MPLS

# Configuración de MPLS

## 1. Activar Cisco Express Forwarding (CEF)

```
Router(config)# ip cef [distributed]  
Router(config-if)# ip route-cache cef
```

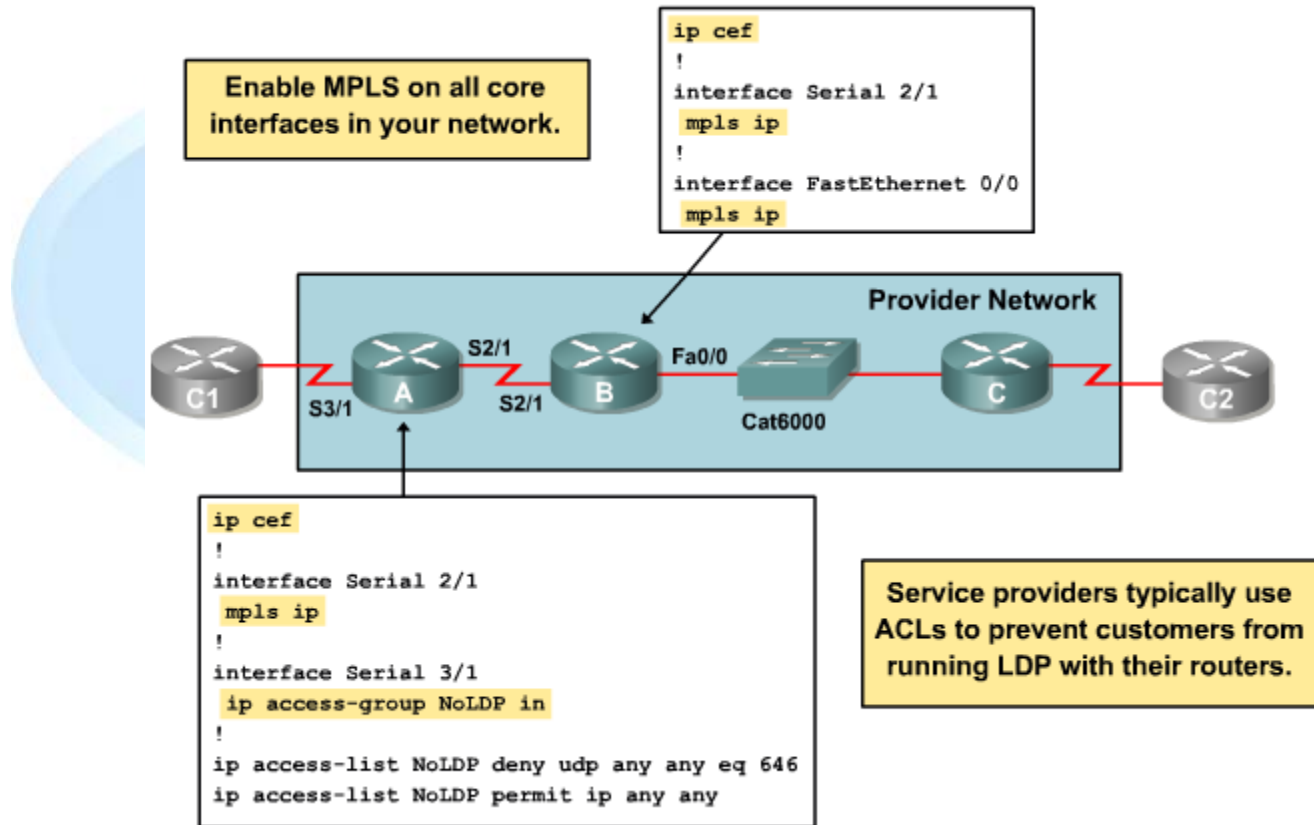
## 2. Configurar MPLS en todas las interfaces que se desea que participen en el protocolo

- Está activo por defecto en las nuevas configuraciones, pero es necesario especificar que interfaces participarán en MPLS

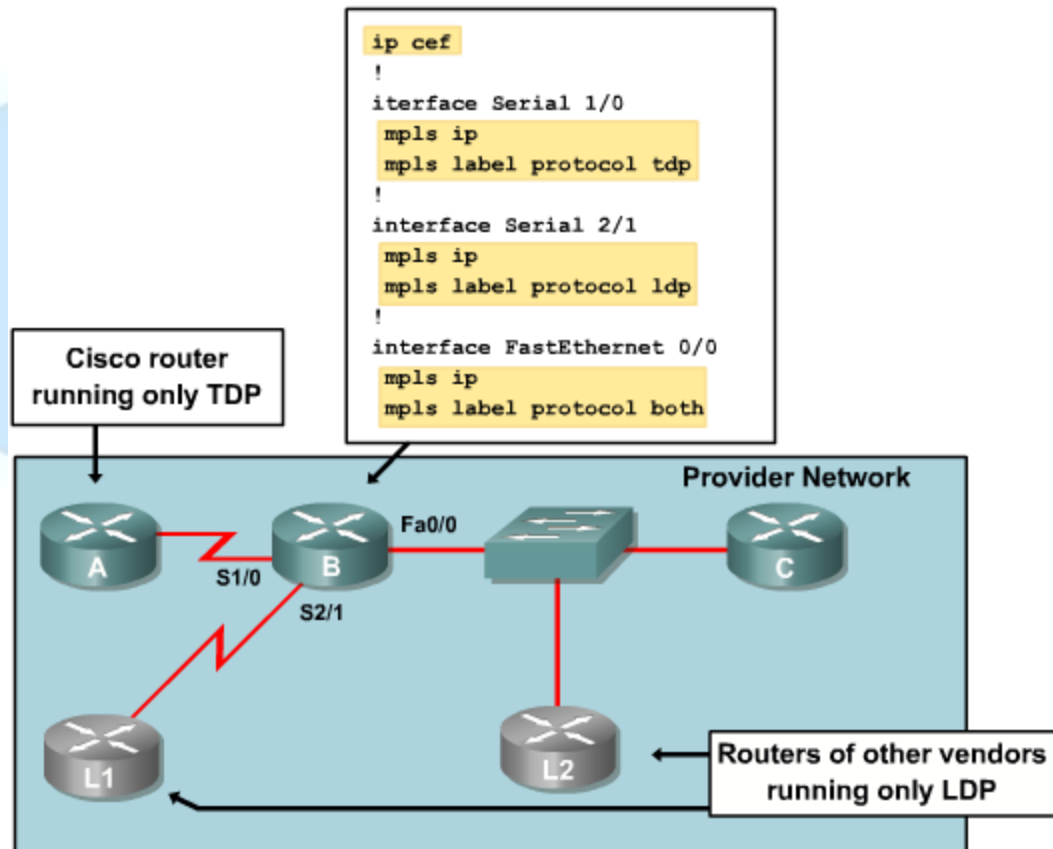
```
Router(config-if)# mpls ip /no mpls ip  
Router(config-if)# mpls label protocol TDP | LDP
```

## 3. Configurar el tamaño de la MTU de las interfaces (opcional)

## Ejemplo de Configuración



## Ejemplo de Configuración

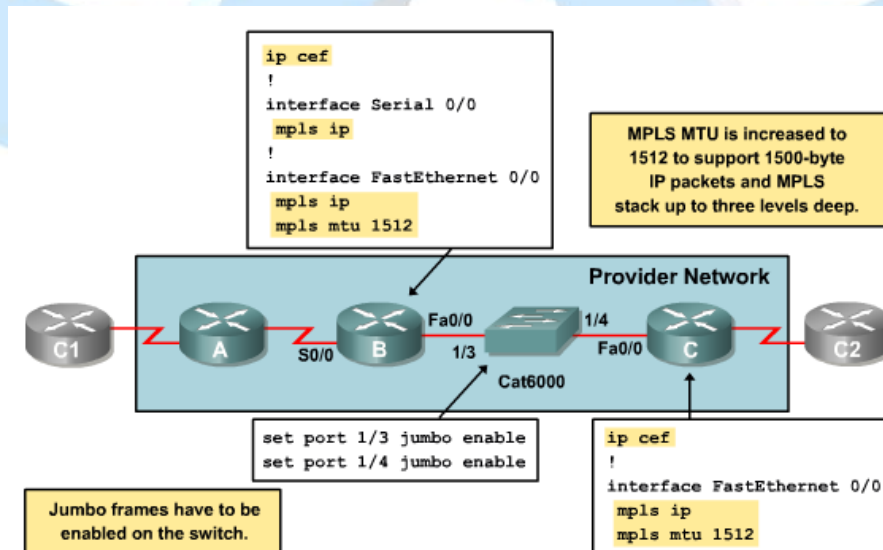


# Protocolos de distribución de etiquetas en MPLS

- Tag Distribution Protocol (TDP):
  - Propio de Cisco.
  - Usa un protocolo de capa de transporte orientado a conexión (TCP).
  - Distribuir, solicitar y liberar información sobre las etiquetas de diferentes protocolos.
  - Abrir, monitorizar y cerrar sesiones TDP.
- Label Distribution Protocol (LDP):
  - Protocolo estándar de distribución dinámica de etiquetas salto a salto.
  - Produce como resultado, junto con los IGPs correspondientes, Label Switched Paths (LSPs)
  - LDP permite solicitar, distribuir y liberar información de los vínculos prefijo-etiqueta.
  - LDP permite descubrir potenciales “peers” y establecer sesiones LDP con ellos.

# Configuración del tamaño de MTU

- Debido a que la etiqueta que se coloca en la cabecera es un campo adicional, aumentar el tamaño de la MTU puede evitar que se incremente la fragmentación.
  - MPLS puro, las MTU de las interfaces Ethernet debería pasar a ser 1504 bytes
  - MPLS VPN → 1508 (dos etiquetas)
  - MPLS VPN TE → 1512
- El aumento del tamaño de la MTU puede generar problemas en algunos switches, que descartarán las tramas



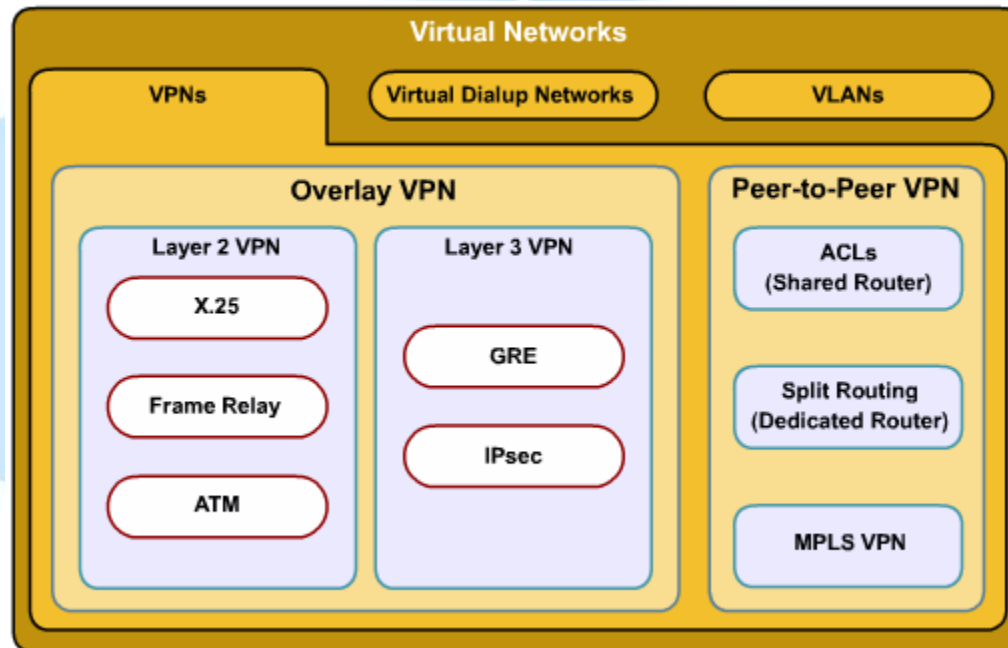
# Tecnología MPLS VPN



# Arquitectura de las VPNs sobre MPLS

- Conceptos relacionados con VPNs:
  - VLANs: Implementación de LANs aisladas sobre una infraestructura de red única
  - VPDNs: Permite usar la infraestructura de “dial-up” de un SP para establecer conexiones privadas.
  - VPNs: Permite utilizar la infraestructura de un SP para implementar redes privadas. Existen dos modelos:
    - Overlay VPNs: Incluye tecnologías como X.25, Frame Relay, ATM, GRE e IPsec
      - Permite el establecimiento de VPNs punto a punto entre las diferentes sedes del cliente.
    - **Peer-to-peer VPNs:** Se implementa mediante routers y filtros, con routers independientes para cada cliente o mediante el uso de MPLS.
      - Los SPs participan en el enrutamiento del cliente.

