ANÁLISIS DE LA INCIDENCIA DE FALLAS MÚLTIPLES EN REDES MPLS.

Monografía presentada como requisito para optar por el título de Ingeniero en Electrónica y Telecomunicaciones

WILLIAM GIRALDO SANDOVAL
RUBÉN DARÍO GUERRERO ENRÍQUEZ

Director: Ing. Oscar Josué Calderón Cortés

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones
Línea de Investigación: Gestión Integrada de Redes, Servicios y Arquitecturas de Telecomunicaciones
Popayán, Junio de 2009

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ECUACIONES

LISTA DE ACRÓNIMOS

IETF: Grupo deTrabajo en Ingeniería de Internet (Internet Engineering Task Force).
ITU: Unión Internacional de Telecomunicaciones (International Telecommunication Union).
IP: Protocolo de Internet (Internet Protocol).
TE: Ingeniería de Tráfico (Traffic Engineering).
QoS: Calidad de Servicio (Quality of Service).
IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers).
LDP: Protocolo de Distribución de Etiquetas (Label Distribution Protocol).
LSR: Enrutador de Conmutación de Etiquetas (Label Switching Router).
LSP: Trayecto de Conmutación de Etiquetas (Label Switched Path)
WP: Camino de Trabajo (Working Path)
BP: Camino de Respaldo (Backup Path)
LER: Enrutador de Etiquetas de Frontera (Label Edge Router).
PML: Enrutador de Combinación de Trayectos (Path Merge LSR).
PSL: Enrutador de Conmutación de Trayectos (Path Switch LSR).
FIS: Señal de Indicación de Fallas (Fault Indication Signal).
RT: Tiempo de Restablecimiento (Restoration Time).
PL: Pérdida de Paquetes (Packet Loss).
FEC: Clase de envío equivalente (Forwarding Equivalence Class).
AS: Sistema Autónomo (Autonomous System)
ATM: Modo de Transferencia Asíncrono (Asynchronous Transfer Mode)
MPLS: Conmutación de Etiquetas Multiprotocolo (MultiProtocol Label Switching)
GMPLS: Conmutación de Etiquetas Multiprotocolo Generalizado (Generalized Multi-Protocol Label Switching).
MTBF: Tiempo Medio entre Fallas (Mean Time Between Failures).
MTTR: Tiempo Promedio para Reparar (Mean Time To Repair).
RSVP: Protocolo de Reserva de Recursos (Resource Reservation Protocol).
BGP: Protocolo de Pasarela de Borde (Border Gateway Protocol).

INTRODUCCIÓN

Durante los últimos años el crecimiento de las redes de telecomunicaciones ha sido muy acelerado debido a la multiplicidad de servicios y aplicaciones que pueden soportarse sobre estas, y que sin duda alguna han brindado inmensas facilidades y capacidades a los usuarios para satisfacer sus necesidades de diversa índole, desde lo profesional y académico hasta lo recreativo. Esto sumado a la masificación que ha tenido Internet en todo el mundo, ha creado nuevas exigencias que han obligado a los operadores a mejorar la infraestructura de sus redes con el fin de garantizar las características de calidad de servicio (QoS: Quality of Service) que requieren los tráficos transportados por ellas.

Estas nuevas tendencias han llevado a muchos operadores a implementar sus redes basadas en la Conmutación de Etiquetas Multiprotocolo (MPLS MultiProtocol Label Switching) como tecnología de soporte en el núcleo de las mismas [1-3]. MPLS basa su operación en la combinación de la eficiencia y simplicidad del enrutamiento junto con las altas velocidades de la conmutación de paquetes [3-6], consolidándose como una alternativa tecnológica para el soporte de flujos de tráfico que exigen grandes capacidades de recursos de red, Calidad de Servicio (QoS: Quality of Service) garantizada y una alta disponibilidad de los mismos, además de las facilidades que tiene para el soporte de funcionalidades de ingeniería de tráfico que buscan la optimización y uso eficiente de los recursos de red [3]-[5-6].

Sin embargo, las redes MPLS así como cualquier otro tipo de red basada en el protocolo IP, son susceptibles a la ocurrencia de algún tipo de falla que pueda comprometer la integridad de la información transportada, degradando la QoS y conduciendo en los casos de mayor gravedad a la pérdida irreparable de información. Por estas razones, la ocurrencia de estos eventos constituye una seria amenaza para los intereses de los operadores de red, pues no solo pueden comprometer la integridad de los tráficos y en consecuencia los servicios y aplicaciones soportados por la red, sino que también pueden perjudicar las pretensiones económicas de los operadores al afectar la imagen que proyectan hacia sus clientes.

