MPLS-TE

Ingeniería de tráfico - Curso 2014-15

Área de Ingeniería Telemática - Departamento de Automática

Universidad de Alcalá

José Manuel Giménez

MPLS-TE

- Introducción.
- Uso de prioridades.
- Cálculo de caminos explícitos.

Introducción

Ingeniería de tráfico (TE): adaptar el tráfico a la red

vs.

Ingeniería de redes: adaptar la red al tráfico

- TE: optimizar el uso de los recursos de red situando el tráfico en los enlaces deseados.
  - Calcular un camino de un origen a un destino sujeto a una serie de restricciones y reenviar el tráfico por dicho camino.
    - Se basa en el encaminamiento explícito.

Introducción

- TE posibilita a los operadores de red:
  - Mejorar/optimizar la utilización de los recursos de red, mediante:
    - Balance de la distribución de la carga de tráfico en la red.
    - Se evitan enlaces congestionados ➔ Se reducen las pérdidas y el retardo y mejora el rendimiento.
  - Garantizar que el trayecto que siga el tráfico cumpla con determinadas características.
    - Ej: que no contenga enlaces de elevada latencia.
  - Garantizar que los recursos necesarios estén disponibles en todo el trayecto.
  - Determinar el tráfico prioritario en momentos de limitación de recursos.
    - Ej: fallo de un enlace o de un nodo.
  - Aumentar los ingresos mediante la oferta de nuevos servicios.
    - Ej: servicio de ancho de banda garantizado, tanto en condiciones normales como ante fallos en la red.
  - Reducir gastos en nuevas inversiones aumentando la utilización de los recursos ya disponibles.

Introducción

- TE:
  - No siempre necesaria:
    - Si se dispone de todo el ancho de banda necesario.
    - Si el ancho de banda disponible tiene muy baja utilización.
    - Si no hay enlaces de alta latencia.
    - Si el tráfico no requiere el cumplimiento de determinados requisitos.
  - Los medios para implementarla y mantenerla deben ser simples.
    - MPLS es una tecnología útil para TE, proporciona simplicidad operacional y flexibilidad para políticas TE complejas.

Introducción

- Ingeniería de tráfico con MPLS (MPLS – TE) se basa en:
  - Determinación del trayecto con determinadas restricciones que debe seguir el tráfico entre LSR de entrada y LSR de salida.
    - En base a las capacidades de **encaminamiento explícito** de MPLS a partir de la fuente, con CR-LDP o RSVP-TE.
  - Reenvío del tráfico por el trayecto LSP establecido.

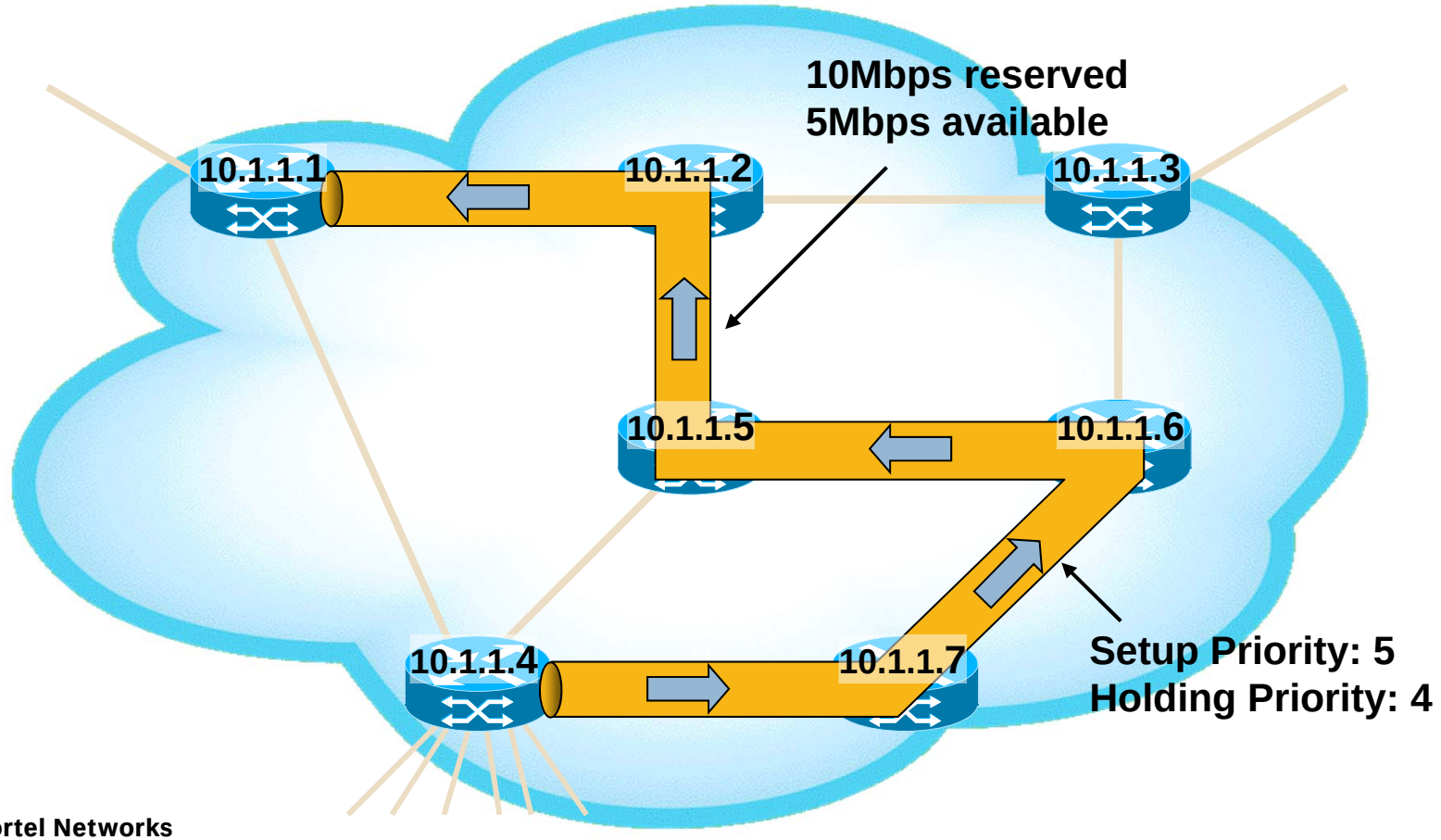
Uso de prioridades

- MPLS emplea prioridades para los LSPs:
  - Objetivo: marcar la importancia de los LSPs en la red para poder realizar desalojos.
- Garantiza:
  - En ausencia de LSPs importantes, los LSPs menos importantes pueden reservar recursos.
  - Un LSP importante siempre se establece por el camino óptimo, independientemente de si existen otros LSPs menos importantes.
  - Cuando se necesita reencaminar (debido a un fallo) los LSPs importantes tienen una mayor probabilidad de encontrar un camino alternativo.

