ANÁLISIS DE LA INCIDENCIA DE FALLAS MÚLTIPLES EN REDES MPLS

ANALYSIS OF THE INCIDENCE OF MULTIPLE FAILURES ON MPLS NETWORKS

AUTOR
WILLIAM GIRALDO SANDOVAL
Ingeniero en Electrónica y Telecomunicaciones
*Universidad del Cauca
wgiraldo@unicauca.edu.co
COLOMBIA

AUTOR
RUBÉN DARÍO GUERRERO ENRÍQUEZ
Ingeniero en Electrónica y Telecomunicaciones
*Universidad del Cauca
rguerrero@unicauca.edu.co
COLOMBIA

AUTOR
OSCAR JOSUÉ CALDERÓN CORTÉS
Profesor Titular Ingeniería Electrónica y Tel.
*Universidad del Cauca
Miembro Profesional IEEE
oscarc@unicauca.edu.co
COLOMBIA

INSTITUCIÓN
*UNIVERSIDAD DEL CAUCA
UNICAUCA
Universidad Pública
Calle 5 # 4 – 70
Popayán, Cauca
COLOMBIA

Recepción: Septiembre 13 de 2009 **Aceptación:** Diciembre 23 de 2009

temática: Convergencia de servicios y redes de telecomunicaciones

Tipo de artículo: Artículo de investigación científica y tecnológica

RESUMEN

Dentro del contexto actual de las redes de telecomunicaciones, las tendencias apuntan al uso de servicios y aplicaciones con altas exigencias de recursos de red, características de QoS y disponibilidad, lo cual ha llevado a los operadores a adoptar MPLS como tecnología de soporte en el núcleo de sus redes, gracias a las ventajas que ofrecen en la velocidad de conmutación y enrutamiento de tráfico. En estas condiciones, la ocurrencia de eventos de falla en la red puede degradar de manera considerable su desempeño y afectar severamente las características de los servicios soportados por la misma, llevando en algunos casos críticos a la pérdida total de información.

Este artículo presenta un análisis del impacto que tiene la ocurrencia de eventos de falla múltiple sobre una red MPLS, evaluando para ello algunos parámetros de desempeño (pérdida de paquetes, desorden, retardo, jitter, tiempo de restablecimiento) sobre los tráficos transportados. Se plantea un escenario de simulación sobre el cual se programan fallas usando el simulador NS-2 (Network Simulator) y se evalúa el impacto ocasionado por estos eventos tanto cuando no se aplica ninguna estrategia de recuperación como cuando se aplican los métodos de protección (Global, Local e Inverso) con el objeto de verificar si es posible recuperar los tráficos comprometidos bajo tales condiciones y mantener las características de QoS requeridos por los servicios soportados por ella.

PALABRAS CLAVES

MPLS
Falla múltiple
Recuperación
Parámetros de desempeño

ANALYTICAL SUMMARY

Nowadys, most network operators have been forced to adopt MPLS as the support technology for the core in their networks, as a result of the trends in the usage of services and applications which demand a lot of network resources, special QoS properties and high availability. MPLS makes it possible thanks to the high switching and routing speeds that this technology offers. In these scenarios, however, the occurrence of failure events in the network could critically decrease its performance, and as a consequence affect the services which are carried by the network, leading in the worst case scenarios to the complete loss of information.

This paper presents an analysis on the impact associated to the occurrence of failure events on MPLS networks. Performance parameters are evaluated such as packet loss, packet disordering, delays, jitter and restorarion time. A simulation scenario is proposed where multiple failure events are simulated by using Network Simulator (NS-2), and the impact induced by these events is evaluated when no recovery strategy is applied and also by using protection methods on the proposed scenario as an alternative to recover the affected traffics, so QoS properties and the original conditions for the services carried by the network can be kept unaltered.

KEYWORDS

MPLS
Multiple Failures
Recovery
Performance parameters

INTRODUCCIÓN

La ocurrencia de fallas en una red MPLS es un evento desfavorable cuya presencia puede afectar el tráfico circulante por la red en mayor o menor grado de acuerdo a sus características, causando la pérdida parcial o total de la información [1-3]. La presencia de dichos eventos puede causar degradación sobre las características de los servicios soportados por la red, llegando a ser un problema crítico en aplicaciones de video y audio en tiempo real donde una interrupción debido a una falla puede causar pérdida de paquetes, lo cual incide negativamente en la inteligibilidad del mensaje y por ende en la experiencia de uso del servicio por parte de sus usuarios [2], además, de repercutir en la imagen y credibilidad que se tiene del operador.

Cuando la ocurrencia de fallas es inminente, es preciso que los operadores de red hagan frente a esta problemática e identifiquen plenamente las causas y los factores asociados con la ocurrencia de estos eventos y de igual forma, determinen el impacto sobre los tráficos transportados por la red.

El impacto de falla en una red MPLS se define como el grado de afectación que recibe el tráfico cursante en términos de la degradación de su calidad de servicio [2]-[4]. Su medición y posterior estudio es útil en cuanto permite a los operadores de red obtener lineamientos a partir de los cuales se pueden adoptar medidas correctivas que permitan mitigar las consecuencias que los eventos de falla tienen sobre el desempeño general de la red y sobre las aplicaciones y servicios soportados por ella.

Para la medición del impacto se tienen en cuenta los parámetros de desempeño, que sirven para evaluar el comportamiento de los tráficos que fluyen a través de la red [2][5]-[6]. Los más representativos son el tiempo de restablecimiento, la pérdida de paquetes, el desorden de los mismos, el retardo, el jitter, entre otros. El análisis del impacto en términos de los parámetros mencionados es subjetivo y depende de las características de la red y de los flujos de tráfico estudiados [4]-[6]. Sin embargo, existen algunas restricciones respecto a los rangos de valores permitidos para estos parámetros que permiten garantizar la QoS de servicios y aplicaciones como se describe en la recomendación G.1010 [7].

