Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

PROYECTO FINAL DE CARRERA

Estudio de la inclusión del sistema PCE en redes GMPLS

Autor: Alberto de Marcos García
Director: Jaume Comellas Colomé

Barcelona

Índice

1. INTRODUCCIÓN

En este capítulo se da una visión histórica sobre la evolución de las redes de telecomunicación desde el nacimiento de IP hasta las actuales redes ópticas, y se conocen las motivaciones que llevaron a la IETF al desarrollo de los estándares MPLS y GMPLS, así como sus ventajas a la hora de gestionar dichas redes.

1.1 IP sobre ATM

Uno de los principales factores de éxito de Internet ha sido la aceptación del protocolo IP como estándar para todo tipo de aplicaciones y servicios. El origen de IP se sitúa en 1981, año en que la agencia estadounidense DARPA publicó la especificación de dicho protocolo en el RFC-791, y en 1983 fue implantado en la red ARPANET, precursora de la actual Internet. A mediados de la década de los 90, IP empezó a ganar terreno como protocolo de red ante otras arquitecturas en uso como: *IPX*, *SNA*, *AppleTalk*, etc. y los proveedores de servicios (NSP *Network Service Provider*) desplegaron las primeras redes troncales IP, construidas con líneas dedicadas T1/E1 y T3/E3.

Posteriormente, el boom de Internet generó un déficit de ancho de banda que provocó la saturación de estas redes. Los operadores vieron entonces la necesidad de integrar el creciente tráfico IP (nivel 3) sobre las nuevas redes ATM (nivel 2). De esta manera se trataba de combinar la rentabilidad y la eficacia de los conmutadores ATM con la capacidad de control de los routers IP. Dicho de otra manera, proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión.

La solución de superponer IP sobre ATM proporciona mayores velocidades y la posibilidad de implementar soluciones de ingeniería de tráfico sobre los circuitos virtuales ATM (PVCs). Sin embargo, este modelo tiene también sus inconvenientes. Por un lado, hay que gestionar dos redes diferentes, una red lógica IP superpuesta sobre una infraestructura ATM, lo que supone un mayor coste para los NSPs. Por otro lado, inconvenientes de carácter técnico, como el *overhead* que conllevan los datagramas IP sobre las celdas ATM (reduciendo el ancho de banda disponible), o el crecimiento exponencial de rutas al aumentar el número de nodos en una topología de red mallada.

1.2 Conmutación IP

A finales de los 90 varios fabricantes desarrollaron nuevas técnicas con el objetivo de realizar una integración de niveles de forma efectiva y evitar así los inconvenientes derivados de la solución IP/ATM. Estas soluciones se conocen como “conmutación multinivel” (*multilayer switching*) o “conmutación IP” (*IP switching*). Ejemplos de estas tecnologías privadas son: *Tag Switching* de Cisco, *Aggregate Route-Base IP Switching (ARIS)* de IBM, *IP Navigator* de Ascend/Lucent, *IP Switching* de Ipsilon Networks, y *Cell Switching Router (CSR)* de Toshiba. [24]

Todas las técnicas de conmutación multinivel se basan en dos conceptos básicos comunes:

- La separación entre los planos de control (*routing* y señalización) y de datos (*forwarding*).

- El sistema de etiquetas para el envío de datos.

El problema que presentaban estas tecnologías privadas era la falta de interoperatividad entre productos de diferentes fabricantes. [3] Además, la mayoría de ellas necesitaban ATM como transporte, y no podían operar sobre otras infraestructuras de transmisión (Frame Relay, PPP, SONET/SDH y Ethernet).

1.3 La convergencia de niveles: MPLS

Por todo ello, se quería obtener un estándar unificado e interoperativo que pudiera funcionar sobre cualquier sistema de transporte de datos (incluso mixto). En este punto el IETF propone el estándar MPLS como solución común a la conmutación IP multinivel. MPLS son las siglas de "*Multi-Protocol Label Switching*".

El IETF (*Internet Engineering Task Force*) es una organización internacional abierta de normalización, creada en EEUU en 1986, que tiene como objetivo contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad, etc. [Wikipedia]

MPLS [RFC 3031] es un estándar que integra sin discontinuidades los niveles OSI 2 (enlace) y 3 (red), combinando eficazmente la simplicidad y rapidez del *switching* con las funciones de control del *routing*, gracias a la conmutación por etiqueta.

MPLS es aplicable en todas las redes de conmutación de paquetes, celdas y/o *frames*. La conmutación ya no se realiza en base a los identificadores propios de cada *host* (dirección IP, MAC, VPI/VCI, etc.), sino a etiquetas que definen el camino a seguir por un cierto tráfico.

No obstante, actualmente no es posible eliminar totalmente el encaminamiento tradicional. [24] Algunos motivos son:

- No es probable que a corto plazo los sistemas finales (*hosts*) implementen MPLS. Se seguirá utilizando encaminamiento convencional para enviar el tráfico a un primer dispositivo de red (que sí soporte conmutación por etiqueta).

- Las etiquetas MPLS solo tienen un significado local. Representan caminos o rutas, pero no identifican a un nodo en concreto. Por tanto es imposible mantener vínculos globales entre etiquetas y nodos en todo Internet.

- El filtrado de paquetes en cortafuegos (*firewalls*) de acceso a redes privadas corporativas requiere examinar la información original de la cabecera de los paquetes.

1.4 Evolución de MPLS al dominio óptico: GMPLS

Con el paso de los años y la creciente tecnología óptica se entendió que la solución que ofrecía MPLS en las redes de conmutación de paquetes podía extenderse a otros tipos de conmutación en el dominio óptico: tiempo, longitud de onda y espacio. Por ello, el IETF realiza una extensión del estándar MPLS dando origen a GMPLS [RFC 3945]. GMPLS son las siglas de "*Generalized Multi-Protocol Label Switching*".

Los dispositivos GMPLS son capaces de gestionar cinco tipos de interfaces [1] [41]:

- Conmutación de paquetes: basada en el contenido de la cabecera del paquete (nivel 3).

- Conmutación de celdas y/o *frames*: basada en el contenido de la cabecera de la celda o *frame* (nivel 2).

- Conmutación en tiempo (TDM): basada en el *slot* temporal de un ciclo repetitivo en el que se reciben los datos. Es la base funcional de SDH/SONET.

- Conmutación de longitud de onda (DWDM): basada en la longitud de onda en la que se reciben los datos.

- Conmutación en el espacio: basada en la fibra o puerto por la que se reciben los datos.

En síntesis, GMPLS es una evolución del plano de control de MPLS hacia un Plano de Control Común que simplifica el funcionamiento y mantenimiento de una red multicapa con cualquier sistema de transporte (incluso mixto), asegurando la interoperabilidad entre los dispositivos de alto nivel (routers) y los de bajo nivel (OXC, PXC, etc.).

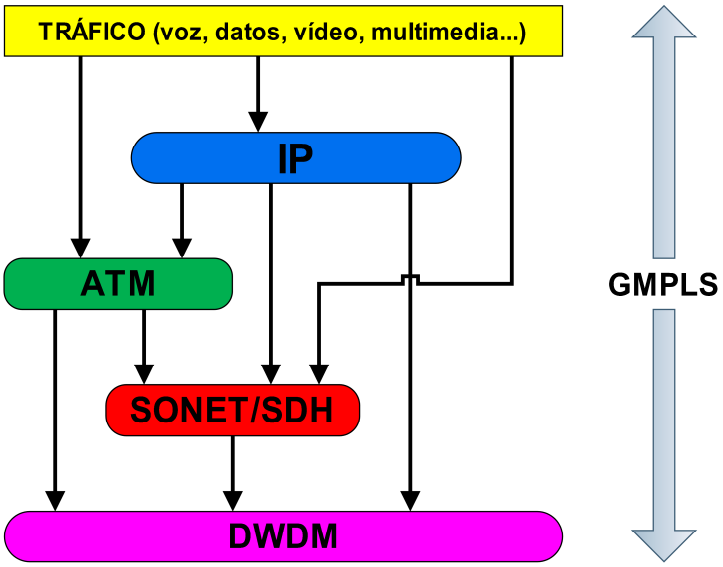

Figura 1.1: Modelo de transmisión sobre fibra óptica

GMPLS puede verse, por tanto, como un integrador de tecnologías, permitiendo la transmisión de información entre los diferentes tipos de redes y unificando el control del tráfico. [9]

El principal beneficio que GMPLS ofrece actualmente a los ISPs es una rápida provisión de servicios de cualquier tipo, en cualquier momento, a cualquier destino, con cualquier calidad de servicio, con cualquier grado de disponibilidad y con un coste operativo muy bajo.

2. MPLS

En este capítulo se ofrece una visión global de MPLS: arquitectura y elementos de red, funcionamiento básico de una transmisión y aplicaciones actuales.

2.1 Arquitectura MPLS y elementos de red

Forwarding Equivalence Class

Una *Forwarding Equivalence Class* (FEC) define el grupo o conjunto de paquetes que se envían por el mismo camino a través de una red MPLS y reciben el mismo trato en el encaminamiento, aun cuando sus destinos finales sean diferentes.

Etiqueta

Una etiqueta es un campo de 20 bits que establece una correspondencia entre el tráfico y una FEC específica. Esta etiqueta es transportada en la cabecera MPLS de un paquete e identifica el camino por el que debe ser enviado. La asignación de dicha cabecera se realiza en función de la dirección de destino, el tipo de servicio, la pertenencia a una red privada VPN y/o siguiendo otros criterios.

Cabecera MPLS

Según las especificaciones de la IETF, MPLS debe funcionar sobre cualquier tipo de transporte: PPP, Ethernet, ATM, Frame Relay, etc. Por ello, si el

protocolo de transporte tiene ya un campo específico para etiquetas (VPI/VCI en ATM y DLCI en Frame Relay), se utilizan estos campos nativos para las etiquetas MPLS. En caso contrario (enlaces PPP o Ethernet) se emplea una cabecera genérica MPLS.

La cabecera genérica MPLS es un campo de 32 bits que se añade a un paquete, entre las cabeceras de nivel 2 y 3, y que define una serie de características y requisitos para su transmisión en una red MPLS.

Su estructura [3] es la siguiente:

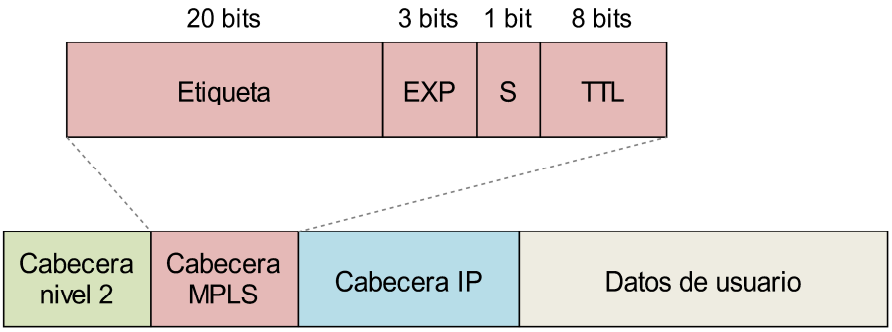

Figura 2.1: Estructura de la cabecera genérica MPLS

- **Etiqueta:** Es el valor actual de la etiqueta MPLS.

- **EXP:** Anteriormente llamado CoS (*Class of Service*). Este campo posibilita la diferenciación de distintos tipos de tráficos con el objetivo de mejorar el rendimiento de un tipo de tráfico respecto a otros.

- **Stack:** También llamado BoS (*Bottom of Stack*). Con este bit se soporta la jerarquización de etiquetas (*Label Stacking*). Un valor positivo indica que existe más de una cabecera MPLS en un mismo paquete. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre

otra, de modo que un router MPLS tratará siempre la que esté más arriba en la pila.

- **TTL:** Este campo es copiado directamente de la cabecera IP y proporciona la funcionalidad de tiempo de vida del paquete o TTL (*Time To Live*) típica de IP, la cual permite mitigar el efecto de posibles bucles en la red decrementando el valor inicial en una unidad por cada salto o nodo por el que pase el paquete.

Label Switch Router

Un *Label Switch Router* (LSR) es un router que soporta MPLS. Es capaz de recibir, procesar y enviar paquetes con etiqueta MPLS por un enlace de transmisión.

En una red MPLS existen dos tipos de LSR:

- *Label Edge Routers* (LER): situados en los extremos de la red MPLS, son el nexo con las redes tradicionales (Ethernet, Frame Relay, ATM…).

- *Intermediate LSR*: situados dentro de la red MPLS, reciben y transmiten los paquetes etiquetados por los enlaces correspondientes.

Un LSR es capaz de realizar tres operaciones básicas: añadir (*push*), eliminar (*pop*) e intercambiar (*swap*) etiquetas MPLS. La acción de añadir la primera etiqueta a un paquete se denomina imposición. Y la acción de eliminar la última etiqueta de un paquete se denomina disposición.

Label Switched Path

Un *Label Switched Path* (LSP) es un camino de tráfico específico a través de la red MPLS. Son unidireccionales por definición.

En el extremo inicial se sitúa el *Ingress* LSR, encargado de clasificar y etiquetar los paquetes, decidiendo qué paquete pertenece a cada FEC.

En el extremo final se sitúa el *Egress* LSR, quien elimina la etiqueta correspondiente a ese LSP.

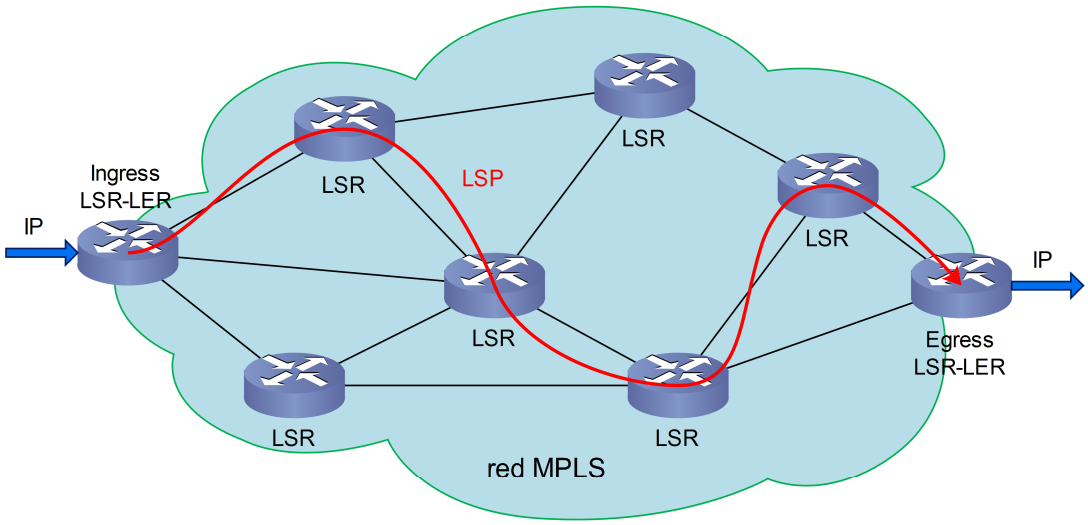

Figura 2.2: Esquema de una red MPLS

El *Ingress* LSR de un LSP no tiene porque ser necesariamente un LER (el primero en etiquetar el paquete). En este caso, añadirá una nueva etiqueta a la pila. Es lo que se denomina “Jerarquización de LSPs”, o LSPs anidados (un LSP dentro de otro LSP) y es posible gracias al *Label Stacking*.

Label Information Base

Una *Label Information Base* (LIB) es la tabla de encaminamiento de un LSR. Cada entrada de la tabla contiene un par {interface de entrada – etiqueta de entrada} y su correspondencia con otro par {etiqueta de salida – interface de salida}. También se conoce como *Label Forwarding Information Base* (LFIB).

2.2 Funcionamiento básico de transmisión

Cuando un paquete llega a una red MPLS, éste es examinado por el *Ingress* LSR-LER y asignado a una FEC en función de su dirección IP de destino y la QoS demandada. Asimismo el router añade la cabecera MPLS con la etiqueta que identifica el LSP por el que debe ser transmitido. A continuación envía el paquete al siguiente LSR.

Cada LSR intermedio identifica la etiqueta de entrada del paquete recibido, consulta su LIB, y la sustituye por otra nueva, de acuerdo con el sistema de intercambio de etiquetas. Finalmente envía el paquete al siguiente LSR del LSP.

El concepto de intercambio de etiquetas se denomina "*Label Swapping*", y está motivado por el hecho de que las etiquetas sólo tienen significado local.

Al llegar el paquete al *Egress* LSR-LER, éste elimina la cabecera MPLS y lo envía por routing convencional de acuerdo a la dirección IP de destino.

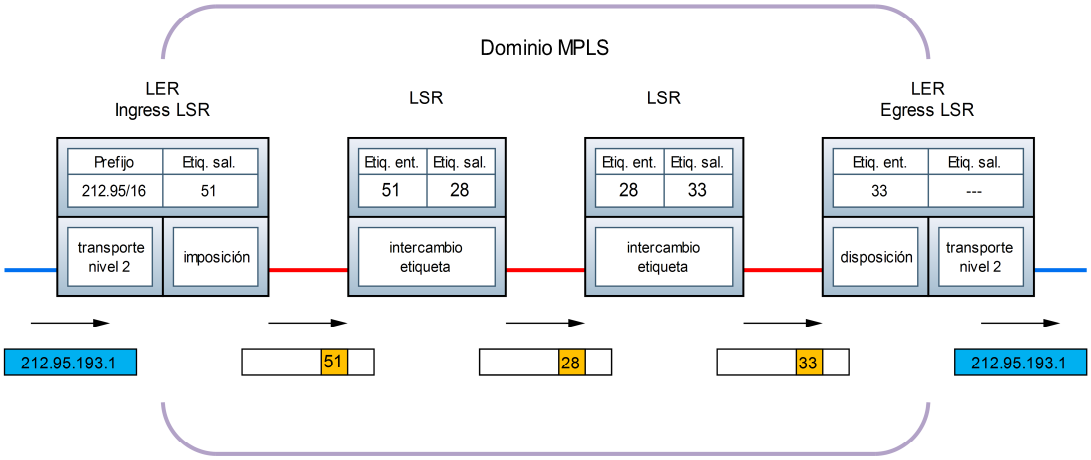

Figura 2.3: Ejemplo de envío de un paquete

Ventajas frente al routing convencional

En el encaminamiento IP tradicional, cada vez que un paquete llega a un router se examina la dirección de destino y otros parámetros de la cabecera. El criterio adoptado a la hora de tomar la decisión sobre el encaminamiento del paquete es elegir la ruta definida por el prefijo más largo (*Best Matching Prefix*) que se ajuste a su dirección. Pero esta operación resulta compleja y costosa en tiempo, que se incrementa en función de la longitud de la tabla de encaminamiento del router.

El encaminamiento en MPLS se simplifica. La elección de rutas se basa en una simple etiqueta que se añade a cada paquete que llega a una red MPLS. Nótese que en ningún momento de la transmisión se examina la cabecera IP del paquete; salvo en los LERs, que conectan la red tradicional con la red MPLS. El tratamiento de los paquetes por parte de los LSRs resulta mucho más sencillo y menos costoso que el método de Best Matching Prefix, lo que supone una mejora de rendimiento respecto al encaminamiento IP tradicional.

2.3 Aplicaciones de MPLS

Las principales aplicaciones [2] que actualmente ofrece MPLS son:

- Ingeniería de tráfico o TE (*Traffic Engineering*)
- Diferenciación de clases de servicio (CoS) o tráfico con diferentes calidades de servicio (QoS)
- Servicio de redes privadas virtuales (VPN)

2.3.1 INGENIERÍA DE TRÁFICO

Se entiende por ingeniería de tráfico el proceso de adaptar los flujos de tráfico a los recursos físicos de la red para optimizar su utilización, de manera que no haya algunos que estén sobrecargados (posibles cuellos de botella) mientras otros estén infrautilizados.

A principios de los 90 los métodos de control del tráfico eran bastante pobres. Considerando que los flujos de tráfico siguen la ruta más corta (con menos saltos) calculada por los algoritmos de encaminamiento tradicionales, cuando un tramo de la red se congestionaba el problema se resolvía a base de añadir más enlaces.

La ingeniería de tráfico consiste en trasladar parte del tráfico de los enlaces más congestionados a otros enlaces menos cargados, aunque estén fuera de la ruta con menos saltos.

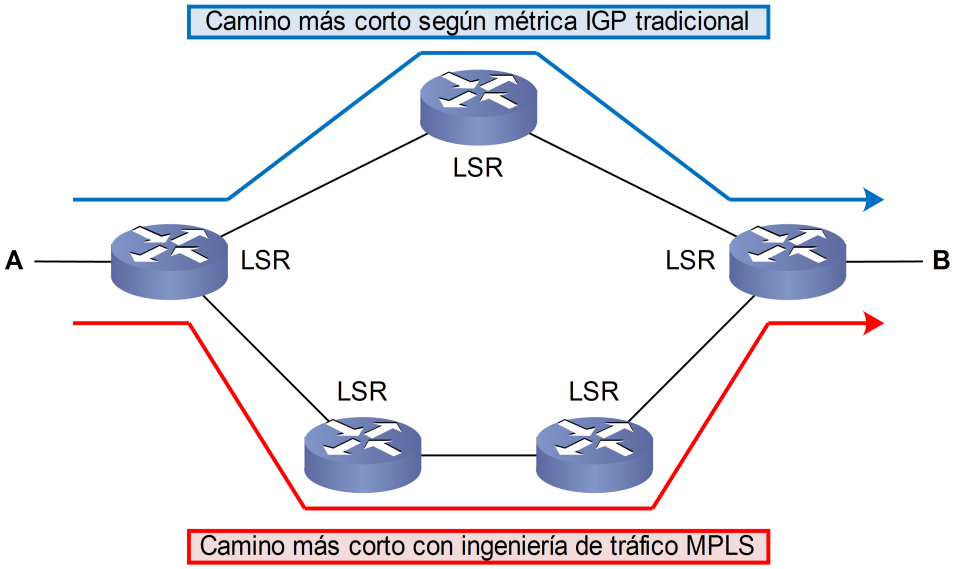

Figura 2.4: Ejemplo de comparación de rutas

En el ejemplo anterior, la ruta calculada entre A y B según la métrica tradicional es la que tiene solamente dos saltos. Pero es posible que un exceso de tráfico sobre esos enlaces haga aconsejable la elección del camino alternativo indicado con un salto más.