Uso de prioridades

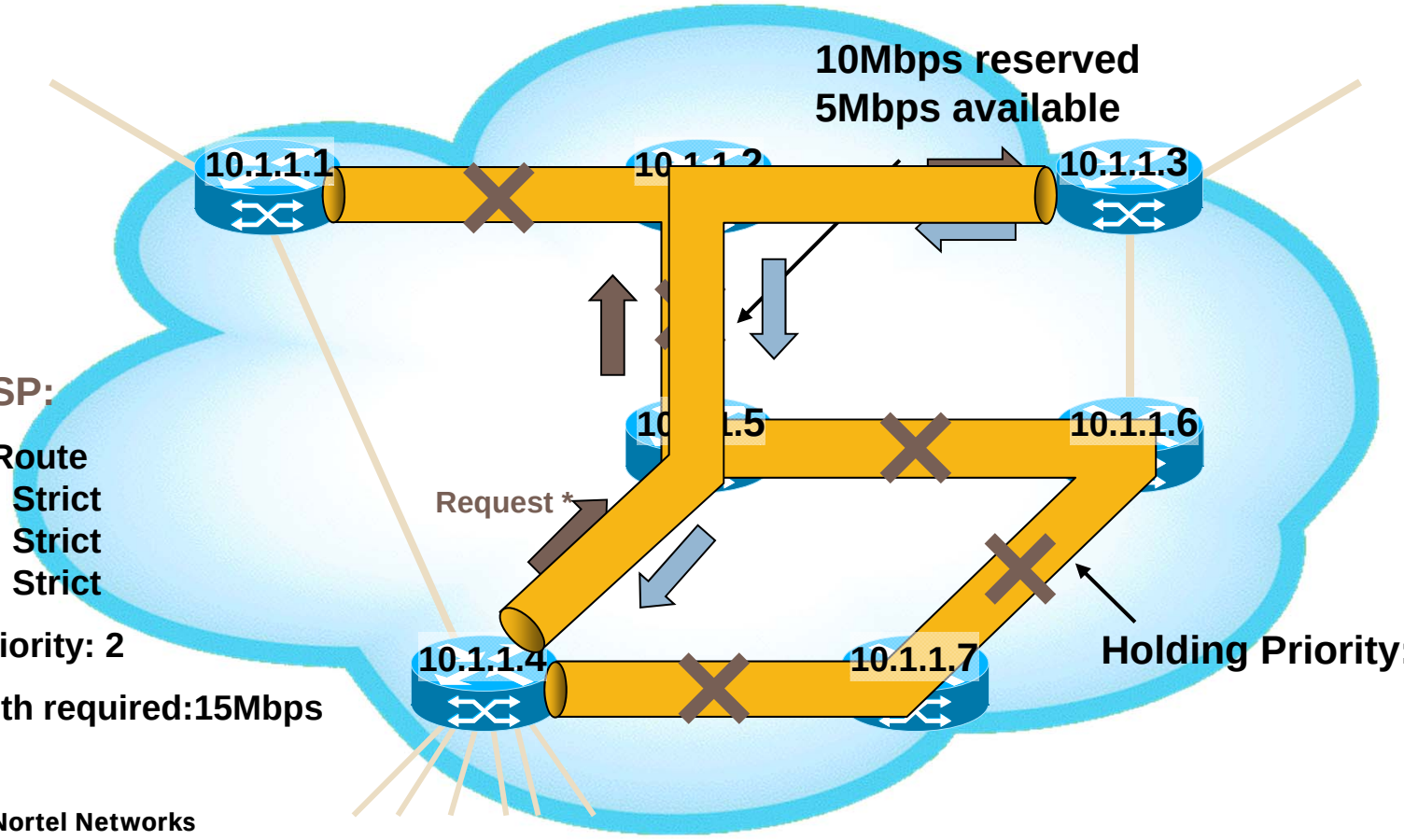
- CR-LDP y RSVP-TE definen dos tipos de prioridades:
  - De establecimiento (*setup*):
    - Controla el acceso a los recursos durante el establecimiento del LSP.
  - De mantenimiento (*hold*).
    - Controla el acceso a los recursos de un LSP que ya está establecido.
  - Durante el establecimiento de un LSP, si no hay recursos suficientes, la prioridad de *setup* del nuevo LSP se compara con las prioridades de mantenimiento de los LSPs que están usando los recursos deseados.
- 8 niveles para cada una: 0 – 7 (0 es la más prioritaria).

Uso de prioridades: ejemplo (i)



Source: Nortel Networks

Uso de prioridades: ejemplo (ii)



***New LSP:**

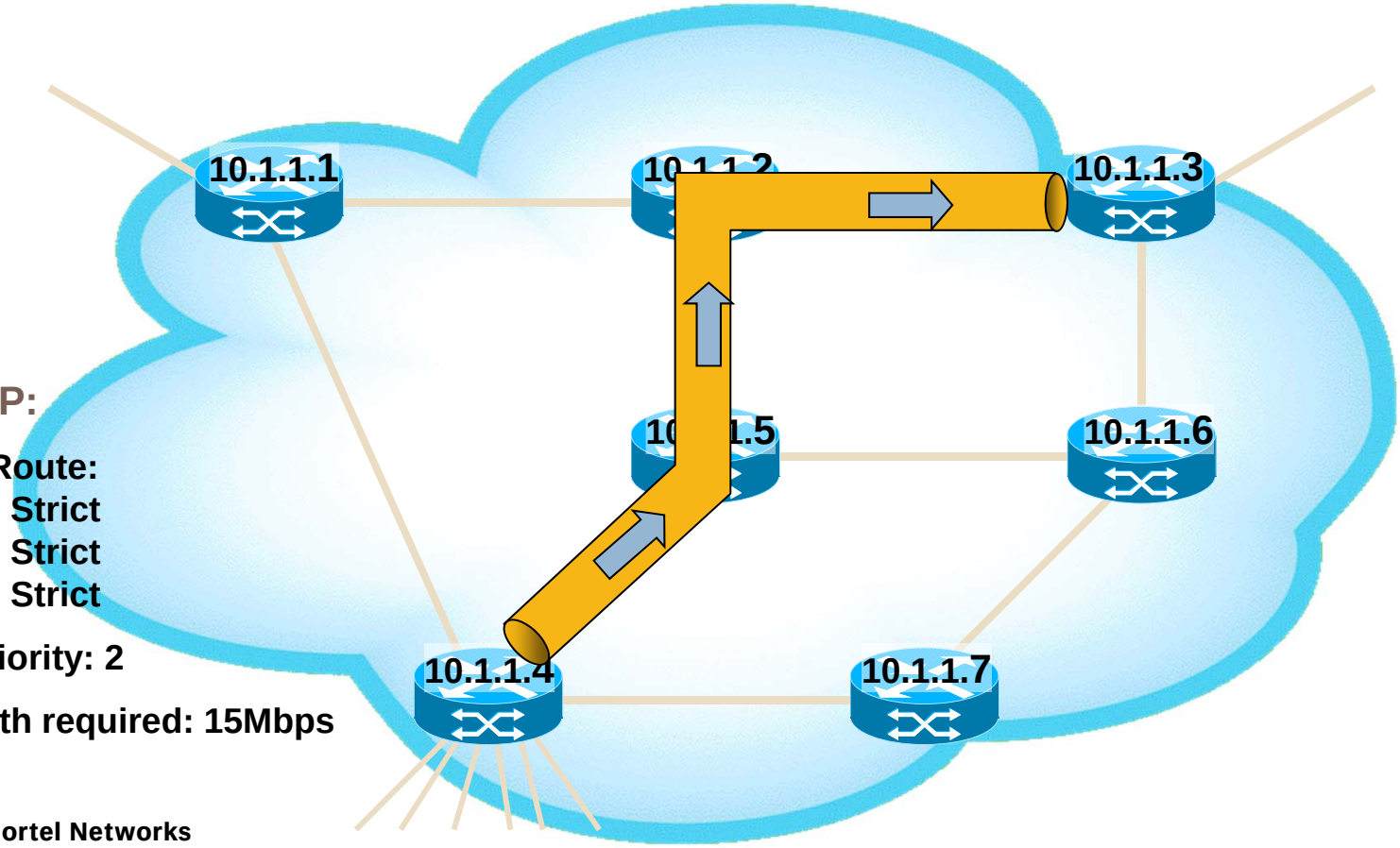
Explicit Route
10.1.1.5 Strict
10.1.1.2 Strict
10.1.1.3 Strict

Setup Priority: 2

Bandwidth required:15Mbps

Source: Nortel Networks

Uso de prioridades: ejemplo (iii)



New LSP:

Explicit Route:
10.1.1.5 Strict
10.1.1.2 Strict
10.1.1.3 Strict

Setup Priority: 2

Bandwidth required: 15Mbps

Source: Nortel Networks

Uso de prioridades

- ¿Es necesario asignar prioridades *setup* y *hold* diferentes a un LSP?
  - Sí, solución por defecto en muchas implementaciones.
- Prioridad *setup* alta (0) y prioridad *hold* baja (7):
  - Puede provocar inestabilidad en la red cuando dos LSPs compiten por el mismo recurso.
    - Desalojos constantes entre un par de LSPs que compiten por el mismo recurso.
  - Consecuencia.
    - La mayoría de las implementaciones no permiten prioridades *hold* peores que prioridades *setup*.
- Prioridad *setup* baja (7) y prioridad *hold* alta (0):
  - Garantía de entorno de red estable.
  - No es posible «desalojo» de LSPs.

