Arquitectura del Sistema de Gestión del ancho de Banda y Protección (SGBP) para entornos de redes MPLS

Eusebi Calle, Pere Vilà, Jose L Marzo, Santiago Cots

Instituto de Informática y Aplicaciones, Universitat de Girona
Av. Lluís Santaló, s/n, 17071 Girona, Spain
{eusebi, perev, marzo, scots}@eia.udg.es

Resumen. En el presente artículo se describe la arquitectura de un sistema integral de gestión del ancho de banda y protección para entornos de redes MPLS. El sistema está formado por dos módulos, el de encaminamiento y el de gestión de recursos. El módulo de encaminamiento escogerá la mejor ruta de trabajo y las posibles rutas de respaldo, teniendo en cuenta los requerimientos de calidad de servicio y de protección de la petición. El módulo de gestión de recursos se encargará de la gestión de fallos en la red y de la mejora de la utilización de los recursos de la red mediante mecanismos de reasignación dinámica del ancho de banda.

1. Introducción

La evolución de las tecnologías de las comunicaciones hacia redes de servicios integrados conlleva un aumento de complejidad en su gestión. Entendemos por *redes de integración de servicios* aquellas redes más dinámicas orientadas a la conexión con garantías de calidad de servicio, con un crecimiento en nodos, usuarios y sobre todo en tráfico. Los mecanismos existentes contemplan la gestión desde una óptica básicamente aislada en cuanto a asignación de anchos de banda, encaminamiento, establecimiento de circuitos y de rutas de respaldo, etc. Por otro lado, dichas gestiones suelen actuar de forma estática, como procesos activados de forma manual y esporádica.

Así pues, nos encontramos ante un nuevo escenario donde se requieren nuevas estrategias que proporcionen a la red el control y el dinamismo que los nuevos servicios requieren.

En el presente artículo se describe el desarrollo de un módulo de gestión de red orientado al encaminamiento con protección (con rutas de respaldo) y a la gestión de los recursos de la red adaptándolos al estado de ésta y a las necesidades de calidad de servicio (QoS: *quality of service*) del tráfico. MPLS es la tecnología elegida para el desarrollo del sistema.

Este trabajo está parcialmente financiado por la CICYT número TEL-99-0976.

En la sección 2 se describe brevemente la tecnología MPLS y cómo ésta se utiliza en la implementación de mecanismos de "ingeniería del tráfico" [1], [2]. La sección 3 presenta la especificación funcional del sistema. Ésta se divide en tres subsecciones: la descripción de los mecanismos de gestión de ancho de banda, mecanismos de protección MPLS y encaminamiento con calidad de servicio y protección. La sección 4 detalla la arquitectura propuesta del sistema. Por último, se presentan las conclusiones y futuros trabajos.

2. Ingeniería del tráfico en entornos MPLS

En esta sección se describe el marco en el que se desarrolla la arquitectura SGBP. Ésta se basa en redes MPLS. Para ello se describe brevemente la arquitectura MPLS y los métodos de ingeniería del tráfico.

MPLS tiene como principal característica la división de los planos de control y de envío. El mecanismo de control se encarga de dos funciones: la creación de las rutas, que implica la construcción de las tablas de encaminamiento, y la señalización de las rutas.

El módulo de envío se encarga de la conmutación de paquetes mediante el mecanismo de intercambio de etiquetas. Gracias a este intercambio de etiquetas se pueden crear los LSP (*label switching paths*), haciendo un paralelismo con ATM, los VCI.

La distribución de la información entre los diferentes nodos (distribución de las etiquetas) se realiza mediante un algoritmo de señalización. Actualmente existen dos alternativas: variaciones a RSVP (*reservation protocol*) o el LDP (*label distribution protocol*).

La arquitectura MPLS está pensada como protocolo en un entorno de red donde podemos encontrar *routers* IP, conmutadores ATM, etc. Una red MPLS estará compuesta por *routers* MPLS: LSR (*label switch routers*). Éstos se dividen en nodos de entrada (*ingress nodes*), nodos de salida (*egress nodes*) y nodos intermedios (*core routers*). Los primeros y los de salida se encargan de encapsular y desencapsular los paquetes, mientras que los intermedios únicamente realizan la conmutación de etiquetas.

