Encaminamiento con calidad de servicio y protección en redes GMPLS sobre WDM

Quality of Service Routing and Protection in GMPLS over WDM Networks

E. Calle, J. L. Marzo, A. Urra, P. Vilà y S. Cots

Resumen

El incremento de tráfico en Internet, junto con la creciente demanda de servicios críticos y las necesidades específicas de calidad de servicio, hace crucial el desarrollar nuevas técnicas de ingeniería de tráfico para ajustar las necesidades a los recursos de red disponibles. En este escenario hay varios aspectos clave, entre ellos el encaminamiento con calidad de servicio y el ofrecer fiabilidad al sistema mediante técnicas de protección.

Este artículo quiere reflejar parte de la investigación que se está llevando a cabo en el grupo de comunicaciones y sistemas distribuidos de la Universidad de Girona. El artículo se centra en la propuesta de algoritmos de encaminamiento con calidad de servicio y protección en redes basadas en *Generalized Multiprotocol Label Switching* (GMPLS).

Palabras clave: Redes GMPLS, WDM, calidad de servicio.

Summary

The traffic increase in the Internet, along with the increasing demand of critical services and the specific Quality of Service (QoS) requests, makes critical the development of new traffic engineering techniques in order to adjust the demand to the available network resources. In this scenario, there are several crucial aspects, among them the QoS routing and the use of protection mechanisms due to the need of reliability.

This paper aim is to introduce the research that is going on in the Broadband Communications and Distributed Systems group in the University of Girona. It is focussed on routing algorithms with QoS and protection capabilities in Generalised Multiprotocol Label Switching (GMPLS) networks.

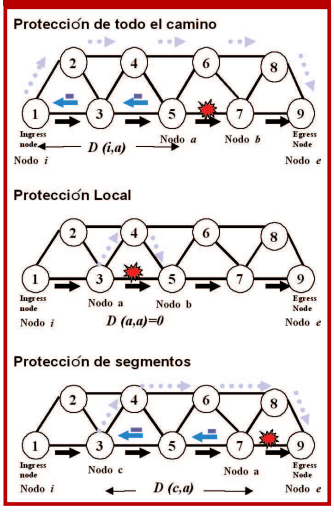
Keywords: GMPLS Networks, WDM, quality of service.

Las redes actuales transportan gran cantidad de información y cuando se produce un fallo se produce una pérdida de paquetes y una degradación de la calidad de servicio

1.- Protección mediante segmentos

Las redes actuales transportan gran cantidad de información y cuando se produce un fallo se produce una pérdida de paquetes y una degradación de la calidad de servicio requerida por el tráfico afectado. Para disminuir estos efectos existen diferentes técnicas para lograr la restauración del tráfico afectado.

FIG 1: PROTECCION CON SEGMENTOS



Hay diferentes elementos a considerar en la restauración. En caso de fallo en la red (supongámoslo en un enlace) el nodo adyacente al que ha fallado será el que lo detecte. A partir de aquí se requiere una notificación de este fallo a la entidad (nodo) responsable de su restauración. En este caso entendemos por restauración la fase que va desde la activación del backup hasta el envío de información por un nuevo camino. Este proceso puede ser más complejo si implicamos la restauración del camino de trabajo inicial o el cálculo del backup una vez detectado el fallo (no preestablecido). Durante la fase de notificación se producirá una pérdida de paquetes que se puede minimizar recortando la distancia entre el nodo de detección del fallo y el responsable de enviar el tráfico por el camino alternativo. El caso óptimo es cuando se utiliza protección local (ver Fig.1).

La figura 1 muestra el proceso de utilización de protección de camino. El nodo **a** detecta el fallo en el enlace 5-7 (ya sea

mediante una señal de alarma de capas inferiores, como un '*loss of light*', o bien mediante monitorización), entonces envía una señal de notificación al nodo de ingreso (nodo **i**), este nodo una vez le llega la señal de notificación para de enviar paquetes por el camino de trabajo y pasa a utilizar el camino alternativo (1-2-4-6-8-9). La distancia de notificación sería la distancia entre los nodos **i-a** (D(**i**,**a**)). En el caso de protección local esta distancia es cero (D(**a**,**a**)) por lo tanto la notificación no existe y la restauración evita, en gran parte, la pérdida de paquetes. Sin embargo, las técnicas de restauración locales implican un gran consumo de recursos si se quiere proteger todo el camino. Una alternativa que intenta ofrecer un consumo de recursos menor y una restauración rápida es la utilización de segmentos. En este caso minimizamos la distancia de notificación (D(**c**,**a**)). La protección con segmentos sólo será útil en el caso que podamos definir cuáles son las zonas sensibles a fallos o bien las zonas no protegidas a otros niveles (como el óptico). En ambos casos necesitamos identificar estos segmentos y utilizar esta información en la fase de encaminamiento.