Cálculo de caminos explícitos

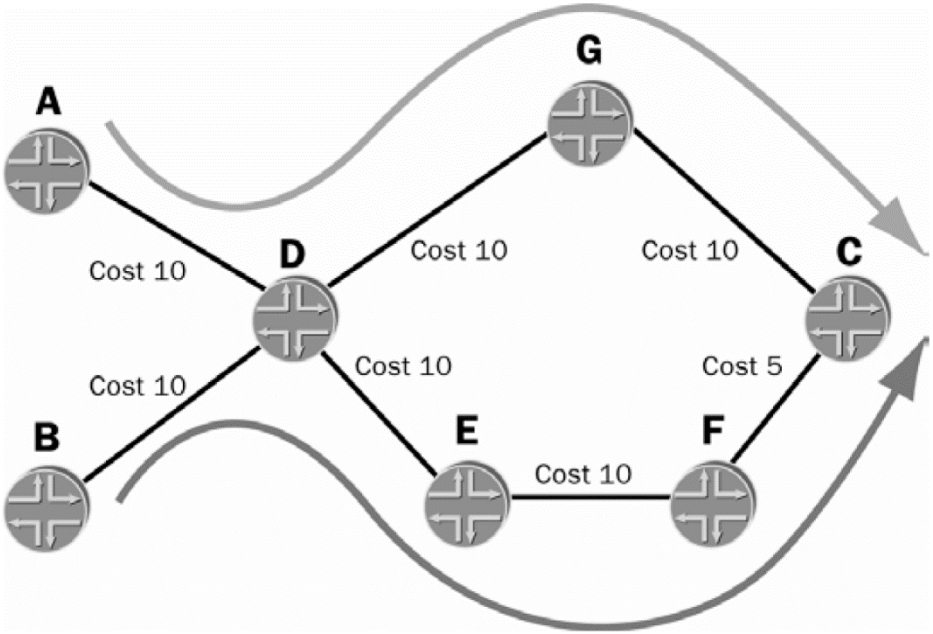
- Dos tipos de restricciones:
  - Relativas a enlaces: ancho de banda disponible, atributos…
  - Relativas a LSPs: número de saltos, prioridades…
- Encontrar un camino en la red que satisfaga una serie de restricciones como:
  - El ancho de banda requerido.
  - Atributos de los enlaces que se permite emplear (colores). Por ejemplo, puede impedirse el uso de enlaces de alto retardo marcándolos con un color.
  - Número de saltos máximo.
  - Prioridad del LSP.
  - …

Cálculo de caminos explícitos

- Uso de CSPF: *Constrained Shortest Path First*.
  - Versión modificada de SPF que elimina de la topología todos los enlaces que no satisfacen las restricciones.
    - Por ejemplo, si la restricción es el ancho de banda, elimina de la topología todos los enlaces que no cumplen con ese requisito.
- Una vez calculado el camino → Se establece el CR-LSP con CR-LDP o RSVP-TE.

Cálculo de caminos explícitos

- Ejemplo (todos los enlaces son de 150Mbps):
  - LSP A-C reserva 100Mbps.
  - LSP B-C requiere 100Mbps, pero como no hay suficientes recursos por el camino más corto (B-D-G-C), se eliminan dichos enlaces en el cálculo CSPF.
  - LSP B-C se establece por B-D-E-F-C.



Fast ReRoute

Ingeniería de tráfico - Curso 2014-15

Área de Ingeniería Telemática - Departamento de Automática

Universidad de Alcalá

José Manuel Giménez

Fast ReRoute

- Introducción.
- Protección local mediante FRR:
  - Caso 1.
  - Caso 2.
  - Caso 3.
  - Caso 4.
  - Protección en anillo.

Introducción

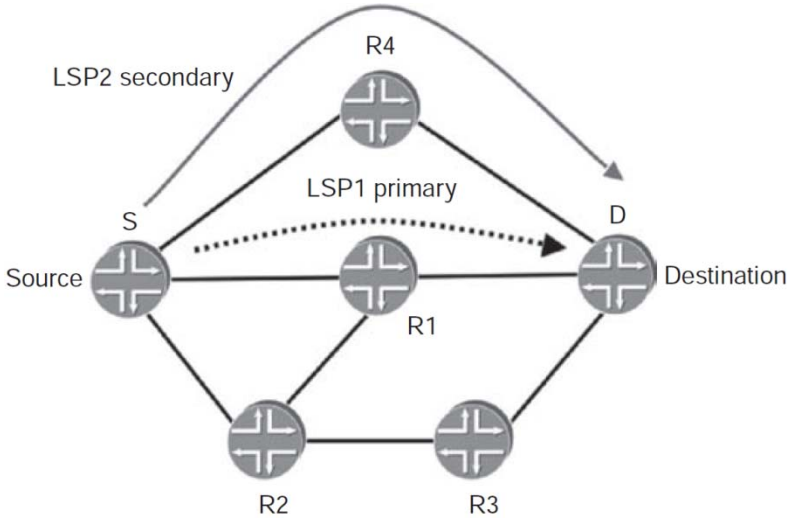
- No solo se requiere QoS para las aplicaciones cuando estas están funcionando, sino que también hay que dar calidad a los servicios tras un fallo en la red → Protección y restauración.
  - Especialmente para servicios de tiempo real como audio o vídeo, que además no admiten retransmisiones como mecanismo de recuperación.
- En ocasiones MPLS-TE se identifica con Fast ReRoute (FRR).
- Convergencia de la red del operador en una única red MPLS → Se deben ofrecer garantías de protección de servicios como en las redes que integra. Ej: SDH APS.
- Objetivo de FRR: dar una garantías similares a las proporcionadas por SDH APS para los túneles MPLS.
- Pero APS protege enlaces, mientras que FRR también:
  - Protege frente a la caída de nodos.
  - No está limitado a una única tecnología.
  - No requiere *hardware* extra.

Introducción

- Tiempo de recuperación:
  - Detección del fallo.
  - Recuperación del fallo, típicamente dirigiendo el tráfico por otro camino.
- Detección de fallos:
  - En algunas tecnologías como SDH se provee en capa física mediante *hardware*.
  - Si no se provee mediante hardware hay que buscar alternativas:
    - Mensajes *hello* de protocolos de encaminamiento como IGP.
      - Se descarta esta opción puesto que los mensajes no se envían tan frecuentemente como sería necesario.
      - No podemos enviarlos más frecuentemente porque requieren carga computacional.
    - Protocolo BFD: *Bidirectional Forwarding Detection*.
      - Detección de fallos en capas bajas.
      - Diseñado por el grupo de IETF BFD. RFC 5880.
      - Es un protocolo simple de envío de *hellos* para detectar fallos entre dos entidades que reenvíen paquetes.
      - Detección de fallos en torno a decenas de ms.

Introducción

- Recuperación de fallos:
  - Extremo a extremo: protección de camino:
    - Usa dos LSPs: primario y secundario (*backup*).
    - Para que sea rápido, el LSP debe estar previamente establecido (señalizado) → Doble reserva de recursos.
      - Puede darse el caso de no establecer un nuevo LSP porque no hay recursos cuando estos no están siendo utilizados por ser LSPs secundarios.
    - Ambos LSPs no deben coincidir en ningún enlace → Diversidad de caminos.