Dos conceptos fundamentales en MPLS lo diferencian de otros protocolos: son la posibilidad de agregar tráfico y la posibilidad de hacer encaminamiento explícito. MPLS clasifica en el nodo de entrada (*ingress node*) el tráfico de modo que le asigna, según el destino y la clase de tráfico, una FEC (*forwarding equivalence class*). Cada flujo de tráfico tendrá asociada una FEC que podrá asignarse a un LSP determinado. Además, tendremos la posibilidad de agregar flujos asignándolos a una FEC determinada.

Por otro lado, podemos hacer un encaminamiento explícito, indicando cuáles son los nodos por los que queremos que pase un LSP. Esto nos permite, a diferencia de otros protocolos de encaminamiento que no ofrecen esta posibilidad (como el encaminamiento en IP), evitar situaciones de congestión. Por ejemplo, si el encaminamiento proporciona una ruta que ya está congestionada, debido a que sólo tiene en cuenta el destino y el número mínimo de saltos. Estas dos herramientas, la agregación de tráfico

y el encaminamiento explícito, hacen de MPLS un protocolo adecuado para gestionar las redes actuales. O dicho de otro modo, para realizar lo que actualmente se conoce como *ingeniería del tráfico* (TE, *traffic engineering*) [1].

Uno de los problemas actuales en redes IP es la falta de "habilidad" para ajustar flujos de tráfico haciendo un uso adecuado del ancho de banda de la red. Tampoco se dispone de mecanismos para diferenciar clases de tráfico. Este problema es el que intenta solucionar la ingeniería del tráfico en entornos MPLS.

Según define el IETF [2], un enlace troncal de tráfico (*traffic trunk*) es un agregado de todo el tráfico entre un *ingress node* y un *egress node*. La idea de la ingeniería del tráfico es cómo se puede realizar el mapeo de *traffic trunks* sobre la red física optimizando el rendimiento (uso de los recursos, balanceo de la carga, etc.). Por lo tanto, la ingeniería de tráfico contempla diferentes tareas: gestión de los recursos, protección y encaminamiento con calidad de servicio.

3. Descripción del sistema

En esta sección se describe cada uno de los elementos necesarios para la construcción del sistema: mecanismos de gestión de recursos, mecanismos de protección y mecanismos de encaminamiento con calidad de servicio y protección.

3.1. Gestión de recursos

MPLS permite establecer LSP y además establecer LSP de respaldo asociados a los de trabajo. El establecimiento de todos estos LSP se realiza usando algoritmos de encaminamiento con calidad de servicio que buscan la ruta óptima, tanto desde el punto de vista de la calidad de servicio requerida como desde el punto de vista del uso de los recursos de la red. A partir de este punto la gestión de recursos básicamente se encarga de ajustar los LSP establecidos en la red adaptándolos al uso real que se esté haciendo de ellos, de forma parecida a la realizada en ATM [3].

Para conseguir esta adaptación al tráfico real de la red, los mecanismos de ingeniería del tráfico deben realizar tareas de monitorización. Por lo tanto, se puede afirmar que los mecanismos de gestión de recursos están constantemente pendientes del estado real de la red y fuertemente relacionados con el establecimiento de LSP de trabajo y de respaldo con algoritmos de encaminamiento con calidad de servicio. Por este motivo, la gestión de recursos también cubre la detección de las alarmas en el momento en que se produce un fallo en la red y la activación de los LSP de respaldo. Por lo tanto, la gestión de recursos cubre la monitorización del estado real de la red y procede a su adaptación (cambiando los LSP existentes) al tráfico real y a los posibles fallos que puedan surgir (activando los LSP de respaldo necesarios). Una vez establecidos los LSP, éstos tendrán una cierta vida, corta o larga, durante la cual pueden sufrir una serie de problemas. Se puede establecer un LSP con un cierto ancho de banda asignado para una cierta cantidad de tráfico con una cierta calidad de servicio.

Sobre este LSP puede suceder que, al cabo de un cierto tiempo, la demanda de tráfico supere la reserva inicial y se produzca un rechazo de tráfico de entrada. Este rechazo o bloqueo se produce debido a algún tipo mecanismo de control de admisión necesario para garantizar la calidad de servicio de las distintas conexiones existentes, y puede cuantificarse calculando la probabilidad de bloqueo para cada LSP. Otro fenómeno que puede suceder es que, una vez reservada una cierta cantidad de ancho de banda para un cierto LSP, después de cierto tiempo este LSP esté poco utilizado y se estén desperdiciando los recursos de la red, cuando posiblemente otros LSP puedan estar congestionados y rechazando tráfico.

