Ingeniería de tráfico

Aplicaciones de MPLS: **calidad de servicio (MPLS-QoS)**.

- Soporte DiffServ en MPLS.
- Soporte IntServ en MPLS.

Aplicaciones de MPLS: **protección y restauración (MPLS-FRR)**.

- Métodos de protección. *Fast Re Route*.
- Protección “salto a salto”. Tipos y ejemplos.

MPLS: calidad de servicio.

- Modelo DiffServ (DS).
  - Modelo/solución para QoS en redes IP mediante clasificación del tráfico en un nº pequeño de clases.
  - Se basa en asignar recursos por clases de tráfico.
  - Clases de tráfico identificadas mediante el valor DSCP de cabecera IP para proveer determinado PHB.
  - Provee garantía QoS **no estricta** por clase de tráfico, funciona bien si la red no está congestionada.
- MPLS.
  - La lógica MPLS no es consciente del paquete IP (cabecera y cuerpo), no procesa la cabecera IP.
  - La lógica MPLS-TE permite establecer LSPs en base a restricciones y reservas de recursos.
- Preguntas:
  - ¿Cómo combinar DiffServ y MPLS si éste no es consciente de las clases de tráfico DiffServ, si el valor DSCP no es "visible" a lógica MPLS?
  - ¿Cómo visualizar el valor DSCP en la cabecera MPLS para que éste sea consciente de DiffServ?
- Respuesta:
  - Visualizar, de alguna manera, el valor DSCP en la cabecera MPLS. **Lo que posibilita**:
    - Redefinir lógica MPLS-TE para reservas de recursos sobre la base de clases de tráfico.
    - Combinar DiffServ y MPLS-TE para obtener garantía QoS **estricta** por clase de tráfico.

MPLS: calidad de servicio.

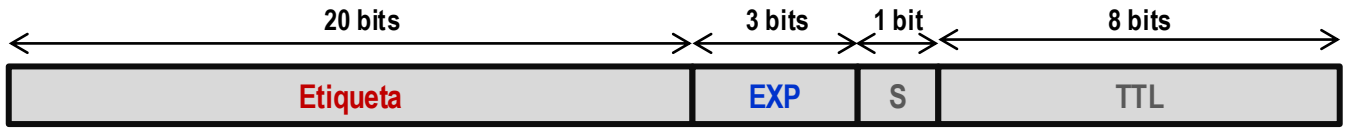
- Soporte DiffServ en MPLS.
  - Requiere **inferir el PHB** de cada paquete a partir de la cabecera MPLS.
    - Por cuanto los LSR toman las decisiones para reenvío de paquetes a partir de la cabecera MPLS.
  - ¿Cómo "visualizar" el valor DSCP en la cabecera MPLS?
    La RFC 2732 especifica dos soluciones.

  - **Solución E-LSP** (*PHB inferred **from the EXP***).
    - Infiere el PHB a partir del campo EXP de la cabecera MPLS.
    - Plantea utilizar el valor EXP de la *shim header* para contener la información DiffServ.
    - Requiere ***mapping*** entre el valor **DSCP** de cabecera IP y el valor **EXP** de la cabecera MPLS.
    - Vincula PHB del paquete y valor EXP de cabecera MPLS con limitaciones: DSCP **6** bits, EXP **3** bits.

  - **Solución L-LSP** (*PHB inferred **from the Label***).
    - Infiere el PHB a partir del valor "etiqueta" o de los valores "etiqueta" y "EXP" de la cabecera MPLS.
    - Conlleva a LSPs separados a partir de los PHB codificados en el campo DSCP de la cabecera IP.

MPLS: calidad de servicio.

- **Solución E-LSP (*EXP inferred*).**
  - LSP cuyo PHB se infiere a partir del valor EXP de la cabecera MPLS.
  - Se basa en el *mapping* directo entre los valores **DSCP** y **EXP**.
    - Valor EXP determina el PHB que recibirá el paquete.
    - Aplicable hasta ocho PHB diferentes.
  - *Mapping* entre valor PHB y valor EXP:
    - Mediante configuración en cada nodo.
    - Procedimiento automatizado o manual (p.e, vía sistema de gestión de red).
    - **No se indica/señaliza el PHB cuando se establece el LSP.**
  - Valor "etiqueta" solo determina dónde reenviar el paquete, no indica cómo tratarlo en cada nodo.

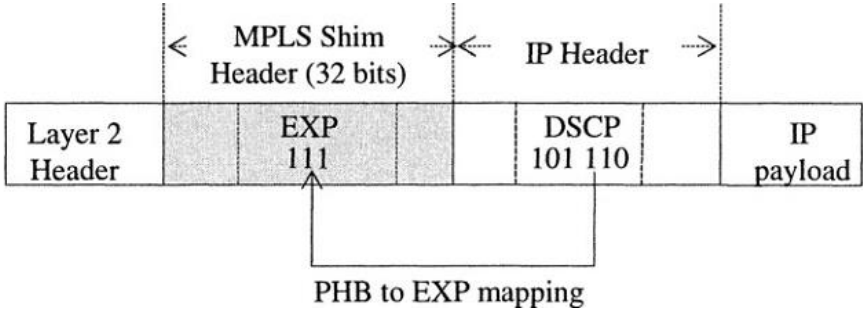


MPLS: calidad de servicio.

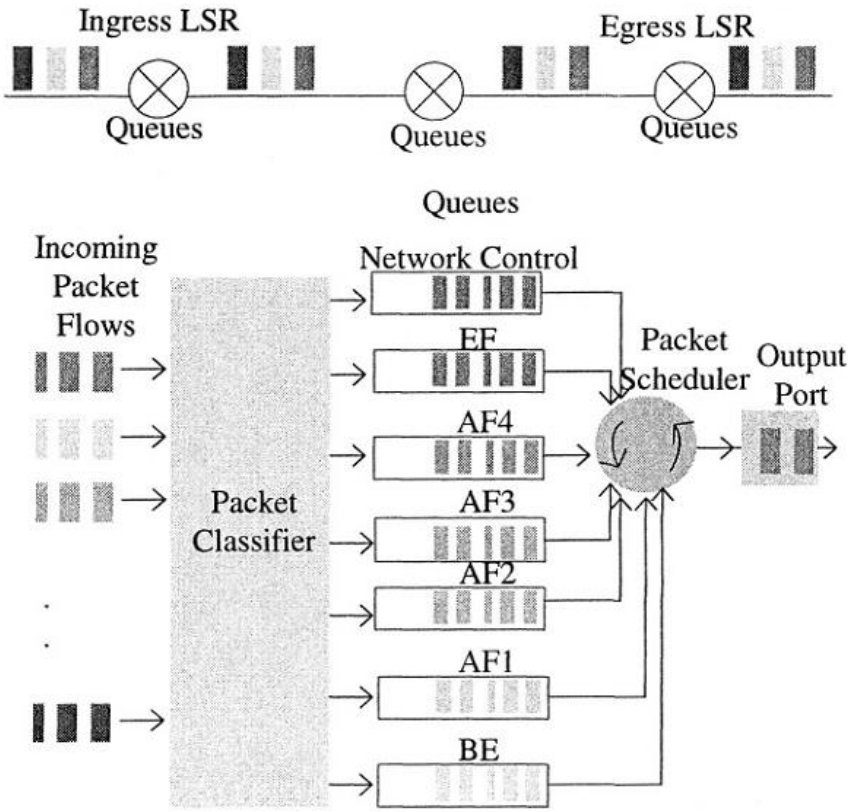
Solución E-LSP (*EXP inferred*) (II).