# Arquitectura de las VPNs sobre MPLS



# Arquitectura de las VPNs sobre MPLS

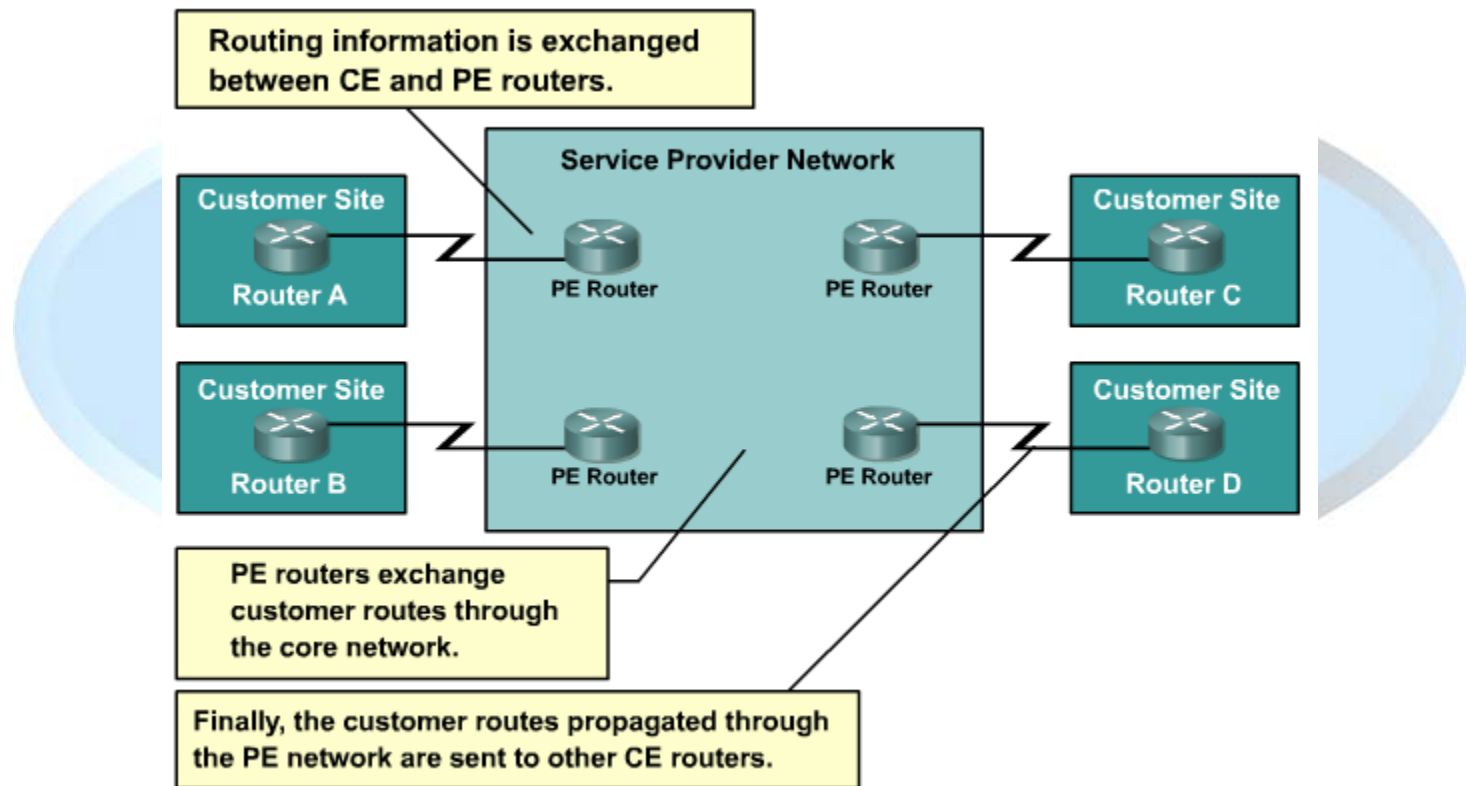
- Overlay VPNs:
  - Capa 2: Se corresponde con el modelo tradicional de tecnologías WAN conmutadas.
    - Tecnologías: X.25, Frame Relay, ATM
    - Los SPs crean circuitos virtuales entre las diferentes sedes de los clientes.
    - El SP es el responsable de transportar las tramas del cliente entre las diferentes ubicaciones.
    - La gestión del tráfico a nivel de capa 3 y superiores depende del cliente solamente, como por ejemplo el enrutamiento entre diferentes sedes de una organización conectadas a través de una red “frame relay” con topología “hub & spoke”.
  - Capa 3: Las técnicas de “tunneling” IP permiten alcanzar un determinado destino sin que el origen tenga que conocer la exactamente la topología intermedia.
    - Permite “unir” (con interfaces lógicas que simulan conexiones directas) dispositivos que no están físicamente conectados
    - Tecnologías: GRE o IPsec.

# Arquitectura de las VPNs sobre MPLS

- **Peer-to-Peer VPNs:**

- El modelo “peer-to-peer” se basa en la utilización de un **esquema de enrutamiento único para cada cliente**.
- Tanto las redes del cliente como las del proveedor utilizan el mismo protocolo de red y el SP “transporta” las rutas del cliente entre las diferentes ubicaciones.
  - Los routers fronterizos del ISP (**Provider Edge, PE**) intercambian información de enrutamiento con los routers fronterizos del cliente (**Customer Edge, CE**), estableciendo adyacencias de enrutamiento en cada sede diferente
  - Esta estructura es óptima para realizar conexiones multipunto, sobre todo “full-mesh”, puesto que evita la necesidad de múltiples interfaces físicas o circuitos virtuales.
  - Sistema escalable y fácilmente mantenible, puesto que no necesita añadir nuevos circuitos físicos o virtuales si se añade una nueva localización.
- En este modelo, **el SP acepta las rutas del cliente, las transporta a través de su infraestructura de red y las envía a los router de cliente adecuados en las ubicaciones remotas**

## Arquitectura de las VPNs sobre MPLS



# Arquitectura de las VPNs sobre MPLS

Ventajas e inconvenientes del modelo “Overlay VPN”:

- Ventajas:
  - La tecnología está muy extendida
  - La implementación es sencilla tanto para el cliente como para el proveedor
  - El SP no participa en el enrutamiento del cliente, con lo cual es sencillo definir la separación entre el dominio de enrutamiento del proveedor y del cliente.
- Desventajas:
  - Overlay de capa 2 necesita una topología “full-mesh” de CVs entre los clientes para un enrutamiento óptimo entre las diferentes sedes.
  - Los VCs deben ser provisionados manualmente y el ancho de banda es asignado “site-to-site”
  - Overlay de capa 3 añade sobrecarga de encapsulamiento: Entre 20 y 80 bytes por datagrama transportado

# Arquitectura de las VPNs sobre MPLS

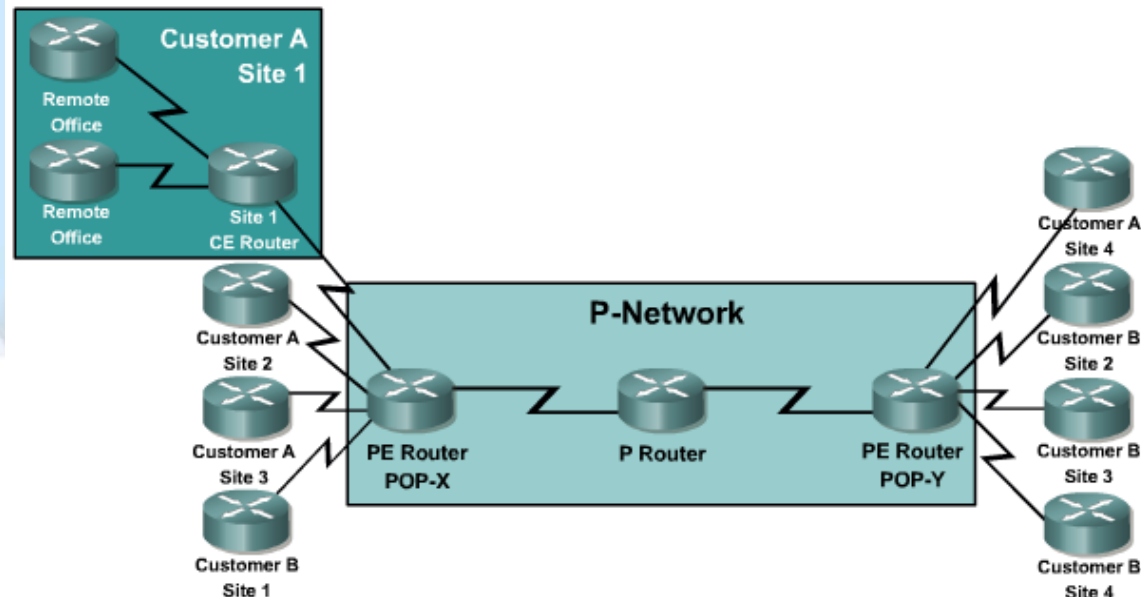
Ventajas e inconvenientes del modelo “Peer-to-peer VPN”:

- Ventajas del modelo “Peer-to-peer VPN”:
  - Enrutamiento óptimo entre los diferentes “sites” del cliente sin necesidad de ningún diseño especial o esfuerzo de configuración
  - Cada nueva sede del cliente puede añadirse sin la necesidad de enlaces adicionales.
- Desventajas del modelo “Peer-to-peer VPN”:
  - Para el SP:
    - El SP es responsable del enrutamiento correcto en las redes del cliente (C-Network), así como de la convergencia rápida.
    - Los PE de los SPs tienen que transportar todas las rutas entre los diferentes sites.
  - Para el cliente:
    - Es necesario un diseño global de los esquemas de direccionamiento IP.
    - Este tipo de VPNs se basan en filtros que pueden requerir un alto coste computacional
    - La implementación de “peer-to-peer” VPN basadas en routers PE dedicados para cada cliente es fácil de mantener y presenta un buen rendimiento, pero tiene un coste prohibitivo → Alternativa: Uso de VRF