El análisis aquí planteado y los resultados obtenidos, corresponden a los resultados finales de investigación del trabajo de grado titulado “Impacto de fallas múltiples en redes MPLS”, desarrollado en la facultad de ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca.

1. GENERALIDADES SOBRE FALLAS EN REDES MPLS

Una falla se define como la terminación de la habilidad de un elemento de red para llevar a cabo una función requerida [8]. Una falla en la red ocurre en un momento en particular, aunque en algunos casos se puede causar por la degradación gradual de sus componentes. En el presente artículo se tienen en cuenta únicamente eventos de falla en el nivel físico, es decir aquellos que comprometen el funcionamiento de los Trayectos Conmutados por Etiquetas (LSRs: Label Switched Path) y los Enrutadores Conmutados por Etiquetas (LSRs: Label

Switch Router) que componen un dominio MPLS, sin considerar las repercusiones que puedan existir sobre otros niveles y que involucren por ejemplo problemas en los procesos de señalización, protocolos y acciones de enrutamiento, entre otros.

En general se considera que en el nivel físico los eventos de falla son independientes [8-9], esto quiere decir que la ocurrencia de una falla en algún componente de la red no guarda relación alguna con la ocurrencia de un evento de falla subsiguiente sobre otro elemento. Esta consideración reviste gran importancia para efectos del análisis de la incidencia que dichos eventos tienen sobre la red y en particular sobre los tráficos transportados, puesto que permite el análisis de eventos de falla programados aleatoriamente sobre la infraestructura de la red sin tener en cuenta factores adicionales.

De acuerdo al número de fallas que se presenten en un momento determinado en una red MPLS, se pueden presentar eventos de falla simple y múltiple. Una falla simple se refiere a un evento en el cual únicamente un nodo o enlace deja de ser operativo en un momento determinado, mientras que las fallas múltiples involucran la ocurrencia simultánea o dentro de un mismo lapso de tiempo de dos o más eventos de falla que afectan los dispositivos y enlaces de una red y en consecuencia su normal funcionamiento [10-12]. En general estos últimos se caracterizan por afectar en mayor grado la infraestructura de la red en comparación con las fallas simples puesto que pueden comprometer no solo los caminos de trabajo por los cuales fluyen los tráficos en condiciones normales sino que también afectan los caminos de respaldo empleados por los mecanismos de recuperación, quitándole a la red la capacidad de contrarrestar las consecuencias que acarrean la presencia de las fallas.

La ocurrencia de fallas puede atribuirse a factores de diversa índole. Estos pueden producirse por la intervención premeditada o indirecta del hombre, por motivos inherentes al funcionamiento de la red o también como consecuencia de fenómenos provocados por la naturaleza. Pueden afectar tanto el hardware como el software de la red y se pueden originar en el interior o el exterior de la misma [13-15].

2. RECUPERACIÓN EN REDES MPLS

El concepto de recuperación es una alternativa que permite a los operadores de red mitigar las consecuencias negativas producidas a partir de la ocurrencia de eventos de falla mediante la utilización de mecanismos que buscan mantener las condiciones iniciales del tráfico comprometido por dichas fallas, preservando las condiciones de QoS de las aplicaciones y servicios soportados por los tráficos que resultan afectados y permitiendo además mejorar la disponibilidad y confiabilidad de las mismas [16-17].

Existen dos enfoques que permiten abordar la recuperación, el modelo de protección y el modelo de restablecimiento. El primero es un esquema de recuperación de fallas en el cual se establece y configura un camino de respaldo con antelación, reservando el ancho de banda necesario para este y dotándolo con capacidades de enrutamiento de tráfico en caso de que el camino de trabajo falle. El modelo de restablecimiento, por otro lado, es un esquema de recuperación dinámico en el cual se establece inicialmente un camino de trabajo a través del cual fluyen los tráficos desde el origen hasta el destino, y en el momento en que ocurra algún evento de falla se computa un camino de respaldo de forma dinámica por el cual se re-enrutan los tráficos afectados para su recuperación. Este proceso es costoso a nivel de procesamiento, pues los recursos que se asignen al camino de respaldo podrían no estar disponibles en el momento de la falla, a diferencia del modelo de protección en el que estos se establecen con antelación, y por lo tanto se requeriría volver a calcular un nuevo camino de respaldo [16]-[18].

FIGURA 1. Enfoques de recuperación en redes MPLS

Para el desarrollo del análisis en este artículo se utilizó el modelo de protección, cuya efectividad ha sido comprobada en contextos de falla simple [18]. En general, el modelo de protección brinda mejores condiciones para tráficos con altos requerimientos en términos de pérdida de paquetes y tiempos de restablecimiento permitiendo por tanto una mayor velocidad de recuperación del tráfico afectado ya que el camino de respaldo se calcula antes de la ocurrencia de algún evento de falla.

Se evaluó el desempeño del modelo de protección en contextos de falla múltiple mediante la utilización de los métodos de protección (global, local e inverso) como alternativa de recuperación para los tráficos afectados por los eventos de falla, teniendo en cuenta el impacto que se inflige a los mismos en términos de los siguientes parámetros de desempeño: pérdida de paquetes, desorden de paquetes, tiempo de restablecimiento, retardo y jitter.

A continuación se presenta el escenario de red propuesto y el plan de pruebas desarrollado.