La técnica habitual para adaptar el ancho de banda de los LSP al tráfico real es la reasignación de banda de los mismos, incrementándola o decrementándola según sea el caso. Para poder incrementar la banda de un LSP es necesario que a lo largo del camino que sigue este LSP (los diferentes enlaces físicos que atraviesa) existan los suficientes recursos libres (figura 1 b). Si esto no sucede, existen dos posibles acciones a tener en cuenta. La primera es buscar en qué enlaces físicos no se cumple la condición de que no exista suficiente banda disponible, y posteriormente, en estos enlaces comprobar si existe algún otro LSP infrautilizado y del que se pueda tomar la banda necesaria (figura 1 c). En otras palabras, consiste en traspasar banda de LSP poco usados a un LSP congestionado y que necesita incrementar su banda. La segunda posibilidad, en el caso de que la primera no sea posible, es reencaminar el LSP que necesita mayor ancho de banda a través de otro camino que pueda satisfacer sus necesidades (figura 1 d). También en este caso, si no es posible reencaminar al LSP congestionado, también existe la posibilidad de reencaminar uno o varios de los demás LSP con los que comparte los mismos enlaces físicos, con lo cual se liberan recursos y permite incrementar su banda (figura 1 e).

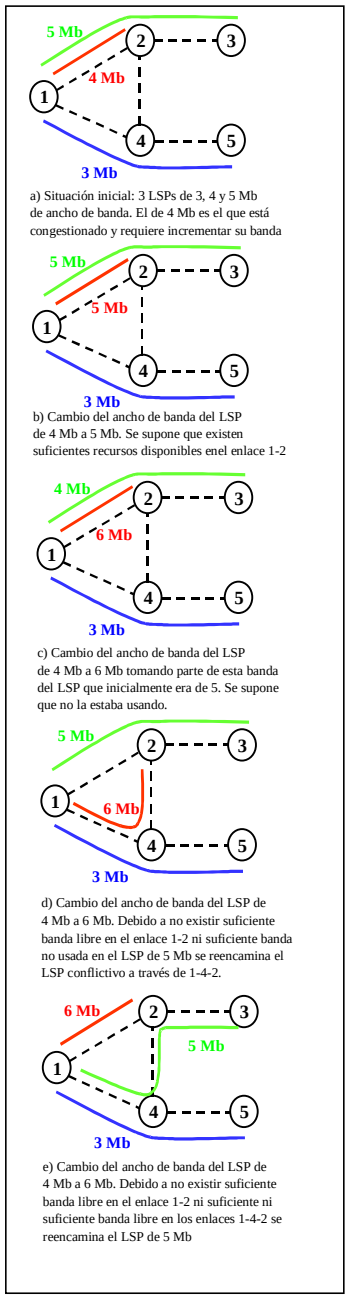

Fig.1. Gestión de banda.

En los casos en los que hay que reencaminar LSP se puede hacer uso de los algoritmos de encaminamiento dinámicos y con calidad de servicio. De ahí que estos mecanismos de gestión de recursos estén estrechamente relacionados

con los mecanismos de establecimiento de LSP de trabajo y de respaldo con calidad de servicio, creando un entorno global de ingeniería del tráfico.

Otro aspecto a tener en cuenta es el de qué mecanismos toman la decisión de adaptar la banda de los LSP y realizar las operaciones anteriormente descritas. Existen diferentes ejemplos en la literatura, y dependiendo de dónde se tome la decisión, se puede hablar de mecanismos centralizados o distribuidos. Estos mecanismos, por las tareas que realizan, se situarían dentro del plano de gestión. Tradicionalmente la gestión, en este caso de recursos y de fallos, se ha realizado de forma centralizada, lanzando algoritmos de optimización que, disponiendo de los datos de monitorización de toda la red, calculan la distribución óptima de los LSP. En redes troncales relativamente grandes por las que circula gran cantidad de LSP es muy difícil disponer de todos los datos de monitorización de forma centralizada y calcular la distribución óptima a tiempo antes de que el estado de la red ya haya cambiado. Una de las opciones que aparecen en la literatura reciente es tratar de mantener la distribución de LSP lo más cercana posible a la óptima haciendo pequeños ajustes usando algoritmos distribuidos. La ventaja principal de los algoritmos distribuidos es que disponen de la información de forma local y permanentemente actualizada. Por el contrario, la desventaja está en que no se dispone de una visión global de la red. Por esta razón algunos algoritmos de este tipo se basan en distintas técnicas de inteligencia artificial y/o en distintas heurísticas para intentar realizar las mejores adaptaciones, aunque no se no dispone de una completa información [4], [5], [6] y [7].