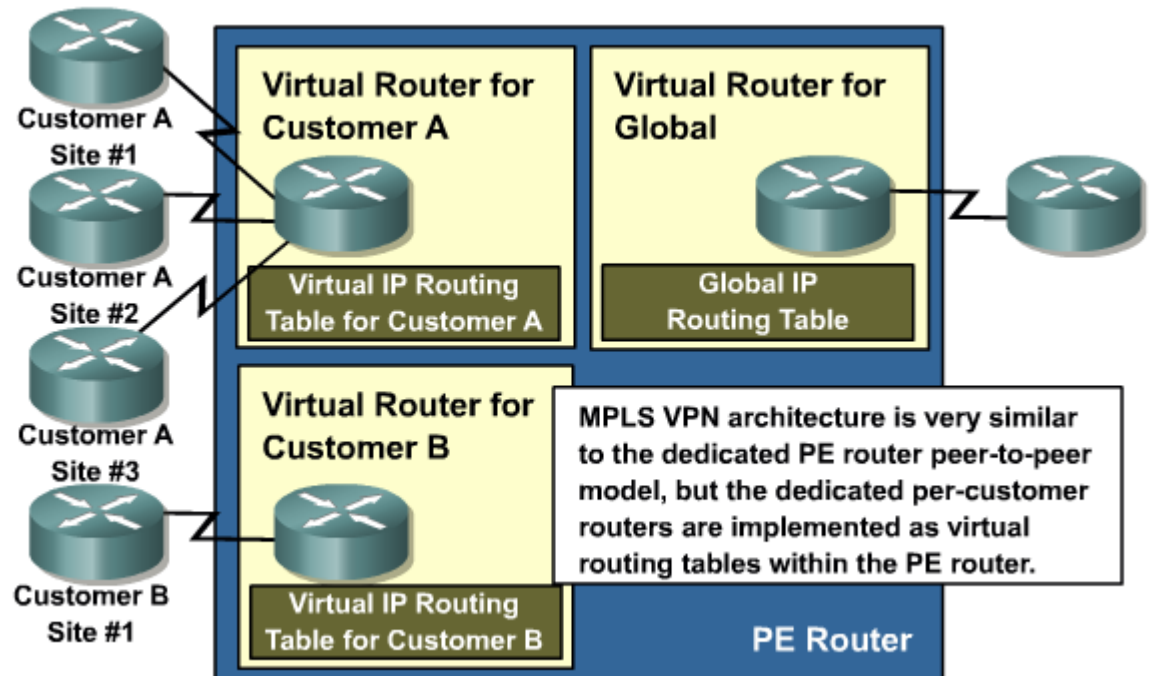
# Arquitectura de las VPNs sobre MPLS

- La arquitectura de VPNs sobre MPLS se compone de:
  - Routers PE que participan en el enrutamiento del cliente, garantizando el enrutamiento óptimo entre las diferentes sedes del cliente
  - Los router PE utilizan una tabla de enrutamiento virtual separada para cada uno de sus clientes, proporcionando de esta forma aislamiento entre los diferentes clientes.
  - Los clientes pueden solapar su direccionamiento, es decir, diferentes clientes pueden utilizar el mismo espacio de direcciones.
- La red se compone de 2 partes:
  - Controlada por el cliente o **C-Network**:
    - Sites
  - Controlada por el proveedor o **P-Network**



## Arquitectura de las VPNs sobre MPLS

- Un router PE en una VPN sobre MPLS contiene una tabla de enrutamiento independiente para cada cliente. Dicha tabla se denomina “**Virtual Routing and Forwarding table**”.
  - Cada una de estas tablas de enrutamiento se correspondería con router individual dedicado, en un modelo tradicional peer-to-peer.
  - El enrutamiento a través de la red del SP se lleva a cabo por medio de otro proceso de enrutamiento que utiliza una tabla de enrutamiento IP principal o global.
- IOS implementa el aislamiento utilizando tablas VRF, con lo que el router se configurará como un solo dispositivo, que ejecutará diferentes instancias de protocolo de enrutamiento

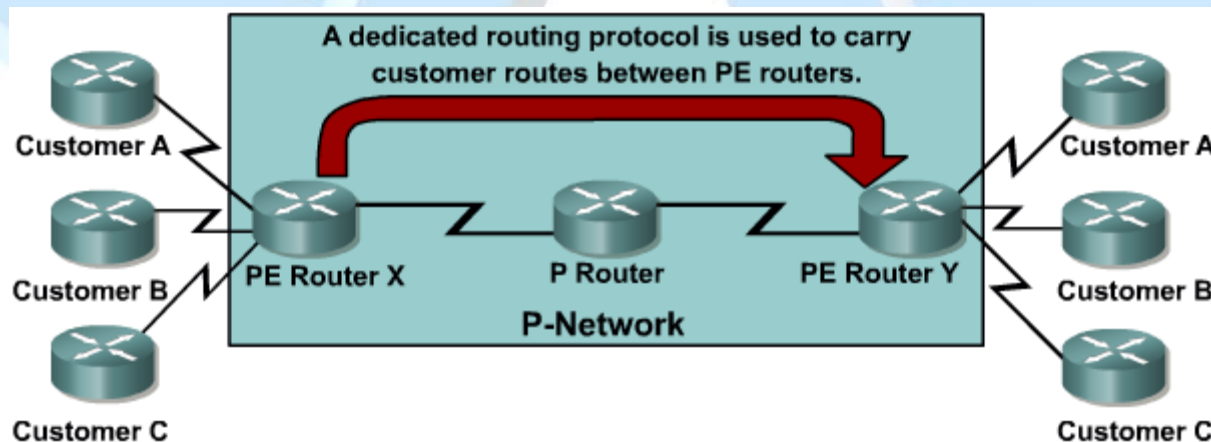


# Arquitectura de las VPNs sobre MPLS

- Propagación de la información de enrutamiento a través de la P-Network
  - Aunque VRF proporciona aislamiento entre los clientes, los datos de sus tablas de enrutamiento tienen que intercambiarse utilizando los routers del SP
  - Es necesario seleccionar un protocolo de enrutamiento que transporte todas las rutas de los clientes a través de la P-Network, manteniendo la independencia de los espacios de direccionamiento de cada uno de los clientes individuales.
  - La mejor solución para la propagación de rutas de cliente es ejecutar un único protocolo de enrutamiento entre los routers PE que intercambiarán todas las rutas de usuario sin implicar a los routers P
- Ventajas:
  - El número de protocolos de enrutamiento ejecutándose entre los routers PE no se incrementa al aumentar el número de clientes
  - Los routers P no son conscientes de transportar rutas de cliente

# Arquitectura de las VPNs sobre MPLS

- Se utiliza como protocolo de enrutamiento entre los PE el protocolo BGP debido a que:
  - El número de rutas a gestionar puede ser muy alto
  - Protocolo estándar ampliamente implantado
  - Permite establecer relaciones de vecindad entre los PE, directamente
    - Basadas en TCP
  - Las actualizaciones pueden enviar atributos que facilitan la gestión de rutas provenientes de diferentes clientes: Atributo **Community**

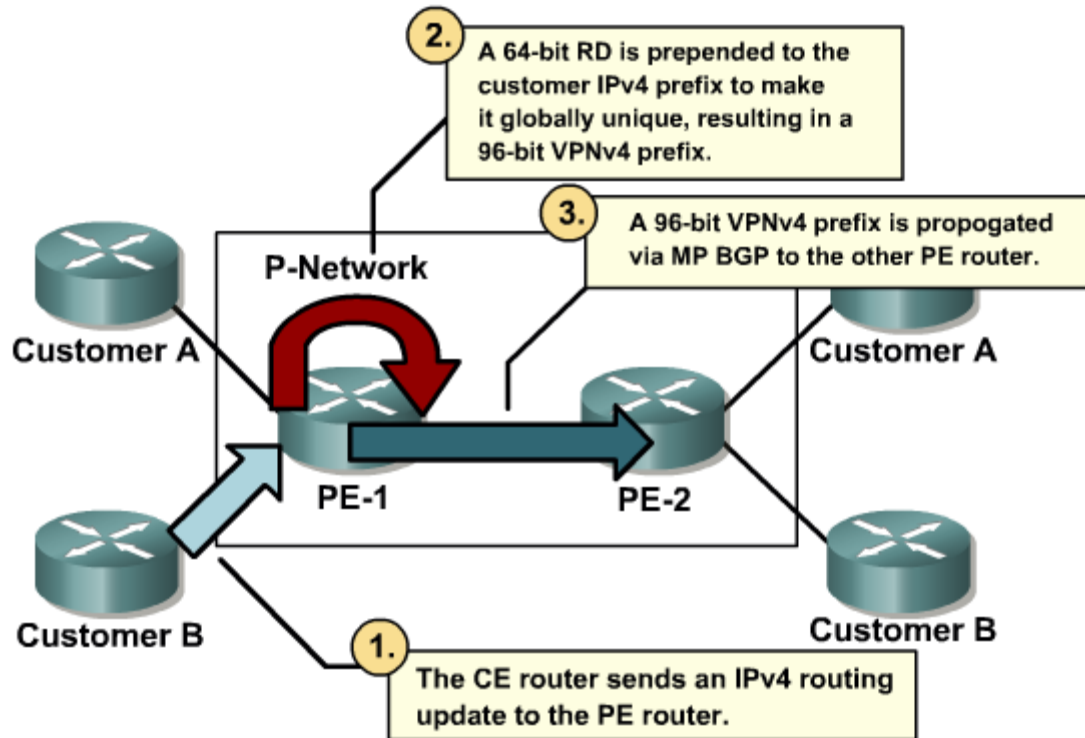


## Arquitectura de las VPNs sobre MPLS

- ¿Cómo se pueden propagar varios prefijos iguales (es decir rutas iguales), pertenecientes a diferentes clientes entre varios PE, manteniendo el aislamiento y usando un solo protocolo de enrutamiento?
  - La identificación de las rutas se expande creando un prefijo único que hace que las rutas, aunque previamente fuesen iguales, se diferencien para cada cliente
  - MPLS VPNs utiliza un prefijo llamado “route distinguisher” (RD) para convertir una ruta de un cliente de 32 bits, no necesariamente única, en una dirección de 96 bits única que será transportada entre los routers PE.
    - Estas direcciones reciben el nombre de direcciones VPNv4
  - Las direcciones VPNv4 solamente se intercambian entre los routers PE
  - Deben establecerse sesiones BGP entre los PEs previamente. Dicha sesión puede soportar múltiples protocolos, entre ellos MP-BGP (Multi-Protocol BGP)
- Las etiquetas RD no tienen ningún significado especial, solo sirven para generar rutas únicas
- El RD se configura solamente en el PE como parte de la configuración del VPN site y no es visible para el cliente final
- Sin embargo, si se utilizase RD como identificador de cliente, no se podrían soportar topologías en los que se quisiese enviar información entre diferentes clientes

