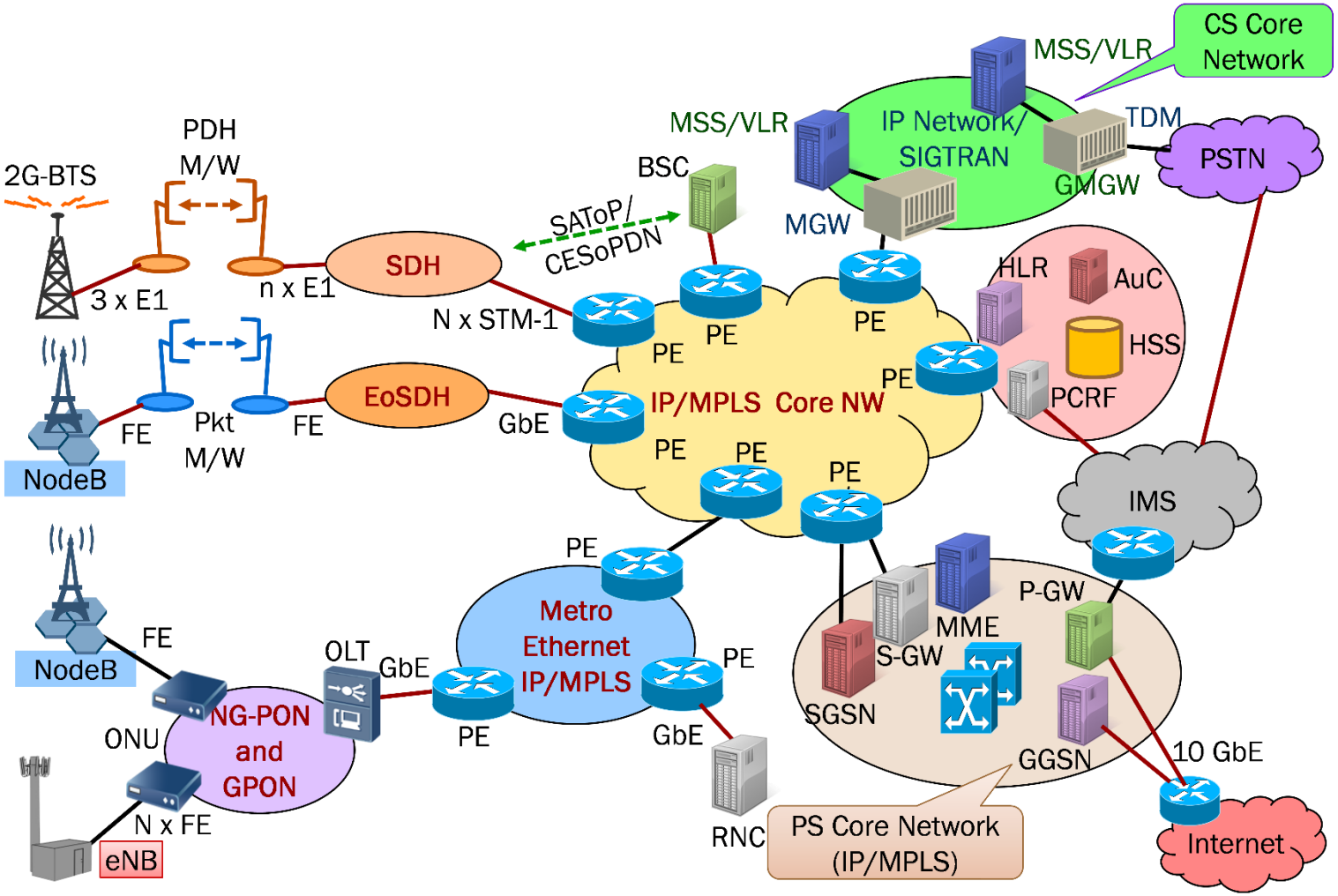
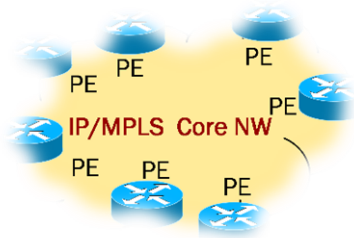
Introducción a las redes MPLS



Significado y motivaciones



Motivaciones:

- En 1996 el IETF comenzó a trabajar con el proyecto.
- En 1997 se conformó el MPLS Working Group para estandarizar las primeras bases de MPLS.
- El objetivo primario:

"estandarizar una base tecnología que integre el "paradigma" del forwarding mediante el intercambio de etiquetas, con el routing de capa de red"

- En 2001 se definió el "Multi protocol Label Switching Architecture" RFC-3031 .

https://www.rfc-editor.org/rfc/rfc3031.txt

Motivaciones:

- Se espera que:
  - Mejore la relación Precio/performance del routing de la capa de red,
  - Mejore la escalabilidad de la misma
  - Entregue mayor flexibilidad en el despacho o entrega de nuevos servicios.

- Se debe considerar al protocolo MPLS como:

"el avance más reciente en la evolución de las tecnologías de Routing y Forwarding en las redes IP, lo que implica ***una evolución en la manera de construir y gestionar las redes."***

Significado:

- MPLS significa “Multi protocol label switching”.
- Define la forma de forwardear o conmutar datos a través de una red.
- Esto basado un “pequeño label” o etiqueta transportada en cada paquete.
- Esta técnica de “label switching” no es una nueva, ya que tanto Frame Relay como ATM la utilizaban para conmutar los frames o celdas.

Significado:

- Cada nodo de la red:
  - extrae el label del paquete
  - lo analiza en una tabla para determinar el siguiente salto
  - finalmente sustituye la etiqueta por una nueva antes de enviarlo.

Que ofrece?

- Que ofrece?

  - Nuevas posibilidades en la gestión de Backbones.

  - Nuevas posibilidades en la **provisión de nuevos servicios de valor agregado**.

Fundamentos bases:

- La arquitectura de MPLS describe:
  - Los ***mecanismos*** para realizar la conmutación mediante el intercambio de etiquetas,
- Esta combina los beneficios del forwarding de paquetes basados en la Capa 2 y los beneficios del routing de capa 3:
  - Capa 2 (Ethernet/ATM/FR) eficiencia en el forwarding y la ingeniería de tráfico.
  - Capa 3 (IP) escalabilidad y flexibilidad.

Fundamentos bases:

- El aspecto fundamental de MPLS consiste en:

"la separación entre las funciones de routing (el control de la información sobre la topología y tráfico en la red), de las funciones de forwarding (envío en sí de los datos entre los elementos de red)"

	IP	MPLS
Forwarding	Destination address based Forwarding table learned from control plane TTL support	Label based Forwarding table learned from control plane TTL support
Control Plane	OSPF, IS-IS, BGP	OSPF, IS-IS, BGP LDP, RSVP
Packet Encapsulation	IP Header	One or more labels
QoS	8 bit TOS field in IP header	3 bit TC field in label
OAM	IP ping, traceroute	MPLS OAM

Porqué de su nombre:

- Multi protocol significa:
  - Que puede funcionar con diferentes protocolos, tanto de capa 2 como de capa 3.
  - Para protocolos *de capa 2* soporta Ethernet como también HDLC, PPP, Frame Relay o ATM.
  - Para protocolos *de capa 3* soporta tanto IPv4 o IPv6 como así también IPX.

Para nuestro caso, consideraremos IPv4 como protocolo L3 y Ethernet como protocolo de L2.

Porqué de su nombre:

- Label switching significa:

- Que en lugar de utilizar la dirección IP destino, se *utiliza un label en el header MPLS para determinar cómo y a donde enviarlo.*

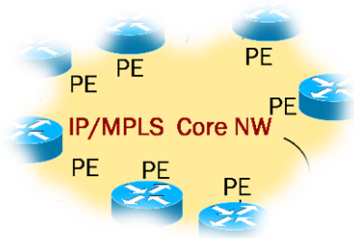
  - Este header MPLS es:

    - *Agregado* al paquete cuando este ingresa a la red MPLS,

    - *Intercambiado* a medida que se conmuta el paquete.

    - *Extraído* cuando egresa de la red (operaciones push/swap/pop).

Cuál es la real necesidad de agregar
un nuevo header al paquete
y protocolos adicionales en la red?.



Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Convergencia real:

- Falta de interoperabilidad entre los productos privados de diferentes fabricantes de las soluciones previas.

- La mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs).

- Se quería *obtener un estándar que pudiera funcionar sobre cualquier tecnología y vendor* de transporte de datos en el nivel de enlace.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de conmutación:

- Ethernet, IP, TCP y los diferentes protocolos de ruteo dinámico fueron y son parte fundamental en la arquitectura de las redes de los proveedores de servicios para crear y proveer conectividad a los usuarios.
- En la actualidad, *esto no es suficiente para proveer servicios y mantener un negocio rentable.*
- Para esto, los proveedores necesitan *optimizar y realizar una utilización lo más eficiente posible de su infraestructura.*

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de conmutación:

- Esto implicó generar redes basadas no solamente en la conectividad sino en un "*modelo de servicios".*
- En este "modelo de servicios", una capa adicional de tecnología es implementada en la infraestructura existente de manera de poder alcanzar el objetivo.

Entonces, lo primero que podríamos indicar es que MPLS fue diseñado para mejorar la eficiencia, mediante la mejora en la velocidad del proceso de conmutación de paquetes.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de conmutación:

- Para lograr esta mejora, MPLS utiliza un label o etiqueta en lugar de una dirección IP destino como elemento necesario para tomar la decisión de conmutación.
- En las redes de core o los backone de los proveedores de servicios, este cambio era de significativa importancia entendiendo que cuando MPLS fue diseñado la capacidad de procesamiento de los dispositivos no era la misma capacidad de los equipos actuales.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de conmutación:

- El ”plano de control o control plane” es un conjunto de protocolos que se utilizan para establecer el “plano de datos o data plane”.
- Los componentes principales del plano de control, son los protocolos de routeo, las tablas de ruteo y otros protocolos de señalización que luego serán utilizados por el plano de datos.
- Este “plano de datos” es la ruta de reenvío de paquetes a través de un router o switch.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de conmutación:

- En la actualidad, este data o forwarding plane es realizado por hardware especializado o ASIC, permitiendo que la conmutación de paquetes IP sea tan rápida como la conmutación de etiquetas.
- Entonces, en términos de eficiencia, implementar MPLS es un beneficio?.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de infraestructura:

- Supongamos la posibilidad que diferentes clientes compartan la misma infraestructura física, pero que estén independizados lógicamente, es decir virtualizados.
- Un *servicio del tipo VPN* puede ser pensado como una serie de túneles conectando diferentes sitios de clientes donde todo el tráfico desde y hacia cada punto es interno al cliente, es decir privado y ningún otro cliente que comparta la infraestructura física puede acceder.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de infraestructura:

- El tráfico del cliente es identificado a medida que ingresa a la red del proveedor de servicio
- Asignado al LSP correspondiente para ser transportado a través de ella.
- Luego, en el punto de egreso, el tráfico es entregado al cliente correspondiente.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de infraestructura:

- De esta forma, desde el punto de vista del cliente, podríamos decir que *el tráfico se transporta sobre redes privadas.*
- La privacidad de una red MPLS VPN es alcanzada utilizando el concepto de VRF o virtual routing forwading y la conmutación en el backbone mediante la utilización de etiquetas.
- El VRF asegura que la información de ruteo de los diferentes clientes se mantenga separada y el bakbone MPLS asegura que el forwarding se realiza con etiquetas y no con información del header IP.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de infraestructura:

- *Esta configuración permite entonces que el proveedor de servicios utilice una infraestructura común para múltiples clientes, manteniendo entre ellos una completa separación.*

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Eficiencia de infraestructura:

- Estas MPLS VPN pueden ser del tipo:
  - **Layer 2** como Virtual Private Wire Services (VPWS) que emulan una conexión punto a punto o del tipo Virtual Private LAN Service (VPLS) que emulan un switch Ethernet.
  - **Layer 3** como Virtual Private Routed Network (VPRN) que emula una red ruteada privada en el cliente.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

- El label que es agregado al paquete en el ingreso de la red, lo *podríamos asociar con más o diferentes ítems que la de una dirección destino.*

- Por ejemplo, podríamos tener un **label** que especifique *alta prioridad de entrega*, *otro servicio normal* pero ambos siempre especificando el mismo destino.

Este, claramente no es un beneficio relacionado a la eficiencia, pero si relacionado a la ingeniería de tráfico o QoS.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

- El objetivo de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red.
- Es decir:

optimizando la utilización de los recursos disponibles de manera que no haya uno sobre utilizados, con posibles puntos calientes y cuellos de botella, mientras otros estén subutilizados.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

Con Ingeniería de Tráfico se pretende:

- Prever calidad de servicio garantizada.
- Buen uso de los recursos de la red distribuyendo el tráfico de forma equitativa entre los enlaces.
- Facilidad de recuperación dinámica ante fallas en enlaces o nodos.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

- De esta forma, podemos claramente influenciar en que camino tomara el paquete.
  - Por ejemplo en función del nivel de SLA del cliente:
    - enviar el tráfico por caminos de baja latencia o jitter
    - o por caminos que no garanticen QoS,
    - utilizar o evitar link específicos,
    - utilizar links que tiene un porcentaje específico de ancho de banda
    - o utilizar un camino que tiene un determinado o un limitado hop count.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

- La ventaja de la ingeniería de tráfico MPLS:
  - Se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo.
  - Todo ello de manera más flexible y con menos costos de planificación y gestión para el administrador y con mayor calidad de servicio para los clientes.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Ingeniería de Tráfico (Traffic Engineering/ TE)

- Los *protocolos de señalización* son los encargados de establecer y mantener túneles a lo largo de la red en el dominio MPLS basándose en los recursos requeridos.
- Esto se logra con dos protocolos conocidos como **CR-LDP** (LDP de Ruta Restringido) y **RSVP-TE** (Resource Reservation Protocol – Trafic Extension).

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Protocolos IGP:

- Eficiencia **relacionada al plano de control.**
- Cuando la red IP de un proveedor de servicios debe renviar paquetes, *cada router debe realizar un look up* de la dirección IP destino.
- Si el paquete debe ser enviado a destinos que son externos a la red, *estos prefijos IP externos deben estar presentes en la tabla de ruteo de cada router.*
- Estos prefijos externos son transportados por el protocolo BGP por lo que *todos los routers de la red del proveedor de servicios deben estar ejecutando este protocolo*.

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Protocolos IGP:

- MPLS permite el reenvío de paquetes basado en el lookup de etiquetas en lugar de direcciones IP, siendo que estas etiquetas son asignadas en los **routers de ingreso** a la red MPLS permitiendo que todos los routers intermedios de la red sepan cómo reenviar el paquete.

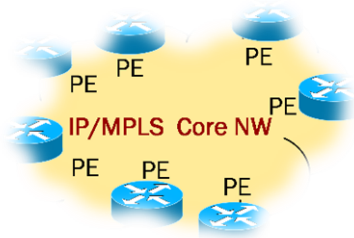
*Por esto, **los routers de core**, no necesitan tener información adicional para reenviar los paquetes basados en dirección IP destino, por esto, no necesitan ejecutar protocolos EGP como BGP (si necesitaran ejecutar protocolos IGP). Los routers externos a la red, si lo necesitan.*

Cuál es la real necesidad de agregar un nuevo header al paquete y protocolos adicionales en la red?.

Protocolos IGP:

- *Considerando que la tabla de ruteo completa de internet tiene al menos 150.000 rutas, no ejecutar BGP en todos los routers de la red, no es menor, considerando el uso de memoria.*

Definiciones



Customer Edge Devices (CE):

- Se encuentra ubicado en el **sitio del cliente**.
- Este provee acceso a la red del proveedor de servicio mediante una conexión con el router PE o Provider Edge.
- Normalmente es propiedad del cliente del cual también depende la gestión del mismo.
- Bajo esta premisa, *este equipo desconoce o no tiene configuración relacionada a los protocolos de tunelización o VPN que utiliza o utilizara el proveedor de servicios en su red*.

Provider Edge Devices (PE):

- Es el dispositivo que permite que **el cliente se conecte a la red del proveedor.**
- Tiene al menos **una interfaz directamente conectada con un CE**.
- Tiene al menos **una interfaz directamente conectada con un Provider Core** devices para conectar al core de la red del proveedor de servicio.
- Tiene que tener la capacidad de soportar diferentes tipos de interfaces, por lo que normalmente se los denomina routers multi servicios.
- A estos dispositivos los podemos definir como los Gateways que tendrán los usuarios para acceder a la red

Provider Router o Provider Core (P):

- Se encuentra ubicado **dentro de la red de core del proveedor del servicio**.

- *Desconocen los diferentes servicios* que se le proveen a cada cliente.

- Simplemente realizan tareas de forwarding basada en la información que le envían los PE.

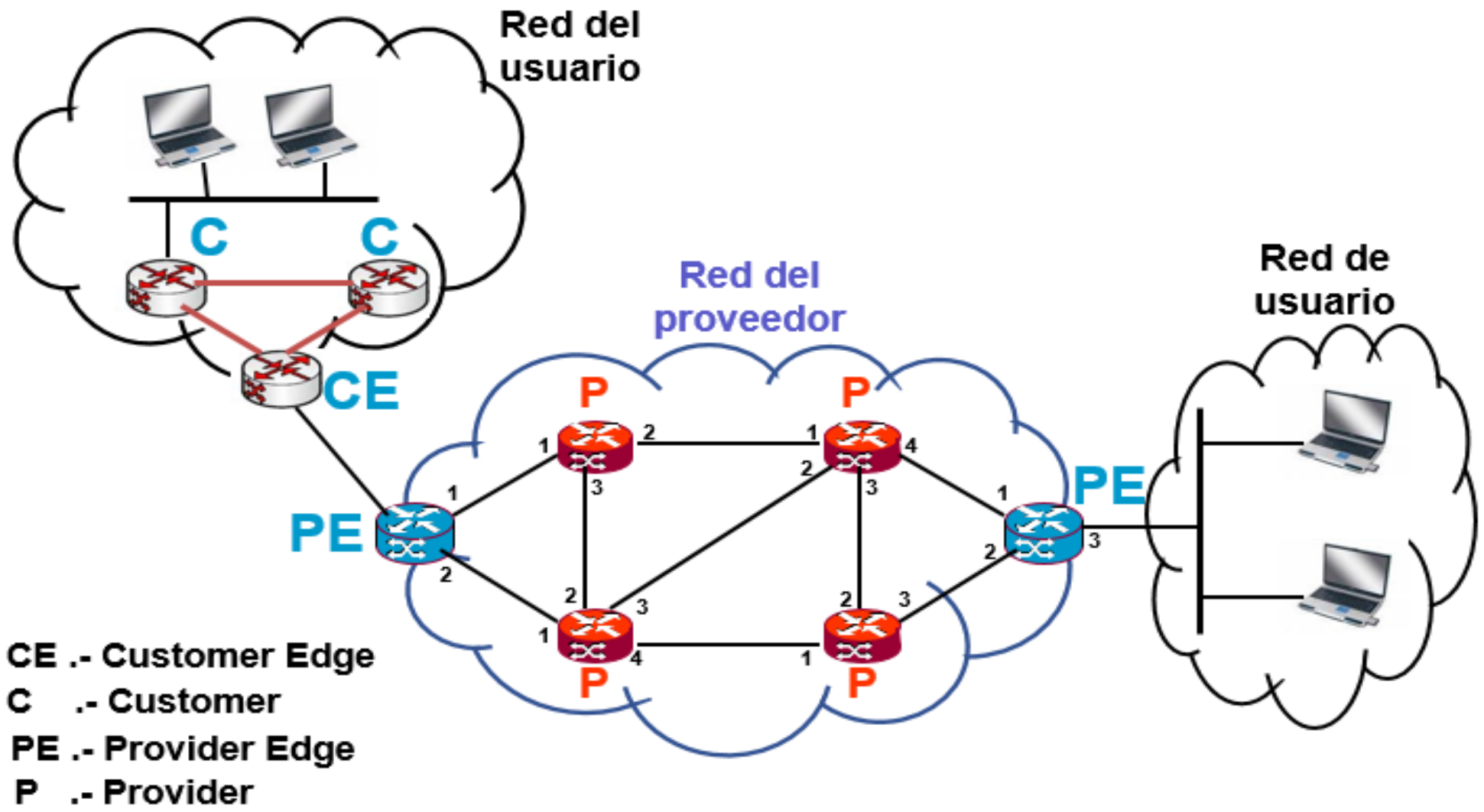
CE / PE / P

•En función de estas descripciones resulta lógico pensar que:

“La mayor inteligencia en la red la proveen los Provider Edge device”

•En estos equipos es **clave la correcta configuración** para poder ofrecer correctamente los diferentes servicios en la red.

CE / PE / P


Red del usuario
C
C
CE
Red del proveedor
P
P
PE
PE
Red de usuario
P
P
CE .- Customer Edge
C .- Customer
PE .- Provider Edge
P .- Provider

Label Switching Patch (LSP)

- MPLS es una tecnología de tunneling.
  - A estos túneles se los conoce como LSP o Label Switching Path.
- Estos LSP son el trayecto de un tráfico específico o circuitos virtuales establecidos a través de la red MPLS.
- Un LSP se define en forma **unidireccional**
  - Se deben establecer dos para lograr un flujo de tráfico bidireccional en la red.
- Un LSP se define mediante el mapeo de labels o etiquetas desde una interfaz entrante a una interfaz saliente.

Label Routers (LER / LSR):

- Los routers o equipos que forwardean los paquetes basándose en las etiquetas MPLS, son conocidos como Label Edge Routers (LERs) or Label Switch Routers (LSRs).

- Los **LER son los endpoint de los túneles MPLS**, normalmente ubicados en el borde de la red MPLS.

- Los **LSR se encuentran en el core de la red** y proveen conectividad entre los LER.