Ejemplos de *mapping* de valores PHB a valores EXP.

PHB class	PHB subclass	DSCP	EXP
EF		101110	111
AF4	AF41	100010	110
	AF42	100100	
	AF43	100110	
AF3	AF31	011010	101
	AF32	011100	
	AF33	011110	
AF2	AF21	010010	100
	AF22	010100	
	AF23	010110	
AF1	AF11	001010	011
	AF12	001100	
	AF13	001110	
BE		000000	010



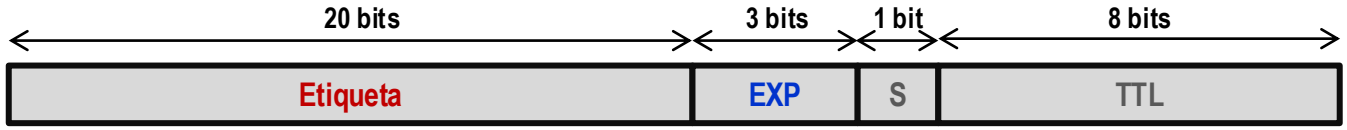
Ejemplo de E-LSP con siete PHB diferentes.



Fuente: Kum I. Park, *QoS IN PACKET NETWORKS*, Springer Science + Business Media, Inc, 2005

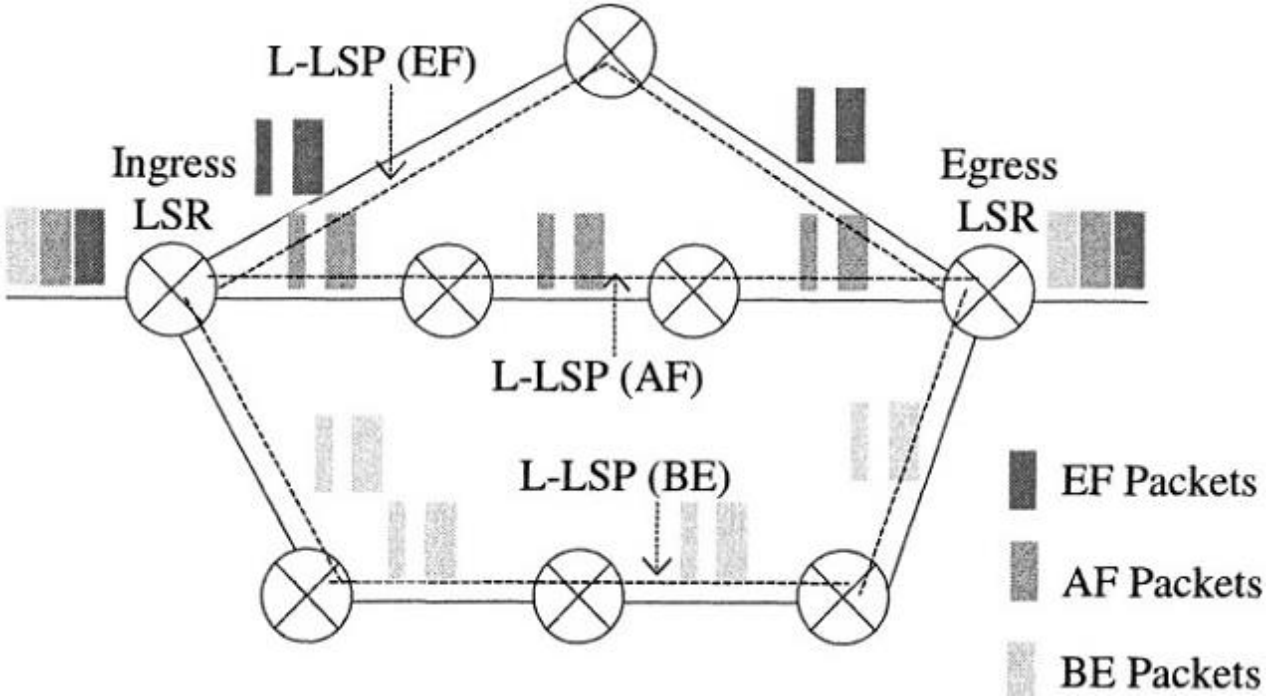
MPLS: calidad de servicio.

- **Solución L-LSP (*Label inferred*).**
  - PHB se infiere a partir del valor "etiqueta" o de los valores "etiqueta" y "EXP".
  - PHB "contenido" en el valor "etiqueta" o en los valores "etiqueta" y "EXP".
    - Etiqueta: determina dónde reenviar el paquete y la clase (planificación) del paquete.
    - EXP: determina la prioridad de descarte del paquete.
    - **Requiere indicar/señalizar el PHB cuando se establece el LSP.**
    - Aplicable a ocho o más PHB.
  - Un L-LSP puede soportar uno o varios PHB que requieran igual planificación (clase) y diferentes prioridades de descarte. P.e, para un grupo de clases **AF_{xy}**:
    - "**x**" indica la clase (mismo tratamiento de planificación).
    - "**y**" indica la prioridad de descarte dentro de una clase, tratamiento diferenciado dentro de una clase.



MPLS: calidad de servicio.

- Solución L-LSP (*Label inferred*) (II).
  - Ejemplo de tres L-LSP, cada uno con PHB diferente.
  - L-LSP (AF) para paquetes que pertenecen a la misma clase (ídem planificación) pero con igual o diferente prioridad de descarte (igual o diferente PHB).



Fuente: Kum I. Park, *QoS IN PACKET NETWORKS*, Springer Science + Business Media, Inc, 2005

MPLS: calidad de servicio.

- Comparativa: E-LSP *versus* L-LSP.

E-LSP	L-LSP
PHB determinado por los bits EXP.	PHB determinado por los bits de la etiqueta, o de manera conjunta por los bits etiqueta y EXP.
Hasta ocho PHB diferentes por LSP.	Soporta cualquier número de PHB: • Un único PHB por LSP, o… • Varios PHB por LSP con el mismo régimen de planificación y diferentes prioridades de descarte.
La etiqueta sólo se utiliza para el reenvío de paquetes.	La etiqueta se utiliza para el reenvío de paquetes y para el trabajo de los planificadores.
No requiere señalización para notificar el PHB.	Requiere señalización para notificar el PHB cuando se establece el LSP.