La ingeniería de tráfico MPLS [4] [27] [30] aplicada en una red permite:

- El establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP, evitando cuellos de botella o puntos de congestión conocidos.

- Un control preciso sobre el redireccionamiento del tráfico cuando una ruta sufre uno o más fallos.

- Un uso más eficiente del ancho de banda disponible de manera que algunos enlaces no se congestionen mientras otros permanecen infrautilizados.

- Maximizar el uso y la eficiencia de los dispositivos de la red.

- Mejorar las prestaciones de la red minimizando la pérdida de paquetes (*packet loss*), minimizando el retardo y maximizando el rendimiento.

- Hacer "encaminamiento restringido" (*constraint-based routing* CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales, con garantías concretas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

- La obtención de estadísticas de uso de los LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella.

La ventaja de la ingeniería de tráfico MPLS frente a otras opciones de optimización de recursos es que se puede aplicar directamente sobre una red IP, independientemente de la tecnología de transporte que utilice. Esto implica una mayor flexibilidad y menor coste en la planificación y gestión por parte del ISP, lo que se traduce en una mejor calidad de servicio para los clientes.

2.3.2 CLASES DE SERVICIO

Los usuarios de Internet demandan continuamente nuevas aplicaciones, y los servicios actualmente soportados tienen unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos. Para satisfacer estas necesidades de manera óptima, los ISPs necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISPs una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

MPLS está diseñado para poder cursar servicios diferenciados según el Modelo DiffServ del IETF [RFC 3270]. Este modelo permite clasificar todo el tráfico en un reducido número de clases de servicio (CoS) con diferentes prioridades [26] [29]. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el correo electrónico, el WWW, o la transferencia de ficheros (para los cuales el retardo no es crítico), de otras aplicaciones más dependientes del retardo y de la variación del mismo, como son las de video-sobre-demanda (streaming) y voz-sobre-IP (VoIP).

MPLS se adapta perfectamente a este modelo, ya que las etiquetas MPLS tienen el campo EXP para poder identificar la clase de servicio CoS de un determinado tráfico en el correspondiente LSP. EXP se hereda del campo ToS (*Type of Service*) de la cabecera IP, rebautizado en DiffServ como el octeto DS (*Differentiated Services field*).

Gracias a este sistema de clasificación, el tráfico que llega a un LSR puede ser asignado a diferentes colas de salida en función de su prioridad. Por otro lado, se pueden establecer múltiples LSPs en una misma ruta pero cada uno de ellos con distintas prestaciones y garantías.

2.3.3 REDES PRIVADAS VIRTUALES (VPNs)

Una red privada virtual (VPN) consiste en la extensión o emulación de una red privada sobre una infraestructura compartida de transporte, y que ofrece las mismas funcionalidades de red y de seguridad que se obtienen con una red privada física, de manera que cada VPN está aislada del resto. Por ejemplo, la VPN de una empresa multinacional permite la interconexión de diferentes localizaciones geográficas (sucursales) a través de Internet.

Históricamente, las VPNs más populares son las que ofrecen las redes Frame Relay y ATM mediante el establecimiento de circuitos privados virtuales (PVCs).
El principal inconveniente de este tipo de VPNs es que la configuración de las rutas es bastante laboriosa, al tener que establecer de manera individual cada PVC entre dos nodos, con la complejidad y el coste que esto supone al proveedor. Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, el hecho de añadir un nuevo emplazamiento supone reconfigurar todos los nodos y restablecer todos los PVCs.

Una solución más flexible y menos costosa que las anteriores es el *Tunneling*. Esta técnica permite establecer una asociación permanente entre dos localizaciones distantes mediante el encapsulado y envío del tráfico privado a través de una red pública IP (no conectiva), de modo que funcionalmente aparezcan conectados.

La principal ventaja del *tunneling* sobre los PVCs es la independencia del medio. Esto permite establecer una VPN sobre cualquier tipo de infraestructura de transmisión (incluso mixta).

Otra ventaja importante que ofrece es el (opcional) cifrado de la información de los paquetes IP mediante el estándar IPSec [RFC 2401]. Este cifrado se puede realizar tanto en dispositivos especializados (p. ej. cortafuegos), como en los propios routers de acceso del NSP a la red pública. El inconveniente del cifrado IPSec es que oculta las cabeceras de los paquetes originales, lo que conlleva que las opciones de CoS sean bastante limitadas, ya que la red no puede distinguir los flujos por aplicaciones para asignarles diferentes niveles de servicio.

A pesar de estas ventajas, el *tunneling* tiene el mismo inconveniente que los PVCs: el hecho de añadir una nueva localización supone reconfigurar individualmente todas las demás.

El concepto básico de esta problemática consiste en que estas VPNs están basadas en un modelo topológico superpuesto sobre la red física existente. Se utilizan conexiones extremo a extremo entre cada par de localizaciones de la VPN del cliente; lo que conlleva una baja flexibilidad en la provisión y gestión del servicio.

Con una arquitectura MPLS se eliminan estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor [3] [7] [9]. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre las distintas localizaciones de una VPN, lo que hay son conexiones locales a una "nube común" a la que solamente tienen acceso los miembros de una misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante LSPs dedicados.

Este modelo acoplado evita la complejidad de gestión de los túneles y PVCs ya que las nuevas conexiones y nuevos LSPs se establecen de forma sencilla y rápida por los protocolos MPLS. La creación de una nueva localización de una determinada VPN sólo afecta al LER que conecta dicha localización a la red global MPLS.

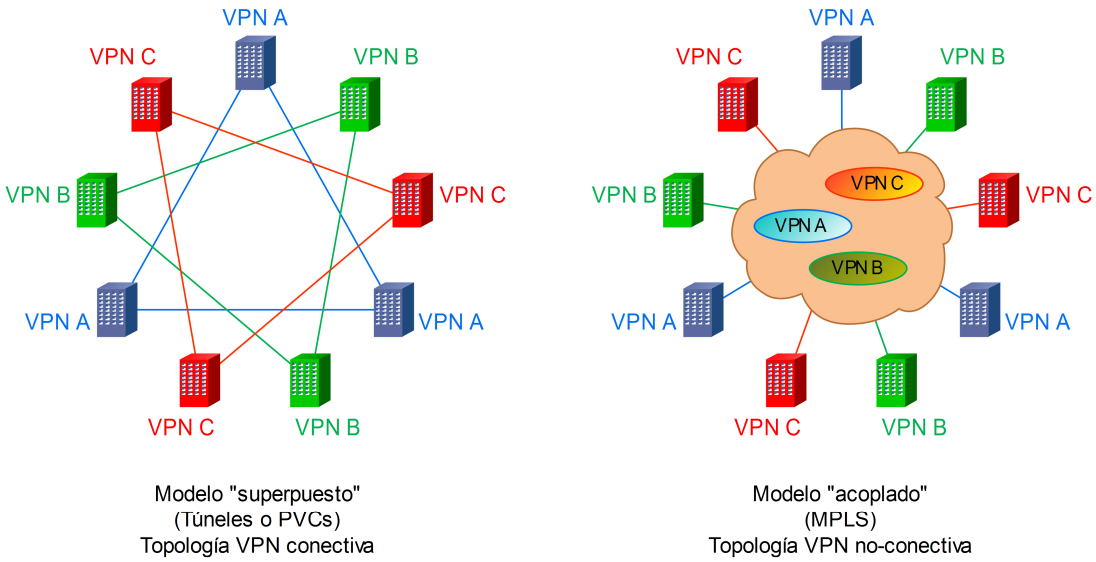

Figura 2.5: Modelo "superpuesto" vs. modelo "acoplado"

La encriptación de la información también se realiza mediante IPSec, pero a diferencia del *tunneling*, se pueden mantener garantías de CoS extremo a extremo. Gracias al campo EXP de las etiquetas MPLS, se pueden separar flujos de tráfico por aplicaciones en diferentes clases de servicio.

Otra importante ventaja de las VPNs establecidas mediante MPLS es que se pueden aplicar todas las técnicas de ingeniería de tráfico que ofrece el estándar.

Peer-to-peer VPN vs. Overlay VPN

MPLS puede aplicarse de acuerdo a dos modelos de servicio de VPN diferentes:

- Modelo VPN overlay
- Modelo VPN peer-to-peer

El grado de visibilidad de la red y el control administrativo de la misma son los rasgos diferenciales de ambos modelos.

Modelo VPN Overlay

El modelo overlay oculta al cliente los detalles de la red interna a través de dos planos de control diferentes con una interacción mínima entre ellos. Un plano opera en el núcleo de red del proveedor, y el otro en la red privada del cliente, de manera que el routing y la señalización de ambas partes son independientes. La conexión entre las dos redes se realiza mediante una interfaz pública denominada UNI (*User-to-Network Interface*) [9] que especifica

los protocolos de señalización entre la red privada del cliente y la red de transporte del proveedor. Se emplean dos dispositivos que son los UNI-C (*UNI-Customer side*) y UNI-N (*UNI-Network side*).

Este modelo impone fronteras de control administrativo ocultando los contenidos y características del núcleo, lo que puede ser muy interesante para los operadores que normalmente no quieren dar a conocer información sobre su red.

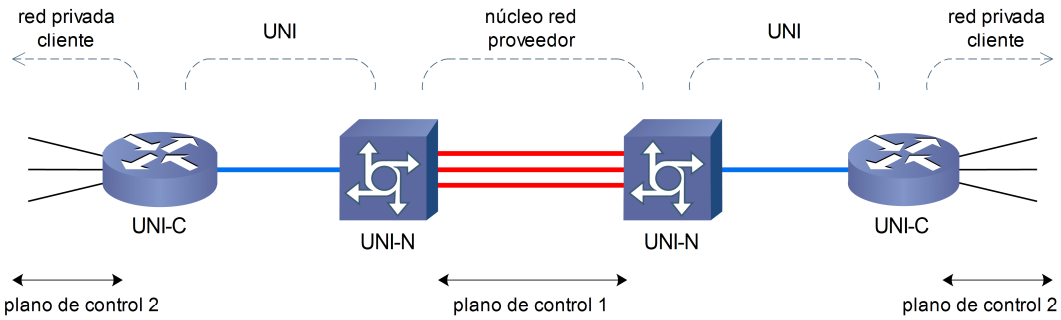

Figura 2.6: Modelo VPN overlay

Modelo VPN Peer-to-peer

En el modelo peer-to-peer, un único plano de control extiende un dominio administrativo compuesto por el núcleo de red del proveedor y la red privada del cliente. El routing y la señalización son comunes en ambas partes. Cada nodo de red posee información completa sobre el resto de nodos y sus capacidades de enlace, y ello facilita en gran medida las tareas de control y de ingeniería de tráfico.

Este modelo resulta mucho más adecuado para las funciones de red dentro del dominio de un proveedor de servicios o entre proveedores de servicios con protocolos compatibles, dado que permite mayor flexibilidad en la optimización de las labores de enrutamiento y aplicación de ingeniería de tráfico.

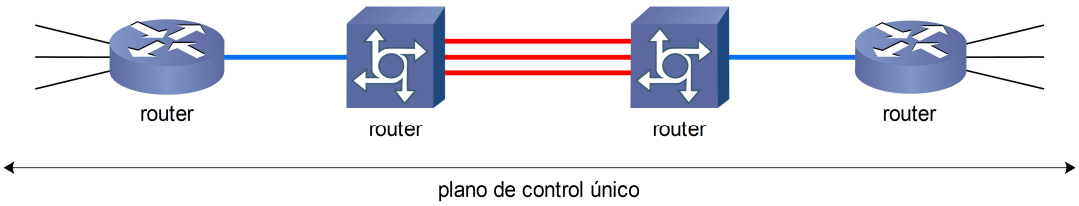

Figura 2.7: Modelo VPN peer-to-peer

3. GMPLS

Siendo GMPLS una extensión o evolución de MPLS, los conceptos explicados en el anterior capítulo sobre MPLS son también de aplicación en GMPLS, salvo en algunos aspectos. En este capítulo se explican las diferencias de GMPLS frente a MPLS, y se conocen nuevos conceptos.

3.1 Arquitectura GMPLS

Separación entre plano de datos y plano de control común

Tal y como se señala en el primer capítulo, en el estándar MPLS existe una separación entre el plano de datos y el plano de control. Esta separación se realiza de manera lógica sobre la misma red MPLS.

En GMPLS esta separación puede ser de manera lógica o física. En una separación lógica los tráficos de datos y de control viajan sobre la misma red. Una separación física significa que el control de la red de datos se realiza a través de otra red externa, que puede ser diferente a la primera. Por ejemplo una red de datos óptica con un plano de control sobre una red IP tradicional.

Etiqueta generalizada

Para ser capaz de soportar dispositivos con diferentes tipos de conmutación, GMPLS introduce el concepto de “etiqueta generalizada” (*generalized label)*. Este nuevo formato de etiqueta puede representar un paquete, una celda/*frame*, un *slot* de tiempo, una longitud de onda o una fibra.

La longitud de la etiqueta generalizada, así como su formato y contenido dependen del tipo de conmutación del enlace.

LSP bidireccional

En GMPLS todos los LSPs son bidireccionales, mientras que en MPLS son unidireccionales. En un LSP bidireccional, ambos sentidos deben tener las mismas características y parámetros de ingeniería de tráfico. Es útil en servicios como videoconferencia o VoIP.

Forwarding Adjacency

Aunque GMPLS soporte dispositivos con diferentes tipos de conmutación, un LSP "simple" solo puede establecerse entre nodos que tengan el mismo tipo de interfaz. Gracias al *Forwarding Adjacency* (FA) se pueden crear LSPs de nivel superior que permiten cambios de conmutación intermedios. Es la evolución de los LSPs anidados de MPLS.

Consiste en considerar un cierto LSP como si fuese un enlace virtual con sus propias características de ingeniería de tráfico. A este enlace se le denomina FA-LSP.

El procedimiento es sencillo: se crea un FA-LSP entre dos LSRs extremos y se informa a los demás nodos. A partir de aquí, el resto de LSRs pueden utilizar este FA-LSP como si fuese un enlace más de la red para establecer otros LSPs superiores, sin preocuparse de la gestión del mismo.

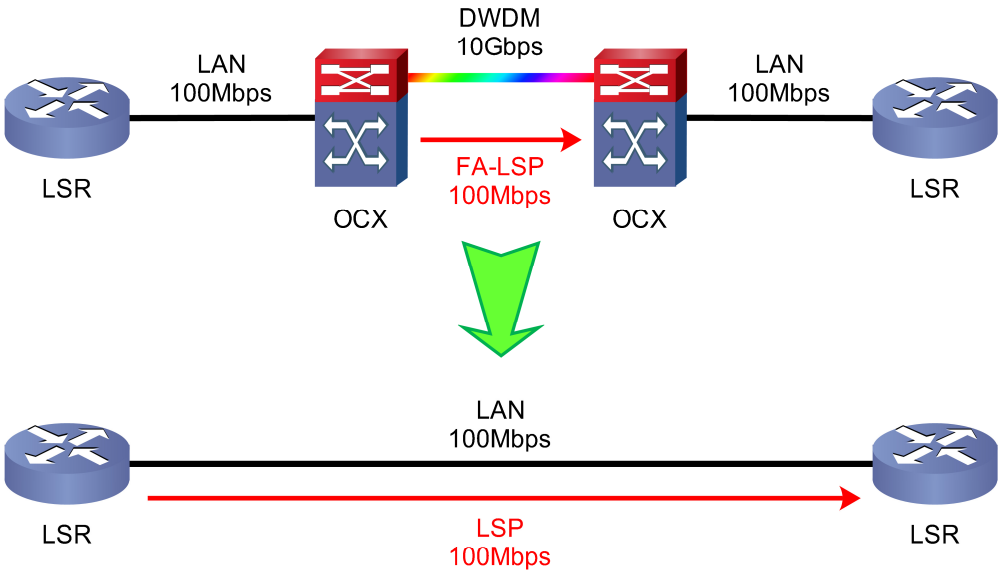

Figura 3.1: Ejemplo de un FA-LSP

Link Bundling

Es de suponer que en una red óptica se despliegan decenas de fibras paralelas entre dos nodos, cada una de ellas transportando centenares de longitudes de onda. El *Link Bundling* [37] permite agrupar todos estos enlaces con una misma señalización de manera que la información de control que se transmite entre los LSRs de la red se reduce considerablemente.

Las restricciones que impone el *Link Bundling* son:

1. Todos los links deben tener como inicio y final el mismo par de LSRs.

2. Todos los links deben tener el mismo tipo de conmutación.

3. Todos los links deben tener las mismas características de ingeniería de tráfico.

Inter-Área LSP

Los mecanismos de Ingeniería de Tráfico sobre redes MPLS/GMPLS fueron definidos originalmente para redes intra-área, esto es, limitados a una sola área. Actualmente, con las alianzas entre NSPs, se requiere extender esta tecnología para poder ofrecer garantías de QoS entre nodos situados en diferentes dominios administrativos que están conectados por los routers frontera ABR (*Area Border Router*). La IETF define una serie de extensiones para MPLS y GMPLS que permiten establecer LSPs inter-área que atraviesan varios dominios, con una estricta QoS y rigurosos parámetros TE [32].

Existen tres modos (que se pueden combinar) para crear un Inter-Área LSP:

- ***Contiguous* LSP:** en este modelo se establece un único Inter-Área LSP extremo a extremo que atraviesa varios dominios. La señalización es común para todo el LSP.

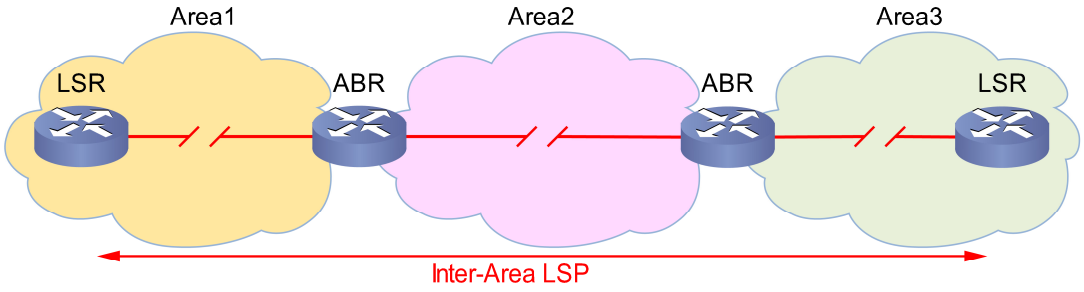

Figura 3.2: *Contiguous* LSP

- **LSP *Stitching*:** en este modelo se establece un intra-área LSP en cada dominio y finalmente se conectan o se “cosen” (*stitching*) en los ABRs. Para el plano de datos aparenta como un único LSP, pero en el plano de control cada segmento tiene su propia señalización.

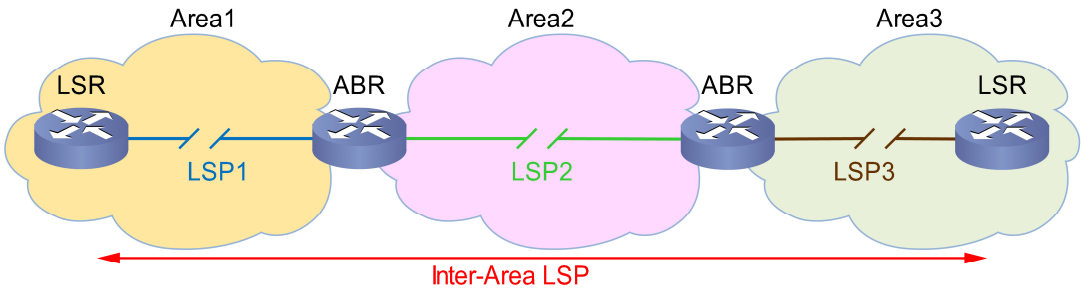

Figura 3.3: LSP S*titching*

- **LSP *Nesting***: en este modelo se utiliza un Intra-Área LSP de gran capacidad entre los ABRs de un dominio para transportar varios Inter-Área LSPs que comparten un mismo camino a través de dicho dominio. Esto se consigue gracias al *Forwarding Adjacency*.

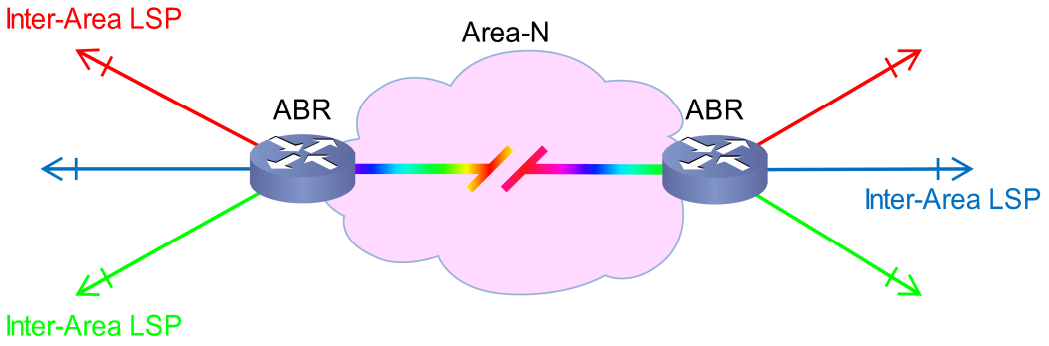

Figura 3.4: LSP *Nesting*

La elección depende de cuestiones administrativas (privacidad del operador) y técnicas (tipos de conmutación y transmisión).