Label Routers (LER / LSR):

- Al ser los LSP son unidireccionales:
  - Un router se identifica como un LER basado en su **posición relativa** respecto a un LSP especifico.
- Los routers donde comienza un LSP se denominan ***ingreses Label Edge Router o iLER***.
- Los routers donde finaliza un LSP se denominan ***egress Label Edge Router o eLER.***

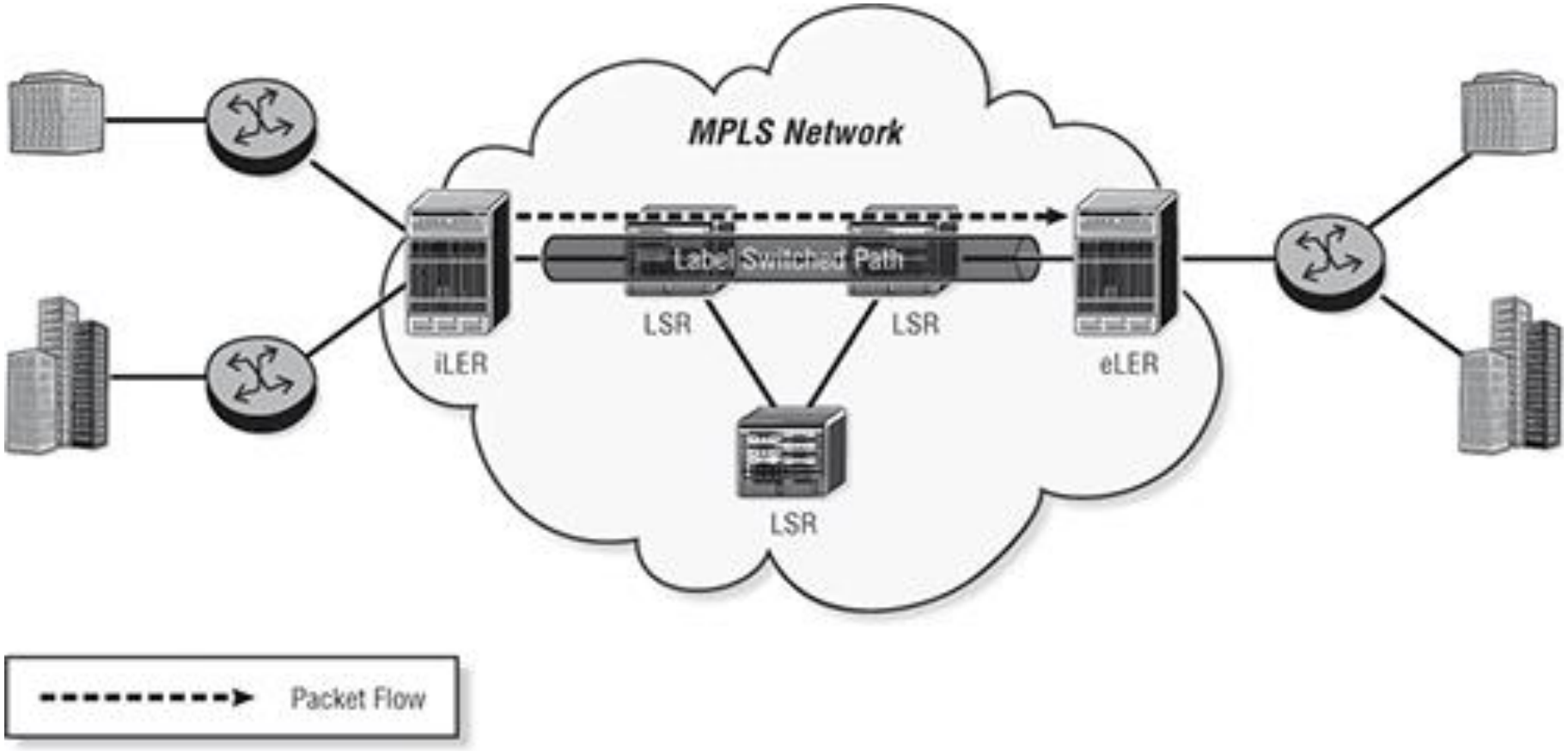
Label Edge Routers (LER)

- Los **iLER**:
  - Reciben los paquetes sin etiquetas o “unlabeled” desde el exterior del dominio MPLS.
  - Le agregan la etiqueta al paquete.
  - Lo forwardean dentro del dominio a lo largo del LSP.
- Los **eLER**:
  - Reciben un paquete etiquetado desde el dominio MPLS,
  - Quita la etiqueta y lo reenvía fuera del dominio MPLS sin el “label MPLS” donde luego, es forwardeado de acuerdo al protocolo “origen” del paquete.

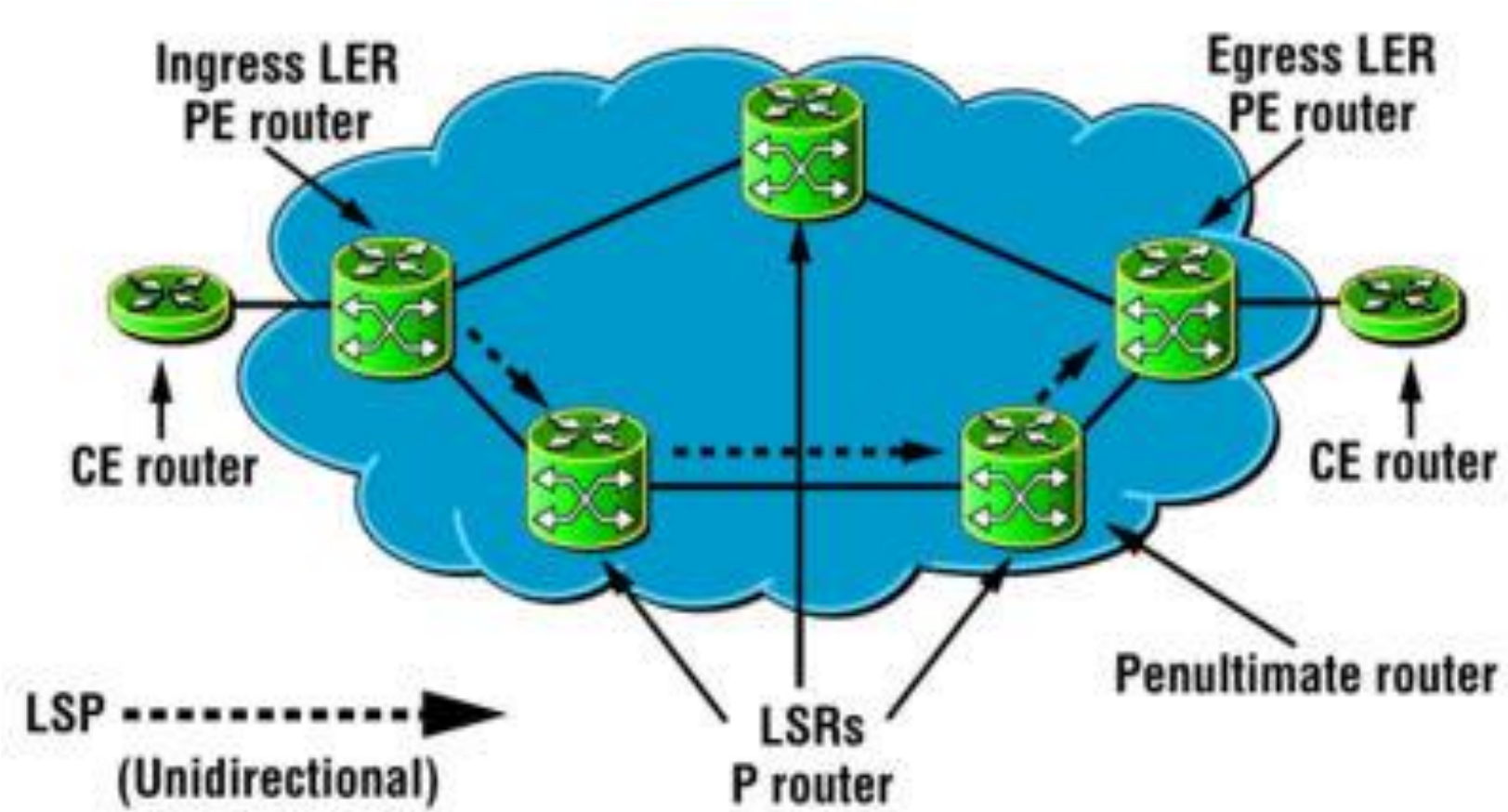
Label Switching Routers (LSR):

- Los **LSR**:
  - Conmutan o switchean los paquetes etiquetados en el core de la red.
  - Estos LSR ignoran cualquier tipo de header posterior al header MPLS, como ser el header IP.
  - Es un router intermedio en la red MPLS entre los LERs de ingreso y egreso.
  - Intercambia etiquetas entra una label entrante y una saliente.
  - Forwardea al paquete al próximo router dentro del dominio MPLS, a lo largo del LSP.

LER / LSR


MPLS Network
Label Switched Path
iLER
LSR
LSR
LSR
eLER
Packet Flow

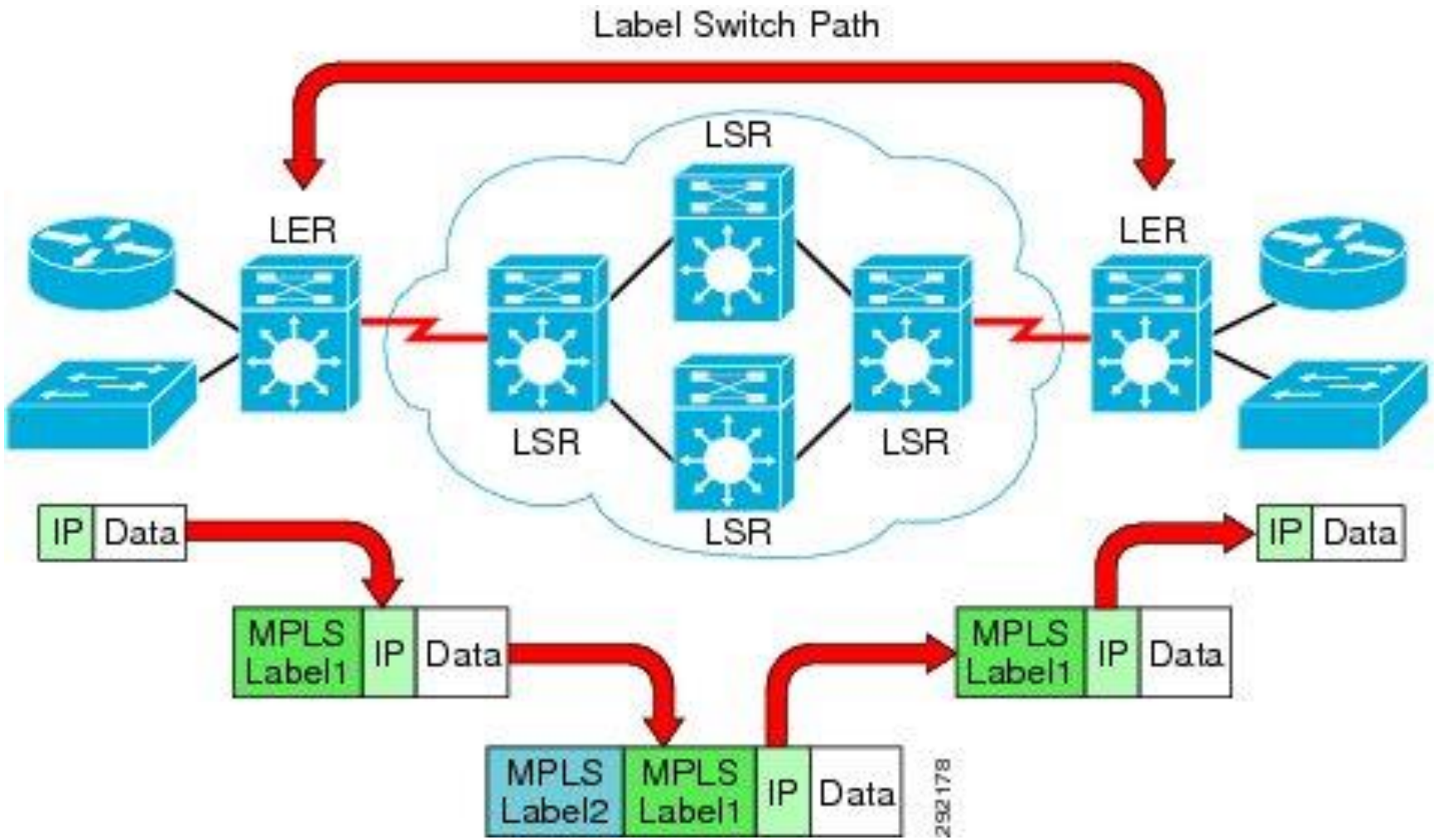
LER / LSR


Ingress LER
PE router
Egress LER
PE router
CE router
CE router
LSP
(Unidirectional)
LSRs
P router
Penultimate router

LSP anidado:

- Los iLER de un LSP no son necesariamente los primeros o únicos routers del dominio MPLS que etiquetan un paquete.
- Este, puede haber sido **previamente "etiquetado"** por algún LSR precedente.
- Esto se denomina **"nested LSP" o "LSP anidado",** es decir un LSP dentro de otro LSP.
- Por esto, un iLER de un LSP anidado, agrega una *segunda etiqueta al paquete.*
  - La etiqueta exterior pertenece al LSP anidado.
  - La etiqueta interior al LSP que abarca todo la red MPLS

LSP anidado:


Label Switch Path
LSR
LER
LER
LSR
LSR
LSR
IP
Data
MPLS
Label1
IP
Data
MPLS
Label2
MPLS
Label1
IP
Data
MPLS
Label1
IP
Data
IP
Data
292178

POP/SWAP/PUSH :

- La etiqueta es un identificador de conexión que sólo tiene significado local.

Establece una correspondencia entre el tráfico y un FEC específico.

- **Se asigna** al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio.

- Un LSR puede realizar tres funciones: **pop, swap o push.**

POP/SWAP/PUSH :

•Debe ser capaz de **agregar o realizar un "pop"** de una o más etiquetas antes de conmutarlo.

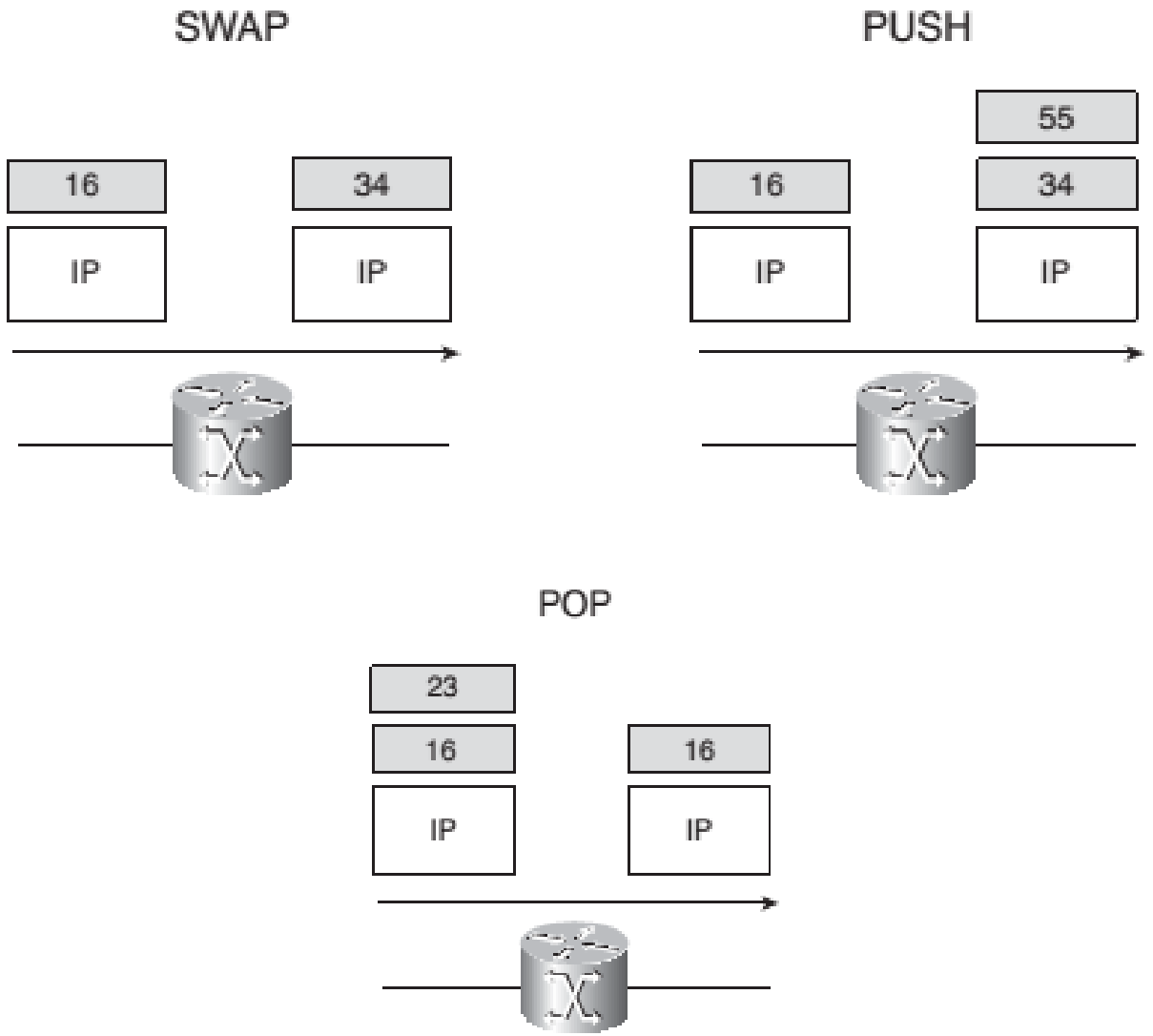
•Debe ser capaz de **quitar o realizar un "push"** de una o más etiquetas del paquete recibido.

•Debe ser capaz de realizar un **intercambio o "swap"** de etiquetas antes de conmutarlo.

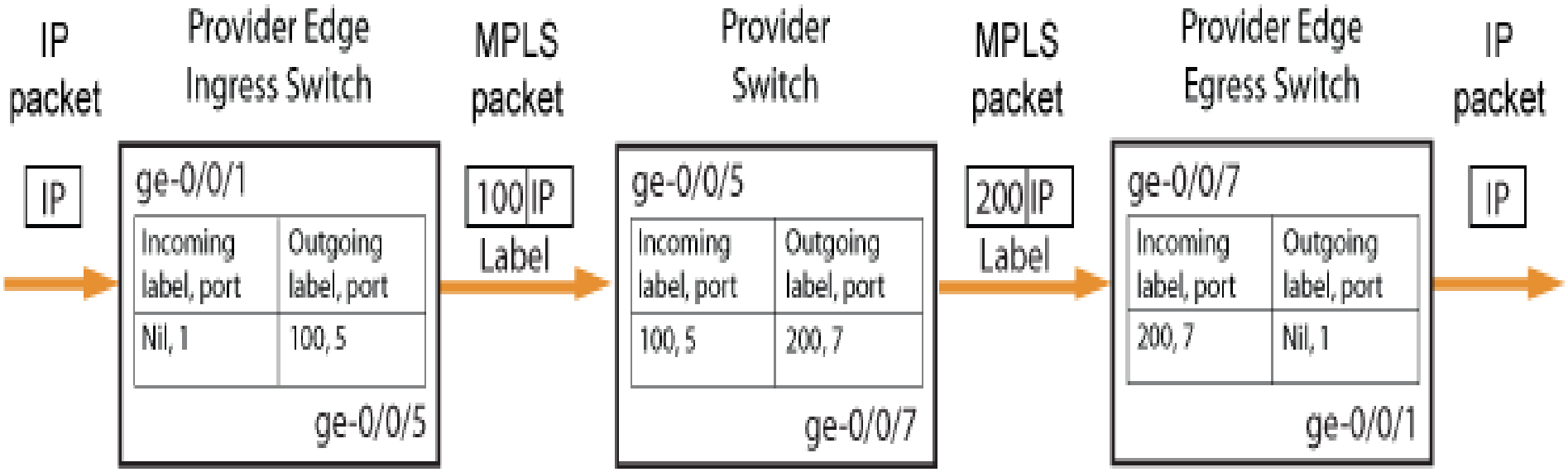
•Los **LER** son los responsables de realizar tanto el push como el pop de las etiquetas.

•Los **LSR son** los responsables de realizar los swap de etiquetas.

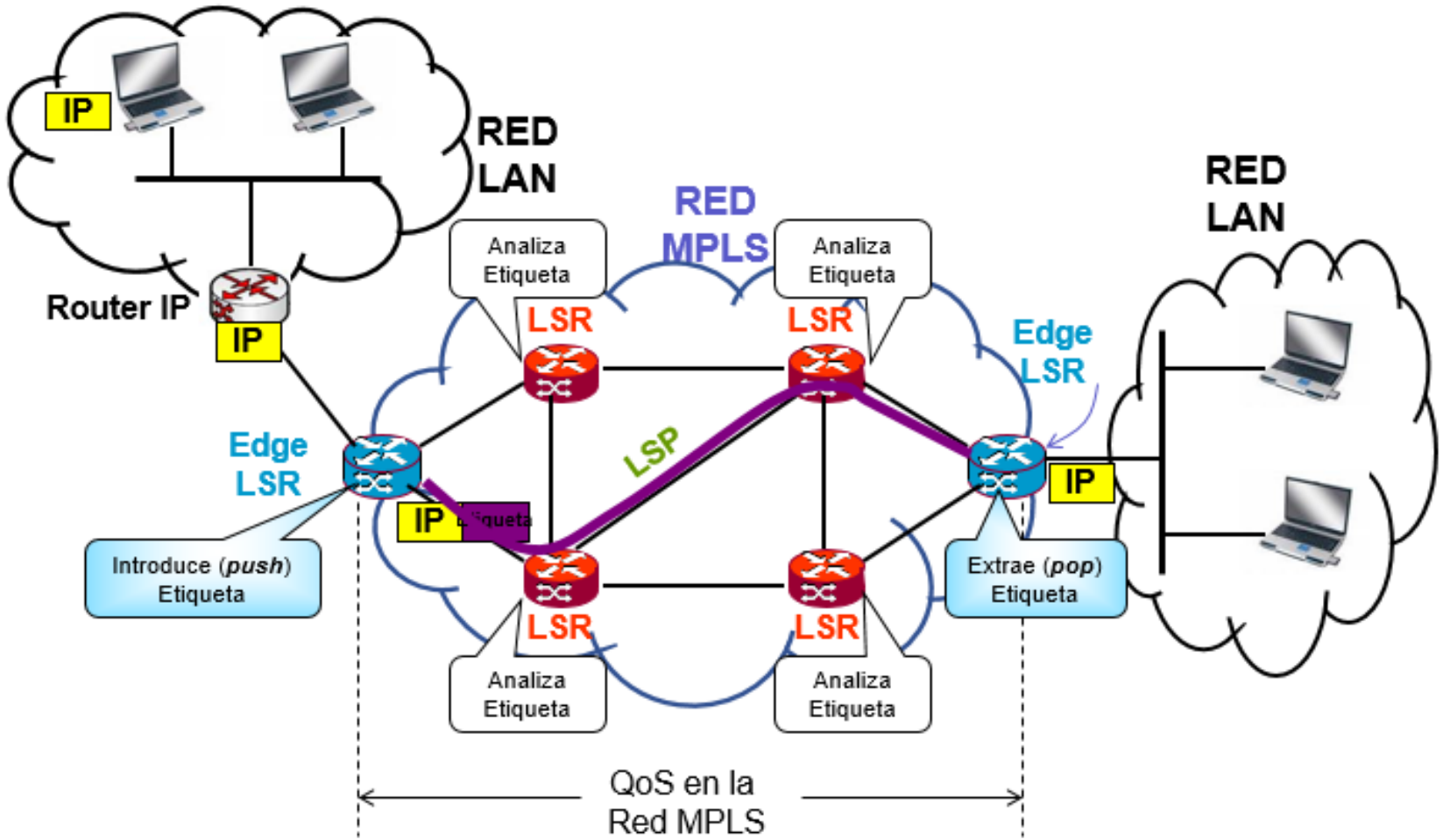
POP/SWAP/PUSH :



POP/SWAP/PUSH :



POP/SWAP/PUSH :



Forward Equivalence Class (FEC) :

Es el conjunto de paquetes que son reenviados sobre el mismo camino o trayecto a través de la red y administrados de la misma forma en lo referido al tratamiento del envío.