# Arquitectura de las VPNs sobre MPLS

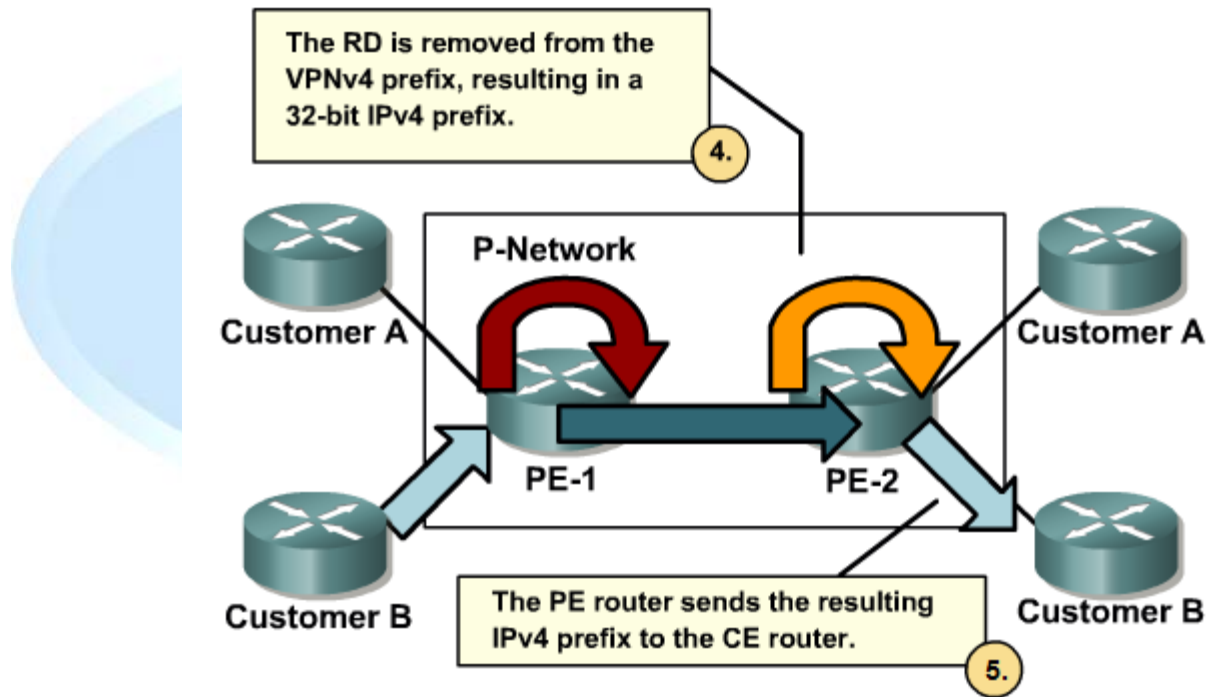
- Propagación de las rutas de cliente a través de una red VPN MPLS:





## Arquitectura de las VPNs sobre MPLS

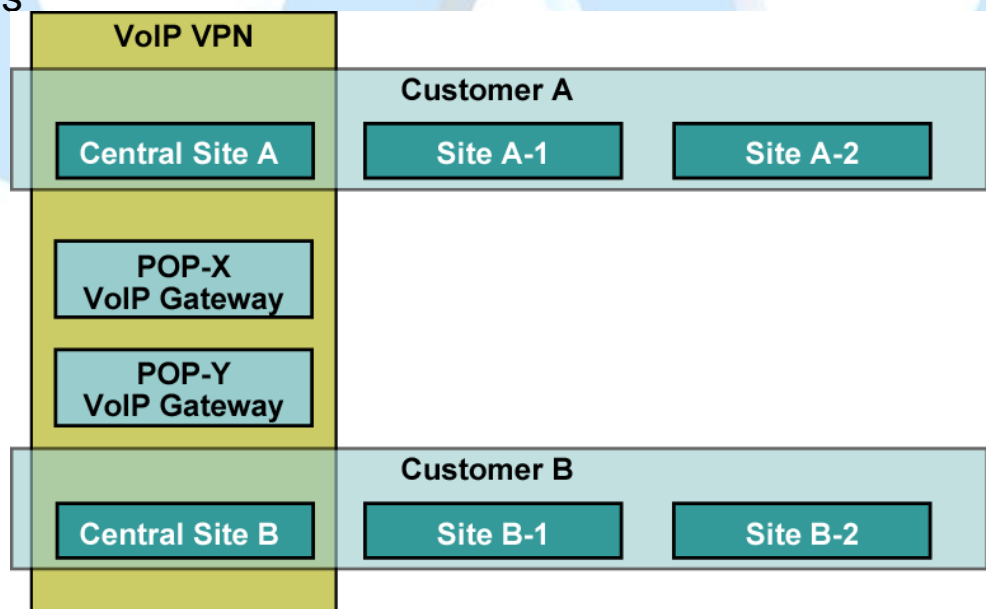
- Propagación de las rutas de cliente a través de una red VPN MPLS:





# Arquitectura de las VPNs sobre MPLS

- Ejemplo de red corporativa: Servicio de VoIP sobre una MPLS VPN: Requisitos:
  - Todas las sedes de un cliente deben comunicarse entre ellas
  - Las sedes centrales de ambos clientes necesitan comunicarse con las pasarelas VoIP
  - El resto de sedes, que pertenecen a clientes diferentes, no deben poder comunicarse entre ellas
- La utilización de “Route Distinguisher” como identificador de cliente no permitiría cumplir estas restricciones

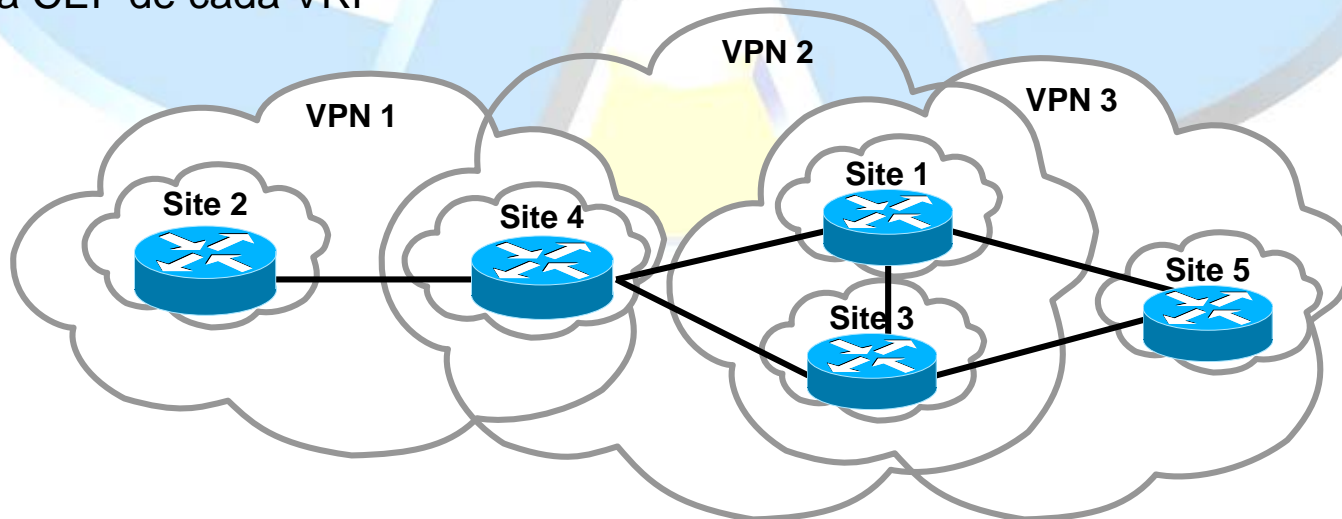


# Arquitectura de las VPNs sobre MPLS

- Cada VPN se asocia con una o más instancias VRF.
- Una VRF define la pertenencia a la VPN de un sitio de cliente conectado a un router PE.
- Una VRF consta de:
  - Tabla de enrutamiento IP
  - Tabla CEF
  - Conjunto de interfaces que utiliza la tabla de envío
  - Conjunto de reglas de enrutamiento
  - Parámetros de enrutamiento
- No tiene por que existir una relación 1 a 1 entre los clientes y las VPNs. Por ejemplo, un site puede pertenecer a múltiples VPNs.
- Sin embargo un site puede solamente asignarse a una VRF, que contiene todas las rutas disponibles para el site.

# Arquitectura de las VPNs sobre MPLS

- Problema: ¿Cómo sabe el router que rutas deben ser insertadas en cada tabla VRF?
  - **Router Target:**
    - Cada ruta VPN es etiquetada con uno o más “route targets” cuando se exporta desde un VRF, lo que le permite ser “ofertada” o “publicada” a otros VRFs.
    - Para insertar una ruta en un VRF se debe etiquetar con el **Route Target** adecuado que referencia al VRF o VRFs en los que podría ser insertada la ruta.
  - La información de envío de paquetes se almacena en la tabla de enrutamiento y en la tabla CEF de cada VRF

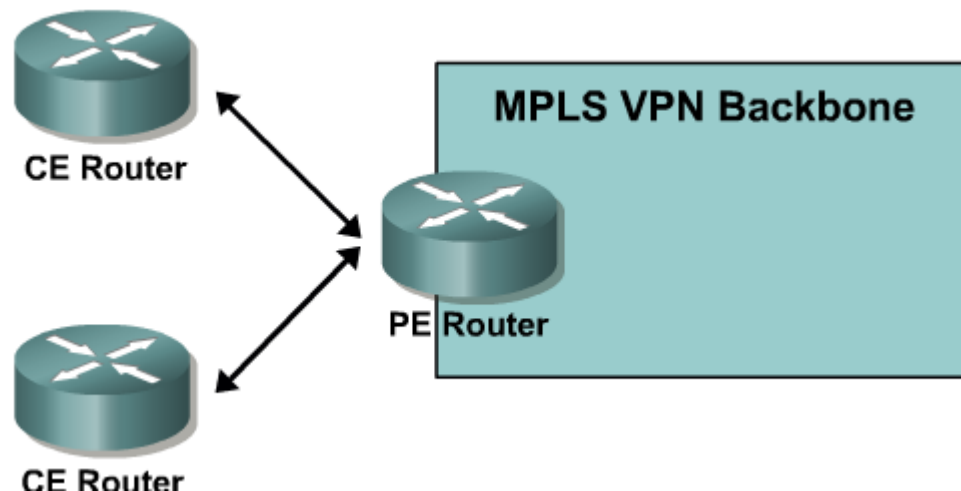


# Arquitectura de las VPNs sobre MPLS

- La distribución de la información de enrutamiento de las VPN se lleva a cabo utilizando **“VPN Route Target Communities”**, que se implementa en BGP con el atributo **“Extended Communities”**.
  - Cuando se aprende una ruta VPN desde un CE, ésta se inyecta en BGP y se le asocia una lista de atributos **“Route Target Extended Community”** (que puede constar de un solo elemento)
    - Esta lista contiene todos los atributos que definen los **Route Targets** que están asociados con los VRF que deben aprender dicha ruta
  - Se asocia una **“import list of route target extended communities”** con cada VRF. Esta lista define los atributos **community** que una ruta debe tener para ser importada por un VRF.
    - Ejemplo: Si la **import list** de un VRF incluye las **target communities A, B y C**, cualquier ruta que contenga el atributo **community A, B o C** será incluida en dicho VRF.