Administración de red

Los proveedores de servicio necesitan monitorizar, configurar y controlar los recursos de sus redes que, por lo general, están diseminados por una geografía más o menos extensa. Para facilitar esta tarea se utiliza un sistema de administración de red o "*Network Management Service"* (NMS).

NMS es una combinación de herramientas hardware y aplicaciones software cuyos objetivos básicos son: operación, administración, mantenimiento y aprovisionamiento de la red.

- Operación: mantener el correcto funcionamiento de la red y monitorizar para detectar problemas.

- Administración: conocer los recursos de la red y asignarlos de manera adecuada.

- Mantenimiento: realizar reparaciones y actualizaciones. Por ejemplo, cuando un equipo debe ser reemplazado o cuando se añade uno nuevo.

- Aprovisionamiento: configurar los recursos para ofrecer un servicio solicitado.

La comunicación entre los dispositivos de la red y el NMS, en el caso GMPLS, se lleva a cabo mediante un protocolo definido por la IETF llamado "*Simple Network Management Protocol*" (SNMPv3) [RFC 3410].

Seguridad

El plano de control de GMPLS debe incluir mecanismos que prevengan o minimicen el riesgo de sufrir ataques que puedan comprometer tanto la información transmitida como la propia red. Son necesarios mecanismos de seguridad que proporcionen autenticación (identificación de dispositivos e integridad de los mensajes) y confidencialidad (imposibilidad de descifrar el contenido de los mensajes por parte de un atacante). Los propios protocolos GMPLS incluyen algunos de estos mecanismos, y adicionalmente se puede utilizar el estándar IPsec.

4. PROTOCOLOS MPLS/GMPLS

En este capítulo se dan a conocer los protocolos que conforman el plano de control de MPLS/GMPLS.

Una vez visto el mecanismo básico de envío de paquetes a través de una red MPLS, y conocido el concepto de ingeniería de tráfico, faltan ahora por concretar dos aspectos fundamentales:

1. Cómo se generan las rutas y las tablas de envío que establecen los LSPs.

2. Cómo se distribuye la información de etiquetas a los LSRs y se reservan los recursos físicos para una transmisión.

4.1 PROTOCOLOS DE ENCAMINAMIENTO (*routing protocols*)

Los protocolos de encaminamiento son los encargados de calcular la ruta entre dos puntos de red, con unas determinadas condiciones o restricciones (*constraints*) para la transmisión de un cierto tráfico. Para realizar este cálculo, es necesario conocer la topología y los recursos de la red.

Podemos diferenciar entre dos grupos de protocolos en función del conocimiento de los LSRs sobre la red:

Protocolos Vector-Distancia

En los protocolos de este tipo, ningún router tiene información completa sobre la topología de la red. Cada uno se comunica con los routers vecinos para intercambiar sus tablas de encaminamiento. El proceso se repite hasta que todas las tablas alcancen unos valores estables. La ruta se elige en función de

la distancia (saltos) hasta el destino. Este tipo de protocolos tienen el inconveniente de ser algo lentos, si bien es cierto que son sencillos de manejar y muy adecuados para redes compuestas por pocas máquinas.

Protocolos Enlace-Estado

En este caso, cada router posee información acerca de la totalidad de la topología y estado de la red. De esta manera, cada uno puede calcular el siguiente salto a cada posible nodo destino de acuerdo a su conocimiento sobre los enlaces (*Link State Database* LSD). La ruta final será entonces una colección de los mejores saltos posibles entre nodos.

Para dar soporte a MPLS/GMPLS y ofrecer la funcionalidad de ingeniería de tráfico, la IETF ha evolucionado dos protocolos del tipo enlace-estado desde sus especificaciones originales:

- *Open Shortest Path First – Traffic Engineering* OSPF-TE [RFC 3630]

- *Intermediate System to Intermediate System – Traffic Engineering* IS-IS-TE [RFC 3784]

OSPF-TE e IS-IS-TE son muy parecidos en cuanto a funcionamiento. Ambos utilizan el sistema de *Link State Advertisements* (LSA) para obtener la información sobre la red y construir la LSD. Los LSA son un conjunto de mensajes que envían los LSR por mecanismo de inundación (*flooding*) de manera periódica, que les permite darse a conocer unos a otros y descubrir nuevos nodos, intercambiar información sobre los enlaces, detectar fallos, etc. para tener actualizadas las LSD.

Para evitar problemas de escalado y un excesivo tráfico de *routing*, las redes se subdividen en áreas o zonas que limitan el *flooding*, donde cada LSR está

identificado de manera única por su dirección IP. A los que no poseen una dirección IP se les denomina "*unnumbered*", y se les asocia un identificador ID también único.

El siguiente paso es construir la tabla de encaminamiento o árbol de encaminamiento. Cada LSR calcula la ruta más corta (*shortest path*) hasta cualquier otro nodo (dentro de la misma área) aplicando el algoritmo de Dijkstra o una variante. Cuándo se produce una variación en la LSD, se recalcula sólo la parte de la tabla/árbol afectada por los cambios.

Para implementar la funcionalidad de Ingeniería de Tráfico, la IETF define posteriormente el concepto de "*Opaque* LSA". En ellos se incluye información como:

- Ancho de banda máximo, ancho de banda reservable y ancho de banda disponible o no-reservado de un enlace.

- Tipo(s) de conmutación de un nodo.

- *Protection Capability*: un enlace pueden proporcionar protección a la comunicación teniendo más de una conexión física entre dos puntos.

- *Shared Risk Link Groups* (SRLG): grupo de enlaces que comparten los mismos recursos físicos, donde un fallo puede afectar a todos.

Con toda esta información añadida, los LSRs pueden construir la *Traffic Engineering Database* (TED), que no es otra cosa que la tabla de encaminamiento con ingeniería de tráfico aplicada.

El adjetivo de "opaco" se entiende porque algunos LSRs de la red pueden no tener implementada la ingeniería de tráfico. Solo interpretan la parte original de los LSA, y realizan los cálculos de rutas omitiendo toda esta información extra.

La existencia de dos protocolos de encaminamiento se debe a una cuestión puramente comercial. Ambos son muy similares, aunque tengan pequeñas ventajas y desventajas. Actualmente los dos protocolos siguen en desarrollo, y ninguno de los dos ofrece un “plus” que le haga tomar ventaja.

4.2 PROTOCOLOS DE SEÑALIZACIÓN (*signaling protocols*)

Los protocolos de señalización son los encargados de:

- Distribuir la información de etiquetas entre los LSR.
- Reservar los recursos físicos de un LSP para poder realizar la transmisión.
- Mantener la conectividad de los enlaces y detectar y notificar errores para la restauración de un LSP.

La IETF ha definido dos de estos protocolos para MPLS y posteriormente extendidos a GMPLS, con soporte de Ingeniería de Tráfico.

- *Resource Reservation Protocol – Traffic Engineering* (RSVP-TE) [RFC 3209 y 3473]. Es la evolución del original RSVP [RFC 2205].
- *Constraint-Based Routing Label Distribution Protocol* (CR-LDP) [RFC 3212 y 3472]. Es la evolución del original LDP [RFC 3036].

Aunque en ciertos aspectos uno pueda ser más ventajoso que el otro, lo cierto es que ambos ofrecen, en general, las mismas funcionalidades y operabilidad. Al igual que ocurre con el *routing*, la existencia de dos protocolos de señalización se debe a una cuestión comercial. Durante el desarrollo e implantación de MPLS, los fabricantes han estado divididos en dos bandos,

optando por uno u otro protocolo. Con la evolución de MPLS hacia GMPLS la balanza se ha decantado hacia el lado de RSVP-TE debido sobretodo a la gran influencia de Cisco y Juniper que han optado por este protocolo. Es por ello que la IETF ha decidido no dar continuidad a CR-LDP.

4.2.1 RESOURCE RESERVATION PROTOCOL – TRAFFIC ENGINEERING

El funcionamiento de RSVP-TE se basa en operaciones de petición/respuesta entre los LSRs de una ruta.

Establecimiento de un LSP

El Ingress LSR envía un *Path Message* al Egress LSR donde le informa del tipo de LSP requerido y el tráfico a transmitir. En este mensaje se incluyen otros parámetros específicos como: registro de ruta, ruta explícita, enlaces coloreados, solicitud de etiqueta, sugerencia de etiqueta, restricción de etiqueta y LSP bidireccional.

El *Path Message* es enviado según la ruta definida por la tabla de encaminamiento de cada LSR que atraviesa. Cuando el mensaje alcanza el Egress LSR, éste calcula los recursos necesarios para la transmisión, y manda de vuelta un *Resv Message* con dicha información siguiendo la ruta inversa. Conforme este mensaje atraviesa los LSR intermedios, se van reservando los recursos indicados. Una vez el *Resv Message* llega al Ingress LSR, el LSP queda establecido.

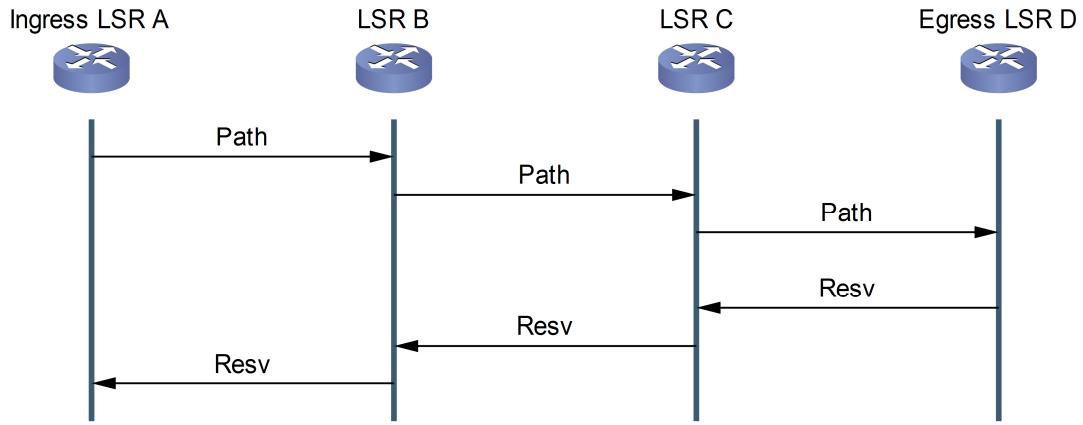

Figura 4.1: Flujo de señalización RSVP para el establecimiento de un LSP

En caso de que un nodo no pueda reservar los recursos necesarios, envía un *PathErr Message* hacia el Ingress LSR, y un *ResvErr Message* hacia el Egress LSR indicando el fallo. El proceso para establecer el LSP debe reiniciarse desde el principio, adoptando las medidas necesarias para evitar otro error (por ejemplo, elegir otra ruta).

En el caso de LSPs anidados, el establecimiento de los mismos debe producirse en orden inverso a la jerarquía, es decir, primero se debe crear el LSP de menor nivel, y hasta que no esté establecido, no se puede continuar con el siguiente.

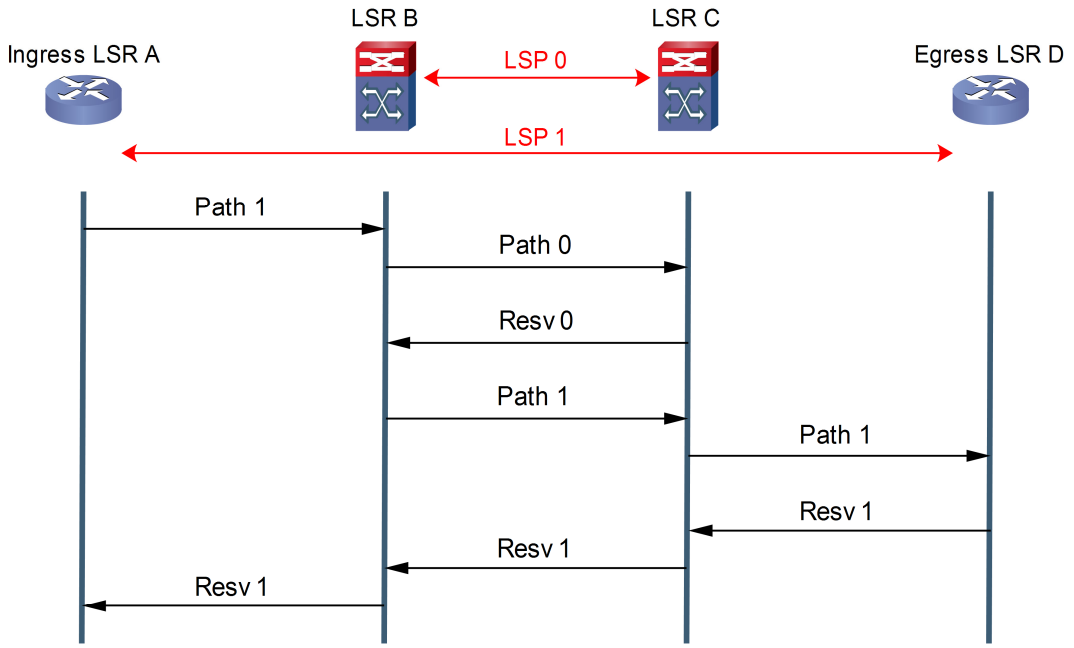

Figura 4.2: Establecimiento de LSPs anidados

Registro de ruta

De manera opcional se puede guardar un registro de los nodos y enlaces que atraviesa el *Path Message* incluyendo un *Record Route Object* (RRO). En ese caso, el *Resv Message* también debe llevarlo.

Este registro permite detectar bucles (*loops*), detectar cambios en los enlaces durante el tiempo de establecimiento de un LSP, o utilizarse para crear una ruta explícita.

Ruta explícita

Es posible establecer un LSP con un cierto tipo de tráfico en una ruta predeterminada por un administrador de la red. Esto se consigue incluyendo un *Explicit Route Object* (ERO) en el *Path Message*.

Esta ruta explícita puede ser estricta (*strict)*, donde se especifican todos los nodos intermedios, o relajada (*loose*), donde los LSR tienen una limitada capacidad de elección.

Enlaces “coloreados”

Otra manera de ejercer un control sobre la ruta de un LSP es mediante los enlaces “coloreados” (*coloured links*). Los enlaces de una red pueden tener tres colores cuyos significados son:

- Exclusión (*exclude any*): enlaces que no deben ser usados
- Inclusión de alguno(s) (*include any*): al menos uno debe ser usado
- Inclusión de todos (*include all*): todos deben ser usados

Estas restricciones se incluyen en un campo del *Path Message* denominado *Session Atribute Object*.

Solicitud y asignación de etiqueta

En la arquitectura MPLS/GMPLS, la decisión de asignar una determinada etiqueta a una cierta FEC es tomada por el LSR final de un enlace

(*downstream*). El Ingress LSR (*upstream*) realiza una petición al Egress LSR, y seguidamente éste informa al primero de la asignación realizada. A este procedimiento se le llama "*Downstream-on-Demand*".

La solicitud de etiqueta se realiza mediante el envío de un *Generalized-Label Request Object* [33] dentro del *Path Message*.

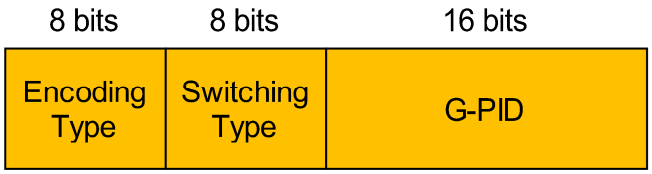

Figura 4.3: *Generalized-Label Request Object*

- ***Encoding Type*:** indica el tipo de tecnología a usar (Ethernet, Sonet, DWDM, etc.). Representa la naturaleza del LSP, pero no la naturaleza de los enlaces que componen el LSP.

- ***Switching Type*:** indica el tipo de conmutación de un enlace (paquete, celda, longitud de onda, etc.). Este campo es importante para aquellos enlaces y nodos que soporten varios tipos de conmutación. Por ejemplo, un nodo de tecnología DWDM puede conmutar una fibra entera o solamente unas determinadas longitudes de onda.

- **G-PID:** *Generalized-Payload Identifier*. Indica el tipo de tráfico a transmitir; más concretamente, el encapsulado de la información. Son válidos los códigos L3PID "*Standard Ethertype*" definidos por la IEEE así como nuevos códigos para tecnología óptica.

Encoding Type	*Meaning*
1	Packet
2	Ethernet
3	ANSI/ETSI PDH
4	Reserved
5	SDH ITU-T G.707 / SONET ANSI T1.105
6	Reserved
7	Digital wrapper
8	Lambda (photonic)
9	Fiber
10	Reserved
11	FiberChannel
12	G.709 ODUk (Digital Path)
13	G.709 Optical Channel
14	Waveband (Photonic)

Figura 4.4: GMPLS *Encoding Types*

Switching Type	*Meaning*
1	Packet-Switch Capable-1 (PSC-1)
2	Packet-Switch Capable-2 (PSC-2)
3	Packet-Switch Capable-3 (PSC-3)
4	Packet-Switch Capable-4 (PSC-4)
51	Layer-2 Switch Capable (L2SC)
100	Time-Division-Multiplex Capable (TDM)
150	Lambda-Switch Capable (LSC)
200	Fiber-Switch Capable (FSC)

Figura 4.5: GMPLS *Switching Types*

Una vez hecha la asignación, el Egress LSR envía un *Generalized-Label Object* dentro del *Resv Message* con la etiqueta asignada. A medida que el *Resv Object* pasa por los LSR intermedios, cada uno de ellos intercambia la etiqueta de acuerdo a su LIB, hasta llegar al Ingress LSR.

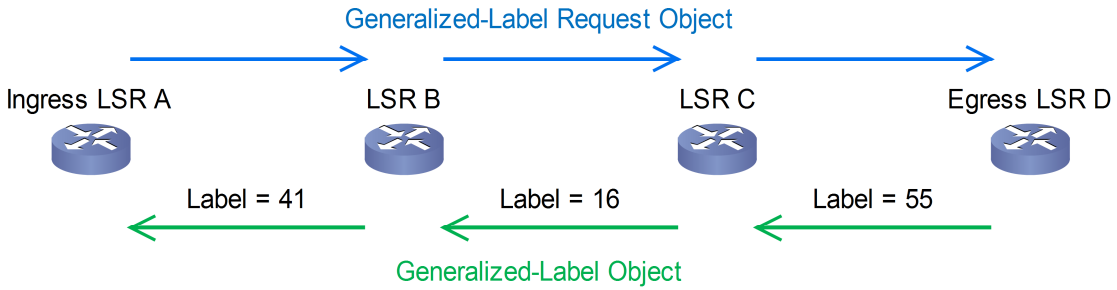

Figura 4.6: Solicitud y asignación de etiqueta

Sugerencia de etiqueta

En GMPLS, el Ingress LSR puede sugerir el uso de una etiqueta en concreto (*Suggested Label*), a la vez que realiza su configuración de hardware antes de recibir la respuesta del Egress LSR.

Se trata de un modo de optimización en aquellos dispositivos en que el tiempo de configuración es considerable, o en casos de fallo de algún enlace que requieran una restauración rápida del LSP. No obstante, si el Egress LSR decide utilizar una etiqueta distinta, el Ingress LSR deberá reconfigurarse.

El *Suggested Label Object* se incluye en el *Path Message*. En su envío, los LSR intermedios realizan el intercambio de esta etiqueta de acuerdo a su LIB.

Restricción de etiquetas

También existe la opción de que un LSR restrinja la elección de la etiqueta al siguiente LSR. Esto se consigue incluyendo en el *Path Message* listas y/o rangos de etiquetas de inclusión o exclusión bajo el nombre de *Label Set Object*. Cada LSR puede imponer sus restricciones al siguiente LSR, a la vez que está obligado a respetar las restricciones del nodo anterior.

La restricción de etiqueta puede ser necesaria en, al menos, cuatro casos en el dominio óptico:

- Un nodo sea capaz de recibir y transmitir únicamente un pequeño grupo de longitudes de onda

- Un nodo no tenga capacidad de conversión de longitudes de onda, de manera que sea necesaria la misma longitud de onda en sus enlaces.

- Limitar las conversiones de longitud de onda para reducir la distorsión de las señales ópticas.

- Los dos extremos de un enlace tengan en común solamente un determinado grupo de longitudes de onda.

LSP bidireccional

Con el objetivo de reducir tráfico de señalización, un LSP bidireccional puede ser establecido con un solo par de mensajes, *Path Message* y *Resv Message*.

Como si de un LSP unidireccional se tratase, el Ingress LSR envía un *Path Message* hacia el Egress LSR del modo en que se ha explicado anteriormente, pero ahora con un nuevo objeto dentro del mensaje, *Upstream Label Object*.

Esta etiqueta (*upstream label*) es la sugerida para el envío de tráfico en sentido contrario (de Egress a Ingress). Al tratarse de una sugerencia de etiqueta, los nodos intermedios pueden ir configurando su hardware. Si el Egress acepta la etiqueta, esta parte del LSP bidireccional queda establecida y ya se puede transmitir datos por ella.

En caso de que rechace la etiqueta, envía un *PathErr Message* de vuelta al Ingress LSR donde se incluye el objeto *Acceptable Label Set* que informa del conjunto de etiquetas que habrían sido aceptables. Este *Acceptable Label Set* tiene la misma forma que un *Label Set Object*, es decir, listas y/o rangos de etiquetas de inclusión o exclusión.

Finalización de un LSP

Cuando un Ingress LSR decide finalizar un LSP, envía un *PathTear Message* hacia el Egress LSR, de manera que se liberen todos los recursos asociados a dicho LSP.