E-LSP y L-LSP pueden usarse conjuntamente cuando se requieren más PHB.

MPLS: calidad de servicio.

- Soporte **IntServ** en MPLS.
  - Modelo IntServ.
    - Modelo para QoS en redes IP mediante reserva previa de recursos.
    - Reserva-asignación de recursos por flujo.
    - Provee garantía QoS **estricta** por flujo.
  - IntServ con MPLS.
    - Mediante asociación de flujos IntServ a etiquetas.
    - Mediante asociación de diferentes flujos IntServ a diferentes LSP.
  - Con protocolos CR-LDP o RSVP-TE se puede desarrollar simultáneamente:
    - Distribución de etiquetas para señalizar - establecer los LSP.
    - Reserva de recursos en los LSR durante el establecimiento de los LSP.
  - No es una solución escalable, requiere reservas por flujo (problemática intrínseca de IntServ).

MPLS: protección y restauración.

- Introducción.
  - La QoS se requiere no solo en condiciones normales de operación, sino también cuando se producen fallos en la red.
    - Cuestión más crítica para tráfico de tiempo real, no admite la retransmisión para recuperación.
    - Se necesitan mecanismos rápidos de protección y recuperación ante fallos en la red.
  - Recuperación rápida.
    - A menor tiempo de recuperación menor afectación sufrirán las aplicaciones.
    - Depende de la demora en detectar el fallo y la demora en reencaminar el tráfico.
    - Solución clásica en capa física: **enlaces en *standby*** que asumen la carga de enlaces activos cuando éstos "caen".
      - P.e, sistemas APS (*Automatic Protection Switching*) en redes SONET/SDH → Rápida conmutación en **menos de 50 ms,** apenas se nota en la capa de aplicación.
      - Coste asociado: enlaces (ancho de banda) desocupados/ociosos además del *hardware* APS.
    - Solución MPLS: procedimiento denominado re encaminamiento rápido (*Fast ReRoute, FRR*).

MPLS: protección y restauración.

- ¿Qué método de protección utilizar?
  - Depende de las aplicaciones, según cuantía de pérdidas que admitan ante fallos de red.
    - Aplicaciones *real time* las más exigentes, algunas toleran pérdidas para más de 50 ms de fallo.
    - P.e, para llamadas telefónicas:
      - Pérdidas mayores a 300 ms se notan en una conversación.
      - Pérdidas de más de 2 s pueden producir desconexión de la llamada.
  - Ante esta flexibilidad podría pensarse en utilizar solo mecanismos IP para protección, pero...
    - Los mecanismos IP no satisfacen rápida detección ni rápida recuperación ante fallos de red.
    - El *routing* IP **no es una solución local** → Mayor tiempo para la detección y recuperación.
    - Para mayor rapidez con IP habría que aumentar la frecuencia de envío de información de *routing* entre *routers* → Más carga de tráfico para la red
  - **Con tecnología MPLS mediante el procedimiento *Fast ReRoute* (FRR).**
    - Basado en decisiones locales → Menor tiempo de recuperación ante fallos.

MPLS: protección y restauración.

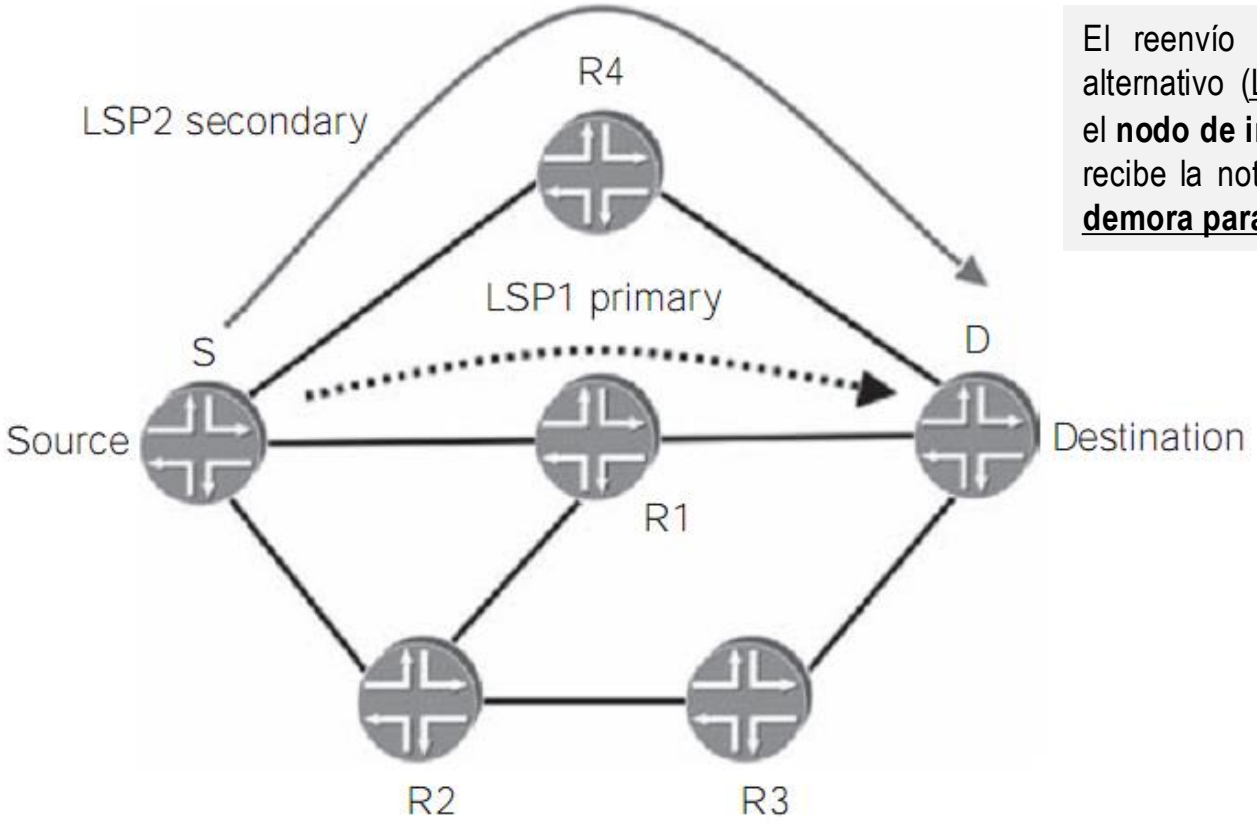
- MPLS FRR, *MPLS Fast ReRoute*.
  - Objetivo:
    - Proveer a los LSP garantías de protección similares a SONET/SDH con APS (menos de 50 ms).
  - Ventajas frente a sistemas APS en redes SONET/SDH.
    - No requiere *hardware* adicional y específico para protección y restauración.
    - No está limitado solo a **fallos de enlaces físicos**, también provee protección ante **fallos de nodos**.
  - En principio dos tipos de protección MPLS FRR.
    - Protección "**extremo a extremo**" (protección de trayecto).
    - Protección "**salto a salto**" (protección local). **Solución más utilizada**.

