UNIVERSIDAD CARLOS III DE MADRID

SUPERVIVENCIA EN REDES MULTICAPA DE PRÓXIMA GENERACIÓN

INGENIERIA DE TELECOMUNICACIONES

PROYECTO FIN DE CARRERA

Alumno: Fernando Muñoz del Nuevo
Tutor: José Alberto Hernández Gutiérrez
Co-Tutor: Óscar González de Dios

ÍNDICE

1 INTRODUCCIÓN 5
1.1 MOTIVACIÓN DEL PROYECTO 5
1.2 OBJETIVOS 6
1.3 CONTENIDO DE LA MEMORIA 6
2 ESCENARIO DE RED Y MECANISMOS DE SUPERVIVENCIA DE RED 8
2.1 ESCENARIOS DE RED 8
2.2 SUPERVIVENCIA EN REDES. 18
2.3 EVOLUCIÓN DE LA RED HACIA UN MODELO MULTICAPA 31
2.4 SUPERVIVENCIA EN REDES MULTICAPA 36
3 ANÁLISIS DE SUPERVIVENCIA MULTICAPA 42
3.1 MODELADO ANALÍTICO 42
3.2 MODELADO MEDIANTE SIMULACIÓN 46
3.3 VALIDACIÓN DE LOS MODELOS ANALÍTICOS Y DE SIMULACIÓN 60
3.4 ESTUDIOS TECNO-ECONÓMICOS. 63
4 DEMOSTRACIÓN DE RESTAURACIÓN MULTICAPA CON EQUIPOS REALES .. 66
4.1 ARQUITECTURA DEL GESTOR DE RESTAURACIÓN MULTICAPA 66
4.2 INTERFACES ESTÁNDAR UTILIZADOS EN EL PROTOTIPO 67
4.3 CASO DE USO 69
5 CONCLUSIONES 80
6 PRESUPUESTO 81
7 ACRÓNIMOS 83
8 BIBLIOGRAFÍA 85
9 ANEXO DE CÓDIGO DE GESTOR MULTICAPA 88

TABLA DE ILUSTRACIONES

FIGURA 1 ESCENARIO DE RED DE UN OPERADOR MEDIO 9
FIGURA 2 ENTRADA DE UNA TABLA DE ENCAMINAMIENTO DE ETIQUETAS [10] 10
FIGURA 3 EJEMPLO DE ETIQUETADO Y CONMUTACIÓN EN RED MPLS [10] 11
FIGURA 4 JERARQUÍA DE LSPS [10] 12
FIGURA 5 ENCAMINAMIENTO BASADO EN CAMINO MÁS CORTO 13
FIGURA 6 ENCAMINAMIENTO HACIENDO USO DE LA INGENIERÍA DE TRÁFICO 13
FIGURA 7 RED DE TRANSPORTE QUE PROPORCIONA CONECTIVIDAD ENTRE ISLAS DE REDESO [15] 14
FIGURA 8 RED EN ANILLO BIDIRECCIONAL [15] 15
FIGURA 9 INTERCONEXIÓN MALLADA DE ANILLOS [15] 16
FIGURA 10 REDES PUNTO A PUNTO [15] 16
FIGURA 11 RED MALLADA [15] 16
FIGURA 12 JERARQUÍA DE SWITCHING TYPES [15] 18
FIGURA 13 EJEMPLO SRLGS 21
FIGURA 14 ESQUEMAS DE PROTECCIÓN DE RED 22
FIGURA 15 PROTECCIÓN EN REDES IP/MPLS [21] 24
FIGURA 16 PROTECCIÓN MEJORADA SONET BLSR [15] 26
FIGURA 17 EJEMPLO DE NÚCLEO DE RED DE OPERADOR MEDIO [24] 27
FIGURA 18 CONECTIVIDAD FÍSICA EN RED MULTI-REGIONAL 28
FIGURA 19 FLUJOS DE TRÁFICO EN RED JERÁRQUICA 28
FIGURA 20 FALLO SIMPLE EN RED JERÁRQUICA 29
FIGURA 21 FALLO DOBLE EN RED JERÁRQUICA 30
FIGURA 22 FALLO EN TRANSPORTE RECUPERABLE 31
FIGURA 23 FALLO EN TRANSPORTE IRRECUPERABLE 31
FIGURA 24 TE-LINKS MULTICAPA 33
FIGURA 25 CONFIGURACIÓN DE TE-LINKS MULTICAPA 34
FIGURA 26 EJEMPLO DE SOLICITUD DE CAMINO MULTICAPA A TRAVÉS DE UNI 35
FIGURA 27 ESTABLECIMIENTO DE LSPS JERÁRQUICOS 36
FIGURA 28 RESTAURACIÓN MULTICAPA EN RED JERÁRQUICA 38
FIGURA 29 RESTAURACIÓN UTILIZANDO EL TRÁNSITO DE OTRA REGIÓN 38
FIGURA 30 RESTAURACIÓN MULTICAPA MANTENIENDO LOS RECURSOS 39
FIGURA 31 RESTAURACIÓN MULTICAPA CON GRANJA DE ROUTERS 40
FIGURA 32 RESTAURACIÓN MULTICAPA SIN PROTECCIÓN EN LAS REGIONES 41
FIGURA 33 DIAGRAMA DE CADENA DE MARKOV PARA 1 REGIÓN 43
FIGURA 34 ESQUEMA DE RED DE DOS REGIONES 44
FIGURA 35 DIAGRAMA DE CADENA DE MARKOV PARA 2 REGIONES 45
FIGURA 36 DISPONIBILIDAD EN FUNCIÓN DEL NÚMERO DE REGIONES 46
FIGURA 37 DEFINICIÓN DE BLOQUES COMPUESTOS EN OMNET++ [28] 47
FIGURA 38 MÓDULO COMPUESTO DE OMNET [28] 50

FIGURA 39 EJEMPLO DE RED COMPLETA 53
FIGURA 40 GESTOR DE SIMULACIÓN 54
FIGURA 41 MÓDULO ROUTER IP/MPLS 55
FIGURA 42 MÓDULO ROADM 56
FIGURA 43 ESQUEMA DE RED MULTICAPA DE 3 REGIONES SIMULADO EN OMNET++ 57
FIGURA 44 ESQUEMA DE RED MULTICAPA CON RECURSOS REGIONALES RESERVADOS 58
FIGURA 45 FALLO DETECTADO EN UN NODO DE TRÁNSITO 59
FIGURA 46 RESTAURACIÓN MULTICAPA INTERREGIONAL 60
FIGURA 47 DISPONIBILIDAD EN RELACIÓN A MTTR/MTBF PARA 3 REGIONES 61
FIGURA 48 DISPONIBILIDAD EN FUNCIÓN DE MTTR/MTBF PARA MÚLTIPLES REGIONES 62
FIGURA 49 DISPONIBILIDAD REDUCIENDO EL NÚMERO DE ROUTERS DE TRÁNSITO 63
FIGURA 50 DISPONIBILIDAD EN FUNCIÓN DE MTTR/MTBF PARA ESTUDIO DE COSTES DE OPERACIÓN 64
FIGURA 51 ARQUITECTURA DEL GESTOR MULTICAPA 66
FIGURA 52 ÁRBOL DE OIDS DE EJEMPLO [35] 69
FIGURA 53 ROUTERS JUNIPER MX-80 70
FIGURA 54 NODO ADVA FSP 3000 71
FIGURA 55 GESTOR MULTICAPA 71
FIGURA 56 ESCENARIO DE RED DEL DEMOSTRADOR 72
FIGURA 57 DIRECCIONAMIENTO DE PLANO DE CONTROL 73
FIGURA 58 DIRECCIONAMIENTO A NIVEL IP/MPLS 74
FIGURA 59 DIRECCIONAMIENTO ESTADO INICIAL DEL DEMOSTRADOR 75
FIGURA 60 RESTAURACIÓN MULTICAPA TRAS EL FALLO 76
FIGURA 61 COMPROBACIÓN DEL FUNCIONAMIENTO DEL DEMOSTRADOR 77
FIGURA 62 PROCEDIMIENTO RSVP PARA EL ESTABLECIMIENTO DEL ENLACE 77
FIGURA 63 MENSAJE RSVP PATH 78
FIGURA 64 MENSAJE RSVP RESV 79
FIGURA 65 DIAGRAMA UML DE LOS MÓDULOS PRINCIPALES 88
FIGURA 66 DETALLE DEL MÓDULO CORE 89
FIGURA 67 DETALLE MÓDULO DISPATCHER 90
FIGURA 68 DETALLE MÓDULO MONITORING 90

AGRADECIMIENTOS

En primer lugar quisiera agradecer a Óscar González de Dios y a José Alberto Hernández Gutiérrez por compartir sus conocimientos y consejos en la realización de este Proyecto Fin de Carrera.

En el camino que, al menos temporalmente, se cierra con la realización de este trabajo han sido muchos lo que me han ayudado y compartido los buenos y malos momentos durante la realización de mis estudios en la Universidad Carlos III. De todos mis compañeros quiero resaltar especialmente a Carlos, Víctor y Ana.

Agradezco también a mis amigos David, Nacho, Jesús y Eduardo con quienes he vivido durante los últimos años de nuestros estudios. Sin vosotros hubiera sido más difícil.

Una mención muy importante se merecen mis compañeros de Telefónica I+D que me han visto crecer profesionalmente y han abierto mi mente enormemente tanto en el terreno profesional como el terreno moral. En especial quiero mencionar a Víctor, Óscar, Juan Pedro, Raúl, Jose Ignacio y Javi Jimenez.

No quiero olvidar a quienes fueron becarios conmigo en I+D y ya no están: Laura Ramírez, Noemí, Sergio Ortiz, Jose Raúl, Dani, César, Jose Manuel, Luis Ma, Rafa y Alejandro.

Para finalizar, los más importantes, mi familia que ha estado desde el principio de todo y me han apoyado siempre que lo he necesitado. En especial a mis padres Silvia y Rafael y mis hermanos Irina, Rafael y Pol. Mi más cariñoso y sincero agradecimiento para vosotros.

Por último, quiero agradecer a Viviana la confianza que ha depositado siempre en mí y que me ha hecho creer que soy capaz de lo que me proponga.

A todos vosotros, muchas gracias.

1 Introducción

El tráfico en las redes de los operadores de internet es cada vez más dinámico y menos predecible. Además, los operadores han de proporcionar servicios con SLA (*Service Level Agreement*, Acuerdo de nivel de servicio) que garantice cierto grado de disponibilidad del servicio en función de los requisitos de los clientes. En este contexto, los actuales mecanismos de supervivencia de red se utilizan para garantizar el cumplimiento de dichos acuerdos (en la medida de lo posible). El objetivo del operador es minimizar costes y flexibilizar la operación en torno a la recuperación frente a fallos de la red manteniendo la garantía de disponibilidad de los servicios de red ofrecidos.

En la mayoría de los casos, tal y como se presenta en [1], las redes actuales de los operadores se dividen en niveles jerárquicos que se detallarán en mayor profundidad a lo largo del presente documento pero, a modo de introducción se puede resumir que se tienen tres niveles. El nivel de acceso que interconecta los clientes de una MAN (*Metropolitan Area Network,* Red de Area Metropolitana), el nivel de tránsito o conexión regional y el nivel de interconexión internacional y con otros operadores. En el núcleo de red, que se extiende desde los routers de acceso hasta el nivel de interconexión, debido a la gran cantidad de tráfico que se cursa, se tienen dos capas de red. Una de ellas es la capa IP/MPLS (*Internet Protocol,* Protocolo de Internet / *Multi-Protocol Label Switching,* Conmutación de etiquetas multi-protocolo) que permite un encaminamiento dinámico en función del destino del tráfico y una capa de transporte.

La red de transporte se encarga de proporcionar conectividad a media y larga distancia entre equipos. Actualmente, una alternativa popular es una red de transporte óptica ya que proporcionan un ancho de banda mucho más elevado que las redes eléctricas convencionales y cada vez están desarrollando una mayor flexibilidad a la hora de transportar el tráfico a múltiples destinos de una forma dinámica [2].

Un caso particular de red de transporte óptico es la malla fotónica que se compone de ROADMs (*Reconfigurable Optical Add Drop Multiplexers*, Multiplexores Ópticos Reconfigurables) interconectados por fibras ópticas que permiten dinámicamente elegir el destino del tráfico emitido por los equipos de la capa IP/MPLS.

Sin embargo, la operación de ambas capas (IP/MPLS y transporte óptico) se encuentra separada y por lo tanto no existe coordinación entre ellas teniendo ambas sus propios mecanismos de supervivencia [3]. Esta separación produce ineficiencias a la hora de recuperar el servicio cuando se produce un fallo y por ello, en general se tiene un sobredimensionado de la red para poder cumplir con los SLAs.

1.1 Motivación del proyecto

Debido a la inexistencia de una operación coordinada entre las diferentes capas de red [3] se producen ineficiencias. Por un lado se tiene una duplicidad de equipamiento lo que hace necesaria una inversión elevada en equipamiento y por otro lado el mantenimiento es más costoso de las redes para garantizar disponibilidad de servicio elevada. Esto lleva a modelos de red con mecanismos de supervivencia muy garantistas como es el caso de la protección 1+1 (expuesto en detalle más adelante).

Es necesario tener en cuenta que no es suficiente la redundancia en el equipamiento para poder ofrecer una disponibilidad del 99.999%, además, los operadores necesitan reparar los fallos en los equipos en unos periodos de tiempo relativamente cortos para cumplir con los objetivos de disponibilidad. En este punto, actualmente se encuentran en la disyuntiva de, o se repara muy rápido los equipos o

se dota de suficiente redundancia a la red para los servicios con requerimientos elevados de disponibilidad. El tipo de servicios que necesitan de alta disponibilidad son tales como las comunicaciones militares, los servicios bancarios, la telemedicina…

En cualquier decisión a tomar por un operador que afecte a su red siempre han de incluirse criterios económicos que apoyen la viabilidad de los cambios que se pretendan introducir. Con esta motivación se realizan estudios tecno-económicos en este trabajo que apoyen o rechacen desde el punto de vista económico los cambios a introducir en la red.

1.2 Objetivos

El objetivo general del proyecto es el estudio de mecanismos de supervivencia multicapa y compararlos con los actuales. Para ello se plantean los siguientes hitos:

1. Estudio del arte de los escenarios de red y tecnologías utilizados en los operadores.
2. Estudio de los mecanismos de supervivencia en redes IP/MPLS, transporte y multicapa.
3. Desarrollo de un modelo analítico para evaluar la disponibilidad en el núcleo de red de un operador.
4. Desarrollo en Omnet ++ de un simulador de red multicapa que permita calcular disponibilidad de red.
5. Validación de los resultados arrojados por el modelo analítico a través de los datos obtenidos del simulador.
6. Evaluación tecno-económica de los resultados obtenidos.
7. Montaje de un demostrador de red multicapa (Routers IP/MPLS sobre nodos de transporte óptico).
8. Desarrollo de un coordinador multicapa para probar la viabilidad de la restauración multicapa.
9. Realización de pruebas y evaluación de los resultados.

1.3 Contenido de la memoria

El presente documento expone en primer lugar un desarrollo del estado del arte en términos de tecnologías de red utilizadas en los operadores de servicios de telecomunicaciones centrándose, en particular, en el tráfico de datos. Una vez presentadas las tecnologías y protocolos utilizados así como sus virtudes y defectos, se recorre el mundo de la supervivencia de red en los escenarios anteriormente mencionados, haciendo hincapié en una justificación económica para garantizar un determinado grado de prestaciones en función de los servicios provistos por la red.

Una vez expuesto el estado del arte y las justificaciones para introducir el concepto de restauración multicapa, se desarrolla un modelo teórico para evaluar las prestaciones desde un punto de vista analítico de la restauración en comparación con los sistemas actuales de supervivencia en los escenarios de red de los operadores. Se ha desarrollado un simulador de red con el objetivo de validar los resultados teóricos. Se ha descrito y el modelado y funcionamiento del simulador y se comparan los resultados obtenidos con el modelo teórico.

A partir de los resultados en términos de disponibilidad de red proporcionados por el simulador, se procede a una evaluación tecno-económica de los datos para medir

de forma cualitativa la variación de costes existente entre los distintos mecanismos de supervivencia de red.

Para finalizar, se desarrolla un prototipo que permita en un entorno con equipamiento real, realizar la restauración multicapa y de este modo presentar su viabilidad en la red de un operador de servicios de telecomunicaciones.

2 Escenario de red y mecanismos de supervivencia de red

En esta sección se va a presentar el escenario de red de un operador nacional típico así como estudiar los diferentes mecanismos de supervivencia en redes de telecomunicaciones.

2.1 Escenarios de Red

Las redes de los proveedores de servicios de telecomunicaciones generalmente se dividen en niveles jerárquicos que suelen estar propiciados por las diferentes tecnologías de red y por los niveles de agregación de tráfico definidos por los operadores para gestionar de un modo más eficiente la red.

Es muy habitual que la jerarquía de red se defina en tres niveles en función de la cercanía al usuario final [1]. Estos niveles son:

- Nivel de red de área metropolitana (MAN): Este nivel incluye desde el acceso a la red por parte de los usuarios finales hasta la agregación del tráfico del área metropolitana. Por lo general, una MAN agrega el tráfico de una o varias provincias en función de parámetros de distancia y tráfico total.
- Nivel de red de núcleo de red: Este nivel agrega el tráfico de todas las MANs, las interconecta entre sí y les proporciona acceso a otros operadores (nivel de interconexión). Incluye los routers de acceso, los routers de tránsito y la parte de los routers de interconexión dedicada al tráfico interno del operador.
- Nivel de red de interconexión: El nivel de interconexión agrega el tráfico del operador con destino a otros operadores. En general, la mayoría del tráfico de los usuarios de un operador se dirige a interconexión (cerca del 70% [Buscar referencia]). En el nivel de interconexión se definen las políticas de relación con otros operadores (peering, proveedor…).

La Figura 1 presenta la definición jerárquica de la red de un operador de nacional expuesta anteriormente. Se trata de una representación genérica que abstrae muchas particularidades de la red, especialmente en el nivel de MAN, pero no se entrará en detalle puesto que el objetivo del proyecto no se enfoca a este segmento de red. A efectos de este trabajo bastará con entender la MAN como el segmento de red que cursa el tráfico de los usuarios entre localizaciones dentro de la misma MAN (por ejemplo sería el caso de una empresa con varias sedes en el área metropolitana).

En el caso de que el tráfico tenga un destino externo a la MAN implicada, la red agrega el tráfico en los routers de acceso, y se dirige a los routers de tránsito que a su vez agregan el tráfico de múltiples áreas metropolitanas. En el nivel de tránsito se distribuye el tráfico entre diferentes regiones (interconexión de los routers de tránsito) y se agrega el tráfico hacia otros operadores (interconexión).

Una vez presentada en líneas generales la jerarquía principal de la red de un operador medio, es importante hacer notar una diferencia sustancial entre las distancias que cubre una MAN y el núcleo de red del operador. Una MAN suele estar limitada a áreas de pocos kilómetros y por lo tanto los enlaces entre los equipos de la MAN no necesitan interfaces de larga distancia. Por el contrario, el núcleo de red tiene que cubrir distancias de centenares de kilómetros, lo que añadido a la necesidad de un mayor ancho de banda para transmitir el tráfico agregado de las MANes, supone un elevado coste si se hace directamente entre los routers.

Esta diferencia lleva a que el núcleo de red necesite, además de una red IP/MPLS (los routers de acceso, tránsito e interconexión) una red de transporte de larga distancia. Esta red de transporte tiene la capacidad de transmitir grandes cantidades de información entre dos puntos remotos. En particular en este estudio se prestará atención a la malla fotónica, concepto que define una red compuesta por nodos ópticos reconfigurables (ROADMs) [2.1.2] capaces transmitir y conmutar información en múltiples longitudes de onda sobre una misma fibra. Esta red de transporte de larga distancia es una red de circuitos con ancho de banda garantizado que tiene la capacidad de configurarse de forma dinámica.

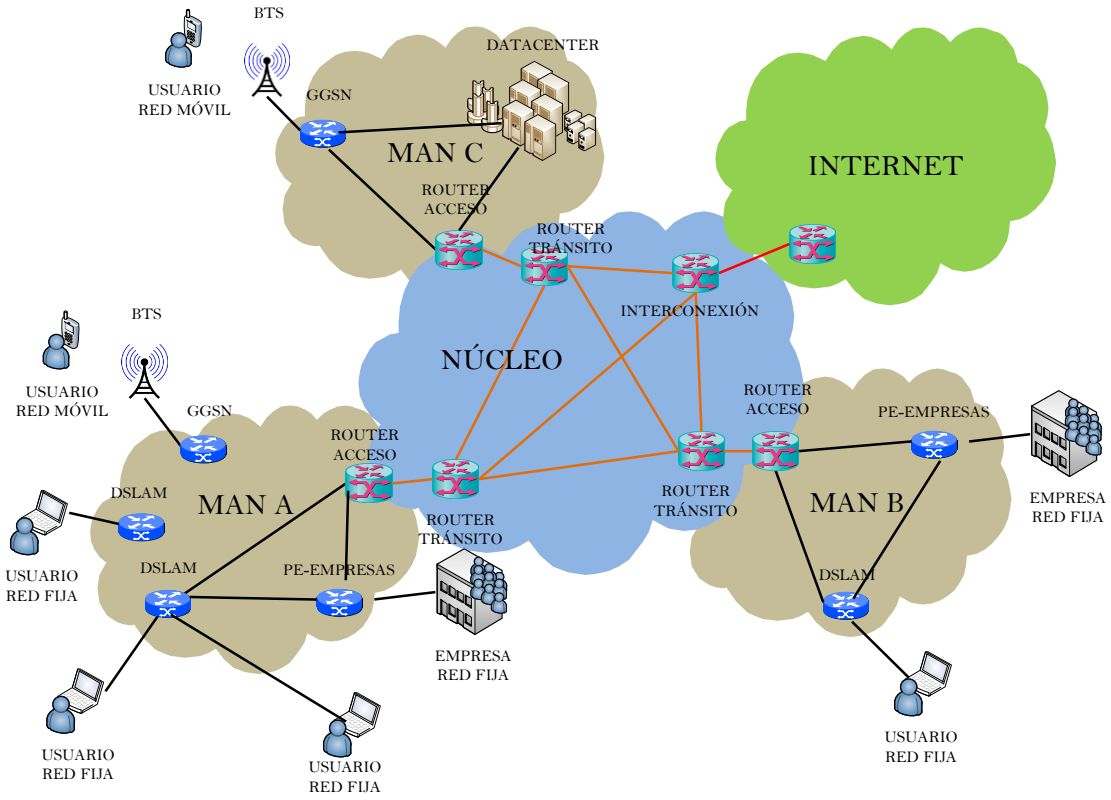

Figura 1 Escenario de red de un operador medio

Prestando atención al concepto de configuración dinámica es interesante recordar el funcionamiento de las redes IP/MPLS actuales. Una red IP/MPLS hace uso de los protocolos de routing OSPF (*Open Shortest Path First*, Primero camino más corto) [4], IS-IS (*Intermediate System To Intermediate System*, Sistema intermedio a sistema intermedio) [5], y protocolos de distribución de etiquetas como LDP (*Label Distribution Protocol*, Protocolo de distribución de etiquetas) [6], es capaz de reconfigurarse automáticamente si se da un cambio en la topología de red. Esto permite que la red pueda continuar operando en entornos cambiantes y por lo tanto hacerla mucho más resistente ante errores así como, haciendo uso de las métricas de enlace, realizar ingeniería de tráfico para gestionar la red de la manera más eficiente posible.

En el caso de las redes de transporte, tradicionalmente se han entendido vulgarmente como “un cable” que, independientemente de las particularidades que tuviera en función del medio en el que se transmitía, era inmutable e invariable y podía funcionar o no, pero siempre unía los dos mismos puntos de la capa de red. Con la aparición de la nueva red de transporte dinámica se permite reconfigurar las conexiones establecidas (por ejemplo los conmutadores intermedios) y por lo tanto se

hace necesario introducir protocolos que permitan operar dinámicamente la red de transporte.

Los protocolos que el IETF ha definido para la operación de la red de transporte óptica son GMPLS (*Generalized Multi-Protocol Label Swithing*, Conmutación de etiquetas multi-protocolo generalizado) [7], OSPF-TE (*OSPF Traffic Engineering,* OSPF de ingeniería de tráfico) [8] y RSVP-TE (*ReSerVation Protocol Traffic Engineering*, Protocolo de reserva con ingeniería de tráfico) con sus extensiones para GMPLS. El conjunto de protocolos estándar que permiten operar una red se conoce como plano de control. Una definición para diferenciar los planos de control puede encontrarse en [9] donde se define como "El plano de control es donde la información de encaminamiento así como las etiquetas son intercambiadas entre los LSR (*Label Swiching Routers*, Encaminadores y conmmutadores de etiquetas)". MPLS es un protocolo de plano de control de tal modo que la información de control debe estar disponible antes de que pueda encaminarse el primer paquete. El encaminamiento de paquetes como tal se realiza en el plano de datos". En definitiva, la definición anterior viene a separar los planos de datos y control por la funcionalidad de los mismos. Mientras por un lado el plano de control es el conjunto de protocolos que define como ha de ser la conmutación de la información (ya sean paquetes, circuitos u otro tipo de recursos a conmutar) y el plano de datos es el que en definitiva transmite la información físicamente.

La existencia de un plano de control permite tanto configurar dinámicamente las conexiones de la capa de transporte como habilitar mecanismos de supervivencia en red operados de forma autónoma por la red.

2.1.1 Capa de Red IP/MPLS

Tal y como se describe en [10], el encaminamiento en la capa de red (en la que se encuentra IP en la torre OSI y a medio camino entre la de enlace y de red se encuentra MPLS) se divide en dos componentes básicos, el control y el encaminamiento. El encaminamiento se realiza a partir de una tabla en la cual se decide por qué interfaz se transmitirá la información recibida. Por su parte el control lo que pretende es construir y mantener dichas tablas de encaminamiento a lo largo de la red para que la información alcance su destino.

El control consiste en uno o más protocolos de encaminamiento que proporcionan el intercambio de información de encaminamiento entre routers así como los procesos (algoritmos) que un router utiliza para a partir de dicha información construir la tabla de encaminamiento. El encaminamiento ha de ser consistente y proporcionar clases equivalentes de tal modo que se pueda agrupar diferentes paquetes bajo una misma categoría de encaminamiento (un ejemplo de ello son los prefijos en conmutación IP).

MPLS utiliza etiquetas para conmutar paquetes como su propio nombre indica. Para poder entrar en más detalle sobre el plano de control MPLS se ha de explicar que se entiende por etiqueta en redes de comunicaciones. Una etiqueta es una estructura de longitud fija sin estructura interna que debe ser corta. Una etiqueta no codifica ninguna información acerca de la cabecera de la capa de red de tal manera que no incluye nada relacionado con las direcciones de fuente o destino de la unidad de información a conmutar.

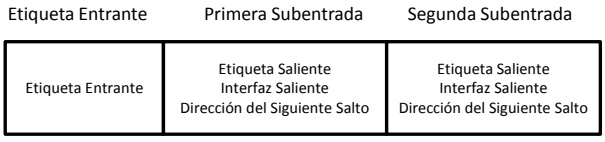

Figura 2 Entrada de una tabla de encaminamiento de etiquetas [10]

La tabla de encaminamiento de etiquetas es mantenida por un LSR y en la Figura 2 se puede observar un ejemplo de entrada de este tipo de tablas. Para explicar de un modo más gráfico este concepto se muestra en la Figura 3 un ejemplo de etiquetado y conmutación basada en dicho etiquetado en una red básica de ejemplo.

El plano de control completaría la tabla de encaminamiento de etiquetas del nodo W tal y como se muestra en la Tabla 1. El nodo V etiqueta todos los paquetes provenientes del host A con dos etiquetas diferentes dependiendo del destino del flujo, en particular, en una red IP/MPLS, el LSR V realiza una asociación entre la dirección de red IP de destino (B o C) y una etiqueta (15 y 10 respectivamente). En W se examina las etiquetas de procedencia y se conmuta en consecuencia hasta los LSR X e Y que proceden a deshacer el etiquetado para que el paquete llegue de un modo transparente a los hosts de destino B y C.

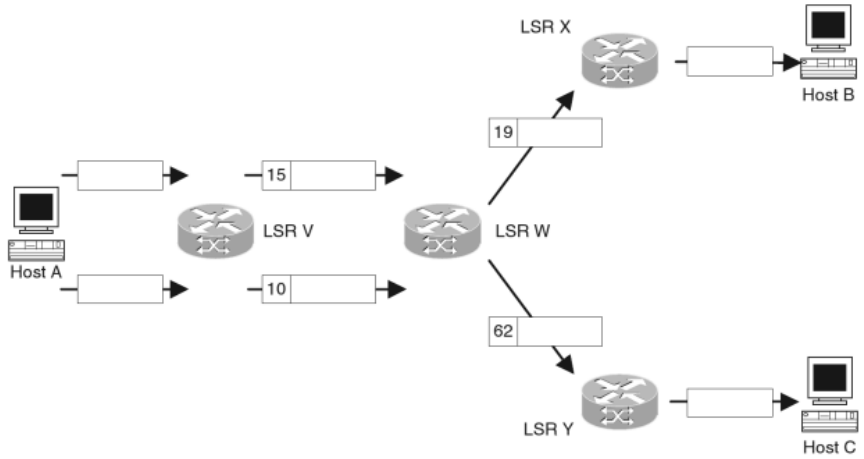

Figura 3 Ejemplo de etiquetado y conmutación en red MPLS [10]

La conmutación que se realiza en W consiste en un intercambio de etiquetas que tienen sentido solo a nivel de siguiente salto, es decir, la etiqueta 19 y 62 sólo tienen sentido para X e Y pudiendo incluso haber sido las mismas etiquetas sin problema ya que los LSR podrían seguir tomando decisiones distintas.

Interfaz de Entrada	Etiqueta de Entrada	Interfaz de Salida	Etiqueta de Salida
Desde LSR V	15	A LSR X	19
Desde LSR V	10	A LSR Y	62

Tabla 1 Tabla de encaminamiento en nodo W

Visto así, MPLS no aportaría ninguna diferencia respecto al encaminamiento IP puro (obviando la diferencia de longitud de la etiqueta respecto a la dirección IP y el coste computacional de calcular el encaminamiento de cada una). En cambio, una de las ventajas principales de MPLS es que permite transportar diferentes capas de red siendo agnóstico de si se transporta IP u otro protocolo de red diferente.

Además MPLS permite una jerarquía de LSPs (*Label Switched Paths*, Caminos de conmutación por etiquetas). Un LSP puede definirse como un flujo de tráfico identificado por una fuente, un destino y unas determinadas propiedades de calidad de tráfico. Esta jerarquía permite tratar de una forma uniforme múltiples LSPs manteniendo sus particularidades en los extremos de la jerarquía. Este concepto

proporciona una mayor escalabilidad en el núcleo de red ya que se puede manejar una mayor cantidad de flujos de tráfico haciendo uso de un número menor de etiquetas. En la Figura 4 se puede observar un ejemplo de la jerarquía de LSPs en el cual se establece un túnel entre los LSR W y Z que desde el punto de vista de los LSPs encapsulados se puede ver como una FA (*Forwarding Adjacency*, Adyacencia de conmutación) entre W y Z. Esta FA permite presentar de un modo transparente desde el punto de vista del encaminamiento a los LSPs encapsulados, es decir, para dichos LSPs lo que se puede observar es que desde el LSR W se salta al LSR Z.

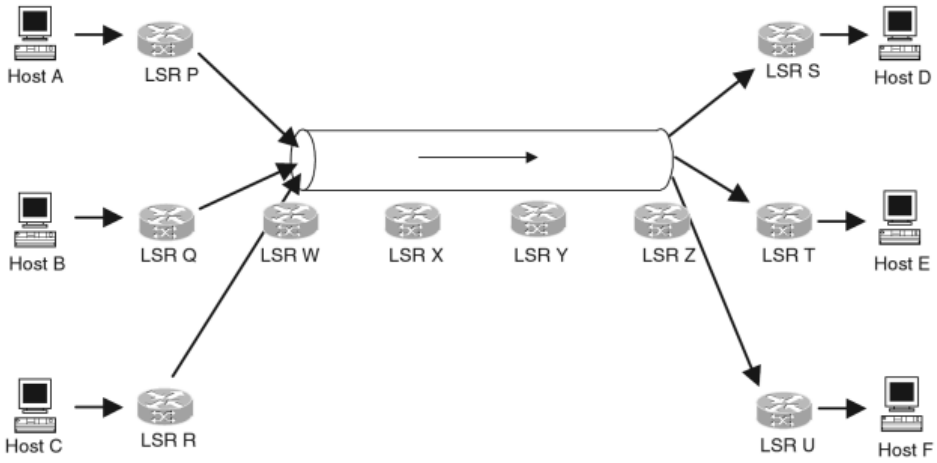

Figura 4 Jerarquía de LSPs [10]

Una vez presentado el funcionamiento básico de MPLS, se procede a exponer la justificación de las extensiones de MPLS para la ingeniería de tráfico (extensiones TE) como paso previo para motivar la aparición de GMPLS en el terreno de las redes de transporte [11].

Los objetivos de la ingeniería de tráfico son, entre otros, evitar situaciones de congestión en la red mientras se tenga recursos infrautilizados, asegurar determinadas características para el tráfico por determinados caminos (conseguir latencias reducidas para servicios en que este parámetro es crítico como la telefonía), asegurar la existencia de recursos de transmisión disponibles, priorizar el tráfico en caso de no poder cursar la totalidad del mismo como por ejemplo en caso de un fallo en la red.

Desde el punto de vista de negocio, un operador puede obtener rédito de la ingeniería de tráfico a través de múltiples aproximaciones que pueden generalizarse en dos.

1. Dimensionar de un modo más preciso los recursos de red necesarios para garantizar el cumplimiento de los SLAs.
2. Ofrecer servicios especiales con garantías adicionales respecto a disponibilidad, ancho de banda, retardo…

Para ilustrar la influencia de la ingeniería de tráfico, supongamos un servicio de VoIP (*Voice over IP*, Voz sobre IP) para el cual estudios han demostrado que el retardo máximo aceptable es de 250 milisegundos [12]. Se tiene un servicio adicional de transferencia de ficheros a través de FTP (*File Transfer Protocol*, Protocolo de transferencia de ficheros) sin requerimientos especiales, es decir, se considera un servicio BE (*Best Effort,* Mejor esfuerzo).

En una red como la de la Figura 5 el resultado de aplicar un algoritmo de cálculo del camino más corto directamente provocaría que ambos servicios fueran cursados por los caminos mostrados en la figura. Como se puede observar en la Tabla 2 el

retardo obtenido para el servicio de VoIP no es suficiente para cumplir con los requisitos del servicio. Frente a esto hay dos alternativas, sustituir los enlaces entre C y F y entre F y G para reducir su retardo con el consiguiente coste económico que supone esto o por el contrario aplicar técnicas de ingeniería de tráfico para desviar el tráfico del servicio de VoIP por el camino superior obteniendo un retardo mucho menor como se puede apreciar en la Figura 6.