Por otra parte, el Egress LSR también tiene capacidad para rescindir el LSP. Para ello envía un *ResvTear Message* hacia el Ingress LSR, de manera que todos los nodos que reciben este mensaje liberan los recursos. Finalmente el Ingress LSR tiene dos opciones: enviar de nuevo una petición de LSP mediante *Path Message*, o dar por finalizada la comunicación ya sea de manera formal enviando de vuelta un *PathTear* o no haciendo nada.

En el siguiente diagrama de flujo se muestran dos ejemplos de finalización de LSP por parte del Ingress LSR y por parte del Egress LSR.

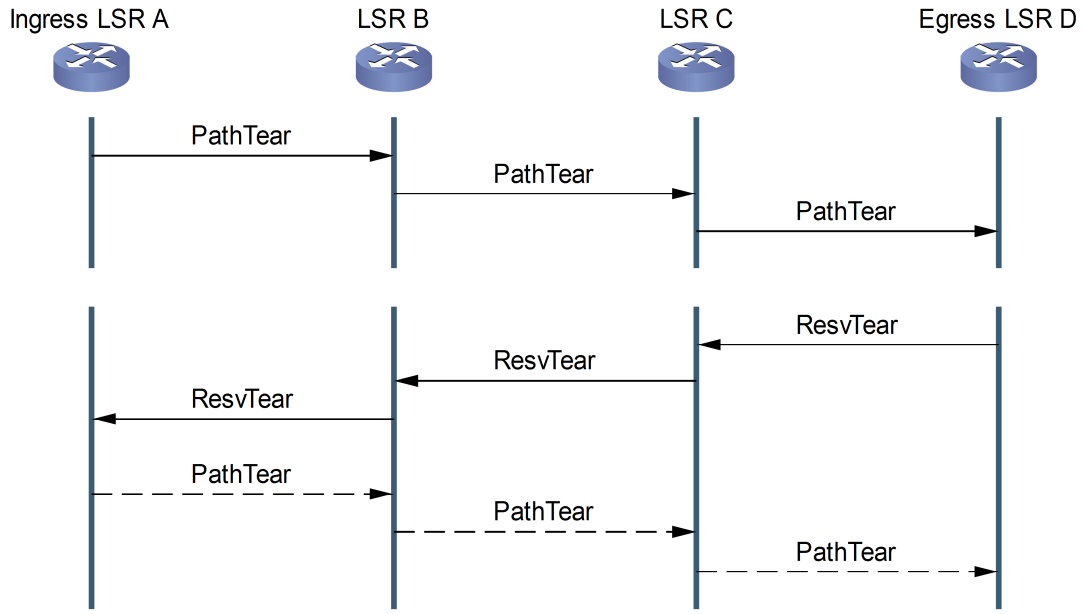

Figura 4.7: Finalización de un LSP

Gestión de errores

Un error se puede producir bien en el establecimiento de un LSP, bien durante la transmisión de datos.

En la fase de establecimiento, un LSR intermedio puede generar un error tanto en *Path Message* como en *Resv Message* por diversos motivos. Los más comunes son por una restricción de etiquetas o por una falta de recursos.

En un error de *Path Message*, el LSR en cuestión devuelve un *PathErr* de vuelta hacia el Ingress LSR. Si el LSR previo no puede solucionar el problema, se continúa con el envío del *PathErr* nodo a nodo. En caso de alcanzar el Ingress LSR, éste tiene la opción de modificar el *Path Message* y volverlo a intentar, o mandar un *PathTear* para cancelar el proceso.

En un error de *Resv Message*, el LSR devuelve un *ResvErr* hacia el Egress LSR. Del mismo modo que antes, el LSR posterior intentará resolver el problema. En caso contrario, el *ResvErr* alcanzará al Egress LSR. Éste puede modificar el *Resv Message* para intentarlo de nuevo, o mandar un *PathErr* directamente al Ingress LSR.

En la siguiente imagen se muestran las dos posibilidades mencionadas:

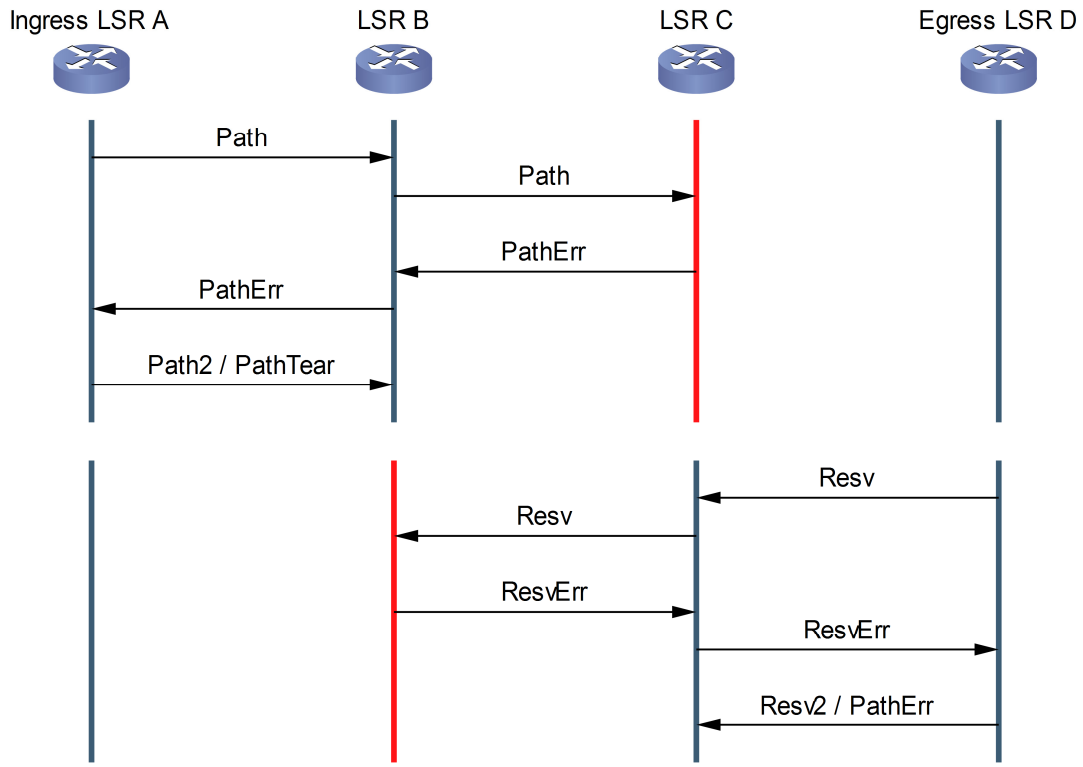

Figura 4.8: Gestión de errores en la fase de establecimiento

Durante la transmisión de datos por un LSP, cada par de nodos adyacentes intercambian entre sí un par de mensajes llamados *Hello* y *HelloAck*. Este intercambio se produce de manera periódica cada X tiempo (RFC 3209 recomienda 5 milisegundos) y sirve para mantener la conectividad de los

enlaces. Si no se recibe respuesta en un intervalo de 3'5X, el enlace se supone caído.

En este punto los dos LSR involucrados generan y envían los mensajes de *PathTear* (hacia el Egress LSR) y *PathErr* (hacia el Ingress LSR y que requerirá el posterior envío de *PathTear* en sentido contrario) que dan por cerrado el LSP.

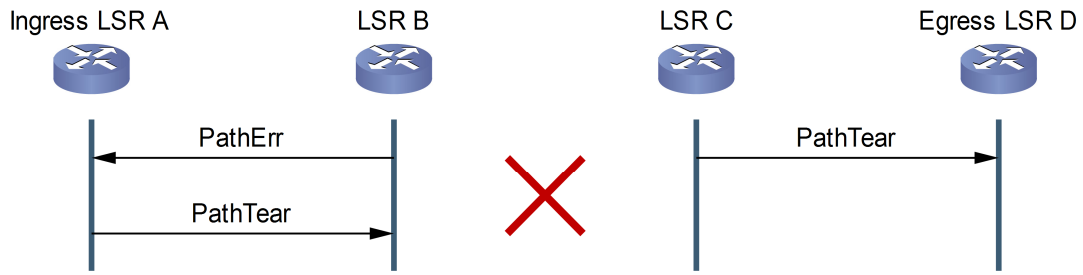

Figura 4.9: Notificación de la caída de un enlace

Extensión GMPLS en la notificación de errores

Cuando se emite un *PathErr Message*, el *Ingress LSR* debe responder con un *PathTear* con el cual ordena la liberación de los recursos asociados.

En GMPLS se añade una extensión que permite, ante la caída de un enlace, reducir tanto el tráfico de notificación de errores como el tiempo de liberación de recursos.

Se introduce una bandera llamada *Path State Removed Flag* en el *PathErr* con la cual se indica que los recursos ya han sido liberados, haciendo innecesario el envío del *PathTear*.

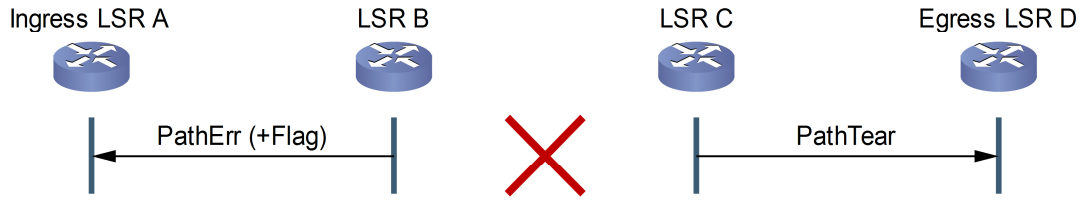

Figura 4.10: Notificación de errores con *Path State Removed Flag*

Extensión GMPLS en el restablecimiento de un LSP

En la propagación nodo a nodo de los *PathErr* y *PathTear* que señalan la caída de un enlace y la consiguiente rotura del LSP, cada LSR procesa estos mensajes y ello supone un coste de tiempo que puede ser muy perjudicial.
Con el objetivo de acelerar el restablecimiento del LSP, se introduce el *Notify Message*.

Este mensaje es enviado por los nodos que detectan el fallo directamente a los LSRs capaces de restablecer el LSP por otra ruta. Se incluye la dirección IP o identificador de dichos LSRs, de manera que los nodos intermedios lo transmiten sin procesarlo.

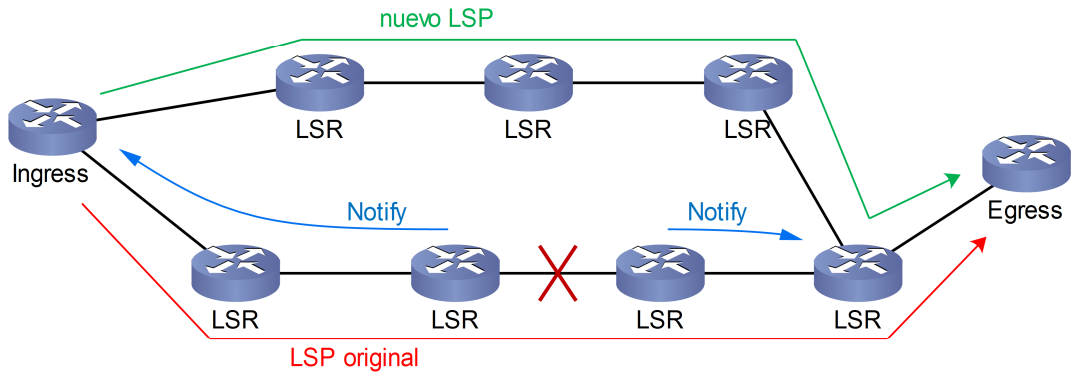

Figura 4.11: Reestablecimiento de LSP con *Notify Message*

4.3 LINK MANAGEMENT PROTOCOL (LMP)

Un canal o enlace es una conexión independiente entre un par de nodos adyacentes. Los canales de control son utilizados para el envío de mensajes de señalización y enrutamiento. Por los canales de datos se transmite la información propiamente dicha.

LMP [RFC 4204] es un protocolo sobre UDP, exclusivo de GMPLS, para la gestión y el mantenimiento de estos canales. No es un bloque esencial ni imprescindible en una red GMPLS, pero ofrece flexibilidad en redes con dispositivos de diferentes fabricantes que tienen distinta configuración, y facilita el mantenimiento a medida que la complejidad de la red se incrementa.

LMP consiste en una serie de procedimientos (opcionales) que proporcionan las siguientes funcionalidades:

Configuración dinámica del canal de control

El establecimiento de un canal de control entre un par de nodos adyacentes se inicia con el envío de un *Config Message* de un nodo al otro. Para ello es necesario conocer la dirección del nodo destino, ya sea mediante configuración manual o enviando el mensaje a la dirección multicast.

Es posible que los dos nodos inicien el procedimiento de configuración al mismo tiempo. Para evitar ambigüedades, el nodo con mayor identificador (comparación numérica) gana la contienda.

El *Config Message* transporta un conjunto de parámetros negociables y no-negociables para la configuración y posterior aplicación de LMP.

Si se aceptan todos los parámetros, el nodo destino responde con un *ConfigAck Message*. En caso contrario envía un *ConfigNack Message* indicando los parámetros no aceptados y proponiendo valores alternativos. Si el nodo origen puede aceptar estos valores, reenvía el *Config Message* modificado. Si no, es necesaria la intervención del operador.

Mantenimiento del canal de control

Una vez activo el canal de control, se utiliza un *Hello Message* para verificar la conectividad del canal.

Los dos nodos intercambian este mensaje de manera periódica. En caso de no recibir respuesta en un cierto tiempo, el canal se da por muerto. Tanto el intervalo de repetición (*Hello_Interval*) como el tiempo de muerte (*Hello_Dead_Interval*) se establecen en el *Config Message*.

Es aconsejable tener varios canales de control como medida de protección frente a posibles fallos. Si un canal se da por muerto, el tráfico se deriva a otro.

Finalización del canal de control

En caso de querer cerrar un canal de control por motivos administrativos, uno de los nodos podrá activar la *ControlChannelDown Flag*, presente en la cabecera de todos los paquetes LMP, y dejar de enviar el mensaje *Hello*. El nodo receptor responderá con un último *Hello Message* con la bandera activa, y dará el canal por cerrado.

Un canal de control solo puede ser cerrado en caso de que existan otro o más canales adicionales.

Estado degradado

Puede darse la situación de que no haya ningún canal de control activo. Esto no es motivo para cerrar los canales de datos. Se dice entonces que estos canales están en un "estado degradado" (*Degraded State)*.

No obstante, no se puede garantizar el mismo nivel de servicio para el presente tráfico de datos; y los protocolos de señalización y enrutamiento deberán informar al resto de nodos de que no se aceptan nuevas conexiones a través de ese enlace.

Verificación de conectividad de un enlace

LMP ofrece la posibilidad de verificar la conectividad de uno o varios canales de datos.

Cualquiera de los dos nodos puede iniciar el procedimiento enviando un *BeginVerify Message*, en el que se indican los enlaces a verificar y las características del test. El otro nodo puede aceptar el test (*BeginVerifyAck Message*) o denegarlo (*BeginVerifyNack Message*).

En caso afirmativo empieza la verificación enviando *Test Messages* por los canales de datos implicados. Esto conlleva que debe haber cierta opacidad en el transporte, puesto que es necesario examinar de algún modo el tráfico para poder reconocer estos mensajes.

Si el enlace es correcto, el nodo destino recibirá el *Test Message* y enviará, por canal de control, un *TestStatusSuccess Message* al nodo emisor.

Si el enlace está roto, el nodo destino no recibirá nada, y después de esperar un cierto tiempo (*Verify_Dead_Interval*) enviará un *TestStatusFailure Message*. Sea cual sea el resultado indicado (éxito o fallo), el nodo origen responderá con un *TestStatusAck Message* por el canal de control.

Para finalizar el test, se envía un *EndVerify Message* y se responde con un *EndVerifyAck Message* por parte de los nodos origen y destino, respectivamente.

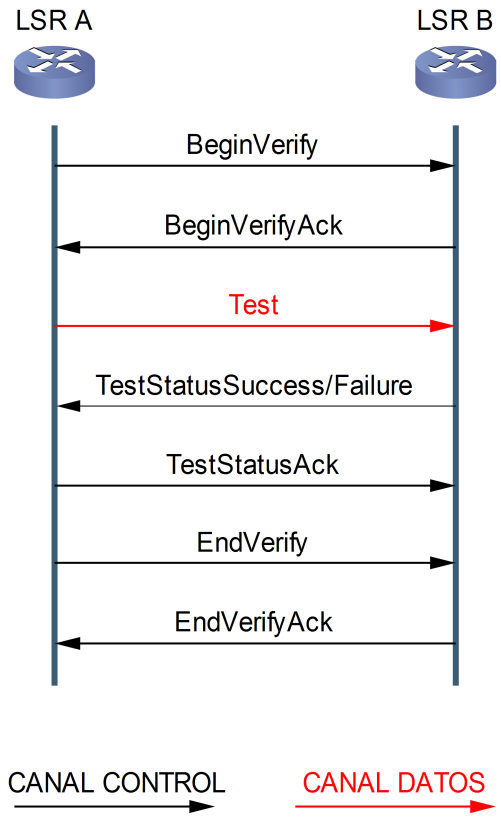

Figura 4.12: Procedimiento LMP para verificación de conectividad

Link Property Correlation

Una vez verificada la conectividad de los canales de datos, los nodos pueden intercambiar información sobre las características de dichos enlaces para activarlos o reconfigurarlos (mapeo de interfaces, características de ingeniería de tráfico, etc.), o también para establecer grupos de enlaces (*Link Bundling*).

Cualquiera de los dos nodos envía un *LinkSummary Message* con toda la información sobre características y parámetros de configuración. El nodo destino puede aceptar contestando con un *LinkSummaryAck Message*, o rechazar mediante un *LinkSummaryNack Message* indicando los elementos no aceptados y proponiendo valores alternativos.

Activación, desactivación y estado de los canales de datos

Finalmente, después de la configuración de los canales de datos, éstos pasan a ser activos. Es necesaria la notificación de activación (*Channel Activation* Indication) mediante el mensaje *ChannelStatus Message* y su respuesta *ChannelStatusAck Message*.

La desactivación se lleva a cabo del mismo modo (*Channel Deactivation Indication*).

Si un nodo desconoce el estado de un canal, le puede preguntar al otro nodo con un *ChannelStatusRequest Message*, que será respondido con un *ChannelStatusResponse Message.*

Notificación y Localización de errores

En algunas situaciones, como una red con dispositivos puramente ópticos (transparentes), el fallo de un canal de datos entre dos nodos es propagado a lo largo de todos los LSR en sentido *downstream* de un LSP (hacia el Egress LSR). Todos estos nodos detectan el error pero sin localizar el punto donde se ha producido; no es posible aplicar *Link Connectivity Verification* ya que los dispositivos no pueden analizar el tráfico.

Para evitar múltiples alarmas debidas a un mismo fallo, LMP proporciona un procedimiento de notificación y localización de errores a través del canal de control, aplicable a estas situaciones.

El procedimiento de detección es independiente. Existen varios mecanismos, aunque el más habitual es el *Loss of Light* (LOL).

Cuando un nodo $^{(n+3)}$ detecta un fallo en un canal, lo notifica al LSR anterior $^{(n+2)}$ mediante un *ChannelStatus Message*, que responderá con un *ChannelStatusAck Message*.

Ahora este LSR $^{(n+2)}$ analizará el enlace anterior en el LSP para ver si el error viene propagado o no. En caso afirmativo, enviará un *ChannelStatus Message* a su LSR superior $^{(n+1)}$ indicando fallo, y otro al nodo posterior $^{(n+2)}$ para informarle de que el canal entre ambos está correcto.

El proceso continua hasta que un LSR $^{(n)}$ observe que el canal anterior es correcto. Se ha localizado el fallo.

En caso de enlaces bidireccionales, el procedimiento se aplica para cada sentido del tráfico.

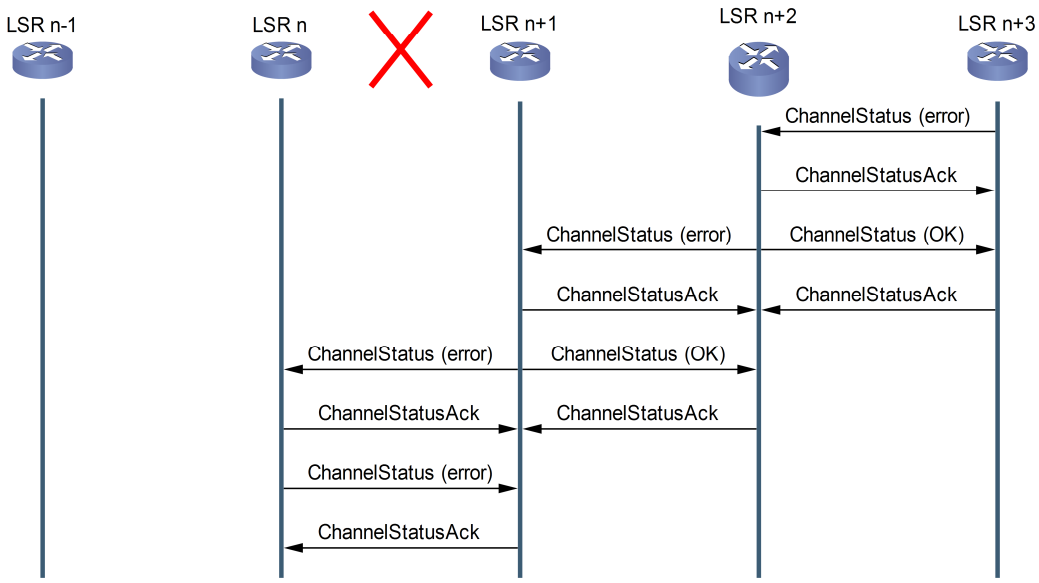

Figura 4.13: Notificación y localización de errores con LMP

5. PATH COMPUTATION ELEMENT

En este capítulo se define un nuevo elemento de las redes MPLS y GMPLS, el Path Computation Element (PCE). Definición y descripción, motivaciones para su uso y arquitectura de red. También se presenta el protocolo de comunicación PCECP.