MPLS: protección y restauración.

- Protección extremo a extremo (protección de trayecto).
  - Mediante LSPs duplicados para lograr rapidez en la recuperación.
    - LSP primario asume el servicio en condiciones normales de operación.
    - LSP secundario (*backup*) asume la carga cuando el primario falla. Ocioso durante la operación normal.
    - El proveedor controla totalmente el trayecto de ambos LSP (principal ventaja).
  - Requiere:
    - Que ambos LSP (primario y secundario) estén establecidos a la vez.
      - Doble reserva de recursos y misma garantía QoS para cada LSP.
      - Puede conducir a la imposibilidad de establecer otros nuevos LSP por carencia de recursos.
    - Que ambos LSP sigan trayectos - rutas diferentes.
      - Coincidencia ninguna o mínima para mayor probabilidad de que LSP secundario esté OK si LSP primario falla.
      - Fácil de lograr dentro un mismo dominio MPLS, no así para LSPs multi dominios.
    - Notificar el fallo a la cabecera del LSP → **Mayor demora en la recuperación** (serio inconveniente).
      - Consecuencia del *routing* para LSP a partir de la fuente (requisito TE- MPLS).

MPLS: protección y restauración.

- Ejemplo de protección extremo a extremo (protección de trayecto).



El reenvío de tráfico por el trayecto alternativo (LSP secundario) lo controla el **nodo de ingreso** del LSP una vez que recibe la notificación del fallo → **Mayor demora para la recuperación**.

Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

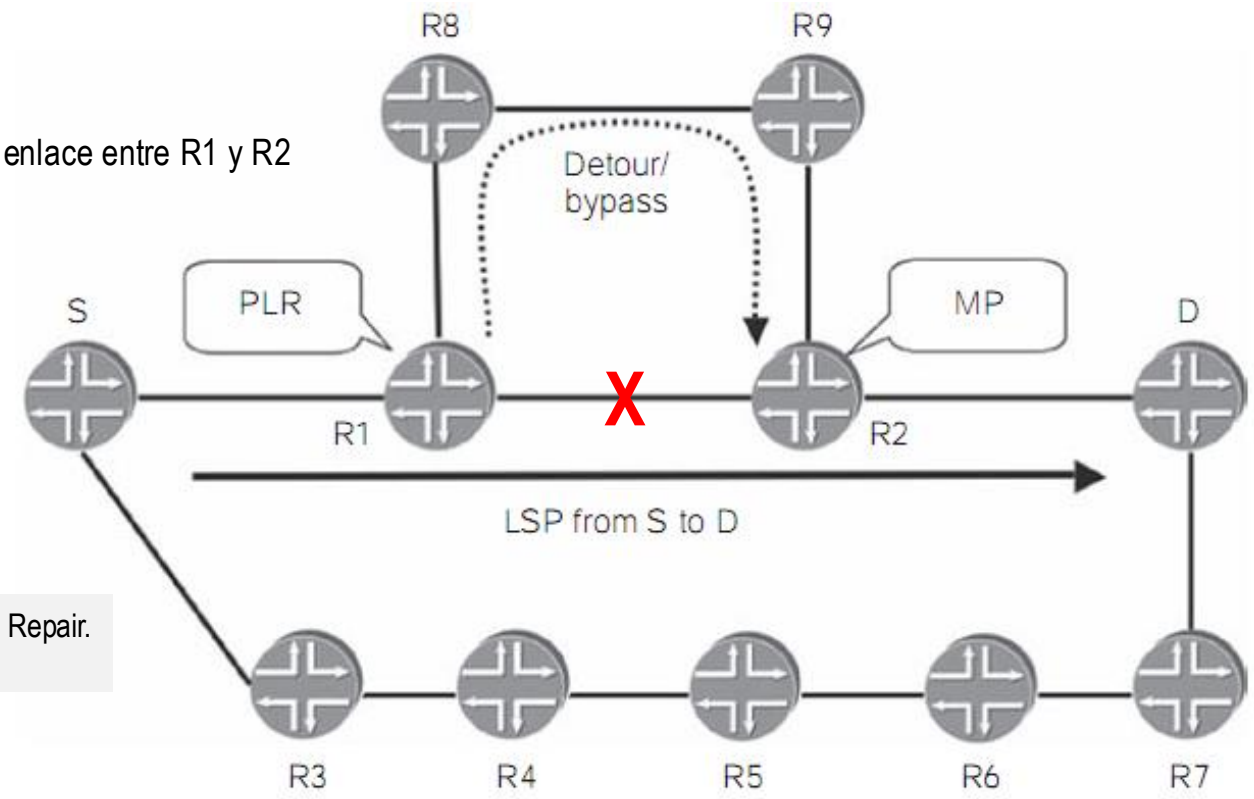
MPLS: protección y restauración.

- Protección salto a salto (protección local).
  - Intenta solventar los problemas de la protección extremo a extremo y lograr **mayor rapidez** en la recuperación.
  - Aplica la protección lo más cerca posible al punto de fallo.
  - Re encamina el tráfico a partir del lugar más cercano posible al punto de fallo.
    - No como la protección de trayecto (desde el LSR de ingreso con trayecto totalmente nuevo).
  - Propiedades atractivas.
    - Protección **más rápida** ya que se aplica cerca del punto de fallo.
    - Protege un recurso único, facilitando así las cosas.
    - No requiere señalizar a otros nodos para utilizar el trayecto alternativo ("desvío").
    - El reenvío por el trayecto alternativo lo realiza el **nodo *upstream* más cercano** al punto de fallo.
      - Determinado solo por el nodo ***upstream*** respecto al punto de fallo y señalizado **previamente**.
    - Una vez que un nodo *upstream* detecta el fallo:
      - **Reencamina el tráfico de inmediato**.
      - **Notifica/señaliza** (con protocolo de distribución de etiquetas) **al LSR de ingreso** para que calcule el nuevo LSP.

MPLS: protección y restauración.

- Ejemplo de protección salto a salto (protección local).

Supuesto: falla el enlace entre R1 y R2



PLR: Point of Local Repair.
MP: Merge Point.

Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

- Funcionamiento de la protección salto a salto (protección local).
  - **Nodo PLR** (*Point of Local Repair*) detecta el fallo, entonces:
    - De inmediato utiliza trayecto de protección local (antes definido) hasta que se establezca el nuevo LSP.
    - Notifica - señaliza al nodo origen/fuente del LSP (LSR de ingreso) para que calcule el nuevo LSP.
  - **Nodo origen del LSP**:
    - Calcula la ruta para el nuevo LSP cuando recibe mensaje de notificación - señalización.
    - Aplica el principio *make-before-break* → Establece nuevo LSP antes de eliminar el anterior.
    - Nuevo LSP puede o no coincidir parcialmente con el viejo LSP, puede incluir el enlace de protección.
  - Una vez establecido el nuevo LSP:
    - Se reenvía el tráfico a su través aunque ya esté recuperado el enlace o nodo antes caído.
    - Se elimina el viejo LSP incluyendo el trayecto de protección.

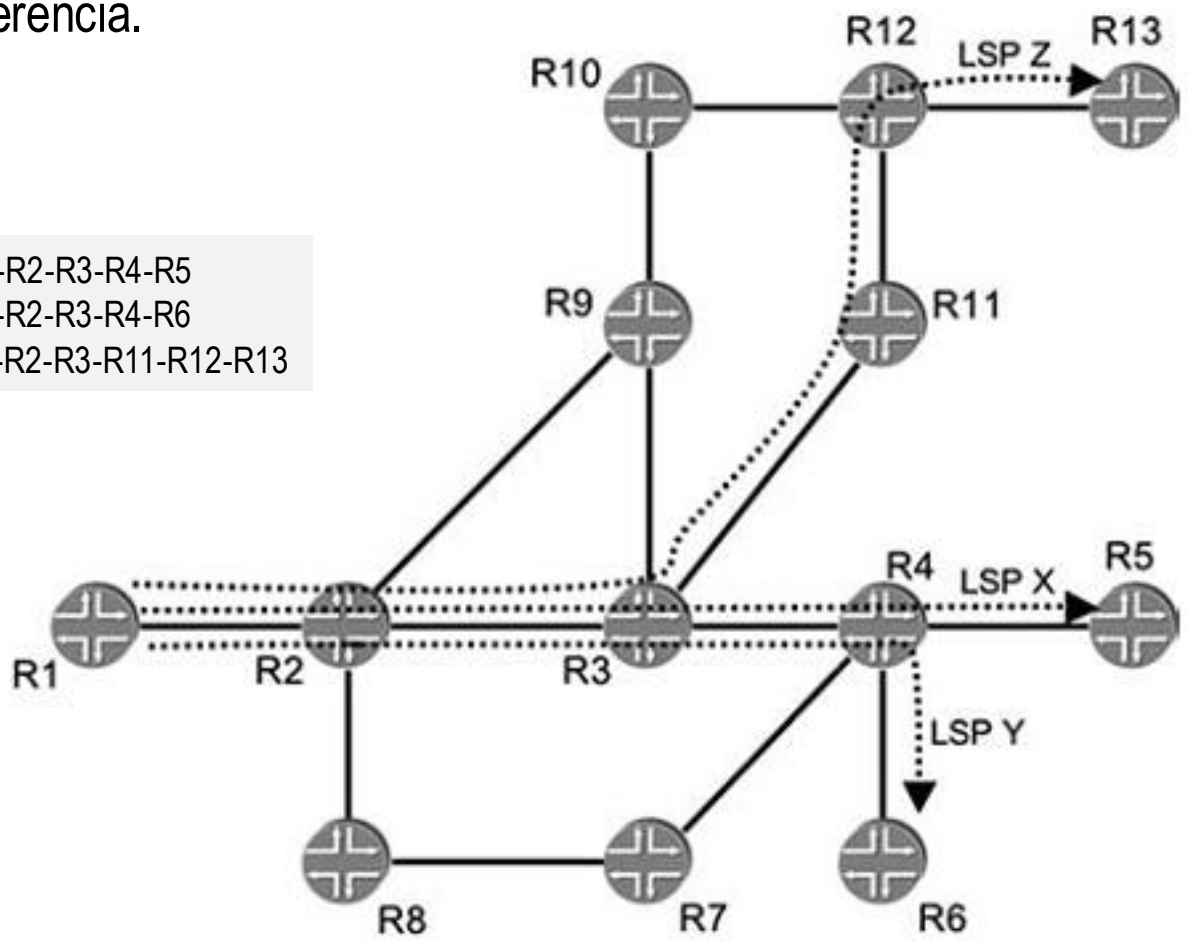
MPLS: protección y restauración.

- Tipos de protección salto a salto (tipos de protección local).
  - Según tipo de recurso protegido:
    - Protección de **enlace** y protección de **nodo**.
    - Determina la localización del trayecto de protección (*backup*).
    - Colectivamente referidos como "protección local" o "FRR".
  - Dos tipos según el nº de LSP protegidos por el "túnel" de protección:
    - **Protección 1:1** (protección uno a uno).
      - El trayecto de protección se denomina "desvío" (*detour*).
      - Trayecto de protección individual para cada LSP a proteger, basado en el trayecto óptimo para cada caso.
    - **Protección N:1** (protección de sistema).
      - El trayecto de protección se denomina "túnel *bypass*".
      - Trayecto de protección común para los LSP a proteger, sin garantía de trayecto óptimo para cada LSP.
  - En principio disponibles cuatro posibles variantes.
  - A continuación ejemplos de cada variante en términos del nº y localización de los trayectos de protección.

MPLS: protección y restauración.

- Ejemplo de protección salto a salto (protección local).
  - Escenario de referencia.