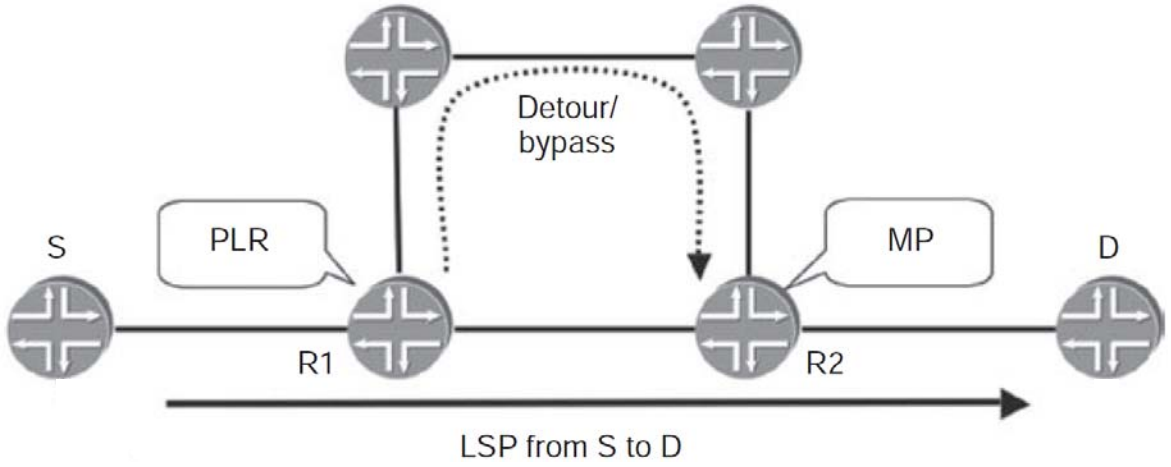


  - Salto a salto (local): Fast ReRoute (FRR).

Protección local mediante FRR

- Objetivo: minimizar el tiempo durante el cual se pierde tráfico → Aplicar la protección lo más cercanamente al punto de fallo.
- Se reencamina el tráfico alrededor del punto de fallo.

- PLR: Punto de reparación local.
- MP: Punto de convergencia.

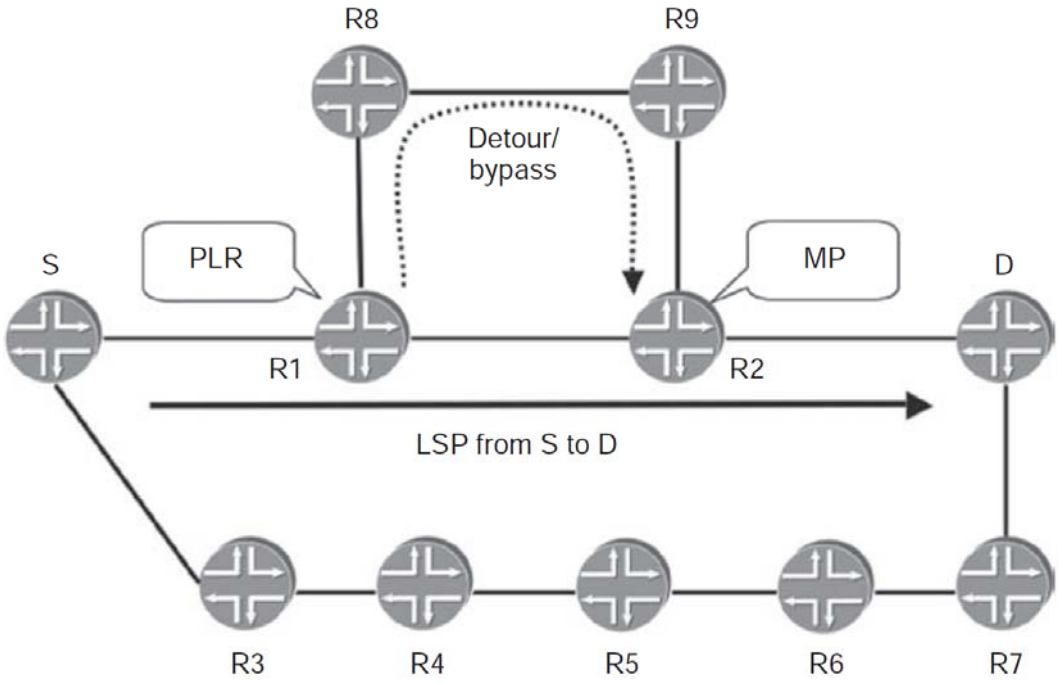


Protección local mediante FRR

- Propiedades interesantes:
  - Se protege un recurso único, por lo que es posible escoger fácilmente qué recursos proteger.
  - La protección es rápida, puesto que se aplica cerca del punto de fallo.
    - El reenvío de tráfico por el camino alternativo lo realiza el nodo que está más cerca del fallo (PLR).
  - El tráfico se envía alrededor del fallo por el desvío, por un camino que ha sido calculado y señalizado previamente → Una vez que el nodo *upstream* (PLR) del punto de fallo detecta el fallo, mueve el tráfico inmediatamente.
    - No hay que señalizar a otros nodos para usar el camino alternativo.

Protección local mediante FRR

- ¿Por qué no usar FRR en redes IP? Porque se basa en "*source routing*".
  - Para que funcione la protección local, el tráfico debe poder alcanzar el inicio del camino de protección.
  - Para el tráfico IP las decisiones de reenvío son independientes en cada salto en función de la dirección destino.
- Ejemplo:
  - Coste de todos los enlaces 1, excepto R8-R9 que es 10.
  - Cuando cae enlace R1-R2, S calcula la nueva ruta S–R3–R4–R5–R6–R7–D → Los paquetes no llegan al camino de protección.



Protección local mediante FRR

- Plano de control para FRR:
  - RSVP-TE:
    - RFC 4090: "*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*", 2005.
  - ¿Y si se quiere usar FRR en una red MPLS que emplea LDP?
    - No existe (a día de hoy) estándar sobre FRR con CR-LDP, aunque existe el draft: *"Fast Re-route using extensions to LDP"* (2012).
    - Están empezando a llegar implementaciones de vendedores.
    - Hasta ahora, lo que se hacía era usar RSVP-TE en los enlaces que requerían protección local.

Protección local mediante FRR

- Funcionamiento:
  - Cuando el PLR detecta el fallo empieza a usar el camino de protección local previamente establecido.
  - Además, el PLR envía mensaje *PathErr* (RSVP-TE) al nodo origen del LSP para que calcule el nuevo LSP.
  - El nodo origen del LSP calcula la ruta del nuevo LSP y lo establece antes de eliminar el anterior (que incluye la protección): método "*make-before-break*".
    - El nodo origen del LSR es responsable de establecer el nuevo LSP.
  - El tráfico se mantiene por el desvío hasta que el origen del LSP calcula un nuevo camino y lo establece.
    - Aunque el enlace/nodo caído se recupere antes.
  - Finalmente se elimina el LSP anterior (que incluye la protección).