5.1 Definición

La ingeniería de tráfico se fundamenta en un algoritmo que calcula la ruta óptima aplicando una serie de variables y restricciones (*Constaint-Based Path Computation*). En grandes redes multicapa, multidominio, y con diferentes áreas, esta operación puede resultar muy compleja e ineficiente para los dispositivos habituales.

Para ofrecer una solución a este inconveniente, la IETF define un nuevo elemento en las redes MPLS/GMPLS:

> "Un *Path Computation Element* (PCE) es una entidad capaz de calcular una ruta en base a la topología de la red, y bajo unas determinadas restricciones o criterios." [RFC 4655]

Cuando un LSR necesita calcular la ruta de un determinado LSP, envía una petición al PCE (*Path Computation Request*), que realiza el cálculo mediante un algoritmo y responde con el resultado obtenido.

5.2 Descripción funcional de un PCE

A la hora de calcular una ruta aplicando la ingeniería de tráfico, el PCE debe tomar en cuenta un conjunto de restricciones (*constraints*). Por un lado están

los recursos disponibles (malla de red, dispositivos, anchos de banda disponibles, enlaces coloreados, etc.) que están reflejados en la TED. Por otro lado, los requisitos demandados para el establecimiento de un LSP (ancho de banda solicitado, número de saltos máximo, retardo permitido, etc.) incluidos en el *Path Computation Request*, además de posibles restricciones por políticas administrativas.

Con todos estos parámetros, el PCE calcula la ruta aplicando un algoritmo de computación. Este algoritmo tiene dos fases. En la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una *Constrained-TED* temporal en la cual solo figuran los enlaces que satisfacen las condiciones. En la segunda fase se aplica el algoritmo matemático a esta nueva TED y se calcula la ruta óptima según el criterio de optimización deseado (ruta más corta, enlaces menos cargados, etc.).

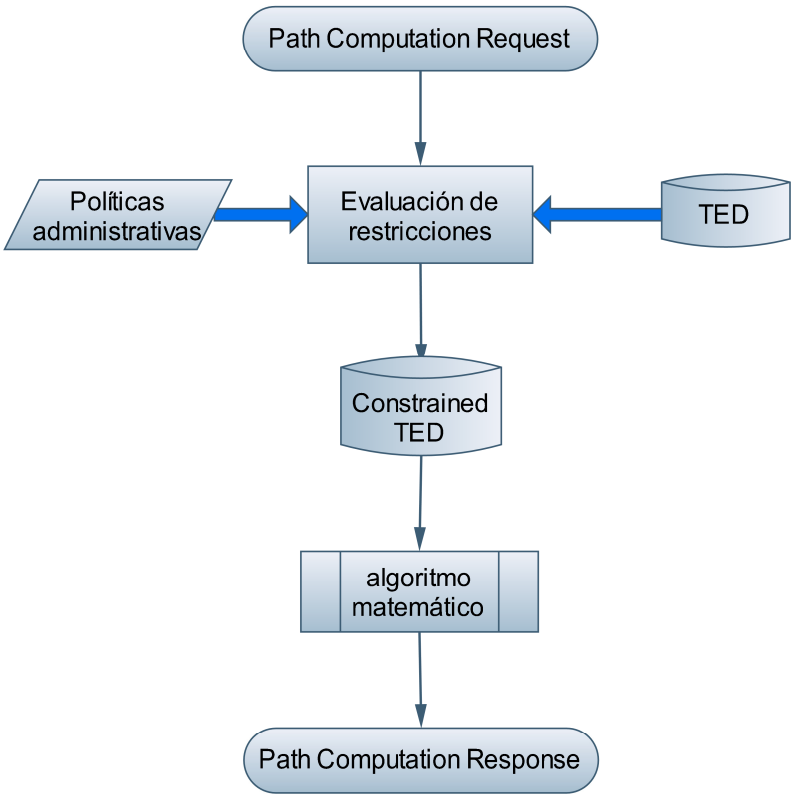

Figura 5.1: Diagrama de flujo de un PCE

5.3 Motivaciones para el uso de PCE

Son diferentes situaciones y escenarios los que sugieren el uso de una arquitectura de red basada en PCE.

Estas son algunas de ellas:

- **Capacidad de procesado limitada:** En ocasiones el cálculo de ruta puede resultar tan complejo que algunos LSRs no dispongan de la capacidad de procesado suficiente para realizar la operación, delegando esta tarea en el PCE, que sí tiene los recursos necesarios.

- **Visibilidad limitada:** En redes con diferentes dominios y/o capas, el conocimiento sobre la red de los LSRs se limita a su propia zona o capa, lo que no siempre puede garantizar la elección de la ruta óptima. La solución puede ser un PCE que tenga acceso a toda la topología de la red, o varios PCEs repartidos en las diferentes regiones y comunicados entre sí.

- **Ausencia de TED:** El mantenimiento de la TED requiere el uso de mucha memoria. Es por ello que en una red con ingeniería de tráfico aplicada puede haber nodos que no soporten las extensiones TE de los protocolos de encaminamiento. En este caso es necesario que la TED sea suministrada externamente por un PCE.

- **Ausencia de capacidad de enrutado:** En las redes ópticas son habituales los dispositivos que no disponen de plano de control o capacidad de *routing*, como pueden ser los conmutadores fotónicos (transparentes). El PCE es el encargado de enviar a estos nodos los comandos de configuración de hardware correspondientes.

- **Cálculo de rutas alternativas:** Un PCE puede ser usado para calcular rutas alternativas para el rápido restablecimiento de un LSP en caso de que la ruta principal falle.

5.4 Arquitectura PCE

Elementos de red

- **Path Computation Client PCC:** cualquier LSR de la red que requiere a un PCE el cálculo de una ruta de acuerdo al servicio solicitado.

- **Path Computation Element PCE:** aplicación que realiza el cálculo de ruta de acuerdo a una petición. Al finalizar el cálculo, el PCE envía la información de dicha ruta al PCC.

- **Traffic Engineering Database TED:** tabla de encaminamiento con ingeniería de tráfico aplicada que utiliza un PCE para realizar el cálculo de rutas.

- **Path Computation Request:** petición de cálculo de ruta que envía un PCC al PCE.

- **Path Computation Response:** respuesta que envía el PCE al PCC con la información de la ruta calculada.

Estructura PCE

La aplicación PCE puede estar implementada en cualquier nodo de la red (*composite*), o en un servidor dedicado (*external*). En este segundo caso, el

PCE “escucha” de manera pasiva toda la información del protocolo de encaminamiento que intercambian los LSR para mantener actualizada su TED.

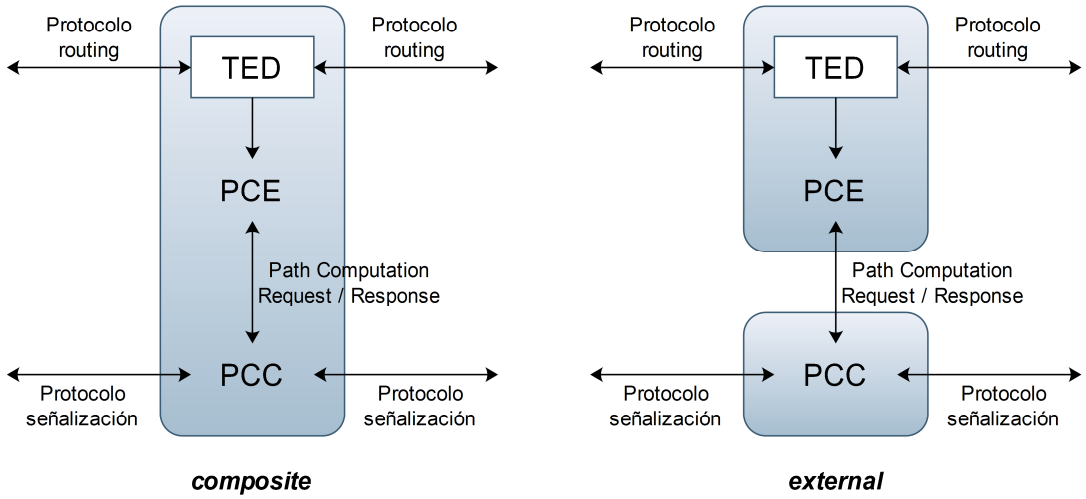

Figura 5.2: PCE *composite* y externo

Modelo de red

En un modelo centralizado, un único PCE es el que recibe las peticiones de todos los PCCs de un mismo dominio o área. Por seguridad, se puede designar un PCE alternativo (*backup*) que tome el control en caso de fallo del PCE primario.

En un modelo distribuido, múltiples PCEs residen en una misma área. Cada PCC puede estar ligado a un particular PCE, o puede ser libre de elegir entre varios. En el caso extremo, cada LSR tiene su propio PCE.

Descubrimiento y selección de los PCEs

En la práctica, un dominio o área contiene múltiples PCEs. Para conseguir que los PCCs seleccionen de manera efectiva los PCEs, esto es, elegir un PCE apropiado en base a sus capacidades y repartir eficientemente la carga de peticiones, un PCC debe conocer la localización y características de todos los PCEs dentro de su área, o incluso fuera del dominio si se permite.

El mecanismo de descubrimiento (PCE *discovery mechanism*) [43] debe permitir la localización de cada PCE, identificado por una dirección IP, en cada área, también identificada por un “Area_ID”.

También debe informar de las características y capacidades de cada PCE. Algunas de ellas son:

- Potencia de cálculo (parámetros estáticos).
- Priorización de las peticiones.
- Capacidad de cálculo sincronizado.
- Tamaño máximo del mensaje de petición.
- Número máximo de solicitudes de ruta en un mensaje de petición.
- Tipos de cálculo de ruta soportados: ruta más corta, ruta por los enlaces menos cargados, etc.
- Restricciones de ruta soportadas: máximo numero de saltos, máximo coste, etc.

- Restricciones de enlace soportadas: ancho de banda, latencia, etc.

- Capacidad de cálculo de LSP bidireccionales.

- Tipos de conmutación y capas soportados.

Tanto la localización como las características de los PCEs se pueden configurar manualmente en cada PCC. Pero esta opción puede ser muy laboriosa en grandes redes, y además no permite el descubrimiento de nuevos PCEs, la eliminación de los no-disponibles, o el cambio dinámico de las características de alguno de ellos.

En este contexto es de aplicación un mecanismo dinámico de auto-descubrimiento. Tanto si un PCE reside en un LSR como si está en un servidor externo, la manera más sencilla y efectiva de darse a conocer es mediante el sistema de inundación (*flooding*).

Se añade además un sistema de temporización que permite a un PCC monitorizar la conectividad con el PCE y detectar fallos en la comunicación entre ambos.

Para todo ello, la IETF define una serie de extensiones en los *Link State Advertisements* (LSA) de los protocolos de encaminamiento OSPF-TE e IS-IS-TE. [RFC 5088] y [RFC [5089].

Políticas administrativas

En una arquitectura PCE es posible establecer una serie de normas o reglas que afecten de manera directa al funcionamiento del sistema. Pueden aplicarse tanto en el mecanismo de cálculo de rutas (restricciones adicionales, rutas predefinidas), como en las comunicaciones entre PCEs y PCCs.

El “administrador de políticas” PM (*Policy Manager*) [RFC 5394], dentro del plano de administración de red, permite a una red llevar a cabo acciones de manera automática en respuesta a eventos o condiciones en base a unas reglas preestablecidas por el administrador.

Ejemplos de estas políticas son:

- Un PCE puede rechazar una petición en base a la identidad del PCC solicitante.

- Un PCE puede aplicar condiciones añadidas en el cálculo de rutas (hora, día, tipo de servicio, cliente que solicita el servicio, etc.) que pueden incrementar o relajar las restricciones del cálculo.

- La existencia de rutas o partes de rutas predefinidas (en forma de ERO) para determinados servicios, pudiendo depender o no de varios factores, como por ejemplo la dirección de origen y/o de destino.

- Un PCE puede restringir y seleccionar la información sobre sus propias características que da a conocer a los demás PCC y PCE.

- La capacidad de un PCC para elegir un PCE u otro en función del servicio solicitado.

- La especificación de la información contenida en un *Path Computation Request*, es decir, las variables o restricciones (*constraints*) aplicables al cálculo de una ruta, así como el criterio de optimización a usar.

La administración de políticas es aplicable a todos los elementos de la red (PCCs y PCEs) de manera general o concreta en cada uno de ellos. El protocolo utilizado para la comunicación entre el PM y los PCCs/PCEs no está

especificado; algunas soluciones son: COPS (*Common Open Policy Service*), Diameter, o vía SOAP/XML (*Simple Object Access Protocol / Extensible Mark-up Language*).

Cálculo de ruta

El cálculo de una ruta puede realizarse de manera “única” o “múltiple”.

En el “cálculo único” (*single path computation*) un único PCE es el que calcula una determinada ruta dentro de un área (aunque haya más PCEs). En este caso, el Ingress LSR inicia el establecimiento del LSP con una ruta explícita estricta (*strict*-ERO) proporcionada por el PCE.

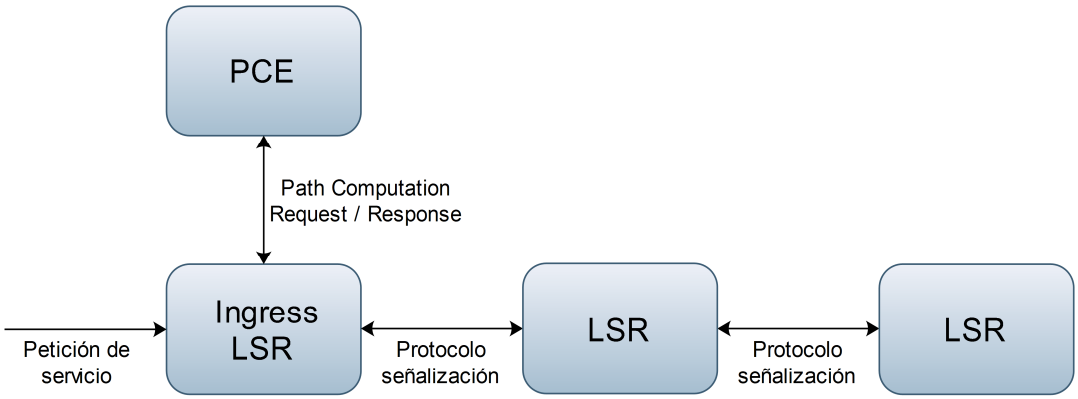

Figura 5.3: Cálculo único de ruta

En el “cálculo múltiple” (*multiple path computation*) varios PCEs son requeridos para calcular una ruta dentro de un área. Este escenario se presenta cuando la ruta no es explícita o es explícita “relajada” (*loose*-ERO).

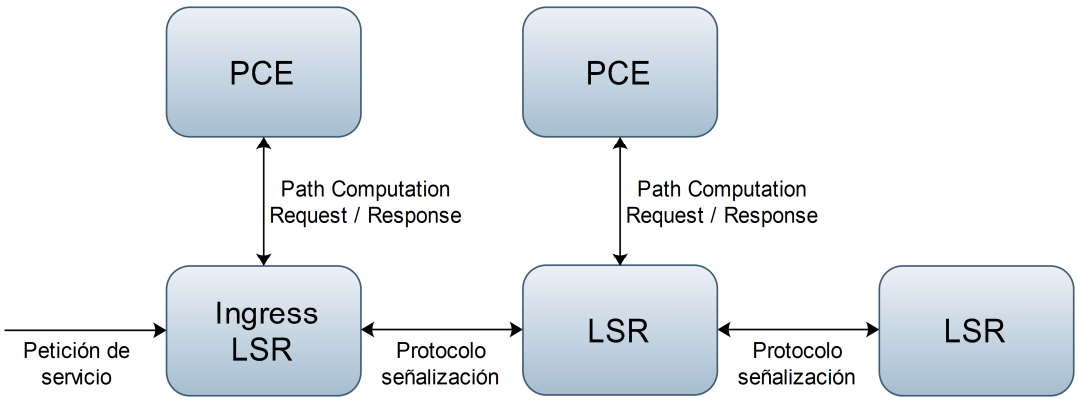

Figura 5.4: Cálculo múltiple de ruta

Sincronización

Uno o varios PCEs pueden ser capaces de calcular varias rutas de manera conjunta (sincronizada o coordinada). De esta manera se consiguen mejores resultados aunque aumenta el tiempo de cálculo y el volumen de tráfico entre ellos.

Las peticiones a procesar pueden provenir de varios PCCs, o de uno solo ya que en ocasiones es necesario disponer de varias rutas para soportar un mismo servicio (elevado volumen de tráfico o caminos alternativos).

En este último caso, el PCC envía una única petición indicando el conjunto de rutas requeridas para ser calculadas de forma sincronizada. También es posible que el PCC especifique que el cálculo puede ser no-sincronizado. Entonces los PCEs son libres de escoger entre un modo sincronizado o no-sincronizado.

Sistema *Online* y *Offline*

Existe un criterio para clasificar un sistema GMPLS-PCE en función de la capacidad de adaptación de los LSPs en forma de variabilidad de ancho de banda y re-enrutado.

En un sistema *Online*, los LSPs pueden ser modificados en ancho de banda o re-enrutados de acuerdo a las necesidades variables de un servicio, a la carga global de la red, o debido a fallos en algunos enlaces o dispositivos. Es necesario, obviamente, que el tiempo de cálculo sea mínimo.

Un sistema *Offline* no ofrece la adaptación dinámica de los LSPs, pero permite un mayor tiempo de cálculo que puede traducirse en la obtención de una ruta más óptima.

Comunicación Inter-PCE

Los PCE también pueden comunicarse entre ellos. Cuando un PCE no es capaz de proporcionar una ruta completa para un determinado servicio solicitado, necesita la cooperación de otro o más PCEs.

Un motivo puede ser el cálculo de una ruta que atraviesa varias áreas o dominios. También puede ser debido a que el PCE no tenga visibilidad en todas las capas de la red.

En estos casos, los PCEs intercambian información entre ellos mediante el denominado *PCE Communication Protocol* (PCECP). Este protocolo permite a un PCE operar como PCC y hacer peticiones de cálculo a otros PCEs.

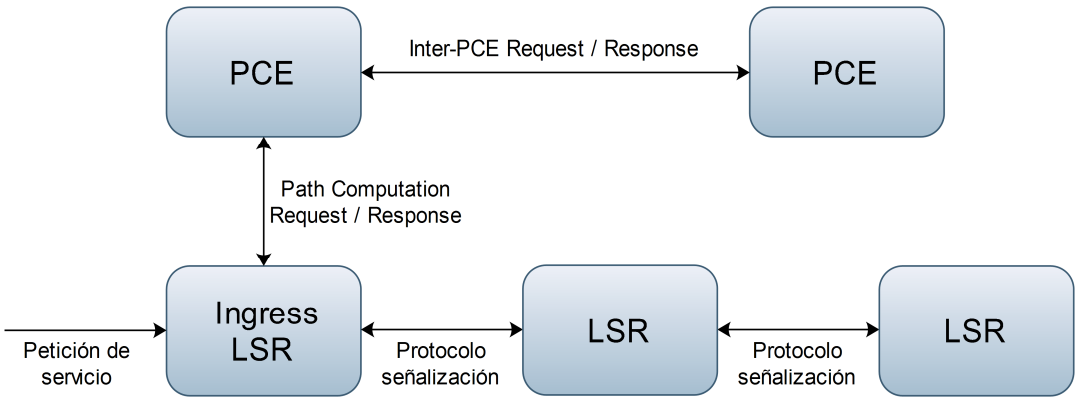

Figura 5.5: Cálculo de ruta con comunicación Inter-PCE

5.5 PCE Communication Protocol (PCECP)

Definición

PCECP [RFC 4657] es un protocolo petición/respuesta (*request/response*) que permite la comunicación PCC-PCE y PCE-PCE. En este segundo caso se considera que el PCE solicitante actúa como PCC.

Comunicación cliente-servidor

PCECP está basado en un modelo cliente-servidor en el cual un PCC puede enviar un mensaje de petición de cálculo a un PCE, y éste responde con otro mensaje que contiene la ruta calculada. Aunque hay casos donde un PCE puede enviar información no solicitada a un PCC.

Path Computation Request

El *Path Computation Request* debe incluir al menos el origen y el destino del LSP que se quiere establecer.

También debe soportar la inclusión de un grupo de una o más restricciones sobre el enlace, entre ellas el ancho de banda requerido u otras condiciones incluyentes/excluyentes sobre los recursos (número de saltos, retardo, tipo de conmutación, etc.)

Adicionalmente se pueden añadir parámetros de ingeniería de tráfico propios del protocolo de señalización (enlaces coloreados, RRO), y otras restricciones administrativas.

El PCC debe poder especificar el criterio de optimización para el cálculo de ruta por el PCE, siempre que éste último lo soporte. Este criterio puede ser:

- MCP (*Minimum Cost Path*): minimizar el coste de la ruta.

- MLP (*Minimum Load Path*): minimizar la carga de los enlaces más saturados.

- MBP (*Maximum residual Bandwidth Path*): maximizar el ancho de banda residual en los enlaces de la ruta.

También existen criterios de optimización cuando se solicita un cálculo sincronizado:

- MBC (*Minimize aggregate Bandwidth Consumption*): minimizar el consumo total de ancho de banda en los enlaces utilizados.

- MLL (*Minimize the Load of the most loaded Link*): minimizar la carga de los enlaces más saturados.