3. ESCENARIO DE SIMULACIÓN

3.1 CARACTERÍSTICAS DEL ESCENARIO DE SIMULACIÓN.

La figura 2 presenta el escenario de red utilizado para las pruebas con el simulador NS-2.

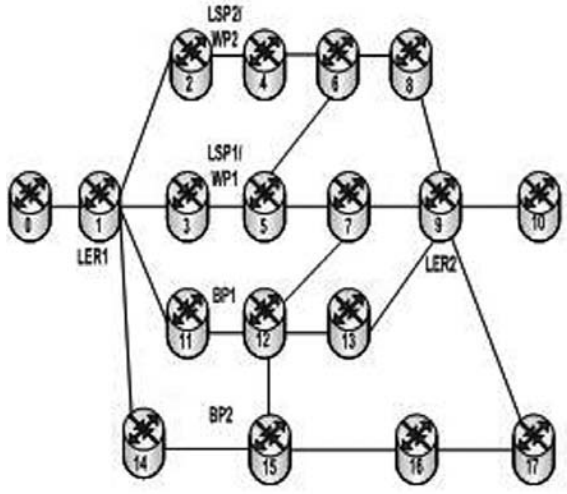


FIGURA 2. Escenario de simulación.

El escenario de simulación propuesto consta de 15 LSRs, 2 LERs y 2 nodos IP. El valor de ancho de banda para todos los enlaces es de 6Mbps. Los caminos utilizados para el flujo de los tráficos se indican en la figura (BPi: Backup Path i y WPi: Working Path i). La longitud de los enlaces tiene una disposición asimétrica de tal manera que sus retardos no son constantes dentro del escenario de red.

3.2 PLAN DE PRUEBAS.

El plan de pruebas realizado constó de dos casos generales. En el primero de ellos se programaron eventos de 3 fallas cuando no se aplica ninguna alternativa de recuperación sobre la red, conforme se describe en la FIGURA 3. En el caso dos se programaron el mismo número de fallas, pero aplicando en esta ocasión los métodos de protección global, inverso y local para tratar de recuperar los tráficos afectados. Los caminos de respaldo relacionados con la ejecución de los métodos de protección para el caso dos no resultan comprometidos por los eventos de falla de manera que no se afecten las acciones de recuperación adoptadas.

La Figura 3 resume las características generales relacionadas con los caminos utilizados para el direccionamiento de los tráficos, ubicación de las fallas y acciones de recuperación para los dos casos propuestos en el plan de pruebas.

Características del escenario de simulación correspondiente al plan de pruebas				
	Caso 1		Caso 2	
LSP/WPS	LSP1 (LSR1-LSR3-LSR5-LSR7-LSR9)	LSP2 (LSR1-LSR2-LSR4-LSR6-LSR8-LSR9)	WP1 (LSR1-LSR3-LSR5-LSR7-LSR9)	WP2 (LSR1-LSR2-LSR4-LSR6-LSR8-LSR9)
Tipo de tráfico	Video y Datos	Voz	Video y Datos	Voz
Ubicación/ (Instante simulación)	LSR7-LSR9 (0.8s) LSR12-LSR13 (0.9s) LSR6-LSR8 (0.95s) (tres fallas)		LSR7-LSR9 (0.8s) LSR12-LSR13 (0.9s) LSR6-LSR8 (0.95s) (tres fallas)	
Acción de recuperación	Ninguna/ Descarte de paquetes		Global inverso: LSR1-LSR14-LSR15-LSR16-LSR17-LSR9 Local: LSR7-LSR12-LSR15-LSR16-LSR17-LSR9.	

FIGURA 3. Características del escenario de simulación correspondiente al plan de pruebas propuesto.

4. RESULTADOS.

A partir de los datos obtenidos en el simulador NS-2 al programar sobre la topología propuesta eventos de falla múltiple correspondientes a los dos casos propuestos, se presentan los siguientes resultados.

4.1. CASO 1: RED CON FALLAS MÚLTIPLES (SIN RECUPERACIÓN)

La figura 4 presenta el throughput correspondiente a los tráficos estudiados cuando ocurren tres eventos de falla conforme se describió en la Figura 3. Los tráficos de video y datos se representan con color rojo y verde respectivamente, mientras que el tráfico de voz se representa con color azul.