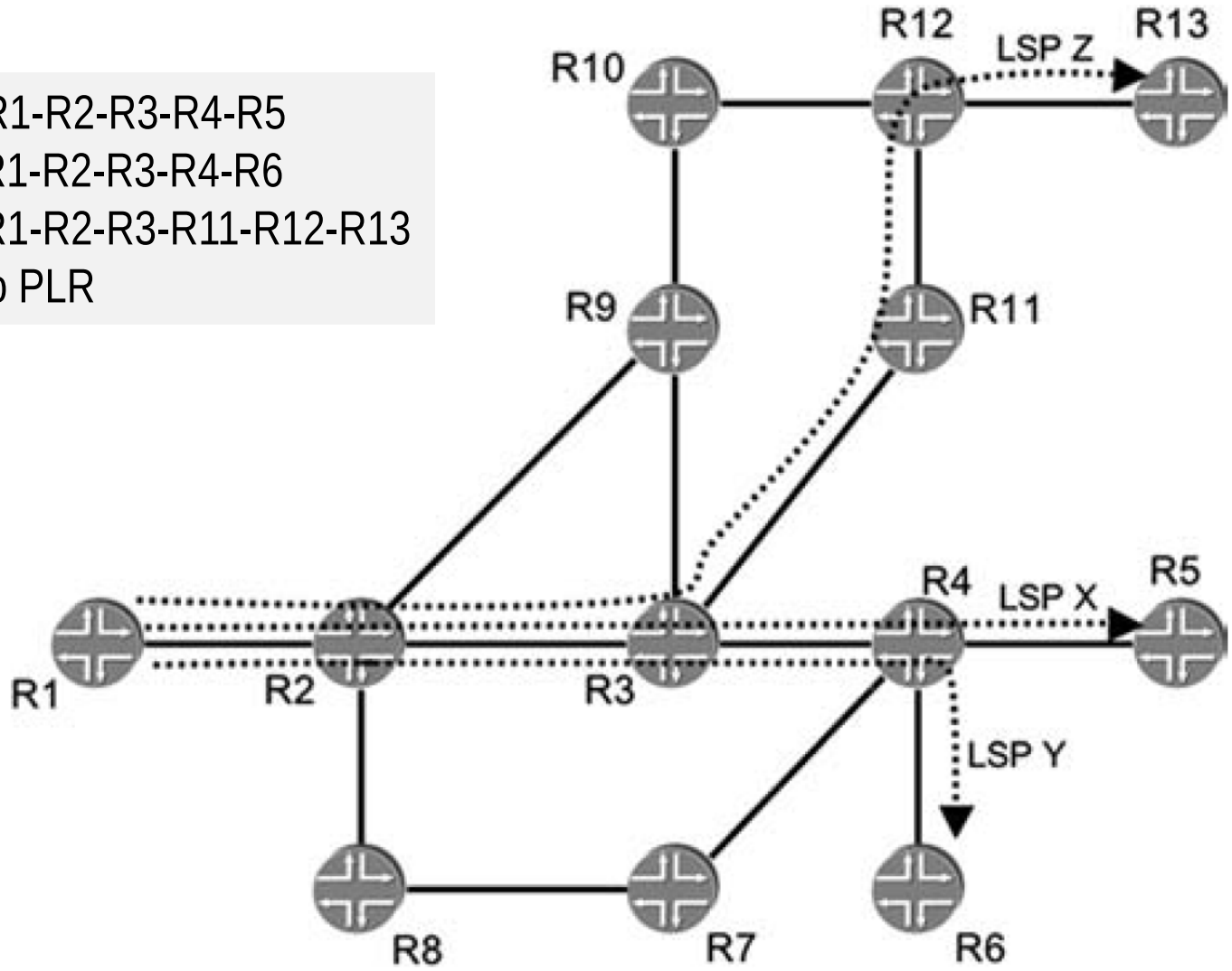
Protección local mediante FRR

- La protección local se puede clasificar mediante dos criterios:
  - El tipo de recursos protegido:
    - Influye en la localización del camino de protección/*backup*.
    - Dos tipos:
      - Enlace.
      - Nodo.
  - El número de LSPs protegidos por el túnel de protección:
    - Dos tipos:
      - 1:1: protección uno a uno.
        - El camino de protección se llama desvío (*detour*).
      - N:1: protección de sistema.
        - El camino de protección se llama *túnel bypass*.

Protección local mediante FRR

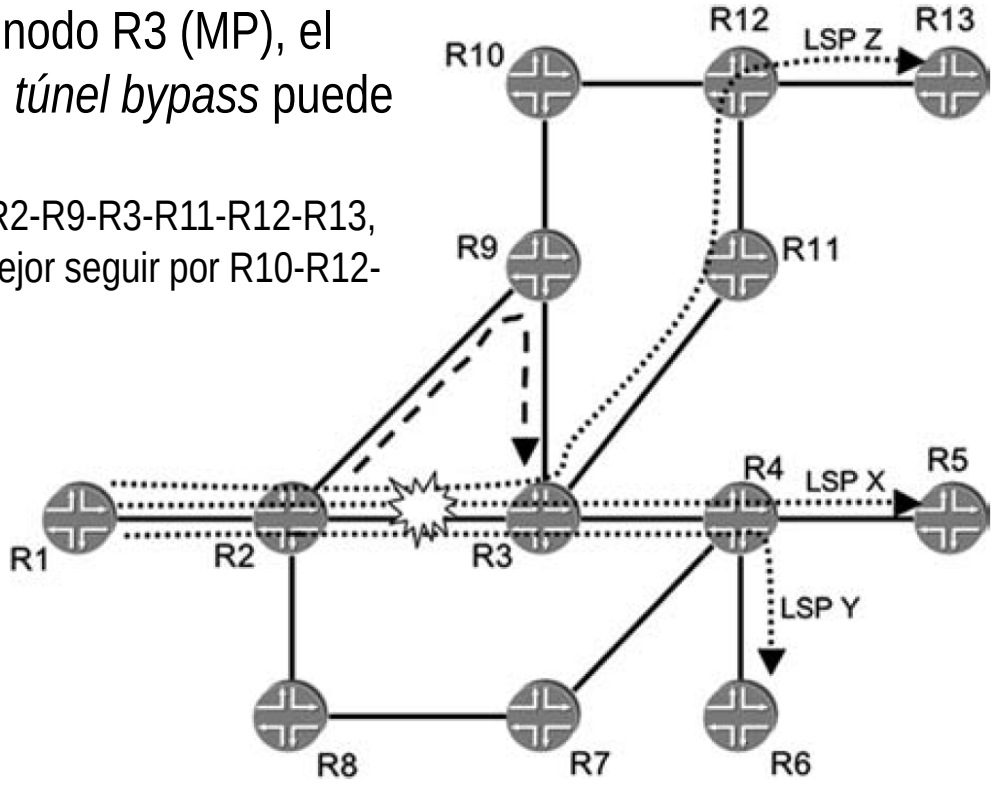
- Escenario marco:

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



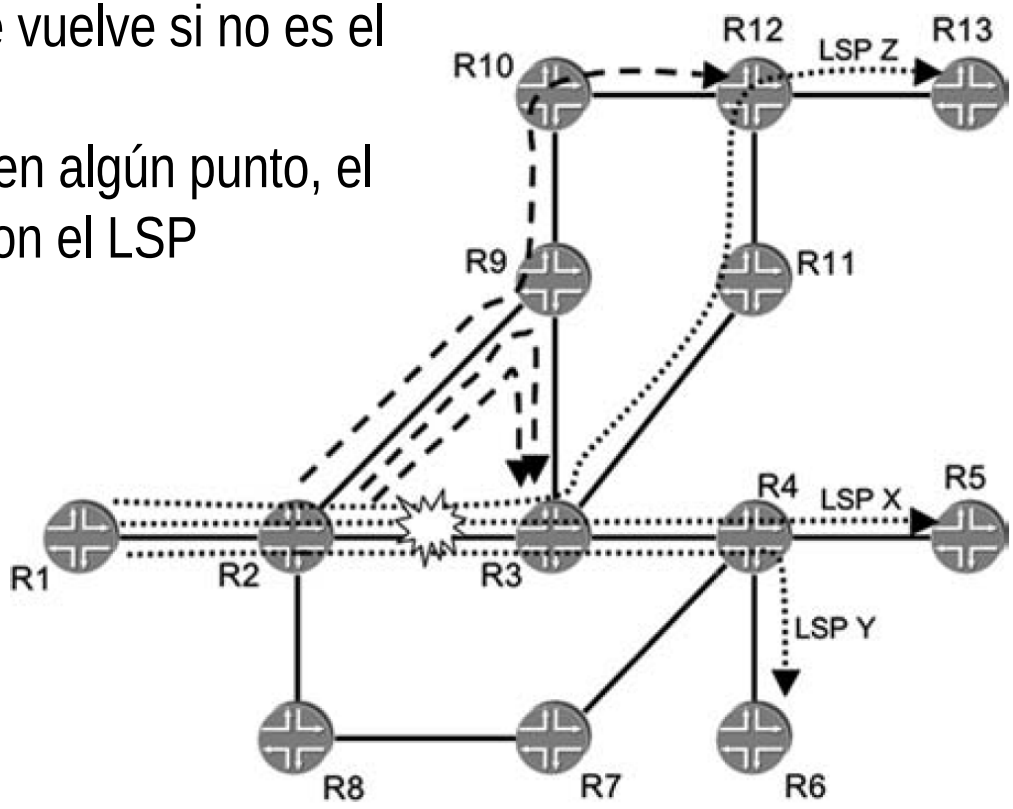
Protección local mediante FRR: caso 1

- Caso 1: protección de enlace N:1.
  - Cae el enlace R2-R3.
  - R2 **debe** establecer el *túnel bypass* de manera que R3 sea MP (el *router* inmediatamente *downstream* del enlace que ha fallado).
  - El *túnel bypass* se comparte por los LSPs:
    - Dado que se llega siempre al nodo R3 (MP), el trayecto global utilizado por el *túnel bypass* puede no ser óptimo.
      - Ej. LSP Z sigue el camino R1-R2-R9-R3-R11-R12-R13, aunque una vez en R9 sería mejor seguir por R10-R12-R13.