- Todos los paquetes que pertenecen al mismo FEC tienen el mismo label.
- Sin embargo, no todos los paquetes que tengan el mismo label significan que pertenezcan al mismo FEC:
  - Los valores del campo EXP pueden ser diferentes y por ende el tratamiento de envío es diferente.

Forward Equivalence Class (FEC) :

- La decisión de pertenencia a un FEC se realiza en el LSR de ingreso al dominio MPLS
- Puede estar fundamentada en **diferentes criterios**:
  - desde algunos más simples como ser únicamente la dirección IP destino
  - hasta criterios más complejos como el ID del protocolo IP, el número de puerto, los bits ToS, etc.

Forward Equivalence Class (FEC) :

•Bajo esta premisa, decimos entonces que:

el ingress LSR es el responsable de identificar el FEC al cual debe pertenecer cada paquete y luego, en función de esto, determinar el LSP y la primera etiqueta que se utilizara para forwardear los paquetes dentro del dominio MPLS.

•Estos LSR incluyen la FEC to Next Hop Label Forwarding Entry FTN mapping table para crear esta relación.

Forward Equivalence Class (FEC) :

- Es un concepto central ya que **el FEC es un conjunto de paquetes que un router**:
  - 1) Reenvía hacia el mismo next hop
  - 2) Lo hace por la misma interfaz de salida
  - 3) Lo hace con el mismo tratamiento (ej encolamiento).

Forward Equivalence Class (FEC) :

Principio de funcionamiento:

- Cuando el paquete arriba al router LSR de ingreso, el FEC es determinado.
- Supongamos que el paquete ingresa por el router R1 y que existe un LSP entre el R1 y el R4, siendo la interfaz de loopback del R4 el punto de terminación del LSP.
- Luego de que en el R1 se determina el FEC, el paquete es encapsulado con el header MPLS y forwardeado por la interfaz correspondiente al siguiente router de la red.
- Los siguientes saltos o routers de la red hasta llegar a R4, simplemente switchean el paquete desde la interfaz entrante hacia la interfaz saliente (en función de la MPLS switching table), con el correspondiente SWAP de etiquetas en cada salto.

Forward Equivalence Class (FEC) :

Principio de funcionamiento:

Es importante destacar que en ningún punto a lo largo del LSP se vuelve a determinar el FEC para el paquete.

•Esto significa, que en una red MPLS, **el FEC es determinado de una única vez, en el ingreso al LSP,** en lugar de saldo a salto como se realiza en el ruteo IP tradicional.

Forward Equivalence Class (FEC) :

•Cuáles son las ventajas de esta forma de definición de las MPLS FEC:

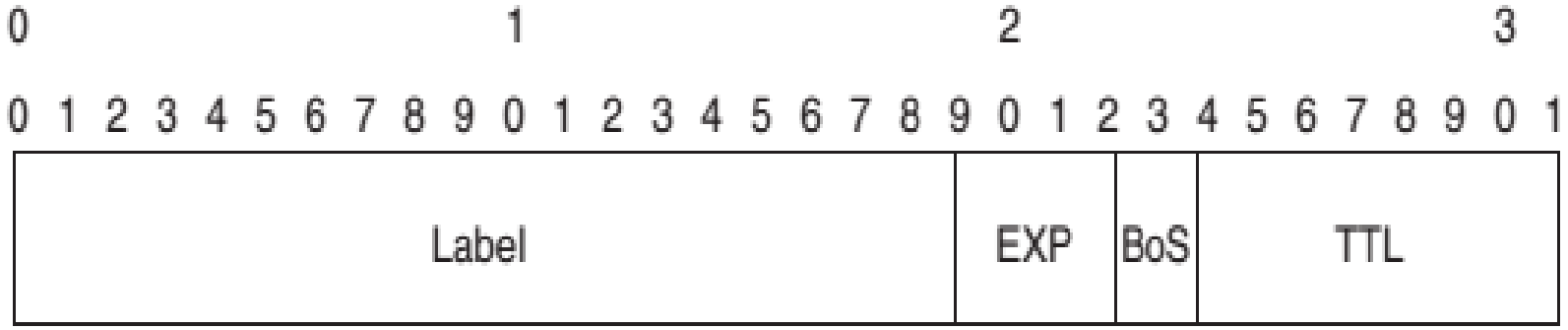
•1) En el core de la red MPLS, solamente se realizan tareas de forwarding con equipos capaces de realizar un lookup y swap de las etiquetas.

•2) Como el FEC es asignado en el punto de ingreso, se pueden utilizar otros parámetros para la asignación del mismo que únicamente los que se encuentran definidos en el header IP, como ser, la interfaz de entrada del paquete.

•3) Se pueden especificar caminos explícitos para un FEC en particular de forma más sencilla comparada con los métodos tradicionales de rute.

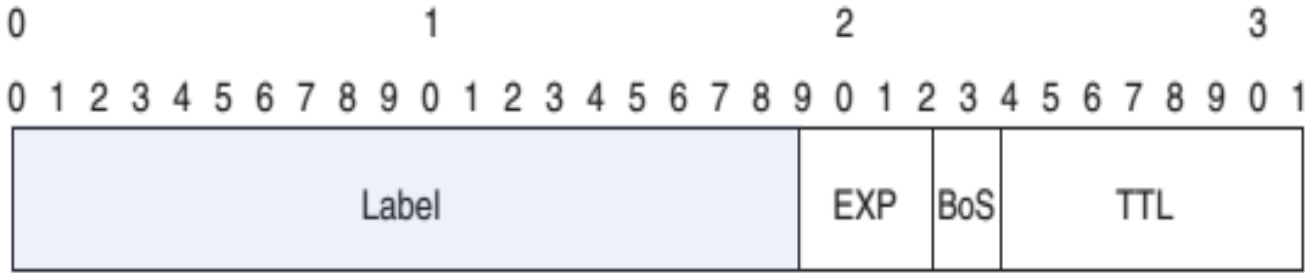
MPLS Labels:

- Un label MPLS consta de **32 bits** con la siguiente estructura:



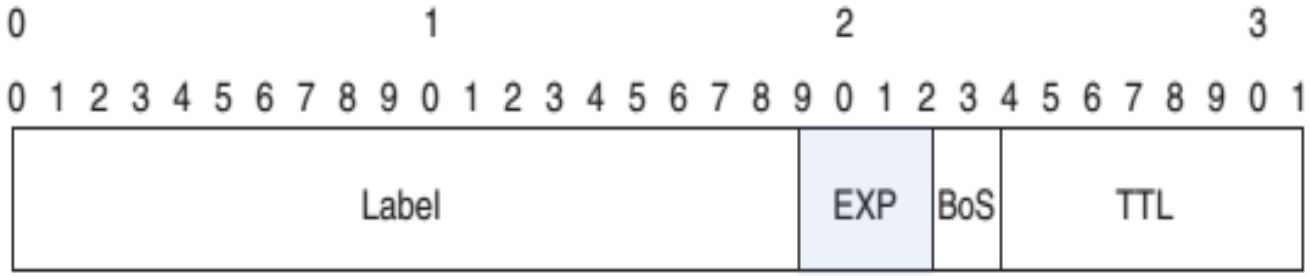
MPLS Labels:

- Los primeros **20 bits**:
  - Son el **campo Label**, donde **se indica el valor del mismo**.
  - Este valor puede ir de 0 a 220-1, es decir 1.048.575.
  - Sin embargo, hay valores reservados exceptuados del uso normal.



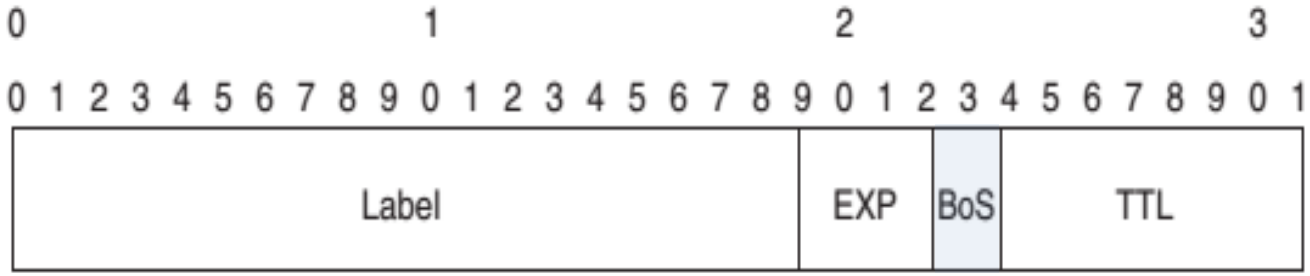
MPLS Labels:

- Los bits del **20 al 22**:
  - Son el **campo Experimental** o EXP, utilizados principalmente para **QoS**.
  - Formalmente se los conoce como campo experimental o EXP, pero actualmente se los denomina Traffic Class (TC) y se utiliza principalmente para funciones de QoS.



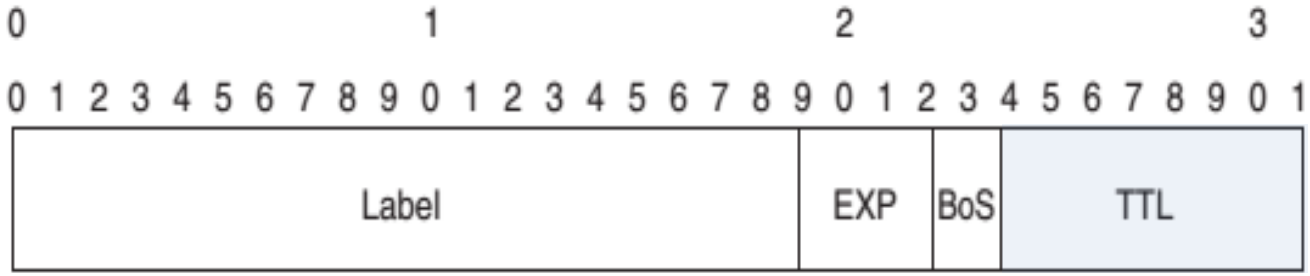
MPLS Labels:

- El bit 23:
  - Es el indicador de Bottom of Stack (BoS).
  - Sera 0, a menos que sea la etiqueta inferior de la pila, en este caso, sera 1.
  - Un stack es una colección de etiquetas, siendo que no hay límites para la cantidad de las mismas,



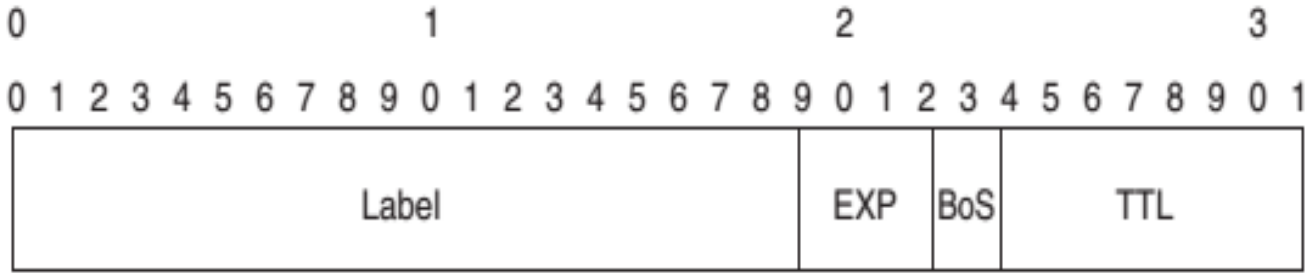
MPLS Labels:

- Los bits 24 a 31:
  - Son los bits utilizados para el TTL.
  - Este TTL tiene la misma función que el TTL que se encuentra en el header IP.
  - Este se decrementa en 1 por cada salto que encuentra.
  - Cuando el TTL alcanza el valor de 0, este se descarta.



MPLS Labels:

```
⊞ Frame 46 (118 bytes on wire, 118 bytes captured)
⊟ Ethernet II, Src: cc:02:02:fc:00:01 (cc:02:02:fc:00:01), Dst: cc:03:02:fc:00:00 (cc:03:02:fc:00:00)
  ⊞ Destination: cc:03:02:fc:00:00 (cc:03:02:fc:00:00)
  ⊞ Source: cc:02:02:fc:00:01 (cc:02:02:fc:00:01)
    Type: MPLS label switched packet (0x8847)
⊟ MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 254
    MPLS Label: 19
    MPLS Experimental Bits: 0
    MPLS Bottom Of Label Stack: 1
    MPLS TTL: 254
⊞ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.4.1 (192.168.4.1)
⊞ Internet Control Message Protocol
```



MPLS Labels reservados:

•Los labels del 0 al 15 son labels reservados.

•Un LSR **no puede utilizar esos valores de etiquetas para el forwarding normal** de paquetes.

- El label 0 esta definido como “explicit NULL label”
- El label 1 esta definido como “router alert label”
- El label 3 esta definido como “implicit NULL label”
- El label 14 esta definido como “OAM alert label”.

•Los restantes labels entre 0 y 15 están reservados pero no tienen una definición especifica aun.

Frame Mode and Cell Mode Labeling:

- Existen dos formas de inserción de la etiqueta:

- Frame mode MPLS:

- En esta, la etiqueta es parte del header de encapsulamiento MPLS.

- Se la denomina **“shim”** ya que el header es insertado en el frame entre el header de Layer 2 y el header de Layer 3.

Frame Mode and Cell Mode Labeling:

•Existen dos formas de inserción de la etiqueta:

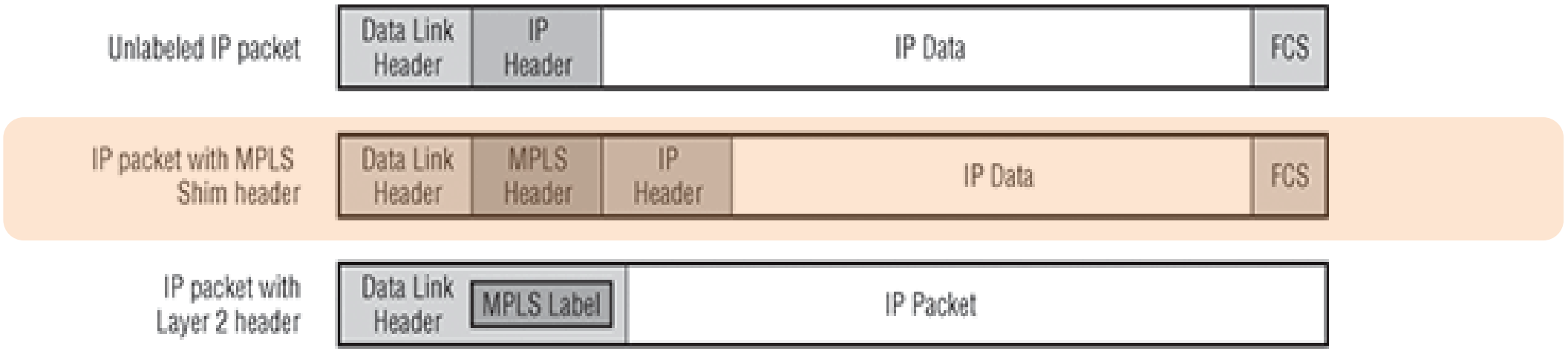
- Cell mode MPLS:

  •Este modo es utilizado en ATM o Fream Relay.

  •En este modo el circuit ID en el header ya existente en la data link layer, es mapeado a la información del label MPLS.

  •En ATM se utiliza el campo VPI/VCI en Frame Relay el campo DLCI.

Frame Mode and Cell Mode Labeling:



Frame Mode and Cell Mode Labeling:

- Por esto, y haciendo referencia al modelo OSI, podemos concluir que:
  - **MPLS NO ES** un protocolo de capa 2 ni un protocolo de capa 3
  - Esto debido a que en el paquete, **los headers de ambos protocolos siguen existiendo**.

Por esto, comúnmente se dice que MPLS es un protocolo de capa 2.5

Frame Mode and Cell Mode Labeling:

•Ahora, como un router MPLS puede **distinguir** entre una paquete etiquetado de uno sin etiquetas?

•Para facilitar esto, se definió **nuevos valores para el campo tipo de protocolos** en la encapsulamiento de Layer 2:

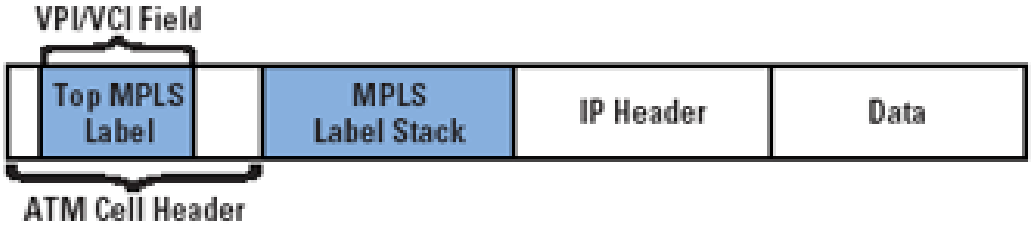
Layer 2 Encapsulation Type	Layer 2 Protocol Identifier Name	Value (hex)
PPP	PPP Protocol field	0281
Ethernet/802.3 LLC/SNAP encapsulation	Ethertype value	8847
HDLC	Protocol	8847
Frame Relay	NLPID (Network Level Protocol ID)	80

```
⊟ Ethernet II, Src: cc:02:02:fc:00:01 (cc
  ⊞ Destination: cc:03:02:fc:00:00 (cc:03:02:fc:00:00)
  ⊞ Source: cc:02:02:fc:00:01 (cc:02:02:fc:00:01)
    Type: MPLS label switched packet (0x8847)
⊟ MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 254
    MPLS Label: 19
    MPLS Experimental Bits: 0
    MPLS Bottom Of Label Stack: 1
    MPLS TTL: 254
```

Frame Mode and Cell Mode Labeling:

(a) Data Link Frame

(b) IEEE 802 MAC Frame



(c) ATM Cell

(d) Frame Relay Frame

Label stacking:

- Es una de las **características más potentes de MPLS**.

- Un paquete etiquetado puede tener varias etiquetas.

- Estas organizadas en una pila LIFO.

- Teniendo el procesamiento siempre como referencia la etiqueta superior.

- Este apilamiento hace posible **enmascarar múltiples LSPs como uno solo**, creando así un túnel.

Label stacking:

•Al **comienzo del túnel**, un LSR asigna la misma etiqueta a los paquetes de varios LSP introduciendo la etiqueta en cada pila.

•Al **final del túnel**, otro LSR extrae el elemento superior de la pila, revelando la etiqueta interna.

•**En cualquier LSR**, una etiqueta puede ser apilada o retirada.

Label stacking:

- El **primer label o más externo** se lo denomina top label.
- El **último o más interno** se lo denomina bottom label.
- Entre estos dos labels, podemos tener cualquier número de etiquetas.
- MPLS admite un **apilado ilimitado**, dentro de las restricciones de tamaño impuestas por la red.