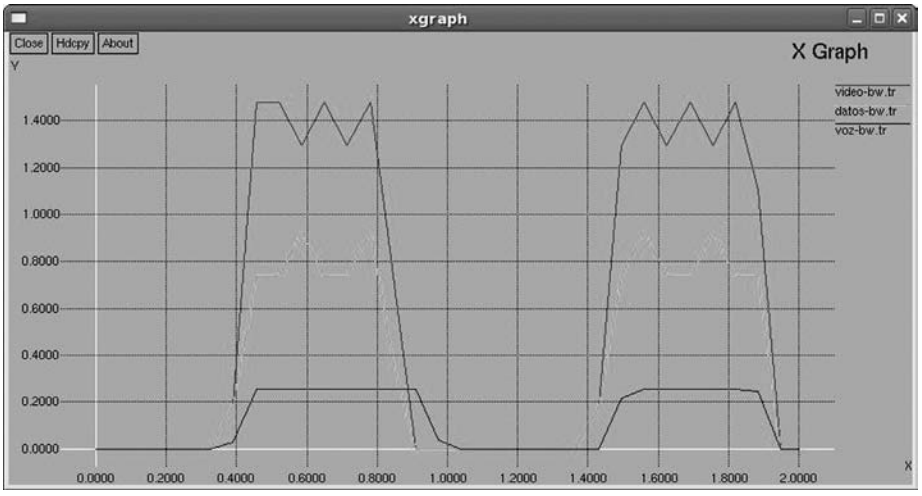
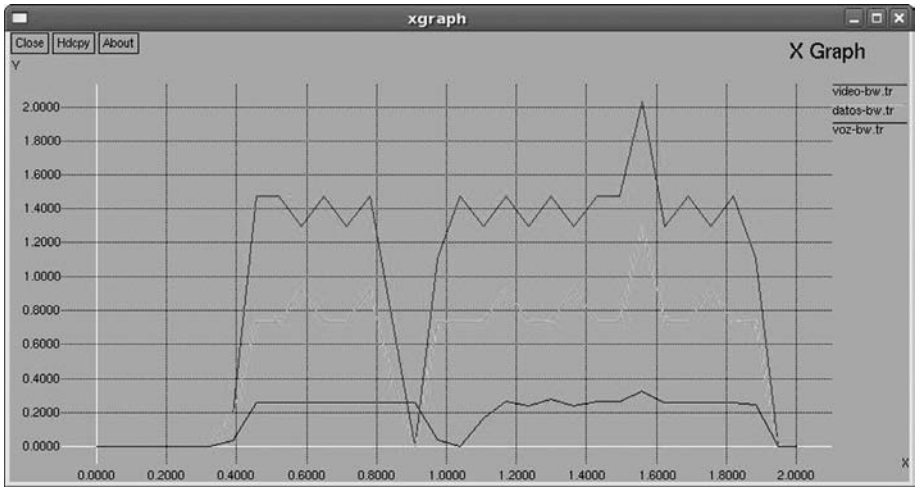


FIGURA 4. Throughput para el evento de 3 fallas en los enlaces sin aplicar mecanismos de recuperación (caso 1).

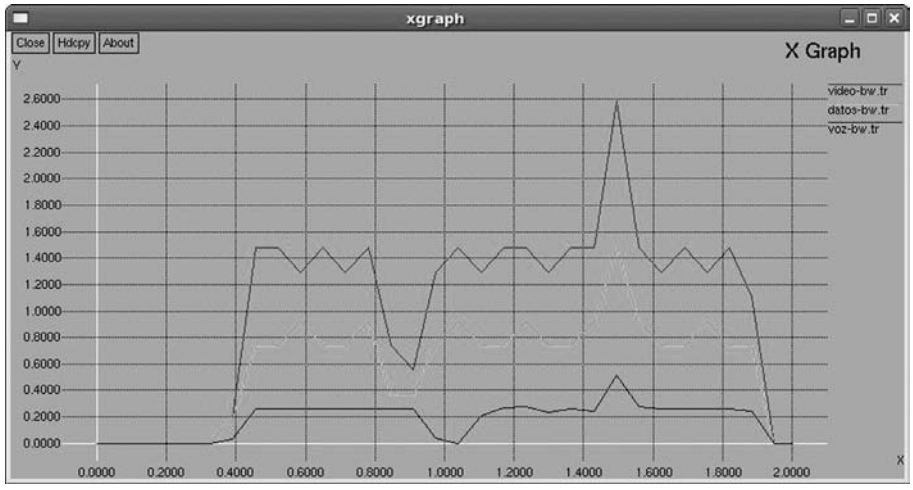
Según la figura 4, la caída total en el throughput para los tráficos de video y datos sobre el instante 0.8 segundos obedece al primer evento de falla. El tráfico de voz sufre de igual manera una caída drástica producida por el tercer evento de falla sobre el instante 0.95. Los paquetes de los diferentes tráficos afectados se descartan mientras los enlaces permanecen caídos hasta los 1.4 segundos del tiempo de simulación, instante en donde recobran su estado operativo.

4.2. CASO 2: RED CON FALLAS MÚLTIPLES (APLICANDO MÉTODOS DE PROTECCIÓN).

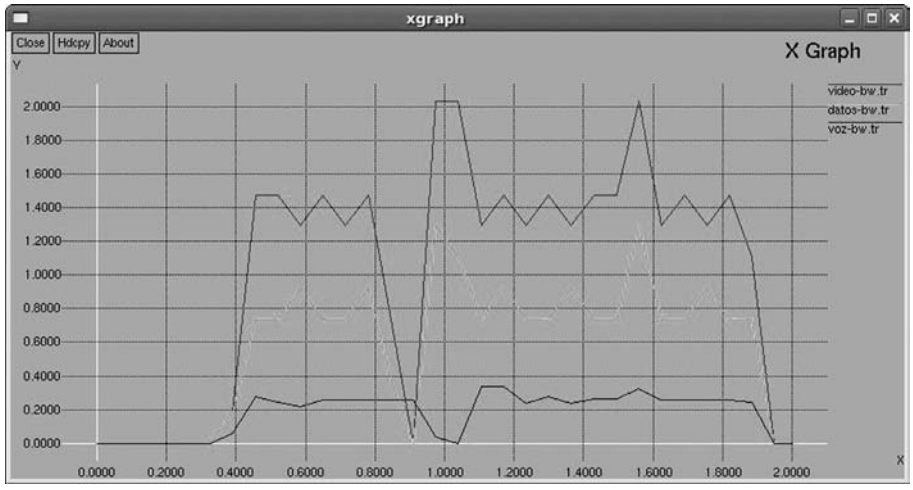
Para este caso de pruebas se programan los mismos eventos de falla que para el caso anterior, aplicando ahora los tres métodos de protección (global, inverso y local). En ninguna de las pruebas realizadas resultó comprometido alguno de los caminos de respaldo presentados en la FIGURA 4, puesto que de hacerlo las acciones de recuperación asociadas a cada uno de los métodos no se podrían completar de manera exitosa, o bien su acción sería parcial y por tanto los resultados arrojados serían muy similares a los obtenidos en el caso 1. Las gráficas de throughput para los tres métodos cuando ocurren tres eventos de falla se presentan a continuación.



a) Método global



b) Método local



c) Método inverso

FIGURA 4. Throughput para el evento de tres fallas en el caso 2 del plan de pruebas usando los tres métodos de protección.