LSP X: R1-R2-R3-R4-R5
LSP Y: R1-R2-R3-R4-R6
LSP Z: R1-R2-R3-R11-R12-R13

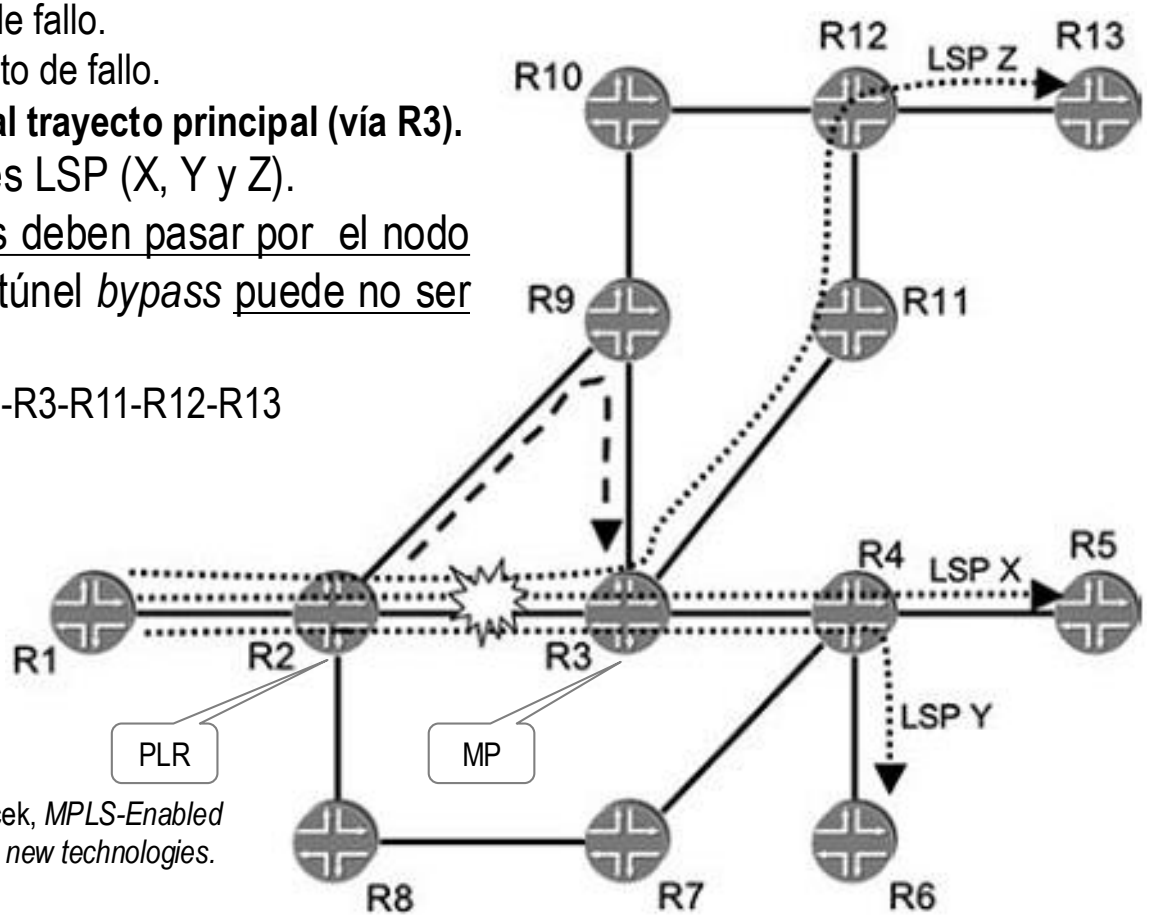


Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

- Ejemplo de protección salto a salto (protección local) (II).
  - Caso 1: **protección de enlace N:1.**
    - Falla enlace R2-R3.
    - R2 (nodo PLR) establece un túnel *bypass* común hacia R3 (nodo MP) vía R9 para los tres LSP (X, Y, Z)
      - R2 nodo *upstrean* inmediato al punto de fallo.
      - R3 nodo *downstream* inmediato al punto de fallo.
      - **Se requiere que el "desvío" vuelva al trayecto principal (vía R3).**
    - Túnel *bypass* se comparte por los tres LSP (X, Y y Z).
    - Dado que todos los LSP restaurados deben pasar por el nodo MP (R3), el trayecto utilizado por el túnel *bypass* puede no ser el óptimo para cada LSP.
      - P.e, **LSP Z** sigue el trayecto R1-R2-R9-R3-R11-R12-R13

Importante: los trayectos de protección se utilizan por poco tiempo, hasta que se establezca el nuevo LSP principal. No es un problema grave para el operador trayectos de protección no óptimos.