- MCC (*Minimize the Cumulative Cost of a set of paths*): minimizar el coste agregado sobre el conjunto de enlaces.

Puede haber casos en los que un solo enlace no pueda acomodar el ancho de banda requerido, pero la combinación de un conjunto de enlaces sí. A esta técnica se le llama "*Load-Balancing*". El PCC debe poder informar al PCE si lo permite o no. Además, puede señalar el número máximo de enlaces balanceados en un grupo y el ancho de banda mínimo para este grupo.

Path Computation Response

El *Path Computation Response* permite al PCE devolver la ruta calculada al PCC que la solicitó, siempre que la operación haya resultado exitosa.

En caso de ruta explícita (ERO), el mensaje debe especificar la combinación de enlaces (*strict, loose* o ambos) que componen dicha ruta. También puede incluir un conjunto de atributos de la ruta, como los costes métricos o el ancho de banda concreto de cada enlace en caso de *load-balancing*.

Cuando no se puede obtener una ruta que satisfaga las restricciones deseadas, o si se produce un error en el cálculo o no se puede llevar a cabo, el PCE debe enviar una respuesta negativa, indicando los motivos del fallo o avisando de las restricciones que no se pueden cumplir (susceptibles de ser relajadas para conseguir un resultado positivo).

Cancelación de peticiones pendientes

Un PCC que haya enviado una petición a un PCE pero que ya no desee respuesta, por ejemplo, porque ya no necesite establecer un LSP para un servicio en concreto, puede enviar un mensaje de cancelación al PCE.

Un PCE también puede cancelar una petición recibida debido a un estado de congestión.

Peticiones y respuestas múltiples

Es posible enviar varias peticiones de cálculo en un mismo mensaje. Estas pueden ser correladas (referentes al mismo servicio) o incorreladas (para diferentes servicios).

De la misma forma, un solo mensaje de respuesta puede contener diversas rutas calculadas, que pueden corresponder a una o diferentes peticiones, correladas o no, del mismo o diferentes mensajes de petición.

Cuando una petición de cálculo o una ruta calculada no puede incrustarse en un único mensaje debido a su tamaño, se envía en una secuencia de mensajes correlados. Esto se denomina “correlación continuada”.

El PCE debe informar al PCC del límite de peticiones por mensaje y el tamaño máximo de mensaje soportados. Esta información puede ser comunicada en el mecanismo de autodescubrimiento del PCE, o también mediante el intercambio de mensajes PCECP entre PCE y PCC.

Comunicación asíncrona y priorización de peticiones

Un PCC puede enviar peticiones sin necesidad de esperar la respuesta de otras anteriores.

El orden de las respuestas puede ser diferente al de las peticiones. Puede ocurrir cuando los mensajes de petición tienen diferentes prioridades. Esto implica que cada petición y respuesta deben estar relacionadas de manera unívoca e inequívoca.

Transporte

La definición de la IETF no especifica qué protocolo de transporte debe utilizarse en PCECP, pero aconseja el uso de alguno existente que posea control de congestión. Además debe ser único para asegurar la interoperabilidad, y no debe limitar el tamaño de los mensajes PCECP.

También debe proporcionar soporte para la inclusión de información referente a políticas administrativas.

Fiabilidad de la comunicación

PCECP debe soportar el intercambio seguro de paquetes. Esta condición puede ser inherente del propio protocolo o puede ser adquirida por la elección de un protocolo de transporte adecuado.

Concretamente, la detección y recuperación de mensajes perdidos debe ser lo suficientemente rápida para no afectar la operación del PCECP.

En algunos casos, como puede ser después de la caída de un enlace, un PCE puede saturarse debido a la recepción simultánea de un alto número de peticiones. Ante esta situación, el PCE debe informar de su estado y puede limitar la tasa de recepción de mensajes de petición.

PCECP o su protocolo de transporte deben ofrecer las siguientes funcionalidades:

- Detección y notificación de mensajes perdidos o corruptos.
- Retransmisión automática de mensajes perdidos.
- Control de mensajes duplicados.
- Control de congestion.
- Detección de fallo de comunicación PCECP.
- Distinción entre fallo de canal y fallo del otro dispositivo (PCE/PCC), después de la recuperación de la comunicación PCECP.

Seguridad de la comunicación

PCECP debe garantizar la seguridad de la comunicación entre entidades. Esta seguridad se traduce en mecanismos que protejan contra:

- La suplantación de identidad (*spoofing*) mediante un sistema de identificación y autenticación.
- La vulneración de confidencialidad (*snooping)* mediante técnicas de encriptación.

- Ataques de denegación de servicio (*DoS*). Ej. filtrado de paquetes, limitación de tráfico.

Una política administrativa puede impedir que un PCE proporcione rutas explícitas. Si un PCC solicita una ruta explícita cuando no está permitido, el PCE envía un mensaje de error y descarta la petición.

5.6 Inter-Área PCECP

El principal inconveniente que presenta el cálculo de ruta para un Inter-Área LSP es que los LSR tienen una visibilidad limitada a su área.

En una red MPLS/GMPLS sin PCE, la única posibilidad consiste en el cálculo por tramos, es decir, una sub-ruta en cada dominio donde el Ingress LSR determina el Ingress LSR del siguiente dominio (en el conjunto de los ABR). [31] Este método de cálculo se llama "*Per-Domain Path Computation Method*", y no garantiza la elección de la ruta inter-área óptima. Además puede presentar problemas de "*crankback*", esto es, si hay un fallo en un área o no dispone de recursos suficientes, debe utilizar un mecanismo de señalización para advertir al área anterior. Ésta última deberá recalcular su sub-ruta o, si no hay alternativa, derivar el problema a otra área anterior. Todo ello afecta a la estabilidad del plano de control y retrasa el establecimiento del LSP.

El cálculo de ruta inter-área es una de las principales aplicaciones de la arquitectura PCE. Todos los inconvenientes del método anterior quedan solventados gracias a los servicios de uno o más PCEs. En el "*Inter-Domain Path Computation Method*" la cooperación entre PCEs, donde cada uno de ellos cubre un área, permite la obtención de la ruta óptima.

La IETF añade una serie de extensiones [33] al protocolo PCECP para el cálculo de rutas inter-área:

Control de cruce de área

En el mensaje de petición se puede indicar si se permite o no atravesar otras áreas. En el caso de que origen y destino estén en el mismo dominio, puede ser que la ruta óptima sea inter-área, pero el operador prefiera escoger un camino intra-área.

También en el caso de que origen y destino estén en el mismo dominio, y se permita el cruce de área, el mensaje de respuesta puede indicar si la ruta calculada es inter-área o no.

Registro de área

A petición del PCC, el mensaje de respuesta puede contener la lista de áreas atravesadas y sus correspondientes segmentos que conforman el inter-área LSP, a no ser que la política de confidencialidad lo prohíba.

Lista de PCEs preferidos y PCEs utilizados

Un PCC puede indicar una lista de PCEs preferidos para ser usados, uno por área. En cada área, el PCE preferido debe ser elegido antes que otro.

Es necesario, pues, que los PCC tengan conocimiento de los PCEs en otras áreas. Esto se puede hacer mediante configuración manual, o permitiendo al mecanismo de autodescubrimiento de los PCE extenderse más allá de las fronteras de cada dominio.

El PCC también puede solicitar la lista de los PCEs que han intervenido en el cálculo, y qué segmento ha calculado cada uno de ellos.

Inclusión/Exclusión de áreas y/o ABRs

En algunas situaciones, el mensaje de petición puede contener una lista de áreas y/o ABRs que deben ser atravesados/excluidos por el LSP. Si alguna de estas restricciones impide la obtención de una ruta, el PCE comunicará el error al PCC.

Identificación de PCC

Una política administrativa puede obligar a los PCC a identificarse, enviando su dirección en los mensajes de petición. Con ello se puede controlar y restringir el uso de algunos PCEs por parte de determinados PCCs.

Prevención de bucles

El cálculo de una ruta inter-área con múltiples PCEs conlleva un riesgo de bucles en los mensajes de petición. Se debe definir un mecanismo para detectar y corregir estos bucles. Por ejemplo, un registro en el mensaje de petición de los PCEs recorridos.

6. ANÁLISIS DE SISTEMAS GMPLS-PCE

La arquitectura GMPLS y la aplicación PCE están en constante estudio y desarrollo. En este capítulo se dan a conocer algunos proyectos sobre estas redes y se hace una evaluación cualitativa de los sistemas GMPLS-PCE con respecto a las características de la ingeniería de tráfico.

6.1 Modelos de cooperación entre PCEs

En el contexto de las redes multicapa, la cooperación entre PCEs se realiza tradicionalmente con un modelo horizontal – *Horizontal Approach* (HA), en el cual cada PCE mantiene la visibilidad restringida a una sola capa. A la hora de hacer un cálculo de ruta, el PCE puede requerir la colaboración de otro PCE que controle una capa diferente.

El siguiente ejemplo presenta una red con dos capas según el modelo HA:

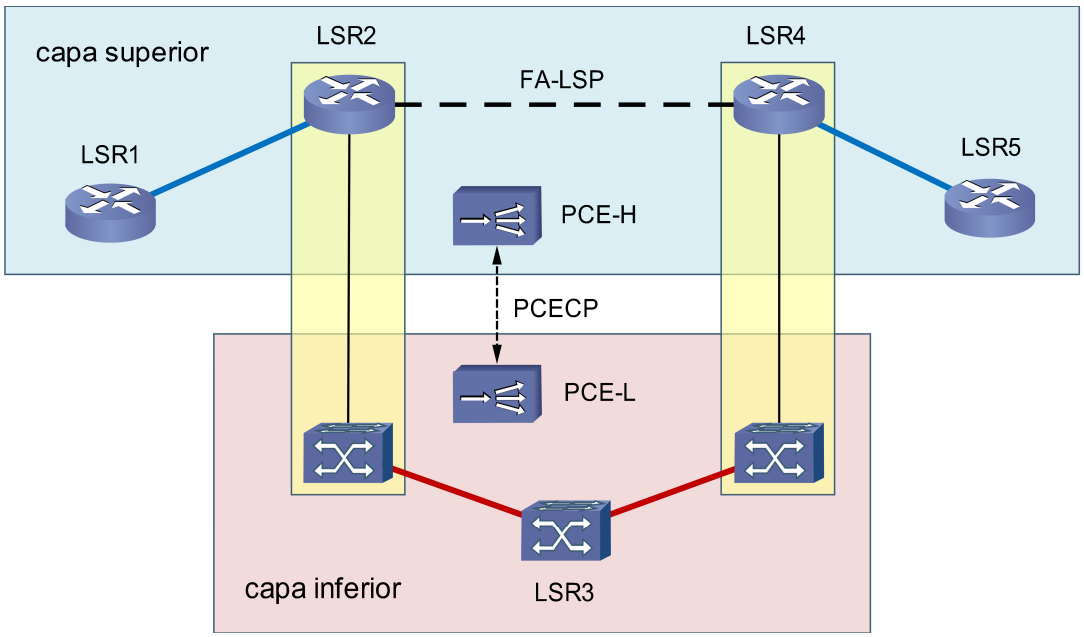

Figura 6.1: Escenario-1 *Horizontal Approach* (HA)

LSR1 y LSR5 pertenecen a la capa superior (p. ej. conmutación de paquetes), LSR3 pertenece a la capa inferior (p.ej. DWDM), LSR2 y LSR4 operan en ambas capas. PCE-H controla la capa superior, y PCE-L la inferior.

LSR1 quiere establecer un LSP con LSR5, y solicita un cálculo de ruta a PCE-H. Dado que no hay recursos disponibles en esta capa (no hay conexión entre LSR2 y LSR4), PCE-H hace una petición a PCE-L para obtener un enlace en la capa inferior. El resultado es una sub-ruta explícita equivalente a un enlace virtual (FA-LSP) en la capa superior, con las características de ingeniería de tráfico requeridas. Con esto, PCE-H ya puede proporcionar una ruta completa de LSR1 a LSR5.

El escenario anterior es muy estricto en lo que a dispositivos se refiere, ya que únicamente dispone de dos LSR que pueden operar en ambas capas (*Horizontal Boundary Nodes*). En la práctica, las redes disponen de un mayor número de estos elementos, llegando al caso en que todos los LSR operan en todas las capas.

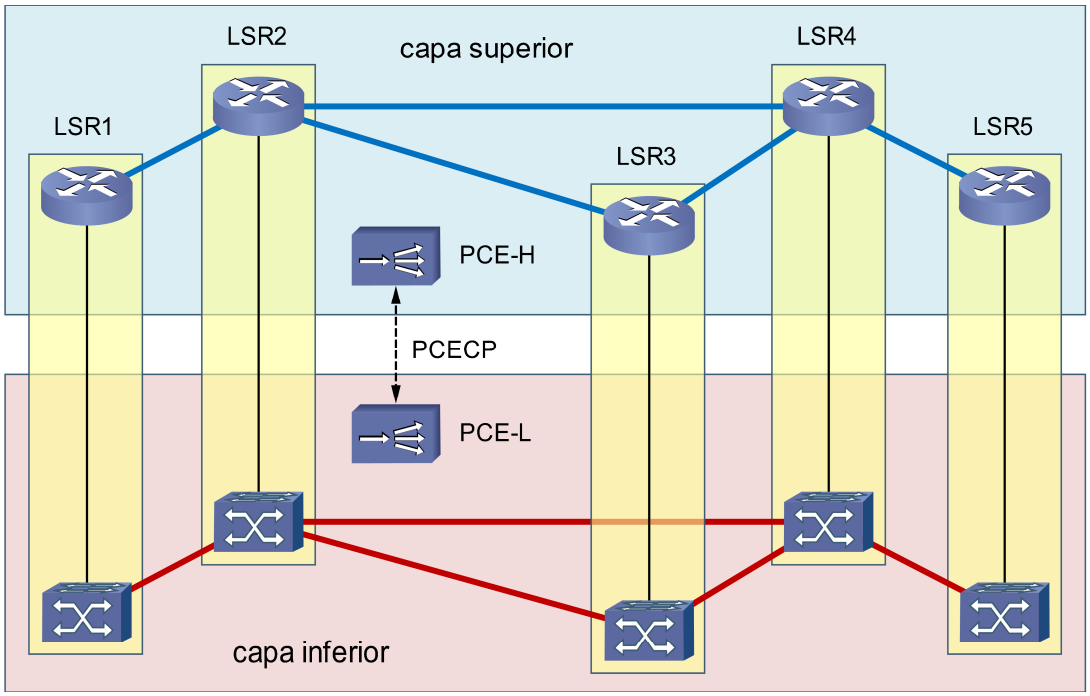

Figura 6.2: Escenario-2 *Horizontal Approach* (HA)

Al querer establecer un LSP entre LSR1 y LSR5, el PCE requerido para calcular la ruta puede escoger ahora entre dos estrategias: *Single Layer* (SL) y *Multiple Layer* (ML).

En el caso de SL el cálculo se restringe a una sola capa, mientras que en ML se abarcan todos los enlaces entre LSR en ambas capas. En este último caso, la ruta resultante puede ser cualquier combinación de enlaces pertenecientes a cualquier capa.

Por un lado, la solución HA-SL no necesita de comunicación inter-PCE, ahorrando así tiempo y recursos. No obstante, la ruta obtenida puede no ser la óptima en tanto que no se tienen en cuenta los recursos de las demás capas.

Por otro lado, la solución HA-ML garantiza la mejor ruta respecto a los requisitos de ingeniería de tráfico. En cambio, puede conllevar un tráfico excesivo de información PCECP y un aumento del tiempo de establecimiento del LSP.

Para solventar las desventajas del modelo HA, el CNIT italiano (*Consorzio Nazionale Interuniversitario per le Telecomunicazioni*) en colaboración con la *Scuola Superiore Sant'Anna* de Pisa, propone un nuevo modelo en la organización de recursos controlados por los PCEs, el modelo vertical – *Vertical Approach* (VA). [21] Cada PCE controla un conjunto de LSRs que operan en todas las capas, y se determinan ciertos nodos frontera (ABR) que conectan estos grupos. De este modo, un PCE puede aplicar por sí solo la estrategia ML en su área, minimizando los inconvenientes del modelo HA-ML.

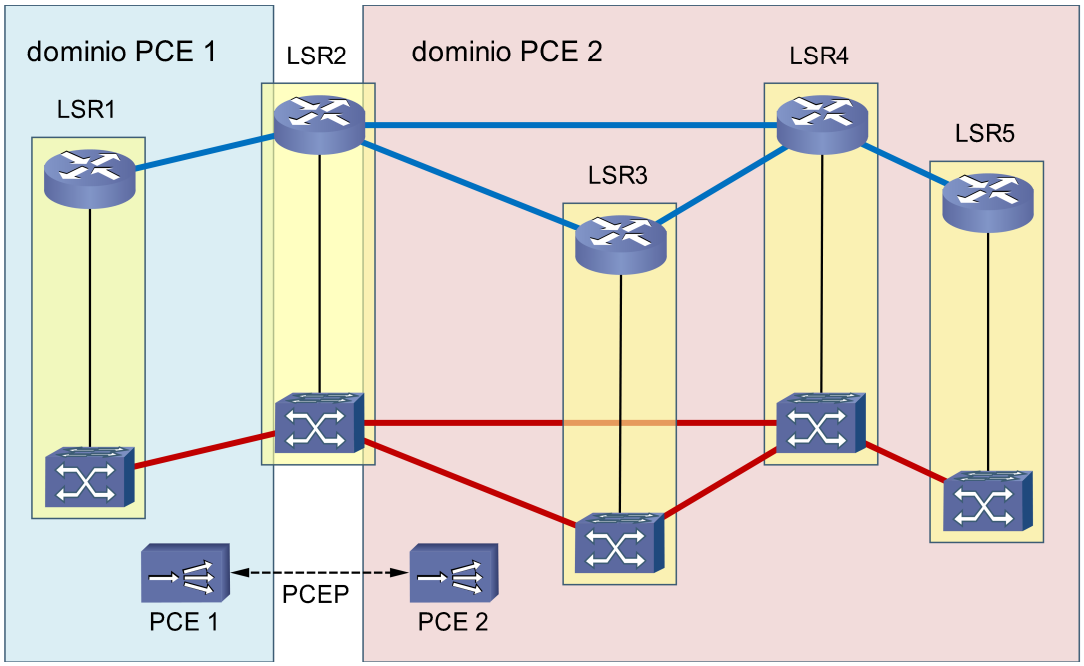

Figura 6.3: Escenario *Vertical Approach* (VA)

El modelo VA-ML es eficiente siempre y cuando el número de nodos frontera sea el más bajo posible. En la práctica esto no supone ningún inconveniente ya que los dominios y áreas que conforman las redes están diseñados habitualmente con un número limitado de nodos frontera.

Se han realizado simulaciones y ensayos que demuestran matemática y estadísticamente que el nuevo modelo VA es más eficiente que HA en sus dos variantes, limitando el intercambio de información PCECP y ofreciendo una ingeniería de tráfico más efectiva en relación a los costes de computación.

6.2 GMPLS-PCE en redes WSON

La aplicación de GMPLS en redes ópticas de conmutación de longitud de onda WSON (*Wavelenght Switched Optical Network*) requiere de la consideración de una nueva problemática no vista hasta ahora.

Gracias a los nuevos dispositivos ópticos como los láseres sintonizables o los *switches* con convertidor de onda, la elección de ruta es similar a la conmutación de circuitos (MPLS y TDM) donde las etiquetas (longitudes de onda) tienen significado local.

Sin embargo, en una red sin convertidores de onda, es necesario que un LSP sea establecido desde origen a destino con una única longitud de onda y que no colisione con la de otro LSP que comparta la misma fibra. Este hecho se denomina “restricción de continuidad de longitud de onda” (*wavelength continuity constraint*). Esta nueva restricción añadida al cálculo de ruta óptima deriva en un proceso RWA (*Routing and Wavelength Assignment*) llevado a cabo por un PCE. [22]

Los elementos y dispositivos de una red WSON poseen una serie de características a considerar en un proceso RWA. Estos datos deben ser trasladados al PCE mediante extensiones en el protocolo de encaminamiento.

Las más importantes son:

- Enlace WDM (fibra): bandas o ventanas de operación, espaciado entre canales.

- Transmisores (láser): fijo o sintonizable, rango y tiempo de sintonización, características espectrales y estabilidad.

- Subsistemas (ROADM, OCX, *splitter*, *combiner*, FOADM): matriz de conectividad, restricciones de longitud de onda en cada puerto, capacidad de conversión de longitud de onda, etc.

El proceso RWA se compone de dos procedimientos: cálculo de ruta (R) y asignación de longitud de onda (WA). Estos dos pasos se pueden realizar de manera combinada o por separado. En este segundo caso existe la posibilidad de utilizar dos PCEs diferentes, uno para cada tarea. Por otro lado, el procedimiento WA puede ser distribuido, es decir, se lleva a cabo en los nodos de la ruta durante la fase de señalización del LSP.

Los métodos de procesado RWA más habituales son:

- **RWA combinado (R&WA)**
  El cálculo de ruta y la asignación de longitud de onda son realizados de manera combinada por una sola entidad. Esta opción requiere que el PCE tenga el suficiente conocimiento sobre la topología de la red, los recursos disponibles y las capacidades de los nodos.

- **R y WA separados (R+WA)**
  En este caso un primer PCE realiza el cálculo de ruta, y el resultado es trasladado a un segundo PCE que realiza la asignación de longitud de onda. Este método es útil cuando no todos los PCEs tienen capacidad de WA. Son necesarias extensiones en el protocolo PCECP para el intercambio de información entre ambos.

- **WA distribuido (R+DWA)**
  El PCE realiza el cálculo de ruta, pero la asignación de longitud de onda es realizada nodo a nodo a lo largo de la ruta. Esto es posible mediante el sistema de restricción de etiquetas del protocolo de señalización (*Label Set Object*) que garantiza la restricción de continuidad de longitud de onda.