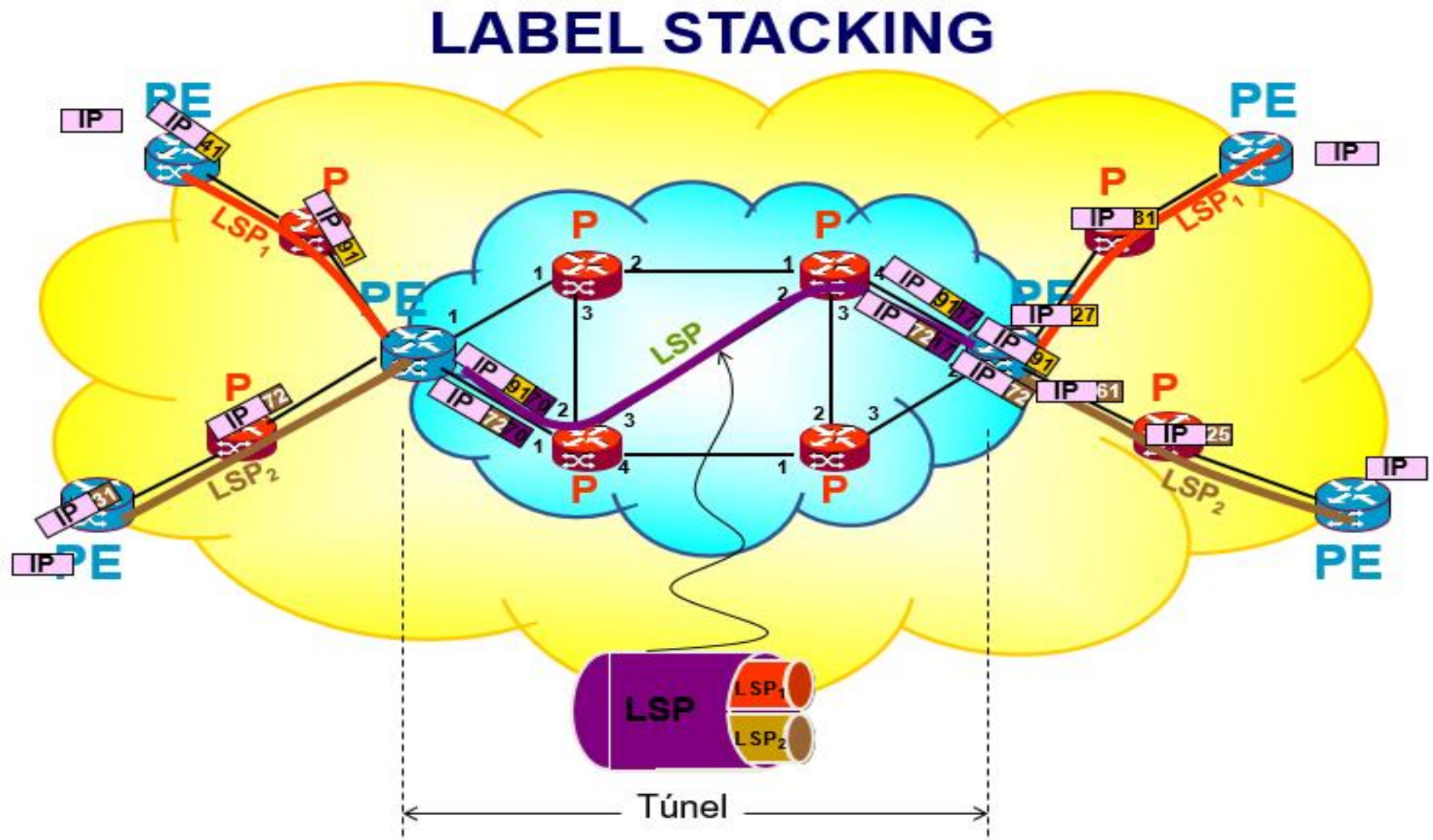
Label stacking:

Label stacking:

- En la figura anterior vemos:
  - Un label stack donde el bit BoS se encuentra en 0 para todas las etiquetas
  - La “bottom” label o más interna que se encuentra en 1.
- Cuando S = 1 **indica que es la última etiqueta** y que al salir quedará vacía la pila.
- Esto generalmente ocurre en el router de salida, cuando es S = 0 indica que por lo menos hay otra etiqueta antes, en la pila.

- *Estos label stack son necesarios en algunas aplicaciones como las MPLS VPNs.*

Label stacking:



Procesamiento del campo TTL:

- Un elemento clave en el encabezado de un paquete IP es el campo TTL y el Limite de Saltos (Hop limit).
- En un ambiente ruteado (basado en IP), dicho campo va disminuyendo en uno hasta que llega a cero y se elimina el paquete.
- Esto es una medida de **prevención de loops de los paquetes L3.**
- En MPLS no se lee el encabezado de los paquetes IP
  - Por eso que es necesario añadir estos 8 bits que manejan el TTL para evitar que ocurra lo mencionado anteriormente.

Procesamiento del campo TTL:

Reglas para procesar el campo TTL:

- Cuando un paquete IP llega al router de entrada de un dominio MPLS:
  - Se añade una etiqueta de entrada a la pila
  - El valor de TTL de este campo se obtiene del valor original del TTL en IP.

(En este paso se da por supuesto que el campo ya fue disminuido, como parte del proceso IP.)

Procesamiento del campo TTL:

Reglas para procesar el campo TTL:

- Cuando un paquete MPLS llega a uno de los LSR internos:
- **El valor del campo TTL de la etiqueta del primer elemento en la pila es disminuido**.
- Entonces:
  - Si el valor es 0:
    - no se reenvía el paquete
    - dependiendo del valor que tenga la etiqueta del paquete puede ser desechado o es enviado al nivel de red para procesamiento de errores.

Procesamiento del campo TTL:

- Si el valor es positivo:
  - se le añade a la nueva etiqueta de la pila en el campo TTL y es reenviado al siguiente salto.
  - El valor del campo TTL del paquete reenviado esta dado en función del valor del campo de Tiempo de Vida del paquete original.

Procesamiento del campo TTL:

- Cuando un paquete MPLS llega a un LSR de salida:
  - El valor del campo TTL en la etiqueta es disminuido (uno por uno)
  - Posteriormente se quita la etiqueta de la pila, lo que deja una pila vacía.
- Entonces:
  - Si el valor es 0:
    - no se reenvía el paquete.
    - dependiendo del valor que tenga la etiqueta del paquete puede ser desechado o es enviado al nivel de red para procesamiento de errores.

Procesamiento del campo TTL:

- Si el valor es positivo:

se coloca en el campo TTL del encabezado IP

- ***es enviado utilizando ruteo IP tradicional.***

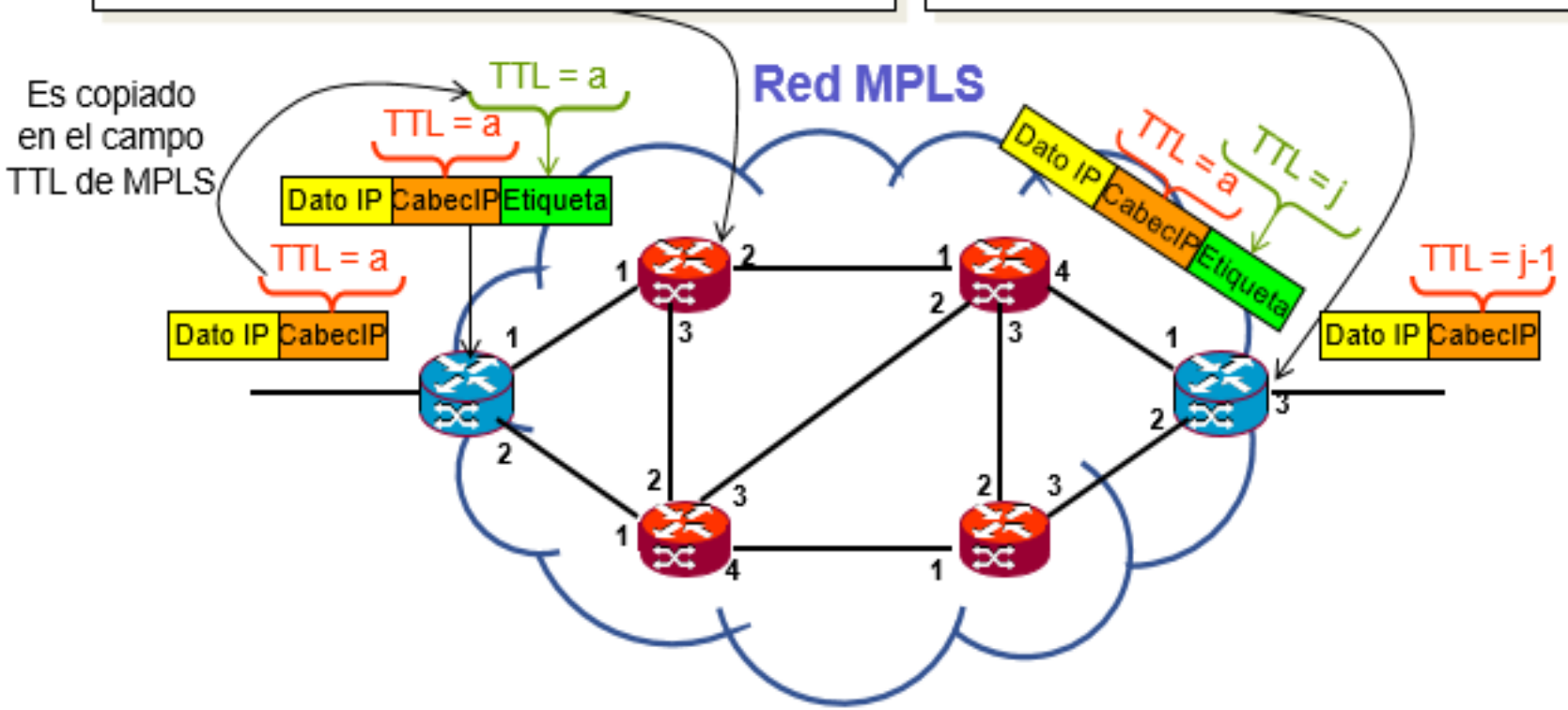
Procesamiento del campo TTL:

a – 1 = 0, No se envía el paquete IP etiquetado
Se descarta simplemente o
se envía a la capa 3 para generar ICMP

a – 1 > 0, Se actualiza el campo TTL de MPLS y el paquete etiquetado en enviado

j – 1 = 0, No se envía el paquete IP etiquetado
Se descarta simplemente o
se envía a la capa 3 para generar ICMP

j – 1 > 0, Se actualiza el campo TTL de IP y el paquete IP es enviado según la capa 3



Relación entre FECs, LSPs y Etiquetas:

•Para que esta relación se lleve a cabo satisfactoriamente se deben de cumplir los **siguientes requisitos:**

•1. Todo tráfico debe de **asignarse a un FEC específico**.

•2. Se necesita un **protocolo de ruteo para determinar la topología** y las condiciones del dominio para que las LSPs puedan ser asignadas a un FEC.

•3. Cada **LSR debe de conocer las LSPs de cada FEC** para poder asignarles una etiqueta de entrada y deben de comunicarla a todos los demás LSR en la ruta de dicho LSP.

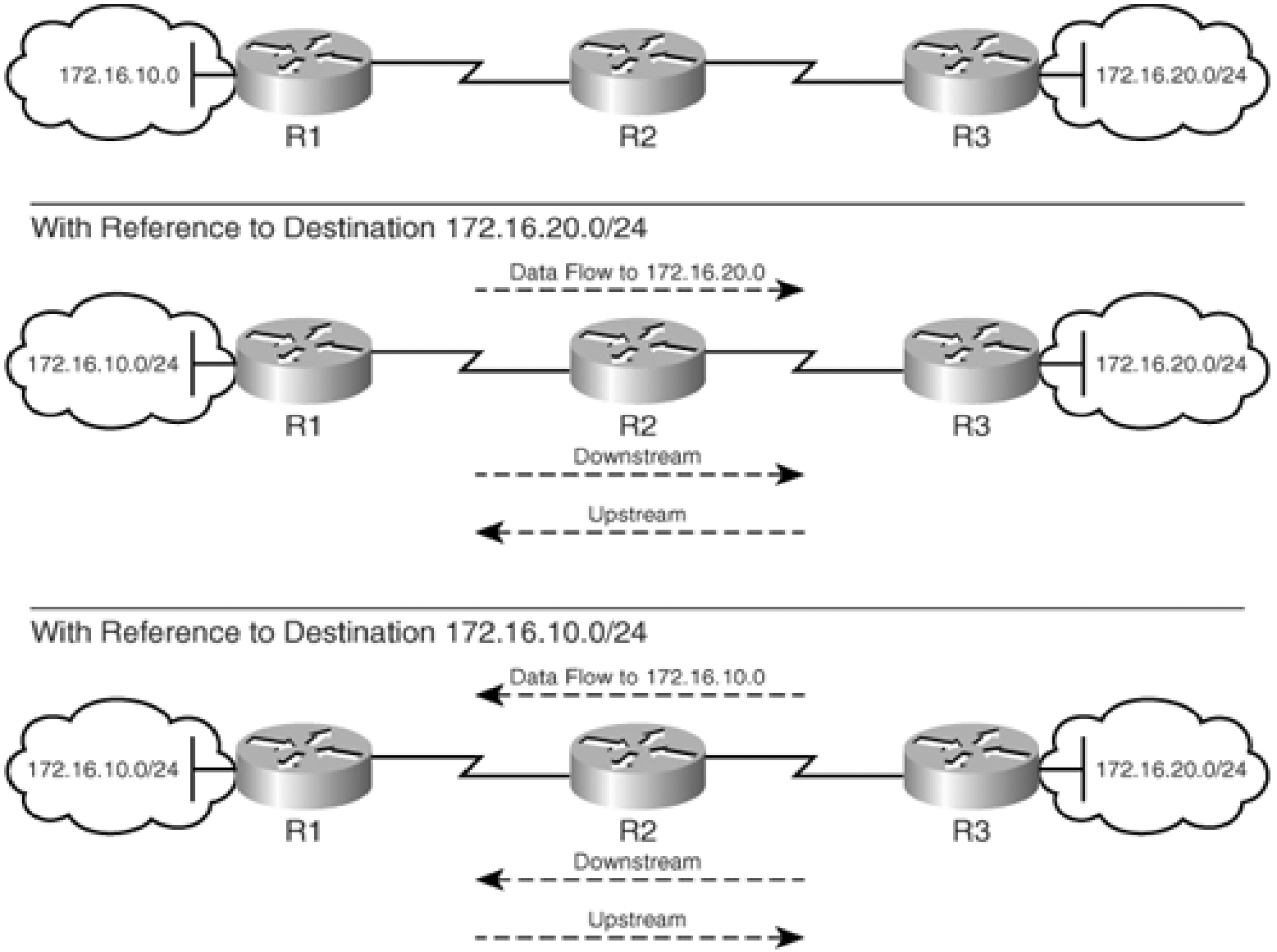
Upstream and downstream:

- Ambos términos están ***definidos en referencia a la red destino***, ya sea prefijo o FEC.

- Los datos **dirigidos a una red destino** en particular siempre circulan “dowstream”

- Las **actualizaciones de rutas o de distribución de etiquetas**, pertenecientes a un prefijo especifico son siempre propagadas “upstream”.

Upstream and downstream:



Penultimate Hop Popping (PHP):

- **Un "egress Edge-LSR" de una red MPLS,** debe realizar *dos lookups* en el paquete recibido de un vecino MPLS con destino a una subred fuera del dominio MPLS.
  - Debe inspeccionar la etiqueta y realizar el label lookup para verificar que acción debe tomar sobre la misma.
  - Debe realizar un lookup en capa 3 en el paquete IP antes de forwardear el paquete a su destino final.
- *Este doble lookup reduce la performance en el nodo*.

Penultimate Hop Popping (PHP):

•Para mejorar esta situación, se realiza el Penultimate Hop Popping PHP.

•Básicamente, si utilizamos PHP, lo que esencialmente hacemos es:

terminar el LSP un salto antes.

•El label MPLS es descartado por el router que conecta al egress router, en lugar de ser descartado por el mismo egress router.

•De esta forma se consigue que el paquete llegue al Egress LSR sin etiqueta y solo haga falta examinar su cabecera de capa de red.

Penultimate Hop Popping (PHP):

- Evitando así la realización de doble consulta en el mismo dispositivo.
- Reduciendo considerablemente el retraso de tratamiento del mismo.

- Si existe más de una etiqueta en la pila, el PHP retira la situada en el nivel superior.
- Para que este PHP funcione, el egress LSR solicita el "popping" mediante LDP.
- Para esto, el egress LSR anuncia **"implicit-null label"** como etiqueta.

Penultimate Hop Popping (PHP):

•La RFC 3032 “MPLS Label Stack Encoding” especifica dos valores reservados que son utilizados en el “last hop” de un LSP

0: explicit NULL:

- •Puede ser utilizado en protocolos de señalización como así también en las etiquetas de los headers.

Penultimate Hop Popping (PHP):

3: implicit NULL.

- Se utiliza únicamente en los protocolos de señalización, nunca debe aparecer en un label stack.

- Se utiliza en los protocolos de señalización para indicar que el “upstream” router deberá realizar penultimate hop pooping PHP, es decir remover el label del stack.

Penultimate Hop Popping (PHP):

- Cuando un egress LSR solicita un PHP para un determinado prefijo IP:

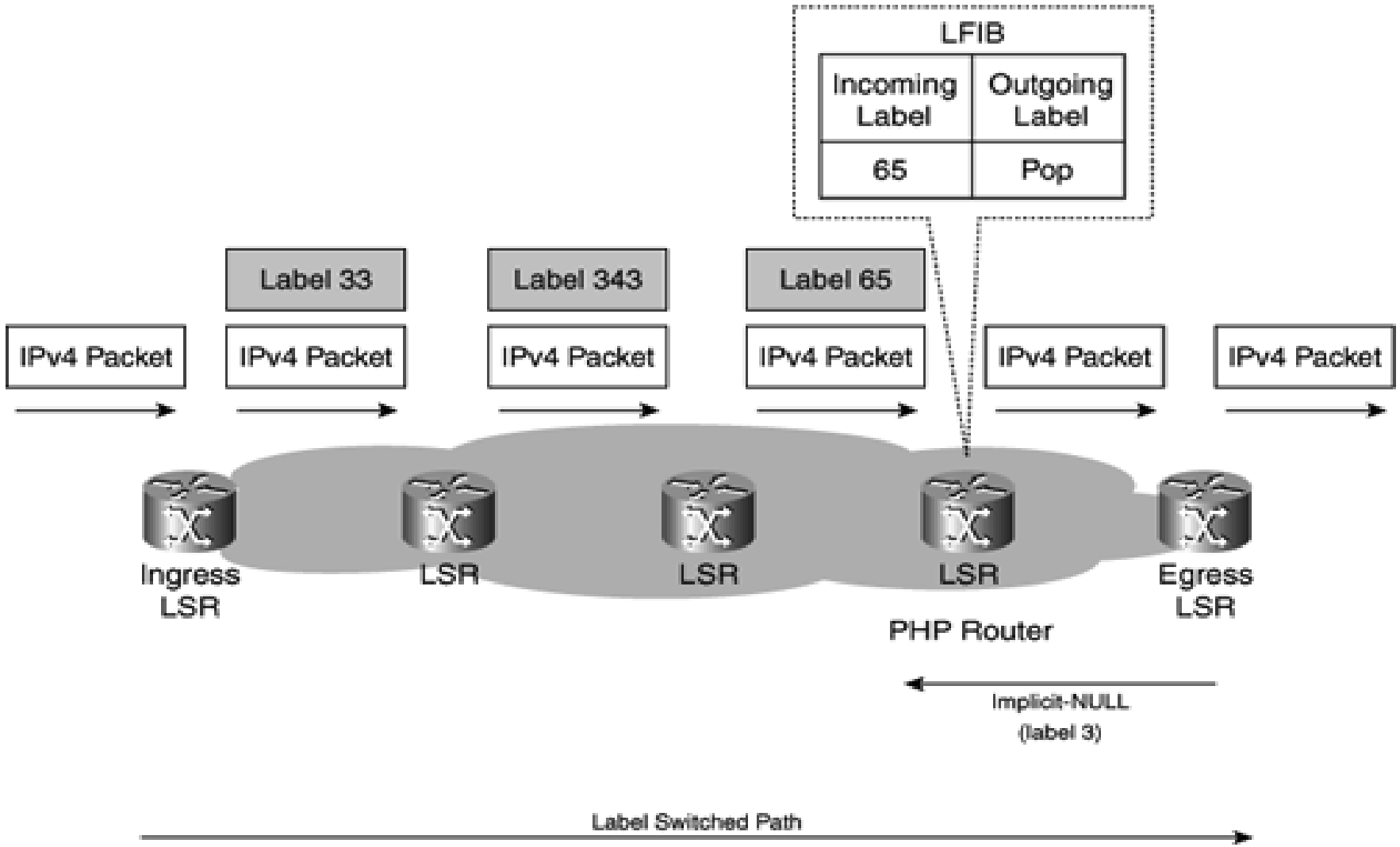
  - la entrada en la **LIB local y la LIB remota** en el LSR upstream,

    indican el valor implicit-null

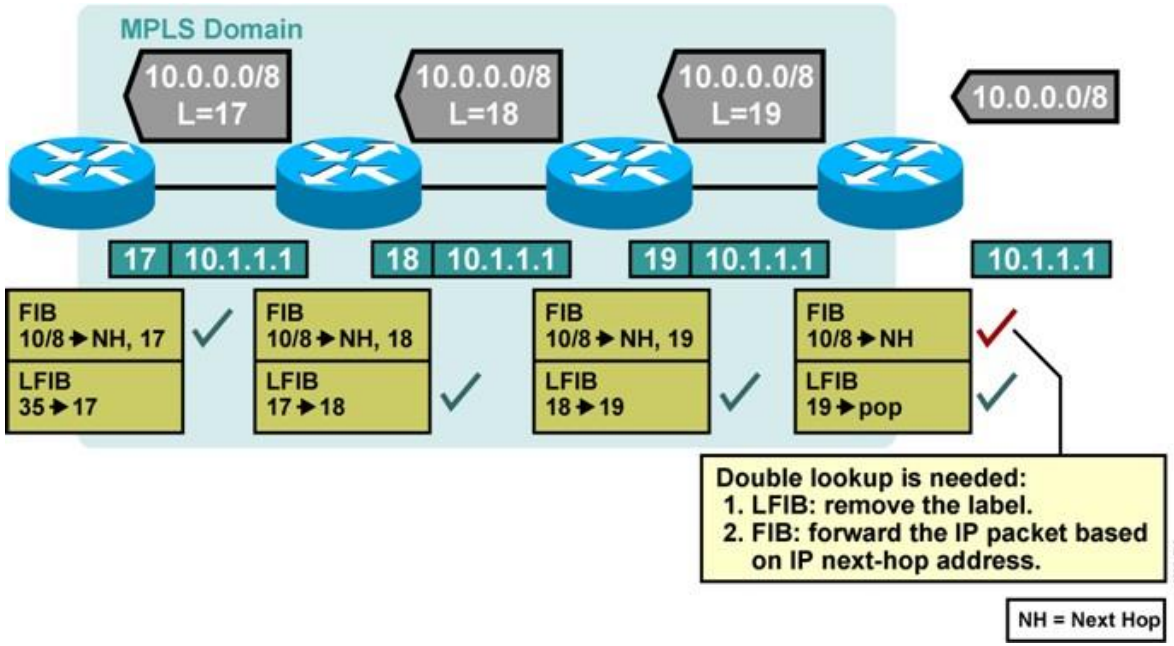
  - en una entrada en la **LFIB del penultimate LSR**

    indica que la operación para el label deberá ser POP.