Cuando la ocurrencia de eventos de falla es inminente, es preciso que se tomen medidas pertinentes para contrarrestar su impacto. En este sentido, la aplicación de mecanismos de recuperación, que permitan brindar alternativas de enrutamiento para la conmutación de los tráficos que se vean comprometidos por fallas hacia caminos de respaldo, así como la adopción de medidas preventivas basadas en una plena caracterización de las causas y factores potenciales asociados con la ocurrencia de estos eventos, se constituyen en medidas significativas que permiten hacer frente a esta problemática, disminuyendo así sus consecuencias negativas sobre la red.

La medición del impacto de los eventos de falla permite a los operadores tener una idea clara sobre el grado de afectación que infligen los mismos a los tráficos y por tanto a los servicios soportados por la red. Su valoración puede realizarse con base a una serie de parámetros como la pérdida y desorden de paquetes, retardos, jitter, entre otros.

Esta monografía describe inicialmente conceptos y aspectos técnicos importantes de MPLS; después de esta sección se introduce el concepto de fallas en el nivel de infraestructura en estas redes. Luego se describe el panorama actual de fallas en las redes MPLS mediante la elaboración de un diagrama conceptual donde figuran los factores, causas, actores y demás entidades que intervienen en su aparición, proponiendo una clasificación de los diversos tipos de falla que pueden presentarse en el nivel físico. Posteriormente se define el concepto de fallas múltiples y su grado de dependencia.

Finalmente se definen los métodos de protección contra fallas, los cuales junto con la descripción de los parámetros de desempeño, sirven como referente para evaluar la respuesta de la red ante la ocurrencia de fallas. Luego se presentan los resultados de la simulación y su interpretación, a partir de los cuales se realiza el análisis del impacto ocasionado en los tráficos cursantes ante la presencia de fallas tanto de tipo simple como múltiple.

Este documento está integrado por 5 capítulos estructurados de la siguiente manera:

Capítulo 1. Generalidades y conceptos relacionados con la problemática de fallas en redes MPLS. Define aspectos técnicos de relevancia referentes a la arquitectura y funcionamiento de estas redes. Además se introduce el concepto de fallas y el impacto que éstas causan sobre los tráficos cursantes por la red.

Capítulo II. Análisis de la ocurrencia de fallas en redes MPLS. Describe el panorama de las fallas en redes MPLS a través de un diagrama conceptual, el cual tiene en cuenta los factores, causas y actores que conllevan a la ocurrencia de fallas simples y múltiples en estas redes. Posteriormente se define cómo se generan fallas en el nivel físico de la red y se analiza el grado de dependencia que existe entre ellas. Por último se describe el concepto de confiabilidad y sus atributos.

Capítulo III. Recuperación en redes MPLS. Este capítulo introduce el concepto de recuperación en redes MPLS y describe los modelos de protección y restablecimiento. Posteriormente se describe el funcionamiento de los métodos de protección y por último se presentan los parámetros de desempeño.

Capítulo IV. Simulación, pruebas y resultados. Describe la herramienta software de simulación seleccionada, el escenario de red y sus características. Además se especifican y describen las pruebas, los parámetros a evaluar, los resultados obtenidos y se

interpretan los mismos. Finalmente se realiza un análisis del impacto de fallas de tipo simple y múltiple sobre el tráfico transportado por la red.

Capítulo V. Conclusiones y Recomendaciones. En este capítulo se exponen las conclusiones derivadas de los resultados del proyecto y se dan una serie de recomendaciones para el desarrollo de futuros trabajos e investigaciones en este campo.

1. GENERALIDADES Y CONCEPTOS RELACIONADOS CON LA PROBLEMÁTICA DE FALLAS EN REDES MPLS.

Considerando la evolución que han experimentado las redes IP desde mediados de los años 90, así como el incremento de la competencia, el desarrollo de servicios y aplicaciones orientadas a satisfacer las necesidades específicas del usuario y las nuevas tendencias que apuntan hacia el uso de servicios de red que demandan gran cantidad de recursos, se han generado motivaciones que han llevado a gran la mayoría de operadores de red a la adopción de MPLS como la tecnología de soporte en el núcleo de sus redes [1-4].

MPLS basa su operación en la combinación de las funciones de enrutamiento (es decir, el control de la información sobre el tráfico en la red), y las funciones de direccionamiento (el envío de los datos entre elementos de red) que operan en planos separados [4-5]. MPLS soporta cualquier tipo de tráfico sobre una red IP, adaptándose a las tecnologías existentes de enrutamiento sin proponer ningún protocolo adicional [4-6]. El gran aporte de MPLS ha sido el incremento de la eficiencia en el procesamiento del encabezado de los paquetes en las redes IP, lo que ha permitido proporcionar nuevas aplicaciones de ingeniería de tráfico, diferenciación de servicios en distintas clases y establecimiento de redes privadas virtuales (VPNs: Virtual Private Networks); así como brindar todo el soporte para que aplicaciones actuales sobre redes IP funcionen de una manera eficiente [3-6].