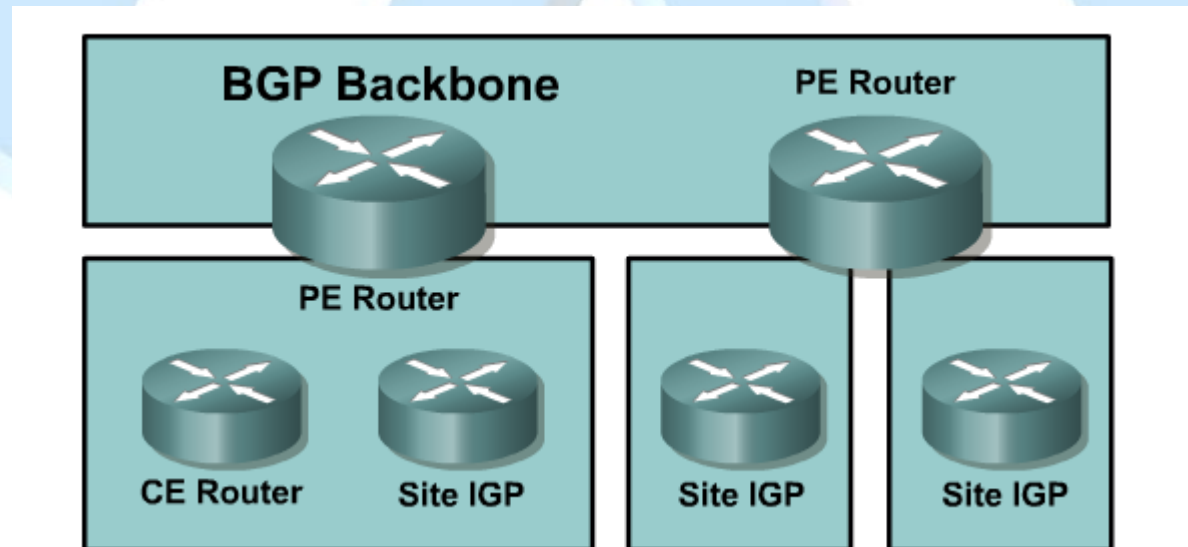
# Arquitectura de las VPNs sobre MPLS

- Los routers CE ejecutan mecanismos de de enrutamiento estándar para intercambiar información con los PE: RIP, OSPF, EIGRP, ...
  - El enrutamiento se configura individualmente en los VRFs del PE
- Para la red de cliente, el VRF que el corresponde en el router PE aparece en su topología como un router de la red de cliente más
- Solamente los routers PE tienen que dar soporte a los servicios de MPLS VPN
- Los routers P no almacenan ni procesan las rutas VPNv4



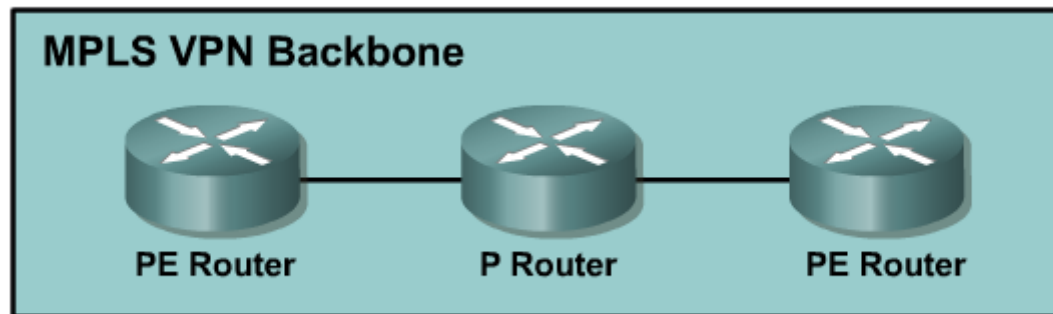
## Arquitectura de las VPNs sobre MPLS: Visión del cliente

- Para el cliente, los routers PE (sus VRFs) aparecen como routers “core” que se conectan entre sí utilizando BGP
  - Los routers P son “transparentes”
- Se suelen combinar IGPs para el enrutamiento dentro de la red del SP y de la red del cliente, con MP-BGP para transportar información de VPNv4 entre clientes



# Arquitectura de las VPNs sobre MPLS

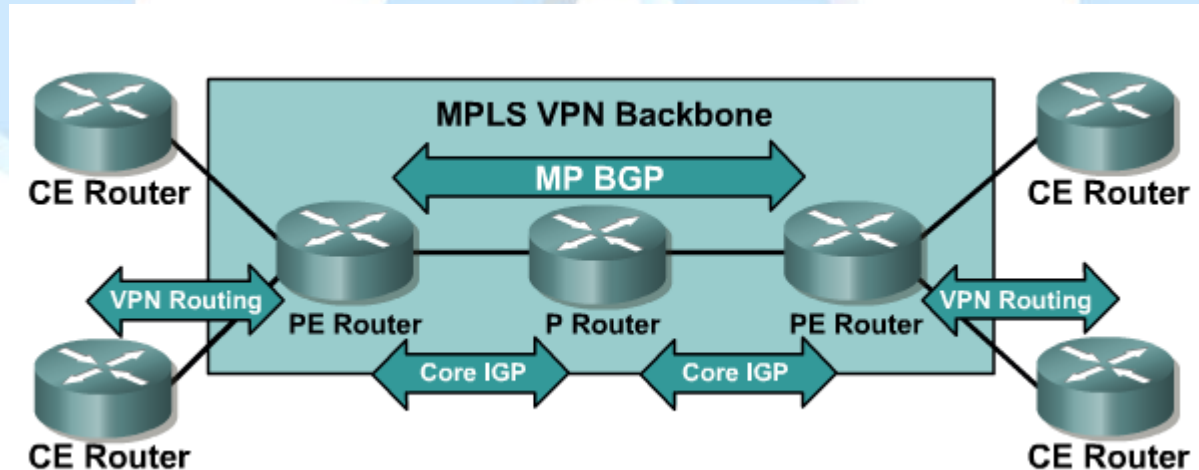
- Los routers P:
  - No participan en el enrutamiento MPLS VPN y no transporta rutas VPNv4
  - Ejecutan un IGP en el backbone del SP, entre ellos y con los routers PE, intercambiando información sobre las subredes globales: Redes dentro del SP, tanto reales como interfaces de loopback)



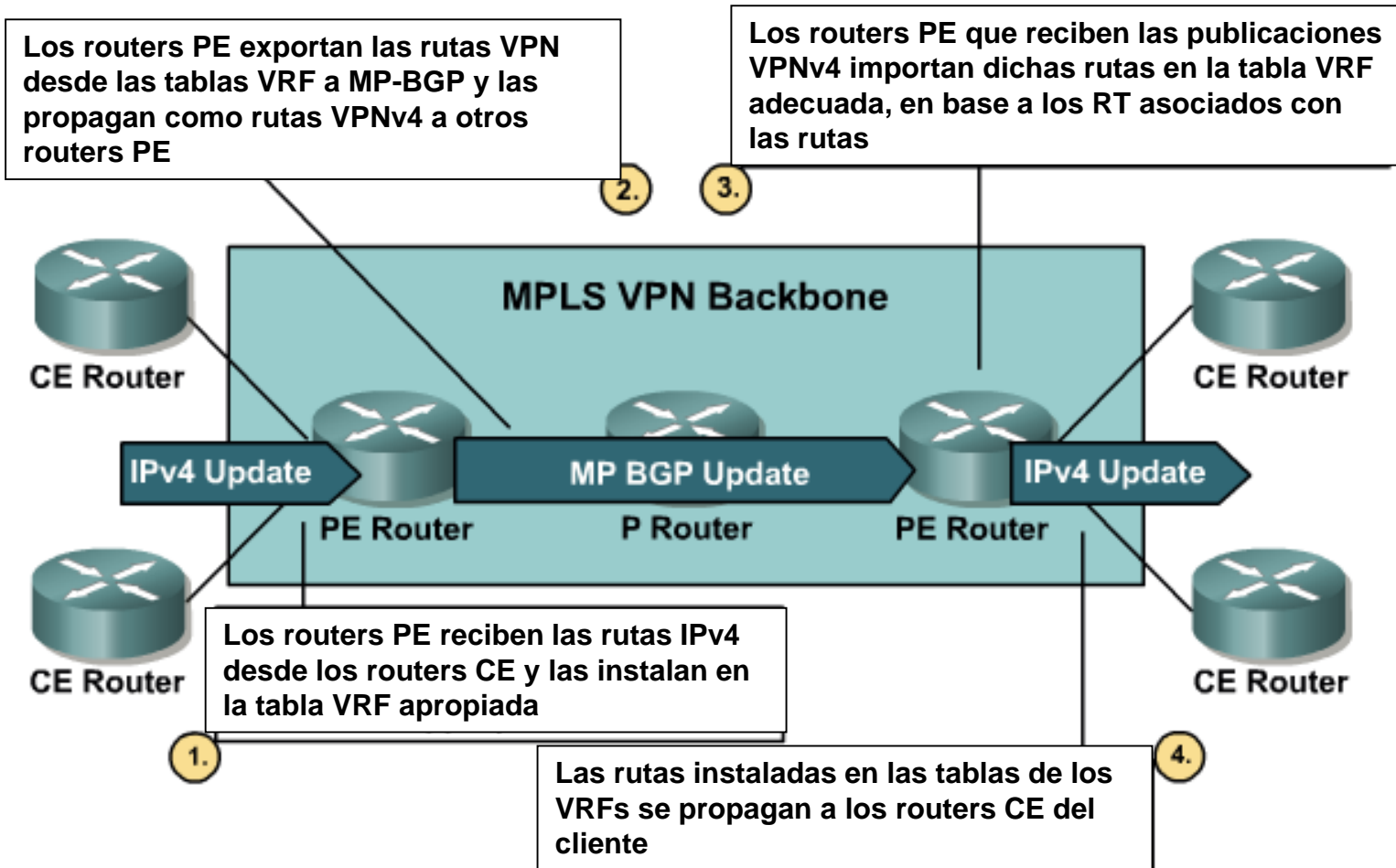


# Arquitectura de las VPNs sobre MPLS

- Los routers PE intercambian:
  - Rutas VPNv4 con los routers CE mediante protocolos de enrutamiento que ejecutan los VRFs que contienen
  - Rutas del “core” del SP con routers P y PE, utilizando para ello IGPs
  - Rutas VPNv4 con otros routers PE mediante sesiones MP-BGP