La identificación de segmentos de red sensibles a fallos implica un análisis de fiabilidad de la red o un estudio de la probabilidad de fallo de sus componentes. En algunos trabajos previos, [3] y [4], hay diversas propuestas para el cálculo y la aplicación a los algoritmos de encaminamiento de la probabilidad de fallo de la red.

La distancia de notificación es uno de los elementos para la reducción del tiempo de recuperación de fallos

Por otro lado la distancia de notificación es uno de los elementos para la reducción del tiempo de recuperación de fallos, aunque existen otros a tener en cuenta. Estos vienen dados por cada una de las fases en el proceso de recuperación y su análisis para la minimización del tiempo de ejecución. En [4] podemos encontrar un análisis más detallado de cómo minimizar cada una de las fases de recuperación de fallos.

El envío de la señal de notificación implica retardos producidos en los enlaces y en los nodos que atraviesa el paquete. Los retardos producidos en los nodos se derivan de los procesos y tiempos de espera en las colas, mientras que los producidos por los enlaces son los de transmisión y propagación. En [4] se establece que el único tiempo importante a tener en cuenta por los algoritmos de encaminamiento es el de propagación, el cual es proporcional a la distancia física. Por lo tanto la reducción de esta distancia (mediante la utilización de segmentos) es la manera más útil de reducir el tiempo de recuperación de fallos.

2.- Protección multicapa

En esta sección explicamos los aspectos a tener en cuenta para proteger la red cuando consideramos la capa *Wavelength División Multiplexing* (WDM) y la capa GMPLS. Suponemos que la topología física es fija y los enlaces son conjuntos de fibras ópticas que unen un par de nodos. En WDM se establece una topología lógica conectando pares de nodos a través de *lightpaths* que son una secuencia de enlaces físicos. Una vez establecida la topología lógica WDM, los cambios en ésta se producen a largo plazo.

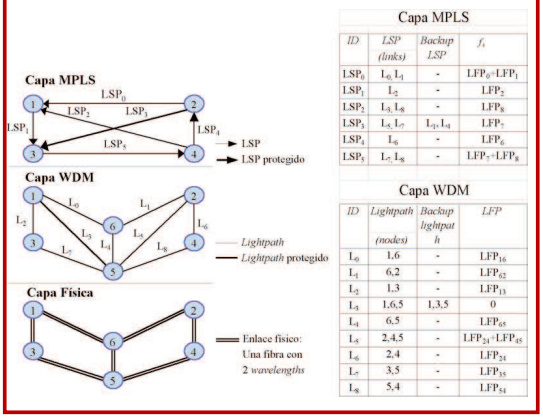
En MPLS se crean los Label Switch Paths (LSPs) conectando los pares de nodos a través de una secuencia de *lightpaths*. Es una topología lógica muy dinámica (se adapta a las necesidades del tráfico).Tanto en MPLS como en WDM se puede aplicar protección. Por ejemplo, supongamos las topologías en la capa WDM y MPLS definidas en las tablas de la figura 2. Por ejemplo el LSP_3 está siendo protegido por un backup LSP que atraviesa los *lightpaths* L_1 y L_4. Ahora bien, si quisiéramos proteger el LSP_2 sólo se tendría que establecer un backup local para proteger el *lightpath* L_8 en MPLS, ya que el *lightpath* L_3 está siendo protegido en WDM por el backup *lightpath* que se indica en la tabla.

Aunque la recuperación en MPLS utiliza un alto número de mensajes de notificación cuando se produce un fallo, éste resulta en mejor utilización de recursos que en WDM.

3.- Encaminamiento con calidad de servicio y protección en redes GMPLS sobre WDM

El trabajo realizado en el grupo se comenzó en el estudio de MPLS como tecnología para añadir calidad de servicio y protección a IP, luego se extendió a GMPLS teniendo en cuenta la expansión de la tecnología óptica. En esta sección vemos la evolución de este trabajo y las diferentes publicaciones donde se puede estudiar con más detalle.

FIG 2: PROTECCIÓN MULTICAPA



Capa MPLS

ID	LSP (links)	Backup LSP	f_i
LSP_0	L_6 L_3	-	LFP_6+LFP_3
LSP_1	L_2	-	LFP_2
LSP_2	L_5 L_8	-	LFP_8
LSP_3	L_5 L_7	L_1, L_4	LFP_7
LSP_4	L_6	-	LFP_6
LSP_5	L_7 L_8	-	LFP_7+LFP_8

Capa WDM

ID	Lightpath (nodes)	Backup lightpath	LFP
L_0	1,6	-	LFP_{16}
L_1	6,2	-	LFP_{62}
L_2	1,3	-	LFP_{13}
L_3	1,6,5	1,3,5	0
L_4	6,5	-	LFP_{65}
L_5	2,4,5	-	LFP_{24}+LFP_{45}
L_6	2,4	-	LFP_{24}
L_7	3,5	-	LFP_{35}
L_8	5,4	-	LFP_{54}