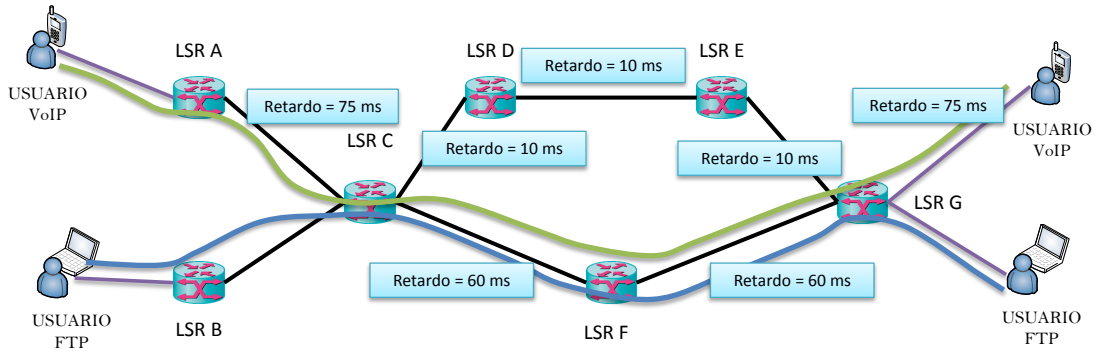

Figura 5 Encaminamiento basado en camino más corto

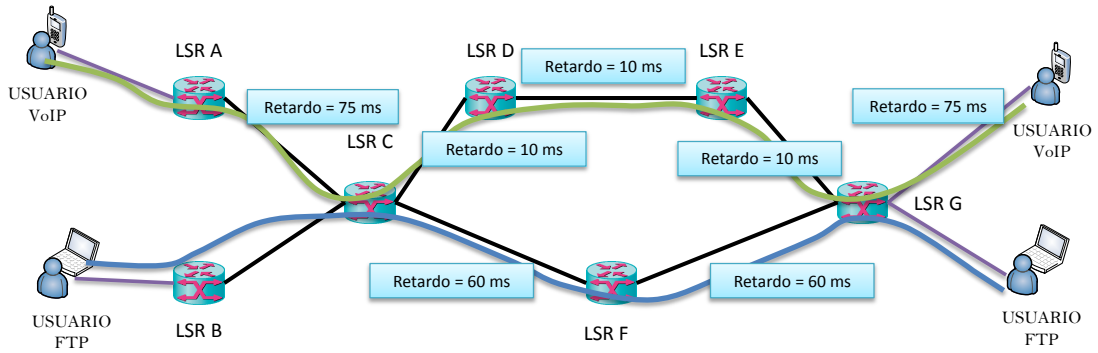

Figura 6 Encaminamiento haciendo uso de la ingeniería de tráfico

Servicio	Camino	Retardo Acumulado
VoIP (Figura 5)	Fuente – A – C – F – G – Destino	270 milisegundos
FTP (Figura 5)	Fuente – B – C – F – G – Destino	270 milisegundos

Tabla 2 Retardo para los servicios con/sin TE

El método que MPLS tiene para fácilmente cursar tráfico por un camino arbitrario es el uso de RSVP-TE con el objeto ERO (*Explicit Route Object*, Objeto de ruta explícita) [13]. Este procedimiento permite encaminar los paquetes de determinado flujo de tráfico por un LSP con un camino definido por el ERO independientemente de las métricas que haya definidas en la red por los protocolos de encaminamiento.

Una de las características adicionales de MPLS-TE es la definición de 8 niveles de prioridad para el tráfico cursado (de 0 como mayor prioridad a 7 como menor prioridad) permitiendo un control de acceso sobre los recursos pudiendo así garantizar el tráfico para determinados servicios.

El uso combinado de la selección explícita de camino con la priorización de flujos de tráfico abre un abanico de posibilidades al operador para definir servicios adaptados a determinadas garantías dentro de la red.

2.1.2 Red de transporte

La definición que la ITU (*International Telecommunications Union,* Union Internacional de Telecomunicaciones*)* de transporte es "el proceso funcional de transferir información entre diferentes localizaciones" [14]. Si bien esta definición puede ser demasiado general para lo que se entiende como red de transporte, explorando más profundamente la recomendación de la ITU se encuentra la siguiente definición "Los recursos funcionales de una red que traslada información de usuario entre localizaciones". La palabra fundamental que marca la diferencia entre las definiciones es que la información que se transferida es de usuario [15] concepto que proporciona una clara separación entre capas en la estructura de red. Bajo esta asunción se puede crear una estructura de red basada en capas con islas conectadas por una o múltiples redes de transporte como se muestra en la Figura 7. Como se puede observar, la red de transporte "sirve" conectividad a las capas "usuarias" de la misma para conseguir interconectar múltiples redes de usuario entre si.

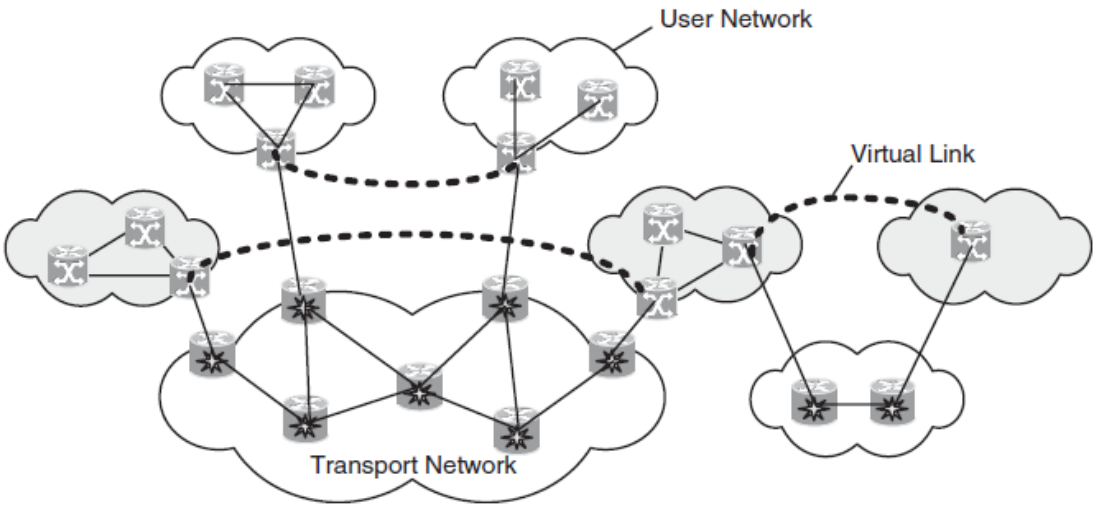

Figura 7 Red de transporte que proporciona conectividad entre islas de redeso [15]

Siguiendo entonces la definición anteriormente expuesta, prácticamente todas las redes podrían entrar en dicha definición pero una regla es generalmente aplicada de tal modo que para considerar una red de transporte debe existir un cambio de tecnología de transmisión en la frontera entre la red usuario y la red de transporte. Un ejemplo de este cambio de tecnología se daría entre una red Ethernet, una red SDH (*Synchronous Digital Hierarchy*, Jerarquía digital síncrona) o red WDM (*Wavelength Division Multiplexing*, Multiplexación por división en longitud de onda) con una red IP.

Es importante precisar en este punto que la capa de transporte tal y como se entiende en este tipo de redes nada tiene que ver con la capa de transporte del modelo OSI definido en la recomendación de la ITU X.200.

Algunas de las principales tecnologías de transporte son las siguientes:

1. **Gigabit Ethernet**: Se ha convertido en una tecnología muy utilizada en LANs (*Local Area Network*, Redes de área local) y se despliega también de un modo significativo en el área metropolitana.

2. **TDM** (*Time Division Multiplexing*, Multiplexado por division en tiempo): Este tipo de técnica basa la transmisión en diferentes periodos de tiempo para separar los flujos de información ha creado dos grupos de estándares similares, SDH y SONET (*Synchronous Optical NETwork*, Red óptica síncrona) desarrollados por la ITU y por el American National Standards Institute respectivamente.
3. **WDM**: Esta técnica consiste en multiplexar varias señales ópticas en la misma fibra haciendo uso diferentes frecuencias portadoras en el espectro óptico. Se divide el espectro en canales con un ancho de rejilla variable en función de la evolución de los filtros ópticos (100, 50 o 25 GHz) permitiendo transmitir en cada canal de la rejilla una señal distinta y por lo tanto se incrementa enormemente el ancho de banda transmisible por una fibra. En la tecnología WDM se puede diferenciar a partir de la densidad de las longitudes de onda utilizables y por lo tanto el ancho de banda total utilizable dos tecnologías, CWDM (*Coarse Wavelength Division Multiplexing*, Multiplexado de división en longitud de onda grueso) y el DWDM (*Dense Wavelength Division Multiplexing*, Multiplexado de división en longitud de onda denso) en los cuales CWDM limita el ancho de banda máximo por longitud de onda a 2.5 Gbps DWDM consigue tasas más elevadas llegando a superar la centena de Gigabits por segundo.
4. **Fiber Switching**: Se considera como la menor unidad de conmutación la fibra óptica en si, siendo transparente totalmente si lo que se transmite es WDM, SDH o cualquier otro tipo de tecnología. Un equipo que conmute fibras sería capaz de extraer toda la información proveniente de una fibra y replicarla en otra fibra destino.

Una vez expuestas algunas de las tecnologías de redes de transporte, se presentan algunas de las topologías más habituales para estas redes con el objetivo de facilitar la comprensión y el funcionamiento de los mecanismos de supervivencia en redes que se expondrán en capítulos posteriores. Entre las topologías más habituales destacan los anillos simples y bidireccionales (Figura 8), interconexión mallada de anillos (Figura 9), redes punto a punto (Figura 10) y redes malladas (Figura 11).

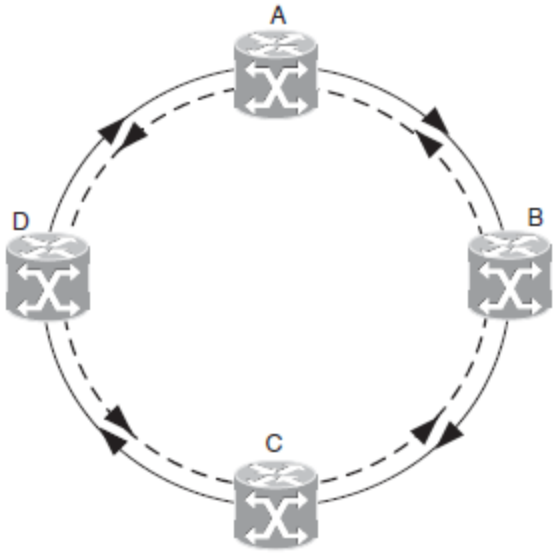

Figura 8 Red en anillo bidireccional [15]

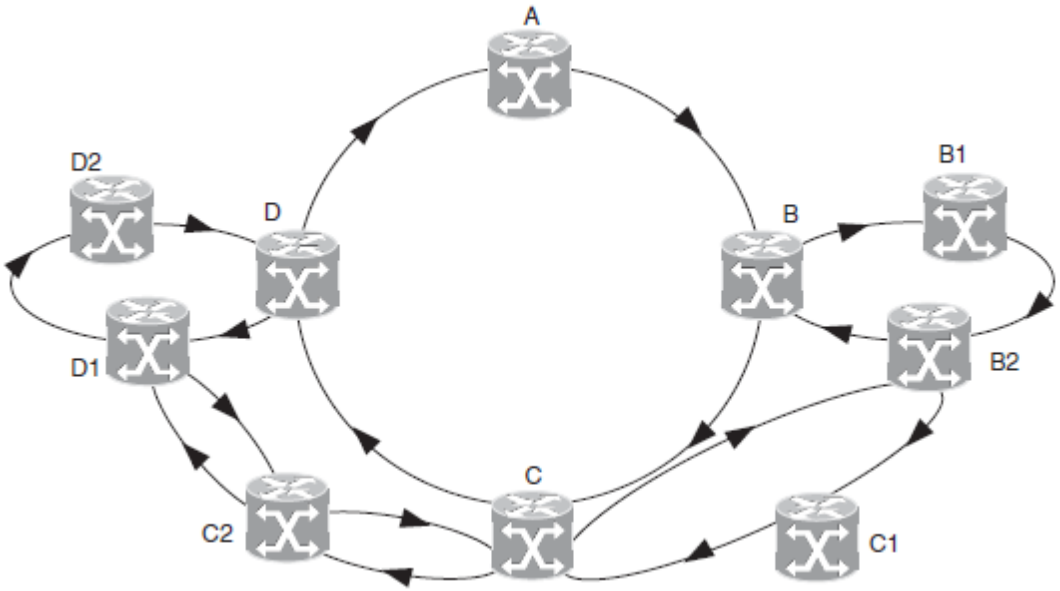

Figura 9 Interconexión mallada de anillos [15]

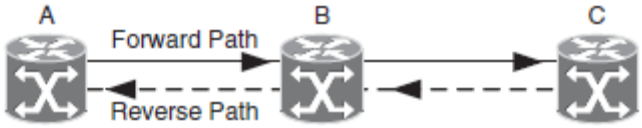

Figura 10 Redes punto a punto [15]

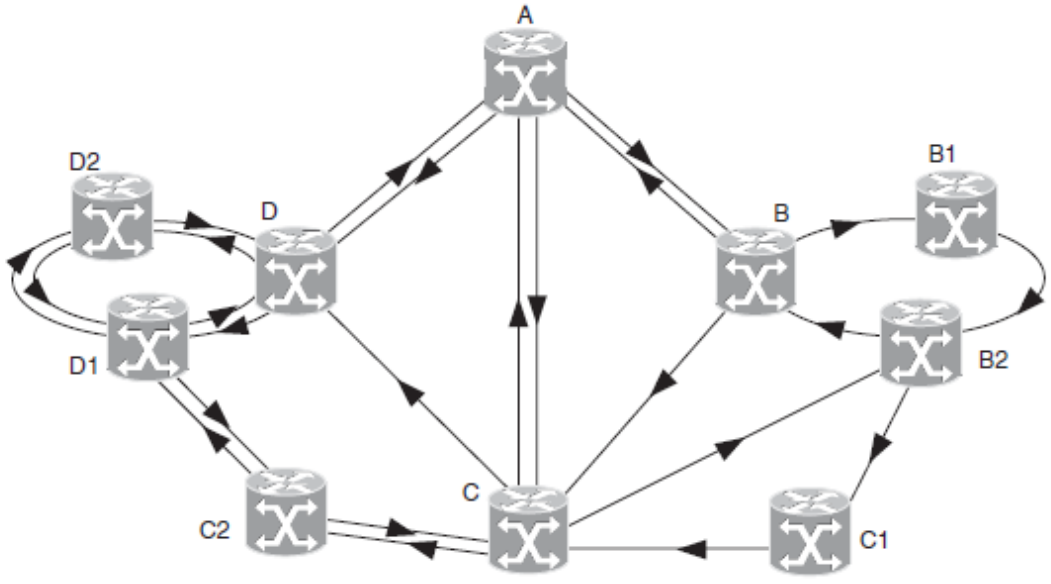

Figura 11 Red mallada [15]

Una vez presentado el plano de datos de las redes de transporte, se presenta el plano de control GMPLS para las redes de transporte. En primer lugar es importante tener en cuenta que consiste en una generalización del protocolo MPLS y que pretende aglutinar los conceptos de las redes de paquetes (redes IP típicamente) con las tecnologías de las redes de transporte que pueden conmutar circuitos como es el caso de las redes WDM en las cuales el circuito conmutado es la longitud de onda. Tradicionalmente, las redes de transporte han sido configuradas y provisionadas de un

modo manual debido a la necesidad de una gran planificación en la mayoría de los casos (ecualización de amplificadores ópticos, mediciones de los vanos de fibra, degradación de señales) y llevaba días e incluso semanas establecer una conexión entre dos extremos de una red. Este tipo de proceso es dado a fallos que pueden prolongar (sino crear inestabilidades o pérdidas de servicio en la red en el peor de los casos) ya que dificulta enormemente la automatización de la red.

El nacimiento de GMPLS pretendía introducir un plano de control en la red de transporte para evitar la elevada intervención humana en el proceso de provisión y mantenimiento de la red de transporte. La disyuntiva nacía a la hora de decidir si se apostaba por una pila de protocolos totalmente nueva y diseñada específicamente para las redes y tecnologías objetivo permitiendo una gestión muy eficiente de cada tecnología. La desventaja de esta aproximación es que la creación de una nueva pila de protocolos suponía un elevado esfuerzo para los fabricantes a la hora de ponerse de acuerdo e implementar los protocolos para cada tecnología de red de transporte. Además, hay una tendencia en las redes de comunicaciones en tener diferentes tramos de la red diferentes redes de transporte lo cual, en caso de tener planos de control específicos de cada tecnología supondrían un problema a la hora de interoperar.

Con la creciente popularidad de las redes WDM al final de los noventa, los fabricantes comenzaron a buscar el plano de control más adecuado para dichas redes y se dieron cuenta de que la mayoría de las operaciones básicas en una red WDM se asemejaban desde un punto de vista lógico al protocolo MPLS (etiqueta de entrada, interfaz de entrada) a conmutar a (interfaz de salida, etiqueta de salida) que es fácilmente relacionado con WDM (fibra de entrada, longitud de onda de entrada) a (longitud de onda de salida, fibra de salida). A partir de esta observación nació Multi-Protocol Lambda Switching que prácticamente cogía prestados todos los protocolos de MPLS y los particularizaba para el caso de conmutación de longitudes de onda.

Una vez en este punto, se decide generalizar para el resto de tecnologías las extensiones necesarias ya que, en definitiva, el tráfico entre una fuente y un destino en una red de transporte puede modelarse como un LSP y por lo tanto, el objetivo de la red de transporte debe ser dar soporte para la creación y mantenimiento en condiciones cambiantes de los LSPs. Para ser rigurosos, definiremos un LSP en una red de transporte como una serie contigua de recursos de conmutación capaces de entregar tráfico entre dos puntos.

En GMPLS se define, con el objetivo de particularizar la tecnología de conmutación de la red de transporte, los Switching Types (tipos de conmutación) que básicamente establece una definición estándar de las conmutaciones posibles en el protocolo como son por ejemplo los PSC (*Packet Switch Capable*, Capacidad de conmutar paquetes) que es la conmutación que realizan los routers, LSC (*Lambda Switch Capable*, Capacidad de conmutar longitudes de onda) que permite modelar redes WDM y más tipos de conmutación.

Un aspecto importante a tener en cuenta en las redes de transporte y especialmente en el caso de las redes de transporte óptico es que el plano de control se transmite fuera de banda, es decir, se necesita una red adicional para transmitir la señalización puesto que el plano de datos no está habilitado hasta que los recursos se configuran adecuadamente. En comparación con una red IP/MPLS típica, una vez se tiene la conexión física entre dos interfaces y se habilitan los protocolos de encaminamiento, estos inundan la información por la red sin mayores requisitos. En el caso de la red de transporte, al necesitar de la configuración de los recursos ópticos antes de que esté funcionalmente disponible la conexión, se necesita esta red

alternativa para informar a los nodos de la configuración necesaria para habilitar la transmisión.

GMPLS al igual que MPLS define jerarquías en este caso de tecnologías de conmutación como se presenta en la Figura 12 que permite encapsular unas tecnologías en otras y así definir cómo se pueden relacionar los diferentes tipos de tecnologías de conmutación.

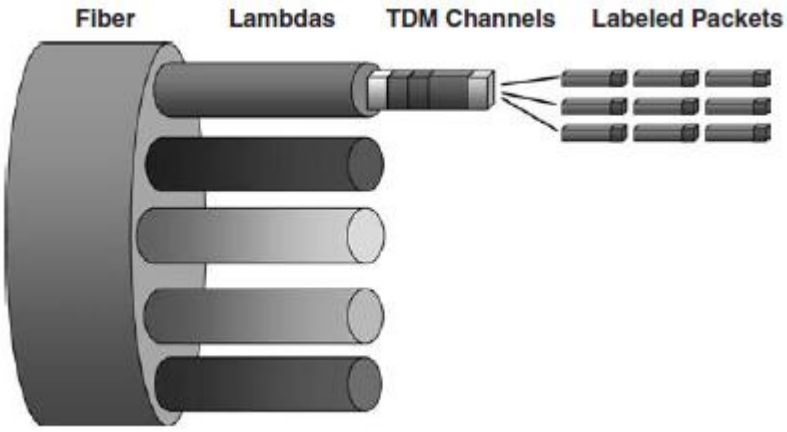

Figura 12 Jerarquía de Switching Types [15]

En este documento, de ahora en adelante se va a prestar atención a redes de transporte DWDM con topologías malladas ya que proporcionan una mayor dinamicidad para grandes flujos de tráfico al poder transmitir grandes cantidades de información a grandes distancias. También se asume que gracias a GMPLS se puede realizar una operación automática de provisión de recursos de la capa de transporte.

2.2 Supervivencia en redes.

La supervivencia en redes de comunicaciones consiste en la capacidad de la red para mantener el servicio en caso de fallos en la misma. La presencia de fallos en una red es algo muy habitual y frente a lo cual el operador debe estar preparado y definir estrategias para garantizar que puede cumplir con los SLA contraídos con sus clientes.

Los fallos se pueden dar desde por fallos de configuración de los equipos en operaciones de mantenimiento o provisión de nuevos servicios, degradación de los equipos por antigüedad, cortes de fibras por excavadoras, incendios en edificios, cortes de fibras submarinas. En [16] la NRSC (*Network Reliability Steering Committee*, Comité para la confiabilidad de la red) estadounidense en su informe bianual de 2006 a 2007 presenta muchas de las causas que desembocan en fallos de red. En muchos casos, los problemas que originan fallos en una red no afectan únicamente a un elemento de la misma, es el caso por ejemplo de los incendios en edificios y los cortes de fibras.

Otros trabajos como [17] justifican la existencia y frecuencia de los fallos en las fibras ópticas presentando estadísticas que incluso en los casos en los que se ha procedido al despliegue con el mayor de los rigores para evitar cortes arrojan datos de 4.39 cortes por año y por 1000 millas de fibra. Este dato podría sonar pequeño, pero en EEUU en 2004 se encontraban instalados más de 100000 millas de fibra lo que suponía un corte al día. También se referencian otros estudios llegando a incrementar esta cifra.

Duración	Efectos Principales/ Características
< 50 mseg	Prácticamente sin efecto. Los sistemas de protección garantizan la llegada de la mayoría de los paquetes y protocolos como TCP recuperan las sesiones afectadas sin mayor incidencia
50 mseg – 200 mseg	Menos del 5% de las conexiones de voz notan el fallo.
200 mseg – 2 seg	Antiguas conexiones de bancos necesitarían ser reiniciadas. TCP tendría dificultades para gestionar este tiempo de desconexión.
2 seg – 10 seg	Todos los servicios de conmutación de circuitos se desconectan. Sesiones de X.25 también se desconecta. Errores de páginas web no disponibles. Los timeouts de TCP se ponen en marcha.
10 seg – 5 min	Todas las llamadas de voz se pierden. Los programas sobre TCP dejan de funcionar. Los usuarios comenzarían a intentar re-llamadas masivas. Cambios en las topologías de red ya que los routers comenzarían a reenviar LSAs (*Link State Advertisements*, Anuncios de estado de enlace) informando de los fallos.
5 min – 30 min	Efectos sobre los negocios. El corte sería bastante visible para los usuarios.
>30 min	El regulador entraría a determinar los daños a la sociedad por el corte sufrido. Los SLAs se verían afectados en su totalidad.

Tabla 3 Repercusión de los fallos en las redes según su duración

Con el objetivo de cuantificar en términos económicos el tiempo que un servicio no está disponible se han realizados múltiples estudios entre los cuales [18] y [19] que proporcionan la Tabla 4 y Tabla 5 respectivamente:

Aplicación de Negocio	Coste por Minuto de Fallo en el Servicio
Gestion de cadena de suministros	11,000 $
Comercio electrónico	10,000 $
Servicio de atención al cliente	3,700 $
ATM/POS/EFT	3,500 $
Gestión financiera	1,500 $
Gestión de capital humano	1,000 $
Mensajería	1,000 $
Infraestructuras	700 $

Tabla 4 Estimación de coste por minuto de fallo en [18]

Aplicación de Negocio	Coste por Hora de Fallo en el Servicio
Operaciones de bolsa	6,450,000 $
Autorizaciones de tarjetas de crédito	2,600,000 $
Canales de tele-tienda	139,000 $
Servicios de pago por visión	150,000 $
Servicios de venta por catálogo	90,000 $
Centros de reserva de aerolíneas	89,500 $
Líneas 900	54,000 $
Servicios de mensajería	28,250 $
Coste medio de los fallos medidos	84,000 $

Tabla 5 Estimación de coste por hora de fallo en [19]

Antes de definir los mecanismos de supervivencia se va a introducir el concepto SRLG (*Shared Risk Link Group*, Grupo de riesgo compartido) para explicar las implicaciones de un fallo en una determinada área de una red. Desde el punto de vista de los esquemas de red, pudiera parecer que todos los enlaces son independientes uno de otro y que cualquier fallo que afecte a uno de ellos no afecta a otro enlace. En la realidad esto es bien distinto puesto que las canalizaciones a través de las cuales se tiende la fibra óptica comparten más de una fibra con destinos distintos (como es lógico por motivos económicos) y por lo tanto equipos distintos.

En la Figura 13 se presenta un ejemplo de SRLGs de múltiples enlaces que, en el caso del SRLG número 1 agrupa tres enlaces como consecuencia de seguir la misma canalización. Los SRLG 7, 8 y 9 incluyen dos enlaces y el resto sólo 1 enlace.

Las implicaciones de este hecho vienen de uno de los motivos de fallo a tener en cuenta en cualquier modelo de fallos, los cortes de fibra debido a excavadoras que por desconocimiento o falta de precaución eliminan canalizaciones completas dejando múltiples fibras cortadas. Es lógico pensar que a partir de ese único evento de fallo se ha tenido una afección mayor que la de un único enlace, por lo que se define el concepto SRLG que agrupa todos los enlaces que discurran por una canalización compartida. Por lo tanto un SRLG agrupa todos los elementos de red susceptibles de ser afectados por un fallo en concreto.

Por tanto, desde el punto de vista de los fallos, lo que se debe tener en cuenta son los SRLGs y no los enlaces a la hora de modelar los efectos de cada evento. En cualquier caso, de cara a los escenarios de red utilizados en este estudio, se asume que cada enlace es un SRLG y que por lo tanto, no existe la posibilidad de que un fallo afecte a más enlaces.

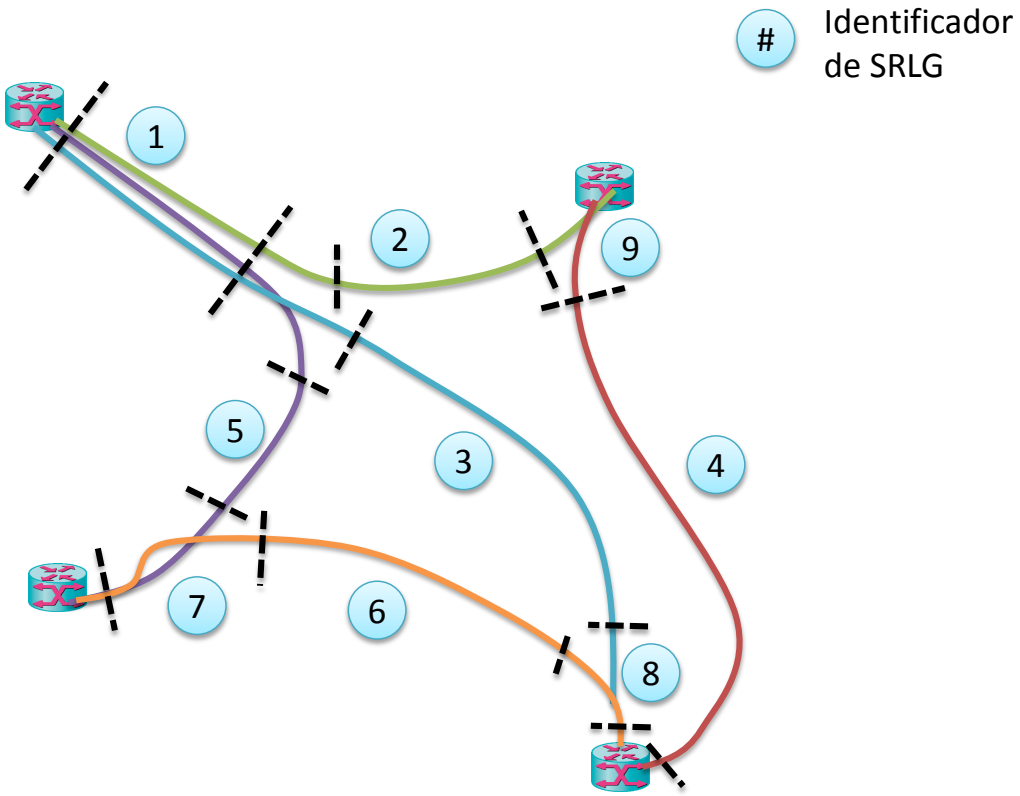

Figura 13 Ejemplo SRLGs

Una vez se ha definido el concepto de SRLG, se procede a detallar los mecanismos de supervivencia genéricos en redes y posteriormente se particularizará para las dos capas de red anteriormente mencionadas, la capa IP/MPLS y la capa de transporte. Para ello, en primer lugar se expone la unidad de medida para cuantificar la capacidad de la red para proporcionar servicio a los clientes.Se define disponibilidad como:

$$Disponibilidad = 100 \cdot \frac{Tiempo\ \text{sin}\ servicio}{Tiempo\ total\ de\ operación}$$

Esta expresión permite relacionar directamente los SLA con una medida directamente obtenible de la red. En función de lo crítico del servicio existen diferentes niveles de disponibilidad que representan un determinado intervalo de tiempo sin servicio a lo largo de un año (Tabla 6).

Objetivo de Disponibilidad [%]	99.9	99.99	99.999	99.9999
Tiempo sin servicio en un año [min]	525.6	52.56	5.256	0.5256

Tabla 6 Relación entre el tiempo de fallo en el servicio y la disponibilidad.

Hay diferentes métodos para garantizar la supervivencia de red pero principalmente un operador tiene tres opciones. En primer lugar puede construir una red con equipamiento muy robusto que no falle prácticamente nunca, esto es incrementar el MTBF (*Mean Time Between Failures*, Tiempo medio entre fallos). Esto dista mucho de ser realizable ya que siempre hay cuestiones que escapan al control del operador como se ha expuesto previamente en esta sección como causas de los fallos en las redes de telecomunicaciones. Como segunda opción se tiene la reducción

del MTTR (*Mean Time To Repair*, Tiempo medio entre reparaciones) lo cual podría llevar a conclusiones absurdas para casos como los objetivos de disponibilidad cercanos a los 9 nueves que implicaría reparar un fallo en menos de cinco minutos desde su detección. Es evidente que no es una alternativa válida por sí sola y que sería costosísima. Por último, la opción que es realmente viable es dotar a la red de mecanismos de supervivencia de tal modo que mientras se procede a reparar el equipamiento que ha sufrido el fallo, la red pueda continuar operando de un modo suficiente para garantizar el cumplimiento de los SLAs.

Los mecanismos existentes actualmente para respuesta frente a fallos son protección y restauración que se explican más detalladamente a continuación:

Protección

Los mecanismos de protección se basan en incluir recursos adicionales en la red con la función específica de proporcionar conectividad en caso de fallo de un modo directo. En particular, la protección se realiza incluyendo equipamiento que se encuentre en SRLGs completamente disjuntos de tal modo que un fallo que afecte a un SRLG en la conexión principal no afecte al camino de protección. Típicamente hay tres esquemas de protección que serían protección 1+1, 1:1 y N:M. Las diferencias existentes entre los tres son (como se muestra en la) el uso de los recursos para el caso de las 1+1 y 1:1. En el caso 1+1 el tráfico se reparte entre los recursos disponibles mientras que el caso 1:1 tiene la mitad de los recursos ocupados al 100% y los recursos de protección sin uso (Figura 14).

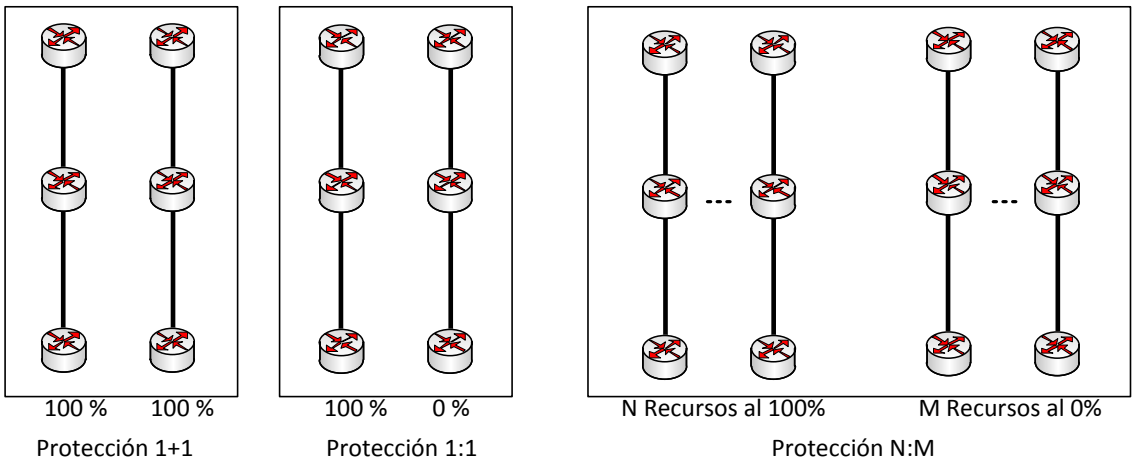

Figura 14 Esquemas de protección de red

La protección N:M en cambio, asume una relación diferente entre los recursos utilizados para proteger determinados flujos de tráfico de tal modo que pueden existir modelos de protección con elevado número de recursos de backup, un ejemplo sería una protección 2:3 o por el contrario un número de recursos de protección inferior como sería el caso 2:1. En caso de fallo, el esquema N:M en que N<M permite protegerse frente a múltiples fallos sin pérdida de tráfico mientras que los casos en que N>M, los flujos de tráfico entran en contienda por los recursos de protección existentes punto en que los métodos de ingeniería de tráfico permiten garantizar mayor grado de disponibilidad y por lo tanto priorizar unos flujos sobre otros.

En la literatura, publicaciones como [20] presentan de un modo más detallado los mecanismos de protección para las redes tanto de transporte óptico como para redes IP/MPLS.

Restauración

El concepto de restauración nace con el objetivo de reducir el coste de los esquemas de protección de red. Mientras los esquemas de protección mantienen un elevado número de recursos de red sin utilizar de un modo parcial o total, la restauración permite hacer uso de recursos de red para recuperar tráfico sin necesidad de tener una previa reserva de los mismos. Los recursos a utilizar para recuperar el tráfico se calculan en el momento en que se produce el fallo de tal modo que estos pueden ser utilizados por varios flujos de tráfico si tener asignados previamente dichos recursos. La restauración permite un uso más eficiente de los recursos de red que la protección. Como desventaja, la red se comporta de un modo menos predecible además de que lleva mayor tiempo la restauración de los flujos de tráfico al tenerse que calcular y provisionar la alternativa para recuperar el flujo de tráfico afectado por el fallo.

2.2.1 Supervivencia en redes IP/MPLS

La supervivencia en redes MPLS debe tener en cuenta que en muchas ocasiones, los fallos que afectan a los servicios no son propios de la red IP/MPLS en sí y por lo tanto puede continuar operando como si nada hubiera sucedido [21]. La mayoría de redes MPLS utilizan protocolos de encaminamiento IP para distribuir la información de la topología de red permitiendo de este modo que la señalización de MPLS sea consciente de los cambios de la topología de red y así señalizar de nuevo los LSP en caso de fallos en la red.