El comportamiento observado en las gráficas de throughput de la figura 5 es similar. Las caídas parciales que se observan sobre el instante 0.8 son considerablemente menores y se extienden por menor tiempo en comparación con las de la figura 4, en donde la ausencia de alternativas de recuperación se traduce en el descarte de paquetes durante el lapso de tiempo en que las fallas afectan los enlaces en la red. En general, el método de protección local presenta la caída de throughput menos pronunciada, debido a que las acciones de recuperación se toman directamente por los nodos contiguos a los enlaces que resultan afectados por los eventos de falla y por tanto no es necesario que las señales de notificación de falla (FIS) deban viajar hasta un nodo que conmute los tráficos hacia caminos de respaldo, obteniendo de esta manera porcentajes de pérdida de paquetes y tiempos de restablecimiento menores en comparación con los otros dos métodos. Los picos que se presentan en el instante 1.4 obedecen al encolamiento que se genera debido a la confluencia de paquetes provenientes del BP2 y del WP1 sobre el LSR9.

La figura 6 presenta el porcentaje de pérdida de paquetes para los dos casos propuestos.

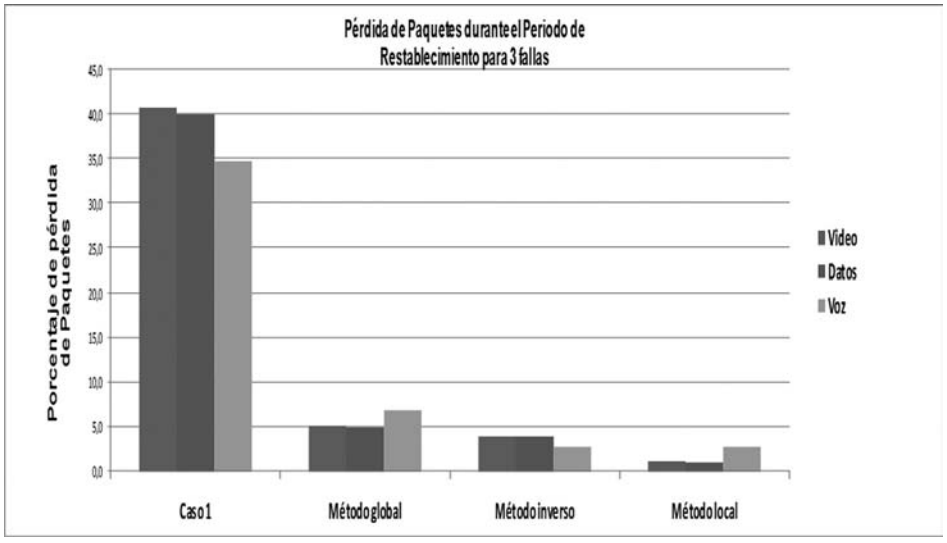


FIGURA 6. Porcentaje de pérdida de paquetes para los dos casos del plan de pruebas.

En la figura 6 se observa claramente la mejora porcentual en la pérdida de paquetes que supone la adopción de métodos de protección que recuperen de manera exitosa los tráficos comprometidos por fallas, en comparación con el caso 1 en el cual no se aplica ninguna estrategia de recuperación, lo cual se ve reflejado en pérdidas del orden del 40%, en contraste con valores que varían entre el 1 y 5% para el caso dos. Estos valores se ajustan a los exigidos por la ITU-T [7] para aplicaciones de tiempo real tales como el streaming de video y audio.

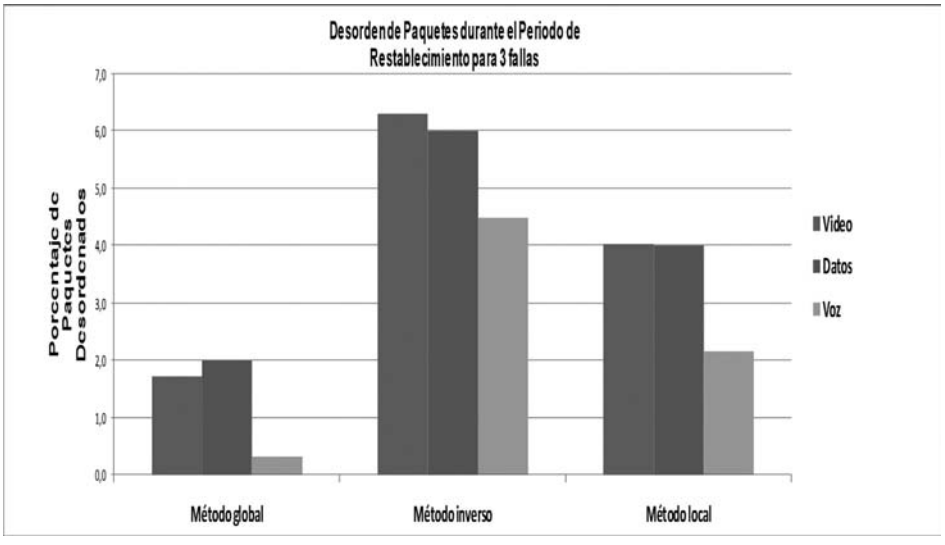


FIGURA 7. Porcentaje de desorden de paquetes para el caso 2 del plan de pruebas.