6.3 Servicios Inter-Área

Como ya se ha comentado en capítulos anteriores, la IETF ha desarrollado soluciones para el establecimiento de LSPs inter-área que atraviesan varios dominios administrativos, tanto en el cálculo de ruta como en la señalización.

No obstante, hay dos importantes cuestiones sin resolver:

- En el cálculo de una ruta inter-área con múltiples PCEs, no se ha definido cómo se calcula la "cadena de áreas" (*area chain*) que identifica las áreas que atravesará el LSP. Es decir, un PCE que recibe una petición de cálculo debe saber seleccionar apropiadamente el siguiente PCE de un área vecina, en base a sus conocimientos sobre las redes adyacentes, para obtener la mejor ruta inter-área. Y así, sucesivamente, se conforma la cadena.

- El establecimiento de un LSP inter-área está sujeto a fuertes aspectos comerciales y de seguridad y confidencialidad. Debe realizarse únicamente entre entidades seguras, y requiere un servicio preliminar de admisión, confirmación y activación.

El proyecto ACTRICE (*Approche Combinée de Technologies Réseaux Inter-domaine sous Contraintes Economiques*), en el marco francés de la ANR (*Agence Nationale pour la Recherche*) propone la introducción de un "plano de servicio" que completaría la arquitectura PCE inter-área mediante el establecimiento de "servicios inter-área". [20]

A continuación se presentan los elementos que conforman este nuevo "plano de servicio", así como su funcionamiento básico.

Elementos del plano de servicio

Un “servicio inter-área” (*Inter-Area Service*) es el conjunto de uno o más LSPs inter-área entre un nodo origen y un nodo destino que atraviesan una cadena de diferentes dominios administrativos. Y se caracteriza por los siguientes parámetros:

- Direcciones de nodo origen y nodo destino
- Área de origen y área de destino
- Cadena de áreas
- Sentido: unidireccional o bidireccional
- Ancho de banda
- Especificaciones de nivel de servicio (*Service Level Specifications* SLSs). Parámetros de rendimiento y coste.
- Nivel de protección: sin protección, protección local, protección global
- Reoptimización: habilitada o deshabilitada

Un “servicio inter-área” es el resultado de la combinación de tres tipos de “elementos de servicio”:

- Servicio de envío (*sender*): asegura el encaminamiento entre el nodo origen y el Ingress LSR de la siguiente área.

- Servicio de entrega (*destination*): asegura el encaminamiento entre el Ingress LSR de la última área y el nodo destino.

- Servicio de tránsito (*transit*): asegura el encaminamiento entre el Ingress LSR de un área y el Ingress LSR de la siguiente área.

Un "elemento de servicio" (*Service Element* SE) se caracteriza por los siguientes parámetros:

- Área

- Tipo de servicio: envío, entrega, tránsito

- Sentido: unidireccional o bidireccional

- Bordes de entrada y salida (*edges*): nodo origen, nodo destino, Ingress/Egress LSRs o áreas adyacentes, según corresponda

- Límites de rendimiento

- Ancho de banda máximo reservable

- Nivel de protección: sin protección, protección local, protección global

- Coste de tránsito: por velocidad (Mb/s) y/o por tiempo

En la siguiente figura se muestra un ejemplo de composición de servicio inter-área:

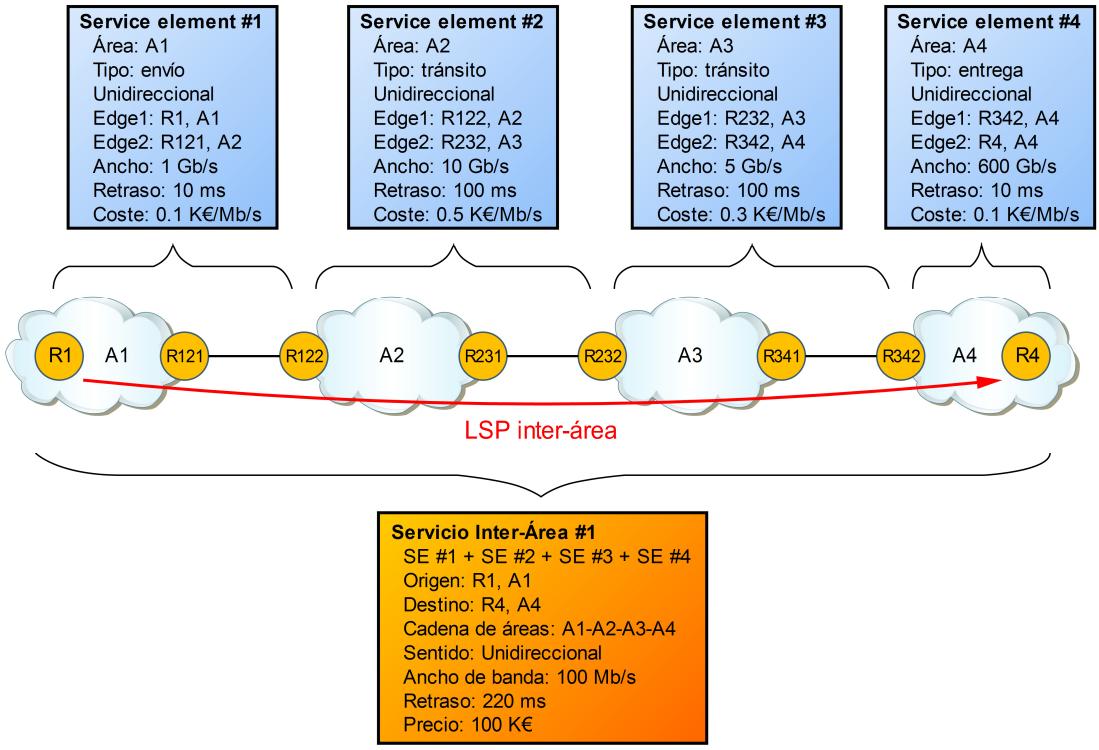

Figura 6.4: Composición de servicio inter-área

El “agente de servicios” SA (*Service Agent*) es un servidor global que recibe las peticiones de los usuarios e inicializa el proceso de establecimiento de los servicios inter-área.

Un “agente de elementos de servicio” SEA (*Service Element Agent*) es un servidor local que controla los elementos de servicio de un área y que implementa los controles de admisión, confirmación y activación.

El “agente de selección de áreas” ASA (*Areas Selection Agent*) es el encargado de la composición de la cadena de áreas para un determinado LSP, mediante un algoritmo de computación.

El "*IP Sphere Forum*" está actualmente desarrollando un marco que permitirá el intercambio de información de servicio multidominio vía SOAP/XML. SA, ASA y SEAs se comunicarían entre ellos mediante este lenguaje.

Con este nuevo plano de servicio, la red queda de la siguiente manera:

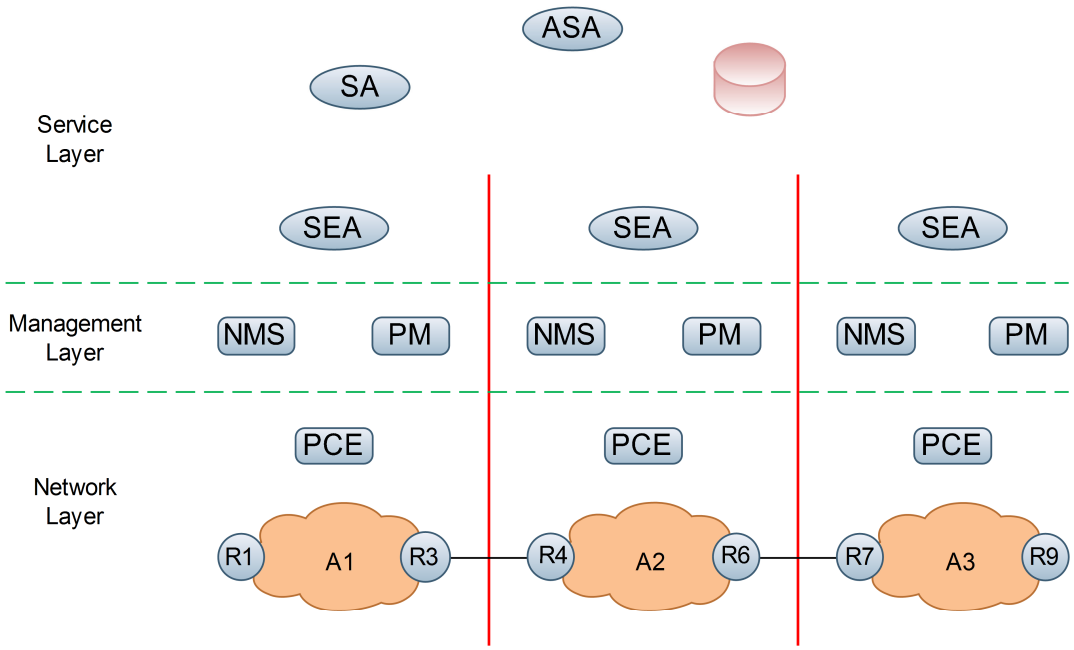

Figura 6.5: Elementos de red inter-área

Establecimiento de un servicio inter-área

El proceso para el establecimiento de un servicio inter-área es el siguiente:

1. **Descubrimiento de los elementos de servicio ofrecidos por cada área.**

   Cada SEA informa de los elementos de servicio de su área y se construye una base de datos a disposición del ASA.

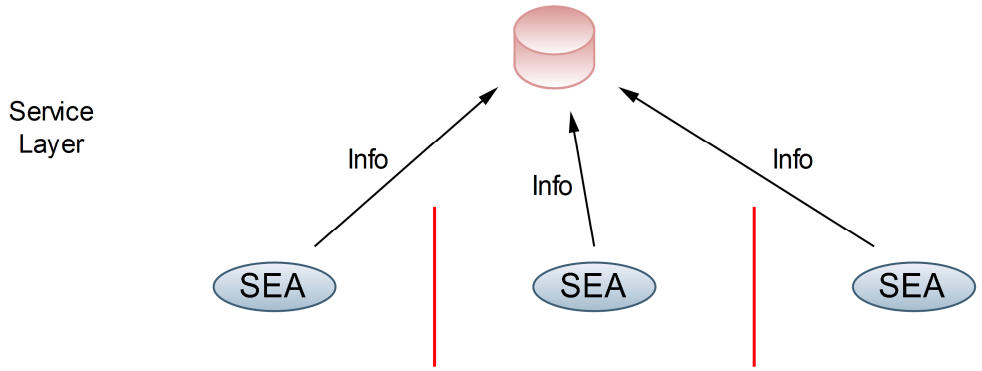

Figura 6.6: Descubrimiento de elementos de servicio

2. **Composición de los elementos de servicio para formar la cadena de áreas.**

   El SA realiza una petición al ASA indicando las especificaciones requeridas para el servicio inter-área (origen, destino, ancho de banda, sentido, SLSs, etc.). Éste aplica un algoritmo CSPF a la base de datos que contiene la información de todos los SEs disponibles, y responde con una o más cadenas de áreas.

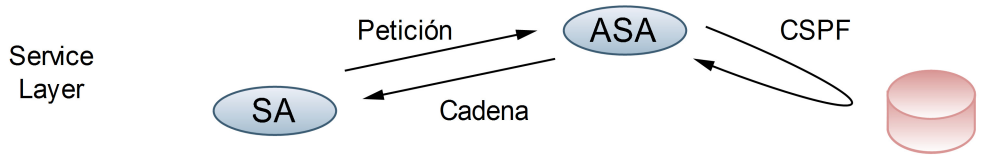

Figura 6.7: Composición de los elementos de servicio (*area-chain*)

3. **Admisión y confirmación del servicio.**

   El SA se comunica con todos los SEAs de las áreas implicadas para verificar la disponibilidad de los elementos de servicio. La petición

contiene un "identificador de servicio" (SID) y las características requeridas para el servicio (ancho de banda, SLSs, etc.). Si los recursos están disponibles, cada SEA responderá al SA con una confirmación positiva OK que contendrá el coste y los SLSs actuales (que pueden haber cambiado). En caso contrario enviará un mensaje NOK (no-OK).

Cuando un SEA deniega la admisión por falta de recursos o por SLSs no aceptables, el SA puede probar con otra cadena.

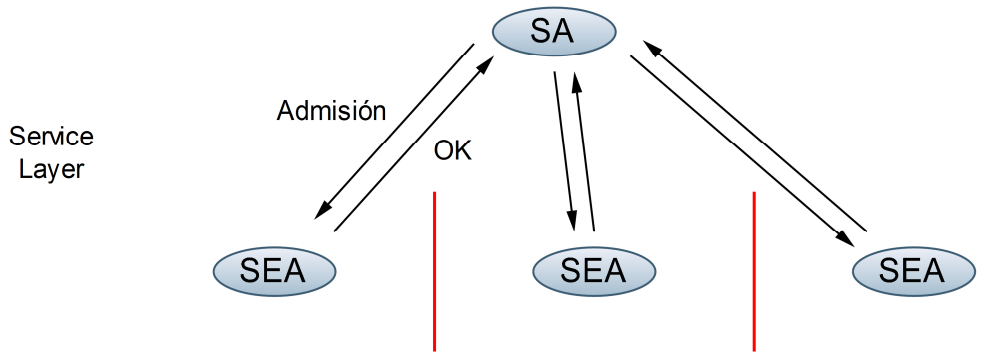

Figura 6.8: Admisión y confirmación del servicio inter-área

4. Activación e inicialización del servicio.

Cuando todos los SEAs confirman positivamente su disponibilidad al SA, éste les envía un mensaje de activación del servicio. Después, cada SEA informará al *Policy Manager* (PM) para que establezca la política administrativa de filtrado sobre PCECP y RSVP-TE. Si no hay ningún error, cada SEA envía de nuevo un mensaje OK al SA; o NOK en caso contrario.

Una vez recibidos todos los mensajes positivos, el SA envía un mensaje de inicialización al SEA de la primera área. El SEA da la orden al NMS

para que inicie la configuración del LSP en el router origen, trasladando los parámetros TE, el SID y la cadena de áreas.

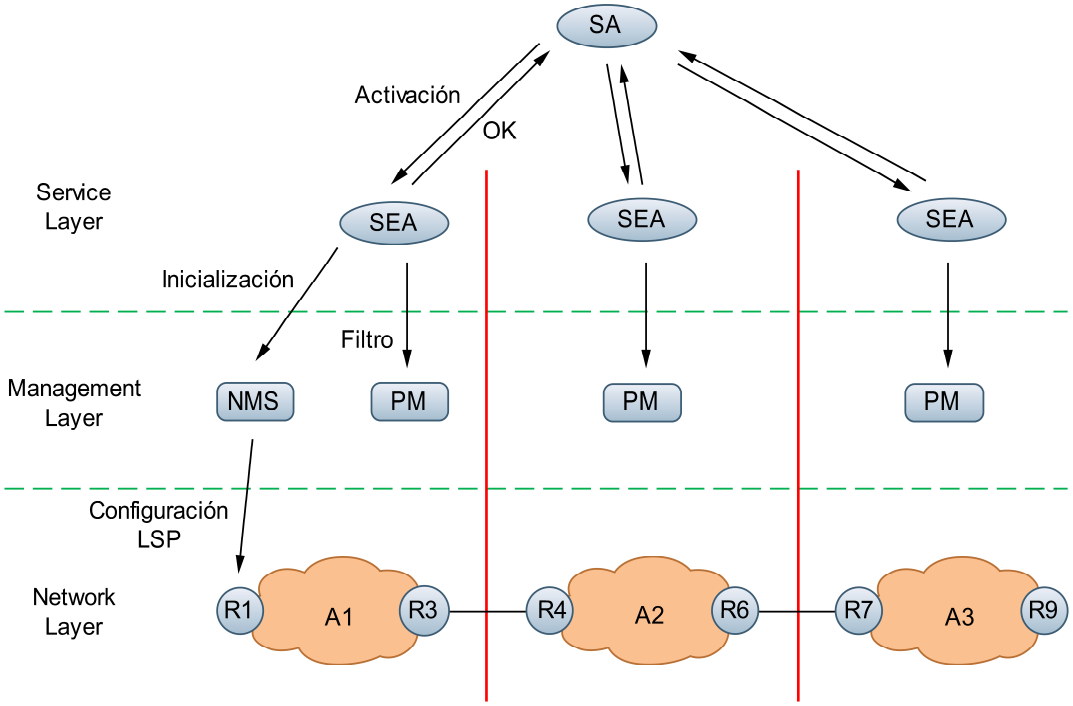

Figura 6.9: Activación e inicialización del servicio inter-área

5. Cálculo de ruta

El router origen, actuando como PCC, envía una petición de cálculo a su PCE. Aquí se inicia el cálculo de ruta inter-área explicado en el capítulo anterior. Las peticiones de cálculo se propagan entre los PCEs de las áreas determinadas en la cadena, para obtener finalmente la ruta inter-área del LSP. Esta ruta será explícita (ERO), bien estricta especificando todos los nodos, o relajada en la cual se señalan los ABRs a cruzar.

Para garantizar la seguridad y confidencialidad, todos los mensajes PCECP son filtrados en base a la política establecida en cada PM. Cuando un PCE recibe un mensaje PCECP, lo reenvía a su PM. Éste

examina el mensaje, extrayendo el SID y los parámetros de la petición, para determinar si cumple lo especificado en el filtro. Dependiendo del resultado, el PM puede aceptarlo, denegarlo, o modificar algunos objetos (por ejemplo la prioridad de una clase DiffServ).

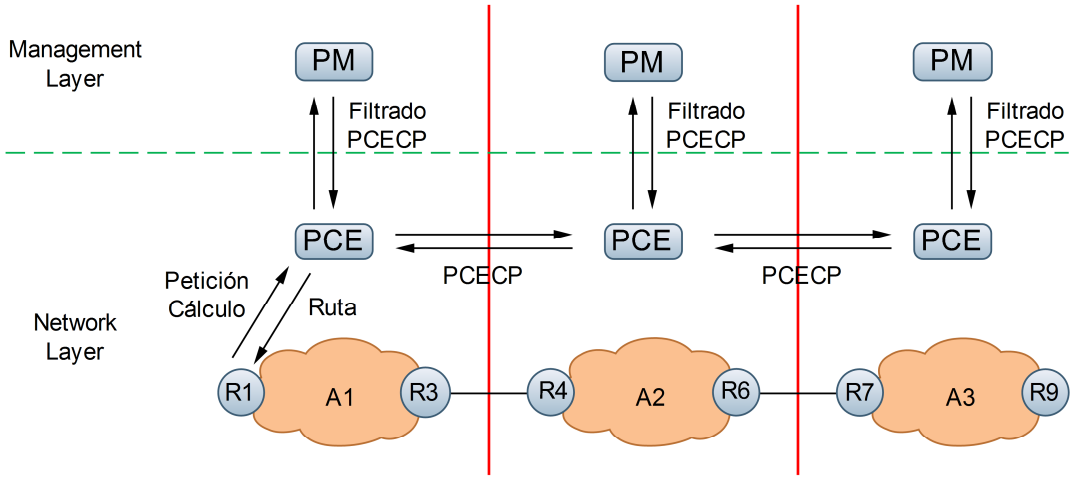

Figura 6.10: Cálculo de ruta inter-área

6. Señalización del LSP

Después de recibir del PCE la ruta inter-área, el nodo origen inicia el mecanismo de señalización para establecer el LSP. Los mensajes de RSVP-TE Path y Resv deben ser extendidos para transportar el SID. El motivo es que todos los ABRs de ingreso en las áreas deben solicitar el filtrado de estos mensajes a su PM.

Cuando un ABR recibe un *Resv message*, envía un mensaje a su NMS informando de la reserva de recursos de su propia área. Los NMSs dan orden a sus SEAs para que actualicen la base de datos del ASA. Finalmente el primer SEA informa al SA de que el LSP está establecido y operativo.

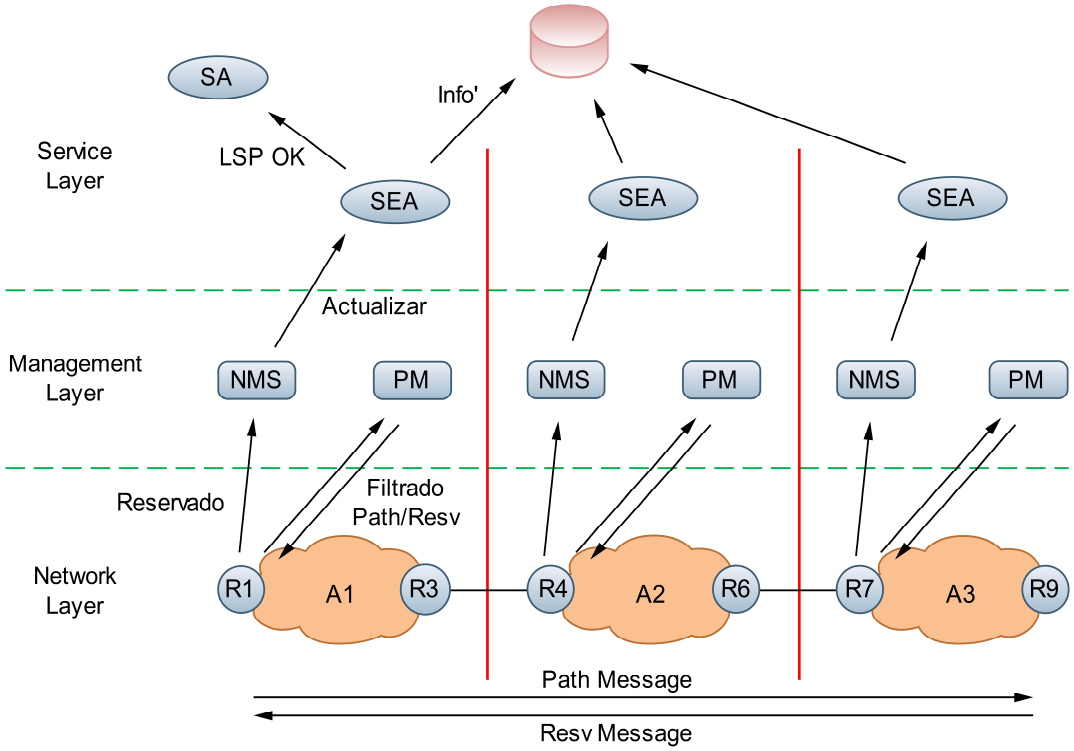

Figura 6.11: Señalización de LSP inter-área

7. Mantenimiento del servicio

Durante el funcionamiento del LSP pueden ocurrir fallos que corten la comunicación. Si el servicio fue definido con una estrategia específica de protección, se debe llevar a cabo en ese momento.