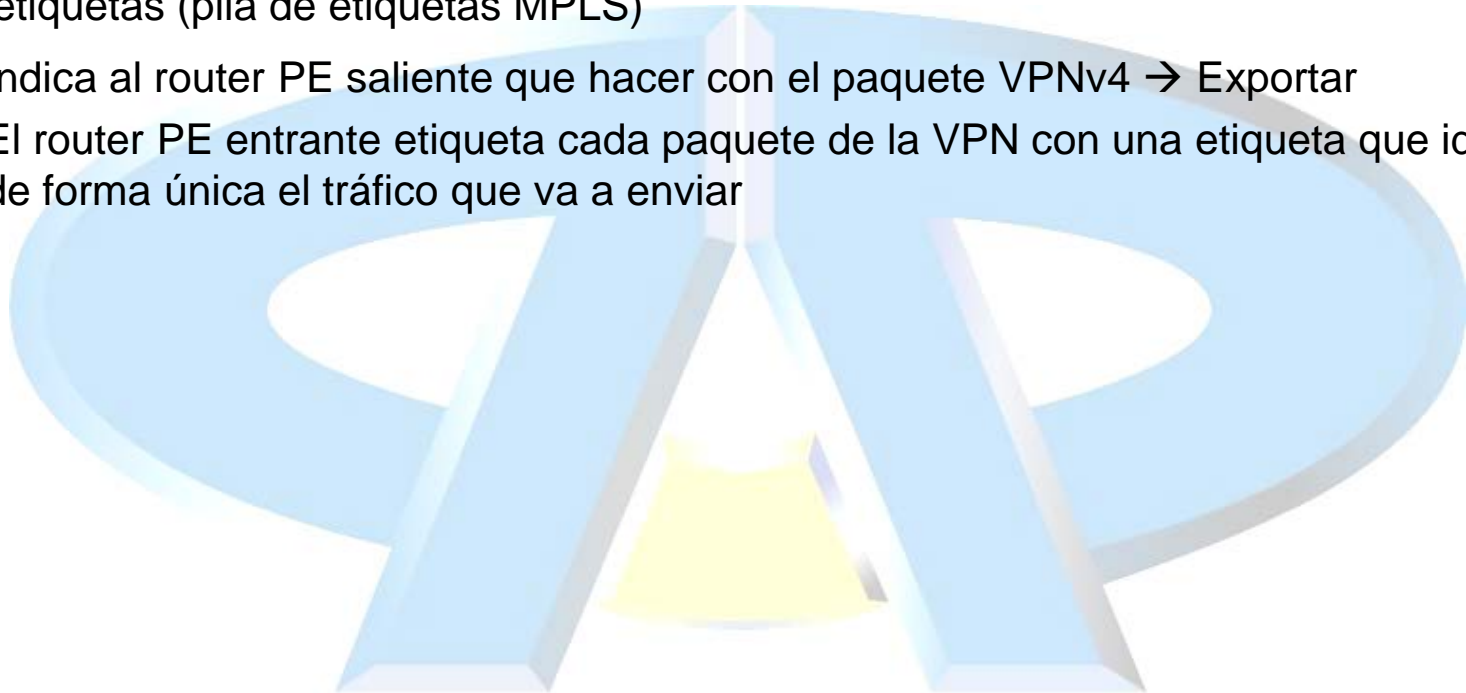


# Arquitectura de las VPNs sobre MPLS



## Pila de Etiquetas MPLS

- MPLS opera anteponiendo a los paquetes una cabecera MPLS que puede contener una o más etiquetas (pila de etiquetas MPLS)
  - Indica al router PE saliente que hacer con el paquete VPNv4 → Exportar
  - El router PE entrante etiqueta cada paquete de la VPN con una etiqueta que identifica de forma única el tráfico que va a enviar

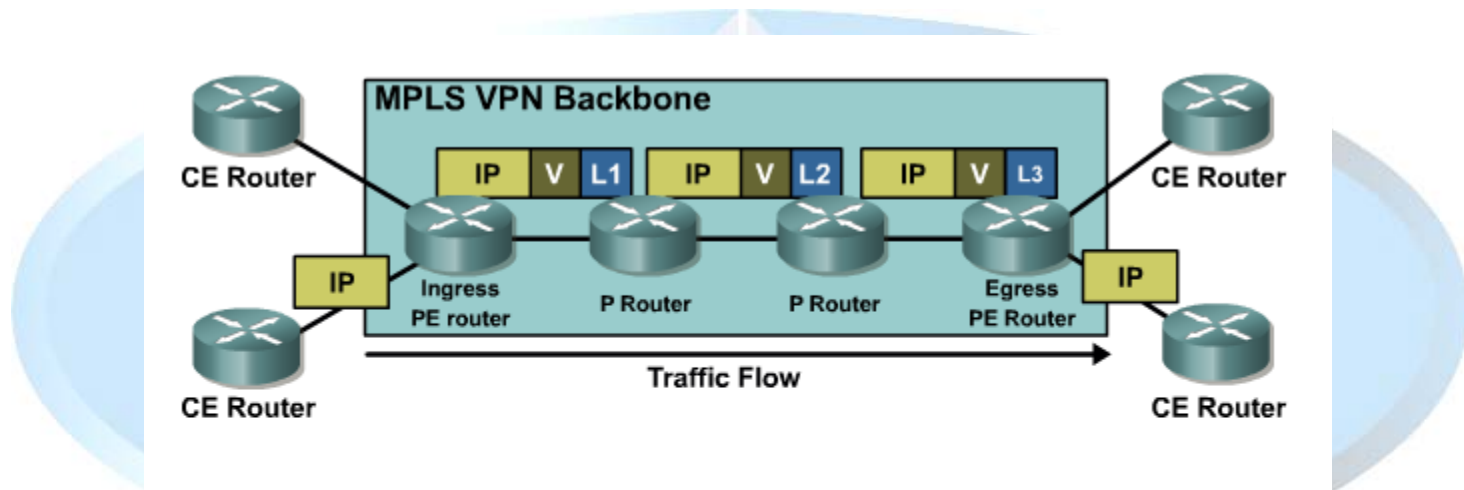


## Pila de Etiquetas MPLS

- Cuando se usa la pila de etiquetas, el router PE entrante etiqueta el tráfico IP entrante con dos etiquetas:
  - La etiqueta que está en la cima de la pila es la etiqueta LDP que se utiliza para enviar una trama convencional en una red MPLS
    - Garantiza que el paquete atravesará el núcleo de la red VPN MPLS y llegará al PE saliente
  - La segunda etiqueta identifica al router saliente. Esta etiqueta le indica al router como enviar el paquete entrante a través de la VPN
    - Puede apuntar directamente a una interfaz de salida
      - En ese caso, el router PE saliente realiza una búsqueda solamente del paquete VPN
        - » El router CE es el siguiente salto de una ruta VPN
    - Puede apuntar también al VRF de destino y por lo tanto realizará una búsqueda IP en la tabla VRF
      - Rutas VPNv4 agregadas, Rutas VPNv4 que apuntan a null0,...
    - Cuando se implementan VPNs sobre MPLS, es necesario incrementar la MTU para permitir estas dos etiquetas

# Pila de Etiquetas MPLS

- MPLS VPNs and Packet Forwarding

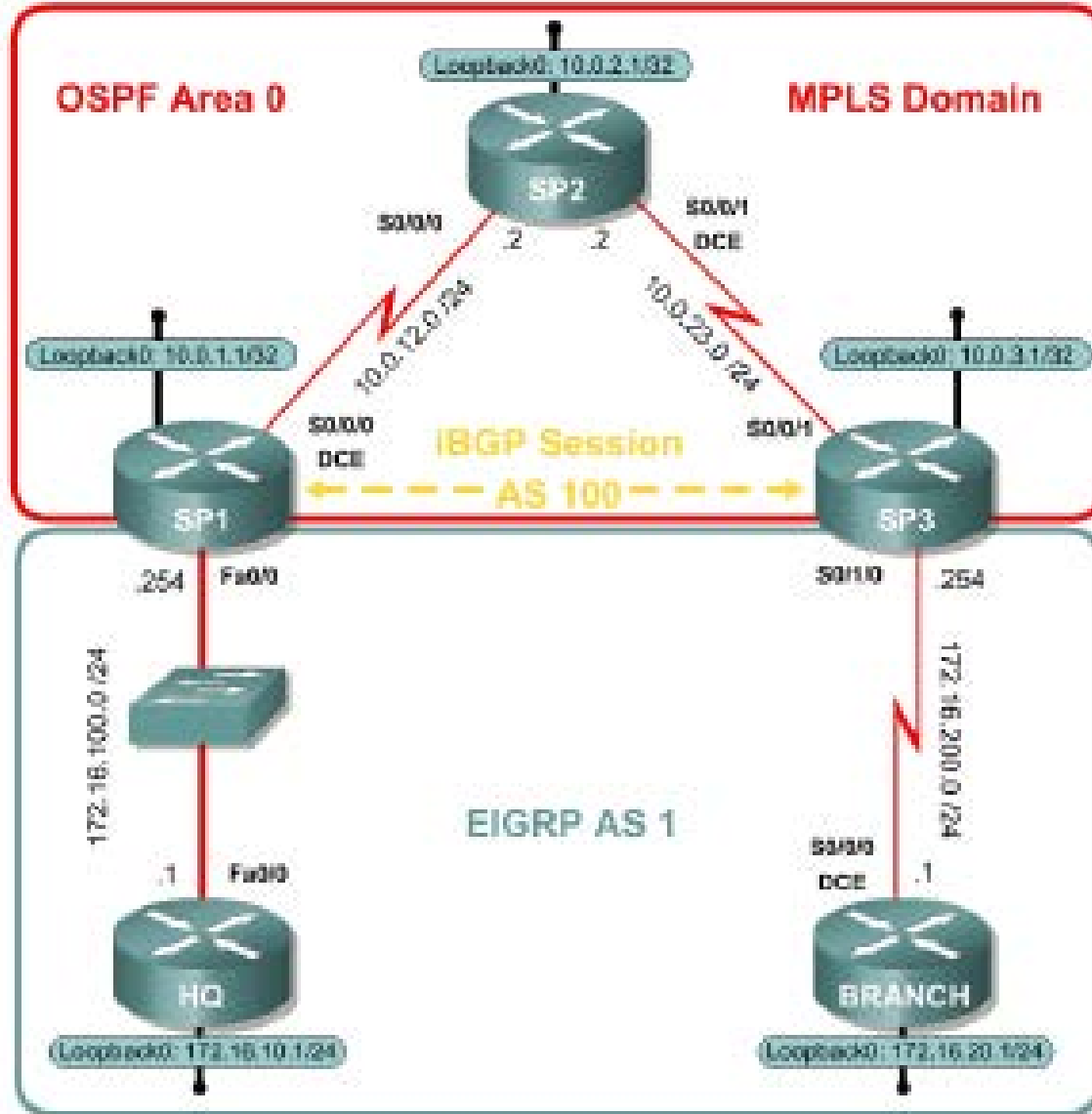


**The PE routers label the VPN packets with a label stack, as follows:**

- Using the LDP label for the egress PE router as the top label
- Using the VPN label that is assigned by the egress PE router as the second label in the stack



# Topología





# Configuración del Dominio MPLS

```
hostname SP1
```

!Paso 1. Configuración del Direcccionamiento IP

```
interface loopback 0
```

```
ip address 10.0.1.1 255.255.255.255
```

```
interface serial 0/0/0
```

```
ip address 10.0.12.1 255.255.255.0
```

```
no shutdown
```

```
interface fastethernet 0/0
```

```
ip address 172.16.100.254 255.255.255.0
```