La figura 7 presenta el porcentaje de desorden de paquetes para el caso dos del plan de pruebas. El uso de caminos de respaldo generalmente introduce desorden en los paquetes ya que para la topología propuesta estos caminos cuentan con retardos distintos a los que tienen los enlaces de los caminos de trabajo, y por tanto los paquetes que fluyen por estos pierden su secuencia al llegar al destino.

El método inverso se distingue porque presenta un porcentaje de desorden de paquetes que alcanza el 7% aproximadamente, siendo comparativamente mayor respecto a los otros métodos. Esto se explica por la acción propia de este mecanismo, en la cual los tráficos comprometidos se re-enrutan en dirección opuesta hasta que una señal FIS alcance el nodo que realiza la conmutación de los tráficos, mezclándose con los paquetes que siguen fluyendo en dirección normal hacia el enlace que presenta la falla. Los valores alcanzados para el método local son del orden del 4%, mientras que para el método global se obtienen los valores porcentuales más bajos, debido a que no hay combinación de tráficos que fluyan en diferentes direcciones a través de un mismo LSP como sucede en el método inverso, presentándose descarte de paquetes hasta tanto no se conmuten los tráficos comprometidos hacia los caminos de respaldo.

4.2.1. Tiempo de Restablecimiento.

Para la medición de los tiempos de restablecimiento para el caso 2, se tiene en cuenta que los nodos LSR6 y LSR7 son los que inician las acciones de recuperación cuando se aplican los métodos de protección.

El método local presenta los valores más bajos de tiempo de restablecimiento puesto que la distancia de notificación de fallas es cero y adicionalmente cada LSR es capaz de realizar el re-enrutamiento del tráfico de manera independiente, obteniendo resultados de 4.8 y 30.17 ms, cuando la recuperación se inicia por los nodos LSR7 y LSR6 respectivamente, en contraste con valores más altos obtenidos para los demás mecanismos donde este proceso ocurre en el nodo de ingreso al dominio MPLS, que son de 54.23 ms para el método global e inverso cuando el LSR6 inicia las acciones de recuperación y de 37.71 y 38.2ms cuando dichas acciones se toman por el LSR7 para los dos métodos respectivamente.

4.2.2. Retardo y Jitter.

El método local presenta los valores más altos de retardo, puesto que su camino de respaldo introduce mayores retardos respecto a los caminos utilizados para los métodos global e inverso, alcanzando un valor máximo de 94.33ms para el tráfico de voz, en comparación con valores que varían entre 50 y 60ms cuando se aplican los demás mecanismos. Ninguno de estos valores sobrepasa el máximo permitido de 150ms para los tráficos de video y voz según las restricciones impuestas por la ITU, y por tanto no habría repercusiones sobre la QoS de los servicios soportados por los mismos.

En cuanto al jitter, los valores obtenidos para los diferentes tráficos al aplicar los métodos de protección son similares y en general varían entre 0.21 y 0.56ms. No se sobrepasa el límite máximo permitido de 1ms para los tráficos de video y voz, por lo cual las aplicaciones soportadas por los mismos no se verían afectadas.

A partir de los resultados obtenidos en las pruebas del caso dos, se puede concluir que la utilización de los métodos de protección ante falla simple se consolida como una alternativa útil de cara a la problemática de fallas múltiples.

5. VALORACIÓN DEL IMPACTO OCASIONADO SOBRE LOS TRÁFICOS DEL PLAN DE PRUEBAS.

A continuación se presenta el análisis del impacto que los eventos de falla múltiple ocasionan a los tráficos establecidos para las pruebas de simulación en términos de los parámetros de desempeño evaluados previamente. Dicho análisis es subjetivo y depende del caso de estudio en cuestión, de la topología propuesta, de la localización de las fallas y demás características que enmarcan el escenario de simulación, sin embargo su desarrollo se puede extender a otras topologías distintas con presencia de múltiples fallas y donde fluyan tráficos de diferentes tipos.

Para la valoración del impacto de manera cualitativa se definen las categorías alto, medio y bajo (A, M y B), que describen respectivamente qué tan afectado resulta cada uno de los parámetros, así como los rangos que permitan valorarlos de manera cuantitativa de acuerdo a los valores establecidos en [7] y a los resultados arrojados por la simulación, los cuales se presentan en la Figura 8. La influencia del retardo y el jitter sobre el tráfico de datos no es significativa pues su efecto no incide sobre las aplicaciones y servicios soportados por él, por tanto no se tienen en cuenta en la figura.

Tipo de tráfico	Porcentaje de pérdida de paquetes (%)			Desorden de paquetes (%)			Tiempo de Restablecimiento			Retardo (ms)			Jitter (ms)		
	A	M	B	A	M	B	A	M	B	A	M	B	A	M	B
Voz	>5	3-5.	<3	>4	2-4.	0-2	>50	20-50	<20	>400	150-400	<150	>3	1-3.	<1
Video	>5	1-5.	<1	>4	2-4.	0-2	>50	20-50	<20	>400	150-400	<150	>3	1-3.	<1
Datos	>1	0-1	0	>4	2-4.	0-2	>50	20-50	<20	NA	NA	NA	NA	NA	NA

FIGURA 8. Rangos de valores para la valoración del impacto de los eventos de falla.