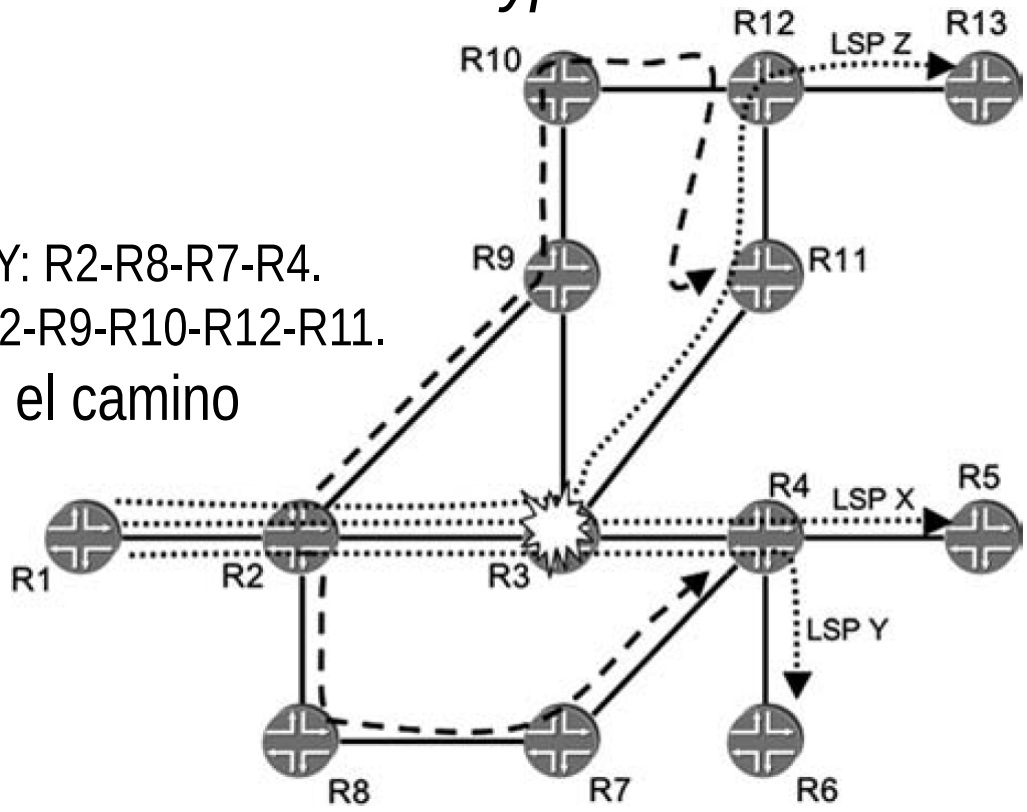
Protección local mediante FRR: caso 2

- Caso 2: protección de enlace 1:1.
  - Cae el enlace R2-R3.
  - Se crea un desvío para cada LSP que use el enlace R2-R3.
  - Cada desvío sigue el camino más corto hasta la salida.
  - No es necesario que el desvío vuelva al camino principal (en el MP R3): no se vuelve si no es el camino óptimo.
  - Si vuelve al camino principal en algún punto, el desvío se fusiona (*merges*) con el LSP principal.
  - Ejemplo:
    - LSP Z: R2-R9-R10-R12, uniéndose con su LSP principal en R12.
    - LSP X e Y se unen con su LSP principal en R3.



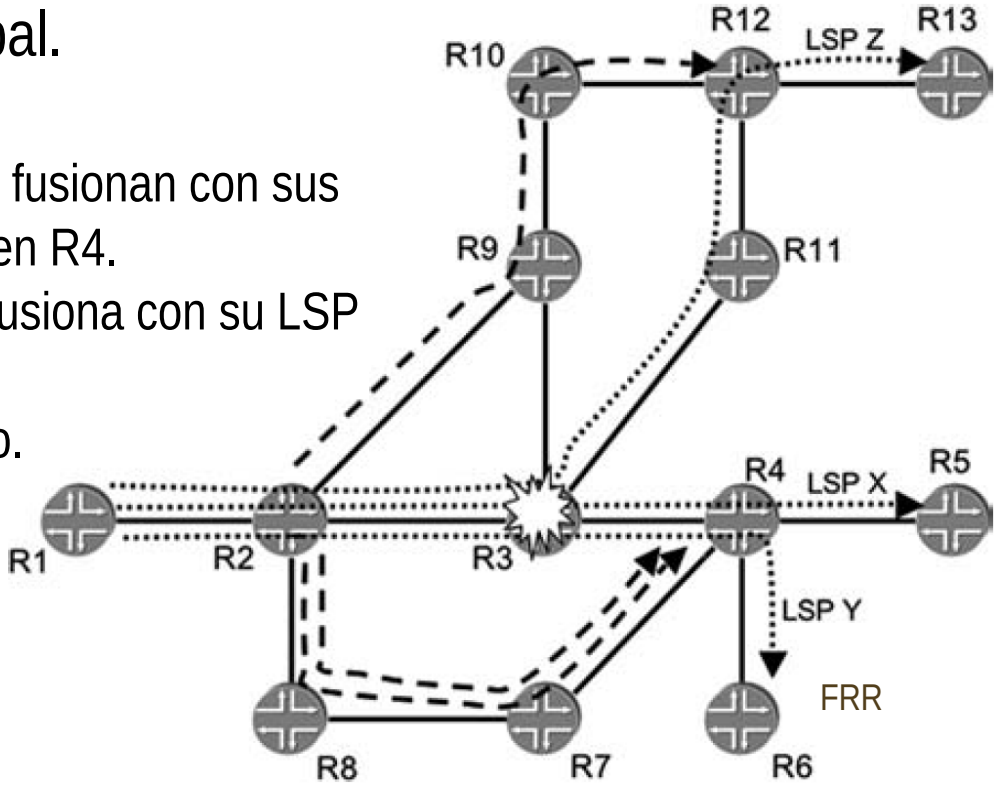
Protección local mediante FRR: caso 3

- Caso 3: protección de nodo N:1.
  - Cae el nodo R3.
  - R2 tiene que identificar todos los siguientes-siguientes-saltos (NNH).
  - No todos los LSPs tienen el mismo NNH, pero **todos los LSPs que tengan el mismo NNH usan el mismo *túnel bypass***.
  - Ejemplo:
    - NNH para LSP X e Y: R4.
    - NNH para LSP Z: R11.
    - *Túnel bypass* para LSP X e Y: R2-R8-R7-R4.
    - *Túnel bypass* para LSP Z: R2-R9-R10-R12-R11.
  - Los LSPs se fusionan con el camino principal en el NNH.
    - LSP Z sigue un camino no óptimo.