Para recuperación rápida de fallos, los caminos MPLS se pueden provisionar de un modo duplicado utilizando recursos MPLS distintos permitiendo en caso de error conmutar rápidamente al LSP de backup provisionado previamente. En este sentido, esto es lo que encajaría como mecanismo de protección en redes MPLS y son conocidos como FR (*Fast Re-route*, Reencaminamiento rápido).

La restauración está implícita en protocolos de red como IP/MPLS debido a que se tratan de protocolos no orientados a conexión. Esto permite que si en determinado momento un nodo de la red deja de recibir información de estado de enlace de un nodo vecino, dicho nodo procederá a eliminar (tras los correspondientes temporizadores) la información obtenida y por lo tanto cambiará su tabla de rutas para alcanzar los destinos disponibles de la red. Los protocolos de encaminamiento son los encargados de resolver las inconsistencias en la topología debido a cambios de estado en los enlaces.

Por definición, la restauración implicará una pérdida de información sustancial, el único modo de que no fuera así es que se informara el fallo y se calculara una alternativa al mismo en toda la red en tiempos realmente pequeños. Esto tendría el problema del exceso de inundación de información de estando creando una sobrecarga de la red difícilmente justificable en el uso normal de la misma. Las causas de la pérdida de información serían las siguientes:

1. El tiempo que tarda en detectar y notificar el fallo del recurso de red. En protocolos como OSPF y LDP puede tardar varios segundos.
2. Se descarta la información porque al detectarse el fallo no se encuentra una ruta viable para entregarla.
3. Se descarta porque la única ruta factible proviene del nodo que envía la información (convergencia de los protocolos de encaminamiento).

Como justifica [21] muchos proveedores de servicios prefieren duplicar completamente la red de tal modo que todo router y enlace tiene un backup exactamente igual y así cualquier fallo es solventado rápidamente. Además se

proporcionan medidas del tiempo que lleva el proceso de restauración situándolo en cantidades superiores a 30 segundos muy superiores a los 50 o 60 milisegundos típicos de la protección MPLS.

La Figura 15 presenta un ejemplo de protección 2:1 en redes IP/MPLS en el cual se tiene un camino de protección reservado y sin tráfico (azul) utilizando un camino menos óptimo en número de saltos para proteger cualquier fallo que pueda producirse en los LSP primarios verde y rojo. Para que la protección sea efectiva y de un tiempo reducido, es necesario que se informe del fallo en poco tiempo. Para ello pueden utilizarse mensajes de notificación que, en el momento que un nodo detecta algún problema en la red, éste informa al creador del LSP del mismo para que emprenda las acciones oportunas para mantener el tráfico.

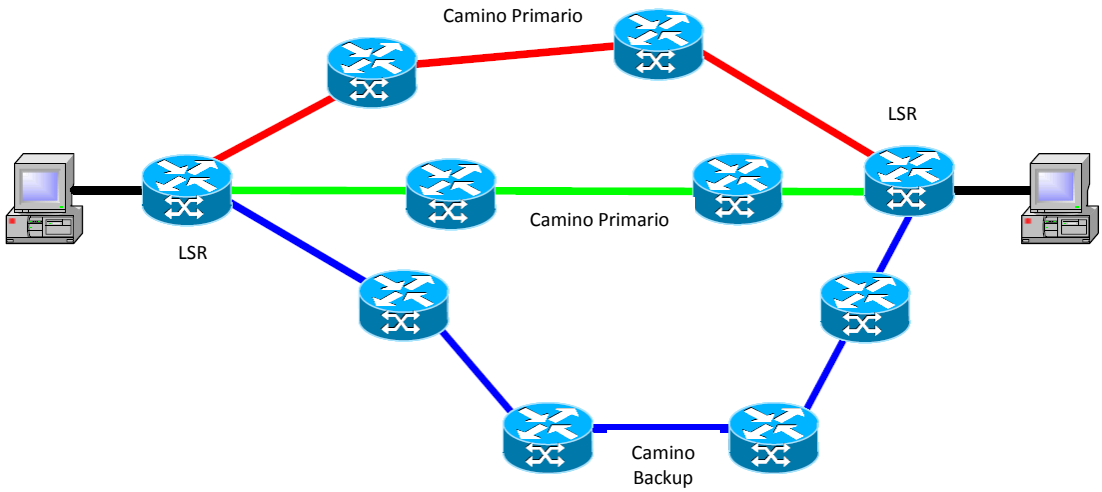

Figura 15 Protección en redes IP/MPLS [21]

2.2.2 Supervivencia en redes de transporte

La supervivencia en redes de transporte aplica los mecanismos generales para la supervivencia en redes con determinadas particularidades [20] y [22]. En algunas redes de transporte como por ejemplo SONET/SDH el plano de datos proporciona mecanismos para la detección de fallos. En otras redes de transporte es el plano de control el que se encarga de esta tarea, y por lo tanto, GMPLS y LMP (*Link Management Protocol*, Protocolo de gestión de enlace) [23] en concreto proporcionan esa función.

Las redes de transporte se encuentran muy cercanas al nivel físico y por tanto los mecanismos de supervivencia deben adaptarse a las implicaciones que la naturaleza de los fallos en este nivel puede tener. Por ello se definen los siguientes mecanismos de protección y restauración.

Protección dedicada unidireccional 1+1

Este esquema implica que cada conexión proporcionada por la capa de transporte a la capa de red se compone de dos conexiones de tal modo que el tráfico que el que atraviesa el enlace se encuentra completamente replicado en ambos. Cuando un fallo es detectado automáticamente se conmuta la recepción de información al enlace de protección manteniendo la conectividad prácticamente inalterable.

El encargado de actuar cuando se detecta el fallo es el nodo iniciador de la conexión y en el momento en que se detecta que el fallo ha sido reparado, se vuelve a la situación inicial.

Protección dedicada bidireccional 1+1

La protección dedicada bidireccional se diferencia de la unidireccional en que ambos extremos de la conexión protegida están encargados de iniciar los procesos de cambio de tráfico. Para sincronizar la protección en ambos nodos, se han de seguir las siguientes reglas:

- Cuando uno de los nodos detecta el fallo, conmuta la recepción de información al camino de protección y envía un mensaje de *Switchover Request* (solicitud de conmutación) al nodo del otro extremo. Sólo se envía este mensaje si el nodo no ha recibido previamente el mismo mensaje del otro extremo. En dicho caso se envía una respuesta *Switchover Response* (respuesta de conmutación).
- Cuando un nodo recibe un Switchover Request conmuta el tráfico y envía el Switchover Response.

En el caso de detección de una reparación, el procedimiento se rige por las siguientes reglas:

- Cuando un nodo que previamente ha detectado un fallo detecta la reparación del mismo, conmuta la recepción del tráfico y envía un mensaje *Switchback Request* (solicitud de vuelta atrás en la conmutación) al nodo en el extremo opuesto. De nuevo, este mensaje sólo se envía si no se ha recibido previamente este mensaje enviando un *Switchback Response* (respuesta de vuelta atrás en la conmutación).
- En el caso de que un nodo reciba un mensaje Switchback Request procede a cambiar la conmutación al camino inicial y responde con un mensaje Switchback Response.

Este procedimiento necesita prestar atención especial a los casos de cambios de estado del enlace continuos conocidos como *flapping* en los que se ha de incluir un timer conocido como WRT (*Wait to Restore Timer*, Temporizador de espera para restaurar) que inhibirá la vuelta al camino inicial durante un periodo de tiempo posterior al fallo de tal modo que se previene el cambio continuo de caminos debido al estado del enlace.

Protección 1:1 con tráfico adicional

Bajo este esquema, el tráfico en lugar de enviarse por ambos enlaces (el nominal y el de protección) se envía por uno de ellos y en caso de fallo se traslada todo el tráfico al enlace de protección. Esto implica que potencialmente, el enlace de protección puede ser utilizado para transmitir otro tipo de tráfico de la red mientras no es necesario para labores de supervivencia del enlace principal.

En estos esquemas se tiene que planificar la prioridad del tráfico adicional (el que se encuentra en el enlace de protección) y el tráfico nominal del enlace principal. El plano de control es quien debe proporcionar los mecanismos (GMPLS lo hace a través de las prioridades de tráfico) para decidir qué tráfico ha de ser el que se curse en caso de fallo. A priori lo lógico podrá ser utilizar el enlace de protección para transmitir tráfico sin prioridad y no garantizado de tal modo que cuando haya que recuperar el fallo en el tráfico protegido se expulse a este tráfico adicional del enlace de protección.

Protección compartida M:N

En el caso de protección compartida con M > N se tiene lo mismo que se ha comentado para el caso general de protección compartida M:N añadiendo mecanismos que en GMPLS permiten mediante el uso de prioridades seleccionar los caminos que tendrán preferencia a la hora de ser recuperados frente a fallos.

Protección Mejorada

Se considera protección mejorada cualquier mecanismo que sea capaz de proporcionar mayor protección que la basada en 1+1. Un ejemplo de este tipo de protecciones es la protección de cuatro fibras en anillo SONET BLSR (*SONET Bidirectional Line-Switched Ring*, Anillo conmutado bidireccional). En la Figura 16 se presenta este esquema de protección que desde el punto de vista de la protección se estudiaría del siguiente modo. Supongamos un servicio entre A y D, antes del fallo el enlace de trabajo sería A-B-C-D con protección D-C-B-A.

Tras el fallo doble de la figura se tendría el enlace de trabajo como A-B-AF-E-D-C-D y el de protección D-C-F-A-B-A permitiendo de este modo tener una protección contra fallo triple lo cual es superior a la protección 1+1.

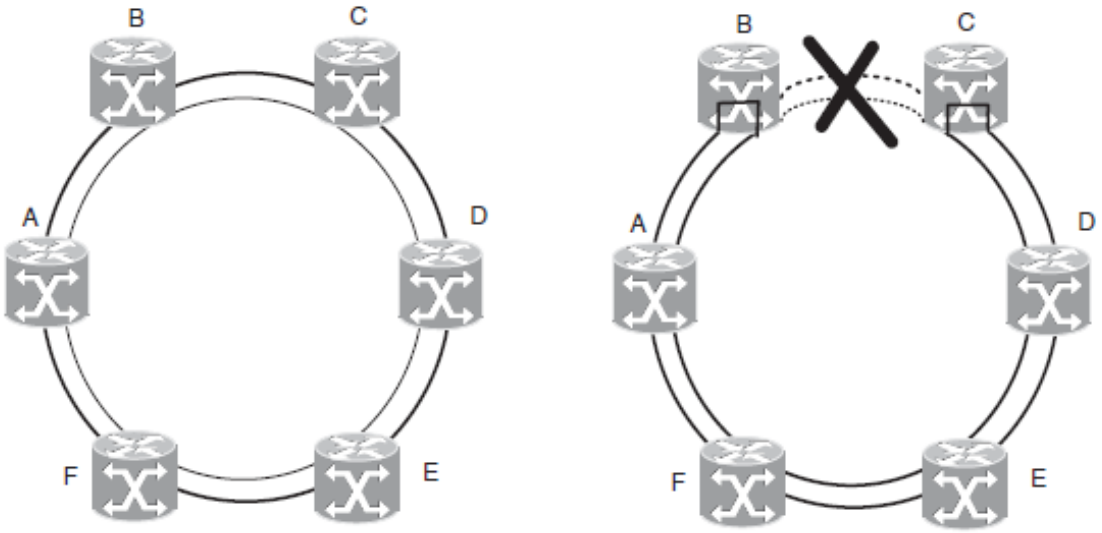

Figura 16 Protección mejorada SONET BLSR [15]

Restauración

Desde el punto de vista del estudio de las redes de transporte, se pueden aplicar los mismos esquemas para protección como para restauración con la diferencia que para la protección los recursos se encuentran reservados completamente y para la restauración esto no es así. En las redes DWDM con GMPLS el tiempo de restauración es superior a la protección debido a la necesidad de sintonizar tanto los láseres como los conmutadores ópticos a lo largo del camino así como la progresión del plano de control a lo largo del camino a establecer.

2.2.3 Supervivencia de red en un operador medio

Actualmente muchos operadores presentan una protección 1+1 en el núcleo de red ([1], [24]) a nivel IP/MPLS con una red de transporte que soporta esa protección. Como muestra la Figura 17 esta protección se da desde la agregación (routers de acceso) hasta el núcleo (interconexión) de una forma separada para las regiones de la red.

Para ilustrar de un mejor modo la problemática de la supervivencia de red medio, se va a presentar la respuesta de la red frente a fallos tanto en la capa IP/MPLS como en la red de transporte. Es importante hacer notar que los mecanismos de supervivencia actualmente en los operadores actúan de forma automática y

descoordinada entre capas por lo que en función de si se tiene protección o restauración y debido a los tiempos de convergencia de los protocolos de plano de control se pueden dar diferentes situaciones.

En primer lugar se presenta el escenario genérico de red de un operador medio en la Figura 18. Como se puede observar se tiene un escenario de protección completa 1+1 con routers espejo para que se mantengan los servicios en caso de fallo simple.

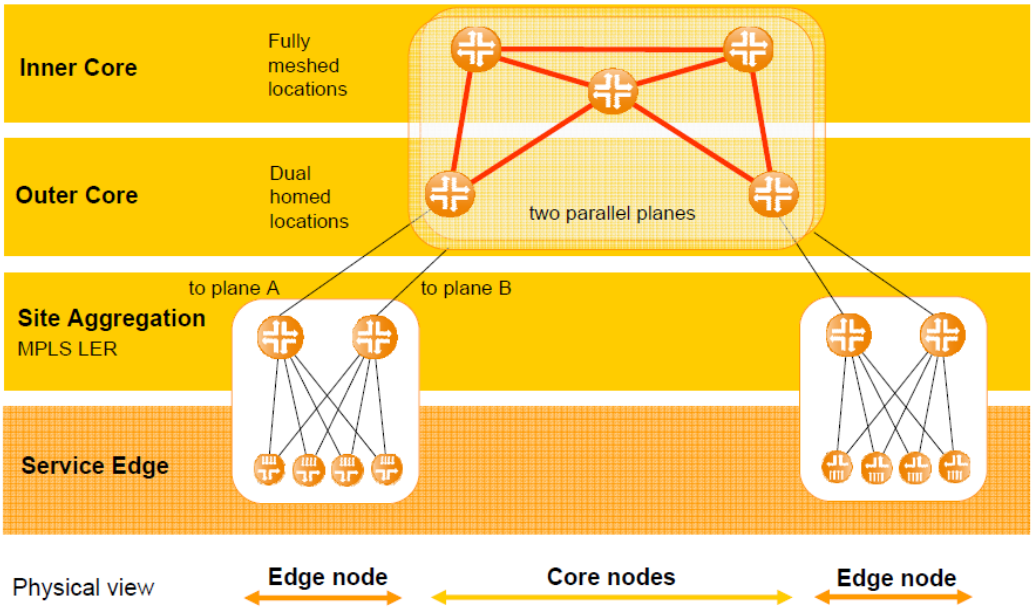

Figura 17 Ejemplo de núcleo de red de operador medio [24]

La Figura 19 representa los servicios establecidos sobre la capa IP/MPLS para tráfico de interconexión e interregional que agrupa la gran mayoría del tráfico del operador. Sobre estos flujos se va a presentar los mecanismos de supervivencia actuales determinando el impacto de un modo cualitativo sobre los servicios.

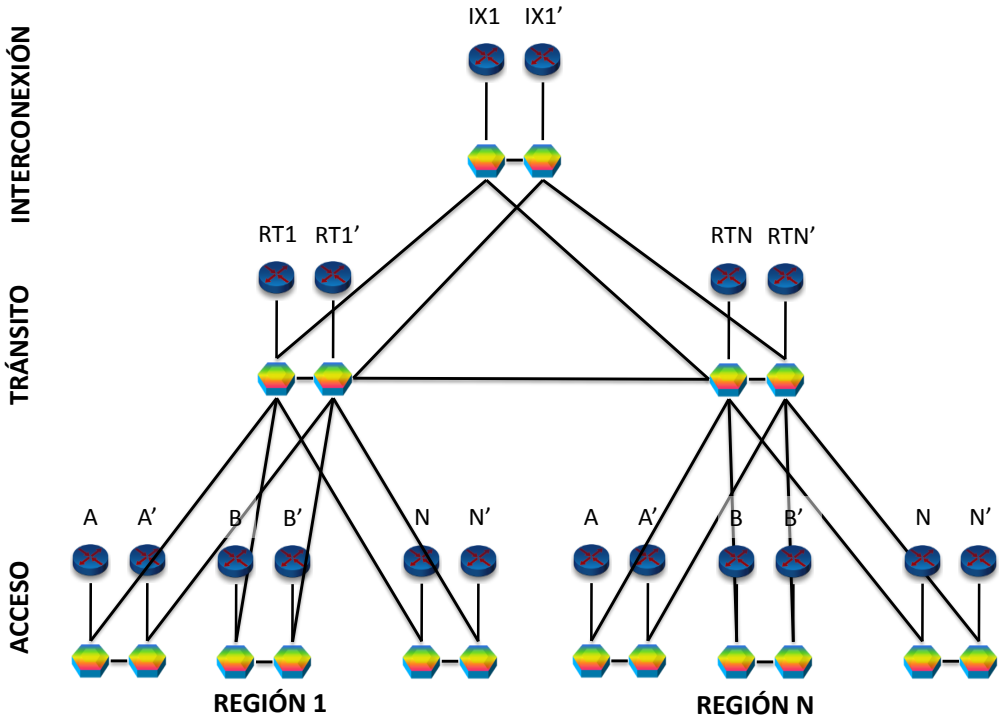

Figura 18 Conectividad física en red multi-regional

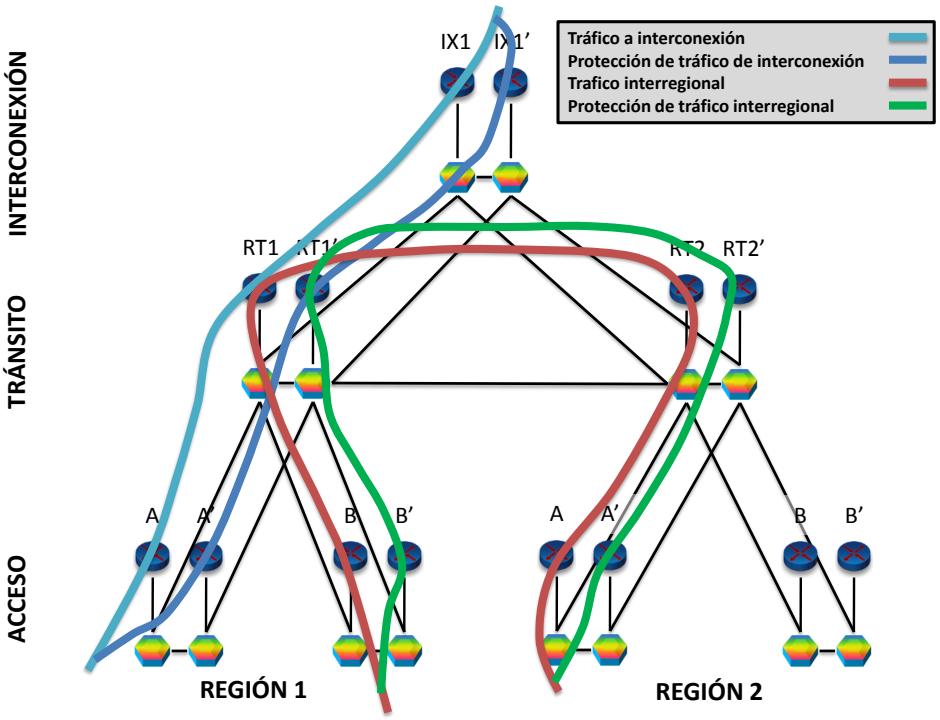

Figura 19 Flujos de tráfico en red jerárquica

Fallos IP/MPLS

Un fallo en un router IP/MPLS, desde el punto de vista de la red de transporte es totalmente transparente de tal modo que las conexiones se mantienen invariables y el tráfico se mueve en la capa IP/MPLS de los routers del camino de trabajo al camino de protección. En la Figura 20 se ilustra las consecuencias de un fallo simple en un router de tránsito en red jerárquica.

Los fallos en las tarjetas IP/MPLS tendrían unas consecuencias semejantes para el tráfico afectado, es decir, mientras que en un fallo total de nodo, el tráfico afectado es el flujo completo, si el fallo se produce únicamente en una tarjeta, la cantidad de tráfico a trasladar será menor y por lo tanto la exposición frente a un fallo de tarjeta tiene menores consecuencias desde el punto de vista de la cantidad de usuarios afectados.

En caso de que se tuviera un fallo doble, los mecanismos IP/MPLS de protección 1+1 no sería capaces de restaurar el tráfico provocando la pérdida de información total. En el caso de las redes jerárquicas como la estudiada no existen conexiones adicionales a otros routers de tránsito, acceso o directas a interconexión por lo que los mecanismos de restauración IP/MPLS en el núcleo no podrían dar solución al fallo doble [Figura 21].

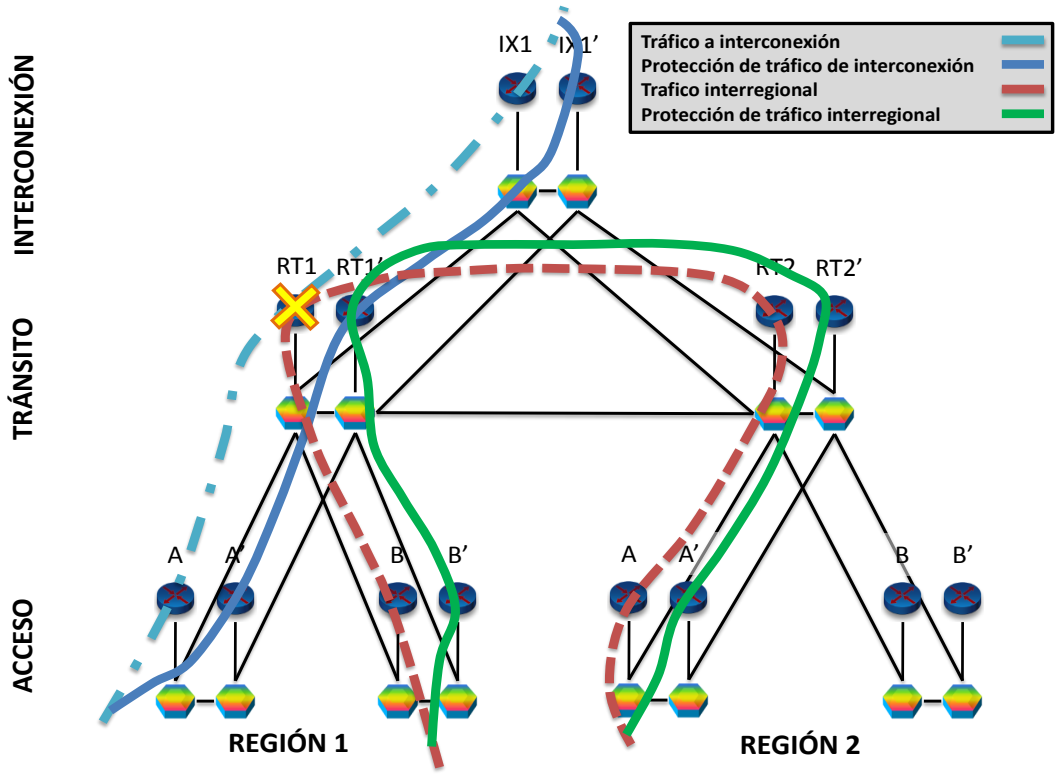

Figura 20 Fallo simple en red jerárquica

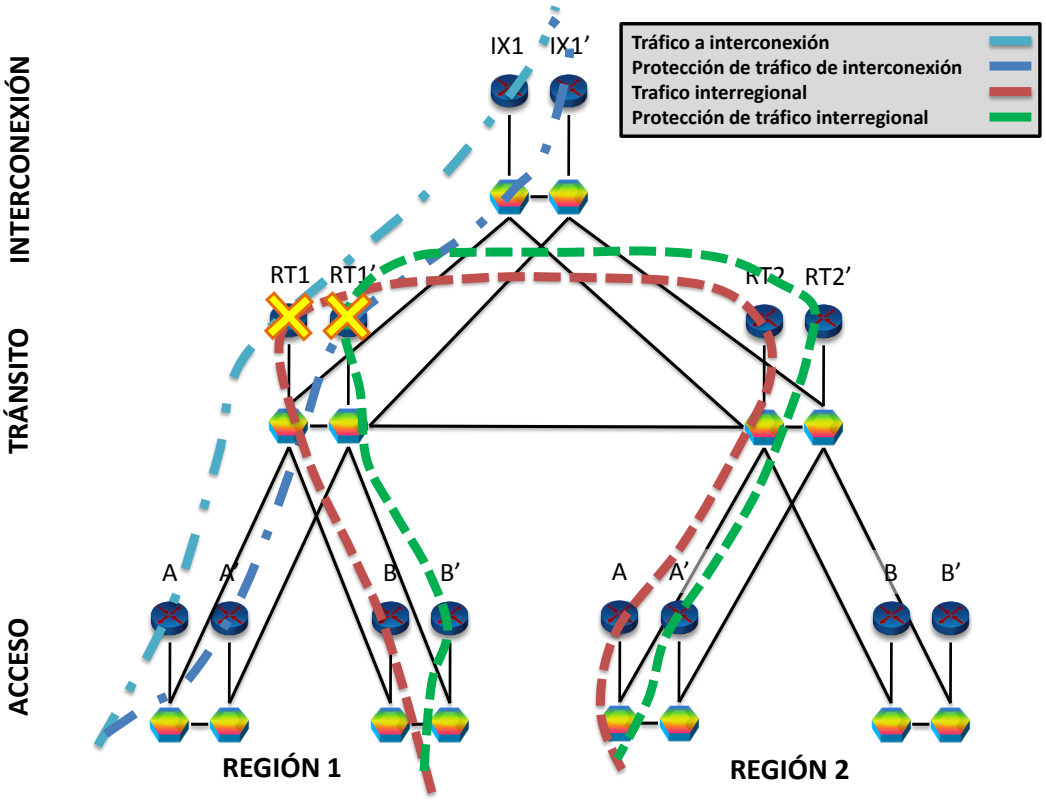

Figura 21 Fallo doble en red jerárquica

Fallos en capa de transporte

Al contrario que sucede en los fallos en la capa IP/MPLS, los problemas en la capa de transporte pueden tener incidencia directa sobre el encaminamiento realizado por la capa IP/MPLS. Suponiendo un esquema de protección en la capa de transporte, si los sistemas de detección de fallo (generalmente protocolos de OAM (*Operation, Administration and Management*, Operación, administración y mantenimiento) en permiten una detección de fallos más lenta que la actuación del fast reroute en la capa IP/MPLS por debajo de 50 milisegundos de conmutación. Esto supone que mientras el procedimiento de cambio de camino de trabajo a camino de protección se está realizando (intercambios de mensajes expuestos en la sección anterior) en la capa de transporte, la capa IP/MPLS ya ha conmutado el tráfico reduciendo enormemente la pérdida de paquetes.

El uso de protección en la capa de transporte en este caso serviría para que el operador mantuviera una protección 1+1 en la capa IP/MPLS pese a haber sufrido un evento de fallo. El inconveniente de este esquema es el coste puesto que implica una doble protección, es decir, se tienen duplicados los routers y tarjetas IP/MPLS así como los nodos ópticos y los transpondedores. Además, hay fallos en la capa de transporte que son críticos, como por ejemplo los transpondedores de conexión a las tarjetas IP/MPLS que, de por sí no pueden protegerse sin añadir protección adicional en la capa IP/MPLS.

La Figura 22 y la Figura 23 muestran la diferencia entre un fallo recuperable por la capa de transporte y uno que no lo es. En el caso del irrecuperable, sólo mediante mecanismos de supervivencia IP/MPLS o completa duplicidad de recursos en ambas capas (tener dos tarjetas IP/MPLS y dos transpondedores de transporte para el mismo tráfico en los nodos) sería posible responder ante el fallo.

Como se desprende de las figuras, una protección 1+1 en ambas capas implica tener los recursos de transporte cuadruplicados y los recursos de IP/MPLS duplicados y no garantiza una protección 1+1+1+1 ya que tiene recursos críticos que en la práctica reducen la supervivencia a esquemas de protección 1+1 mejorados.

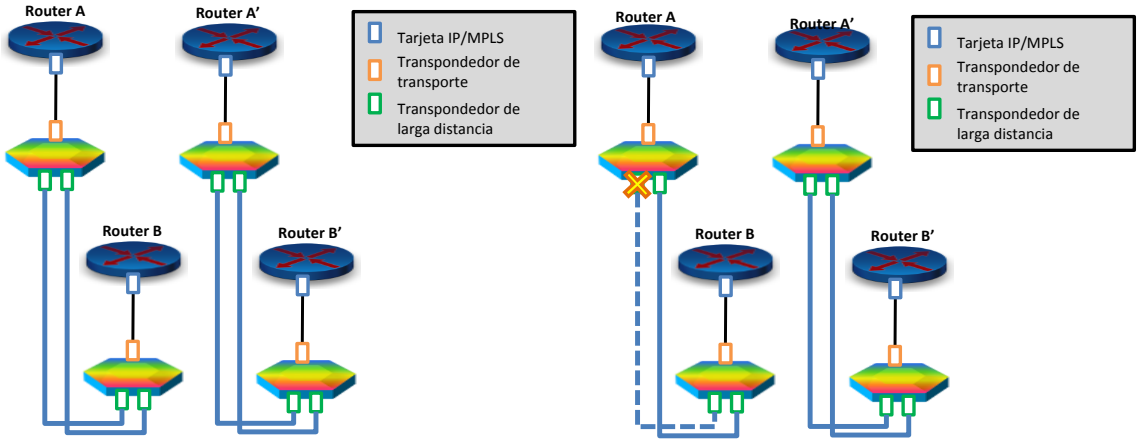

Figura 22 Fallo en transporte recuperable

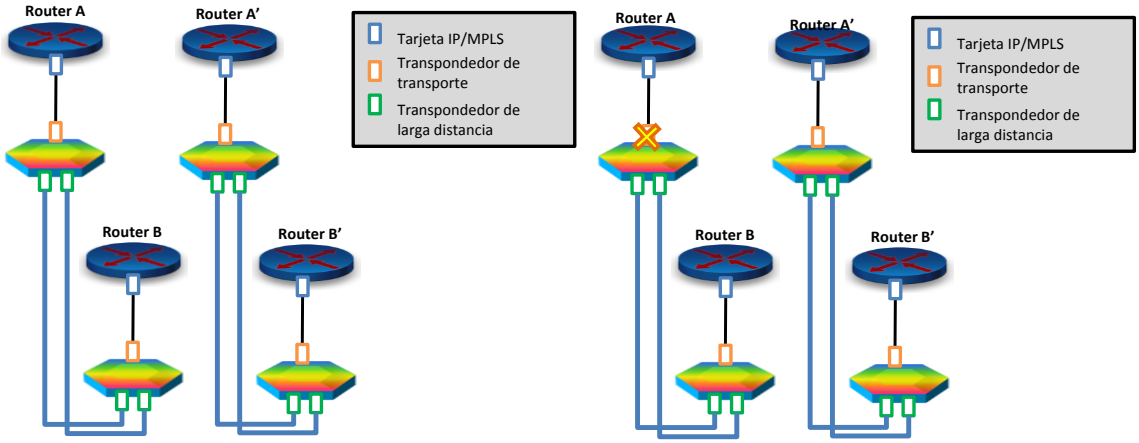

Figura 23 Fallo en transporte irrecuperable

2.3 Evolución de la red hacia un modelo multicapa

En la sección anterior se ha presentado el funcionamiento de los mecanismos de supervivencia en redes con capas separadas operadas de forma totalmente independiente. Debido a las limitaciones que lleva consigo esta separación de capas, tanto los organismos de estandarización como expertos del sector trabajan en definir un marco de control multicapa que permita una operación conjunta de la red. Para ello se define el plano de control multicapa.

2.3.1 Plano de control multicapa

El plano de control para redes formadas por múltiples capas presenta importantes retos con respecto a los planos de control con una única capa. Hay dos aproximaciones principales, un modelo “overlay”, en el cual la relación de confianza entre ambas capas es limitada, y por tanto, el intercambio de información en el plano de control entre equipos de ambas redes es reducido. Así, se emplean los protocolos con las opciones totalmente estándar, habitualmente en una versión limitada, así como poca información en ellos.

La otra aproximación asume una relación de confianza mayor, tanto entre ambas capas, como entre los fabricantes de los nodos de ambas capas, de tal forma que se puede emplear los protocolos con todas las extensiones necesarias y toda la información que se desee para así lograr un mejor comportamiento y aprovechamiento de los recursos. Si bien el modelo integrado es la solución ideal "final", se propone ir aumentando en el estándar la riqueza de la comunicación entre capas, mejorando así la interoperabilidad.

Al juntar capas con modelos de control relativamente distintos surgen varios retos. Un ejemplo claro es el paso de un plano de control en banda (IP/MPLS) a uno fuera de banda (GMPLS). En una red IP/MPLS las interfaces de datos son utilizadas para emitir y recibir los mensajes de plano de control. Esto supone que en el momento en que dos interfaces de dos equipos se interconectan (y son compatibles) el plano de control anuncia esta conexión como por ejemplo en OSPF. Simplemente el hecho de conectar dos equipos a través dos interfaces hace que ambos conozcan su existencia y los destinos que se pueden alcanzar a través de dichas interfaces. Esto supone una facilidad y comodidad desde el punto de vista de uso y configuración pero no es viable en entornos donde existe un plano de control fuera de banda. En estos casos, hay que incluir mecanismos adicionales que describan y mantengan dichos enlaces.

Por ejemplo, una red de transporte necesita configuración adicional como las longitudes de onda que se va a utilizar para transmitir información entre dos interfaces. En este caso, el proceso de anunciamiento y configuración cambia sustancialmente. Para que esto pueda realizarse con el plano de control, es necesaria una señalización fuera de banda, lo que quiere decir que se necesita una red alternativa establecida previamente para intercambiar los mensajes de plano de control ya que las interfaces del plano de datos no podrán realizar este papel por lo ya comentado anteriormente. Esta señalización fuera de banda puede consistir en una red Ethernet que interconecte los equipos, una longitud de onda configurada por gestión para transmitir el plano de control… en definitiva, es necesario el establecimiento de una red que permita la información de adyacencias, las solicitudes de reserva de recursos y demás operaciones realizables mediante plano de control.

En las redes multicapa, siguiendo el modelo "overlay" actual, la relación entre capas de red y de transporte no puede ser establecida automáticamente al conectar las interfaces de equipos de ambas capas por las particularidades de cada capa. Esto supone que el plano de control para poder operar en entornos multicapa debe resolver las siguientes tareas:

- Relacionar e informar de las conexiones entre las interfaces de datos. Estas conexiones pueden ser dentro de una misma capa o entre capas.
- Proporcionar una interfaz para solicitar caminos entre ambas capas.
- Proporcionar un método que permita señalizar e informar de las reservas de recursos y cambios en las mismas.

Para facilitar la realización de estas tareas se presentan los siguientes elementos del estado del arte.

2.3.1.1 TE-Links Multicapa

El plano de control en redes multicapa necesita relacionar las capas adyacentes para poder operar, direccionar y reservar recursos. Se utilizan los TE-Links para esta función y éstos se definen de tal modo que permiten crear adyacencias entre equipos de diferentes capas.

Los TE-Links permiten direccionar las interfaces de conexión entre capas, por lo que en el proceso de provisión de caminos es necesario incluirlos como parte del

camino. Debido a que no se anuncia ni se inunda la información de los TE-Links entre capas, actualmente es necesario el conocimiento de este direccionamiento por el operador de red para poder establecer caminos multicapa.