5.1 IMPACTO OCASIONADO POR EVENTOS DE FALLA MÚLTIPLE SIN LA APLICACIÓN DE MECANISMOS DE RECUPERACIÓN.

El impacto ocasionado a los tráficos en términos del porcentaje de pérdida de paquetes es alto en todos los casos de falla estudiados debido a que no se toma ninguna medida para su recuperación efectiva, a excepción del caso donde ocurre un solo evento de falla en el enlace LSR7-LSR9, cuyo efecto sólo compromete los tráficos de video y datos, por lo que las características del tráfico de voz no resultan especialmente alteradas. Lo anterior se evidencia claramente en las caídas del throughput y en las gráficas de porcentajes de pérdidas de paquetes presentadas anteriormente en la secciones 5a y 5b respectivamente.

A raíz de lo anterior, la calidad de servicio de las aplicaciones y servicios soportados por los tráficos transportados en la red se verá degradada de manera crítica, hecho que inevitablemente perjudicara la experiencia de uso de los usuarios finales.

Por otro lado, el impacto que tiene el desorden de paquetes es bajo, puesto que al no aplicarse acciones de recuperación las causas de desorden asociadas a su ejecución tales como la combinación de tráficos que fluyen en diferentes direcciones a través de un mismo LSP y la conmutación de tráfico a través de un camino de respaldo que puede introducir mayor o menor retardo que el del camino de trabajo no suponen ningún problema en este caso.

En este análisis de impacto solo se considera el comportamiento de la pérdida y el desorden de paquetes de entre los cinco parámetros de desempeño establecidos. El tiempo de restablecimiento no se tiene en cuenta puesto que no se aplican estrategias de recuperación, mientras que el valor de retardo y jitter no se puede calcular con precisión por el simulador cuando los tráficos no se recuperan de manera efectiva y por tanto no se definen.

5.2 IMPACTO OCASIONADO POR EVENTOS DE FALLA MÚLTIPLE CUANDO SE APLICAN LOS MÉTODOS DE PROTECCIÓN.

Según los resultados obtenidos en la Figura 9, se observa una notable mejora del impacto ocasionado a los tráficos de video, datos y voz que fluyen a través de la red tras la ocurrencia de múltiples fallas. Se evidencia que el método de protección global es el que registra el impacto más alto en términos del número de paquetes perdidos en comparación con los demás métodos, sin embargo el impacto del desorden de paquetes introducido es el más bajo, puesto que no hay combinación de tráficos que fluyan en distintos sentidos en un mismo LSP como sucede en el método inverso, el cual presenta el impacto más alto respecto a este parámetro.

Por otro lado, el método local registra el impacto más bajo respecto a la pérdida de paquetes, ya que ofrece el menor tiempo de restablecimiento por sus características de funcionamiento. En este sentido, dicho método está especialmente indicado para la recuperación de tráficos que requieran un alto grado de protección. El tiempo de restablecimiento del método global e inverso también puede mejorarse al reducir la distancia D(i,a) y usar enlaces físicos con tecnologías que permitan disminuir el tiempo de propagación para implementar la red MPLS [1][3]- [8].

A partir de los resultados obtenidos, se evidencia que todos los métodos analizados cumplieron con las restricciones de retardo y jitter requeridas para el correcto funcionamiento de las aplicaciones y servicios asociados a los tráficos estudiados, gracias en parte al bajo retardo introducido por los enlaces que componen los caminos de trabajo y de respaldo. Por ello, para lograr bajos niveles de retardo es importante escoger de manera conveniente los enlaces que componen los LSPs a través de los cuales fluye el tráfico, de manera que su efecto no perjudique la calidad de las aplicaciones soportadas por la red. Por otra parte, para mitigar el efecto del jitter se recurre al uso de buffers encargados de organizar y reenviar los paquetes en el destino. Sin embargo, entre mayor sea su tamaño, mayor el retardo adicional que se generará por efectos del mismo [1]-[3].

El método local es el más apto de los mecanismos para la recuperación efectiva de los tráficos afectados por la presencia de fallas múltiples en la red, debido a que en general brinda el mejor nivel de protección, lo cual se comprueba en el impacto percibido por los tráficos transportados según los valores de los parámetros de desempeño obtenidos previamente, lo que redunda en un mejor rendimiento de las aplicaciones y servicios soportados por la red. No obstante, su principal desventaja reside en la utilización ineficiente de recursos, además de la necesidad de dotar a la red con tantos pares de nodos PSL (Path Switch LSR) y PML (Path Merge LSR) como enlaces se desee proteger.

En conclusión, cuando los métodos de protección se aplican utilizando caminos de respaldo libres de fallas, se consolidan como una buena alternativa para la recuperación de los tráficos cursantes cuando estos resultan afectados por la ocurrencia de uno o más eventos de falla, respecto a cuando la red no implementa mecanismos de recuperación o bien si su aplicación no se completa de manera exitosa.

Impacto ocasionado en los tráficos cursantes en contextos multifalla (Caso 2b)						
Métodos de protección	Tipos de tráfico	Pérdida de paquetes	Desorden de paquetes	Tiempo de Restablecimiento	Retardo	Jitter
Método Local	Video	Medio	Medio	Bajo	Bajo	Bajo
	Datos	Medio	Medio	Bajo	Bajo	Alto
	Voz	Bajo	Medio	Bajo	Bajo	Bajo
Método Inverso	Video	Medio	Alto	Alto	Bajo	Bajo
	Datos	Alto	Alto	Alto	Bajo	Alto
	Voz	Bajo	Alto	Alto	Bajo	Bajo
Método Global	Video	Alto	Bajo	Alto	Bajo	Bajo
	Datos	Alto	Bajo	Alto	Bajo	Alto
	Voz	Alto	Bajo	Alto	Bajo	Bajo

FIGURA 9. Valoración cualitativa del impacto ocasionado a los tráficos cursantes para eventos de falla múltiple (Caso 2 del plan de pruebas).