Otro tema importante es el de la frecuencia con la que se realizan las adaptaciones de los LSP. Existen mecanismos que las realizan periódicamente, otros que las realizan cada vez que se detecta un problema, etc. La frecuencia máxima sería cada vez que se realiza una conexión nueva o finaliza una conexión antigua. Por el contrario, una frecuencia mínima sería no cambiar nunca los LSP. Con respecto a los mecanismos periódicos, depende del periodo y de cómo se calcule la nueva distribución de LSP, pero en general pueden calcular la nueva distribución cuando no se está produciendo el problema. Una frecuencia excesiva provocaría una gran generación de mensajes de señalización en la red con un efecto contrario al buscado, un empeoramiento del rendimiento de la red. Parece que de nuevo es necesario realizar los cambios en cuanto se detectan los problemas, pero evaluando correctamente si vale la pena o no realizar el cambio en ese momento, por lo que de nuevo se precisa una cierta inteligencia en estos mecanismos.

3.2. Protección en entornos MPLS

Los enlaces físicos o virtuales de una red están expuestos a fallos de conectividad. El objetivo de los mecanismos de protección consiste en minimizar el riesgo de desconexión. Dichos métodos de protección siguen un ciclo, que va desde la detección de un fallo en un camino de datos, hasta que el tráfico puede reestablecerse en dicho camino. Este ciclo involucra a varios componentes: un método de encaminamiento que selecciona caminos de trabajo y de respaldo; un método de reserva de banda en ambos caminos; un método de señalización para configurar (distribuir las etiquetas) en los caminos de trabajo y respaldo; un mecanismo de detección y otro de notificación de

fallos, necesarios para indicar al nodo responsable de tomar las acciones de respuesta al fallo que se ha producido; y, finalmente, un mecanismo para desviar el tráfico desde el camino de trabajo (en el que se ha producido el fallo) hasta el camino de respaldo (acción de *switchover*). Opcionalmente, podemos disponer de un mecanismo de detección de la recuperación del camino original y de los elementos necesarios para volver a restablecer el tráfico.

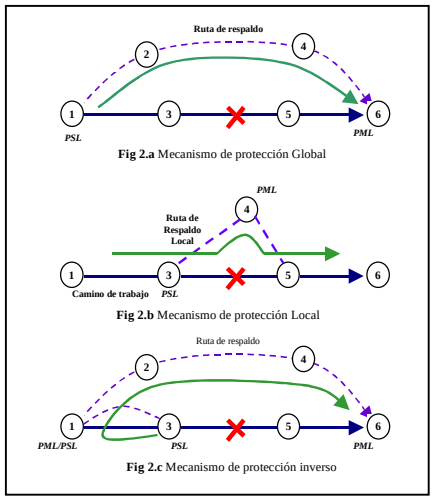

Fig 2.a Mecanismo de protección Global

Fig 2.b Mecanismo de protección Local

Fig 2.c Mecanismo de protección inverso

Fig 2: Mecanismos de protección MPLS

Un aspecto que distingue a MPLS de otros mecanismos de protección es que podemos aplicar protección a diferentes niveles [8]. En los dominios MPLS, podemos disponer de mecanismos de protección para todo el camino o bien para un segmento de éste. En la protección a nivel de toda la ruta, la protección siempre vendrá activada por los nodos extremos del LSP, independientemente de dónde se origine el fallo. Estos mecanismos implican propagar la señal de indicación de fallo FIS (*fault indication signal*) hasta el nodo inicial (*ingress node*), lo cual implica un cierto coste en términos de tiempos de restauración.

En la protección por segmentos o protección local, las acciones de recuperación se activan en el propio nodo que detecta el fallo. Este LSR tiene que estar provisto de funcionalidades PSL (*protection source LSR*). En el otro extremo tendremos otro nodo con funcionalidades de PML (*path merge LSR*) que permiten mezclar los tráficos que provienen del propio camino de trabajo y el de respaldo en un solo LSP. Evidentemente, si bien este mecanismo es más rápido que el anterior, no permite proteger todo el camino. Para ello tendríamos que proteger cada uno de los segmentos del camino de trabajo con el coste en recursos que esto implica.

A continuación se realiza un análisis de los tres métodos más comunes de protección MPLS. Las ventajas e inconvenientes de cada uno de ellos serán analizados y comparados entre los diversos esquemas.