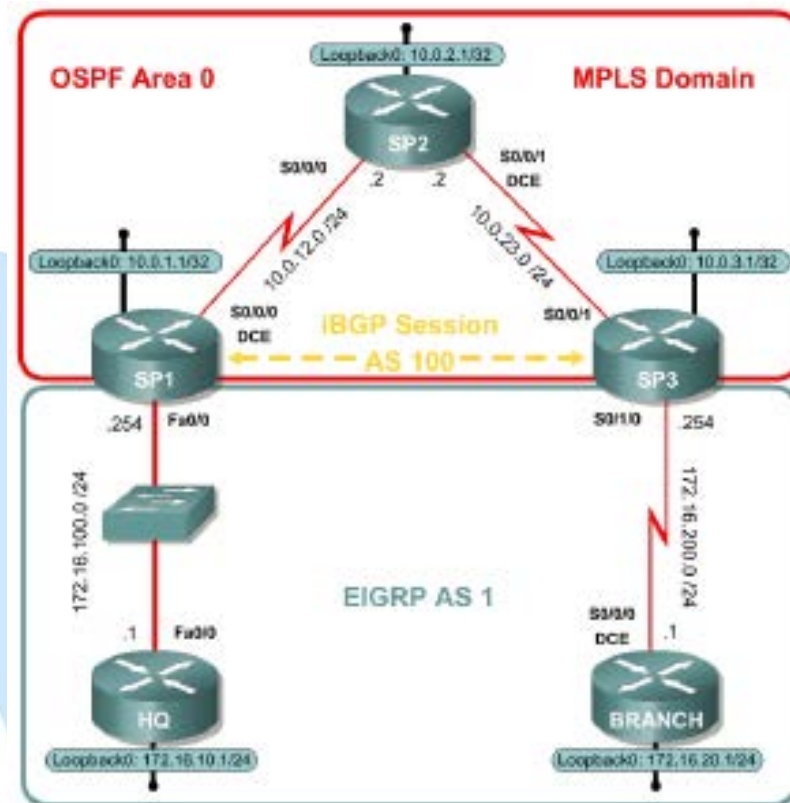
```
no shutdown
```

!Paso 2. Configuración del Enrutamiento

```
router ospf 1
```

```
network 10.0.1.0 0.0.0.255 area 0
```

```
network 10.0.12.0 0.0.0.255 area 0
```



# Configuración del Dominio MPLS

```
hostname SP2
```

!Paso 1. Configuración del Direcccionamiento IP

```
interface loopback 0
```

```
ip address 10.0.2.1 255.255.255.255
```

```
interface serial 0/0/0
```

```
ip address 10.0.12.2 255.255.255.0
```

```
no shutdown
```

```
interface serial 0/0/1
```

```
ip address 10.0.23.2 255.255.255.0
```

```
no shutdown
```

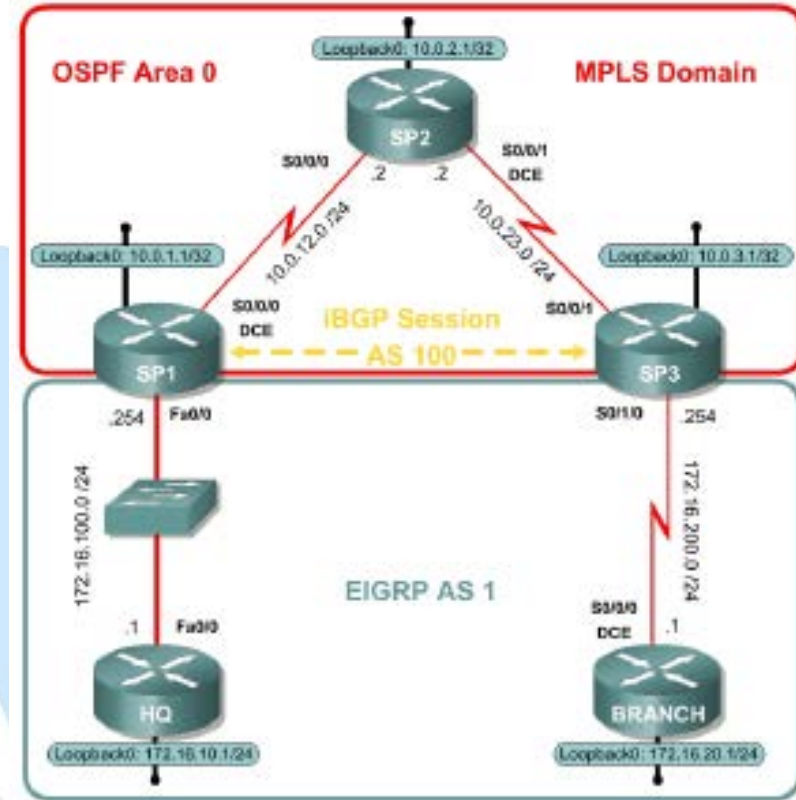
!Paso 2. Configuración del Enrutamiento

```
router ospf 1
```

```
network 10.0.2.0 0.0.0.255 area 0
```

```
network 10.0.12.0 0.0.0.255 area 0
```

```
network 10.0.23.0 0.0.0.255 area 0
```



# Configuración del Dominio MPLS

```
hostname SP3
```

```
! Paso 1. Configuración Direcccionamiento IP
```

```
interface loopback 0
```

```
ip address 10.0.3.1 255.255.255.255
```

```
interface serial 0/0/1
```

```
ip address 10.0.23.3 255.255.255.0
```

```
no shutdown
```

```
interface fastethernet 0/0
```

```
ip address 172.16.200.254 255.255.255.0
```

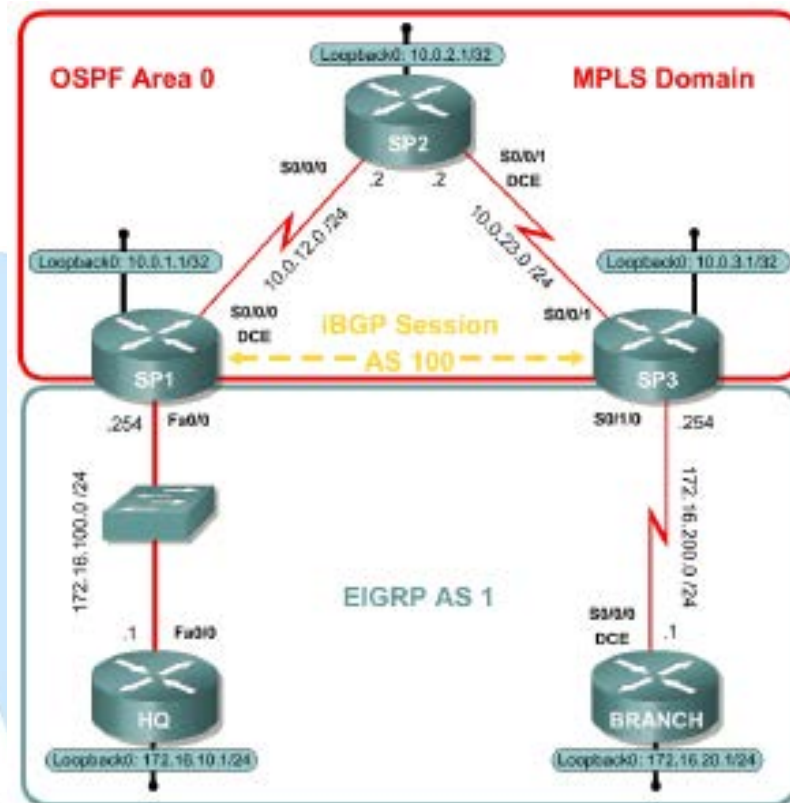
```
no shutdown
```

```
! Paso 2. Configuración del Enrutamiento
```

```
router ospf 1
```

```
network 10.0.3.0 0.0.0.255 area 0
```

```
network 10.0.23.0 0.0.0.255 area 0
```



# Configuración del Dominio MPLS

! Paso 3. Activación de MPLS en el SP

**! hostname SP1 → Router de Tipo Provider-Edge**

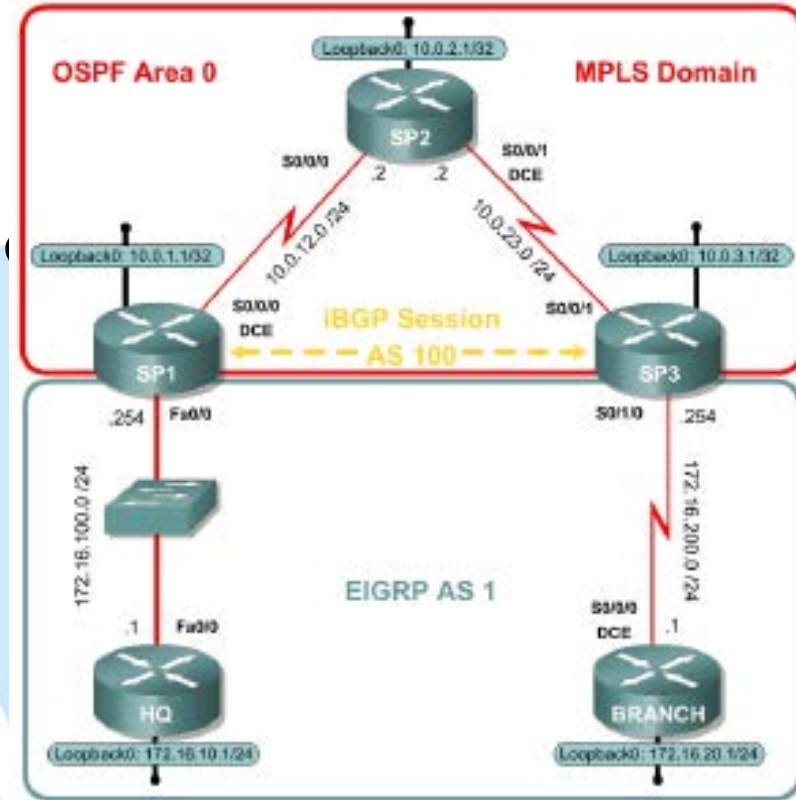
```
mpls ldp router-id loopback0 force
interface serial0/0/0
mpls ip
```

**! hostname SP2 → Router de Tipo Provider (P)**

```
mpls ldp router-id loopback0 force
interface serial0/0/0
mpls ip
interface serial0/0/1
mpls ip
```

**! hostname SP3 → Router de Tipo Provider-Edge (PE)**

```
mpls ldp router-id loopback0 force
interface serial0/0/1
mpls ip
```



# Configuración de VPNs MPLS

! Paso 4. Creación de los VRFs en los PEs

**! hostname SP1**

```
ip vrf customer1
```

```
rd 100:1
```

```
route-target both 1:100
```

```
interface fastethernet 0/0
```

```
ip vrf forwarding customer1
```

```
ip address 172.16.100.254 255.255.255.0
```

```
no shut
```

**! hostname SP3**

```
ip vrf customer1
```

```
rd 100:1
```

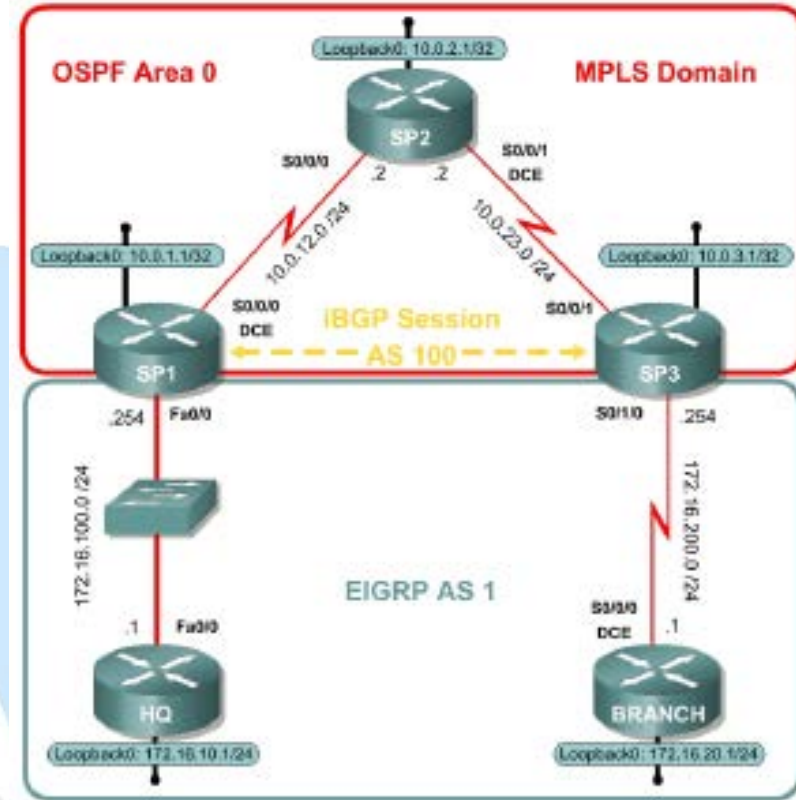
```
route-target both 1:100
```

```
interface fastethernet 0/0
```

```
ip vrf forwarding customer1
```

```
ip address 172.16.200.254 255.255.255.0
```

```
no shut
```