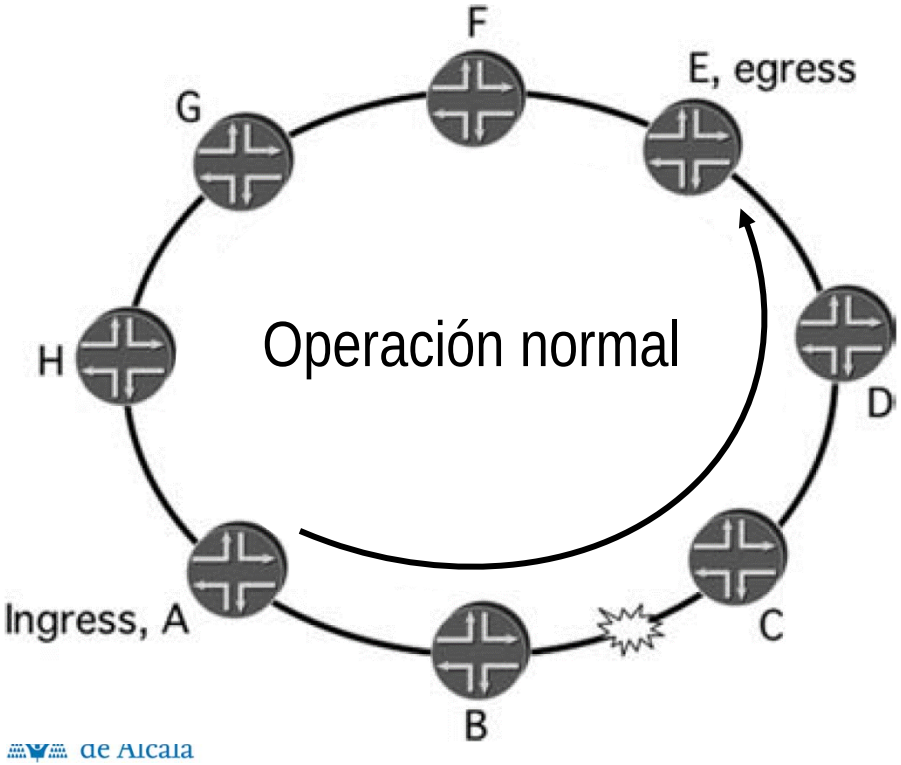
Protección local mediante FRR: caso 4

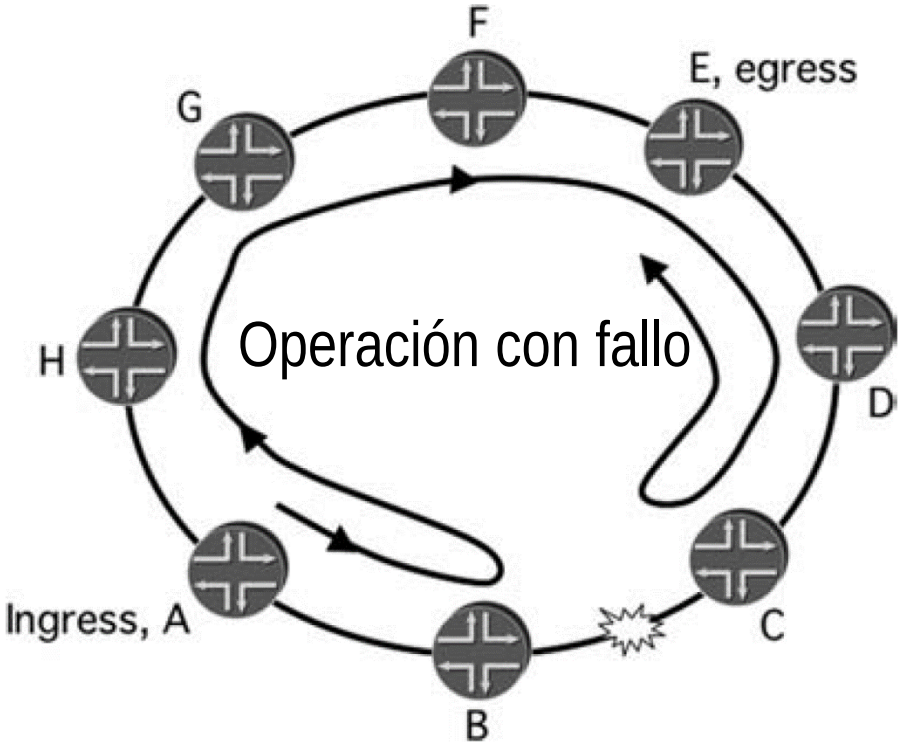
- Caso 4: protección de nodo 1:1.
  - Cae el nodo R3.
  - Se crea un desvío separado para cada LSP → Siguiendo el camino más corto para cada LSP.
  - Si vuelve al camino principal en algún punto, el desvío se fusiona (*merges*) con el LSP principal.
  - Ejemplo:
    - LSP X e Y: R2-R8-R7-R4 y se fusionan con sus respectivos LSPs principales en R4.
    - LSP Z: R2-R9-R10-R12 y se fusiona con su LSP principal en R12.
    - LSP Z sigue un camino óptimo.



Protección local mediante FRR: anillo

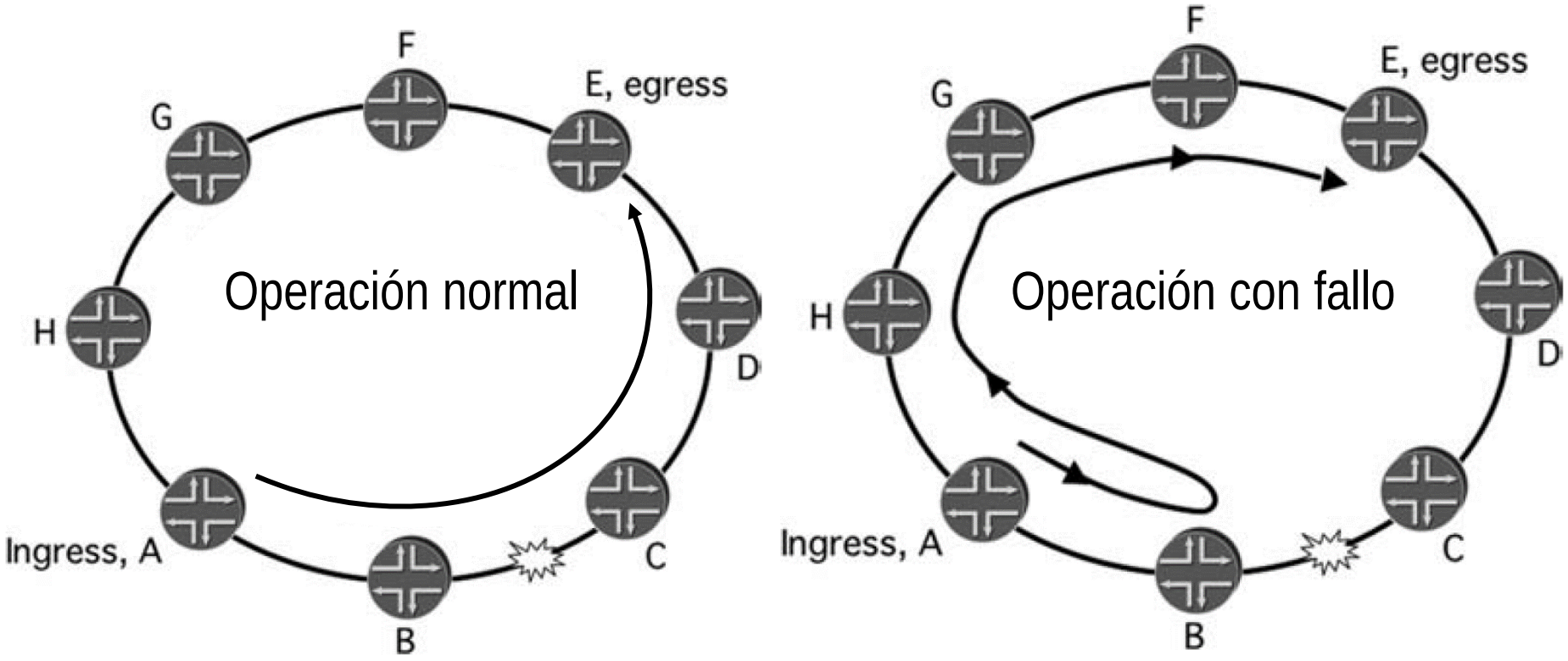
- Caso protección enlace N:1:
  - LSP inicial: A-B-C-D-E.
  - Se cae el enlace B-C: el *bypass* debe ir desde el PLR (B) hasta el MP (C), que es el siguiente salto *downstream*.
  - El tráfico seguirá el siguiente camino: A-B-A-H-G-F-E-D-C-D-E.





Protección local mediante FRR: anillo

- Caso protección enlace 1:1:
  - LSP inicial: A-B-C-D-E.
  - Se cae el enlace B-C: el desvío debe ir desde el PLR (B) hasta la salida (E), siguiendo el camino más corto.
  - El tráfico seguirá el siguiente camino: A-B-A-H-G-F-E.



QoS en MPLS

Ingeniería de tráfico - Curso 2014-15

Área de Ingeniería Telemática - Departamento de Automática

Universidad de Alcalá

José Manuel Giménez

QoS en MPLS

- Introducción.
- Soporte MPLS de IntServ.
- Soporte MPLS de DiffServ.