Método global. En este modelo, el nodo inicial (*ingress node*) es el responsable de resolver la restauración cuando la FIS llegue [8]. Este método necesita de un camino de respaldo disjunto al camino de trabajo.
Las acciones de protección siempre se activan en el *ingress node*, independientemente de donde ocurra el fallo (a lo largo del camino de trabajo). Esto significa que la información del fallo tiene que propagarse desde el nodo donde éste es detectado hasta el nodo inicial. Si no disponemos de ningún LSP inverso, la detección del fallo se tendrá que realizar con otro tipo de mecanismo como el testeo continuo del camino de trabajo.

Este método tiene la ventaja de tener que configurar una única ruta de respaldo para cada camino de trabajo y, además, es un método centralizado, lo que significa que

un único nodo tiene que ser provisto de las funciones de PSL. Por otro lado, este método presenta un alto coste en términos de tiempos de restauración y pérdida de paquetes.

La figura 2.a nos enseña un escenario simple formado por seis LSR donde el camino de trabajo (LSR1-LSR3-LSR5-LSR6) y el camino de respaldo (LSR1-LSR2-LSR4-LSR6) están preestablecidos. En condiciones normales, el tráfico se transmite desde el *ingress node* LSR1 hasta el *egress node* LSR6 a través del camino de trabajo. Cuando se detecta un fallo (por ejemplo entre el nodo LSR5 y LRR6), el tráfico cambia hacia el camino de respaldo.

Método local. En este método la restauración se activa en el mismo punto donde se produce el fallo; es, por lo tanto, un método transparente al *ingress node*. Su principal ventaja es que ofrece mejores tiempos de restauración que los métodos globales.

En este método la dificultad principal reside en tener que proveer de funcionalidades PSL (y en su caso PML) a todos los nodos (origen-destino) de los segmentos del camino de trabajo que queramos proteger. Además, tendremos que buscar tantos caminos de respaldo como segmentos a proteger (a diferencia del esquema global, donde era necesario un único *backup*). Otra ventaja, sin embargo, es que en este método no se producen pérdidas de paquetes como en el esquema global.

La figura 2.b muestra este caso. El modelo de red es el mismo: tenemos un camino de trabajo formado por los nodos (LSR1-LSR3-LSR5-LSR6) y una ruta de respaldo formada por LSR3-LSR4-LSR6. Cuando se produce un fallo (por ejemplo, entre LSR5-LSR6) se restaura el tráfico en el mismo punto usando la ruta de respaldo local.

Método inverso. La principal idea de este método es devolver el tráfico al nodo inicial (*ingress node*) usando un backup inverso desde el punto donde se produce el fallo. Así se evitan las pérdidas de paquetes [9].

La principal desventaja es que tiene un tiempo de restauración igual al del método global. Además, necesita introducir una nueva ruta de respaldo, con lo cual la utilización de los recursos es aún peor que en el método global. Su única ventaja es que disminuye la pérdida de paquetes y simplifica la notificación del fallo.

La figura 2.c muestra un ejemplo de utilización del método inverso. Se establecen los caminos de trabajo y respaldo igual al modelo global y además añadimos una ruta de respaldo inversa desde LSR5 (LSR5-LSR3-LSR1) hacia el *ingress node*. Cuando se detecta un fallo en el LSP (LSR5-LSR6), el tráfico se desvía hacía el LSR1 (*ingress node*) a través de la ruta de respaldo inversa; una vez allí, el modelo se comporta igual que el global.

3.3. Encaminamiento con calidad de servicio y protección

El establecimiento de una ruta de origen a destino se puede hacer de varias maneras. La opción más sencilla es buscar un camino que sea lo más corto posible (familia SPR, *shortest path routing*). Si suponemos que se mide la distancia en número de saltos, el algoritmo más sencillo sería un MHA (*minimun hop algorithm*). Si consideramos algoritmos de encaminamiento con calidad de servicio, éstos tendrán en cuenta

el hecho de maximizar la utilización de los recursos y la minimización de la carga (en términos de banda) de la red. Aquí entraríamos en otra familia de algoritmos como son los WSP (*widest shortest path*), SWP (*shortest widest path*), DAP (*dynamic alternative path*) ([10], [11]). En estos algoritmos los dos objetivos usados para la elección de la ruta son: el número de saltos (maximizar la utilización de los recursos) y el ancho de banda disponible (balancear la carga de la red). Estos algoritmos consiguen maximizar el número de peticiones de establecimiento de las rutas.