# Configuración de VPNs MPLS

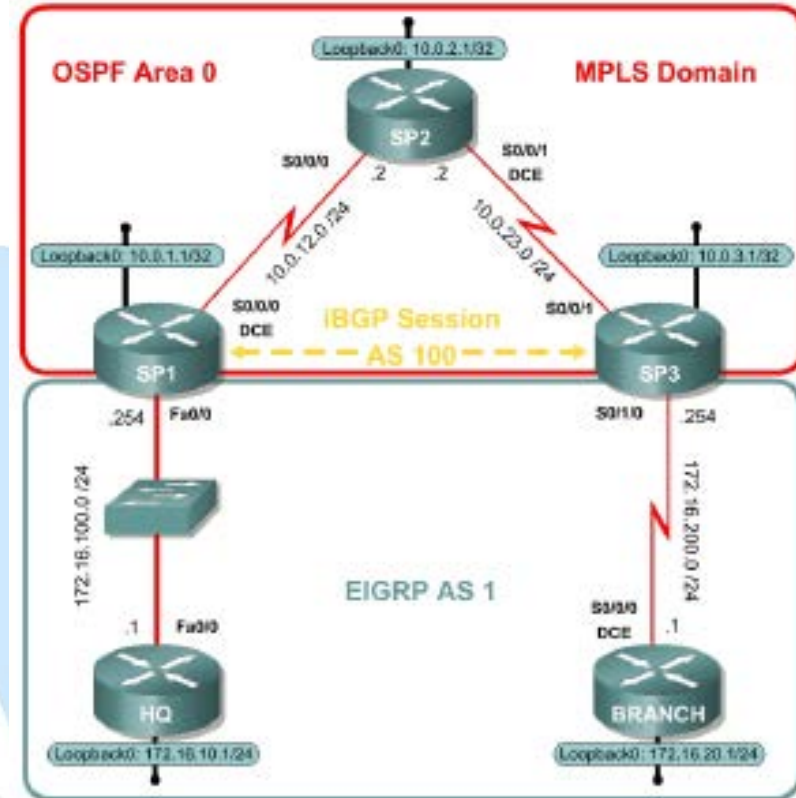
! Paso 5. Configuración del enrutamiento PE-CE

**! hostname SP1**

```
router eigrp 100
  address-family ipv4 vrf customer1
  autonomous-system 1
  no auto-summary
  network 172.16.0.0
```

**! hostname SP3**

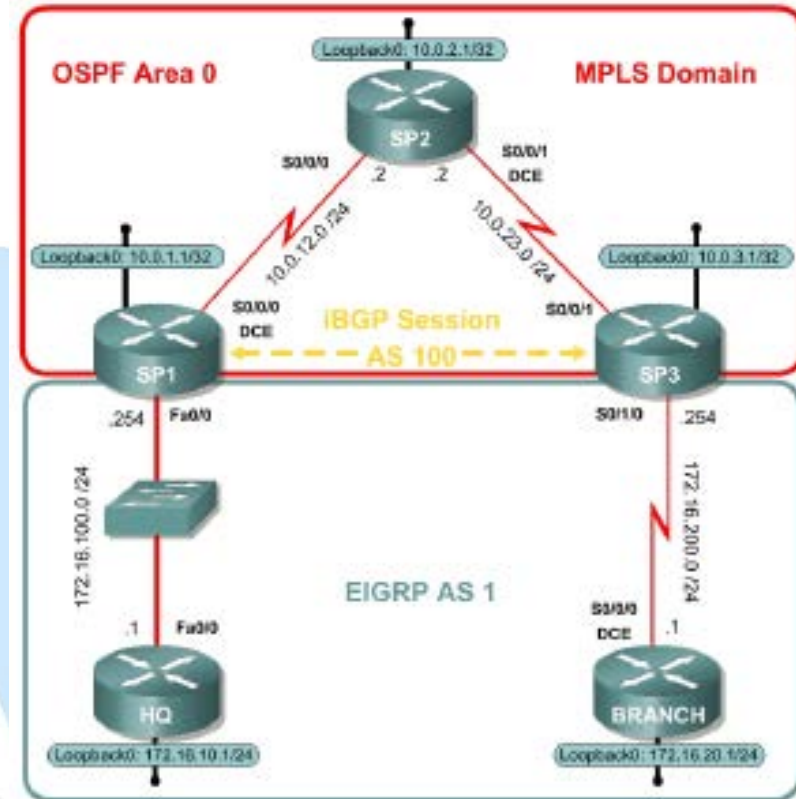
```
router eigrp 100
  address-family ipv4 vrf customer1
  autonomous-system 1
  no auto-summary
  network 172.16.0.0
```



# Configuración de VPNs MPLS

! Paso 6. Configuración de MP-BGP

```
router bgp 100
neighbor 10.0.3.1 remote-as 100
neighbor 10.0.3.1 update-source loopback0
address-family vpnv4
neighbor 10.0.3.1 activate
neighbor 10.0.3.1 send-community both
address-family ipv4 vrf customer1
redistribute eigrp 1
exit
exit
router eigrp 100
address-family ipv4 vrf customer1
redistribute bgp 100 metric 64 1000 255 1 1500
exit
exit
```

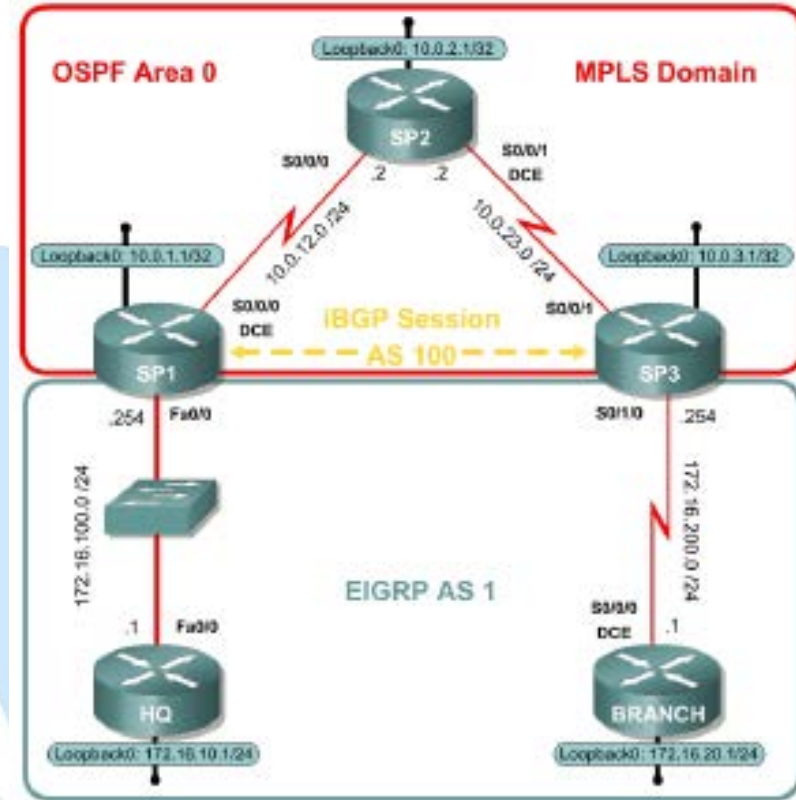




# Configuración de VPNs MPLS

! Paso 6. Configuración de MP-BGP

```
router bgp 100
neighbor 10.0.1.1 remote-as 100
neighbor 10.0.1.1 update-source loopback0
address-family vpnv4
neighbor 10.0.1.1 activate
neighbor 10.0.1.1 send-community both
exit
address-family ipv4 vrf customer1
redistribute eigrp 1
exit
exit
router eigrp 100
address-family ipv4 vrf customer1
redistribute bgp 100 metric 64 1000 255 1 1500
exit
exit
```



# Configuración de Cliente

hostname HQ

! Paso 1. Configuración del Direccionamiento IP

interface loopback 0

ip address 172.16.10.1 255.255.255.0

interface fastethernet 0/0

ip address 172.16.100.1 255.255.255.0

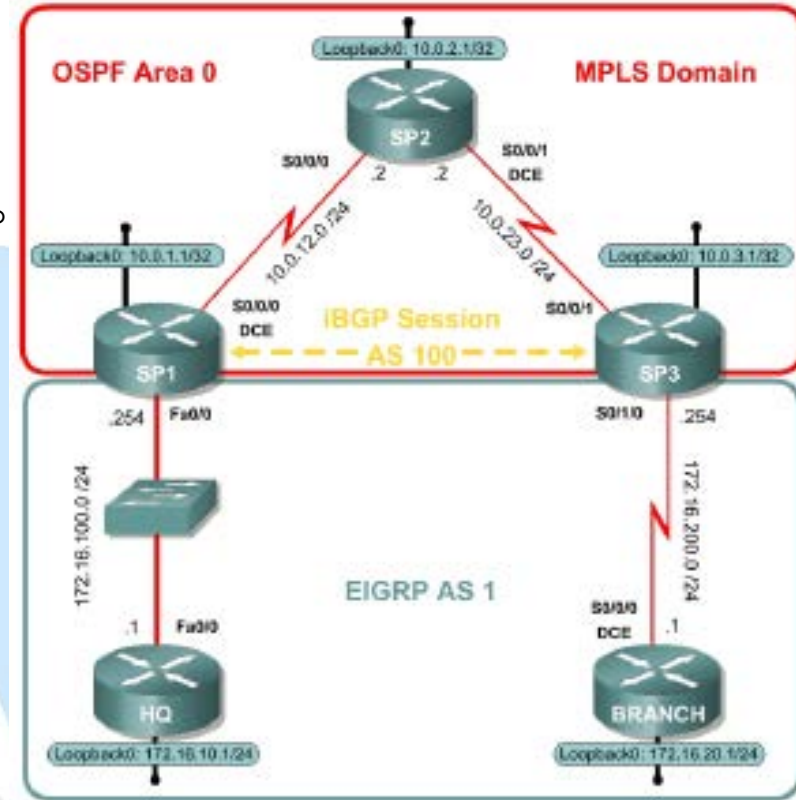
no shutdown

! Paso 2. Configuración del Enrutamiento CE-PE

router eigrp 1

no auto-summary

network 172.16.0.0



# Configuración de Cliente

```
hostname Branch1
```

```
! Paso 1. Configuración del Direcccionamiento I
interface loopback 0
```

```
ip address 172.16.20.1 255.255.255.0
```

```
interface fastethernet 0/0
```

```
ip address 172.16.200.1 255.255.255.0
```

```
no shutdown
```

```
! Paso 2. Configuración del Enrutamiento CE-PE
router eigrp 1
```

```
no auto-summary
```

```
network 172.16.0.0
```