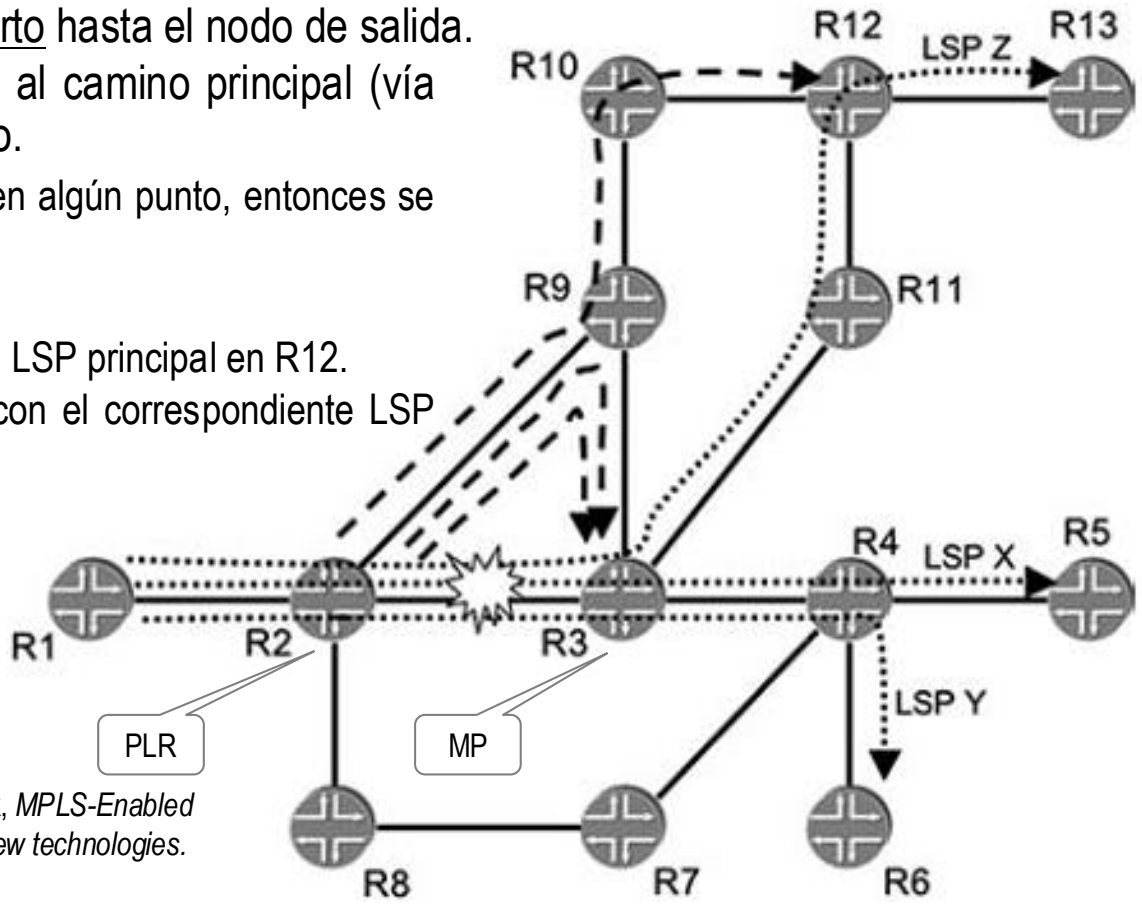


PLR: Point of Local Repair
MP: Merge Point

Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

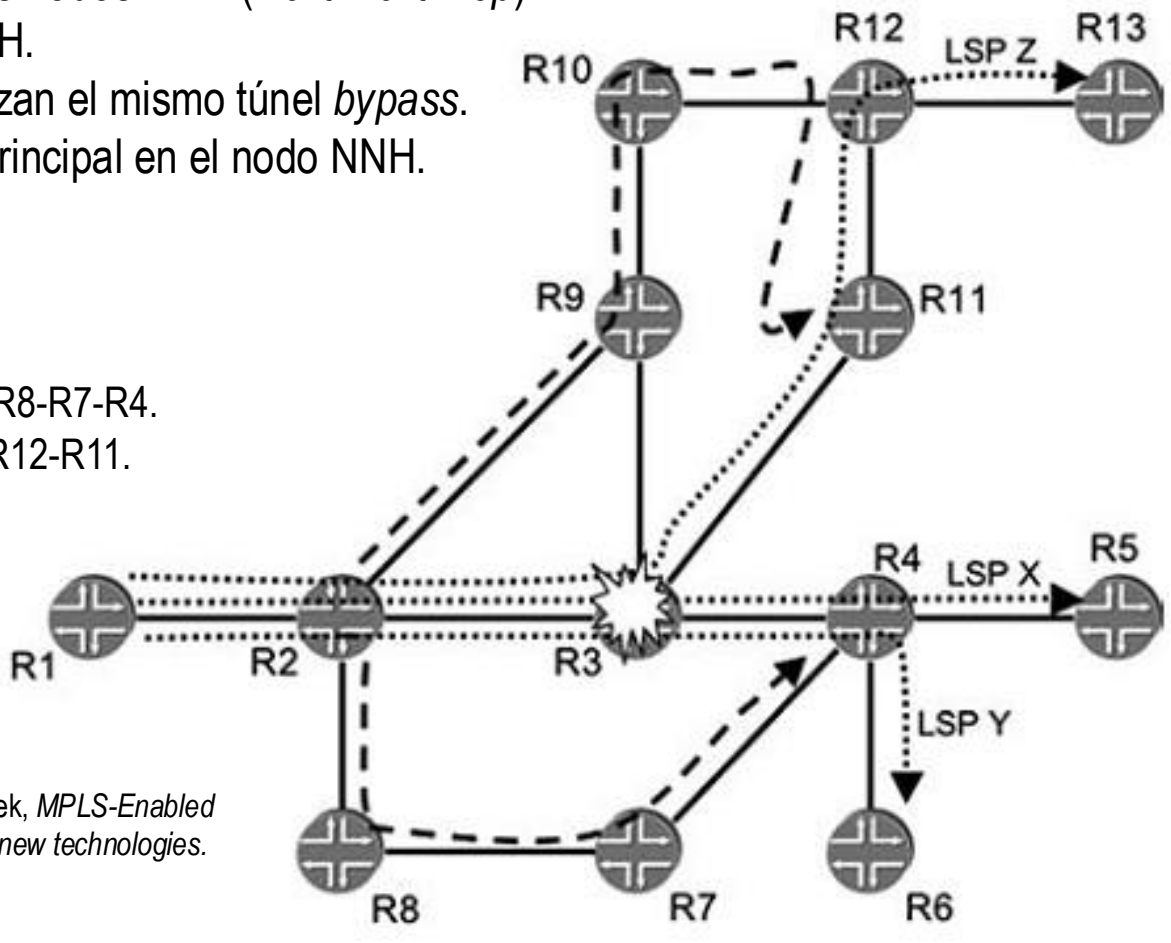
- Ejemplo de protección salto a salto (protección local) (III).
  - Caso 2: **protección de enlace 1:1.**
    - Falla enlace R2-R3.
    - Se crea **un "desvío" para cada LSP** que utilice el enlace R2-R3.
    - Cada "desvío" sigue el trayecto más corto hasta el nodo de salida.
    - No se requiere que el "desvío" vuelva al camino principal (vía MP, R3) si no está en el trayecto óptimo.
      - Si el desvío vuelve al trayecto principal en algún punto, entonces se fusiona (*merge*) con el LSP principal.
    - Ejemplo:
      - **LSP Z**: R2-R9-R10-R12 se fusiona con el LSP principal en R12.
      - **LSP X**, **LSP Y**: R2-R9-R3 se fusionan con el correspondiente LSP principal en R3.



Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

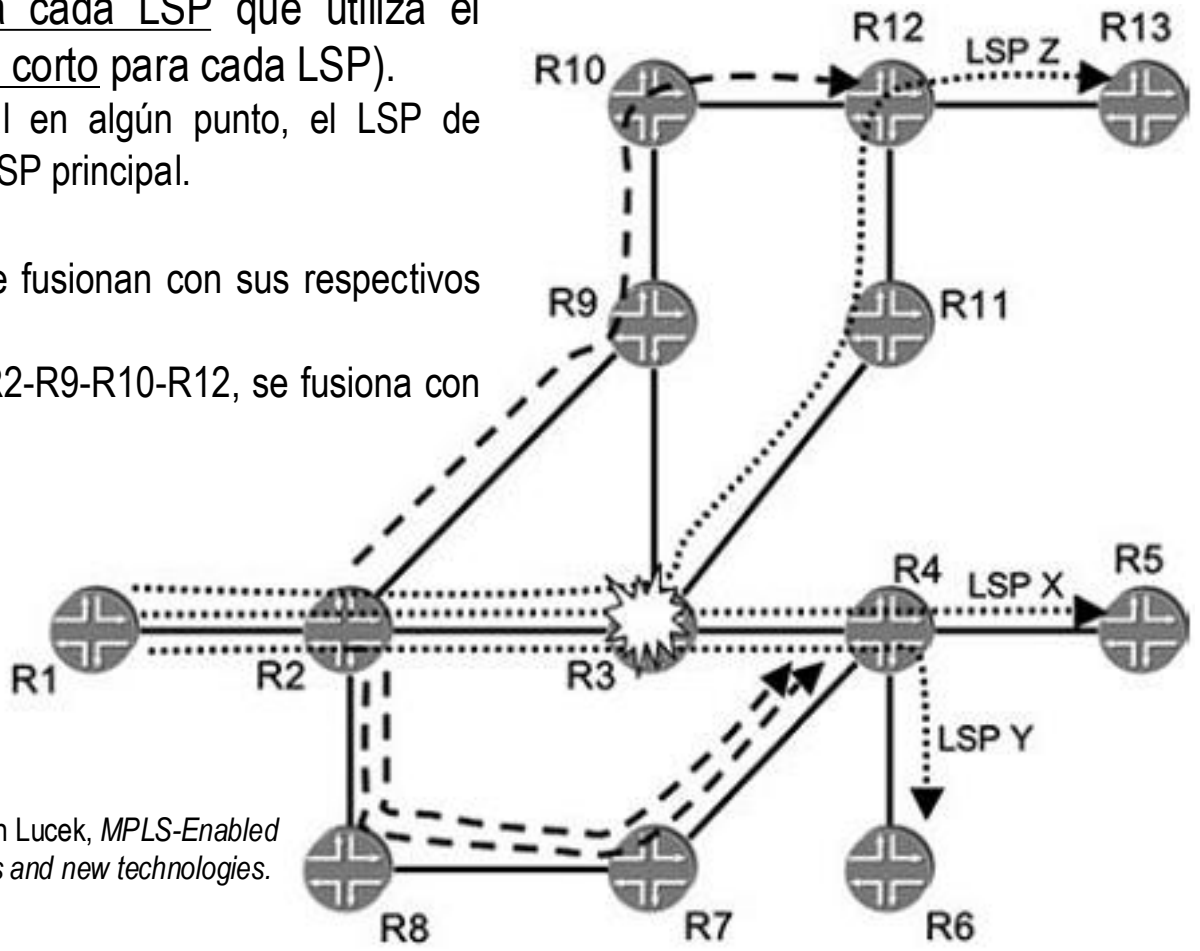
- Ejemplo de protección salto a salto (protección local) (IV).
  - Caso 3: **protección de nodo N:1.**
    - Falla nodo R3.
    - Nodo R2 tiene que identificar todos los nodos NNH (*Next-Next-Hop*).
    - No todos los LSP tienen el mismo NNH.
    - Los LSP con el mismo nodo NNH utilizan el mismo túnel *bypass*.
    - Los LSP se fusionan con el trayecto principal en el nodo NNH.
    - Ejemplo:
      - NNH para **LSP X** y **LSP Y**: R4.
      - NNH para **LSP Z**: R11.
      - Túnel *bypass* para **LSP X** y **LSP Y**: R2-R8-R7-R4.
      - Túnel *bypass* para **LSP Z**: R2-R9-R10-R12-R11.



Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

- Ejemplo de protección salto a salto (local) (V).
  - Caso 4: **protección de nodo 1:1.**
    - Falla nodo R3.
    - Se crea "desvío" separado para cada LSP que utiliza el enlace R2-R3 (por el trayecto más corto para cada LSP).
      - Si se vuelve al trayecto principal en algún punto, el LSP de desvío se fusiona (*merge*) con el LSP principal.
    - Ejemplo:
      - **LSP X** y **LSP Y**: R2-R8-R7-R4, se fusionan con sus respectivos LSP principales en R4.
      - **LSP Z** sigue un trayecto óptimo: R2-R9-R10-R12, se fusiona con su LSP principal en R12.



Fuente de la figura: Ina Minei & Julian Lucek, *MPLS-Enabled Applications, emerging developments and new technologies.* John Wiley & Sons Ltd. 2011.

MPLS: protección y restauración.

- MPLS, protección y DiffServ.

Ejemplo: dos LSP, cada uno con una reserva de 60 Mbps.

LSP1: A-B-E (tolera algunas pérdidas).

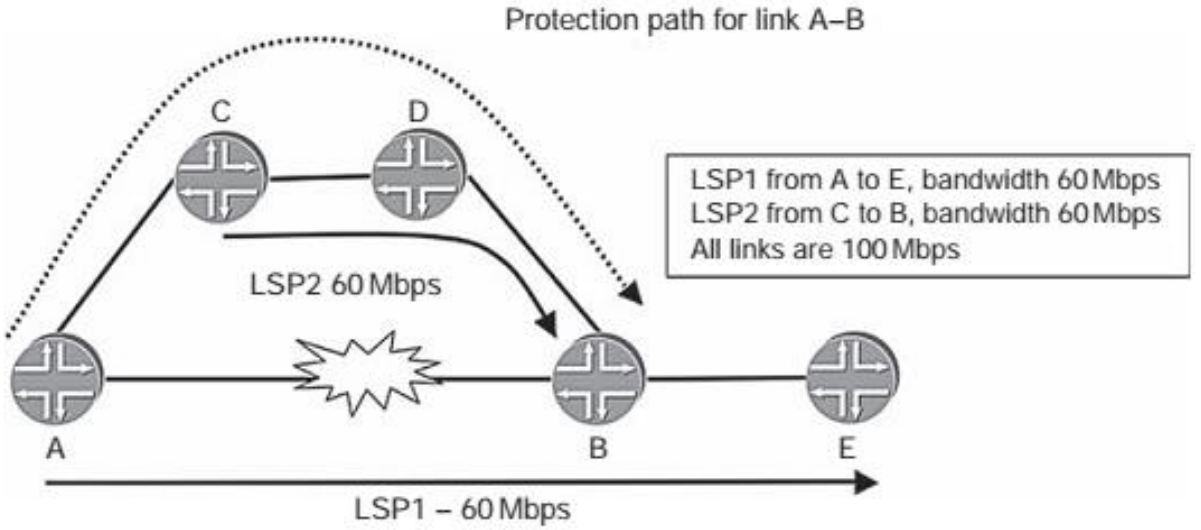
LSP2: C-D-B.

Todos los enlaces son 100 Mbps.

Protección del enlace A-B se provee por medio del trayecto A-C-D-B.

¿Qué ocurre si falla el enlace A-B?

- Se envían 60 + 60 = 120 Mbps por los enlaces C-D y D-B → Congestión y pérdidas.
- Tráfico perdido puede ser de LSP1 o LSP2, fallo de LSP1 afecta a LSP2.
- Mediante marcado DiffServ de paquetes del LSP1 en nodo "A" se puede paliar el efecto negativo sobre LSP2 que pueden producir éstos en base a diferentes prioridades de descartes (bits EXP).



MPLS: conclusiones.

- MPLS, conclusiones.
  - Tecnología para el reenvío de paquetes a través de una solución "conectiva" en redes "no conectivas IP", mediante:
    - Conexiones lógicas denominadas LSPs, conformadas de manera automatizada mediante protocolos de control-señalización para distribución de etiquetas.
    - "Etiqueta" añadida a los paquetes y conmutación de "etiquetas".
    - Inicialmente desarrollada para agilizar la operativa de los *routers*.
    - Posteriormente e interés actual para diferentes aplicaciones de uso.
  - Aplicaciones MPLS de interés:
    - VPN de capa 3 y de capa 2.
    - Ingeniería de tráfico.
    - QoS a partir de los modelos DiffServ e IntServ desarrollados para redes IP puras.
    - Protección y restauración.

MPLS: bibliografía.

- Bibliografía.
  - I. Minei and J. Lucek:
    - *MPLS-Enabled Applications*. John Wiley & Sons, 3rd Ed, 2011.
  - H. Jonathan Chao and Xiaolei Guo:
    - *Quality of Serice Control in High-Speed Networks*. 2002 John Wiley & Sons, Inc.
  - L. De Ghein:
    - *MPLS Fundamentals*. Cisco Press, 2007.
  - V. Alwayn:
    - *Advanced MPLS Design and Implementation*. Cisco Press, 2001.