Si el fallo está limitado dentro de un área, el restablecimiento del LSP debe hacerse dentro de la misma área para no afectar al plano de servicio. Si afecta a un tramo inter-área, el LSP debe ser re-enrutado en un nuevo camino entre las dos áreas involucradas. Si el problema es irreparable, se envía un mensaje NOK al SA para que proceda con una nueva petición de servicio.

6.4 Evaluación de sistemas GMPLS-PCE

Para hacer una evaluación de la eficiencia de un sistema GMPLS-PCE en términos de Ingeniería de Tráfico, se definen cuatro criterios:

- **Optimización:** la habilidad de maximizar la cantidad de tráfico que puede transitar por una red con unas garantías QoS. Se pueden considerar diferentes criterios de optimización, como por ejemplo, minimizar la carga total de la red, maximizar el ancho de banda residual de los enlaces más saturados, o, en caso de congestión, minimizar el número de peticiones rechazadas.

- **Escalabilidad:** la habilidad de escalar bien al incrementar el número de cualesquiera de sus elementos: enlaces, LSRs, PCEs, etc.

- **Estabilidad:** la habilidad de evitar re-enrutados y reconfiguraciones y minimizar cualquier perturbación en la red como consecuencia del establecimiento de nuevos LSPs.

- **Reactividad:** la habilidad de reaccionar y adaptarse rápidamente a una redistribución del tráfico como consecuencia de un cambio en la topología de la red (nuevos enlaces o fallos en los existentes).

Dependiendo de la arquitectura de la red, las características anteriores tendrán un mayor o menor peso. En la posterior comparativa entre diferentes escenarios de red se tienen en cuenta tres aspectos:

- Sistema o*nline* (On) u o*ffline* (Off)

- Estructura centralizada (Cen) o distribuida (Dis)

- Cálculo sincronizado (Sinc) o no-sincronizado (NoSinc)

Si se toman estos aspectos por separado se pueden deducir algunas líneas generales:

- ✓ Un sistema o*nline*, por el menor tiempo de cálculo favorece la reactividad, pero empeora la optimización ya que las rutas pueden no ser las óptimas. Esto deriva en una peor estabilidad.

- ✓ Un sistema *offline* presenta mejor optimización en detrimento de reactividad.

- ✓ Una estructura centralizada tiene mala escalabilidad, ya que cada nuevo LSR debe poder comunicarse con el PCE central. Además, debido a las distancias que puede haber entre dispositivos, la reactividad se resiente.

- ✓ Una estructura distribuida posee mayor escalabilidad al haber más PCEs disponibles.

- ✓ Un cálculo sincronizado proporciona una buena optimización pero empeora la reactividad.

- ✓ Un cálculo no-sincronizado ofrece peor optimización y mejor reactividad.

Sin embargo la combinación de estos tres esquemas (8 posibles escenarios) arroja un resultado difícilmente predecible a propósito de los criterios de ingeniería de tráfico anteriormente definidos. [15] [18] Algunas simulaciones sugieren una evaluación expresada en la siguiente tabla:

Escenario	Optimización	Escalabilidad	Estabilidad	Reactividad
On/Dis/NoSinc	*	***	**	****
On/Dis/Sinc	***	*	***	***
On/Cen/NoSinc	*	**	**	**
On/Cen/Sinc	***	**	***	**
Off/Dis/NoSinc	**	***	****	*
Off/Dis/Sinc	****	*	****	*
Off/Cen/NoSinc	**	**	****	*
Off/Cen/Sinc	****	**	****	*

(“****” muy buena, “***” buena, “**” mala, “*” muy mala)

Figura 6.12: Tabla comparativa de escenarios GMPLS-PCE

La elección de un escenario u otro para implementar un sistema GMPLS-PCE en una red dependerá del orden de prioridades que se decida respecto a las características de ingeniería de tráfico requeridas.

7. CONCLUSIONES

Este proyecto tiene como objetivo ofrecer una visión global y genérica de las arquitecturas MPLS y GMPLS desarrolladas por la IETF, además del sistema de enrutamiento que proporciona el PCE.

En el primer capítulo se ha hecho un repaso a la evolución tecnológica y las necesidades que motivaron el desarrollo de estos estándares. En concreto, la creación de un plano de control común e inteligente que permite a los diferentes operadores la configuración, utilización y mantenimiento de sus redes de un modo seguro, fácil, más eficiente y menos costoso, sobre cualquier tecnología de transporte y transmisión de datos.

En el segundo capítulo se ha visto la estructura básica de una red MPLS y su funcionamiento. La transmisión y encaminamiento de la información es mucho más rápida y sencilla gracias a las etiquetas, que simplifican y aceleran la tarea de los LSRs respecto al *routing* IP tradicional. También se exponen las tres principales ventajas que proporciona MPLS: la ingeniería de tráfico, cuyo objetivo es optimizar los recursos de la red; las clases de servicio, que permiten diferenciar entre diferentes tipos de tráfico de datos y otorgarles tratamientos distintos; y la flexibilidad para crear redes privadas virtuales, gracias al modelo acoplado inherente de un sistema MPLS.

El tercer capítulo muestra las mejoras y adaptaciones que se introducen en la evolución de MPLS a GMPLS, como son los LSPs bidireccionales, el *forwarding adjacency*, o el *link bundling*. Además de la cobertura que proporciona MPLS/GMPLS sobre diferentes áreas y dominios. Por último, unas nociones sobre administración y seguridad de estas redes.

Los protocolos MPLS y GMPLS han centrado el cuarto capítulo. Los dos protocolos de encaminamiento, OSPF-TE e IS-IS-TE, recaban todo tipo de información sobre la red (topología, enlaces, dispositivos, etc.) que servirá

posteriormente para calcular y definir las diferentes rutas de tráfico de acuerdo a las reglas de la ingeniería de tráfico. Se ha detallado el funcionamiento del protocolo de señalización RSVP-TE, encargado del establecimiento y mantenimiento de los LSPs. Finalmente, el protocolo LMP, exclusivo de GMPLS, que gestiona los canales de control y datos entre los dispositivos de la red.

El quinto capítulo presenta el Path Computation Element (PCE), una entidad avanzada de cálculo de rutas con ingeniería de tráfico aplicada, que puede resultar a veces imprescindible en redes complejas, extensas o sin capacidad de *routing*. Se ha explicado la arquitectura y funcionamiento de un sistema PCE, las motivaciones para su uso, y las ventajas que aporta, como por ejemplo la posibilidad de cálculo sincronizado o la obtención de rutas óptimas inter-área. También se ha estudiado el protocolo PCECP que soporta este sistema.

En el sexto capítulo se han explicado algunas carencias y problemáticas que presentan las redes GMPLS-PCE, y las propuestas que ofrecen diferentes grupos de trabajo para solventarlas o complementar dichas redes. Por ejemplo, la adaptación a las redes WSON de tecnología óptica. Para finalizar se ha hecho un análisis comparativo entre diferentes escenarios de una red GMPLS-PCE.

En definitiva, los sistemas GMPLS-PCE son un peldaño más en la constante evolución del mundo de las telecomunicaciones, proporcionando una adaptación inteligente de las redes al crecimiento exponencial del tráfico, integrando las diferentes tecnologías existentes, y ofreciendo el soporte para los nuevos servicios y aplicaciones que los usuarios demandan.

Glosario de acrónimos

- **ABR:** *Area Border Router*
- **ACTRICE:** *Approche Combinée de Technologies Réseaux Inter-domaine sous Contraintes Economiques*
- **ANR:** *Agence Nationale pour la Recherche*
- **ANSI:** *American National Standards Institute*
- **ARIS:** *Aggregate Route-Base IP Switching*
- **ARPANET:** *Advanced Research Projects Agency Network*
- **ASA:** *Areas Selection Agent*
- **ATM:** *Asynchronous Transfer Mode*
- **BOS:** *Bottom Of Stack*
- **CBR:** *Constraint-Based Routing*
- **CNIT:** *Consorzio Nazionale Interuniversitario per le Telecomunicazioni*
- **COPS:** *Common Open Policy Service*
- **COS:** *Class Of Service*
- **CPE:** *Cell Processing Engine*
- **CR-LDP:** *Constraint-Based Routing Label Distribution Protocol*
- **CSPF:** *Constrained Shortest Path First*
- **CSR:** *Cell Switching Router*
- **DARPA:** *Defense Advanced Research Projects Agency*
- **DIFFSERV:** *Differentiated Services*
- **DLCI:** *Data Link Connection Identifier*
- **DOS:** *Denial Of Service*
- **DS:** *Differentiated Services field*
- **DWDM:** *Dense Wavelength Division Multiplexing*
- **ERO:** *Explicit Route Object*
- **ETSI:** *European Telecommunications Standards Institute*
- **EXP:** *Experimental*
- **FA:** *Forwarding Adjacency*
- **FA-LSP:** *Forwarding Adjacency Label Switched Path*

- **FEC:** *Forwarding Equivalence Class*
- **FOADM:** *Fixed Optical Add-Drop Multiplexer*
- **FSC:** *Fiber-Switch Capable*
- **GMPLS:** *Generalized Multi-Protocol Label Switching*
- **G-PID:** *Generalized-Payload Identifier*
- **HA:** *Horizontal Approach*
- **ID:** *Identificator*
- **IEEE:** *Institute of Electrical and Electronics Engineers*
- **IETF:** *Internet Engineering Task Force*
- **IP:** *Internet Protocol*
- **IPSEC:** *Internet Protocol Security*
- **IPX:** *Internetwork Packet Exchange*
- **IS-IS-TE:** *Intermediate System to Intermediate System – Traffic Engineering*
- **ISP:** *Internet Service Provider*
- **ITU:** *International Telecommunication Union*
- **L3PID:** *Layer 3 Payload Identifier*
- **LAN:** *Local Area Network*
- **LDP:** *Label Distribution Protocol*
- **LER:** *Label Edge Router*
- **LFIB:** *Label Forwarding Information Base*
- **LIB:** *Label Information Base*
- **LMP:** *Link Management Protocol*
- **LOL:** *Loss of Light*
- **LSA:** *Link State Advertisement*
- **LSC:** *Lambda-Switch Capable*
- **LSD:** *Link State Database*
- **LSP:** *Label Switched Path*
- **LSR:** *Label Switch Router*
- **MAC:** *Media Access Control*
- **MBC:** *Minimize aggregate Bandwidth Consumption*

- **MBP:** *Maximum residual Bandwidth Path*
- **MCC:** *Minimize the Cumulative Cost of a set of paths*
- **MCP:** *Minimum Cost Path*
- **ML:** *Multiple Layer*
- **MLL:** *Minimize the Load of the most loaded Link*
- **MLP:** *Minimum Load Path*
- **MPLS:** *Multi-Protocol Label Switching*
- **NMS:** *Network Management Service*
- **NOK:** *No-OK*
- **NSP:** *Network Service Provider*
- **OSI:** *Open System Interconnection*
- **OSPF-TE:** *Open Shortest Path First – Traffic Engineering*
- **OXC:** *Optical Cross-Connector*
- **PCC:** *Path Computation Client*
- **PCE:** *Path Computation Element*
- **PCECP:** *Path Computation Element - Communication Protocol*
- **PDH:** *Plesiochronous Digital Hierarchy*
- **PM:** *Policy Manager*
- **PPP:** *Point-to-point Protocol*
- **PSC:** *Packet-Switch Capable*
- **PVC:** *Permanent Virtual Circuit*
- **PXC:** *Photonic Cross-Connector*
- **QOS:** *Quality Of Service*
- **RFC:** *Request For Comments*
- **ROADM:** *Reconfigurable Optical Add-Drop Multiplexer*
- **RRO:** *Record Route Object*
- **RSVP:** *Reservation Protocol*
- **RSVP-TE:** *Resource Reservation Protocol – Traffic Engineering*
- **RWA:** *Routing and Wavelength Assignment*
- **SDH:** *Synchronous Digital Hierarchy*
- **SE:** *Service Element*

- **SA:** *Service Agent*
- **SEA:** *Service Element Agent*
- **SID:** *Service Identificator*
- **SL:** *Single Layer*
- **SLS:** *Service Level Specification*
- **SNA:** *Systems Network Architecture*
- **SNMP:** *Simple Network Management Protocol*
- **SOAP:** *Simple Object Access Protocol*
- **SONET:** *Synchronous Optical Network*
- **SRLG:** *Shared Risk Link Group*
- **TCP:** *Transmission Control Protocol*
- **TDM:** *Time-Division Multiplexing*
- **TE:** *Traffic Engineering*
- **TED:** *Traffic Engineering Database*
- **RSVP:** *Resource Reservation Protocol*
- **TOS:** *Type Of Service*
- **TTL:** *Time To Live*
- **UDP:** *User Datagram Protocol*
- **UNI:** *User-to-Network Interface*
- **UNI-C:** *UNI-Customer side*
- **UNI-N:** *UNI-Network side*
- **VA:** *Vertical Approach*
- **VCI:** *Virtual Channel Identifier*
- **VOIP:** *Voice Over IP*
- **VPI:** *Virtual Path Identifier*
- **VPN:** *Virtual Private Network*
- **WDM:** *Wavelength Division Multiplexing*
- **WSON:** *Wavelength Switched Optical Network*
- **WWW:** *World Wide Web*
- **XML:** *Extensible Mark-up Language*

Relación de figuras

Bibliografía

[1] Adrian Farrel, Igor Bryskin. *"GMPLS Architecture and Applications"*. Morgan Kaufmann.

[2] Regis J. Bates. *"Broadband Telecommunications Handbook"*. McGraw-Hill TELECOM, 2002.

[3] Luc De Ghein. *"MPLS Fundamentals"*. Cisco Press, 2007.

[4] Eric Osborne, Ajay Simha. *"Traffic Engineering with MPLS"*. Cisco Press, 2002.

[5] Jim Guichard, François Le Faucheur, Jean-Philippe Vasseur. *"Definitive MPLS Network Designs"*. Cisco Press, 2005.

[6] *"Generalized Multiprotocol Label Switching"*. The International Engineering Consortium.

[7] *"Cisco Segmented Generalized Multiprotocol Label Switching for the IP Next-Generation Network"*. Cisco Public Information, 2006.

[8] *"Converge IP and DWDM Layers in the Core Network"*. Cisco Public Information, 2007.

[9] Javier Martín Rodríguez. *"GMPLS, el futuro de las redes IP"*. Alcatel España.

[10] Adrian Farrel. *"The Internet and its Protocols"*. Morgan Kaufmann.

[11] José M. Huidobro Moya, Ramón J. Millán Tejedor. *"MPLS (MultiProtocol Label Switching)"*. Ericsson España, 2002.

[12] Adolfo García Yagüe. *"Redes MPLS y GMPLS. Servicios y Aplicaciones"*. Unitronics Comunicaciones, 2005.

[13] *"MPLS Applications Configuration Guide"*. Juniper Networks, 2007.

[14] Sukrit Dasgupta and Jaudelice C. de Oliveira, Drexel University. Jean-Philippe Vasseur, Cisco Systems. *"Path-Computation-Element-Based Architecture for Interdomain MPLS/GMPLS Traffic Engineering: Overview and Performance"*. Drexel University Libraries, 2007.

[15] Imene Chaieb and Jean-Louis Le Roux, France Telecom. Bernard Cousin, IRISA. *"MPLS-TE Routing: Adopting a Generic Architecture and Evaluating Various Implementation Approaches"*.

[16] Aruna Prem Bianzino, Jean-Louis Rougier, Stefano Secci, TELECOM ParisTech (ENST). Ramon Casellas, Ricardo Martinez, Raul Muñoz, Centre Tecnològic de Telecomunicacions de Catalunya (CTTC). Nabil Bachir Djarallah, Richard Douville, Hélia Pouyllau, Alcatel-Lucent Bell Labs. *"Testbed Implementation of Control Plane Extensions for Inter-Carrier GMPLS LSP Provisioning"*.

[17] Jing Fu, Peter SjÄodin and Gunnar Karlsson. *"Intra-Domain Routing Convergence with Centralized Control"*. KTH, Royal Institute of Technology, 2008.

[18] D.Adami, C.Callegari, S.Giordano, M.Pagano. *"Distributed and Centralized Path Computation Algorithms: Implementation in NS2 and Performance Comparison"*. CNIT Research Unit - Dept. of Information Engineering - University of Pisa, 2008.

[19] J.L. Le Roux, France Telecom. J.P. Vasseur, Cisco System Inc. Y. Lee, Huawei. *"Encoding of Objective Functions in the Path Computation Element Communication Protocol (PCEP)"*. Draft-ietf-pce-of-05.txt. IETF, 2008.

[20] Richard Douville, Alcatel-Lucent Bell Labs. Jean-Louis Le Roux, Orange Labs France Telecom. Jean-Louis Rougier, TELECOM ParisTech (ENST). Stefano Secci, TELECOM ParisTech (ENST), Politecnico di Milano. *"A Service Plane over the PCE Architecture for Automatic Multidomain Connection-Oriented Services"*. IEEE Communications Magazine, 2008.

[21] F. Cugini, A. Giorgetti, N. Andriolli, F. Paolucci, L. Valcarenghi, P. Castoldi. *"Multiple Path Computation Element (PCE) Cooperation for Multi-layer Traffic Engineering"*. Optical Society of America, 2007.

[22] Greg Bernstein and Young Lee. *"Extending GMPLS/PCE for use in Wavelength Switched Optical Networks"*. IEEE, 2008.

[23] Takehiro Tsuritani, Masanori Miyazawa, Shuntaro Kashihara and Tomohiro Otani. *"Optical Path Computation Element interworking with Network Management System for Transparent Mesh Networks"*. Optical Society of America, 2008.

[24] María Sol Canalis. *"MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI"*. Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina.

[25] Daniel King, Young Lee, Huiying Xu, and Adrian Farrel. *"Path Computation Architectures Overview in Multidomain Optical Networks Based on ITU-T ASON and IETF PCE"*. IEEE, 2008.

[26] T. Li, Y. Rekhter. *"A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)"*. RFC 2430. IETF, 1998.

[27] D. Awduche, J. Malcolm, J.Agogbua, M. O'Dell, J. McManus. *"Requirements for Traffic Engineering Over MPLS"*. RFC 2702. IETF, 1999.

[28] E. Rosen, A. Viswanathan, R. Callon. *"Multiprotocol Label Switching Architecture"*. RFC 3031. IETF, 2001.

[29] F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen. *"Multi-Protocol Label Switching (MPLS) Support of Differentiated Services"*. RFC 3270. IETF, 2002.

[30] J. Boyle, V. Gill, A. Hannan, D. Cooper, D. Awduche, B. Christian, W.S. Lai. *"Applicability Statement for Traffic Engineering with MPLS"*. RFC 3346. IETF, 2002.

[31] J.L. Le Roux, J. P. Vasseur, J. Boyle. *"Requirements for Inter-Area MPLS Traffic Engineering"*. RFC 4105. IETF, 2005.

[32] Farrel, J. P. Vasseur, A. Ayyangar. *"A Framework for Inter-Domain Multiprotocol Label Switching Traffic Engineering"*. RFC 4726. IETF, 2006.

[33] J. L. Le Roux. *"Path Computation Element Communication Protocol (PCECP) Specific Requirements for Inter-Area MPLS and GMPLS Traffic Engineering"*. RFC 4927. IETF, 2007.

[34] L. Berger. *"Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description"*. RFC 3471. IETF, 2003.

[35] L. Berger. *"Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions"*. RFC 3473. IETF, 2003.

[36] E. Mannie. *"Generalized Multi-Protocol Label Switching (GMPLS) Architecture"*. RFC 3945. IETF, 2004.

[37] K. Kompella, Y. Rekhter. *"Link Bundling in MPLS Traffic Engineering"*. RFC 4201 IETF, 2005.

[38] J. Lang. *"Link Management Protocol (LMP)"*. RFC 4204. IETF, 2005.

[39] J. P. Lang, Y. Rekhter, D. Papadimitriou. *"RSVP-TE Extensions in Support of End-to-End Generalized Multi-protocol Label Switching (GMPLS) Recovery"*. RFC 4872. IETF, 2007.

[40] Farrel, A. Satyanarayana. *“Crankback Signaling Extensions for MPLS and GMPLS RSVP-TE”*. RFC 4920. IETF, 2007.

[41] Farrel, J. P. Vasseur, J. Ash. *“A Path Computation Element (PCE)-Based Architecture”*. RFC 4655. IETF, 2006.

[42] J. Ash, J. L. Le Roux. *“Path Computation Element (PCE) Communication Protocol Generic Requirements”*. RFC 4657. IETF, 2006.

[43] J. L. Le Roux. *“Requirements for Path Computation Element (PCE) Discovery”*. RFC 4674. IETF, 2006.

[44] Bryskin, D. Papadimitriou, L. Berger, J. Ash. *“Policy-Enabled Path Computation Framework”*. RFC 5394. IETF, 2008.