Penultimate Hop Popping (PHP):

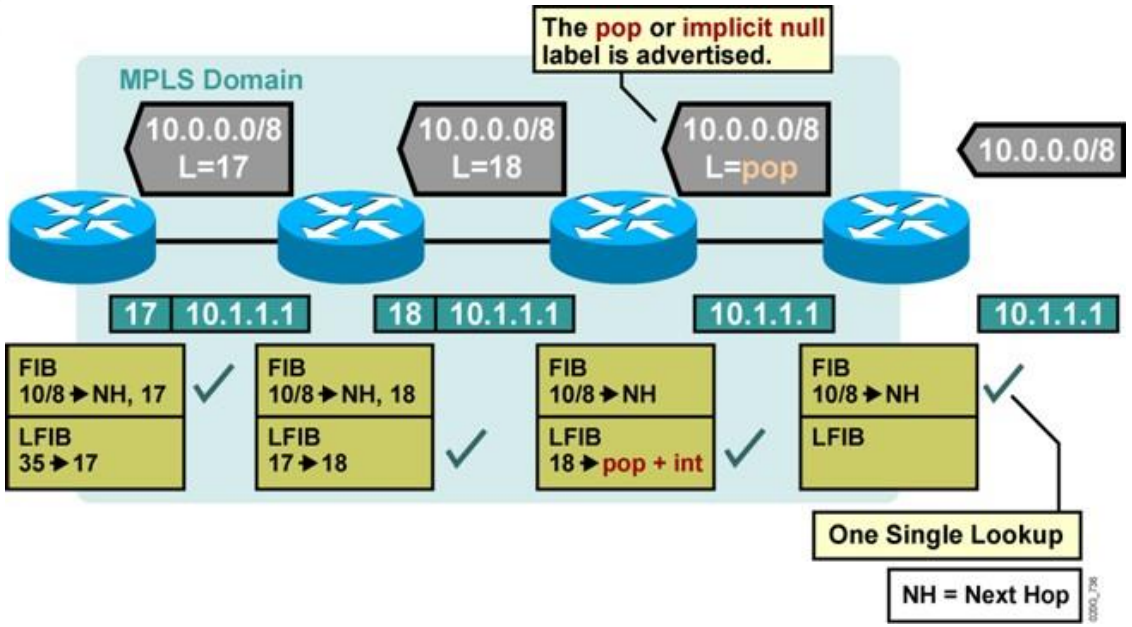


Penultimate Hop Popping (PHP):



SIN PHP

CON PHP



Control Plane / Data Plane:

- Estos planos de operación son los **componentes básicos de la arquitectura en capas** que las redes han evolucionado hasta la actualidad.

- Todos los nodos de una red MPLS deben correr alguna instancia de routing.

- Ya sea con ruteo estático o con ruteo dinámico.

- En este sentido, cada nodo de la red MPLS, es entonces un router IP en el **plano de control.**

Control Plane / Data Plane:

•Los nodos MPLS intercambian etiquetas de subredes específicas que están contenidas dentro de la tabla de ruteo.

•Estas etiquetas intercambiadas son utilizadas para construir la Label Forwarding Table.

•Esta tabla es la base de datos del **plano de forwarding** que se utiliza para conmutar los paquetes dentro de la red MPLS.

Control Plane / Data Plane:

- El **Plano de Control**:
  - Son los elementos necesarios para que el routing funcione dentro del dispositivo.
  - Es decir, la señalización de la red.
  - En el plano de control, los paquetes están destinados “a” o localmente originados por el dispositivo.

Control Plane / Data Plane:

- El **Plano de Control**:
  - Toma doma decisiones respecto donde el tráfico es forwardeado
  - Los paquetes del plano de control son destinado a o localmente originados por el dispositivo.
  - Incluye funciones tales como configuración del sistema, management e intercambio de información de routing.
  - En este plano, el dispositivo intercambia información de la topología con otros routers para construir la tabla de routing.

Control Plane / Data Plane:

- El **Plano de Control**:
  - Es el ***plano de señalización de la red.***
  - Debido a que las funciones de control no son realizadas en cada paquete que arriba, podemos considerar que *son menos "time-critical" para el procesamiento*.
  - La principal tarea del plano de control es anunciar las etiquetas y las direcciones y relacionarlas; esto es, asociar (mapear) etiquetas y direcciones.

Control Plane / Data Plane:

- El **Plano de Datos o Forwarding Plane**:
  - Es básicamente todo aquello que atraviesa el router y no está dirigido hacia el router.
  - Esta es, quizás, la principal diferencia entre los planos de datos y de control, es decir:

la forma en la que el dispositivo o router lo procesa.

  - Reenvía o forwardea el trafico al siguiente salto a lo largo del camino para alcanzar un determinado destino de la red, de acuerdo a la información obtenida del plano de control.
  - Este plano de datos, es **la clave de los elementos de conmutación de nuestra red**.

Control Plane / Data Plane:

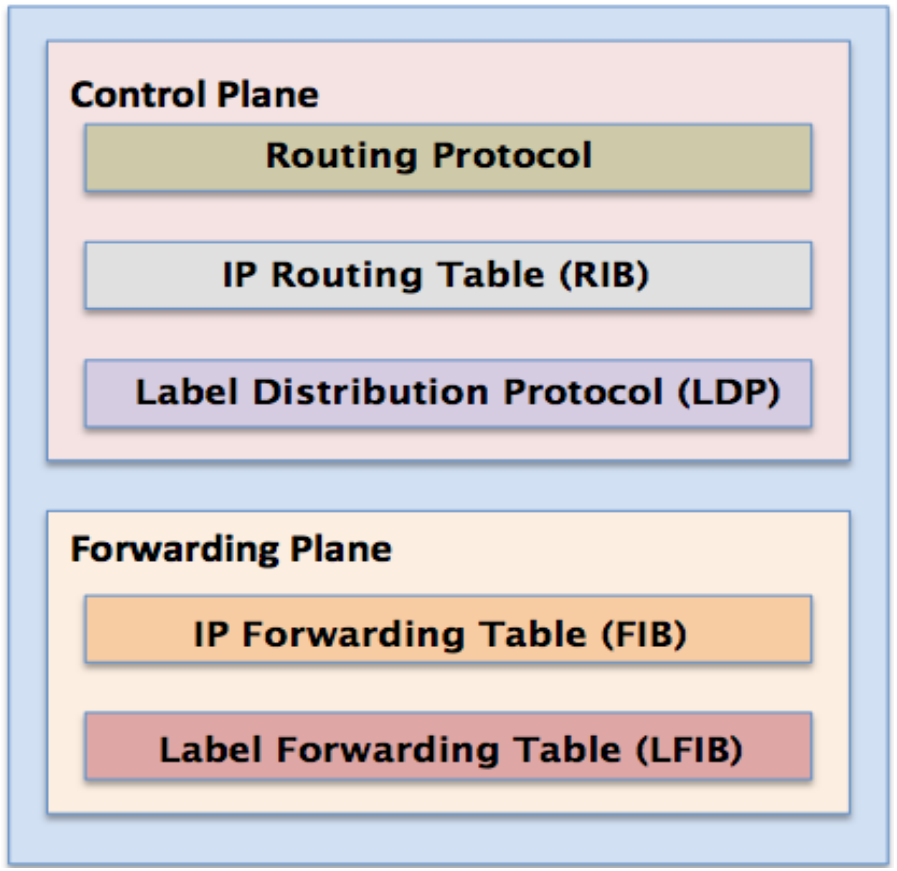
- El **Plano de Datos o Forwarding Plane**:
  - Todas las operaciones que realiza, deben ser "fast path" para mantener la performance de la red.
  - Para alcanzar este objetivo, se utilizan diferentes tipos de componentes, como ASICs, TCAM, NPU o FPGA.

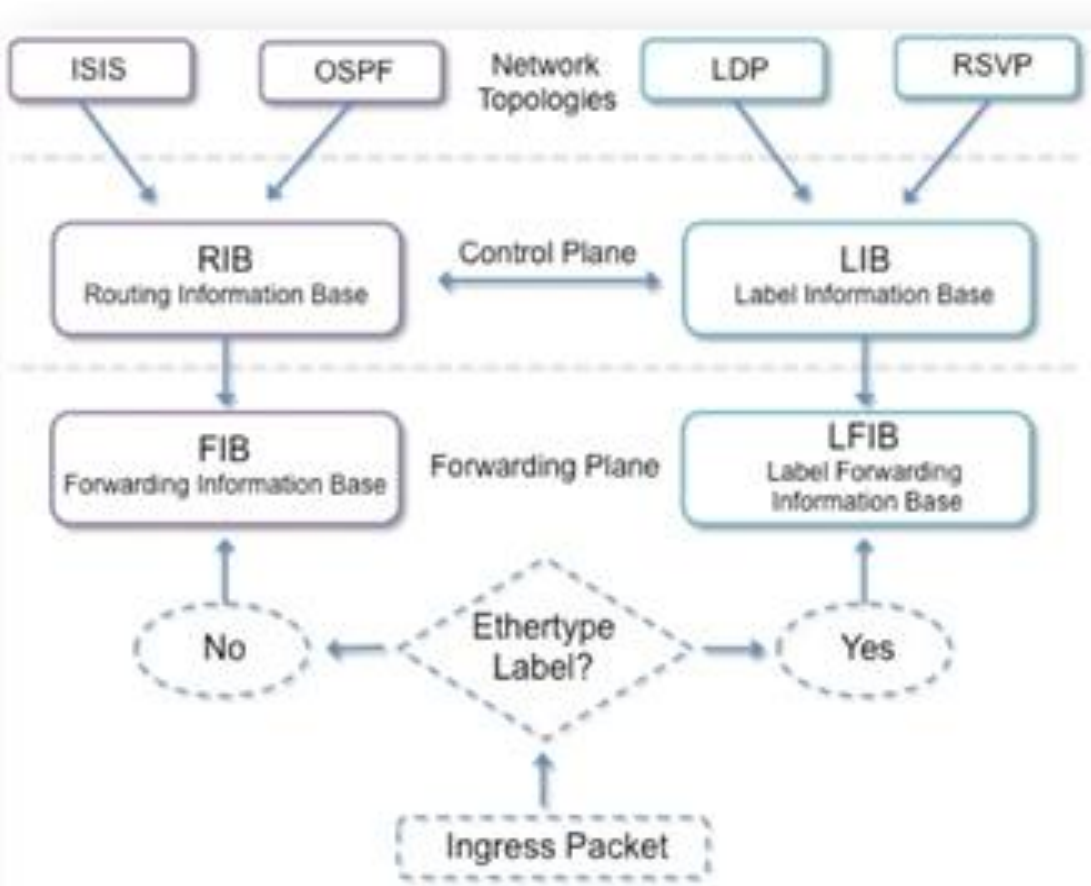
El plano de datos de MPLS reenvía el tráfico examinando la etiqueta en el encabezado del paquete MPLS.

Control Plane / Data Plane:

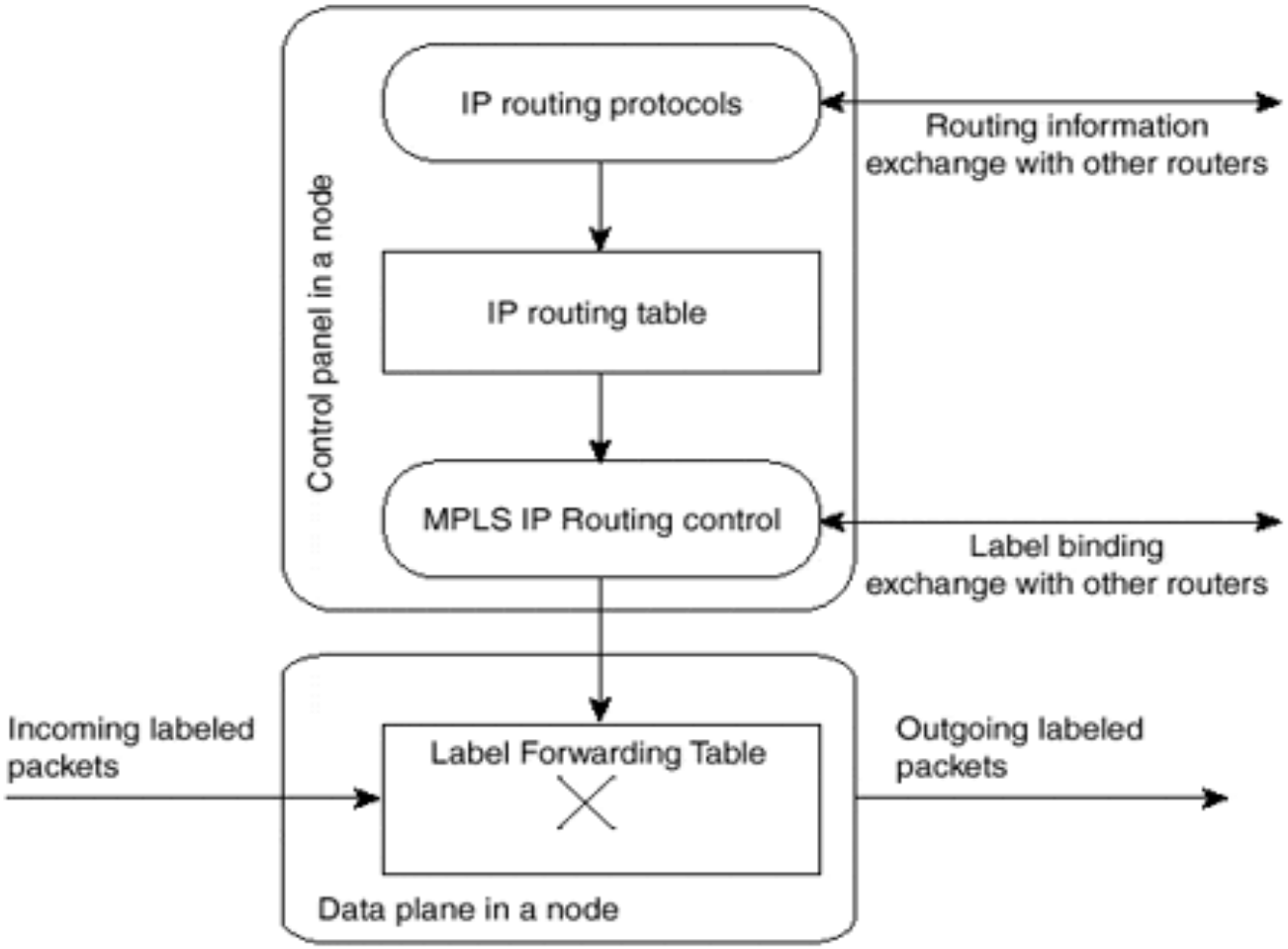
- El **Plano de Datos o Forwarding Plane**:
  - Dos estructuras son importantes y construidas en base a la información creada en el plano de Control.
    - La Forwarding Information Base o **FIB**
    - La Label Forwarding Information Base o **LFIB.**

Control Plane / Data Plane:





Control Plane / Data Plane:

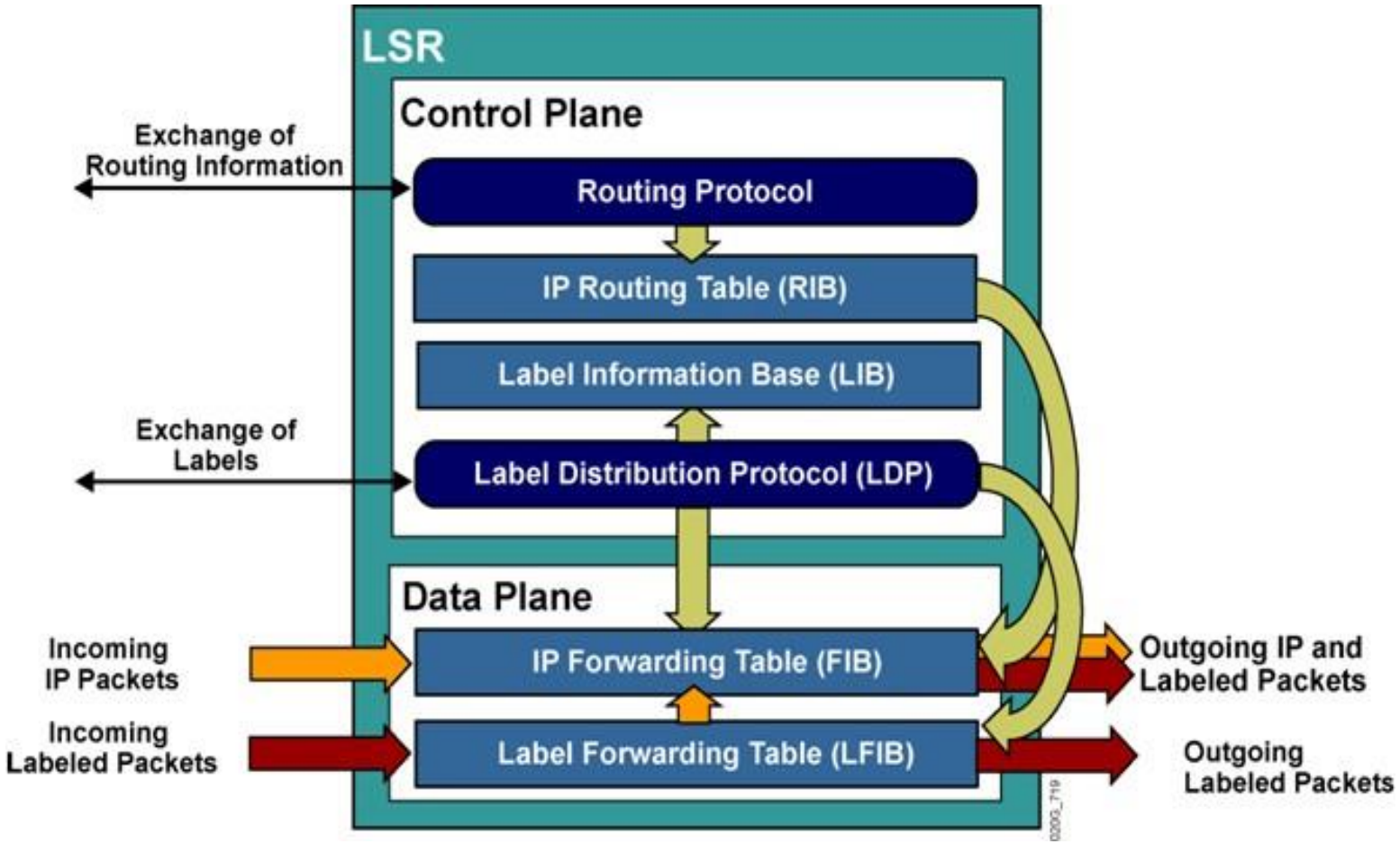


Control Plane / Data Plane:

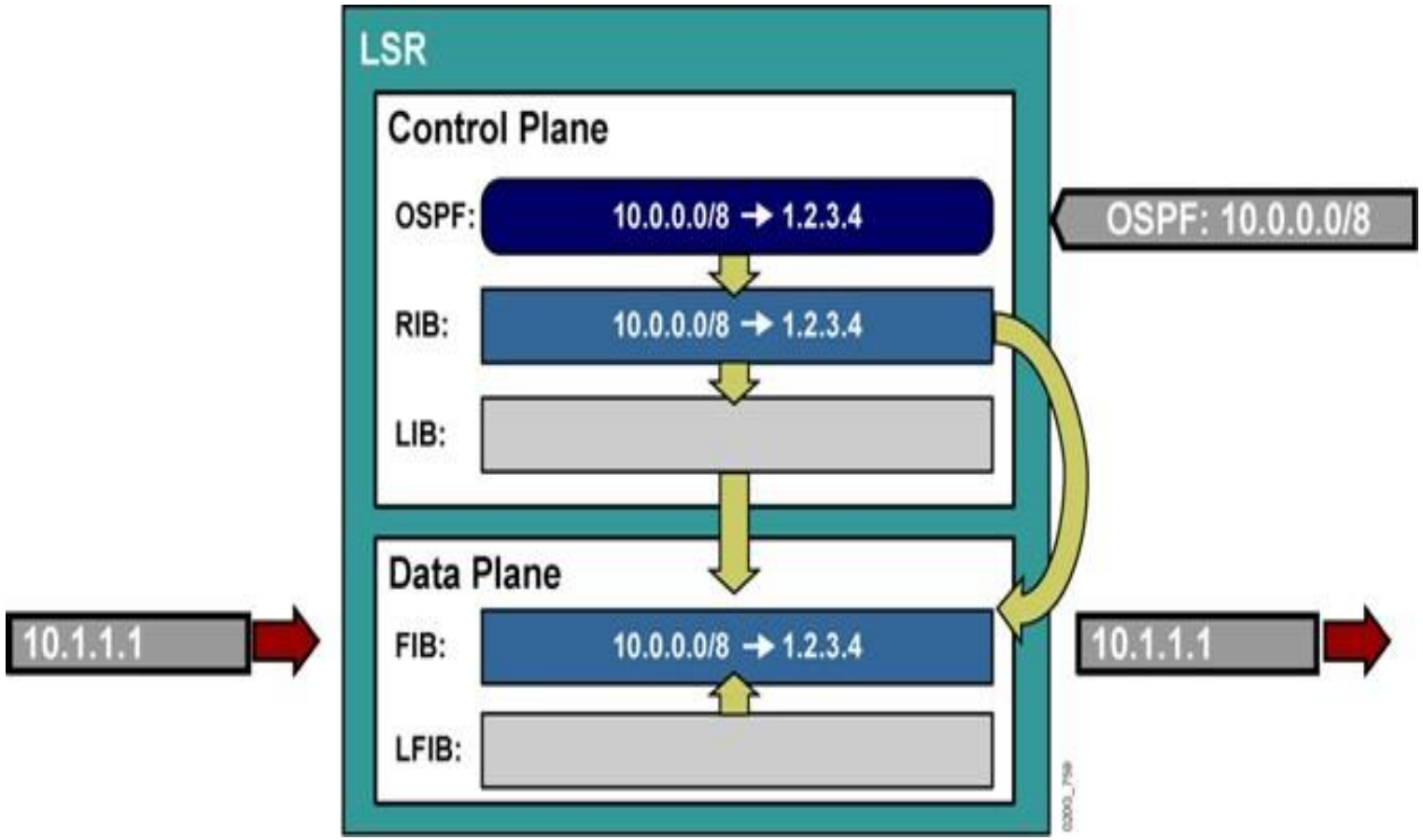
- Entonces, se puede pensar:
  - MPLS es una tecnología que ubica la **"inteligencia" al borde de la red**
  - Dejando el **núcleo para hacer la conmutación**.

En otras palabras, el plano de control de red se encuentra en el borde y el plano de reenvío está en el core.