Otra familia de algoritmos de encaminamiento con calidad de servicio, donde sí tenemos como objetivo la maximización de este parámetro, son los de mínima interferencia [12]. Se busca establecer rutas que maximicen el sumatorio de los máximos flujos de la red, con lo cual se permite el poder establecer un mayor número de peticiones.

MIRA es una propuesta de encaminamiento con mínimas interferencias que además tiene en cuenta las características de una red MPLS (a priori podemos conocer el conjunto de *ingress-egress nodes*). Este tipo de algoritmos, a diferencia de los anteriores, realiza una fase de preproceso para crear un grafo con pesos donde posteriormente se aplica un SPR. Si en el MIRA se aplica el preproceso de cálculo de máximos flujos y enlaces críticos (véase [12]), hay otras propuestas donde el preproceso usa otro tipo de cálculo. Por ejemplo, en [13] el preproceso se basa en un cálculo de flujos multiactivos. En otros el cálculo de las rutas se realiza usando métodos de programación entera [14], [15].

En la mayoría de estas propuestas el objetivo principal es establecer un camino de trabajo. Si bien algunas contemplan el establecimiento de caminos de respaldo, suele ser un tratamiento secundario. En algunas propuestas (como en MIRA) el establecimiento de rutas de respaldo se reduce al simple hecho de que el algoritmo permite un mejor aprovechamiento de la banda de la red, lo cual permite hacer reencaminamiento en caso de fallo. Otras propuestas como el PBR (obviamente propuestas anteriores como el WSP) no contemplan ningún esquema de protección. La mayoría, como mucho, dejan los esquemas de protección a tener un camino alternativo entre origen y destino para el caso de fallos.

Una de las pocas propuestas donde se intenta ofrecer un camino de trabajo y un camino de respaldo con ciertas garantías de calidad de servicio (básicamente banda) es [14]. En ella el algoritmo de encaminamiento intenta encaminar un camino de trabajo y una ruta de respaldo (global y disjunto al camino de trabajo); en caso de no ser posible, la petición es rechazada. Aunque este primer esquema sólo tiene en consideración el establecimiento de esquemas globales de protección, esta propuesta viene completada en [15], donde sí se contempla la posibilidad de establecer otros esquemas de protección (en concreto, protección local).

En cualquier caso, pocas propuestas tienen en cuenta el hecho de que no sólo disponemos de un esquema de rutas de respaldo (globales) para ofrecer protección a nuestros caminos de trabajo (o segmentos del camino de trabajo), sino que existen otros esquemas: locales, inversos e híbridos de éstos para ofrecer protección. Además, pocos tienen en cuenta las ventajas y desventajas de utilizar uno u otro esquema.

La aplicación de uno u otro esquema, como hemos visto en la sección anterior, tendrá asociada unos parámetros de velocidad de recuperación, pérdida de paquetes, consumo de recursos, etc. que hay que tener en consideración. En definitiva, la aplica-

ción de uno u otro esquema permite obtener una cierta QoS en el tráfico y optimizar el rendimiento global de la red.

Estas características y cómo y dónde aplicar un esquema u otro de protección son un campo poco explorado en la literatura. En [15] sí se hace mención de las ventajas de aplicar una protección local frente a una global. En [16] se propone el uso de uno o más esquemas en función de las necesidades de protección de nuestra red.

4. Arquitectura del sistema de gestión del ancho de banda y protección

En esta sección describimos la arquitectura básica del módulo a desarrollar y sus principales dependencias funcionales. Sus componentes básicos son: el módulo de encaminamiento y el módulo de gestión de recursos.

A partir de la red física y de la definición de tráfico inicial, el módulo de encaminamiento con calidad de servicio configurará una topología de red lógica inicial. Para ello se deben utilizar algoritmos de encaminamiento que establezcan tanto la ruta de trabajo como la de respaldo; de esto se encargará el módulo de encaminamiento. Ambos caminos deben asegurar la calidad de servicio acordada con los usuarios. La obtención de estos caminos no es simple, y se debe establecer un compromiso entre la eficiencia en la utilización de los recursos de red y la velocidad de respuesta a las peticiones de conexión que impliquen la evaluación de nuevas rutas. Las técnicas conocidas que obtienen los mejores resultados son inapropiadas para respuestas dinámicas o bajo demanda (*on-line*). El establecimiento de ese equilibrio es uno de los objetivos de esta arquitectura. Básicamente este módulo tiene en cuenta tanto los parámetros de calidad de servicio del encaminamiento de caminos de trabajo: maximización de los recursos, optimización del número de peticiones aceptadas y balanceo de la carga, como los de las rutas de respaldo: pérdidas de paquetes, tiempos de respuesta ante fallos y utilización de recursos.