6. CONCLUSIONES.

A medida que el número de fallas en la red aumenta, el impacto ocasionado sobre los tráficos transportados es más crítico, en cuanto se reduce la disponibilidad de los caminos por los cuales fluyen.

La herramienta de simulación NS-2, así como el módulo MNS permitieron caracterizar adecuadamente los tráficos inyectados a la red, lo cual condujo a la obtención de resultados confiables.

El impacto que tiene la ocurrencia de eventos de fallas sobre los tráficos transportados es crítico cuando la red no implementa mecanismos de recuperación.

Se comprobó que los métodos de protección ante eventos de falla simple se adaptan bien a contextos de falla múltiple.

Los resultados de simulación indican que el método de protección local es el que mejor responde ante eventos de falla múltiple, en contraste al método global, el cual registra el peor desempeño teniendo en cuenta los parámetros evaluados.

Los resultados obtenidos evidencian que se cumple con los requerimientos de desempeño especificados por la ITU-T cuando se recuperan de manera exitosa los tráficos comprometidos por eventos de falla, al aplicar los distintos métodos de protección.

7. REFERENCIAS

[1] HUNDESSA GONFA, Lemma. Enhanced fast rerouting mechanisms for protected traffic in MPLS Networks, Cataluña, 2003, 159 p. Tesis doctoral (Doctora en Ingeniería Telemática). Universidad Politécnica de Cataluña. Departamento de Arquitectura de Computadores.

[2] CALLE, Eusebi, MARZO, José. Protection performance components in MPLS networks. Advances in Computer Communications. Vol 27, Edición 12, p.1220-1228. Girona: Universidad de Girona, 2003.

[3] HADJIONA, Maria GEORGIOU, Chryssis, VASSILIOU, Vasos.A Hybrid Fault-Tolerant Algorithm for MPLS Networks. Software in Telecommunications and Computer Networks, 2006. SoftCOM 2006. International Conference on. P. 369-369, Chipre, 2007.

[4] MARZO, José, CALLE, Eusebi, SCOGLIO, Caterina, TRICHA, Anjali. Adding QoS protection in order to Enhance MPLS QoS routing. Communications, 2003.

[5] PETERSON, Olof. MPLS based recovery mechanisms. Oslo, 2005. 137 p. Tesis de Maestría. ().(). Universidad de Oslo.

[6] HARRISON, Ed, FARREL, Adrian, MILLER, Ben. Protection and restoration in MPLS networks. Versión 2. Enfield. Data Connection Limited. 2006. 42 p.

[7] Recomendación ITU-T G.1010, End-User multimedia QoS categories series G: transmission systems and media, digital systems and networks quality of service and performance, (Ginebra, 2001).

[8] VASSEUR, *Jean-Philippe*, PICKAVET, *Mario,* DEMEESTER, *Piet*. Network recovery- protection and restoration of optical, SONET-SDH, IP and MPLS. Edición X. Oxford. Morgan Kauffman Publishers, 2004. 521 p.

[9] HUSSAIN, Iftekar. Fault-Tolerant IP and MPLS networks. Indianapolis. Cisco Press. 2005. 336 p.

[10] BARAKOVIC, Jasmina, BAJRIC, Himzo, HUSIC, Amir. Multimedia traffic analysis of MPLS and non-MPLS network. En: INTERNATIONAL SYMPOSIUM ELMAR. (48a: 2006: Zadar). pp 285-288.

[11] SAAHEL, Alouneh, AGARWAL, Anjali, EN-NOUAARY, Abdeslam. A novel approach for fault Tolerance in MPLS networks. En: INNOVATIONS IN INFORMATION TECHNOLOGY. (3a:2006:Dubai). pp.1-5

[12] BANIMELHEM, Omar, AGARWAL, Anjali ATWOOD, William. A new MPLS-based local failure recovery for multicast communication. En: IEEE/ACS INTERNATIONAL CONFERENCE ON COMPUTER SYSTEMS AND APPLICATIONS. (2006: DUBAI). pp 228-231.

[13] AVIZIENIS, Algirdas, LAPRIE, Jean-Claude, RANDELL, Brian, LANDWEHR, Carl. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions No 1, vol 1: 2004

[14] MARKOPOULOU, Athina, IANNACONNE, Gianluca, BHATTACHARYYA, Supratik, CHEN-NEE, Chuah. Characterization of failures in an IP backbone. En: INFOCOM 2004. (33: 2004: Hong Kong). pp. 2307-2317.

[15] AVIZIENIS, Algirdas, LAPRIE, Jean-Claude, RANDELL, Brian. Fundamental concepts of dependability. En: INTERNATIONAL WORKSHOP ISW 2000. (3ª: 2003: Cambridge)

[16] AMIN, Mina, KIN-HON, Ho, PAVLOU, George, HOWARTH, Michael. Improving survivability through traffic engineering in MPLS networks. En: COMPUTERS AND COMMUNICATION ISCC 2005. (10: 2005: Cartagena). pp. 758-763.

[17] MENTH, Michael, RUEDIGER, Martin, ULRICH, Spoerlein. Impact of unprotected multi-failures in resilient SPM Networks: a capacity dimensioning approach. En: GLOBAL TELECOMMUNICATIONS CONFERENCE: GLOBECOM 2006. (49: 2006, San Francisco). pp1-6.

[18] HUNDESSA GONFA, Lemma, DOMINGO-PASCUAL, Jordi. Optimal and guaranteed alternative LSP for multiple failures. En: COMPUTER AND COMMUNICATIONS AND NETWORKS ICCCN 2004 (13: 2004: Chicago).pp 59-64