Introducción

- Requisitos de QoS:
  - Retardo, *jitter*, ancho de banda garantizado, tiempo de recuperación frente a fallos…
- Sin embargo, puesto que la red MPLS permite al proveedor ofrecer, mediante una única red, servicios IP, ATM, FR…
  - Debe poder ofrecer garantías de QoS equivalentes a los proporcionados por estas redes.
    - Por ejemplo, ATM proporciona requisitos QoS estrictos que DiffServ no es capaz de cumplir por sí solo.
      - DiffServ funcionará satisfactoriamente si la red no está congestionada.
    - Combinando DiffServ y la formación de LSPs basados en restricciones (TE-MPLS) se pueden garantizar requisitos QoS estrictos para cada clase de tráfico: **DiffServ-TE**.

Soporte MPLS de IntServ

- MPLS puede incorporar IntServ:
  - Asociación de flujos IntServ a LSPs (o túneles MPLS).
  - LSPs vs. Flujos IntServ:
    - Asociación de etiquetas a flujos.
  - Durante el establecimiento del LSP (por ej. mediante RSVP-TE) se reservan recursos en los LSRs.
  - Si se emplea RSVP-TE se puede emplear el mismo proceso tanto para la reserva de recursos IntServ como para la distribución de etiquetas MPLS.
    - RSVP-TE usa DoD con control ordenado para establecer etiquetas.
  - La etiqueta MPLS evita la consulta a la cabecera IP, por lo que IntServ sobre MPLS es más rápido, pero...
  - IntServ NO es una solución escalable.

Soporte MPLS de DiffServ

- DiffServ se desarrolló para proveer Calidad de Servicio (QoS – *Quality of Service*).
  - Divide el tráfico en un número pequeño de clases y se reparten recursos para cada una de estas clases.
  - La clase a la que pertenece un paquete se indica en su cabecera IP en el campo DSCP (*DiffServ Code Point*): 6 bits.
  - DSCP determina el comportamiento QoS de un paquete: PHB (*Per-Hop Behavior*).
  - PHB se expresa en términos del comportamiento del paquete en planificadores y prioridades de marcado/descarte.

Soporte MPLS de DiffServ

- MPLS basa sus decisiones de reenvío en la cabecera MPLS únicamente.
  - Se asignan los 3 bits EXP de la cabecera MPLS para transportar la información DiffServ en MPLS → Ya se tiene el PHB en la cabecera MPLS.
- Pero… DSCP es un campo de 6 bits y EXP es un campo de 3 bits.
  - DSCP puede codificar 64 valores, mientras que EXP solo 8.
  - Dos posibles soluciones.
- SOLUCIÓN 1:
  - Para redes que soportan menos de 8 PHBs.
  - Se mapea el DSCP en el campo EXP (o el operador emplea los bits EXP para realizar DiffServ), lo que comportará indicar un PHB.
  - Durante el reenvío:
    - La etiqueta indica donde enviar el paquete.
    - Los bits EXP determinan el PHB.
  - Los bits EXP no se señalizan al establecer el LSP.
  - Los LSPs para los que el PHB se deduce de los bits EXP se llaman E-LSPs (*EXP-LSPs*).

Soporte MPLS de DiffServ

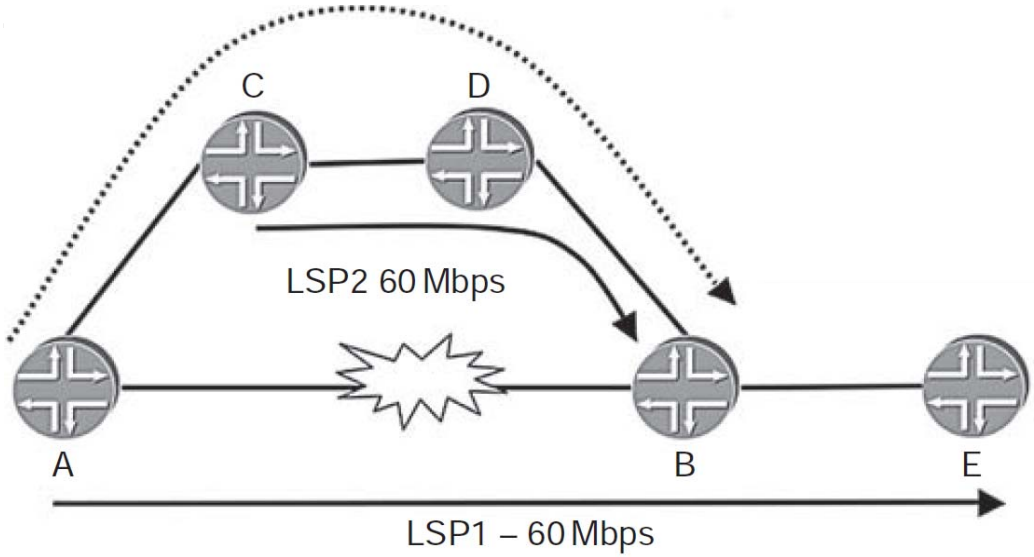
- SOLUCIÓN 2:
  - Para redes que soportan más de 8 PHBs → Los bits EXP no son suficientes para transportar la información necesaria para distinguir entre PHBs.
  - Adicionalmente, se emplea la etiqueta para indicar PHBs:
  - Puesto que el PHB indica:
    - El comportamiento en los planificadores.
    - La política de descarte.
  - Durante el reenvío se emplea:
    - La etiqueta para indicar el reenvío Y el comportamiento en los planificadores.
    - El campo EXP se emplea para indicar únicamente la política de descarte.
  - El PHB se indica tanto en la etiqueta como en el campo EXP.
    - Puesto que la etiqueta implica un PHB esta información requiere ser acordada durante el establecimiento del LSP.
  - Los LSPs que emplean la etiqueta para indicar el PHB se llaman L-LSPs (*Label-LSPs*).
  - Un L-LSP puede:
    - Transportar paquetes con un único PHB.
    - Transportar paquetes con varios PHBs que tienen el mismo comportamiento en los planificadores pero se diferencian en sus prioridades de descarte.

Soporte MPLS de DiffServ: E-LSP vs. L-LSP

E-LSP	L-LSP
Los bits EXP determinan el PHB	La etiqueta o la etiqueta junto con los bits EXP determinan el PHB
Pueden transportar tráfico de hasta 8 PHBs diferentes en un único LSP	Pueden transportar un único PHB por cada LSP o varios PHBs con el mismo comportamiento en los planificadores y diferentes prioridades de descarte
Uso conservador de etiquetas y de estado, puesto que la etiqueta se emplea solo para reenviar tráfico	Usa más etiquetas y hay que mantener más posibles estados, porque la etiqueta se emplea tanto para el reenvío de tráfico como para el tratamiento en los planificadores
No se requiere señalización para transmitir la información de PHB	Se requiere transmitir información de PHB cuando se establece el LSP
Se pueden soportar hasta 8 PHBs cuando solo se emplean E-LSPs. Se pueden usar junto con L-LSPs cuando se requieren más PHBs	Se puede soportar cualquier número de PHBs en la red

Protección y DiffServ

- La protección es cara: no todos los LSPs la requieren.
- Ejemplo:
  - Todos los enlaces son de 100 Mbps.
  - Hay dos LSPs, cada uno con una reserva de 60 Mbps:
    - LSP1: A-B-E (no requiere protección puesto que tolera pérdidas el servicio).
    - LSP2: C-D-B.
    - Protección del enlace A-B se provee por medio de A-C-D-B.
  - ¿Qué ocurre si cae el enlace A-B?
    - Se envían 120 Mbps por los enlaces C-D y D-B.
    - Se pierde tráfico de LSP1 y LSP2, pese a que LSP1 no requiere protección.
    - A LSP2 le afecta un fallo en LSP1
  - Marcado de paquetes de LSP1 como preferible para el descarte.
    - Marcado DiffServ conforme se conmuta al camino de *backup*.
    - El campo EXP de la etiqueta indica la política de descarte.



Bibliografía

- I. Minei y J. Lucek, "*MPLS-Enabled Applications*", John Wiley & Sons, 3rd Ed, 2011.
- E. Osborne y A. Simha, "*Traffic Engineering with MPLS*", Cisco Press, 2002.
- L. De Ghein, "*MPLS Fundamentals*", Cisco Press, 2007.
- RFC 4090, "*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*", 2005.