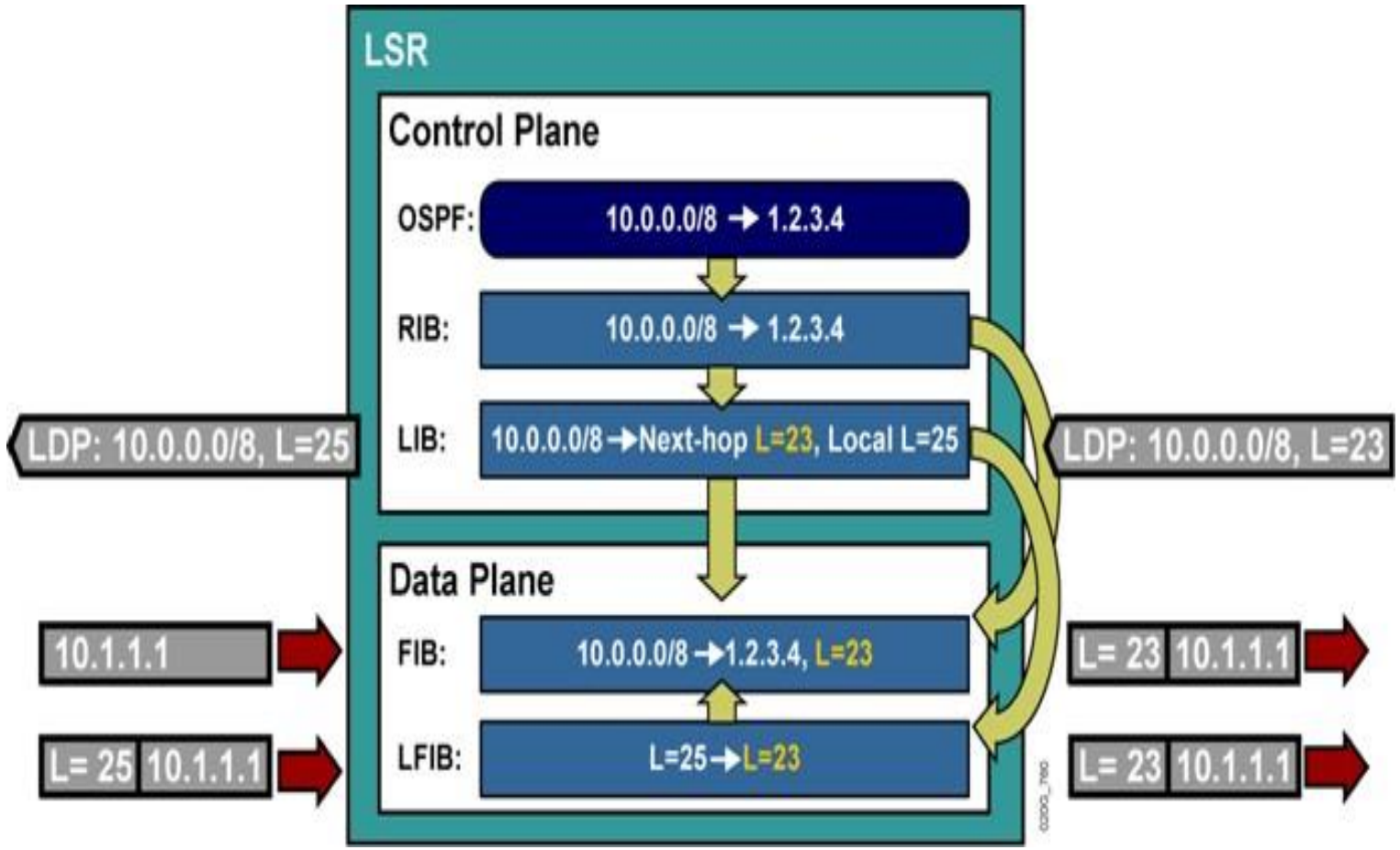
Control Plane / Data Plane:



Control Plane / Data Plane:



Control Plane / Data Plane:



RIB / FIB / LIB / LFIB:

- **Routing Information Base (RIB):**
  - Es básicamente la tabla de ruteo.
  - Es completada con información de rutas estáticas, directamente conectadas o provenientes de protocolos de ruteo dinámico.
  - Para poder observar esta tabla de ruteo, utilizamos el comando **#show ip route.**

RIB / FIB / LIB / LFIB:

- **Routing Information Base (RIB):**

```
P1#show 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

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 10.0.12.1, 00:08:11, FastEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/12] via 10.0.24.4, 00:08:11, FastEthernet0/1
                [110/12] via 10.0.12.1, 00:08:11, FastEthernet0/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.0.24.4, 00:08:11, FastEthernet0/1
     10.0.0.0/24 is subnetted, 4 subnets
C       10.0.12.0 is directly connected, FastEthernet0/0
O       10.0.13.0 [110/11] via 10.0.12.1, 00:08:12, FastEthernet0/0
C       10.0.24.0 is directly connected, FastEthernet0/1
O       10.0.34.0 [110/11] via 10.0.24.4, 00:08:13, FastEthernet0/1
```

RIB / FIB / LIB / LFIB:

- **Forwarding Information Base (FIB):**
  - Es la tabla que el router finalmente utilizara para forwardear paquetes.
  - Cisco con CEF (cisco express forwarding) utiliza la información proveniente de la RIB para completar la FIB.
  - **Contiene:**
    - el router del siguiente salto (next-hop)
    - la interfaz de salida para cada prefijo IP de destino en la RIB.
  - Para poder visualizar la CEF FIB, utilizamos el comando **#show ip cef**:

RIB / FIB / LIB / LFIB:

- **Forwarding Information Base (FIB):**

```
P1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
0.0.0.0/32          receive
1.1.1.1/32          10.0.12.1           FastEthernet0/0
2.2.2.2/32          receive
3.3.3.3/32          10.0.24.4           FastEthernet0/1
                    10.0.12.1           FastEthernet0/0
4.4.4.4/32          10.0.24.4           FastEthernet0/1
10.0.12.0/24        attached            FastEthernet0/0
10.0.12.0/32        receive
10.0.12.1/32        10.0.12.1           FastEthernet0/0
10.0.12.2/32        receive
10.0.12.255/32      receive
10.0.13.0/24        10.0.12.1           FastEthernet0/0
10.0.24.0/24        attached            FastEthernet0/1
10.0.24.0/32        receive
10.0.24.2/32        receive
10.0.24.4/32        10.0.24.4           FastEthernet0/1
10.0.24.255/32      receive
10.0.34.0/24        10.0.24.4           FastEthernet0/1
224.0.0.0/4         drop
224.0.0.0/24        receive
255.255.255.255/32  receive
```

RIB / FIB / LIB / LFIB:

La diferencia entre la RIB y la FIB es que :

****) la RIB opera en el plano de control***

****) la FIB en el plano de forwarding o datos.***

RIB / FIB / LIB / LFIB:

- **La LIB (Label Information Base):**
  - Es una base de datos que almacena información acerca de los posibles destinos y la forma de alcanzarlos.
  - Los protocolos de intercambio de etiquetas asignan un label local a cada prefijo IP de su tabla de ruteo.
  - Este mapeo label/prefijo en el router es llamado “local binding”.
  - Luego de esto, el router publicara este mapeo a sus vecinos.

RIB / FIB / LIB / LFIB:

- **La LIB (Label Information Base):**
  - Adicionalmente los routers vecinos LDP también realizaran el mismo mapeo y lo publicaran.
  - El mapeo label/prefijo recibido de los vecinos LDP entonces serán los remote bindings en el router.
  - **Tanto los local bindings como los remote bindings son almacenados en la Label Information Base (LIB).**
- Para observar el contenido de la LIB, utilizamos el comando **#show mpls ldp bindings**

RIB / FIB / LIB / LFIB:

- **La LIB (Label Information Base):**
  - De forma similar a la información de rutas, donde un router puede aprender diferentes caminos hacia un vecino, debiendo seleccionar el mejor trayecto hasta el, la LIB puede contener **más de un remote binding para un prefijo particular**, debiendo también seleccionar el mejor camino (etiqueta e interfaz saliente) a utilizar.

RIB / FIB / LIB / LFIB:

- **La LIB (Label Information Base):**

```
P1#show mpls ldp bindings
  tib entry: 1.1.1.1/32, rev 12
        local binding:  tag: 18
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 21
  tib entry: 2.2.2.2/32, rev 2
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: 19
        remote binding: tsr: 4.4.4.4:0, tag: 18
  tib entry: 3.3.3.3/32, rev 10
        local binding:  tag: 17
        remote binding: tsr: 1.1.1.1:0, tag: 18
        remote binding: tsr: 4.4.4.4:0, tag: 17
  tib entry: 4.4.4.4/32, rev 8
        local binding:  tag: 16
        remote binding: tsr: 1.1.1.1:0, tag: 17
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
  tib entry: 10.0.12.0/24, rev 4
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 20
  tib entry: 10.0.13.0/24, rev 16
        local binding:  tag: 20
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
        remote binding: tsr: 4.4.4.4:0, tag: 19
  tib entry: 10.0.24.0/24, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 1.1.1.1:0, tag: 21
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
  tib entry: 10.0.34.0/24, rev 14
        local binding:  tag: 19
        remote binding: tsr: 1.1.1.1:0, tag: 20
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
  tib entry: 10.0.100.0/24, rev 17
        remote binding: tsr: 1.1.1.1:0, tag: imp-null
  tib entry: 10.0.200.0/24, rev 19
        remote binding: tsr: 4.4.4.4:0, tag: imp-null
  tib entry: 192.168.100.0/24, rev 18
        remote binding: tsr: 1.1.1.1:0, tag: 16
  tib entry: 192.168.200.0/24, rev 20
        remote binding: tsr: 4.4.4.4:0, tag: 16
```

RIB / FIB / LIB / LFIB:

- **La LFIB (Label Forwarding Information Base)**
  - Es utilizada para:
    - Determinar cómo procesar los paquetes entrantes etiquetados.
    - Determinar el próximo nodo que debe recibir el paquete.

La LFIB es para MPLS lo que la tabla de rutas es para IP.

- Esta LFIB es una estructura de datos donde destinos y las etiquetas entrantes son asociados con interfaces salientes y nuevas etiquetas.

RIB / FIB / LIB / LFIB:

- **La LFIB (Label Forwarding Information Base)**
  - Cuando un paquete etiquetado es recibido por un LSR, el switch utiliza esta etiqueta como un “index” en la LFIB.
  - Cada entrada en la LFIB consiste en:
    - un “incoming label”
    - una o más subentradas como ser:
      - outgoing label, outgoing interface, outgoing link-level information.
- El comando para visualizar la LFIB es **#show mpls forwarding-table.**

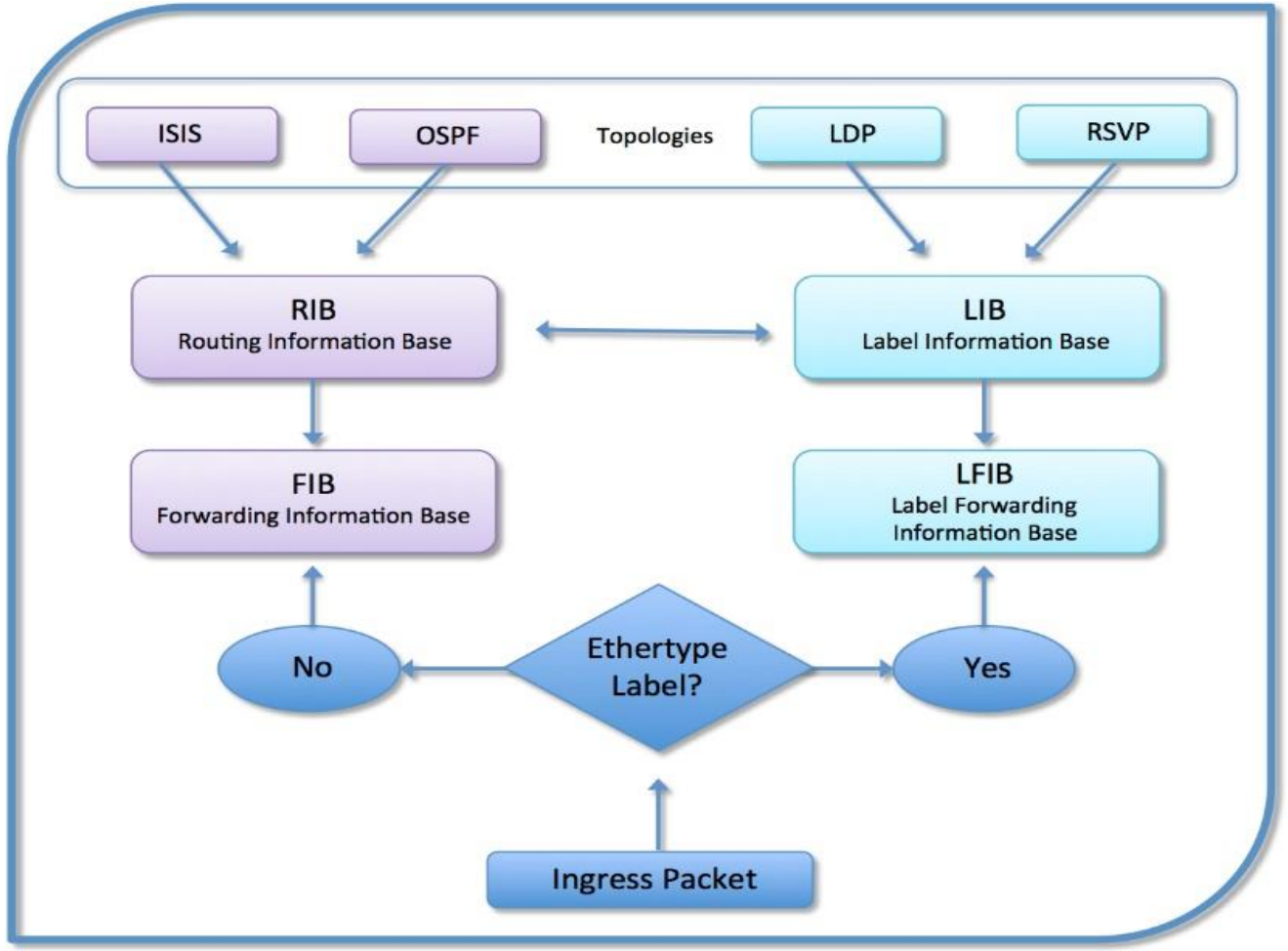
RIB / FIB / LIB / LFIB:

- **La LFIB (Label Forwarding Information Base)**

```
P1#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     4.4.4.4/32       1597       Fa0/1       10.0.24.4
17     17          3.3.3.3/32       0          Fa0/1       10.0.24.4
       18          3.3.3.3/32       0          Fa0/0       10.0.12.1
18     Pop tag     1.1.1.1/32       2353       Fa0/0       10.0.12.1
19     Pop tag     10.0.34.0/24     0          Fa0/1       10.0.24.4
20     Pop tag     10.0.13.0/24     0          Fa0/0       10.0.12.1
```

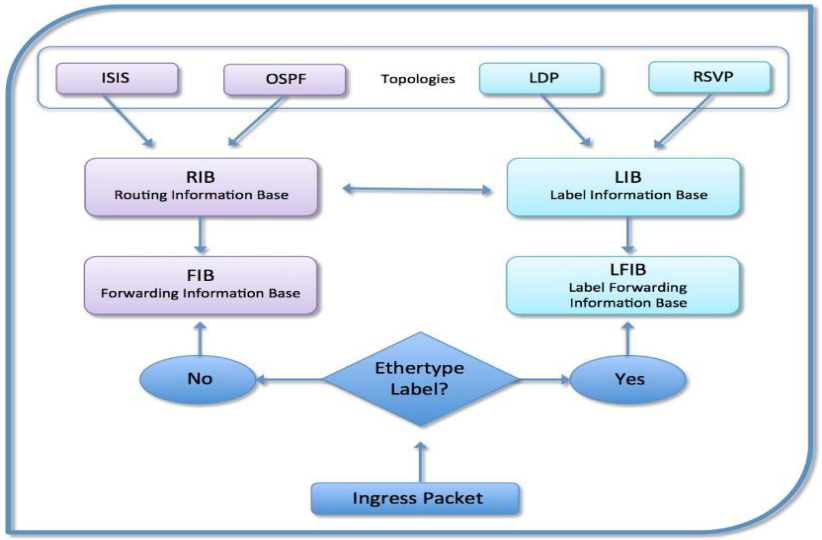
Ejemplo de inter-relación entre la table RIB, FIB, LIB y LFIB:

- **RIB -> show ip route.**
- **FIB -> show ip cef:**
- **LIB -> show mpls ldp bindings**
- **LFIB -> show mpls forwarding-table.**



Ejemplo de inter-relación entre la table RIB, FIB, LIB y LFIB:

- **RIB -> show ip route.**
- **FIB -> show ip cef:**
- **LIB -> show mpls ldp bindings**
- **LFIB -> show mpls forwarding-table.**



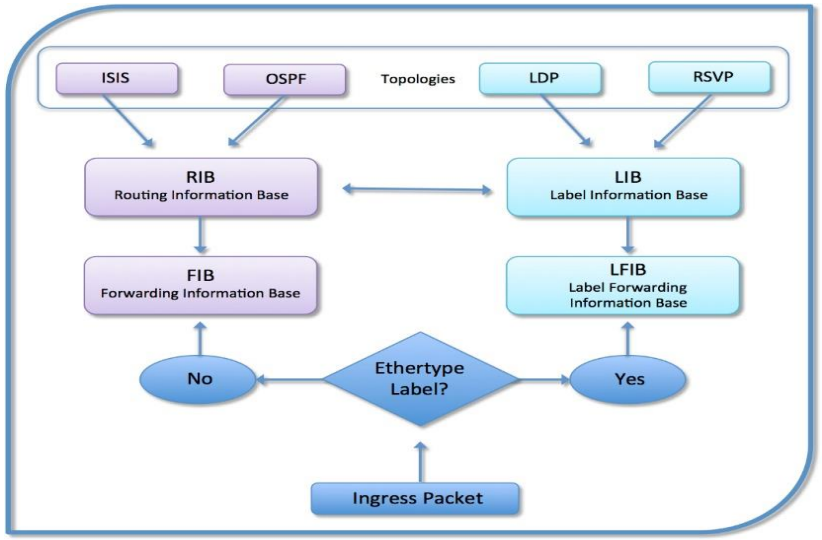

```
PE1#show ip route | include 10.3.3.0
D    10.3.3.0 [90/2812416] via 192.168.12.2, 00:04:33, Serial0/0/1
                                                                    (1)
PE1#show mpls ldp bindings 10.3.3.0 24
                                                                    (3)
tib entry: 10.3.3.0/24, rev 28
   local binding:  tag: 24
   remote binding: tsr: 2.2.2.2:0, tag: 22
   remote binding: tsr: 4.4.4.4:0, tag: 86

PE1#show mpls ldp neighbor                                          (4)
Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.60635 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 75/76; Downstream
        Up time: 00:35:20
        LDP discovery sources:
          Serial0/0/1, Src IP addr: 192.168.12.2
(2)     Addresses bound to peer LDP Ident:
          192.168.12.2  2.2.2.2  192.168.1.112  192.168.24.2
          192.168.23.2

Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 4.4.4.4.11711 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 26/30; Downstream
        Up time: 00:06:17
        LDP discovery sources:
          Serial0/1/1, Src IP addr: 192.168.14.4
        Addresses bound to peer LDP Ident:
          192.168.14.4  4.4.4.4  192.168.24.4  192.168.34.4
```

Ejemplo de inter-relación entre la table RIB, FIB, LIB y LFIB:

- **RIB -> show ip route.**
- **FIB -> show ip cef:**
- **LIB -> show mpls ldp bindings**
- **LFIB -> show mpls forwarding-table.**




```
! This next command shows the FIB entry, which includes the local tag (24), the
! tags (label) imposed, and outgoing interface.
PE1# show ip cef 10.3.3.0
10.3.3.0/24, version 65, epoch 0, cached adjacency to Serial0/0/1
0 packets, 0 bytes
  tag information set
    local tag: 24
    fast tag rewrite with Se0/0/1, point2point, tags imposed: {22}
  via 192.168.12.2, Serial0/0/1, 0 dependencies
    next hop 192.168.12.2, Serial0/0/1
    valid cached adjacency
    tag rewrite with Se0/0/1, point2point, tags imposed: {22}
! The next command lists the LFIB entry for 10.3.3.0/24, listing the same basic
! information—the local tag, the outgoing tag (label), and outgoing interface.
PE1# show mpls forwarding-table 10.3.3.0 24
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
24     22          10.3.3.0/24      0          Se0/0/1     point2point
```

MPLS Path (LSP) Setup (ejemplo detallado):

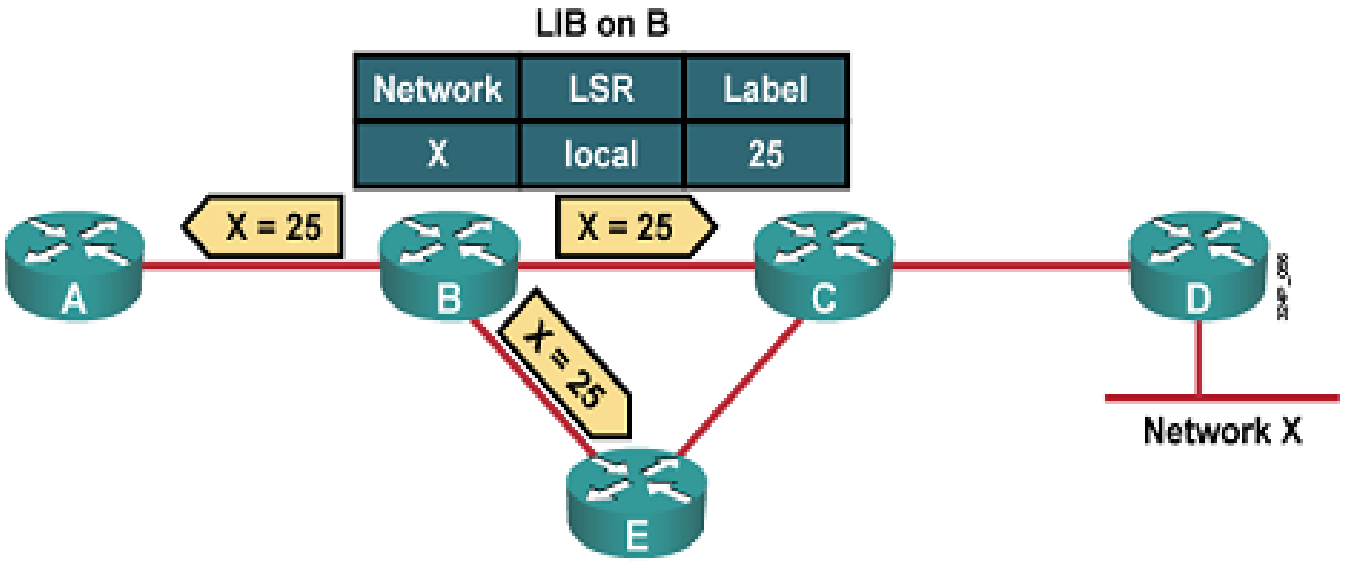
•Una vez el router tiene la tabla FIB completa por el protocolo de routing, a cada destino que aparece en dicha tabla, le asocia una etiqueta y la anuncia a sus vecinos.