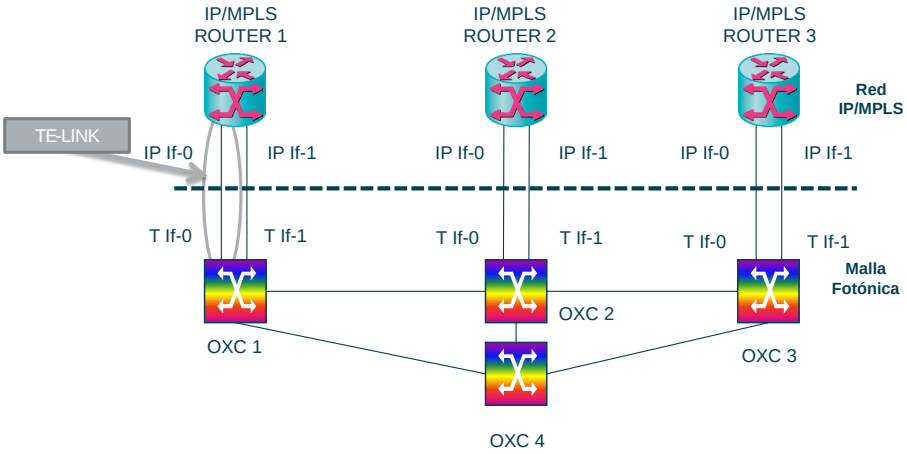

Figura 24 TE-Links Multicapa

Para el funcionamiento de los TE-Links entre capas han de ser configurados los siguientes parámetros:

- Equipos IP/MPLS
  - La interfaz asociada al TE-Link en el equipo IP/MPLS
  - El identificador local de la interfaz conectada en el equipo de transporte. Este dato solo se puede conocer manualmente consultando en el equipo de transporte.
  - Un canal de control para intercambiar la información con el equipo de transporte.
  - El identificador (puede ser una IP) con el que se podrá direccionar el TE-Link en el equipo IP/MPLS y el identificador del extremo de transporte.
- Equipos de Transporte
  - La interfaz asociada al TE-Link en la capa de Transporte.
  - El identificador local de la interfaz conectada en el equipo IP/MPLS. Este dato solo se puede conocer manualmente consultando en el equipo IP/MPLS.
  - Un canal de control para intercambiar la información con el equipo IP/MPLS.
  - Un identificador (puede ser una IP) con el que se podrá direccionar el TE-Link en el equipo de transporte y el identificador del extremo IP/MPLS.

Este es el modo en que se puede asociar los equipos de dos capas diferentes. Por el canal de control, el protocolo LMP se encargará de informar de las tecnologías de conmutación permitidas por los equipos. Actualmente no hay diseñado mecanismo alguno para conocer mediante plano de control los identificadores lógicos que tiene cada interfaz física dentro de los equipos por lo que no es posible configurar un TE-Link multicapa automáticamente basado en la información de plano de control. Se necesita una configuración manual y debe seguir una secuencia combinada entre los equipos de las dos capas.

Una vez se ha expuesto el método de entrelazamiento de capas desarrollado actualmente, se plantea el siguiente paso, la reserva de recursos. Lo anteriormente expuesto simplemente presenta el método seguido para asociar equipos de dos capas

diferentes, pero en definitiva, el objetivo es establecer enlaces y adyacencias en la capa superior atravesando las tecnologías y capas que sean necesarias permitiendo reservar unos recursos determinados y en su caso, con criterios de ancho de banda y calidad de servicio.

Utilizando la como referencia, se pretende establecer un enlace de un determinado ancho de banda (BW) desde el ROUTER 1 hasta el ROUTER 3. Como se observa, para conseguir este objetivo es necesario atravesar equipamiento en las dos capas y por lo tanto, el equipamiento de la capa superior tendrá que solicitar a la capa inferior la reserva de este camino.

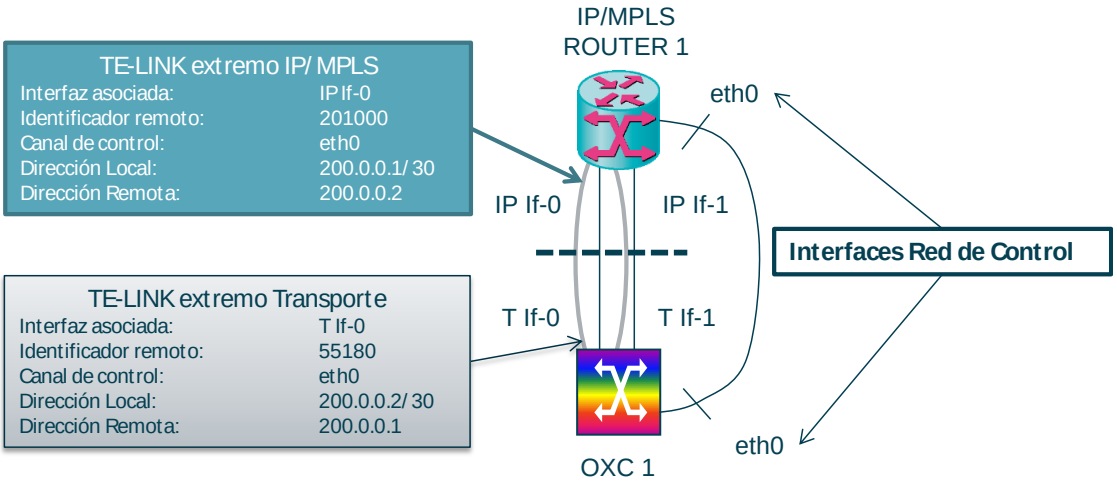

Figura 25 Configuración de TE-Links Multicapa

2.3.1.2 Interfaz de provisión multicapa

El comportamiento en este caso de la capa IP/MPLS es de cliente de la capa de Transporte que actúa como servidor de recursos. Para estandarizar estas peticiones el IETF ha definido el UNI (*User to Network Interface*, Interfaz de usuario a red) que establece los protocolos que se han de utilizar y el modo de hacerlo para que la capa servidora pueda responder adecuadamente a las solicitudes de la capa cliente.

El UNI estándar define RSVP-TE (y sus extensiones para GMPLS) como el protocolo a utilizar para la reserva de recursos y OSPF-TE para anunciar las adyacencias creadas tras el establecimiento de la reserva. Mediante los mensajes RSVP PATH y RSVP RESV se procede a la solicitud y confirmación respectivamente del enlace deseado. La solicitud ha de incluir como parámetros al menos:

- La conmutación deseada en el LSP. Es un parámetro asociado a la tecnología del equipamiento por lo que por ejemplo, en una red DWDM este parámetro es LSC pero a nivel IP/MPLS este parámetro es PSC.
- El ancho de banda requerido. Es un parámetro que va unido a la tecnología de conmutación por lo que no tendría sentido solicitar un ancho de banda de 50Gbps en un sistema DWDM que sólo tiene longitudes de onda de 10, 40 o 100 Gbps.
- El camino a reservar ERO que define explícitamente la ruta que ha de ser reservada o al menos unos puntos que ha de recorrer el camino. En el actual modelo de plano de control, al tener las capas separadas, esta información no se intercambia por lo que el router que haga la solicitud no podrá elegir por sí mismo el camino que la capa inferior debe proporcionarle. El ERO en el caso multicapa debe incluir los identificadores

de los TE-Link del router que realiza la solicitud, el del equipo conectado de la capa inferior y los de los equipos de destino (tanto el de transporte como la capa IP/MPLS).

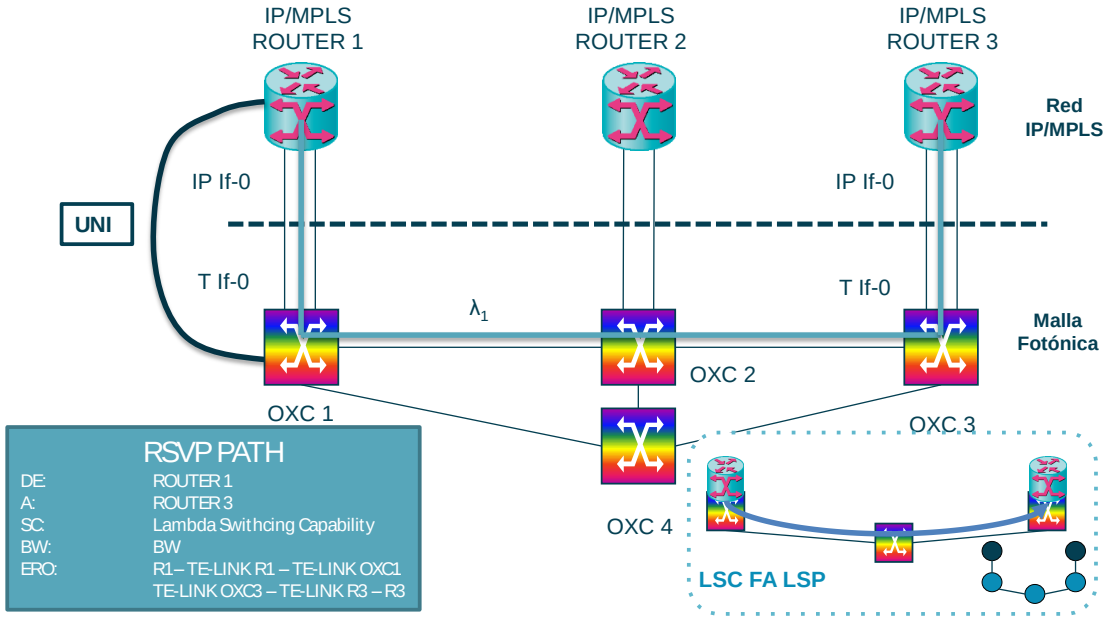

Figura 26 Ejemplo de solicitud de camino multicapa a través de UNI

La Figura 26 presenta la solicitud con el plano de control de una reserva de recursos entre la capa IP/MPLS y la de transporte utilizando el interfaz UNI. Una vez se establece este LSP, sobre el mismo, se utiliza la técnica de LSPs jerárquicos para definir reservas de recursos con mayor granularidad e independientes de la capa inferior, permitiendo de este modo abstraer las particularidades de la capa inferior en el modelo de control de la capa superior.

El procedimiento de establecimiento de LSPs jerárquicos continuaría la situación de la Figura 27 utilizando el LSP establecido previamente para reservar una determinada capacidad para la conmutación de paquetes (PSC) sobre el LSP de conmutación de lambdas. Esto permite crear diferentes adyacencias sobre ese enlace con diferentes características como por ejemplo diferente ancho de banda, diferente prioridad, diferentes características de protección y más factores importantes a la hora de operar una red.

La Figura 28 presenta la jerarquía de LSPs expuesta y cómo desde el punto de vista de los LSPs 1 y 2 no existe la capa de transporte y el proceso de reserva se convierte en hacer uso de una adyacencia y reservar un ancho de banda sobre la misma con determinadas prioridades basadas en la ingeniería de tráfico.

En definitiva, en esta sección se ha presentado cómo actualmente se gestionan las redes multicapa, el conocimiento que ambas capas tienen unas de las otras y como se interrelacionan. Las limitaciones que vienen impuestas por este modelo y los motivos de dichas limitaciones. En busca de solventar estos problemas, se propone en secciones siguientes los pasos necesarios para conseguir una operación completa y óptima de las redes multicapa.

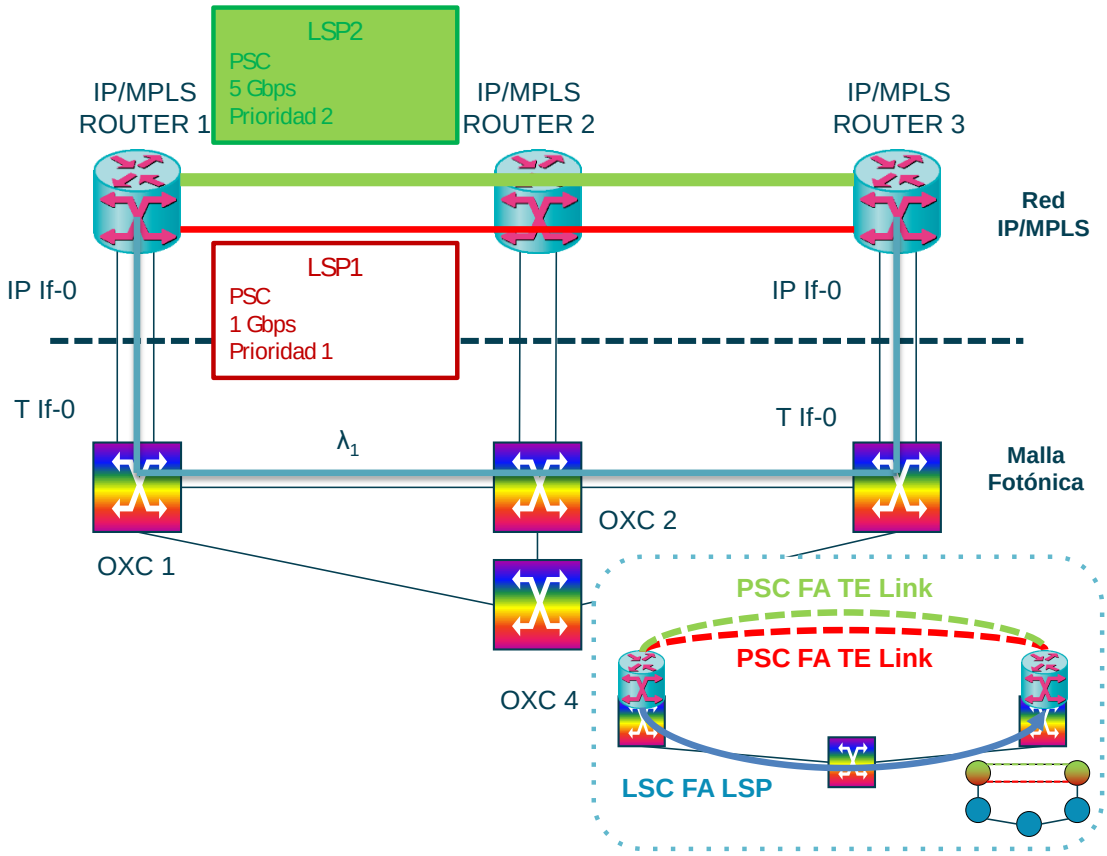

Figura 27 Establecimiento de LSPs jerárquicos

En redes de una sola capa, las solicitudes de recursos pueden requerir un camino explícito en la petición por lo que el protocolo de señalización proporciona un objeto específico para estas funciones (ERO). Como en secciones anteriores se ha explicado, el ERO para el caso multicapa no puede completarse mediante la información obtenida por el plano de control tal y como está definido actualmente en los estándares.

Para solventar este problema está en proceso de estandarización en estado de Draft [25], el objeto ERO para el caso multicapa. Las propuestas actuales consisten en la separación por capas de la información de los equipos (End Points) que ha de atravesar el camino a reservar. Se define el sub-objeto Server Layer Info a incluir en el ERO para permitirla interrelación entre capas. El objeto Server Layer Info indica que el camino a recorrer desde que se encuentra en el ERO pertenece a una capa servidora, típicamente la capa de transporte jugaría este papel. Cuando el objeto se encuentra por segunda vez, indica que el recorrido por la capa servidora ha terminado.

De este modo, la composición de un ERO multicapa se reduce a obtener los caminos de las capas por separado e incluirlos con los separadores de capa en el ERO a utilizar. De este modo el operador puede elegir el camino para una solicitud dada.

2.4 Supervivencia en Redes Multicapa

Como previamente se ha expuesto, la red actual, desde el punto de vista de la supervivencia se comporta como dos redes independientes completamente separadas. Por un lado la capa IP/MPLS tiene sus mecanismos de protección que pretenden dar solución a los fallos desde la perspectiva IP/MPLS (LSPs pre-

configurados, OSPF…). Por otra parte tenemos la capa de transporte que también mediante mecanismos de protección propios responde a los eventos de fallo desde su perspectiva teniendo dos capas descoordinadas completamente aunque en definitiva son capaces de reponerse ante gran cantidad de fallos.

Los inconvenientes de éste modelo de supervivencia de red nacen de diferentes aspectos los cuales se enumeran y explican a continuación:

1. La red no es 100% predecible. La descoordinación existente en éste modelo provoca una duplicidad de tareas, es decir, los fallos se detectan por diferentes entidades de cada capa y la recuperación frente a ellos también por lo que no se puede saber a priori como va a ser el comportamiento de la red. Esto no es nada aconsejable desde el punto de vista del administrador/gestor de la red puesto que puede incurrir en comportamientos no detectados que impliquen resultados no deseados y que afecten negativamente al rendimiento de la red.
2. Exceso de recursos necesarios: Una red con el modelo de supervivencia actual tiene mucho más difícil la optimización de los recursos de red, de tal modo que cada capa se dimensiona según sus propios intereses y provoca un exceso de recursos reservados.

En caso de existir una coordinación entre las capas, no sería necesario tener protección en ambas capas, es decir, se podría elegir el punto en el que hacerlo ahorrando en equipos/enlaces.

Teniendo en cuenta que el objetivo de una red de comunicaciones es transportar la información entre dos puntos de la red garantizando determinados parámetros de calidad de servicio, la cuestión primordial desde el punto de vista de la supervivencia de red es proporcionar los mecanismos que, de la manera más predecible posible nos permitan asegurar determinados niveles de disponibilidad. En redes multicapa se ha de coordinar las acciones del plano de control de modo que, como hemos expuesto en secciones anteriores, no se den duplicidades a la hora de recuperar fallos en la red. Además, el conocimiento de la topología de red multicapa permitirá la creación de nuevas adyacencias que con planos de control separados serían totalmente irrealizables.

En la siguiente figura se muestra un ejemplo de red jerárquica en la que se ha omitido los routers de protección de las regiones 1 y 2 para hacer más comprensible la explicación. Desde el punto de vista IP/MPLS los routers de acceso sólo pueden alcanzar la interconexión a través de sus tránsitos ya que la red de transporte no tiene establecidas conexiones entre los accesos y otros routers de tránsito para evitar el anuncio de estas adyacencias. Esto se hace con el objetivo de evitar una explosión de adyacencias entre todos los nodos de la red y controlar y predecir de un mejor modo el comportamiento de la red. El problema de este modo de operar la red es que cuando se produce un fallo doble en una región las interfaces de los routers de acceso quedan inútiles al tener predefinidos los destinos (los tránsitos de su región) ya que la capa de transporte no tiene modo de decidir por sí misma que para alcanzar interconexión sería viable el uso de otros tránsitos u otros accesos de otras regiones. Si bien son alcanzables creando una conexión de transporte, sólo se puede solicitar la creación de la misma si éstas posibles conexiones se anuncian a la capa IP/MPLS como viables y se proporciona un mecanismo de establecimiento. El plano de control multicapa permitiría el establecimiento de este enlace.

La Figura 29 presenta la utilización de estos mecanismos multicapa para mantener la conectividad entre acceso e interconexión cuando un fallo crítico se diera en una

región creando una nueva adyacencia entre el acceso de la región 1 y el tránsito de la región 3 usado para protección, con capacidad suficiente para mantener el servicio.

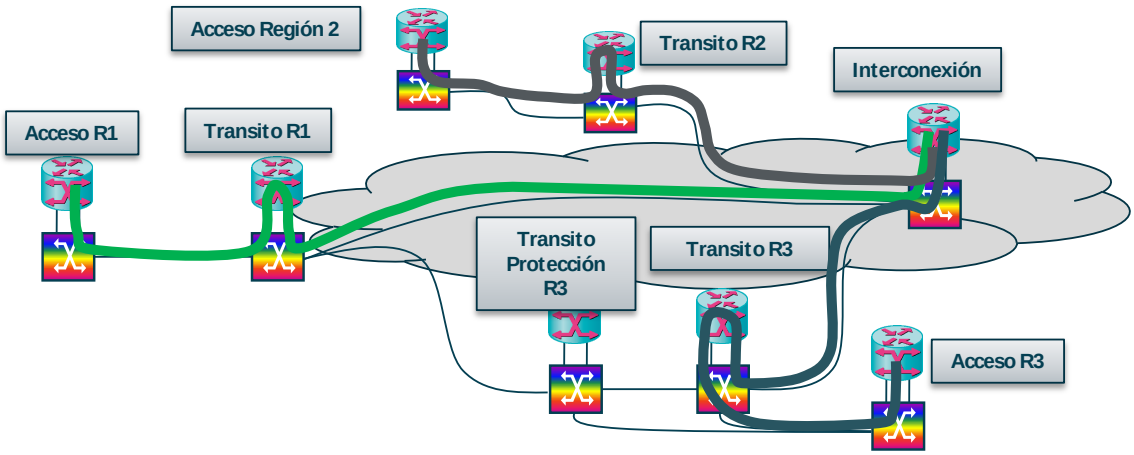

Figura 28 Restauración multicapa en red jerárquica

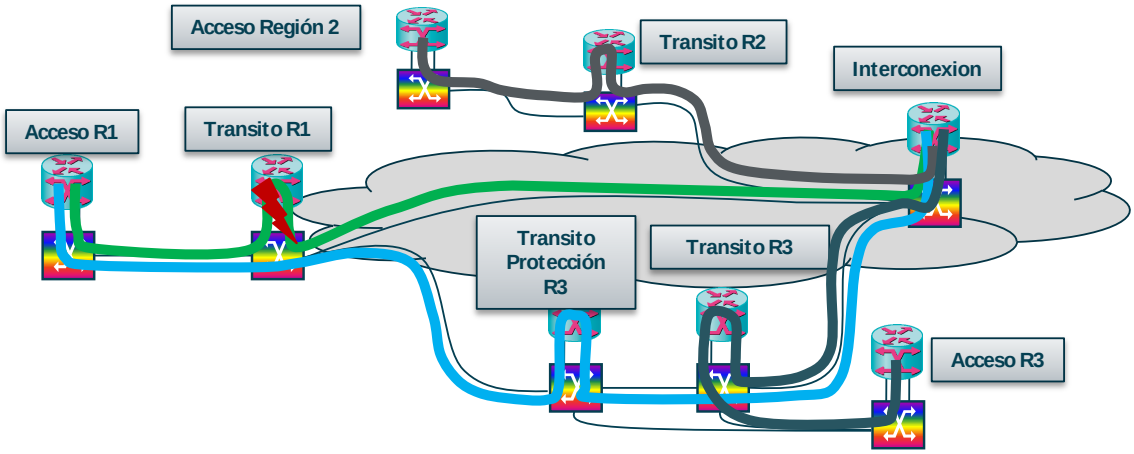

Figura 29 Restauración utilizando el tránsito de otra región

Una vez expuesto un ejemplo básico y asumiendo una conectividad total entre los equipos de transporte de a nivel de tránsito, se proponen diferentes procedimientos para la restauración multicapa para obtener diferentes prestaciones de supervivencia en la red ya sea un mayor tiempo de reparación para conseguir el mismo objetivo de disponibilidad o reducir el equipamiento necesario para garantizar la misma.

Restauración utilizando los routers de protección existentes

Este procedimiento es el más sencillo de incluir ya que no supone ninguna modificación sobre el equipamiento existente. En la Figura 30 se muestra el procedimiento, que consistiría en el caso de un fallo doble en vaciar el router de tránsito de protección de una región adyacente cargando el router nominal al 100% y permitiendo alojar el tráfico de la región con un fallo doble.

Al tratarse de un procedimiento de establecimiento de enlace nuevo tras el segundo fallo, el tiempo que se tardará en establecer el nuevo enlace depende de la velocidad de la capa de transporte para sintonizar el nuevo camino. Todo este tiempo, la región afectada por el fallo doble se encontrará sin servicio. La sucesión de eventos asociada a este caso es la siguiente:

1. Fallo en un router de tránsito en una región.
2. El mecanismo de protección mueve el tráfico hacia el router de backup de la región afectada.
3. En una región con capacidad suficiente se libera equipamiento de tránsito para permitir la restauración a través de los mismos y se establece un nuevo enlace entre el acceso de la región afectada y el tránsito libre.
4. Se produce el fallo doble.
5. El tráfico se transmite hacia la región utilizada para la restauración multicapa.

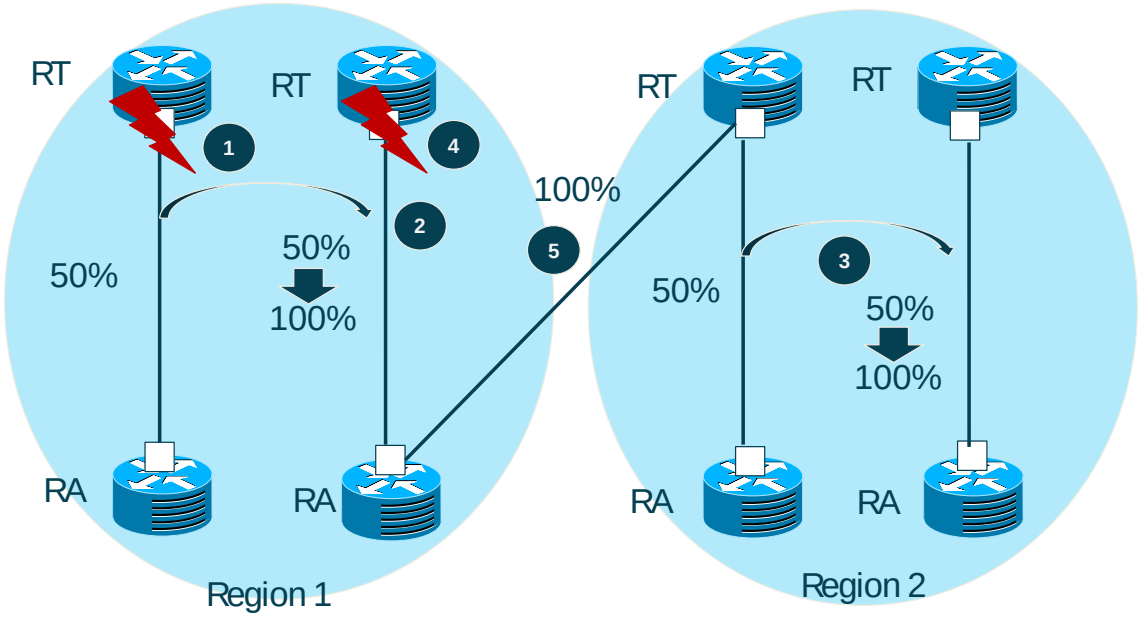

Figura 30 Restauración multicapa manteniendo los recursos

Restauración utilizando un router adicional

Con este procedimiento, el operador puede decidir crear una granja de routers de tránsito disponibles para recuperar los fallos dobles de las regiones. Esta granja tendría un coste adicional pero permitiría elevar la disponibilidad por encima de los esquemas de restauración multicapa anteriores. Además este esquema permite establecer el nuevo enlace cuando se produce el primer fallo y de este modo evitar tener pérdidas de tráfico mientras se crea.

En la Figura 30 se muestra la sucesión de eventos de este modelo de restauración multicapa:

1. Se produce un fallo en un router de tránsito en una región.
2. El mecanismo de protección vuelca el 100% del tráfico sobre el router de backup.
3. El mecanismo de restauración multicapa establece un nuevo enlace hacia un router auxiliar y se vuelve a dividir el tráfico entre este nuevo enlace y el que sigue activo de la región afectada.

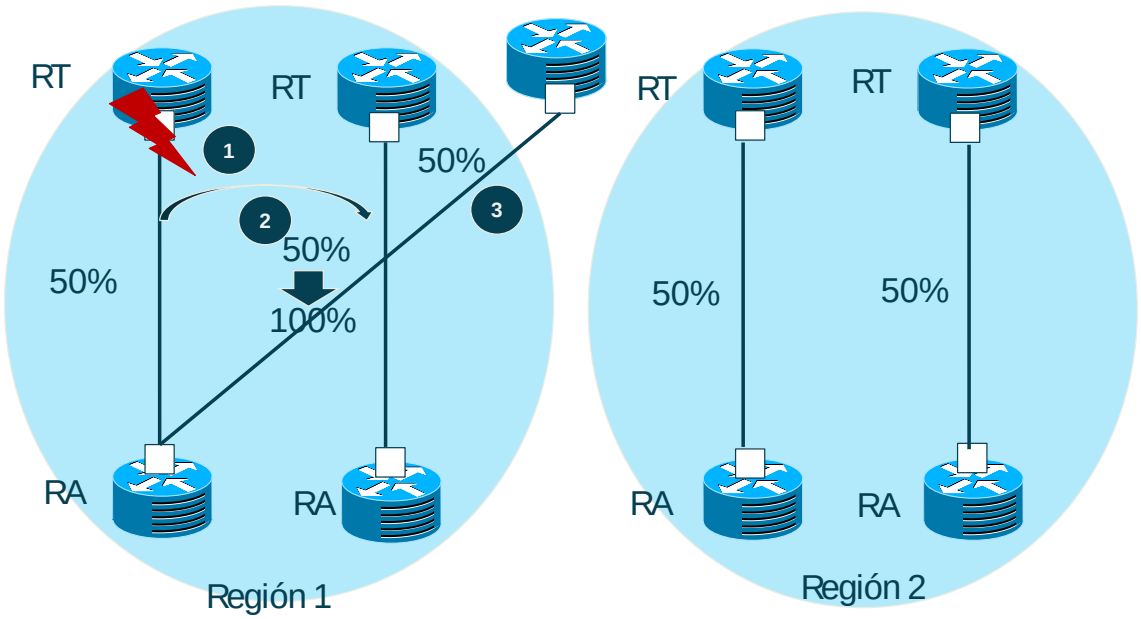

Figura 31 Restauración multicapa con granja de routers

Restauración eliminando routers de protección

En un entorno multi-región el operador podría decidir eliminar parte de los routers de protección con la esperanza de, al compartir los restantes, mantener la disponibilidad en niveles aceptables para cumplir con los SLAs. Este mecanismo es el menos garantista de todos ya que establecería los nuevos enlaces hacia el router de protección compartido en el momento del fallo simple sufriendo una pérdida de conectividad en ese momento. En teoría supondría un ahorro de costes por equipamiento si se deja de invertir en recursos de protección.

En la Figura 32 se presenta la sucesión de eventos para este procedimiento de restauración multicapa:

1. Se detecta un fallo en una región sin protección.
2. Se establece un nuevo enlace hacia un router compartido de protección para cursar el tráfico afectado.

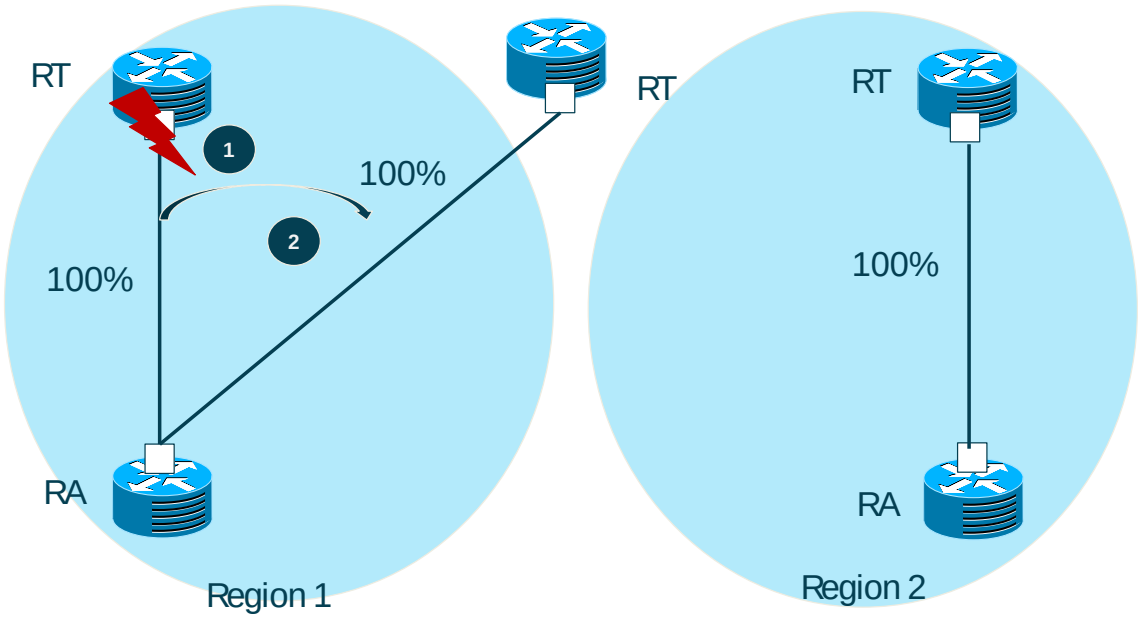

Figura 32 Restauración multicapa sin protección en las regiones

3 Análisis de supervivencia multicapa

Tras haber expuesto en la sección anterior los diferentes mecanismos de supervivencia en redes de telecomunicaciones, se plantea la necesidad de comparar los mecanismos de protección a nivel IP/MPLS puro con la restauración multicapa haciendo uso de las propiedades dinámicas de la capa de transporte para y resolver los fallos que ninguna de las dos capas pueden resolver por si mismas. El tipo de fallos que no puede resolver la capa IP/MPLS son los fallos dobles que afectan al equipamiento IP/MPLS y a sus conexiones con la capa de transporte. Se asume que la capa de transporte es capaz de restaurar fallos por corte de fibra y equipamiento óptico por si misma. Tal y como se ha presentado en la sección anterior, el escenario de red objetivo del estudio consistirá en un agregado de múltiples regiones IP/MPLS separadas por routers de tránsito con una capa de transporte con un mallado suficiente para establecer conexiones entre cualquier par de routers de acceso y tránsito si le es requerido por el plano de control GMPLS.

En primer lugar se reduce el problema al cálculo de la disponibilidad de red en una única región con tráfico entre los niveles de acceso e interconexión. Se modelan fallos equipos de tránsito IP/MPLS aunque el estudio aquí desarrollado se puede aplicar a cualquier arquitectura de red en la cual haya equipos que desarrollen el papel de tránsito.

3.1 Modelado analítico

Para modelar el problema se utiliza la herramienta matemática conocida como cadena de Markov [26]. Esta herramienta se basa en la definición de diferentes estados dentro del modelo a evaluar así como las probabilidades de transición entre dichos estados. No es la primera vez que se utiliza para el modelado de fallos en redes como se puede ver en [27]. Mediante el cálculo de esas probabilidades y de la definición de los requisitos del problema se puede obtener medidas para la disponibilidad de una red que es el caso que se necesita.

Se definen los estados de un router IP/MPLS en función de la posibilidad utilizarlo como:

- Fallo: 1
- No fallo: 0

La transición entre los estados de fallo y no fallo se debe a la los tiempos que se tarda en reparar los equipos así como el tiempo que tardan en fallar. Estas variables vienen dadas por los parámetros MTBF y MTTR. Debido a que la cadena de Markov requiere el uso de frecuencias y no tiempos medios, se definen las transiciones entre estados del siguiente modo:

$$0\ a\ 1 \Rightarrow \lambda = 1 / MTBF \quad (1)$$

$$1\ a\ 0 \Rightarrow \mu = 1 / MTTR \quad (2)$$

En las expresiones anteriores se presentan los parámetros λ y μ que son frecuencia de llegada de fallos y frecuencia de llegada de las reparaciones respectivamente. En función a estos parámetros se construye el diagrama de estados de la cadena de Markov para el caso de una región con routers de tránsito duplicados, es decir, aplicando la protección 1+1 a nivel IP/MPLS. A continuación se detalla el estudio de la disponibilidad para una región.