La aplicación de la interferencia presenta distintos problemas, como el alto grado de complejidad en su implementación

Un primer estudio de las técnicas de encaminamiento con calidad de servicio y su evolución actual en entornos MPLS lo podemos encontrar en [1 y 2] donde se resumen las diferentes opciones y técnicas utilizadas para el encaminamiento con garantías de calidad de servicio. Una de las últimas técnicas en el diseño de algoritmos de encaminamiento con calidad de servicio, con más rendimiento, se basa en el concepto de mínima interferencia (MIRA) [8]. La idea básica es evitar escoger caminos en la red que provoquen su congestión rápida. No obstante la aplicación de la interferencia presenta distintos problemas, como el alto grado de complejidad en su implementación. Aunque actualmente existen técnicas para reducirlo tal como el Light MIRA.

Por otro lado las últimas técnicas en protección se basan en el cálculo de rutas alternativas que se ajusten a las necesidades del tráfico. Así tendremos tráfico con protección dedicada, con protección compartida o simplemente tráfico no protegido. La identificación del concepto de calidad de protección y sus parámetros de evaluación (como pérdidas de paquetes o retardos) son claves para asignar el tipo de protección más adecuado a cada servicio. Varias propuestas como nuestros trabajos en [3, 4, 5 ó 6] muestran cómo hacer esta asignación de tipo de tráfico con mecanismo de protección.

Otro aspecto importante en la implementación de las técnicas de protección es la interacción entre capas. Así, las protecciones al nivel de capa óptica (por ejemplo en WDM) y en GMPLS deben tenerse en cuenta para evitar duplicaciones de protección, malgastando recursos y complicando la gestión de fallos.

La información disponible por las entidades de encaminamiento en la red es también un aspecto crucial en el desarrollo de algoritmos de encaminamiento aplicables a entornos reales de red. En estos trabajos previos la información necesaria para cada algoritmo así como propuestas para la implementación de estos con más o menos precisión en estos datos también se ha considerado.

4.- Conclusiones

En resumen, en este artículo sólo enmarcamos los aspectos considerados por el grupo de comunicaciones de la UdG para el desarrollo de nuevas técnicas de encaminamiento con protección en redes basadas en GMPLS.

El estudio de algoritmos de encaminamiento con técnicas de mínima interferencia y el uso de información de red más o menos detallada, junto con la definición de protección de segmentos de red con diferenciación de tráfico y técnicas para compartir el ancho banda se han considerado en este artículo.

Referencias

[1] Eusebi Calle, José L Marzo, Anna Urra "Protection Performance Components in MPLS Networks" Elsevier Computer Communications Journal, July 2004 Vol 27 Issue 12 pp. 1220-1228.

[2] J. L. Marzo, E. Calle, C. Scoglio, T. Anjali "QoS On-Line Routing and MPLS Multilevel Protection: a Survey" IEEE Comunication Magazine, vol. 41(10), pp. 126-132, October 2003.

[3] J. L. Marzo, P. Vilà, A.Bueno, L. Fàbrega, E. Calle "Automatic Self-Configuration of the Logical Network using Distributed Software Agents" In proceedings of IEEE Global Communications Conference IEEE GLOBECOM 2004 Dallas, Texas (USA), 29 Nov-3 Dec 2004.

[4] E. Calle, J. L. Marzo, A. Urra, LL. Fàbrega "Enhancing Fault Management Performance of Two-Step QoS Routing Algorithms in GMPLS" In proceedings of ICC 2004, 20-24 June, 2004, Paris (France). IEEE 2004, ISBN 0-7803-8533-[0/9].

[5] Eusebi Calle, José L Marzo, Anna Urra "Evaluating the Probability and the Impact of a Failure in GMPLS Based Networks" In proceedings of DRCN 2003, Alberta (Canadá) IEEE 2003, ISBN 0-7803-8118-1.

[6] Eusebi Calle, José L Marzo, Anna Urra, Pere Vila "Enhancing MPLS QoS Routing Algorithms by Using the Network Protection Degree Paradigm." In proceedings of GLOBECOM 2003, San Francisco (USA) IEEE 2003. ISBN: 0-7803-7974-8.

[7] J. L. Marzo, E .Calle, C. Scoglio, T. Anjali "Adding QoS Protection in Order to Enhance MPLS QoS Routing" In proceedings of ICC 2003. Anchorage, Alaska (USA). IEEE 2003, ISBN 0-7803-7804-4.

[8] M. Kodialam, T. V. Lakshman. "Minimum Interference Routing with Applications to MPLS Traffic Engineering". In proceedings of IEEE Infocom, 2000.

Eusebi Calle, José L. Marzo,
(eusebi@eia.udg.es), (marzo@eia.udg.es),
Anna Urra, Pere Vilà,
(aurra@eia.udg.es), (perev@eia.udg.es),
Santiago Cots
(scots@eia.udg.es)
Instituto de Informática y Aplicaciones
Universidad de Girona