•Esta asociación queda registrada en la tabla LIB en el plano de control.

•El plano de datos, que es el que realiza el trabajo de conmutación, lo que hace es mantener las tablas de FIB (para enrutar los paquetes de red directamente) y la tabla LFIB (para conmutar las tramas MPLS utilizando las etiquetas y reenviar la trama a la interfaz de salida correspondiente).

•De forma simplificada en las dos siguientes figuras se explica el funcionamiento del MPLS utilizando las tablas LIB, LFIB y FIB.

MPLS Path (LSP) Setup (ejemplo detallado):



MPLS Path (LSP) Setup (ejemplo detallado):

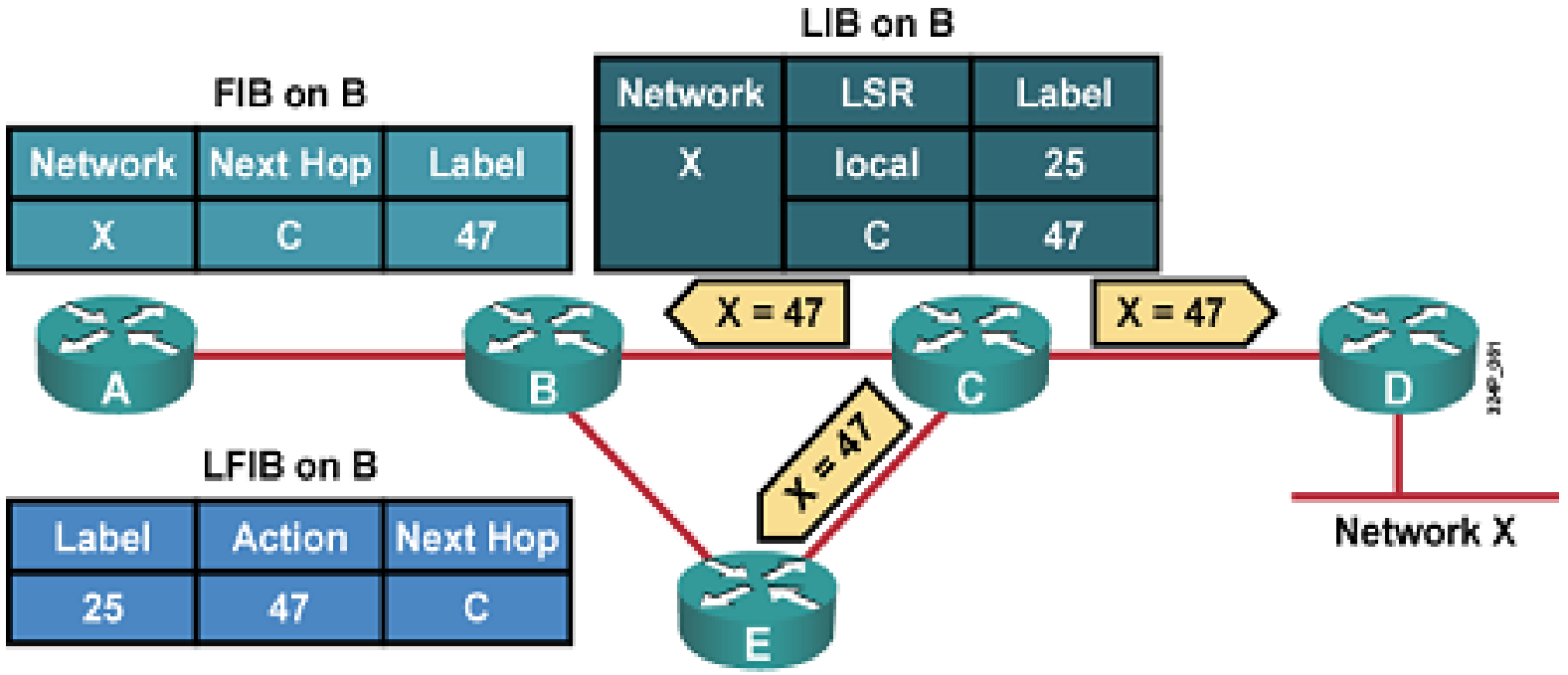
•En la figura anterior se observa que la red X (network X) es anunciada por el router D y el router B la tiene en su tabla de rutas.

•Para ese destino (red X), el router B elige una etiqueta, en concreto la 25 y envía su decisión a los routers vecinos A, E y C respectivamente.

•La asociación realizada queda registrada en la tabla LIB del router B.

•Ahora, cuando el router A tenga que enviar a la red X, el router A encapsulará el paquete dirigido a X en una trama MPLS con etiqueta 25, dado que B sabe qué hacer con dicha etiqueta.

MPLS Path (LSP) Setup (ejemplo detallado):

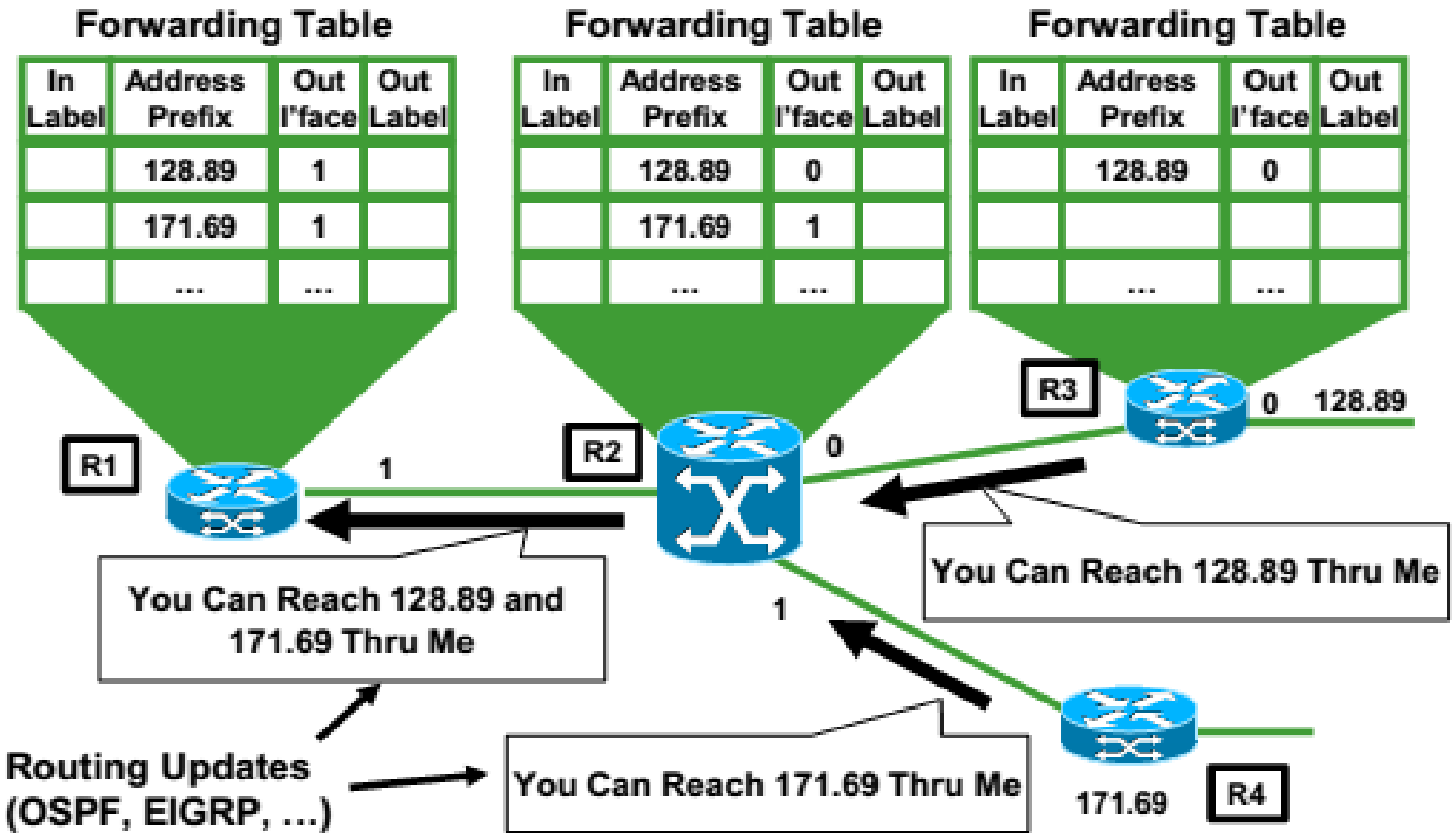


MPLS Path (LSP) Setup (ejemplo detallado):

- Como se observa en la figura anterior:
  - Una vez que tenemos las tablas inicializadas, FIB, LIB y LFIB en el router B, cuando llegue un paquete del router A con etiqueta 25:
    - El router B sabe que tiene que cambiar la etiqueta a 47 consultando la tabla LFIB y conmutar:
      - Es decir sacarla por la interfaz que conecta con el router C.

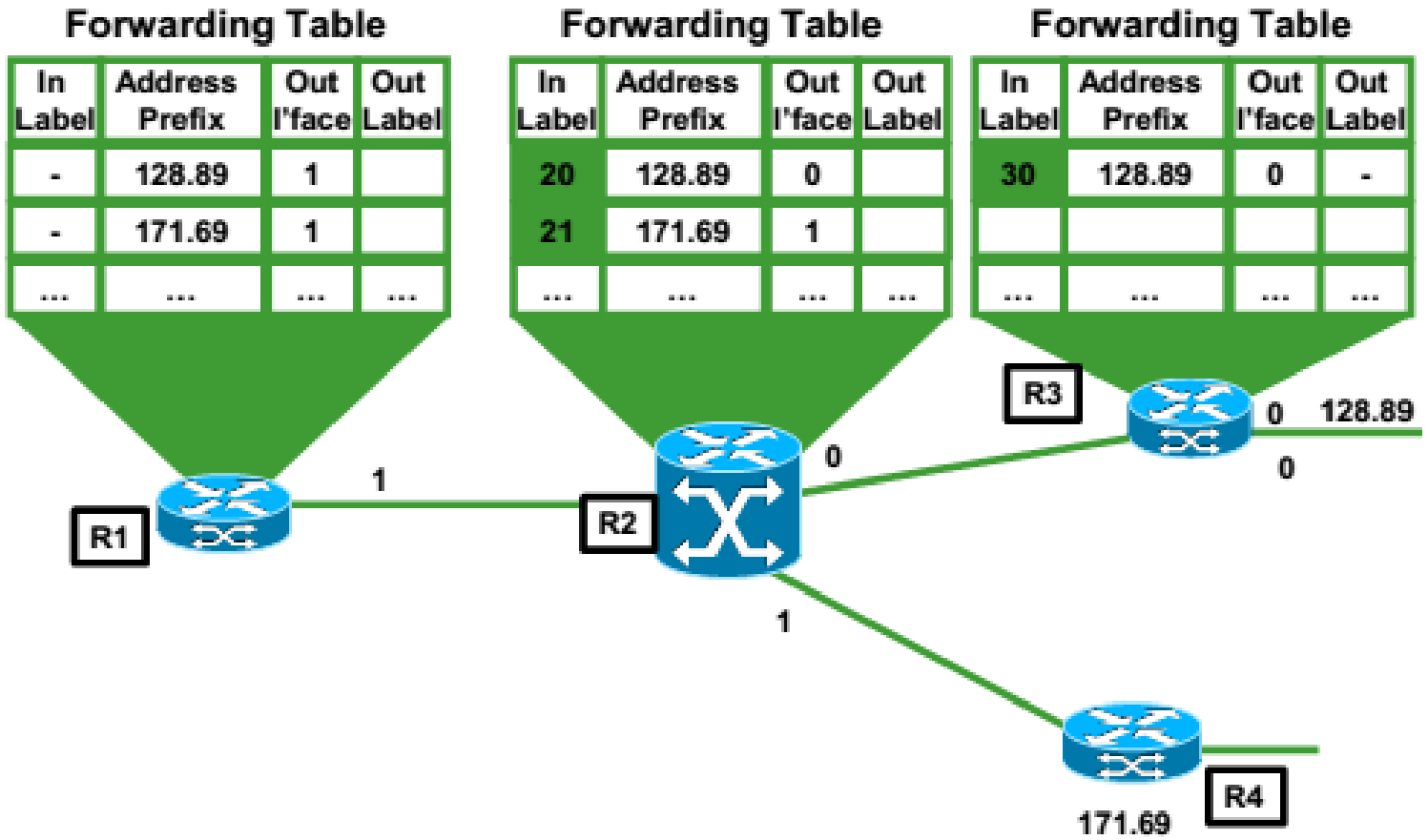
MPLS Path (LSP) Setup:

- **Paso 1: Convergencia del routeo IP / Establecimiento de conectividad IP**



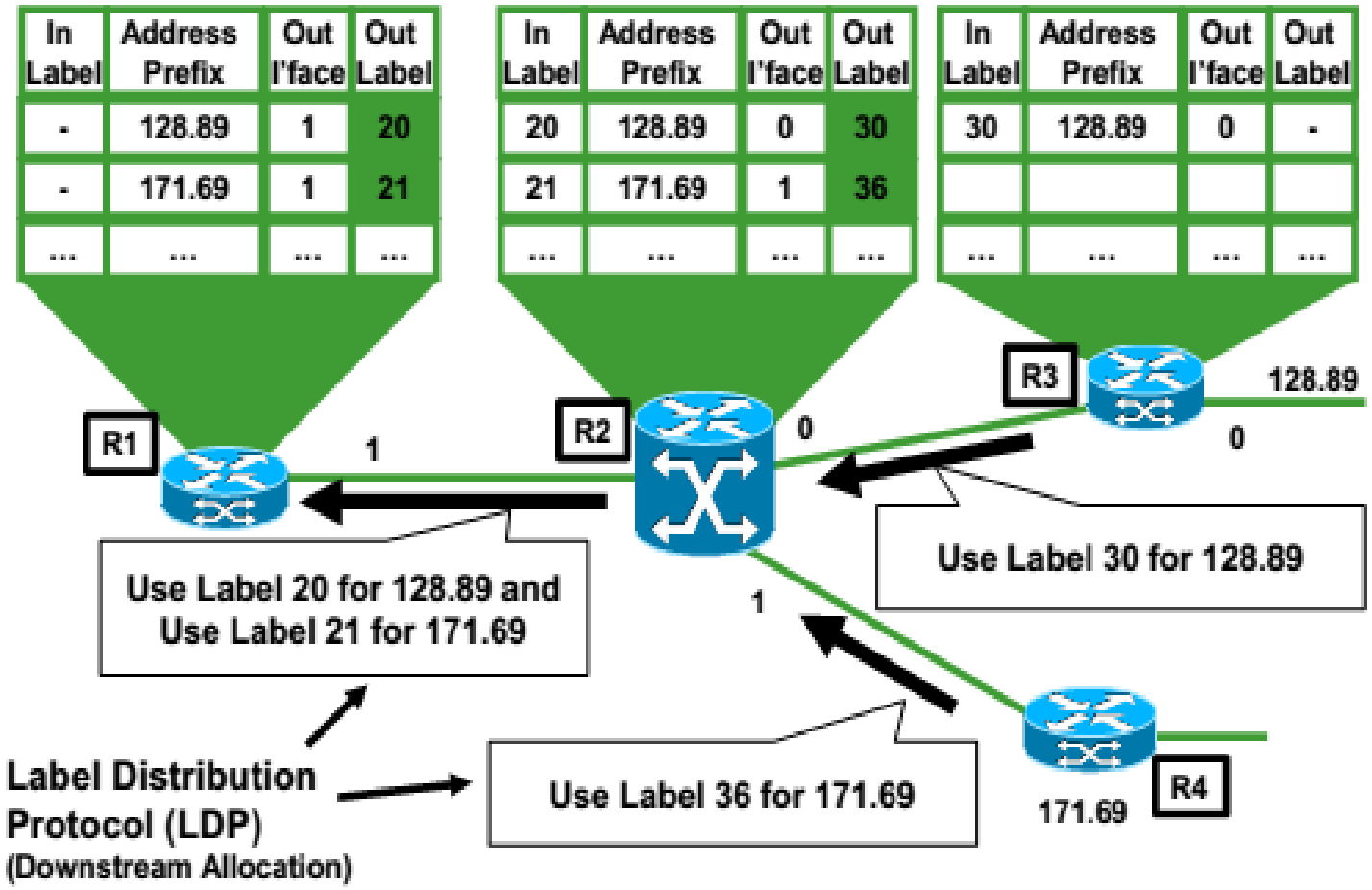
MPLS Path (LSP) Setup:

•Paso 2A: Asignación de etiquetas locales. Cada nodo MPLS asigna una etiqueta local a cada entrada/prefijo en su tabla de ruteo local (in label).



MPLS Path (LSP) Setup:

•**Paso 2B: Asignación de etiquetas remotas. El mapeo local de etiquetas se envía a todos los nodos conectados. Estos labels recibidos se agregan a la tabla (out label)**

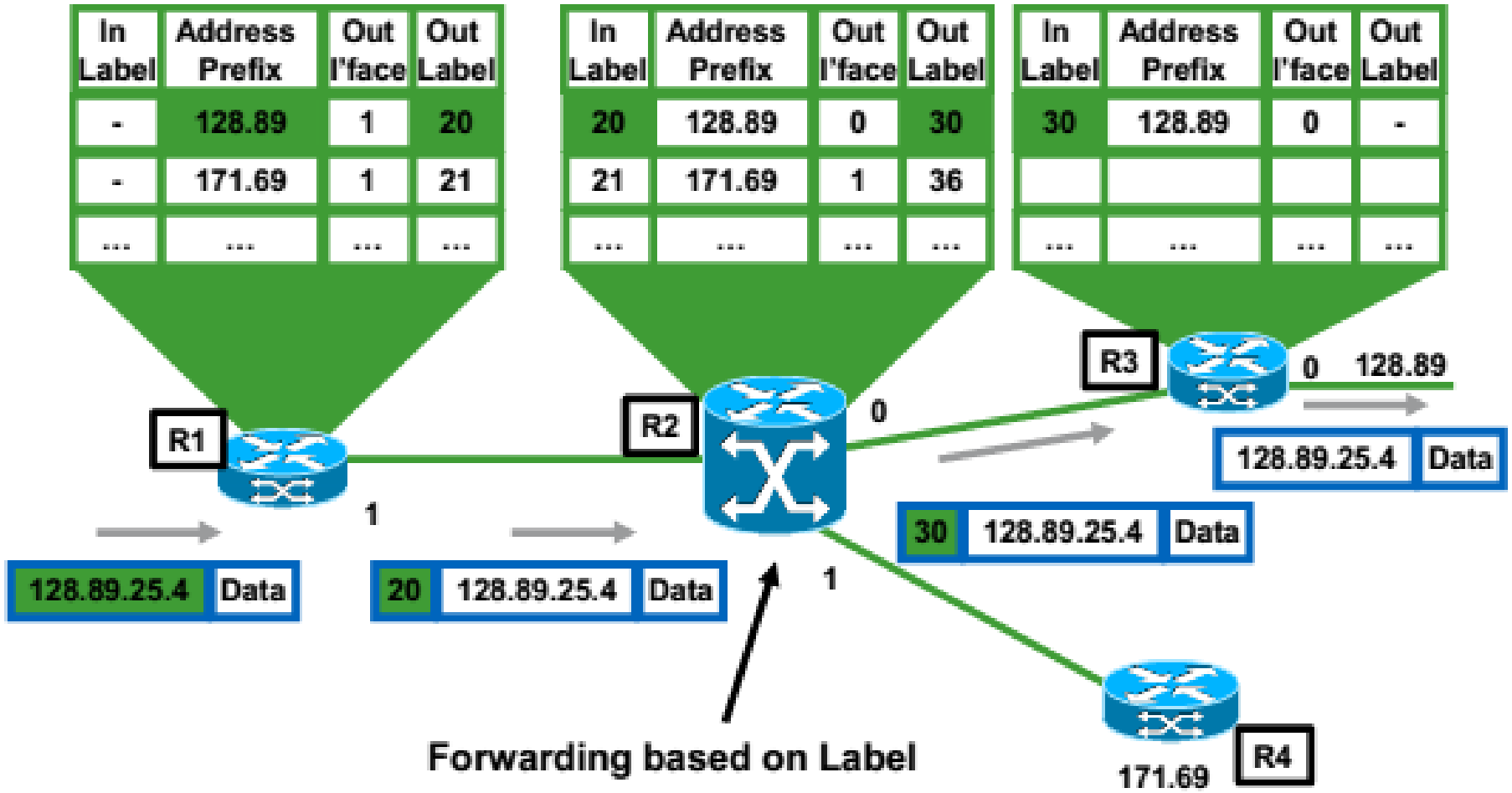


MPLS Path (LSP) Setup:

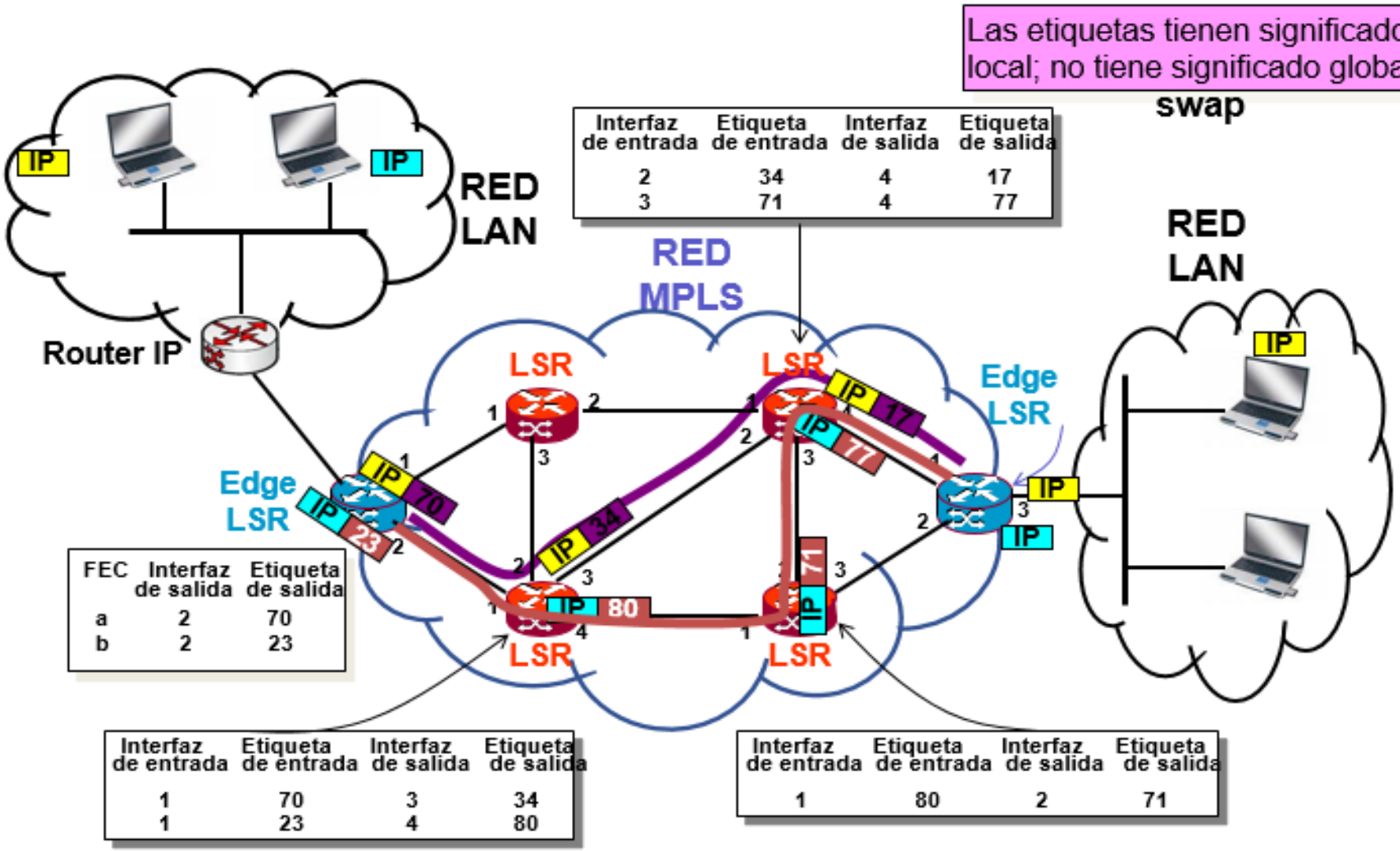
- **Paso 3 – Forwarding utilizando etiquetas.**
- **Los nodos de ingreso PE agregan la etiqueta al paquete (push)**
- **Los nodos downstream utilizan las etiquetas para tomar una decisión de forwading e intercambio de etiqueta (swap). Esto también determina la interfaz y la etiqueta de salida.**
- **Los nodos de egreso PE, remueven la etiqueta del paquete (pop) y forwardean el paquete original.**

MPLS Path (LSP) Setup:

- **Paso 3 – Forwarding utilizando etiquetas.**



MPLS Path (LSP) Setup con 2 FEC:



Virtual Routing and Forwarding (VRF):

- Es una instancia virtual de ruteo.

- Separada de la instancia global de ruteo en el dispositivo.

- Permite que **múltiples instancias de una tabla de ruteo coexistan** dentro de un mismo router al mismo tiempo.

- Entre otros beneficios, tener una VRF nos permite la **duplicación (solapamiento) de direcciones IP entre diferentes clientes**, ya que las rutas se procesas basadas en las etiquetas.

Virtual Routing and Forwarding (VRF):

- Cuando activamos una nueva instancia o VRF:

  el router puede y debe ejecutar sus propios procesos de routing como ser BGP, OSPF, ISIS o static.

- También debemos indicar en cada interface a que VRF queremos que pertenezca.

- Podemos decir que *los VRF son a la capa 3, lo que las vlans son a la capa 2.*

Virtual Routing and Forwarding (VRF):

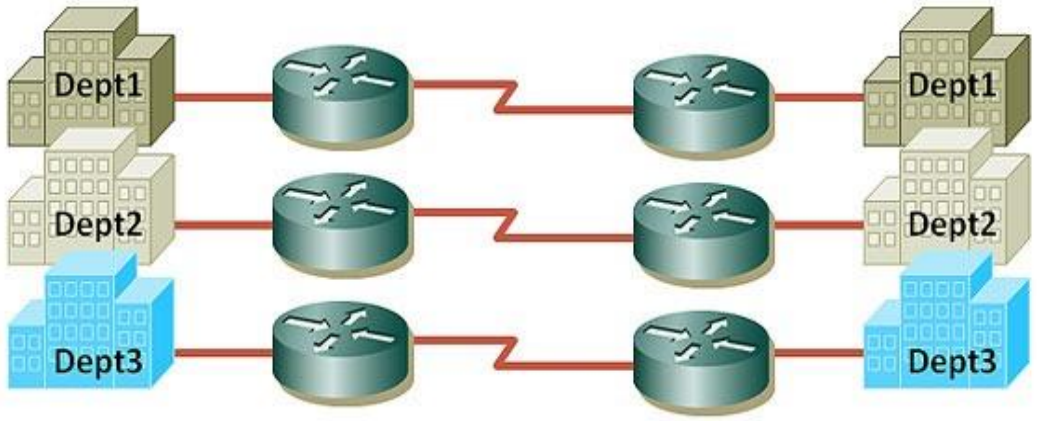
- A menos que se hayan aplicado políticas de importación/exportación**, las rutas** (y por ende los paquetes) **no podrán pasar de un VRF a otro**

- Esto de manera similar a lo que ocurre en una VLAN.

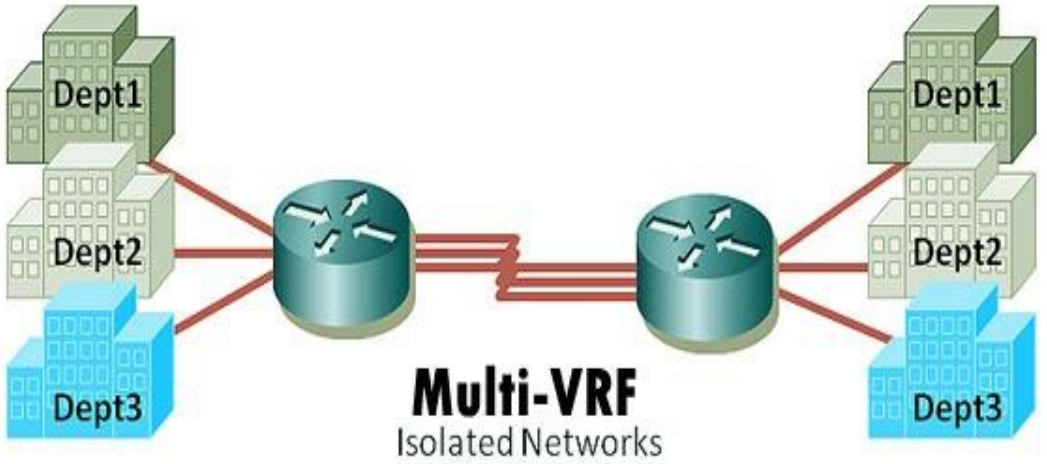
- Es decir, los paquetes que ingresan en un router en el VRF A solo podrán alcanzar rutas de la tabla de ruteo de este VRF A.

- En sintonía a las VLANs, las **VRF solo tienen significancia local en el router**.

Virtual Routing and Forwarding (VRF):



Multiple Routers
Isolated Networks



Virtual Routing and Forwarding (VRF):

- Las VRFs no son una característica propia de MPLS.
- La implementación más sencilla de una VRF es la del tipo **VRF lite.**
  - Cada router dentro de la red participa dentro del entorno de ruteo virtual de una manera basada en pares.
  - Es sencilla de desplegar y apropiada para pequeñas y medianas redes.
  - No son escalables, ya que se requieren que sean implementadas en cada router, incluidos los intermedios en la red.

Virtual Routing and Forwarding (VRF):

- Para el caso de una red extensa, existe las **full VRF,** o VRF implementadas en MPLS L3 VPN.
  - Solo debemos configurar o terminar las VRFs en los routers PE.
  - El core de la red no necesita conocer sobre las VRF y esto la hace escalable y altamente extensibles.
- Pero como entonces interconectamos estas VRFs?
- Para esto se desarrolló **Multiprotocol BGP (MP-BGP or BGP-MP)** que se utiliza únicamente para intercambiar rutas entre diferentes VRFs.

Virtual Routing and Forwarding (VRF):

- Estas rutas son importadas dentro de BGP con un “tag” propio para el intercambio.

- Es importante destacar que los routers de core MPLS pueden reenviar el trafico desconociendo la configuración de las VRF.

- Estos tags que utilizaremos para importar o exportar rutas se denominan “route targets”.

RD (Route Distinguisher):

•MPLS nos da la posibilidad de utilizar el mismo backbone para distintos clientes o servicios manteniendo una separación entre ellos.

•Para esto, le asignamos a cada cliente su propia VRF, de manera que esa superposición de subredes quede aislada dentro de su respectivo dominio de routing.

•Esto funciona correctamente dentro de un mismo router, pero cuando interconectamos varios routers con varios VRF dentro de una red, necesitamos de alguna forma poder administrar o tener un seguimiento sobre a qué cliente pertenece cada paquete perteneciente a la misma subred.

•**Para esto utilizamos los route distinguishers.**

RD (Route Distinguisher):

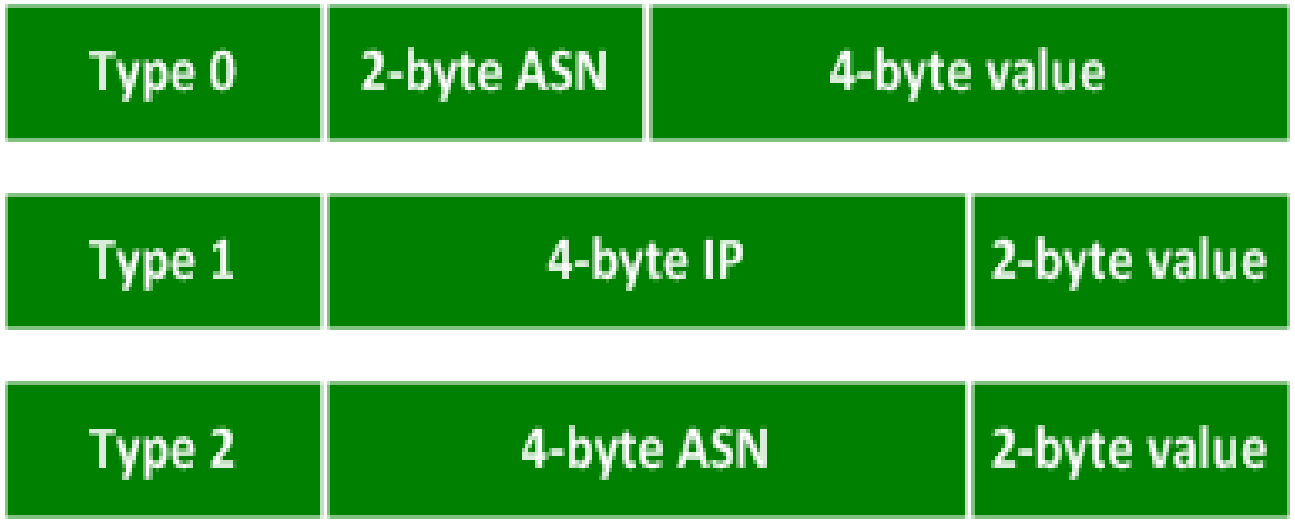
- Estos ***distinguen un set de rutas (de un VRF) de otro***.

- Es un **número único que se antepone a cada ruta** dentro de un VRF para identificarla como perteneciente a un VRF o cliente particular.

- Estos RD son transportados con la ruta a lo largo vía MP-BGP cuando se intercambian rutas VPN con otros routers PE.

RD (Route Distinguisher):

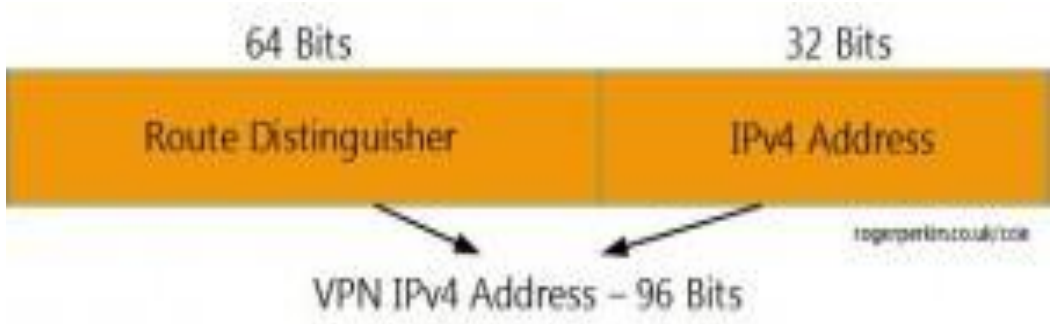
- El RD tiene **64 bits de longitud** que comprenden tres campos:
  - el campo tipo (dos bytes),
  - El campo administrador
  - El campo valor.
  - Existen actualmente definidos tres formatos de RD que pueden ser utilizados



RD (Route Distinguisher):

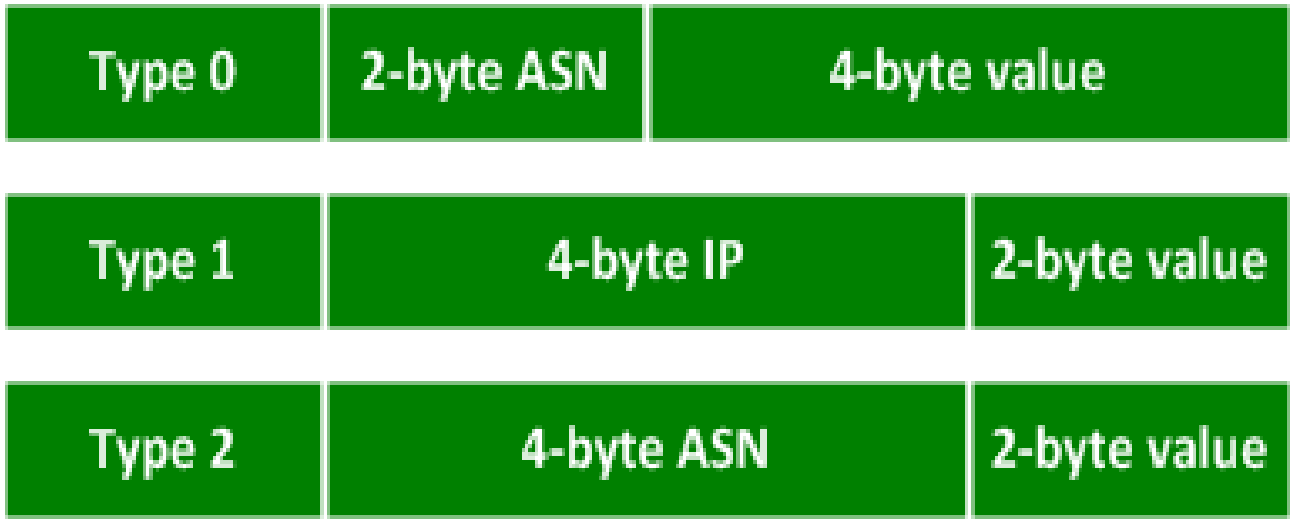
•Utilizando el Route Distinguisher, entonces **transformamos la dirección IP de 32 bits en una dirección de 96 bits, única en la red.**

•De esta forma los routers Provider Edge (PEs) en MPLS no anuncian redes de 32 bits vía mBGP, sino un prefijo de 96 bits.



RD (Route Distinguisher):

•Por ejemplo, una ruta para la subred 192.168.2.0/24 en el VRF del Site_B finalmente se publica como 65535:20:192.168.2.0./24, donde 655335 es el número de AS y el 20 es el site ID.



RT (Route-Target):

- Es un campo de **8 bytes (64 bits)** que es parte de los BGP extended Communities Attribute definidos en la RFC 4360.

- Mediante este campo, ***definimos que prefijos serán importados y exportados en los routers PE.***

- Cuando exportamos prefijos en un VRF, agregamos a estos una comunidad de Route-Target.

- De esta forma cuando el PE en un sitio remoto tiene que importar prefijos en el VRF, puede identificarlos fácilmente, escogiendo que prefijos quiere importar basándose en este valor.

RT (Route-Target):

•El route target tiene formato similar al route distinguisher, pero sirve para propósitos diferentes.

•**Que el route target pueda tener el mismo formato que el route Distinguisher, no significa que exista una relación directa entre estos dos.**

•Mientras que:

- **los RD son utilizados** para mantener la identificación univoca de rutas similares en diferentes VRFs.
- **los RT pueden ser utilizados** para compartir rutas entre estos VRFs, es decir podemos utilizar los RT para controlar que rutas importamos y exportamos entre los VRFs.

RT (Route-Target):

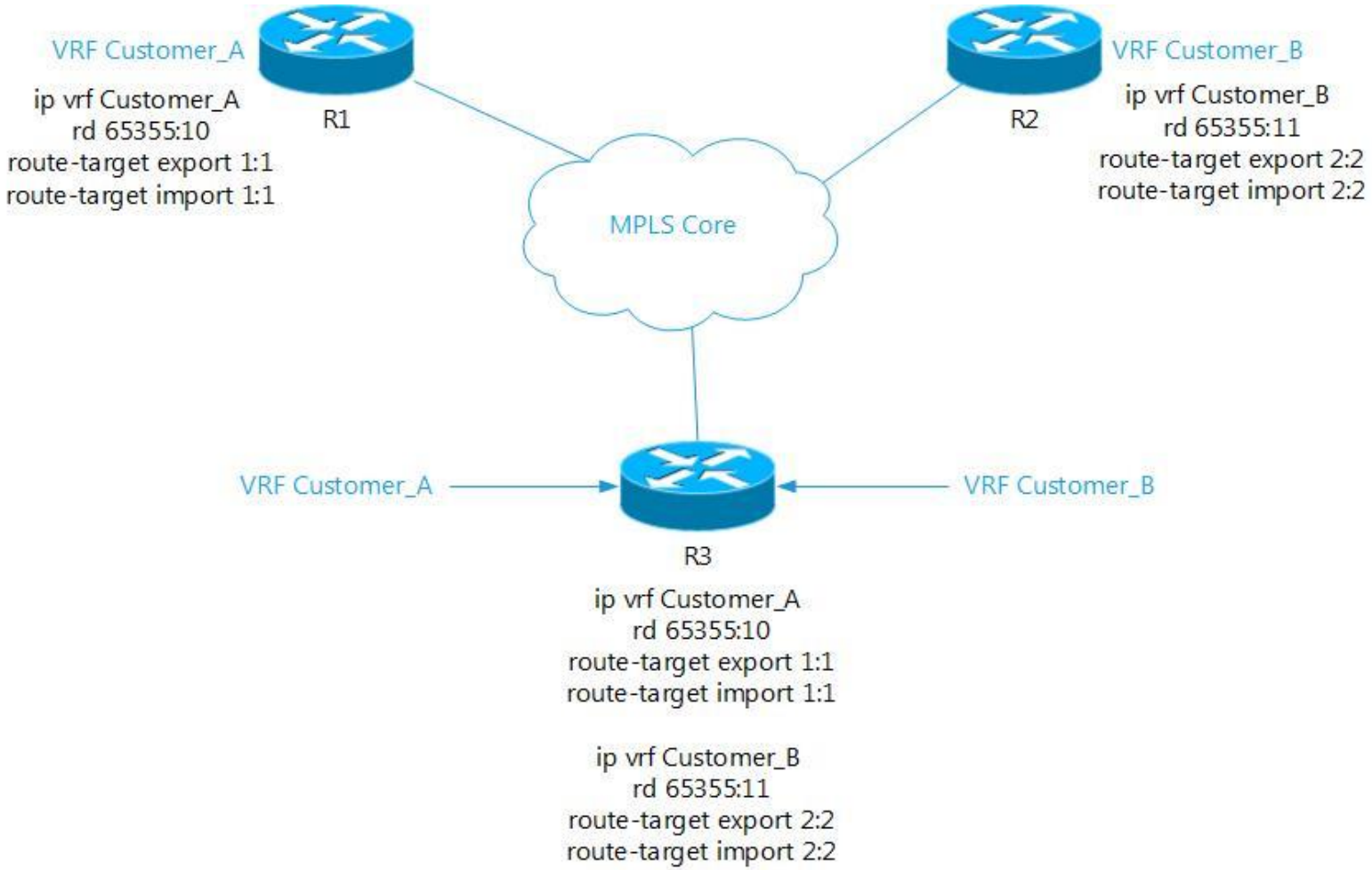
- Imaginemos que:
  - Utilizando el mismo RD para todos los sitios del cliente A,
  - No deseamos que todos las sedes se puedan conectar a todos los sedes.
  - Podríamos tener una configuración en donde el Site-2 tenga visibilidad de los prefijos de Site-1 pero no para Site-3.
  - Igualmente para Site-3, podríamos hacer que tuviera visibilidad de Site-1 pero no de Site-2.

RT (Route-Target):

- Ejemplo:
  - El R3 tiene 2 VRFs configurados, el vrf Customer_A y el vrf Customer_B
  - En el router R3 queremos exportar e importar prefijos de los vrf Customer_A y Customer_B.
  - Sin embargo, en el R1 solamente queremos importar y exportar prefijos para el vrf Customer_A y en el R2 solamente queremos importar y exportar prefijos para el vrf Customer_B.
- De esta forma, la configuración seria la siguiente:

RT (Route-Target):

- Ejemplo:



¿dudas?