El módulo de reconfiguración actúa simplemente de interfaz entre el módulo de encaminamiento, el de gestión de recursos y la red real. Utilizará los procedimientos estandarizados más adecuados al escenario propuesto. En este sentido, resulta muy interesante la posibilidad de programar este módulo de configuración para que pueda interactuar con los nodos de una red real usando el protocolo de gestión SNMP (*simple network management protocol*). Este protocolo es el estándar de gestión en IP y lo soportan prácticamente todos los *routers* y conmutadores.

El módulo de gestión de recursos observa de manera continua el estado de la red. Éste está compuesto, entre otros, por los siguientes parámetros:

- Ocupación de cada LSP (banda utilizada)
- Retraso
- Pérdidas
- Probabilidad de bloqueo ante la petición de nuevas conexiones
- Caídas de enlaces y nodos

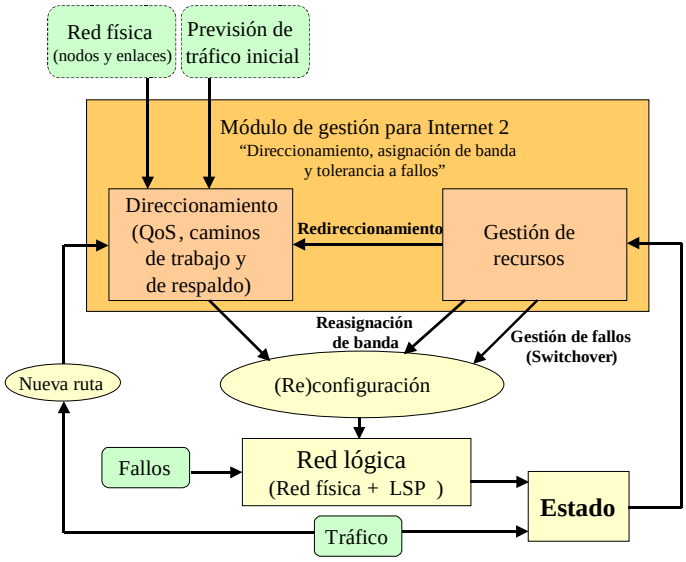

Fig 3. Arquitectura del SGBP.

En función del estado de la red, el módulo de gestión de recursos puede "decidir" acciones de reconfiguración de la red que podemos resumir en las tres siguientes:

- Reasignación de banda. A partir de un análisis del estado de la red, se decide que la acción a tomar es la de reasignar banda (o bien tomándola del conjunto de banda residual disponible o bien tomándola de caminos donde no se utiliza exhaustivamente, *preemption*). La acción se lleva a cabo reconfigurando la red de forma directa (como se indica en la figura 3).

- Reencaminamiento. Un problema detectado puede ser de características tales que no tenga solución mediante una reasignación de banda y se debe modificar la topología de la red. En este caso debe intervenir el módulo de encaminamiento. Aquí caben dos estrategias: a) recalcular todas las rutas para obtener una nueva solución al sistema, o b) obtener una solución al problema de forma rápida y con el mínimo de cambios en la topología. Aquí aparece de nuevo el compromiso entre eficiencia en la utilización de recursos y una respuesta más ágil (simple) al problema.

- Gestión de fallos de red (funciones de *switchover*). Esta acción se corresponde con la detección de una caída de un enlace (o nodo). La casuística aquí es muy variada, desde la simple activación de las tablas de encaminamiento hacia los caminos de respaldo previamente establecidos y con banda asignada, pasando por la captura de banda y nuevos encaminamientos si fuera necesario. La característica principal de estas funciones es que deben dar una respuesta rápida. Estos aspectos son objeto de investigación del proyecto, como se detallará.

El módulo de encaminamiento se basa en modelos complejos pero generalmente bien definidos, mientras que para el módulo de gestión de recursos podrán utilizarse diversas técnicas que permitan solucionar la toma de decisiones.