3.1.1 Estudio del caso de una región.

Debido a que la protección 1+1 implica un dimensionamiento de los routers de tránsito de tal modo que sean capaces por si solos de absorber el tráfico de la región entera, se asume que los estados de 0 fallos y 1 fallo no suponen un corte en el servicio y el estado de 2 fallos si afecta a la disponibilidad global de la red.

- Estado 0: No se afecta el servicio
- Estado 1: No se afecta el servicio
- Estado 2: Servicio afectado, cortes de conectividad.

La cadena de Markov se rige por las siguientes expresiones:

$$\underline{\Pi}\underline{\underline{Q}} = \underline{0} \tag{3}$$

$$\sum_i \Pi_i = \underline{1} \tag{4}$$

Donde $\underline{\Pi}$ es el vector de probabilidades de estado y $\underline{\underline{Q}}$ es la matriz de transiciones entre estados que para el caso particular modelado anteriormente se define del siguiente modo:

$$\underline{\underline{Q}} = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\mu+\lambda) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix} \tag{5}$$

$$\underline{\Pi} = [\Pi_0 \quad \Pi_1 \quad \Pi_2] \tag{6}$$

Expandiendo (5) Π_1 y Π_2 se obtienen como función de Π_0. Entonces se puede obtener Π_0 utilizando (6).

$$2\lambda\Pi_0 = \mu\Pi_1 \implies \Pi_1 = (\lambda/\mu)\Pi_0 \tag{7}$$

$$\lambda\Pi_1 = \mu\Pi_2 \implies \Pi_2 = (\lambda/\mu)^2\Pi_0 \tag{8}$$

$$\Pi_0 = 1/(1 + 2(\lambda/\mu) + (\lambda/\mu)^2) \tag{9}$$

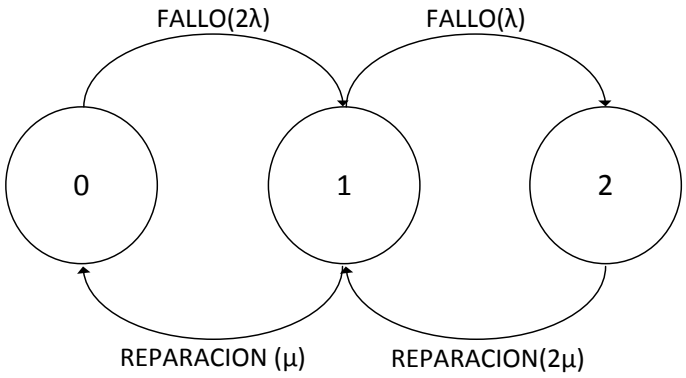

Figura 33 Diagrama de cadena de Markov para 1 región

Es importante hacer notar que en el modelo se asume que los recursos de red se reparan todos simultáneamente en lugar de uno por uno. Esto implica que los pasos de estado donde hay más de un fallo tienen una tasa de cambio de estado $k\mu$ donde k

es el número de routers en estado de fallo. En caso de que solo se pudiera reparar un router simultáneamente la tasa de cambio de estado sería siempre μ.

Una vez se tienen las probabilidades de los estados, se define el concepto de disponibilidad como la suma de la probabilidad de los estados que no afectan el servicio o por el contrario, 1 menos la probabilidad de los estados que afectan al servicio. En este caso es más sencillo modelar la disponibilidad siguiendo el segundo esquema.

$$Disponibilidad = 1 - \Pi_2 = 1 - (\lambda/\mu)^2 \Pi_0 \tag{10}$$

$$Disponibilidad = 1 - \frac{(\lambda/\mu)^2}{1 + 2(\lambda/\mu) + (\lambda/\mu)^2} \tag{11}$$

Para tener una aproximación más cercana a los parámetros medibles y con significado en la red, la expresión de la disponibilidad puede obtenerse en función del MTTR y MTBF. El resultado se muestra en la siguiente expresión.

$$A = 1 - \frac{(MTTR/MTBF)^2}{1 + 2\frac{MTTR}{MTBF} + \left(\frac{MTTR}{MTBF}\right)^2} \tag{12}$$

En este caso, es importante hacer notar que la disponibilidad obtenida para el caso de protección 1+1 es igual al de restauración multicapa puesto que el número de recursos utilizables para realizar la restauración (Routers de tránsito) es el mismo para los dos mecanismos. En caso de aumentar el número de regiones con tránsitos dimensionados al 100% del tráfico de región, la disponibilidad del mecanismo de protección 1+1 se mantiene constante puesto que no hay modo de derivar el tráfico de una región a otra en caso de fallo doble en los tránsitos de dicha región. Por el contrario, el caso de restauración multicapa es capaz de utilizar tránsitos de otras regiones para recuperar el tráfico (si hay capacidad disponible).

3.1.2 Estudio del caso de dos regiones

De ahora en adelante pasaremos a asumir que el tráfico de todas las regiones involucradas es idéntico. En futuros estudios, se podría incluir diferentes matrices de tráfico para obtener resultados con escenarios de red distintos.

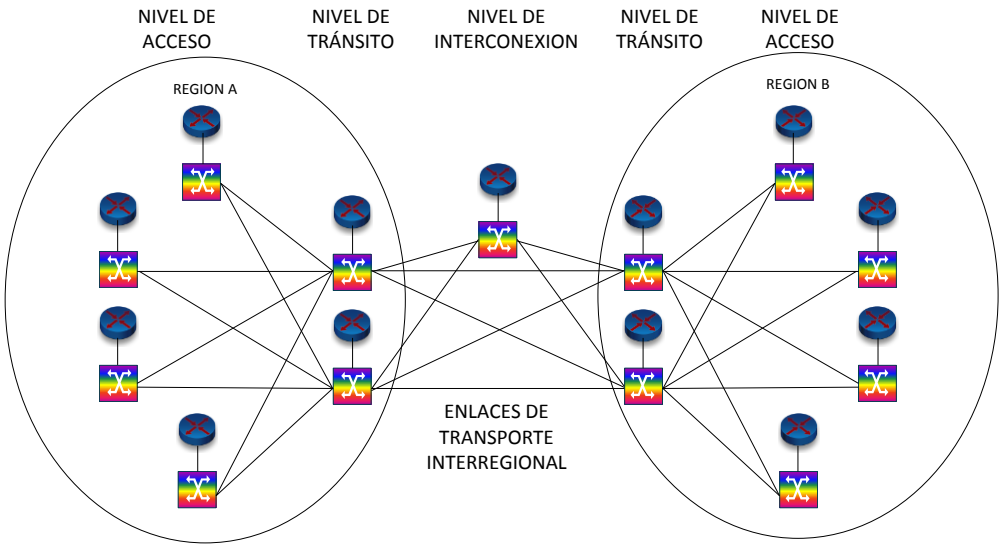

Figura 34 Esquema de red de dos regiones

En el caso de dos regiones, tenemos que para mantener el servicio activo es necesario que al menos haya 2 de los 4 routers totales sin fallos para poder encaminar el tráfico. Las combinaciones posibles pasarían desde los 4 routers activos, 2 activos en una región y 1 en otra, 2 activos en una región y ninguno en la otra o 1 router activo en una región y 1 en la otra. Esto se puede modelar mediante la siguiente cadena de Markov.

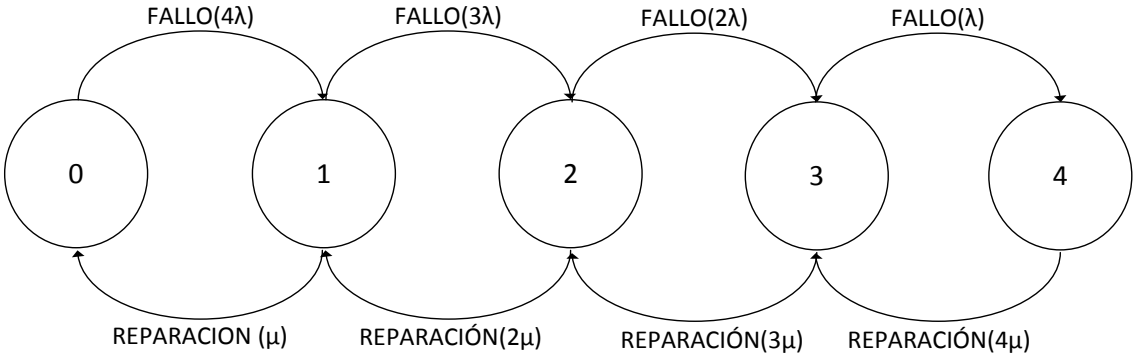

Figura 35 Diagrama de cadena de Markov para 2 regiones

Aplicando el mismo procedimiento que el caso anterior:

$$\underline{\underline{Q}} = \begin{bmatrix} -4\lambda & 4\lambda & 0 & 0 & 0 \\ \mu & -(\mu+3\lambda) & 3\lambda & 0 & 0 \\ 0 & 2\mu & -2(\mu+\lambda) & 2\lambda & 0 \\ 0 & 0 & 3\mu & -(3\mu+\lambda) & \lambda \\ 0 & 0 & 0 & 4\mu & -4\mu \end{bmatrix} \quad (13)$$

$$4\lambda\Pi_0 = \mu\Pi_1 \implies \Pi_1 = 4(\lambda/\mu)\Pi_0 \quad (14)$$

$$3\lambda\Pi_1 = 2\mu\Pi_2 \implies \Pi_2 = 6(\lambda/\mu)^2\Pi_0 \quad (15)$$

$$2\lambda\Pi_2 = 3\mu\Pi_3 \implies \Pi_3 = 4(\lambda/\mu)^3\Pi_0 \quad (16)$$

$$\lambda\Pi_3 = 4\mu\Pi_4 \implies \Pi_4 = (\lambda/\mu)^4\Pi_0 \quad (17)$$

$$\Pi_0 + \Pi_1 + \Pi_2 + \Pi_3 + \Pi_4 = 1 \quad (18)$$

$$\Pi_0 = \frac{1}{1 + 4\frac{\lambda}{\mu} + 6\left(\frac{\lambda}{\mu}\right)^2 + 4\left(\frac{\lambda}{\mu}\right)^3 + \left(\frac{\lambda}{\mu}\right)^4} \quad (19)$$

Teniendo en cuenta que el estudio se ciñe a resultados en los que la proporción entre MTTR y MTBF es inferior a 0.1 (MTBF > 10 MTTR) se puede considerar despreciable la influencia del polinomio más allá del grado 2. Por lo tanto podemos establecer que:

$$Disponibilidad = 1 - \Pi_3 - \Pi_4 \quad (20)$$

$$k = MTTR/MTBF \quad (21)$$

$$Disponibilidad = 1 - \Pi_0(4k^3 + k^4) \quad (22)$$

$$Disponibilidad = 1 - \frac{4k^3 + k^4}{1 + 4k + 6k^2} \quad (23)$$

Esto se debe a que los estados con influencia en la disponibilidad son los estados en los que del total de 4 routers de las dos regiones, hay al menos 3 en estado de fallo.

3.1.3 Estudio para N regiones

Generalizando la expresión anterior para el caso de n regiones:

$$\Pi_0(n) = \frac{1}{1 + 2nk + n(2n-1)k^2} \tag{24}$$

$$A(n) = 1 - \Pi_0(n)\left(\sum_{i=n+1}^{2n} (k)^i \left[\frac{2n!}{(2n-i)!\,i!}\right]\right) \tag{25}$$

Obteniendo los resultados de la expresión anterior, podemos presentar la siguiente figura en la que se representa la disponibilidad de la red frente al MTTR/MTBF.

Los resultados mostrados en la Figura 36 presentan un incremento de la disponibilidad por el uso de la restauración multicapa.

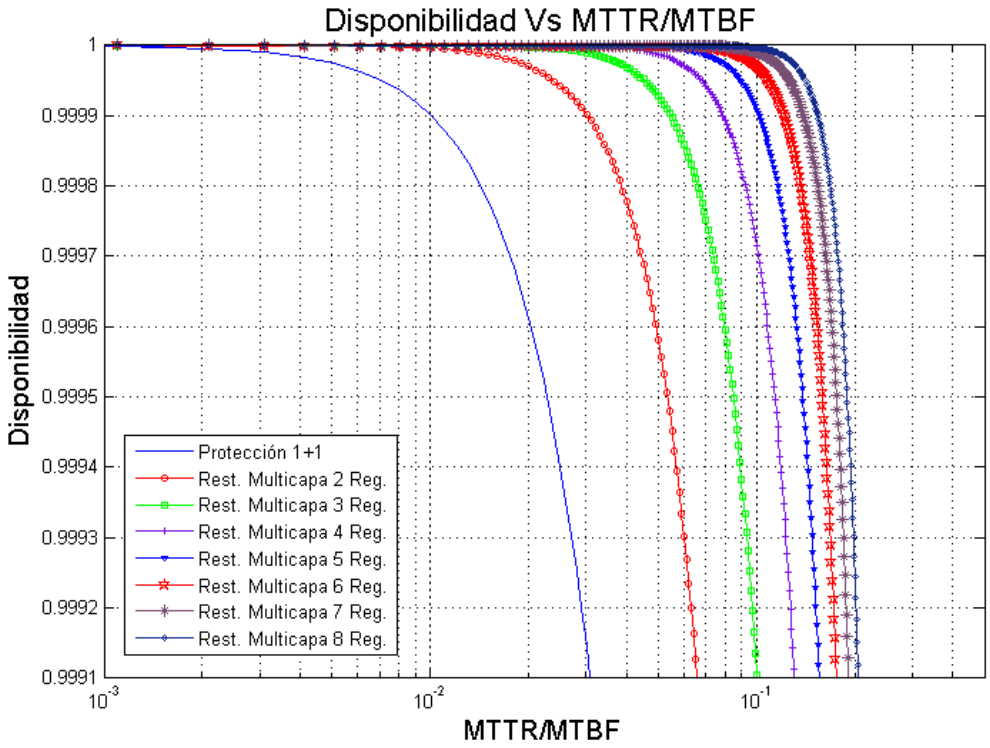

Figura 36 Disponibilidad en función del número de regiones

3.2 Modelado mediante simulación

El simulador, realizado en Omnet++ 4.0, ilustra el comportamiento de los casos teóricos introduciendo cierta complejidad relacionada con la realidad física que se esconde detrás del modelo teórico. En primer lugar, el modelo teórico hace determinadas suposiciones que el simulador da la opción de eliminar con el objetivo de obtener resultados más fidedignos.

- El modelo teórico asume que el establecimiento de los circuitos ópticos es instantáneo, el simulador permite establecer un determinado tiempo para realizar la reserva de la conexión. Esto tendría impacto en la disponibilidad.
- De igual modo, el modelo teórico asume que cada fallo y reparación son instantáneas, no teniendo en cuenta el retardo entre la aparición del evento y su efecto en el tiempo de reparación.
- El modelo teórico asume que la red óptica siempre tiene recursos disponibles para satisfacer las peticiones, el simulador por el contrario puede establecer restricciones que hagan el modelo más real.

De todos modos, el simulador siempre se puede adaptar para reflejar el modelo teórico tal y como se ha definido para obtener simulaciones que verifiquen dicho modelo. Utilizar las funcionalidades adicionales del simulador aportaría ventajas desde el punto de vista de la estimación de la operación real de la red lo cual puede tener aplicaciones interesantes para los operadores.

3.2.1 Características de Omnet++

Adentrándonos en el simulador, como características principales del mismo se puede decir que Omnet es una plataforma que basa su funcionamiento en el paso de mensajes entre bloques. En concreto, [28] define Omnet como “Un entorno y librería de simulación extensible, modular y basada en componentes en C++ construida para simuladores de red”. Omnet++ ofrece un entorno basado en Eclipse, un entorno de ejecución gráfico así como extensiones para simulación en tiempo real, emulación de redes y alternativas de integración para lenguajes de programación diferentes a C++.

Omnet en definitiva es un simulador de eventos discretos que proporciona una arquitectura basada en componentes que modelan el comportamiento de entidades dentro de la red. Omnet posee un lenguaje de scripting de alto nivel llamado NED que agrupan los módulos individuales definidos en C++.

Un ejemplo de cómo se organizan las entidades dentro de Omnet se puede observar en la siguiente figura:

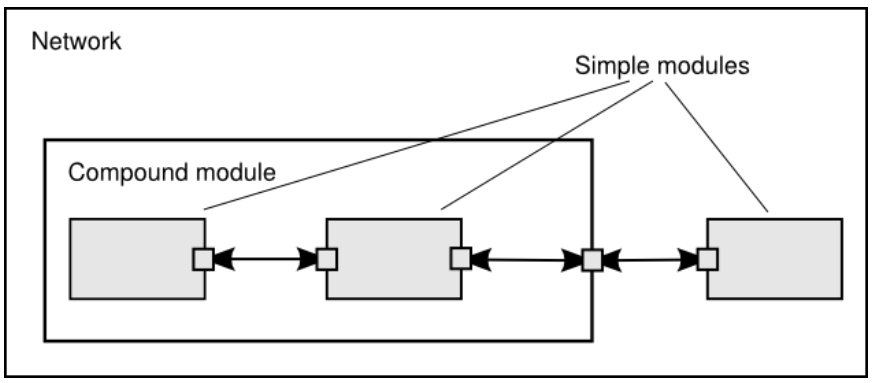

Figura 37 Definición de bloques compuestos en Omnet++ [28]

Una red en omnet se construye a partir de lo que se entiende por módulos simples que interconectados y agrupados forman componentes compuestos y estos, a su vez interrelacionados crean la red. Los módulos se comunican mediante mensajes que pueden contener datos arbitrarios además de campos habituales como la marca de tiempo de creación del mensaje. Se definen puertas en los módulos actuando como interfaces que controlan el acceso y envío de los mensajes entre módulos. Se trata de una estructura jerárquica en la que las puertas de los módulos compuestos se corresponden con las puertas de los sub-módulos comprendidos dentro del módulo compuesto.

Para modelar las redes de comunicaciones, Omnet proporciona mecanismos de creación de enlaces con información de tasa binaria, retardo de propagación, tasa de error que pueden ser habilitados o deshabilitados según se necesite.

Un ejemplo de definición de red mediante el lenguaje NED de omnet sería el siguiente:

```
//
// A network
//
network Network
{
   submodules:
      node1: Node;
      node2: Node;
      node3: Node;
      ...
   connections:
      node1.port++ <--> {datarate=100Mbps;} <--> node2.port++;
      node2.port++ <--> {datarate=100Mbps;} <--> node4.port++;
      node4.port++ <--> {datarate=100Mbps;} <--> node6.port++;
      ...
}
```

Como se puede observar en el código, el lenguaje de definición de redes se nombra la red en este caso ***Network*** y define los sub-módulos involucrados en la red ***Node1, Node2…*** En la sección del código de conexiones (o enlaces) se relaciona las puertas de los sub-módulos con información de la tasa binaria en este caso (***100 Mbps***). Estos son los elementos básicos de definición de una red en Omnet++ aunque con el objetivo de simplificar y facilitar la creación de redes grandes, los enlaces con características iguales, los Channels (Canales).

```
//
// A Network
//
network Network
{
   types:
      channel C extends ned.DatarateChannel {
         datarate = 100Mbps;
      }
   submodules:
      node1: Node;
      node2: Node;
      node3: Node;
      ...
   connections:
      node1.port++ <--> C <--> node2.port++;
      node2.port++ <--> C <--> node4.port++;
```

```
        node4.port++ <--> C <--> node6.port++;
        ...
}
```

Como se puede observar en el código, para grandes redes con enlaces con características iguales, se hace mucho más cómodo y sencillo el proceso de definición de la red agrupando los enlaces por canales.

El proceso de creación de módulos simples se compone de dos partes, por un lado se tiene el código NED que define las interfaces, módulos y parámetros. Por otra parte está el código C++ que define la operación del módulo basado en los mensajes entrantes por las puertas, las funciones a implementar utilizando los parámetros del módulo y el envío de los resultados de las operaciones realizadas por el módulo hacia el módulo destinatario según corresponda. Un ejemplo del código NED de varios módulos simples sería el siguiente:

```
simple App
{
   parameters:
      int destAddress;
      ...
      @display("i=block/browser");
   gates:
      input in;
      output out;
}

simple Routing
{
   ...
}

simple Queue
{
   ...
}
```

En este ejemplo se muestra por primera vez la forma de definir atributos visuales, la cláusula @display permite elegir los iconos, texto, fuente, localización y más parámetros asociados a la representación visual de los módulos en el entorno gráfico. No tienen mayor funcionalidad más allá de convertir en más atractivo y entendible el comportamiento del simulador.

Un módulo compuesto se construye relacionando entradas y salidas de módulos simples como puede verse en la figura y código siguientes:

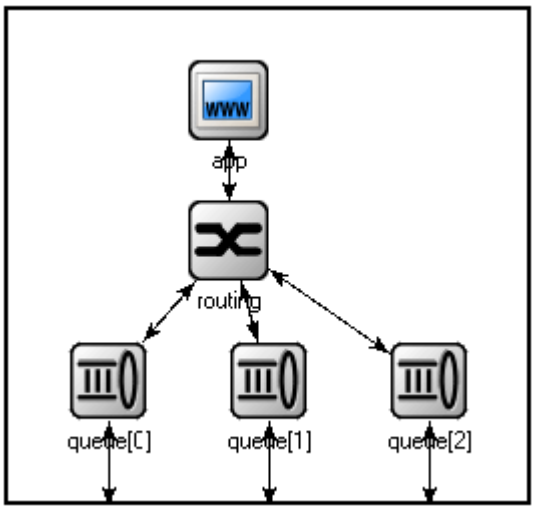

Figura 38 Módulo compuesto de Omnet [28]

```
module Node
{
    parameters:
        int address;
        @display("i=misc/node_vs,gold");
    gates:
        inout port[];
    submodules:
        app: App;
        routing: Routing;
        queue[sizeof(port)]: Queue;
    connections:
        routing.localOut --> app.in;
        routing.localIn <-- app.out;
        for i=0..sizeof(port)-1 {
            routing.out[i] --> queue[i].in;
            routing.in[i] <-- queue[i].out;
            queue[i].line <--> port[i];
        }
}
```

En el código se puede comprobar la inclusión de los módulos simples en la red y la conexión entre los mismos en la asociación ***routing.out[i] --> routing.in[i]*** donde además se puede ver la existencia de puertas con múltiples entradas y salidas, es decir, arrays de puertas con un mismo identificador. De este modo se puede interconectar múltiples módulos de un modo rápido y sin hacerlo uno por uno como si se utilizara puertas con distintos nombres. Otro punto a destacar es la existencia de puertas unidireccionales que sólo permiten el envío o recepción de mensajes. Esto supone en la práctica la posibilidad de definir redes asimétricas con diferentes características en función del sentido de la conexión a realizar (un ejemplo típico sería la simulación de una red ADSL (*Asymmetric Digital Subscriber Line***,** Línea de suscriptor digital asimétrica) en la que el ancho de banda de bajada desde el DSLAM (*Digital Subscriber Line Access Multiplexer*, Multiplexor de línea de acceso digital del

suscriptor) hacia el suscriptor es superior en al ancho de banda de subida. En definitiva, con estos elementos, la definición de un gran número de redes diferentes se hace posible.

En referencia al proceso de simulación es necesario explicar cómo se realiza y cuáles son las fases (eventos) que se dan en instancias discretas de tiempo. Se asume que no sucede nada interesante en el tiempo que separa dos eventos discretos por lo que en ese tiempo no se toma ninguna acción. La definición de "interesante" lógicamente depende mucho de lo que se pretenda simular. Un ejemplo de esto podría ser:

- Inicio de la transmisión de un paquete
- Fin de la transmisión de un paquete
- Un temporizador de retransmisión se agota

Este modelo asumiría que entre el inicio y la finalización de la transmisión del paquete no sucede nada salvo el hecho de considerar el paquete en estado de transmisión. Asociado a estos eventos se incorpora la marca de tiempo o timestamp que permite calcular el tiempo de transmisión como la resta entre la aparición de dichos eventos. La prioridad en el procesado de los eventos sigue las siguientes reglas:

1. El evento con menor timestamp se ejecuta primero. En caso de que el timestamp sea idéntico:
2. El evento con menor prioridad numérica se ejecuta antes. En caso de que la prioridad numérica sea igual:
3. El evento programado antes o enviado antes (en tiempo real de ejecución) se procesa antes.

Respecto al tiempo de simulación, debido al uso de números de 64 bits, la separación mínima necesaria entre eventos limita el tiempo máximo de duración de la simulación. Por lo tanto, si se necesita una resolución de nanosegundos se tendría menor tiempo máximo de simulación que si se trata de milisegundos. La muestra la relación entre la resolución y el tiempo de simulación:

Exponente	Resolución	Rango Aproximado
-18	10^{-18}s (1aseg)	+/- 9.22 segundos
-15	10^{-15}s (1fseg)	+/- 153.72 minutos
-12	10^{-12}s (1pseg)	+/- 106.75 días
-9	10^{-9}s (1nseg)	+/- 292.27 años
-6	10^{-6}s (1useg)	+/- 292271 años
-3	10^{-3}s (1mseg)	+/- 2.9227e8 años
0	1seg	+/- 2.9227e11 años

Tabla 7 Relación entre la resolución y la duración de la simulación [28]

Una vez expuestas las características del entorno de simulación a utilizar, se detalla la implementación básica de los módulos que permitirá crear las redes multicapa objeto del estudio de este documento.

3.2.2 Desarrollo de los bloques del simulador

El simulador se ha desarrollado siguiendo una jerarquía de bloques que, desde la parte superior de la jerarquía a la inferior es la siguiente:

- Red Completa
  - Gestor de simulación
    - Control de mensajes
    - Control de topología
    - Control de conexiones
    - Control de fallos
  - Gestor de conexiones IP/MPLS y DWDM
    - Control de mensajes
    - Control de topología
    - Control de conexiones
    - Control de fallos
  - ROADM
    - Control de mensajes
    - Control de conexiones
  - ROUTER
    - Control de conexiones
    - Control de rutas

A continuación se expone módulo por módulo la funcionalidad y tareas desempeñadas así como la información almacenada. También se detallan las interfaces y los mensajes utilizados para la comunicación entre módulos y sub-módulos.

Red Completa

La red completa comprende todos los elementos implicados en las simulaciones y las interconexiones entre ellos. Una red como la de la Figura 39 crea dos topologías. La topología IP/MPLS es virtual y por tanto necesita de infraestructura de transporte para el establecimiento de conexiones. La topología de transporte DWDM es real y posee las conexiones determinadas por las uniones entre fibras que a su vez permite la creación lightpaths entre ROADMs que servirán para la creación de la topología virtual IP/MPLS.

Para el control de los eventos de la simulación como la reserva de la matriz de tráfico y la creación de eventos de fallo y reparación se utiliza el *gestor de simulación*. El gestor tiene enlaces con todos los nodos de la red y el gestor de conexiones de tal modo que se permite enviar mensajes relacionados con todos los eventos de la simulación.

Para el control del encaminamiento, almacenamiento y mantenimiento de la TED (*Traffic Egineering Database*, Base de datos de ingeniería de tráfico [29], [30]) se utiliza el gestor de conexiones que entre sus funciones principales destaca el cálculo de rutas multicapa y la toma de decisiones para la restauración interregional. Además transforma los eventos de simulación de creación de reservas, restauración y fallos en mensajes y actuaciones sobre la TED.

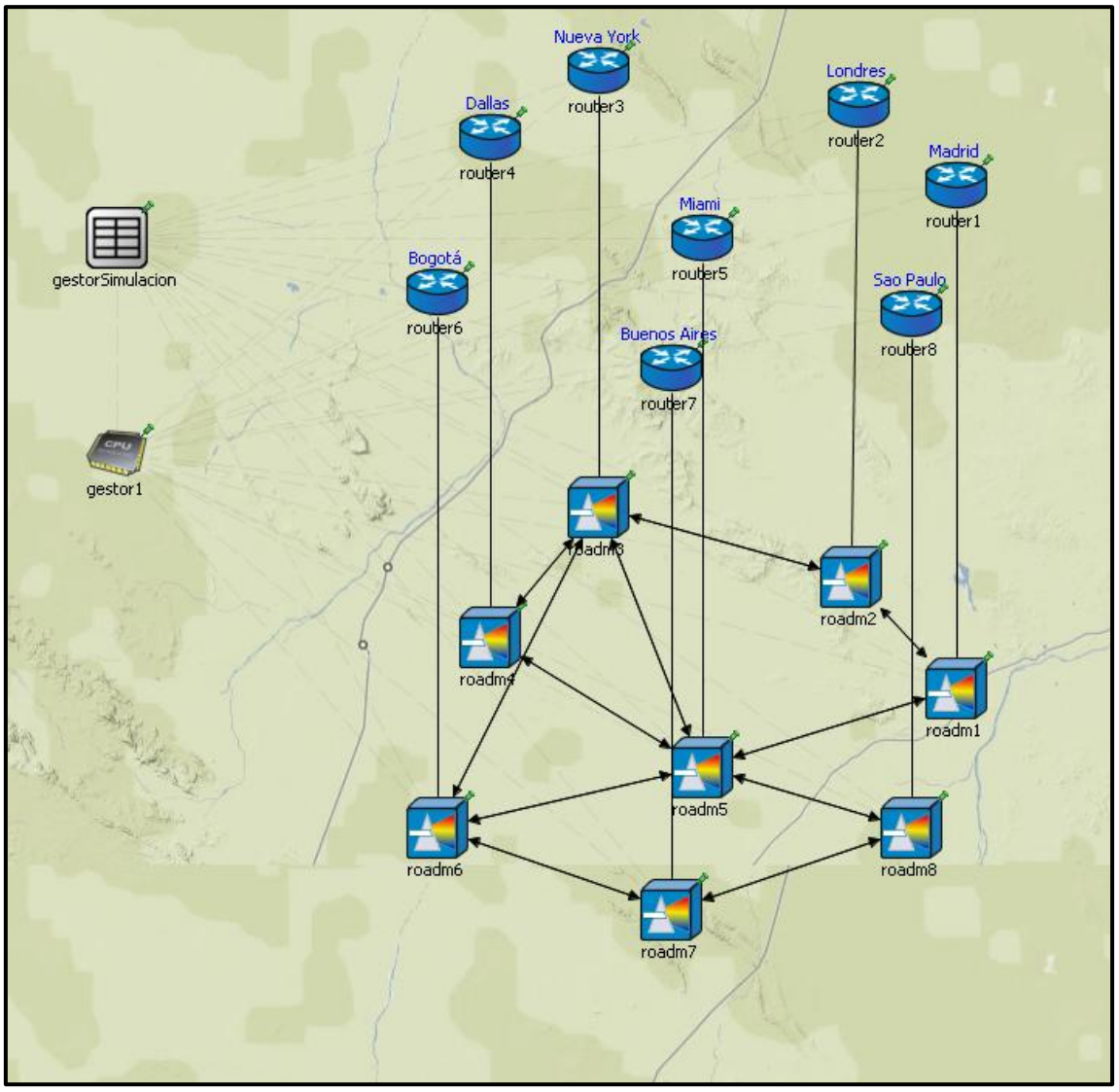

Figura 39 Ejemplo de red completa

Gestor de Simulación

El gestor de simulación se compone de cuatro sub-módulos interconectados entre sí del modo en que se observa en la Figura 40. Se incorpora el módulo de gestión de mensajes que discriminará entre los mensajes de llegada aquellos que correspondan a cada sub-módulo y a su vez decidirá en función del destino del mensaje, por qué interfaz ha de enviar dicho mensaje.

En el caso del gestor de simulación, el módulo de control de la topología se encarga de almacenar el grafo de la topología de red. El módulo de control de conexiones tiene la función de, cuando se genera una matriz de tráfico, leerla del fichero, interpretarla con la ayuda de la topología (relaciona la información leída en el fichero con la topología almacenada) y crear un mensaje que solicite la creación de los enlaces virtuales en la capa IP/MPLS al gestor de conexiones IP/MPLS y Transporte DWDM. En este punto el módulo de control de conexiones lee un fichero de texto en el que se recogen las demandas IP/MPLS siguiendo la siguiente regla:

- Identificador de nodo fuente
- Identificador de nodo destino
- Ancho de banda

A partir de esos parámetros y el fichero de definición de parámetros de ejecución de la simulación (.ini) en el cual se define si las conexiones tendrán protección a nivel IP/MPLS o no, se crea un mensaje que contiene la siguiente información:

- Identificador de la conexión (identificador único).
- Identificador de router IP/MPLS fuente
- Identificador de router IP/MPLS destino
- Identificador de tarjeta IP/MPLS fuente (Información extraída de la topología).
- Identificador de tarjeta IP/MPLS destino (Información extraída de la topología).
- Mecanismo ante fallo (Protección o Ninguno)

Con esta información, el mensaje llega al módulo de control de mensajes y lo encamina hacia el gestor de conexiones IP/MPLS y transporte DWDM quien, lo procesará y obtendrá el camino explícito que deberá recorrer el tráfico IP/MPLS.

El módulo de control de fallos lee de un fichero los nodos, tarjetas y enlaces físicos incluidos en el modelo de fallos. Tras leer todos los identificadores de los elementos sujetos a fallos y añadiendo la información del fichero de definición de parámetros de ejecución de la simulación en la que se recoge los parámetros de frecuencia de fallos y reparaciones (MTTR y MTBF) planifica la creación de eventos de fallo con distribución exponencial de media MTTR para las reparaciones y MTBF para los fallos.

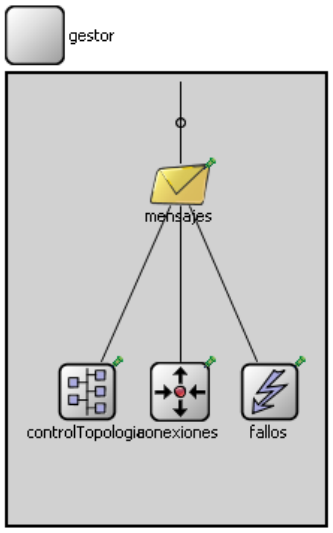

Figura 40 Gestor de simulación

Gestor de conexiones IP/MPLS y transporte DWDM

El gestor de conexiones IP/MPLS y transporte DWDM almacena la TED de la red completa de tal modo que en cualquier instante de la simulación puede saber el estado de reserva de recursos de los nodos y tarjetas de ambas capas. Esta TED se almacena en el módulo control de topología y consta de dos instancias de la misma, una TED que controla el estado en “tiempo real” de la red y otra TED que almacena las operaciones en curso como por ejemplo, en caso de solicitar el establecimiento de un enlace entre dos nodos de transporte DWDM, para evitar que durante el proceso de establecimiento se produzca un cálculo de ruta que solicite los mismos recursos, se almacenan como reservados en esta TED temporal. Una vez se confirman las reservas de recursos, la TED temporal y la TED primaria deben tener la misma información almacenada.

El gestor de conexiones, pese a poseer los módulos de control de fallos y conexiones no hace uso de ellos pues la relación entre la TED y las reservas se realiza en la misma topología manteniendo una tabla con las conexiones existentes y el estado en que se encuentran (fallo o activas).

Como tarea principal del gestor de conexiones éste debe decidir en caso de producirse una solicitud de establecimiento de conexión la ruta en la capa de transporte que permitirá reservar una longitud de onda que pueda cursar el tráfico IP/MPLS necesario. Además, el gestor controlará el algoritmo multicapa a partir del cual procederá a mover el tráfico en las regiones con fallo doble hacia los tránsitos de una región que tenga capacidad suficiente para albergar el de la región fallida.

Router IP/MPLS

El módulo de router IP/MPLS posee un gestor de mensajes que opera del mismo modo que lo realizan los gestores de mensajes del resto de módulos. En el sub-módulo de rutas el router define la ocupación y estado de las tarjetas además de iniciar la propagación información de fallo cuando estos son informados por parte del generador de la simulación. Cuando un fallo es detectado en una demanda naciente en el router implicado, se informa al gestor de conexiones IP/MPLS y DWDM del fallo para que decida sobre la alternativa a realizar y este vuelve a informar al router fuente de la conexión para que modifique sus parámetros del modo que se considere oportuno.

Además, el router recopila estadísticas acerca de las demandas que inicia y las informa al gestor de conexiones para que al final de la simulación se pueda evaluar la disponibilidad de cada demanda y posterior procesado.

En referencia a las conexiones entre módulos, el router IP/MPLS se encuentra únicamente conectado al nodo de transporte DWDM que cursará sus peticiones. Para la creación de la topología virtual a nivel IP/MPLS se utilizan las librerías de creación dinámica de enlaces de Omnet que permite la creación, modificación y eliminación de puertas y conexiones entre las mismas.

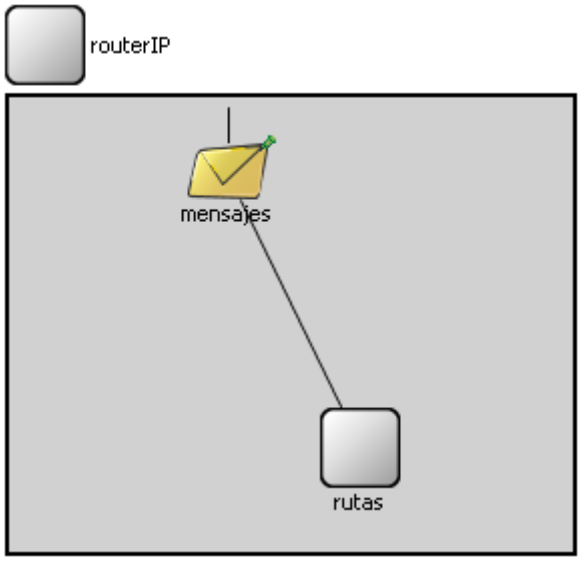

Figura 41 Módulo router IP/MPLS

ROADM

El ROADM, al tratarse de una entidad con topología real física, se inicializa con las conexiones correspondientes a la topología que implementa. Desde el punto de vista

de control de establecimiento de reservas el ROADM propaga los paquetes de reserva hasta el último nodo del camino a reservar. Una vez el paquete alcanza el destino, se propaga en camino inverso reservando los recursos (en este caso longitudes de onda en las fibras ópticas) y transmitiendo tanto al router fuente como al gestor de conexiones el resultado del procedimiento de establecimiento.

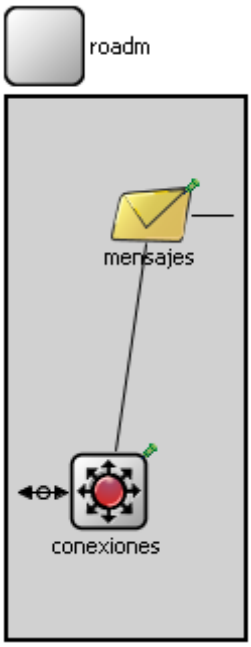

Figura 42 Módulo ROADM

3.2.3 Funcionamiento del simulador

El funcionamiento del simulador sigue una secuencia de eventos programados para desarrollar la comparación propuesta por el modelo teórico.

Los pasos que sigue la simulación son los siguientes:

1. Lectura de la matriz de demandas y de la topología IP. (Figura 43)
2. Establecimiento de las demandas y enlaces así como solicitud a la malla fotónica de los recursos necesarios para cursar el tráfico. (Figura 44)
3. Se espera la aparición de eventos de fallo.
4. A la llegada del primer evento de fallo se activa la protección IP. No hay pérdida de conectividad en ningún momento.
5. Ante un fallo simple puede suceder dos cosas:
    a. Llega un evento de reparación antes que llegue el siguiente fallo, por lo tanto se devuelve la red a su estado original.
    b. Llega un evento de fallo al router que soporta en ese instante todo el tráfico de la región afectada. Por lo tanto, la red procede a establecer nuevas adyacencias con los tránsitos de otra región en caso de tener capacidad para ello. (En este caso asumimos que es posible, ya que de no serlo simplemente se computa como tiempo de indisponibilidad).
6. Suponiendo el estado actual de la red el caso de la Figura 46, puede, en función de los eventos que lleguen dar lugar a diferentes resultados en la red:

a. Nuevo evento de fallo en un router de la región restauradora. En este caso prevalece la protección, expulsando a la región que estaba siendo restaurada de los tránsitos y perdiendo la conectividad totalmente. En este punto, se recuperará la conectividad cuando uno de los routers de tránsito propios de la región sean reparados.
b. Llega evento de reparación. La región que está siendo restaurada, vuelve a ocupar el router que se repara y activa de nuevo los mecanismos de protección.

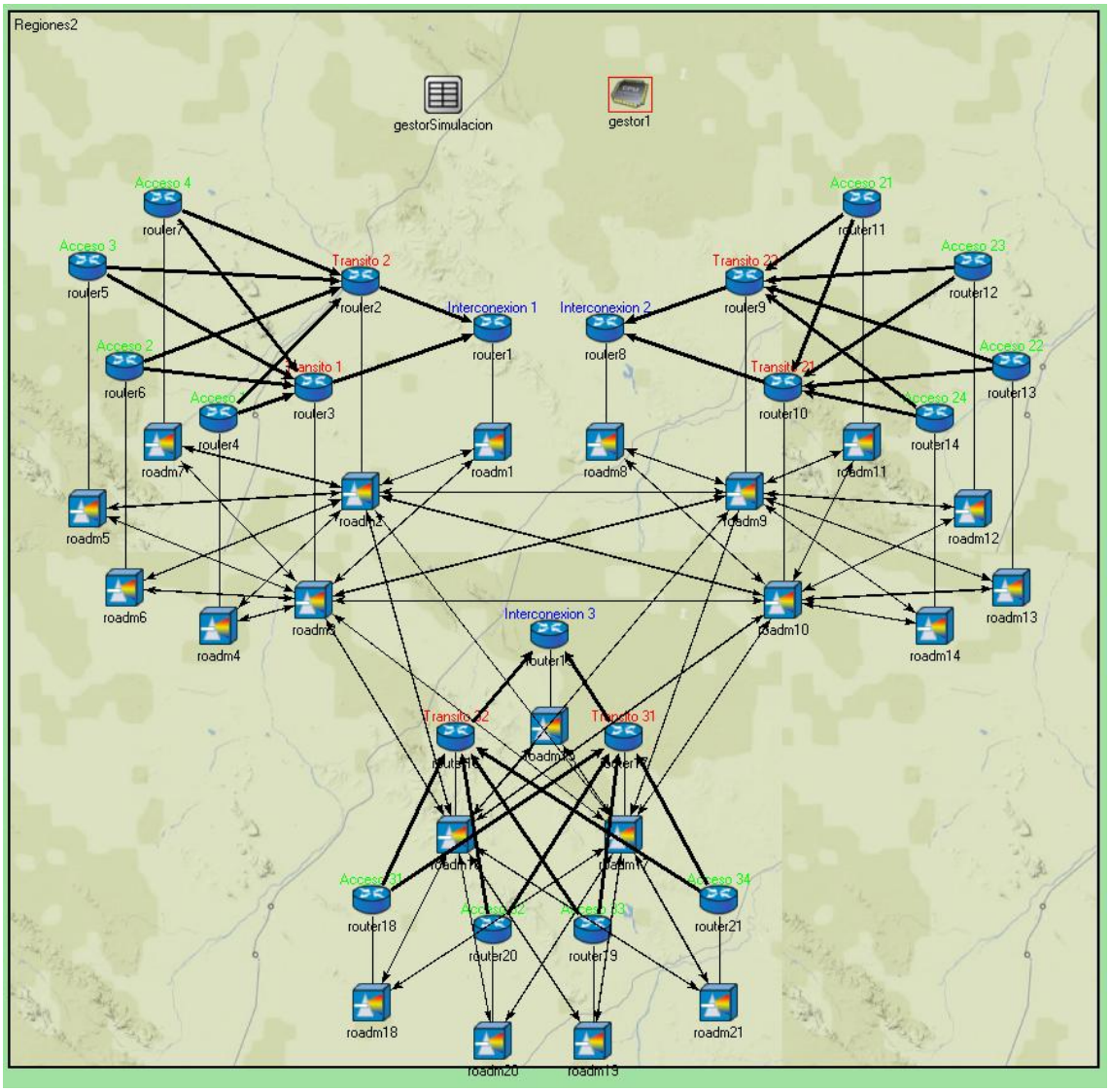

Figura 43 Esquema de red multicapa de 3 regiones simulado en Omnet++

A partir de aquí la casuística se convierte en pasos intermedios entre los distintos puntos de la lista anterior sin modificaciones sustanciales, por lo que resumiendo, sólo hay pérdida de conectividad en el momento en que una de las regiones pierde a sus dos routers y, se de uno de los dos supuestos siguientes:

- La región restauradora tiene al menos un router en fallo. En este caso no se restaura debido a la falta de recursos libres suficientes.

- La región restauradora a priori tiene todos los routers activos y restaura la región fallida, pero posteriormente uno de sus routers falla y tiene que expulsar a la región que estaba siendo restaurada.

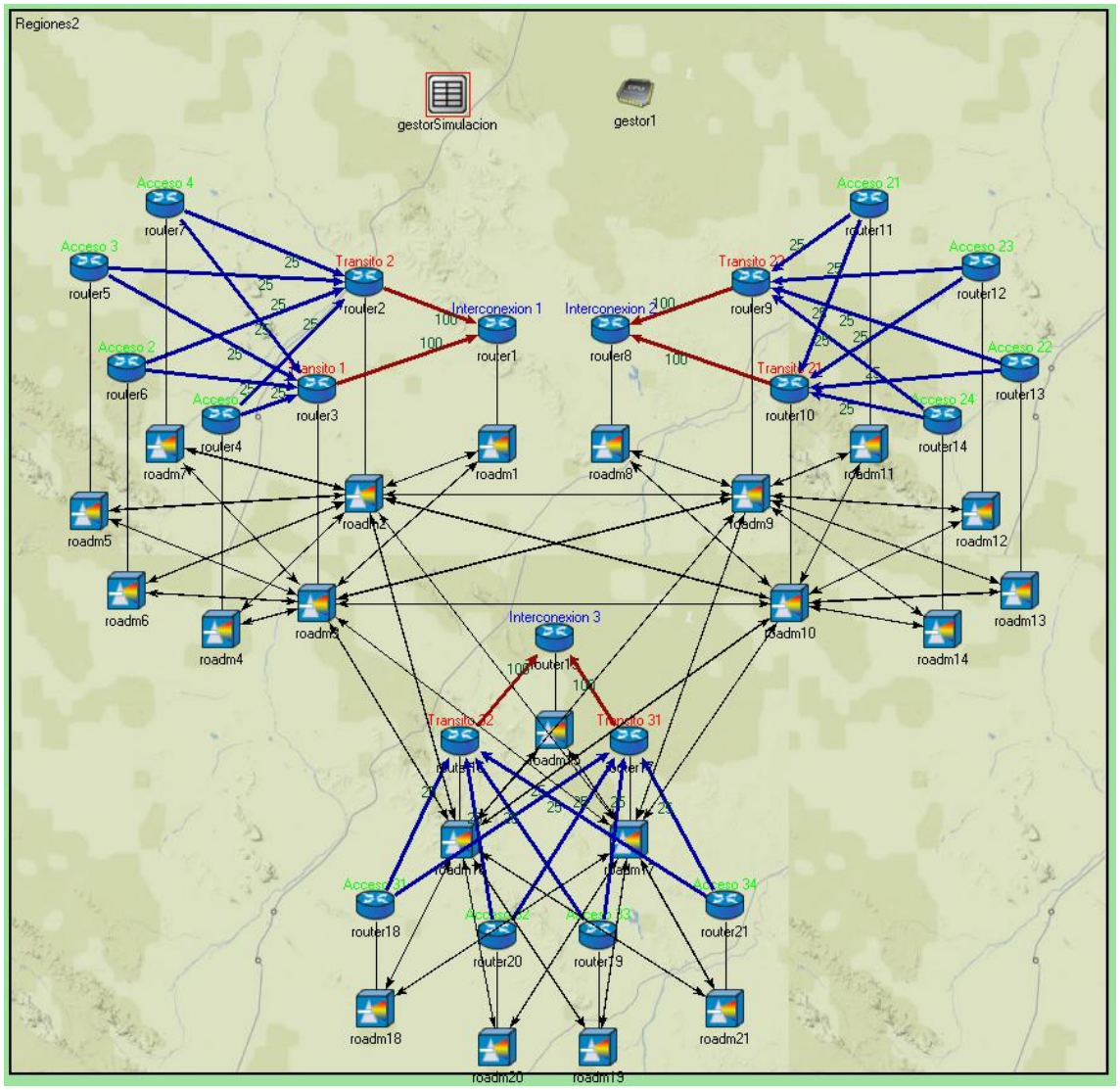

Figura 44 Esquema de red multicapa con recursos regionales reservados

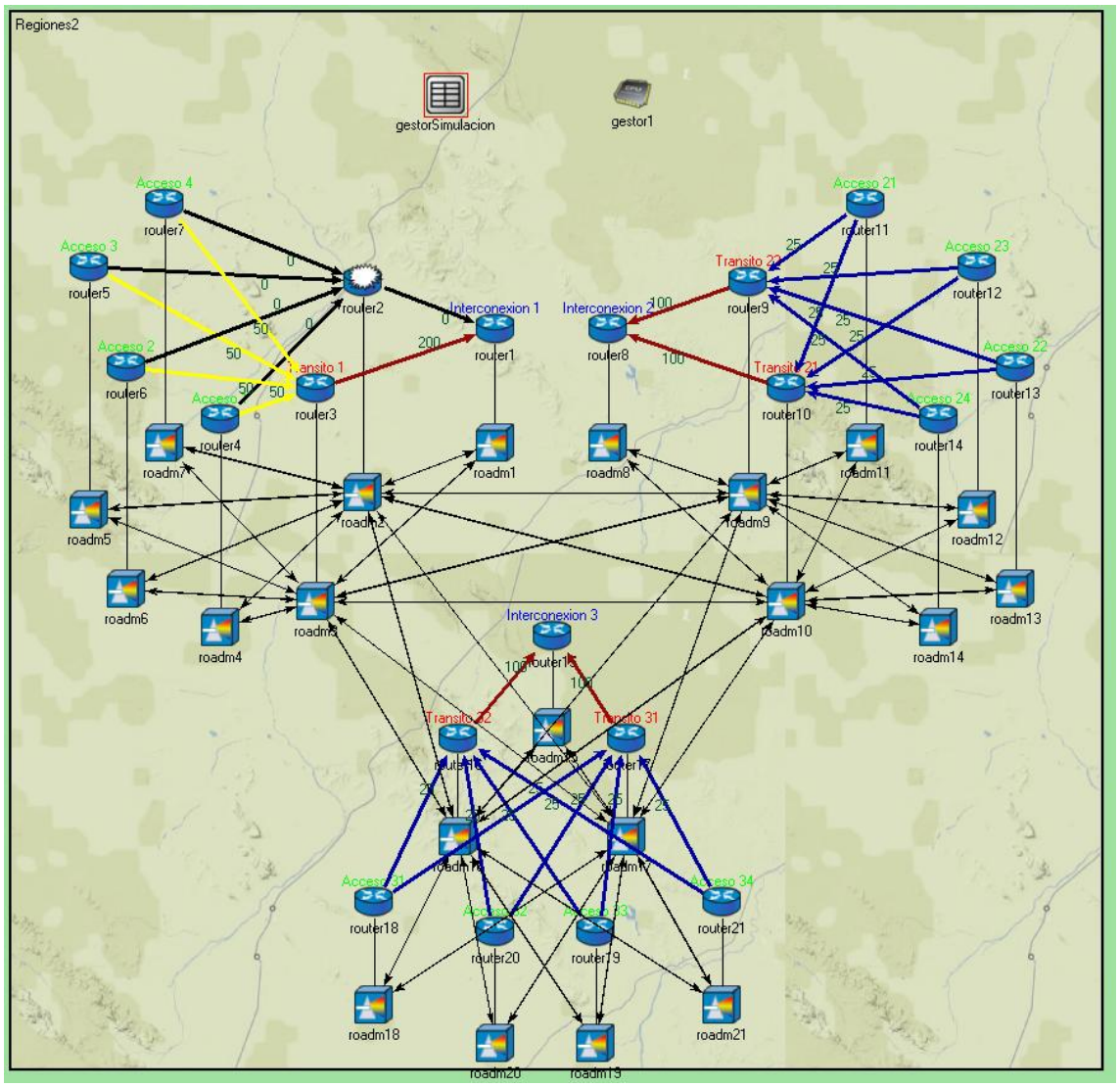

Figura 45 Fallo detectado en un nodo de tránsito

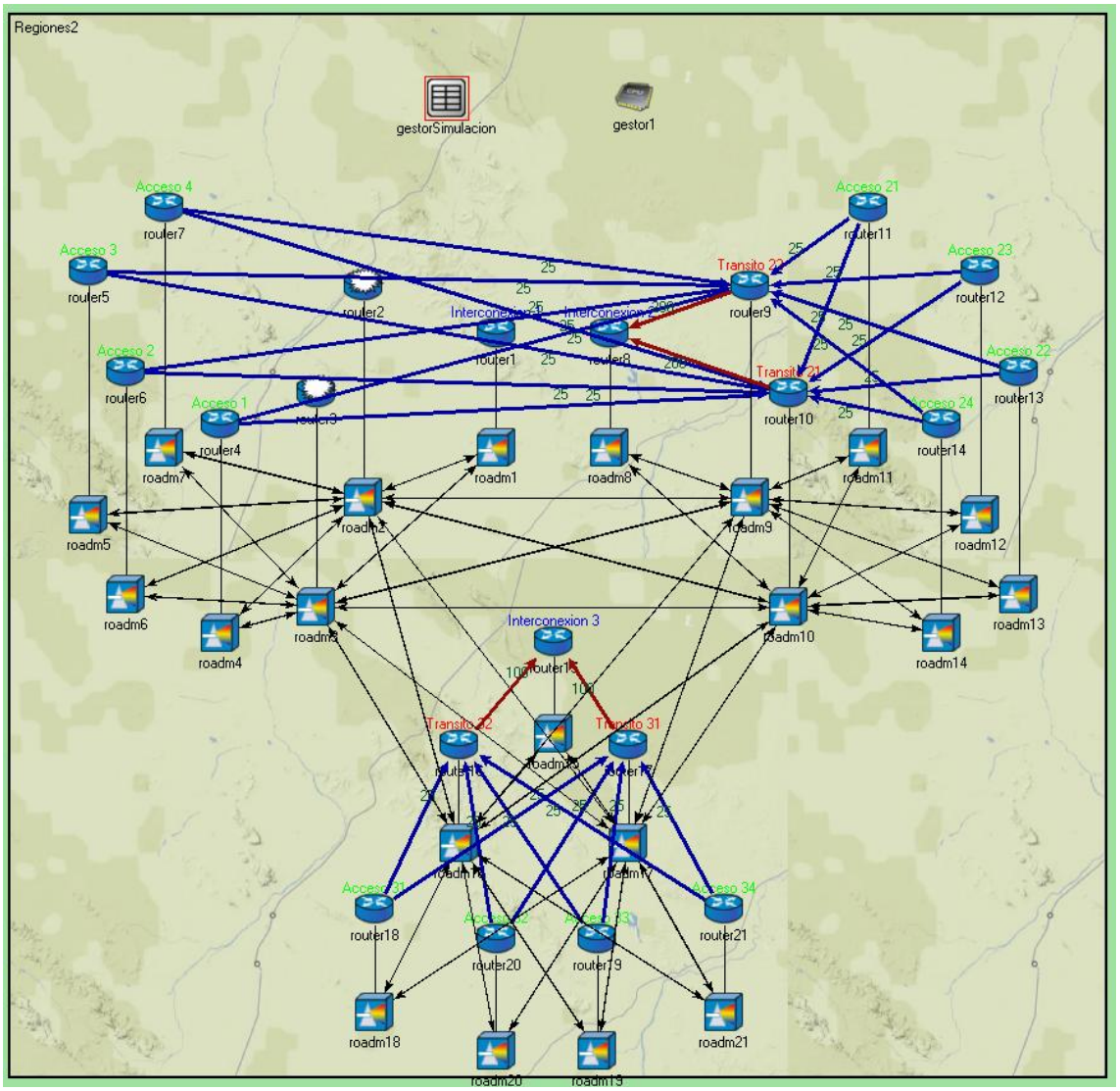

Figura 46 Restauración multicapa interregional

Para el cálculo de la disponibilidad se realiza una media ponderada de la disponibilidad de cada uno de los flujos de tráfico hacia interconexión. La disponibilidad de cada flujo es la siguiente:

$$Disponibilidad_{Demanda} = 1 - \frac{\text{Tiempo no disponible de la demanda}}{\text{Duración de la simulación}} \qquad (26)$$

3.3 Validación de los modelos analíticos y de simulación

En una primera iteración para la validación de los datos del estudio analítico se procede a simular únicamente los fallos en los routers IP/MPLS de tránsito. Los parámetros del estudio son los siguientes:

- MTBF: 1 a 5 años.
- MTTR: 0.5 a 180 días.
- Duración de la simulación: 50 años.

Para comparar estos datos con los del estudio analítico, se presentan los casos hasta 3 regiones en la Figura 47. Como se puede observar, los resultados coinciden lo que valida los resultados obtenidos por el modelo analítico.

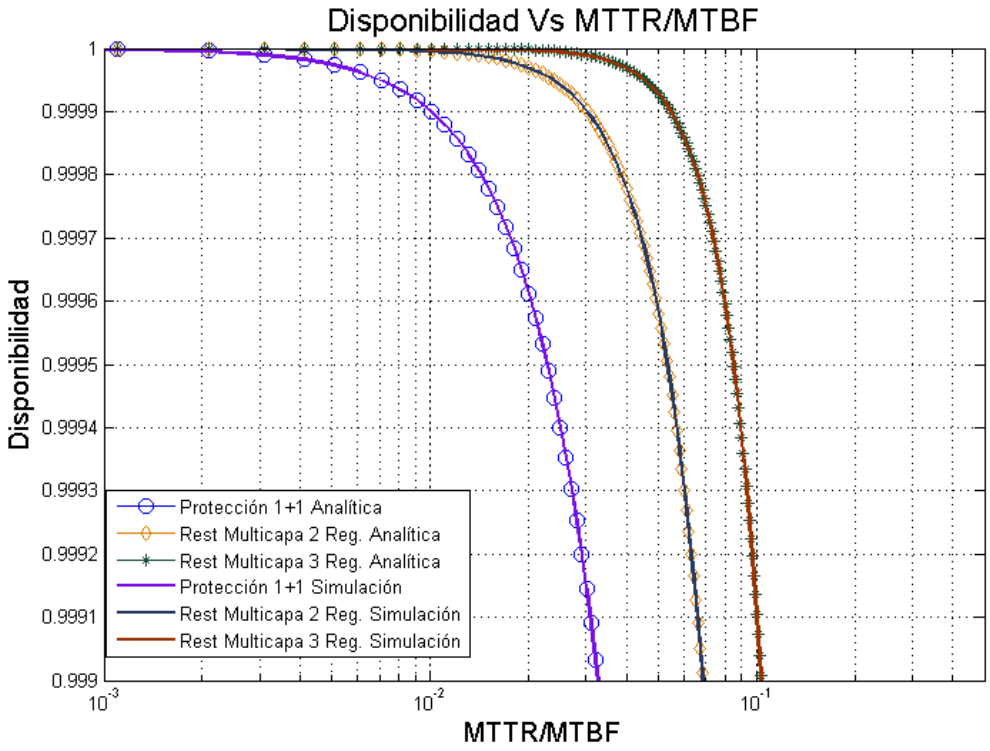

Figura 47 Disponibilidad en relación a MTTR/MTBF para 3 regiones

La interpretación de la Figura 48 se realiza comparando la relación entre el MTTR/MTBF con la disponibilidad obtenida. Si se fija una disponibilidad de 5 nueves se puede comparar la relación MTTR/MTBF necesaria con cada método para conseguir el objetivo de disponibilidad. Por ejemplo, para el caso de protección 1+1 es necesario que MTTR/MTBF sea igual a 5.5x10-3 para obtener 5 nueves.

$$\mathrm{A(Proteccion\ 1+1)} = 0.0055 = \frac{\mathrm{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 6.02\ \ Días \qquad (27)$$

El significado de esto es que **si tenemos un fallo cada 3 años en un equipo, con la protección 1+1 necesitaremos reparar ese fallo antes de 6.02 días** para no encontrarnos con un fallo doble que genere una pérdida de conectividad. Aplicando esto para los casos de restauración multicapa de 2 regiones y 8 regiones como casos extremos, tenemos los siguientes resultados:

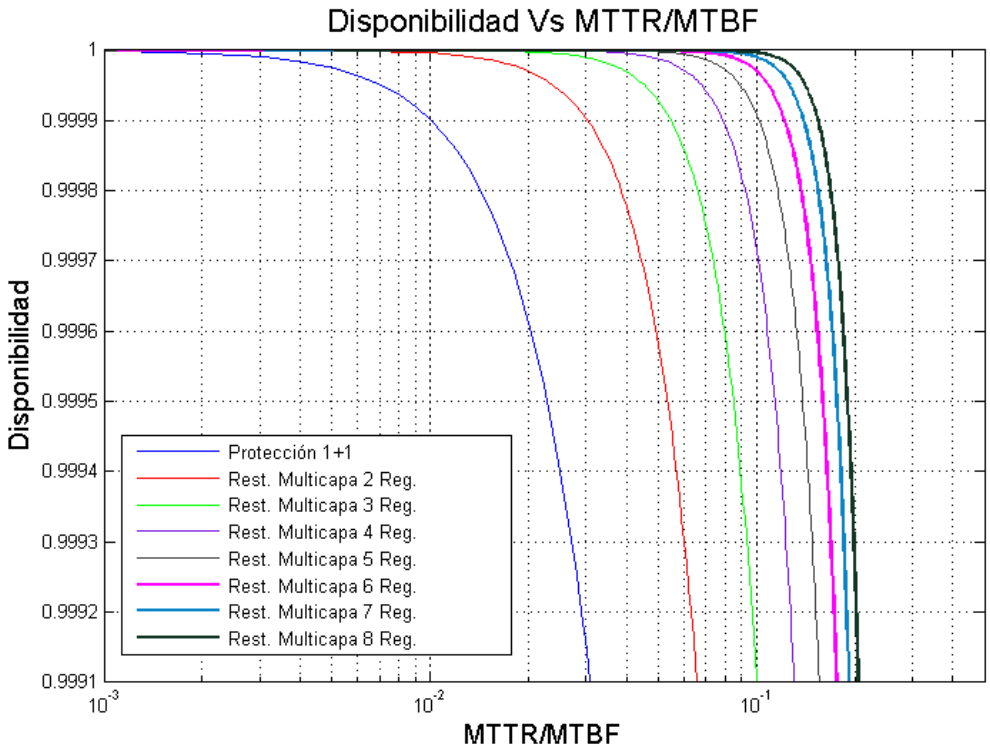

Figura 48 Disponibilidad en función de MTTR/MTBF para múltiples regiones

$$\text{A(MR 2 Regiones)} = 0.018 = \frac{\text{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 19.71\ Días \tag{28}$$

$$\text{A(MR 8 Regiones)} = 0.115 = \frac{\text{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 125.925\ Días \tag{29}$$

3.4 Estudios Tecno-económicos.

La restauración multicapa proporciona un incremento de disponibilidad para una relación MTTR/MTBF dada significativo. Para el caso de la red de 8 regiones, Se puede interpretar de diferente modo los beneficios obtenidos.

3.4.1 Estudio de costes de equipamiento

Una de las aproximaciones consiste en reducir la necesidad de invertir en nuevas tarjetas y nodos en el tránsito IP/MPLS manteniendo la disponibilidad objetivo. Este enfoque permite conseguir los siguientes resultados:

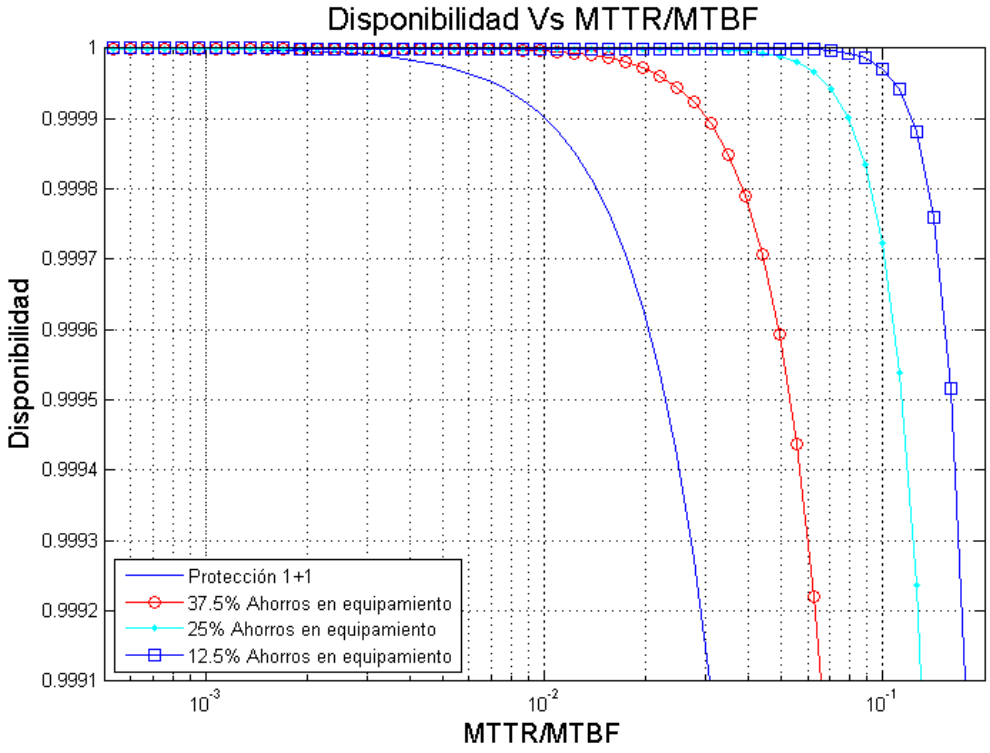

Figura 49 Disponibilidad reduciendo el número de routers de tránsito

Los resultados mostrados en la Figura 49 se interpretan del siguiente modo:

- Para una red de ocho regiones y con protección 1+1 cada una de ellas se obtiene la curva de disponibilidad vs MTTR/MTBF etiquetada por Proteción 1+1 en la figura.
- A esa red protegida 1+1 en sus ocho regiones le quitamos recursos IP/MPLS del tránsito (o dejamos de invertir en incrementar su capacidad) por capacidad de 2 routers. El resultado de esta reducción de recursos supone un ahorro del 12.5% puesto que se pasa de tener 16 routers a tener 14. La disponibilidad obtenida es la representada por la curva etiquetada como 12.5% Ahorros en equipamiento.
- Siguiendo con el mismo procedimiento se continua disminuyendo capacidad de tránsito hasta alcanzar el 37.5%.

La conclusión es que, por el hecho de incluir **la restauración multicapa** se puede **reducir los costes en el tránsito de la red IP en un 37.5% sin ver afectada la disponibilidad**.

3.4.2 Estudio de costes de operación

La inclusión de la restauración multicapa puede enfocarse desde el punto de vista de los costes de operación de la red. Si se tiene en cuenta que cada operación de reparación, cambios en la configuración de los equipos y operaciones semejantes necesitan de una rápida acometida en caso de ser críticos (como el caso de un fallo doble para los esquemas de protección 1+1), es importante prolongar los tiempos necesarios reparar y reconfigurar equipamiento manteniendo la disponibilidad constante. Esta extensión del tiempo de reparación necesario es otra manera de interpretar los resultados obtenidos anteriormente. En la Figura 50 se presentan los beneficios en costes de operación de la restauración multicapa.

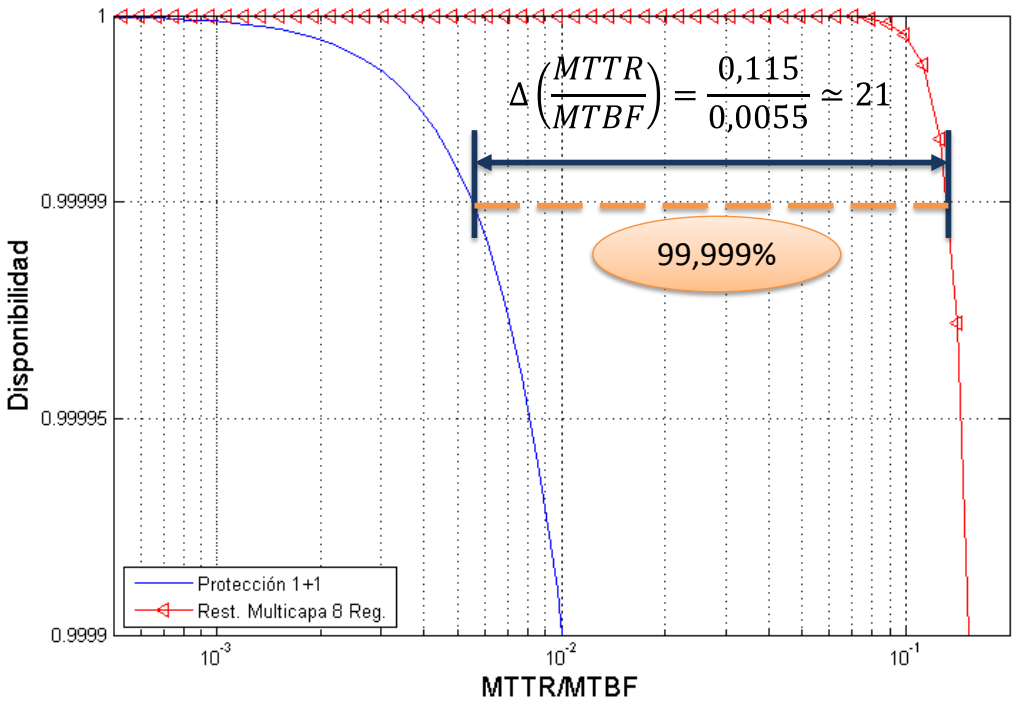

Figura 50 Disponibilidad en función de MTTR/MTBF para estudio de costes de operación

La interpretación de la Figura 50 se realiza comparando la relación entre el MTTR/MTBF con la disponibilidad obtenida. Si se fija una disponibilidad de 5 nueves se puede comparar la relación MTTR/MTBF necesaria con cada método para conseguir el objetivo de disponibilidad. Por ejemplo, para el caso de protección 1+1 es necesario que MTTR/MTBF sea igual a 5.5×10^{-3} para obtener 5 nueves.

$$\mathrm{A(Proteccion\ 1+1)} = 0.0055 = \frac{\mathrm{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 6.02\ Días \qquad (30)$$

El significado de esto es que **si tenemos un fallo cada 3 años en un equipo, con la protección 1+1 necesitaremos reparar ese fallo antes de 6.02 días** para no encontrarnos con un fallo doble que genere una pérdida de conectividad. Aplicando esto para los casos de restauración multicapa de 2 regiones y 8 regiones como casos extremos, tenemos los siguientes resultados:

$$\mathrm{A(MR\ 2\ Regiones)} = 0.018 = \frac{\mathrm{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 19.71\ Días \tag{31}$$

$$\mathrm{A(MR\ 8\ Regiones)} = 0.115 = \frac{\mathrm{MTTR}}{MTBF = 3 * 365} \rightarrow MTTR = 125.925\ Días \tag{32}$$

En consecuencia, la **restauración multicapa permite multiplicar el tiempo de reparación (MTTR) en 3.6 veces para el caso de 2 regiones hasta en 21 veces para el caso de 8 regiones**.