5. Conclusiones y trabajo futuro

En este artículo se ha presentado la arquitectura de una propuesta de un sistema integral de gestión de recursos y protección para redes en entornos MPLS. La novedad en esta arquitectura es la unión de varios mecanismos hasta ahora desarrollados de forma independiente en la mayoría de las arquitecturas actuales. Las ventajas de la integración de estos mecanismos es que permiten, dentro de un mismo sistema, la coexistencia de mecanismos que trabajan a distintas escalas temporales. Por otro lado, esta integración permite, a diferencia de la mayoría de mecanismos actuales, el aprovechar las ventajas que ofrece cada sistema por separado de forma coordinada. Es decir, evita situaciones donde la aplicación de un mecanismo entre en conflicto con el otro.

Actualmente se ha terminado el diseño del sistema y se han implementado algunos de sus módulos [16] y [17]. Como trabajo futuro se plantea el desarrollo y prueba de diversas alternativas a los módulos descritos en la propuesta. Concretamente, se realizarán experimentos con algoritmos de encaminamiento con soporte MPLS, calidad de servicio, bajo demanda (*on-line*) y con soporte de protección. Por otro lado, para el desarrollo del módulo de gestión se evaluarán distintas técnicas de toma de decisiones en entornos de sistemas multiagentes.

Referencias

1. Xipeng Xiao, Alan Hannan, Brook Bailey, Traffic Engineering with MPLS in the Intenet IEEE Networks. March/April 2000
2. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, Requirements for Traffic Engineering Over MPLS Sep 1999 RFC2702
3. V.J. Friesen, J.J. Harms, J.W. Wong, Resource Management with Virtual Paths in ATM networks IEEE Network, vol 10 no 5, September/October 1996
4. Jim Hardwicke, Rob Davison, Software Agents for ATM Performance Management. IEEE NOMS'98 Network Opertaions and Management Symposium, New Orleans (USA), February 1998
5. J. Bigham, L.G. Cuthbert, A.L.G. Hayzelden, Z. Luo, Multi-Agent System for Network Resource Management. International Conference on Intelligence in Services and Networks, IS&N'99, Barcelona (Spain), April 1999
6. Z. Luo, J. Bigham, L.G. Cuthbert, A.L.G. Hayzelden, Traffic Control and Resource Management using a Multi-Agent System. 5th International Conference on Broadband Communications, Hong Kong (China), November 1999
7. Greg Osinaike, Rachel Bourne, Chris Phillips, Agent-Based Dynamic Configuration of Differentiated Traffic using MPLS with CR-LDP Signalling. 17th UK Teletraffic Symposium UKTS 2001, May 16-18, Dublin, Ireland.

8. S. Makam, V. Sharma, K. Owens, C. Huang Protection/Restoration of MPLS Networks (work in progress) Internet Draft draft-makam-mpls-protection, Oct 1999
6. D. Haskin, R. Krishnan. A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute (work in progress) Internet Draft draft-haskin-mpls-fast-reroute, Nov 2000
10. R. Guerin, D. Williams, A. Orda, QoS Routing Mechanisms and OSPF Extensions Proceedings of Globecom 1997.
11. Q. Ma and P. Steenkiste On Path Selection for Traffic with Bandwidth Guarantees, Proceedings of IEEE International Conference of Network Protocols. Oct. 1997
12. M. Kodialam, T.V. Lakshman, Minimum Interference Routing with Applications to MPLS Traffic Engineering, in Proceedings of the conference of Computer Communications (Infocom 2000). Mar.2000
13. S. Subhash,M. Waldvogel ,P. Warkhede .Profile-Based Routing: A New Framework for MPLS Traffic Engineering 2nd International Workshop on Quality of future Internet Services OoSFis'01
14. M Kodialam and T. V. Lakshman, Dynamic routing of bandwidth guaranteed tunnels with restoration. In Proceedings of the Conference on Computer Communications (IEEE Infocom), Mar. 2000.
15. M. Kodialam, T.V. Lakshman, Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information. In Proceedings of the conference of Computer Communications (Infocom 2001)
16. E. Calle, T. Jové, P. Vilà, J.L. Marzo. A dynamic multilevel MPLS protection domain DCRN'2001. Third International Workshop on Design of Reliable Communication Networks. 7-10 October 2001, Budapest, Hungary
17. P. Vilà, J.L. Marzo, E. Calle. "Dynamic Bandwidth Management as part of an Integrated Network Management System based on Distributed Agents" to appear in proceedings of IEEE Global Communications Conference (GLOBECOM 2002), Taipei (Taiwan), November 17-21, 2002