Los resultados para el barrido de número de regiones implicadas son los siguientes:

- 2 Regiones: 3.27 veces MTTR/MTBF
- 3 Regiones: 7.6 veces MTTR/MTBF
- 4 Regiones: 11 veces MTTR/MTBF
- 5 Regiones: 14 veces MTTR/MTBF
- 6 Regiones: 18 veces MTTR/MTBF
- 7 Regiones: 20 veces MTTR/MTBF
- 8 Regiones: 21 veces MTTR/MTBF

4 Demostración de restauración multicapa con equipos reales

Una vez se ha analizado la viabilidad de la restauración multicapa desde el punto de vista teórico y mediante simulación, se procede a demostrar cómo actualmente puede realizarse con equipamiento real la restauración multicapa. Puesto que el equipamiento actual no implementa un plano de control multicapa que permita realizar el cómputo multicapa de rutas y establecimiento de las mismas de forma autónoma cuando los eventos de fallo se presentan, es necesario el diseño e inclusión de una entidad que gestione esta inteligencia adicional para permitir la realización de la restauración multicapa.

Como consecuencia, se ha desarrollado un gestor multicapa en lenguaje de programación Java que interactúe con los elementos de red y en función de las medidas obtenidas de los equipos, tome decisiones de configuración coherentes con los algoritmos multicapa.

4.1 Arquitectura del gestor de restauración multicapa

En primer lugar, el gestor multicapa necesitará cumplir con determinadas funciones que se detallan a continuación para ser eficaz a la hora de restaurar el tráfico cuando ninguna de las dos capas es capaz de hacerlo por sí misma. Para ello, el gestor de restauración multicapa debe ser capaz de detectar los fallos en la red por lo que deberá incluir un módulo de monitorización. En segundo lugar, el gestor debe ser capaz de tomar la decisión más adecuada en función de la información de que dispone en cada momento. Para ello, se incluye el un módulo que controle el estado de la red y toma las decisiones sobre los cambios a realizar en la red. En tercer lugar, el gestor debe ser capaz de configurar el equipamiento de red del modo adecuado para que las directrices tomadas por el controlador sean implementadas en el equipamiento de red lo que resulta en un módulo de configuración de equipos.

Por último, es necesario poder operar el gestor para cambiar políticas de operación referente a la restauración multicapa así como otras funciones típicas de administración de equipos por lo que se define un módulo de administración. La arquitectura resultante es la siguiente:

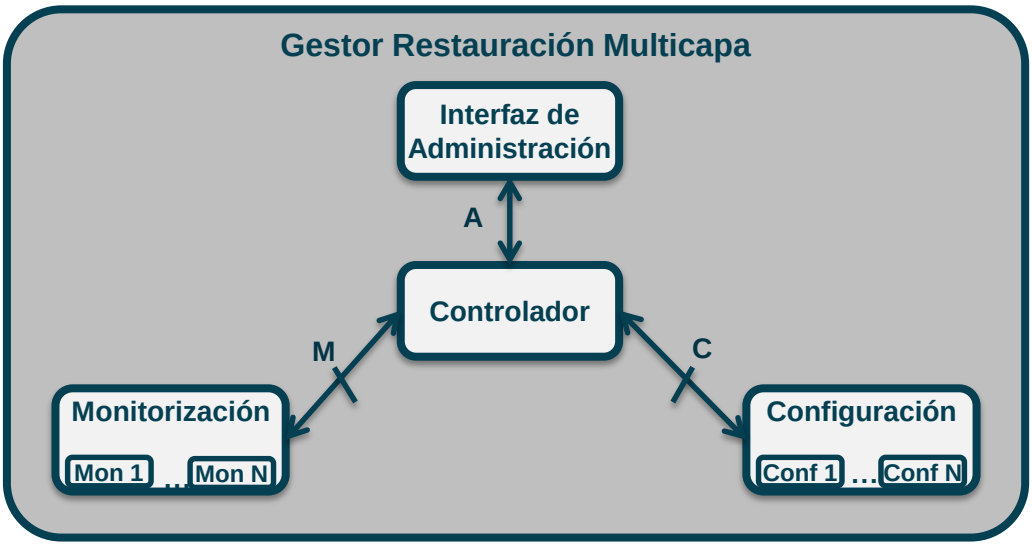

Figura 51 Arquitectura del gestor multicapa

En el anexo se incluye el diagrama de clases Java del desarrollo del gestor multicapa.

4.2 Interfaces estándar utilizados en el prototipo

Con el objetivo de hacer lo más interoperable posible el prototipo, se pretende elegir las interfaces utilizadas para monitorización y configuración a partir de protocolos estándar en lo posible.

4.2.1 Configuración

En el proceso de establecimiento de enlaces a nivel IP/MPLS y transporte se necesita llevar a cabo diferentes procesos de configuración que recorren desde el direccionamiento y encaminamiento a nivel IP/MPLS hasta la creación dinámica de lightpaths en la capa de transporte para posibilitar el establecimiento de nuevas adyacencias en la capa IP/MPLS. En este punto se ha de diferenciar la configuración de la capa IP/MPLS y la capa de transporte puesto que se utilizaran mecanismos diferentes.

Capa IP/MPLS

En la capa IP/MPLS se utilizará CLI (*Command Line Interface*, Interfaz de línea de comandos) para realizar las operaciones de configuración. CLI es una interfaz propietaria con comandos diferentes para cada fabricante lo que supone la necesidad de desarrollar los comandos necesarios para cada equipo que se desee configurar.

Como ventajas, CLI permite la configuración, monitorización y provisión de servicios de un modo seguro (siempre que se CLI se ejecute en entornos controlados desde el punto de vista del control de acceso) y además, al tratarse de una interfaz desarrollada por el fabricante, la exactitud y precisión de las instrucciones proporcionadas es máxima. Por el contrario, otros protocolos de configuración que pueden ser estándar, pueden no tener todas las funcionalidades que permite el equipamiento por tratarse de configuraciones muy específicas del fabricante en concreto.

Como desventajas, la configuración se trata de un proceso secuencial de introducción de comandos que, en general, para elaborar una configuración que implique a varios protocolos puede llevar un tiempo de configuración mayor. Con el objetivo de automatizar la configuración se puede optar por la creación de diferentes scripts que secuencien la sucesión de comandos a ejecutar para completar diferentes tareas de configuración pero cada vez que hay una actualización de software en la que comandos se ven afectados, es posible que sea necesario realizar modificaciones en los scripts con el coste consecuente que este proceso supone.

Otras opciones se han barajado para configurar el equipamiento IP/MPLS tales como NETCONF (*NETwork CONFiguration protocol*, Protocolo de configuración de red). En el caso de NETCONF ([31], [32]) se trata de un protocolo diseñado específicamente para la configuración de equipamiento, por lo que la arquitectura de entidades necesarias y la estructura del protocolo están pensadas para mantenimiento de estados de configuración, vuelta atrás de las mismas, backups, permitir configuraciones simultáneas de varios operadores… En cualquier caso, NETCONF no define los modelos de datos del equipamiento, tarea que recae sobre YANG [33] que es el lenguaje basado en XML (*Extensive Markup Language*, Lenguaje extensivo de marcas) utilizado para definir de forma estándar los parámetros necesarios para la configuración de los equipos. En caso de que la penetración en el mercado fuera elevada, haría de NETCONF un protocolo interesante para ser incluido en sistemas

como el prototipo en cuestión ya que permitiría una implantación para múltiples fabricantes.

Se ha elegido CLI por su simplicidad de implementación para un caso concreto como el de este demostrador.

Capa de transporte DWDM

En la capa de transporte DWDM el procedimiento de configuración será a través del UNI iniciado por el router IP/MPLS siguiendo un modelo overlay, es decir, los equipos de transporte actuarán como capa servidora de conexiones a los equipos de la capa IP/MPLS que solicitarán conexiones a la capa de transporte. El interfaz UNI [34] define RSVP como protocolo para intercambio de mensajes de reserva de recursos entre la capa IP/MPLS y la capa de transporte en el modelo overlay en GMPLS.

Para el correcto funcionamiento del interfaz UNI es necesario la definición previa de los enlaces entre los equipos de transporte e IP/MPLS de tal modo que se les asigne un direccionamiento IP que permita al equipo IP/MPLS transmitir el paquete RSVP. El mantenimiento del estado del enlace se realiza mediante LMP y el direccionamiento se realizaría siguiendo las reglas definidas en la sección 2.3.1.1. Al no existir plano de control multicapa, no existe protocolo que anuncie estas adyacencias existentes entre ambas capas así como tampoco hay modo de informar que equipamiento IP/MPLS es alcanzable a través de la capa de transporte DWDM.

A consecuencia de esto, el controlador del gestor de restauración multicapa debe guardar un contexto de la topología entre capas así como las rutas posibles entre la capa IP/MPLS y de transporte que puedan dar lugar a nuevas adyacencias con objetivo de realizar la restauración multicapa de un modo satisfactorio.

4.2.2 Monitorización

La monitorización del estado de la red se ha de realizar mediante protocolos de gestión orientados al control de estado de equipamiento. En particular, en este prototipo se ha decidido utilizar SNMP (*Simple Network Management Protocol*, Protocolo de gestión de red simple) debido a su sencillez, al número de distribuciones libres existentes y a que la práctica totalidad de los equipos de red lo implementan.

En principio SNMP fue diseñado para la gestión de nodos de red ya fueran servidores, routers, equipos de transporte… El protocolo de transporte utilizado para la comunicación es UDP (*User Datagram Protocol*, Protocolo de datagramas de usuario) que no es orientado a conexión y no garantiza la entrega de los paquetes. La no garantía de la entrega de paquetes, es decir, la no confirmación de la realización de las tareas solicitadas mediante SNMP es una limitación que no lo hace un buen candidato para configurar equipos pero por el contrario, no supone un problema serio a la hora de monitorizarlos.

La información de estado de los equipos se almacena en MIBs (*Management Information Base*, Base de información de gestión) [35] que si bien tiene definido el modelo de datos de un modo estándar para los equipos, los fabricantes han añadido extensiones en sus MIBs para la gestión de información propietaria a través de sus NMSs (*Network Management System*, Sistemas de gestión de red). En la MIB la información se almacena formando árboles de OIDs (*Object IDentifier*, Identificador de objetos) que organizan como muestra la Figura 52.

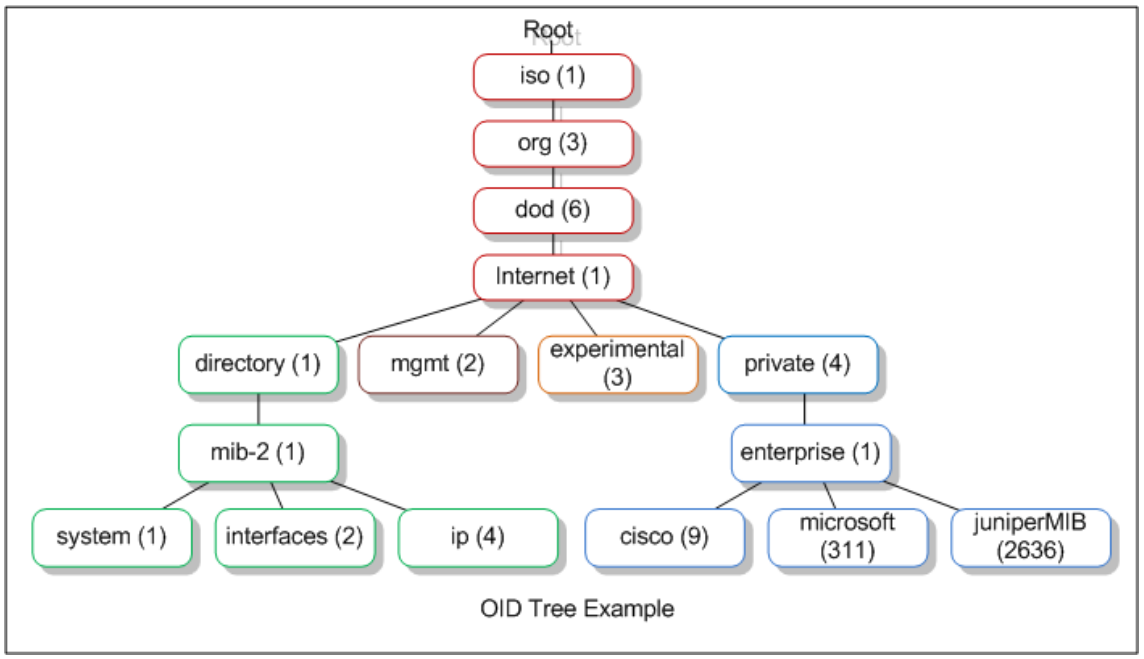

Figura 52 Árbol de OIDs de ejemplo [35]

Hay múltiples versiones de SNMP cuyas diferencias se presentan a continuación:

- SNMP v1: Se trata de la primera implementación y es más básica que permite realizar la mayoría de tareas de gestión de equipos en la red. Se definen operaciones tales como *Get, Get-Next y Trap* que permiten obtener valores de determinadas variables de estado de los equipos como el estado de las interfaces, los paquetes y octetos transmitidos, la velocidad de la interfaz y demás información de interés desde el punto de vista de la gestión de equipos.
- SNMP v2: La segunda versión de SNMP añade a la primera mejoras relacionadas con la agrupación de respuestas sobre múltiples consultas reduciendo la carga de la red. Además se añade la operación *Get-Bulk* que permite solicitar de una vez una gran cantidad de información de la MIB.
- SNMP v3: La tercera y última versión de SNMP añade capacidades de administración y seguridad incluyendo además procedimientos de configuración remota gracias al añadido de nuevas operaciones *SET*.

4.3 Caso de uso

El caso de uso a demostrar es la restauración multicapa para lo cual se ha contado con un equipamiento IP/MPLS de Juniper, en concreto los modelos MX80 con interfaces de 10 Gbps. Se cuenta con tres nodos que con el firmware de los equipos con versión Junos 10.4R2.6.

Las interfaces de los routers transmiten sobre la longitud de onda 1310nm (fibra monomodo) y se conectan a nodos FSP 3000 con clientes DWDM de 10 Gbps. Estos nodos poseen conmutación y reconfiguración dinámica óptica, es decir, se trata de ROADMs. En la Figura 56 se muestra la interconexión realizada con el objetivo de demostrar la que la restauración multicapa es realizable.

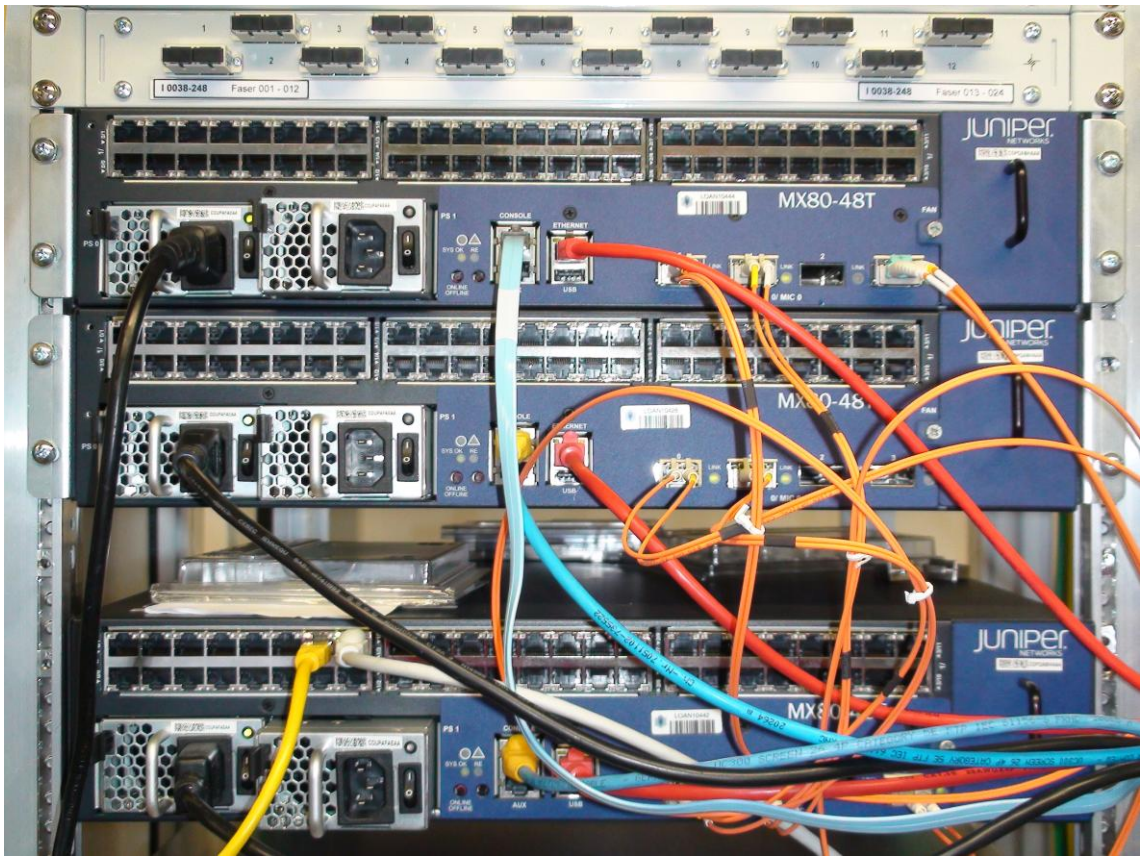

Figura 53 Routers Juniper MX-80

El escenario inicial constará de dos enlaces IP/MPLS utilizando la capa de transporte, uno entre los equipos MX80 ONE y MX80 TWO y el segundo entre los equipos MX80 TWO y MX80 THREE. Este conexionado asemeja al de una red jerárquica en la que el router MX80 ONE actuaría como nivel de acceso, el MX80 TWO desempeñaría la función de tránsito y por último en el caso del nodo MX80 THREE sería el nivel de interconexión.

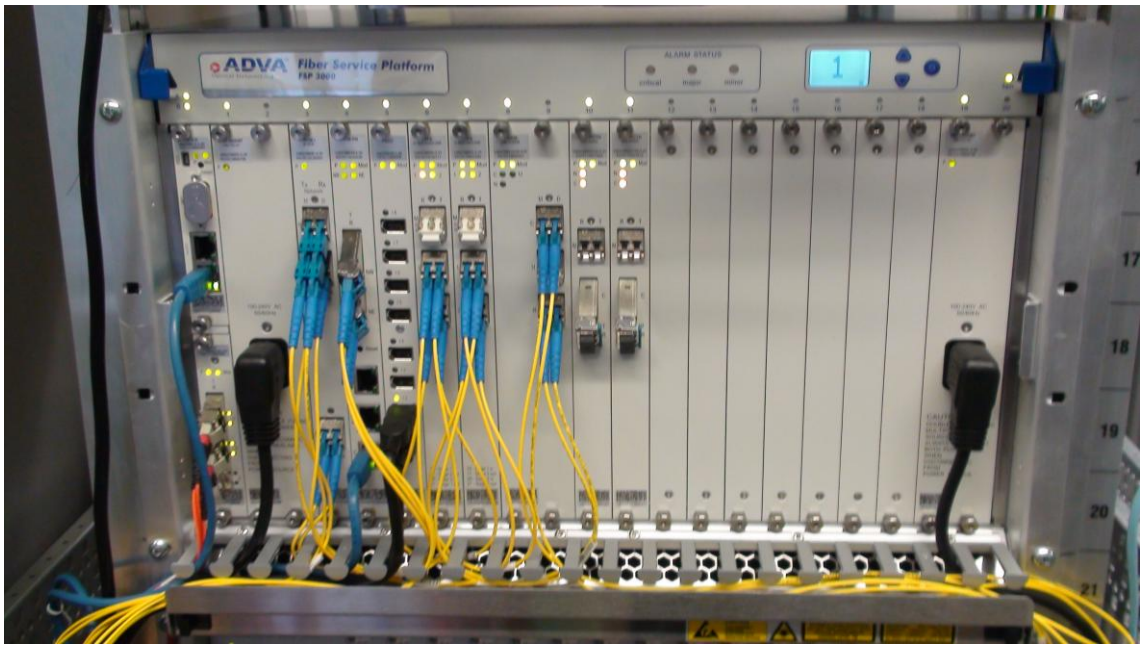

Figura 54 Nodo Adva FSP 3000

Como ejemplo de utilidad de la restauración multicapa, sería razonable pensar que si se posee una capa de transporte basada en malla fotónica, ésta permitiría alcanzar desde el acceso la interconexión simplemente haciendo uso de la reconfiguración de los equipos ópticos. En el caso de uso actual, por limitaciones de equipamiento no se puede incluir routers de protección ni más ROADMs pero desde un punto de vista funcional, la demostración no varía puesto que lo que se evalúa es la capacidad de, mediante una entidad adicional (gestor de restauración multicapa) y las capacidades dinámicas de la red, responder frente a un fallo irresoluble por los planos de control separados de ambas capas.

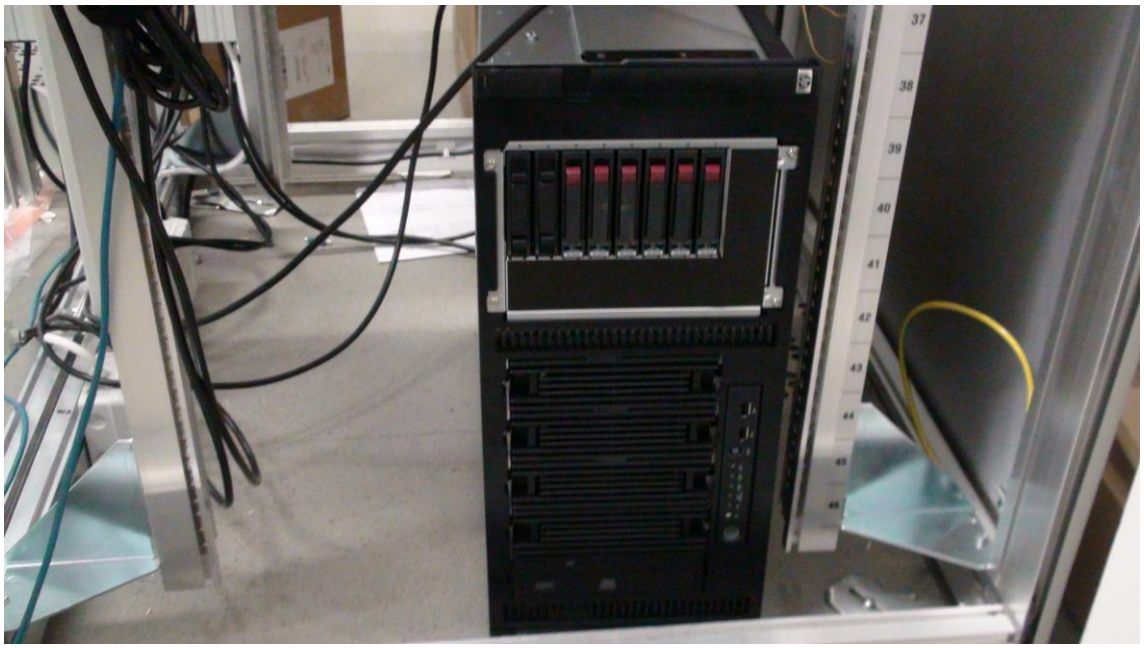

Figura 55 Gestor Multicapa

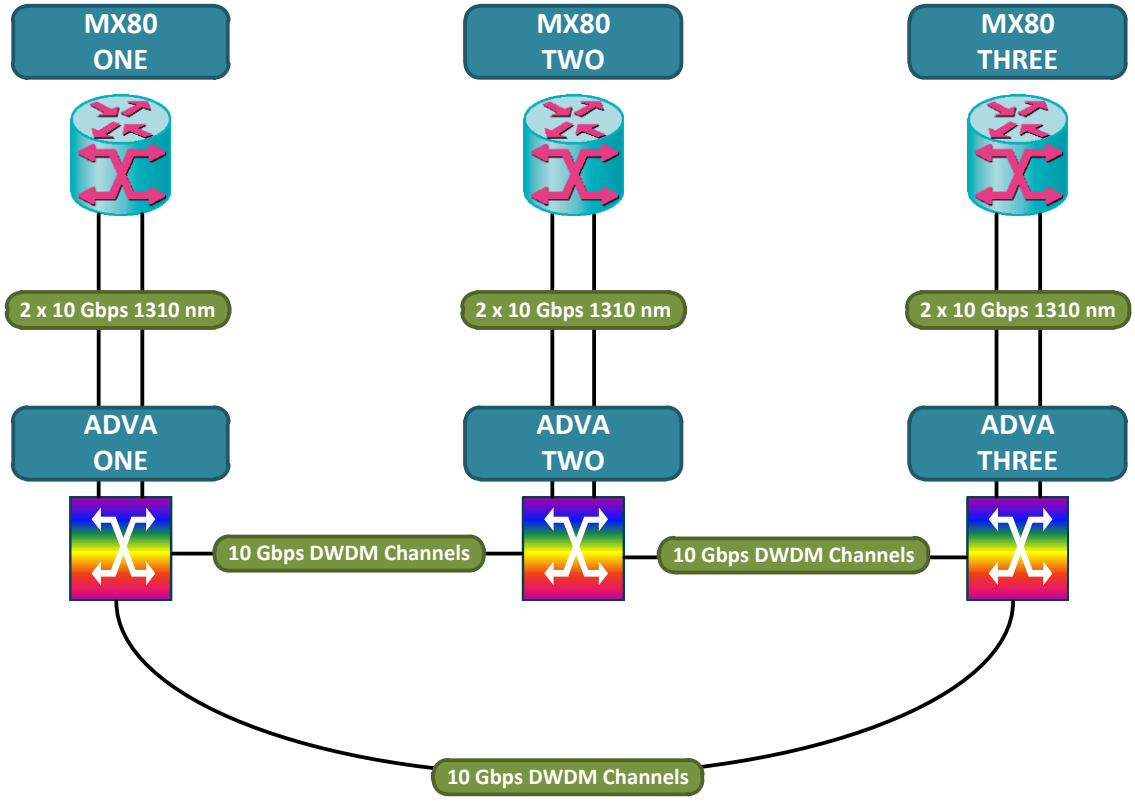

Figura 56 Escenario de red del demostrador

Para permitir el establecimiento de enlaces de un modo dinámico mediante la interfaz UNI, se realiza un plan de direccionamiento en los enlaces entre capas que detallado a continuación:

- Router MX80 ONE a nodo ADVA ONE
  - Router MX80 ONE id: 172.16.100.1
    - Interfaz xe-0/0/0: 180.0.0.2
    - Interfaz xe-0/0/1: 200.0.0.2
  - Nodo ADVA ONE: 10.10.10.1
    - Transpondedor WCC-PCTN-10G Modulo 3: 180.0.0.1
    - Transpondedor WCC-PCTN-10G Modulo 4: 200.0.0.1
- Router MX80 TWO a nodo ADVA TWO
  - Router MX80 TWO id: 172.16.100.2
    - Interfaz xe-0/0/0: 201.0.0.2
    - Interfaz xe-0/0/1: 190.0.0.2
  - Nodo ADVA TWO: 10.10.10.2
    - Transpondedor WCC-PCTN-10G Modulo 7: 201.0.0.1
    - Transpondedor WCC-PCTN-10G Modulo 8: 190.0.0.1
- Router MX80 THREE a nodo ADVA THREE
  - Router MX80 THREE id: 172.16.100.3
    - Interfaz xe-0/0/0: 191.0.0.2
    - Interfaz xe-0/0/1: 181.0.0.2
  - Nodo ADVA THREE: 10.10.10.3
    - Transpondedor WCC-PCTN-10G Modulo 3: 191.0.0.1
    - Transpondedor WCC-PCTN-10G Modulo 4: 201.0.0.1

Utilizando la secuencia de direcciones IP adecuada, los routers IP/MPLS pueden solicitar la creación de un enlace a través de la capa de transporte hacia otro router

IP/MPLS eligiendo las interfaces de fuente y destino. En este escenario, los enlaces establecidos inicialmente se crearán utilizando los siguientes EROs:

- Router ONE a Router TWO:
  - Fuente 172.16.100.1
  - Destino 172.16.1.100.2
  - ERO:
    - 200.0.0.2
    - 200.0.0.1
    - 201.0.0.1
    - 201.0.0.2
- Router TWO a Router THREE:
  - Fuente 172.16.100.2
  - Destino 172.16.100.3
  - ERO
    - 190.0.0.2
    - 190.0.0.1
    - 191.0.0.1
    - 191.0.0.2

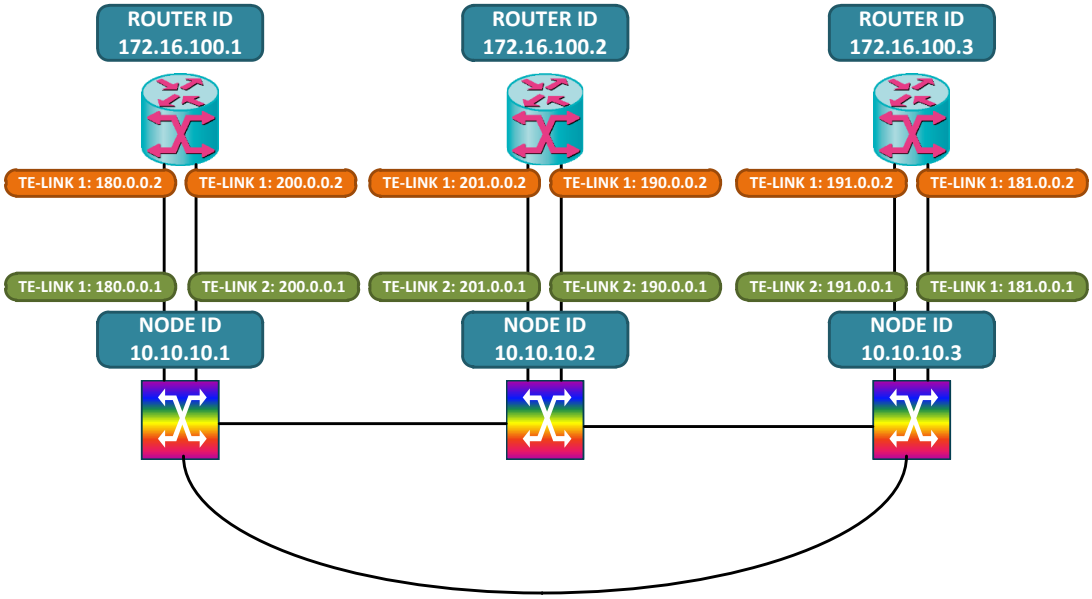

Figura 57 Direccionamiento de plano de control

El fallo que se va a simular para comprobar el funcionamiento de la restauración multicapa se creará en la tarjeta IP/MPLS del router MX80 TWO xe-0/01 que utilizada para conectarse al router MX80 THREE. El fallo ocasionará la pérdida del tráfico entre el router MX80 ONE y el router MX80 THREE que necesite atravesar el router intermedio. El camino nuevo enlace a establecer para recuperar el tráfico entre el router ONE y el router THREE se realizará utilizando las tarjetas libres en ambos routers y utilizarán la siguiente configuración del mensaje RSVP para realizar la reserva de recursos:

- Router ONE a Router THREE:
  - Fuente 172.16.100.1
  - Destino 172.16.1.100.2
  - ERO:

- 180.0.0.2
- 180.0.0.1
- 181.0.0.1
- 181.0.0.2

Además, es necesario un direccionamiento a nivel IP/MPLS que permita el tránsito de paquetes a nivel IP a través de la red. Dicho direccionamiento se muestra en la Figura 58.

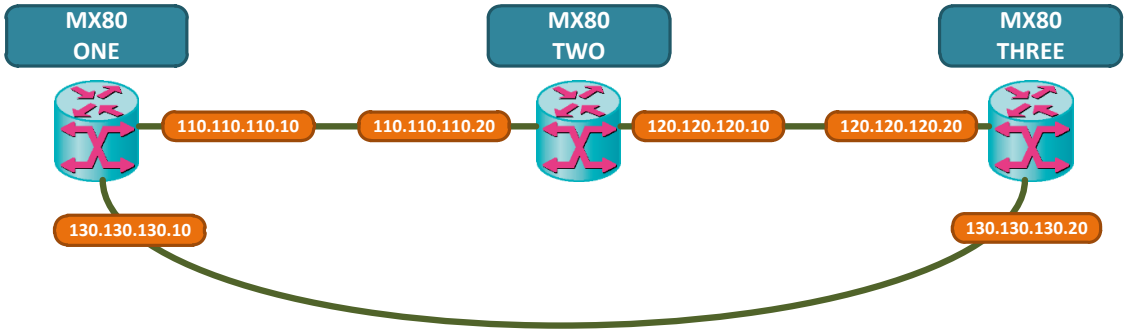

Figura 58 Direccionamiento a nivel IP/MPLS

Se planifica el enlace que se creará para la restauración multicapa que unirá el router ONE con el router THREE con direccionamiento 130.130.130.10 y 130.130.130.20 respectivamente. Con objetivo de hacer pruebas con tráfico elevado, se incluye un generador a 10 Gbps que inyecte tráfico en el router ONE a través de un enlace con direccionamiento 160.160.160.10 que tendrá como destino un interfaz en el router THREE con dirección 150.150.150.10. Para que el tráfico pueda alcanzar su destino es necesario definir las siguientes rutas en los equipos:

Equipo	Destino	Siguiente Salto
Router ONE	150.150.150.10/32	110.110.110.20
Router TWO	150.150.150.10/32	120.120.120.20
Router TWO	160.160.160.10/32	110.110.110.10
Router THREE	160.160.160.10/32	120.120.120.10

Tabla 8 Tabla de rutas en estado inicial del demostrador

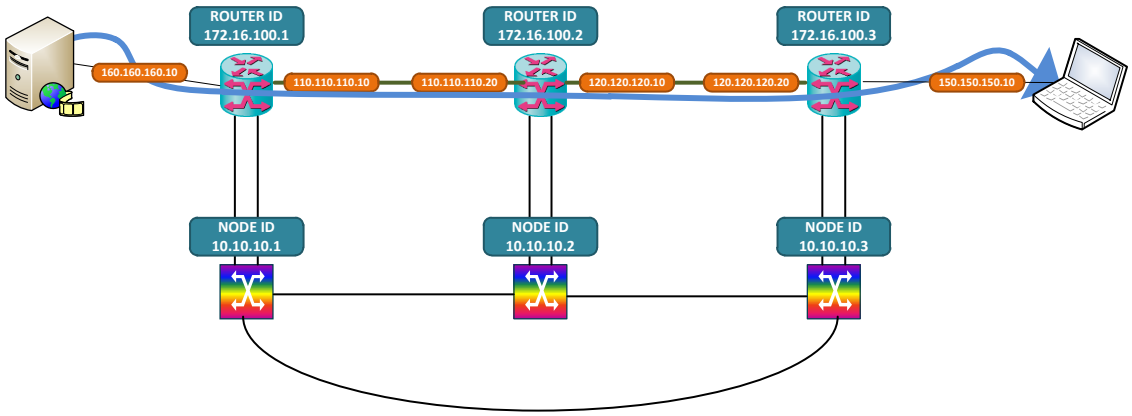

Figura 59 Direccionamiento estado inicial del demostrador

Evento de fallo

Para monitorizar el estado de los enlaces se opta por el uso de traps SNMP que sean enviados al gestor de restauración multicapa. En caso de cambio en el estado administrativo o físico de una interfaz, el router procede a enviar un mensaje en referencia a la variable "*ifOperStatus*" con OID .1.3.6.1.31.2.2.1.8 y valores posibles:

- up(1)
- down(2)
- testing(3)

En el caso de recibir un valor *down(2)* se iniciaría el proceso de restauración multicapa. Para simular un fallo en el equipamiento se cambia el estado de la interfaz xe-0/0/1 en el router TWO mediante utilizando la siguiente secuencia de comandos:

```
edit
set interfaces xe-0/0/1 disable
commit
```

Tras la detección del fallo se inicia el proceso de restauración dividido en dos fases, por un lado uso del UNI para la creación del enlace directo entre el router ONE y el router THREE y por otro el cambio de ruta para que el tráfico alcance el destino. En caso de haber incluido OSPF como protocolo de encaminamiento en la capa IP/MPLS no sería necesario el cambio de ruta sino activar el protocolo en la interfaz del enlace directo. En el caso del establecimiento del enlace mediante UNI sólo es necesario configurar el LSP en uno de los routers ya que por definición en GMPLS los LSPs son bidireccionales.

Los comandos que transmitirá el gestor multicapa a través de la sesión remota por el CLI son para el router ONE:

```
// Creación del LSP en el router ONE
edit
// Definición del ERO
set protocols mpls path router_ONE_to_router_THREE 180.180.180.2
set protocols mpls path router_ONE_to_router_THREE 180.180.180.1
set protocols mpls path router_ONE_to_router_THREE 181.181.181.1
set protocols mpls path router_ONE_to_router_THREE 181.181.181.2
// Definición de parámetros del LSP
set protocols mpls label-switched-path ONE_THREE from 172.16.100.1 to 172.16.100.3
set protocols mpls label-switched-path ONE_THREE primary router_ONE_to_router_THREE
```

```
set protocols mpls label-switched-path ONE_THREE no-cspf
set protocols mpls label-switched-path ONE_THREE lsp-atributes signal-bandwidth 10gigether switching-type lambda
// Definición de nueva ruta
set routing-options static route 150.150.150.10/32 next-hop 130.130.130.20
// Eliminación de la ruta anterior
delete routing-options static route 150.150.150.10/32 next-hop 110.110.110.20
commit
```

Los comandos necesarios en el router THREE son los siguientes:

```
// Definición de nueva ruta
set routing-options static route 160.160.160.10/32 next-hop 130.130.130.10
// Eliminación de la ruta anterior
delete routing-options static route 160.160.160.10/32 next-hop 110.110.110.10
commit
```

La situación a la que dará lugar los cambios de configuración será la mostrada en la siguiente figura:

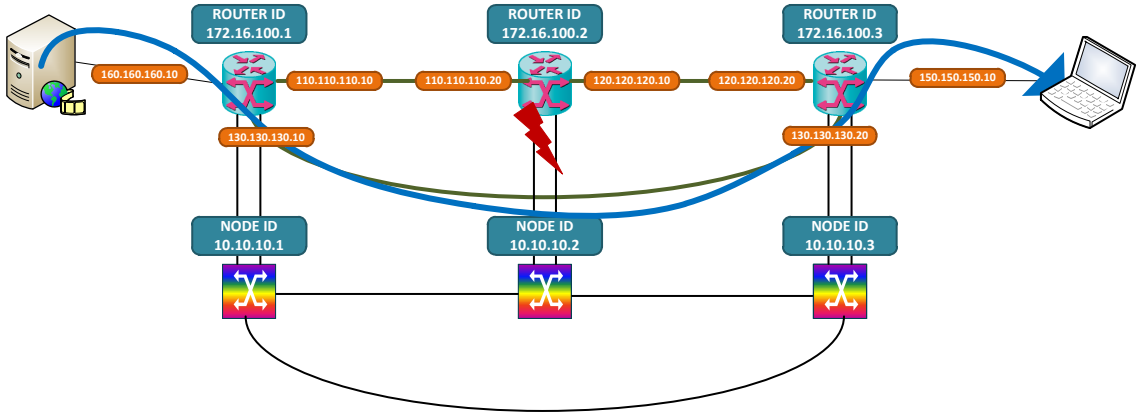

Figura 60 Restauración multicapa tras el fallo

Para mostrar las consecuencias de los cambios de estado en el caso de uso se ha capturado un envío continuo de paquetes ICMP (*Internet Control Message Protocol*, Protocolo de control de mensajes de internet) con la herramienta ping hasta la dirección IP del destino (150.150.150.10) y se ha comprobado la afectación sobre el tráfico del fallo así como el tiempo que tarda el gestor de restauración multicapa en recuperar la conexión. Para controlar que la ruta utilizada para alcanzar el destino cambia, se ha utilizado la herramienta traceroute con misma dirección de destino y con ejecución periódica. Esto se refleja en la Figura 61 con una pérdida en la secuencia de paquetes de 26 así como el cambio de ruta en la misma.

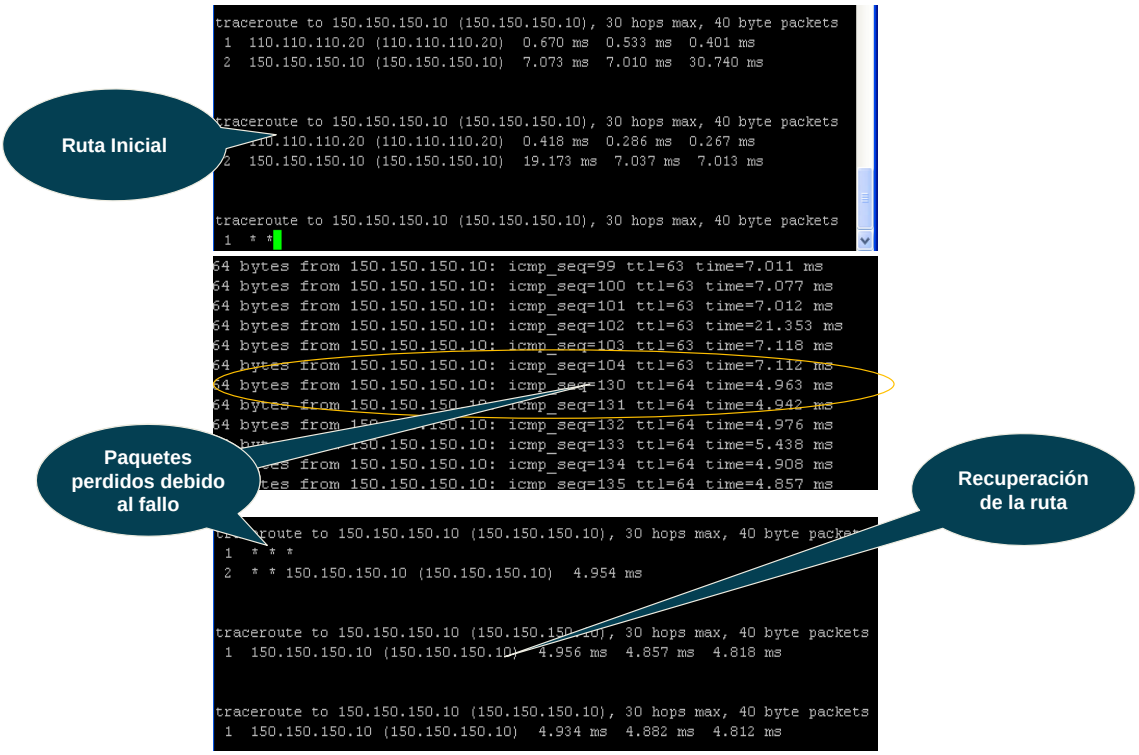

Figura 61 Comprobación del funcionamiento del demostrador

La Figura 62 muestra el intercambio de mensajes, la Figura 60 presenta el mensaje RSVP Path y la Figura 61 el mensaje RSVP Resv confirmando la reserva de recursos. Como se puede observar el tiempo de establecimiento del camino es de 49 segundos.

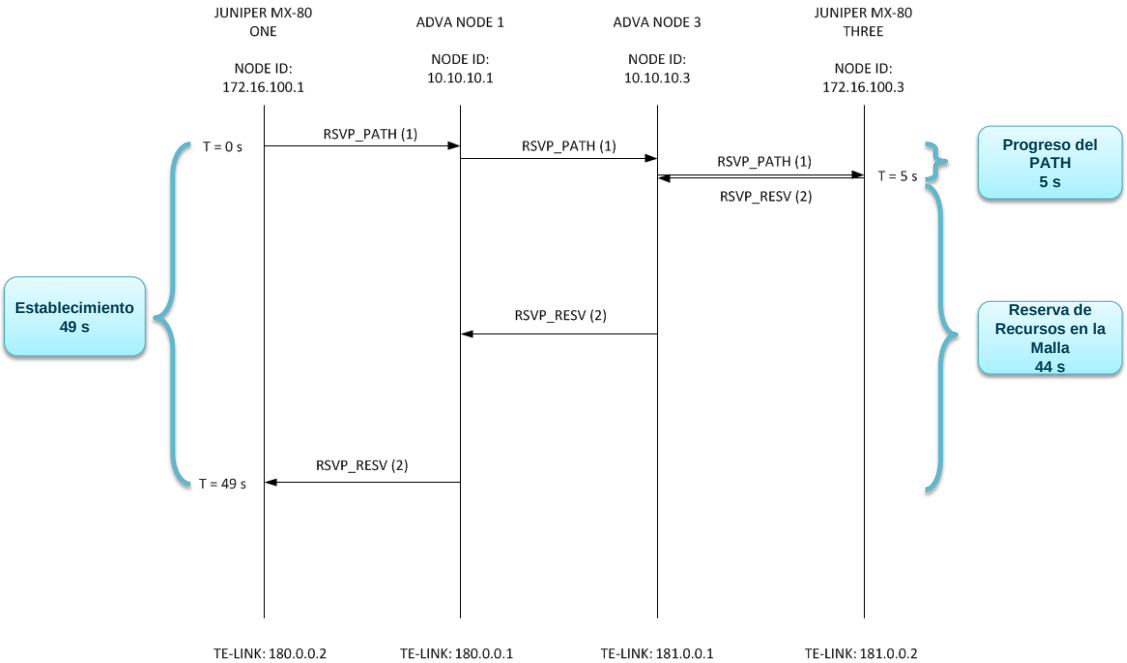

Figura 62 Procedimiento RSVP para el establecimiento del enlace

Los campos más importantes de los mensajes RSVP son los siguientes:

- PATH:
  - Session: Dirección de destino del LSP reservado: **172.16.100.3**. Identificador del LSP:
  - ERO: **180.0.0.1 – 181.0.0.1 – 181.0.0.2** (Como se puede comprobar no se muestra el 180.0.0.2. Esto es debido a que es un TE-Link local al router y cuando el paquete sale de la interfaz no es necesario incluirlo. Por el contrario, en el campo Hop si se ha incluido como parte del camino recorrido).
  - Label Request: Se incluye el tipo de camino solicitado: **Lambda Switching Capable**.
  - Sender Template: Refleja quién es la fuente de la solicitud de recursos, en este caso es **172.16.100.1** como era de esperar.

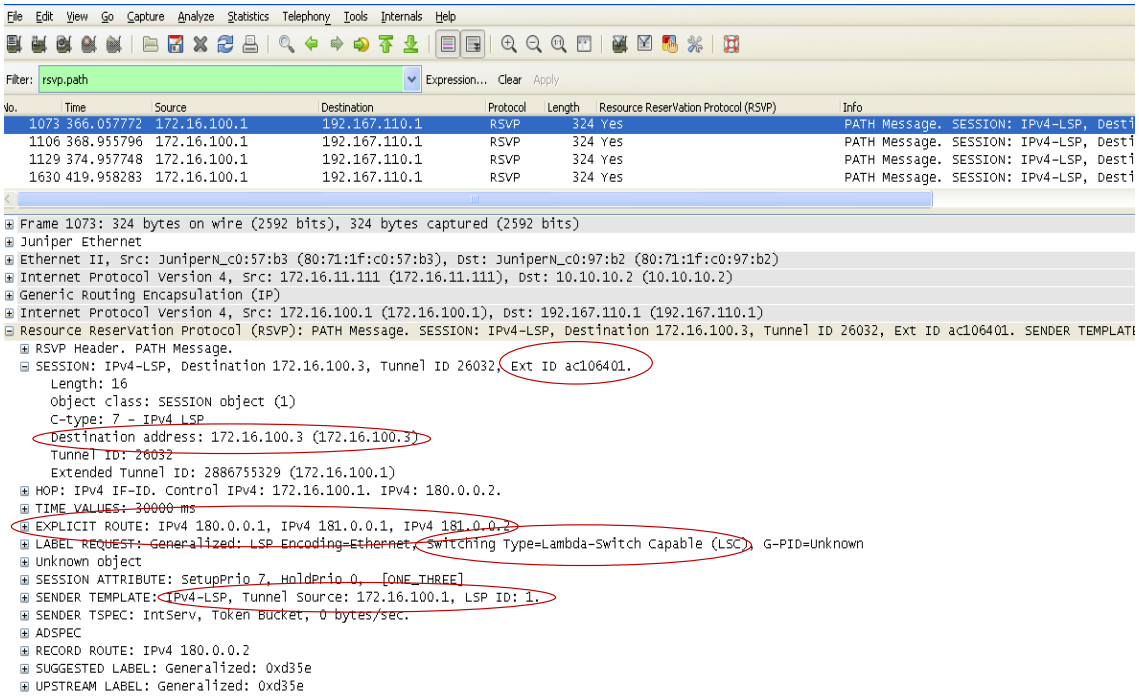

Figura 63 Mensaje RSVP Path

- RESV:
  - Session: Dirección de destino del LSP reservado: **172.16.100.3.** Identificador del LSP: **ac106401.**
  - FilterSpec: Refleja quién es la fuente de la solicitud del LSP: **172.16.100.1.**

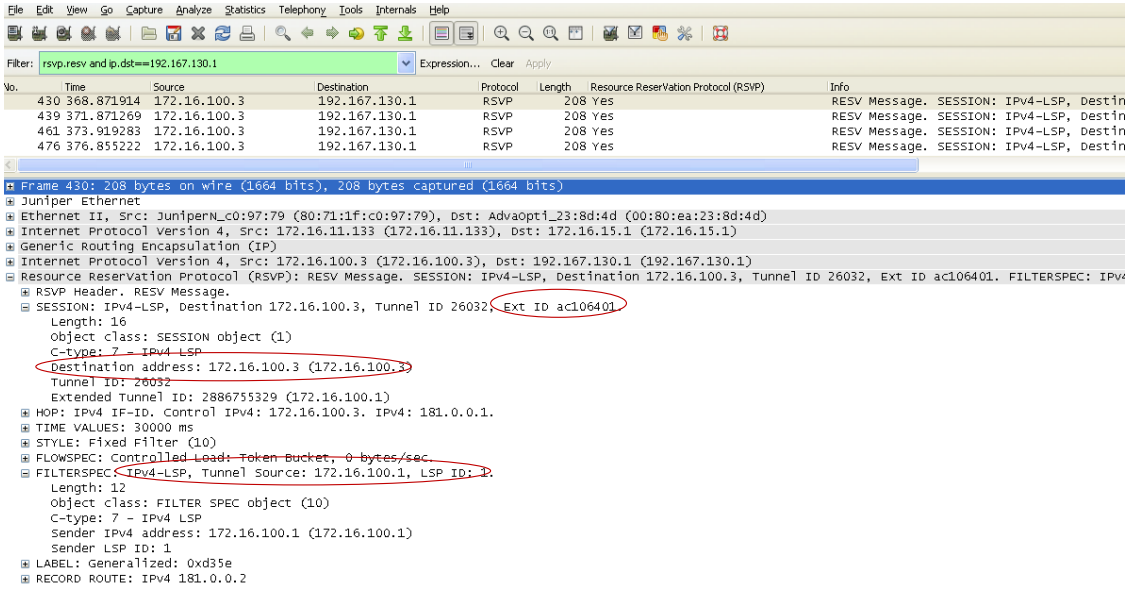

Figura 64 Mensaje RSVP Resv

5 Conclusiones

En el inicio de este trabajo se partía de una situación en la red de los operadores en la que las capas de red en el núcleo (IP/MPLS y transporte óptico) se encontraban separadas lo que suponía un desafío en términos de operación y limitaciones a la hora de responder ante fallos en la red. Mediante el estudio de los protocolos de red utilizados actualmente así como propuestas nuevas, se presenta la posibilidad de operar de un modo conjunto las capas de red y por lo tanto habilitar la restauración multicapa como mecanismo de supervivencia en la red de los operadores.

Tras el estudio de la restauración multicapa, se puede concluir que puede ser beneficiosa en términos económicos para el operador llegando a conseguir ahorros cercanos al 37.5% en equipamiento o una reducción del tiempo necesario de reparación en el equipamiento IP/MPLS de tránsito en 21 veces el tiempo necesario en escenarios de protección 1+1 para garantizar la misma disponibilidad.

Desde el punto de vista de la viabilidad técnica, se presentan múltiples desafíos para que los protocolos de plano de control en las redes actuales puedan desarrollarla de forma nativa. La industria debe hacer un esfuerzo en impulsar el desarrollo del plano de control para el caso de redes multicapa que permita hacer frente a los casos de fallos que involucren a varias capas. Pese a la falta de un marco multicapa que resuelva este problema, se ha demostrado que se puede desarrollar una entidad externa que mediante el uso de protocolos de configuración y monitorización así como tomando ayuda de los protocolos de plano de control existentes, se puede realizar la restauración multicapa con éxito en entornos con equipamiento real.

Como próximos pasos en el desarrollo de la restauración multicapa, se observa la necesidad previamente mencionada de un plano de control capaz de gestionar la restauración multicapa por si misma con elementos basados en los estándares de la industria. Además, hay múltiples puntos que podrían ampliar el estudio actual y darle una aplicación en otros escenarios de red de operadores distintos a los jerárquicos estudiados en este documento. Los puntos propuestos serían los siguientes:

- Inclusión de escenarios no jerárquicos con redes más horizontales y destinos menos predecibles.
- Añadir patrones de tráfico en escenarios jerárquicos con diferencias entre el tráfico de regiones.
- Incluir diferentes tipos de tráfico sujetos a diferentes SLAs y estudiar la influencia en los mecanismos de supervivencia para cumplir con ellos.
- Profundizar en los modelos de costes, particularmente en los costes de operación para intentar traducir la extensión de MTTR a euros así como incluir las penalizaciones económicas por incumplimiento de SLAs en el modelo.

6 Presupuesto

Duración del proyecto: 11 meses

Presupuesto total del proyecto: 48118 Euros

Desglose presupuestario

Costes de Personal

Apellidos y Nombre	Categoría	Dedicación (Hombres mes)	Coste del hombre mes	Coste Total (Euro)
Fernando Muñoz del Nuevo	Ingeniero	11	2694.39	29638.29
			Total	29638.29

Tabla 9 Costes Personal

Costes de Equipos

Descripción	Coste (Euro)	% Uso dedicado	Dedicación (Meses)	Periodo de depreciación	Coste Imputable
3 Chasis Juniper Mx 80	60000	100	2	60	20000
6 XFP 10G Juniper	1800	100	2	60	60
3 Tarjetas de puertos 10G	12000	100	2	60	400
3 ADVA FSP 3000 con 6 TX 10 G	240000	100	2	60	8000
				Total	10460

Tabla 10 Costes Equipos

No hay costes de subcontratación de tareas ni otros costes directos del proyecto.

Resumen de costes

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	29.638
Amortización	10.460
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	8.020
Total	48.118

7 Acrónimos

ADSL	Asymmetric Digital Subscriber Line
BLSR	Bidirectional Line Switched Rings
CLI	Command Line Interface
DSLAM	Digital Subscriber Line Access Multiplexer
ERO	Explicit Route Object
FR	Fast Re-route
FTP	File Transfer Protocol
GMPLS	Generalized Multi-Protocol Label Switching
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocol
LMP	Link Management Protocol
LSC	Lambda Switching Capable
LSP	Label Switched Path
MAN	Metropolitan Area Network
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NMS	Network Management System
NRSC	Network Reliability Steering Committee
OAM	Operation Administration and Management
OSPF	Open Shortest Path First
OSPF-TE	OSPF Traffic Engineering
PSC	Packet Switching Capable
ROADM	Reconfigurable Optical Add Drop Multiplexer
RSVP	ReSerVation Protocol
RSVP-TE	RSVP Traffic Engineering
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement

SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SRLG	Shared Risk Link Group
TED	Traffic Engineering Database
UDP	User Datagram Protocol
UNI	User to Network Interface
VoIP	Voice over IP
WDM	Wavelenght Division Multiplexing

8 Bibliografía

[1] Juan Pedro Fernández-Palacios. (Julio 2011) Blog Empleados Telefónica I+D. [Online]. http://www.lacofa.es/index.php/general/soluciones-de-red-multicapa-ipmalla-fotonica-para-un-nucleo-de-red-eficiente-y-escalable

[2] Rajiv Ramaswami, Kumar N. Sivarajan, y Galen Hajime Sasaki, *Optical Networks: A Practical Perspective*, Morgan Kaufmann, 2009.

[3] Admela Jukan et al., "D 2.1 Definition of requirements and use cases", European Project ONE, Deliverable 2011.

[4] J. Moy. Ascend Communications, "RFC2328, OSPF Version 2", Abril 1998.

[5] Oran, D. Digital Equipment Corp, "RFC1142, OSI IS-IS Intra-domain Routing Protocol", Febrero 1990.

[6] L. Anderson, I. Minei, y B. Thomas, "RFC 5036, LDP Specification", October 2007.

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

[8] K. Kompelia y Y. Rekhter, "RFC 4203, OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", Octubre 2005.

[9] Eric D. Osborne y Ajay Simha, "MPLS Forwarding Basics", en *Traffic Engineering With MPLS*., Cisco Press, cap. 2, p. 28, 2003.

[10] Bruce S. Davie y Adrian Farrel, "Overview of the MPLS Data Plane", en *MPLS: Next Steps*., Morgan Kaufmann, cap. 2, 2008.

[11] Ina Minei y Julian Lucek, *MPLS-Enabled Applications*, John Wiley & Sons, Ltd., 2011.

[12] Fundamentos de la Telefonía IP, IPOnline. [Online]. http://www.iponline.com.ar/es/telefoniaip.php

[13] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, y G. Swallow, "RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels", Diciembre 2001.

[14] International Telecommunications Union, "Recommendation G.805," 2000-2003.

[15] Adrian Farrel y Igor Bryskin, *GMPLS, Architecture and Applications*, Morgan Kaufman, 2006.

[16] NRSC. (2008) Network Reliability Steering Comimittee Biennial Report. [Online]. http://www.atis.org/NRSC/Docs/ATIS-0100023R1.pdf

[17] Wayne D. Grover. (Febrero 2004) Fiber Cable Failure Impacts, Survivability Principles and Measures of Surviability. [Online]. http://www.informit.com/articles/article.aspx?p=169456

[18] Tom Pisello y Bill Quirk. (March 2004) How to Quantify Downtime. [Online]. http://www.webpronews.com/how-to-quantify-downtime-2004-03

[19] Randolph A. Fisher. (2003) Business Recovery Over Wide Area NetWorks: Are You Ready? [Online]. http://www.wancom.net/business_continuity.htm

[20] Jean-Philippe Vasseur, Mario Pickavet, y Piet Demeester, *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP and MPLS*, Morgan Kaufmann, 2004.

[21] Ed Harrison, Ben Miller, y Adrian Farrel. (October 2001) Protection And Restoration In MPLS Networks. [Online]. http://network-technologies.metaswitch.com/download/mplsprotwp2.pdf

[22] Andrea Fumagalli, Luca Valcarenghi, y Erik Jonsson, "IP Restoration versus WDM Protection: Is there any Optimal Choice", October 2000.

[23] Thomas Theimer. (2009) ECOC 2009 Presentatios. [Online]. http://conference.vde.com/ecoc-2009/programs/documents/ws4_thomas%20theimer.pdf

[24] E. Oki, Tomonori Takeda, J-L Le Roux, A. Farrel, y Fatai Zhang, "IETF Draft: Extensions to the Path Computation Element communication Protocol", Julio 2012.

[25] Wai-Ki Ching, Michael K. Ng, *Markov Chains: Models, Algorithms and Applications*, Springer, 2005.

[26] Guanglei Liu y Chuanyi Ji, "Resilience of All-Optical Network Architectures under In-Band Crosstalk Attacks: A Graphical Model Approach", *IEEE Journal on Selected Areas in Communications*, 2006.

[27] Omnet. OMNeT ++ Network Simulation Framework. [Online]. http://www.omnetpp.org/

[28] Tomohiro Otani, Kenji Kumaki, y Thomas D. Nadeau, "IETF Draft Traffic Engineering Database Management Information Base in support of MPLS-TE/GMPLS", November 2012.

[29] Traffic Engineering: An Overview. [Online]. http://fengnet.com/book/OSPFandISIS/ch11lev1sec2.html

[30] Jürgen Schönwälder. (2008) Internet Management Protocols. [Online]. http://osnove.tel.fer.hr/nastavnici/randic/oum/Seminar0809/Pages%20from%20D1%5B1%5D.3-2.pdf

[31] R. Enns, M. Bjorklund, J. Schoenwaelder, y A. Bierman, "RFC 6241 Network Configuration Protocol (NETCONF)".

[32] M. Bjorklund, "IETF RFC 6020, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", October 2010.

[33] G. Swallow, J. Drake, H. Imshimatsu, y Y. Rekhter, "RFC 4208 Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", October 2005.

[34] K. McCloghrie y M. Rose, "RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II", March 1991.

9 Anexo de código de gestor multicapa

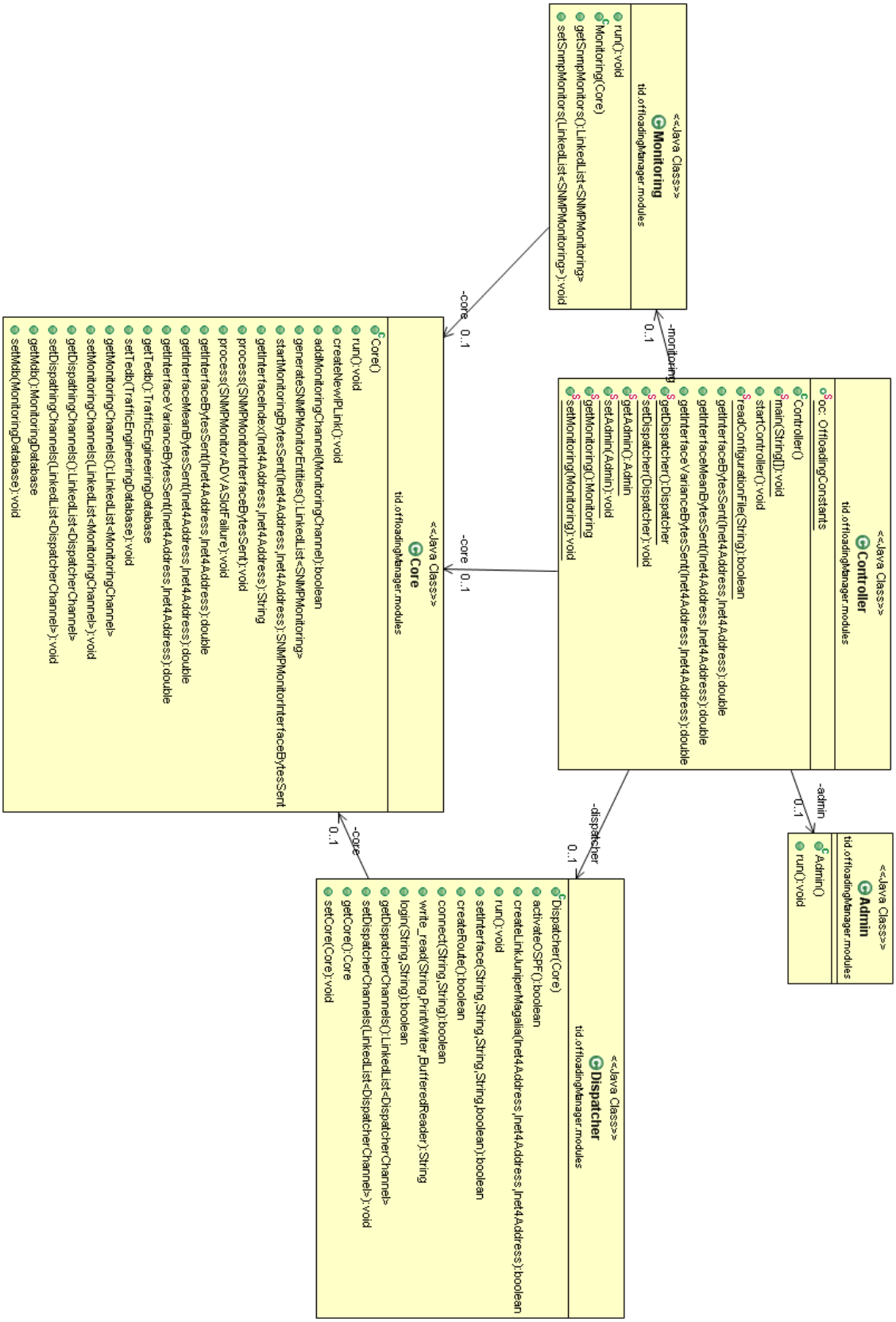

Figura 65 Diagrama UML de los módulos principales

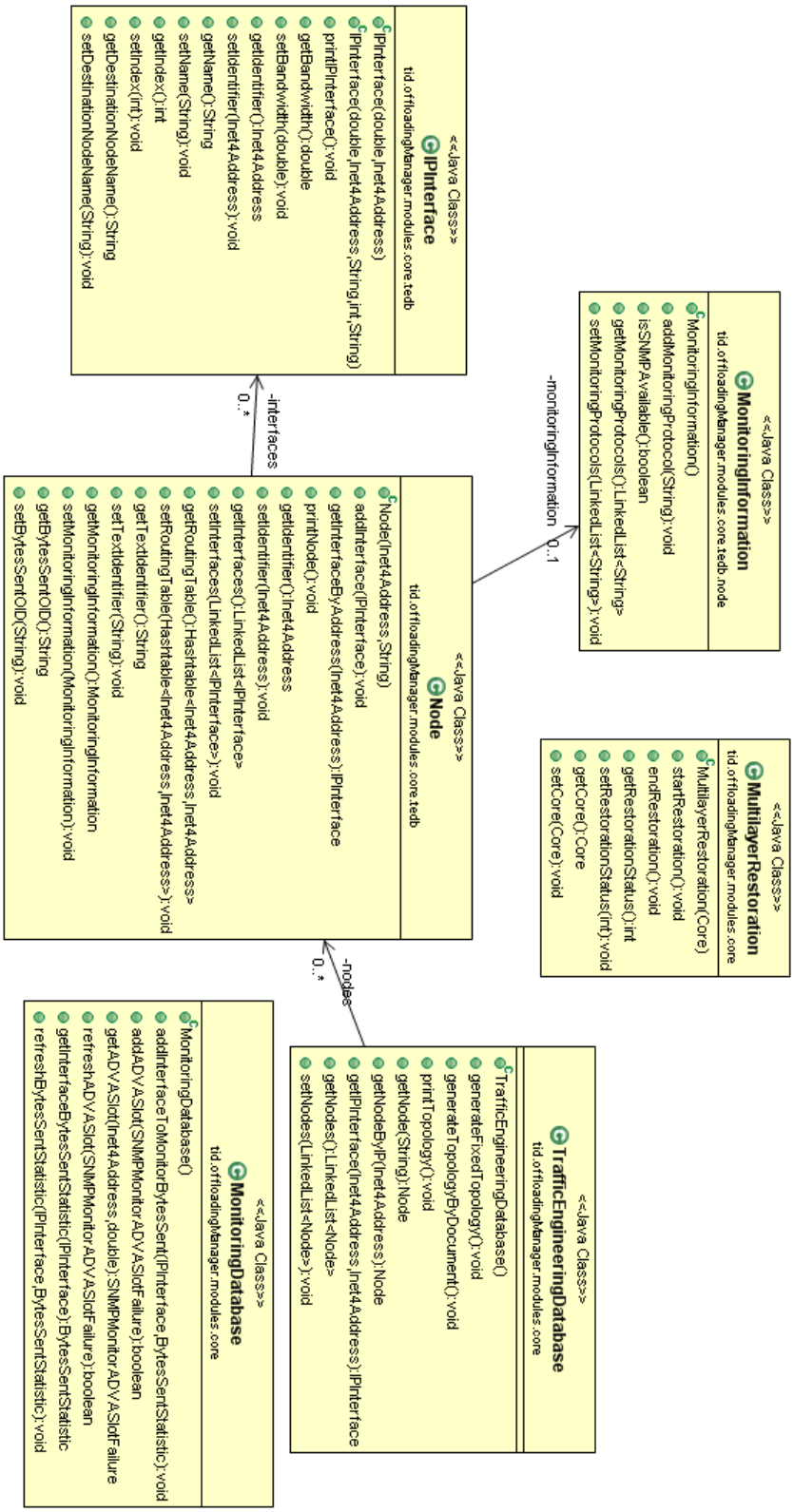

Figura 66 Detalle del módulo Core

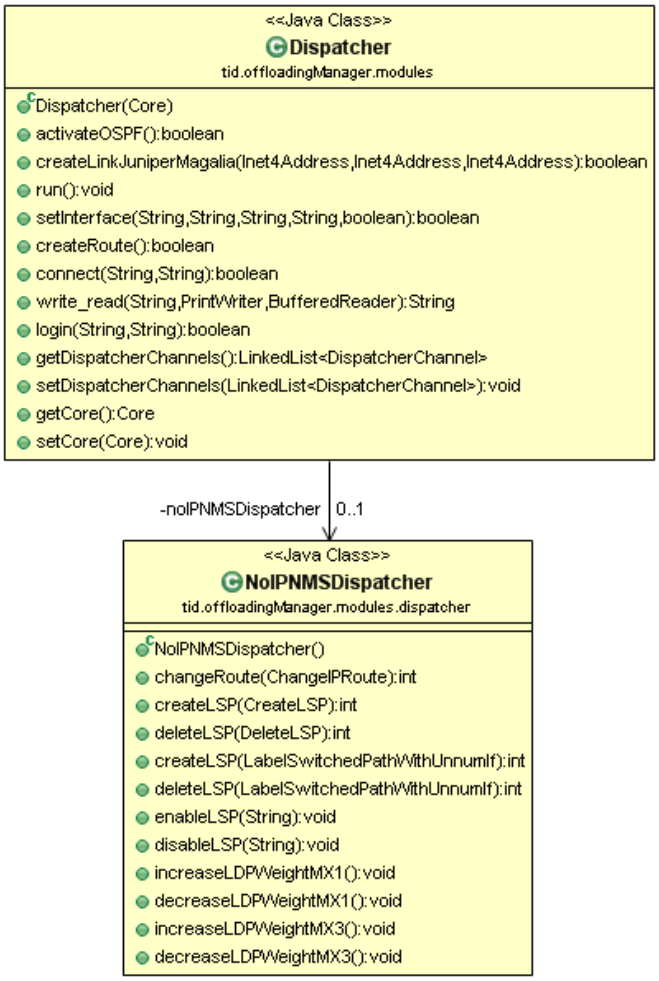

Figura 67 Detalle módulo dispatcher

Figura 68 Detalle módulo monitoring