Sin embargo, a medida que aumentan las capacidades y prestaciones de la red, la velocidad de los flujos de tráfico transportados y los servicios que estas soportan, se requiere de una gran infraestructura que sea capaz de brindar las condiciones necesarias que se exigen para su buen desempeño [6-8]. En este sentido, la presencia de eventos de falla[1] tanto de naturaleza simple como múltiple en el núcleo de la red puede afectar de forma notable la infraestructura de la red, perjudicando los flujos de tráfico cursantes y por ende alterando la calidad en la prestación de los servicios y aplicaciones soportados por la misma, lo cual redunda en la disminución de la credibilidad y los ingresos del proveedor de servicios, así como en la pérdida de valor de su marca o imagen [9-13].

En este capítulo se describen algunos aspectos técnicos relevantes sobre la arquitectura de MPLS, así como se introduce el concepto de fallas en estas redes para brindar una visión general de esta problemática, que sirve como soporte para abordar el desarrollo de los conceptos referentes a la ocurrencia de fallas y los mecanismos de recuperación para afrontarlas**.**

[1] Terminación de la habilidad de un elemento de red para llevar a cabo una función requerida [4]. 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.

1.1. ASPECTOS TÉCNICOS DE LA ARQUITECTURA EN REDES MPLS.

1.1.1. Descripción de la Arquitectura MPLS.

Acorde al RFC 3031 [14] un dominio MPLS se define como "*un conjunto de nodos contiguos que realizan enrutamiento y direccionamiento y los cuales se encuentran dentro de un dominio de enrutamiento o de un dominio administrativo*". La figura 1-1 muestra la representación de un dominio MPLS.

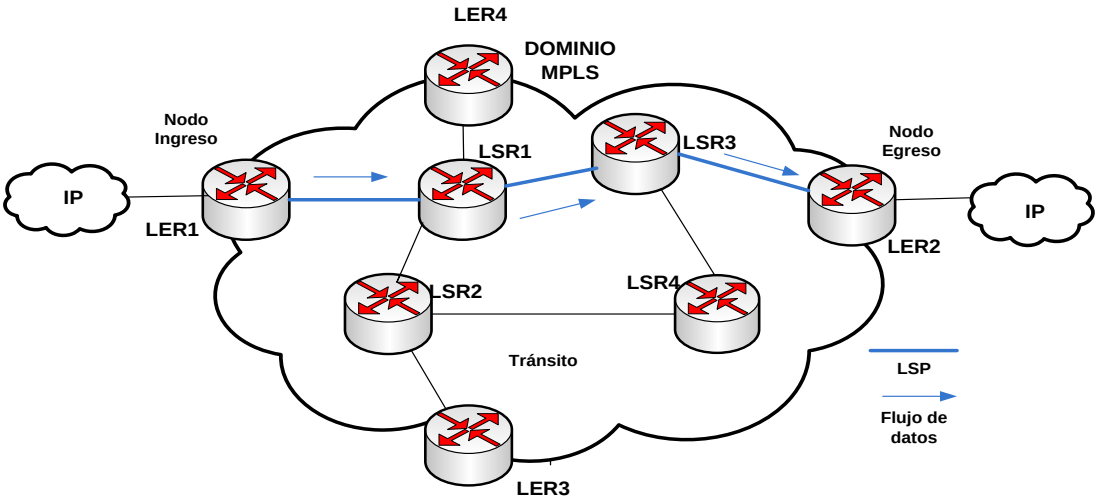


Figura 1-1. Dominio MPLS.

El dominio MPLS puede dividirse en dos áreas fácilmente reconocibles: el Núcleo MPLS (Core MPLS) y la Frontera MPLS (Edge MPLS) [16]. El núcleo está compuesto por nodos que operan únicamente con esta tecnología, mientras que en la frontera del dominio existen nodos que pueden interactuar con otros que no necesariamente soporten MPLS. Los nodos que hacen parte del núcleo de un dominio MPLS son llamados de forma general enrutadores de conmutación de etiquetas (LSRs: Label Switching Routers), los cuales realizan el proceso de intercambio de etiquetas y además participan en el establecimiento de los caminos por los cuales se direccionan los paquetes que se transportan a través de la red, usando para este fin protocolos de señalización de etiquetas, así como de conmutación del tráfico entre los trayectos establecidos. Los nodos del núcleo se denominan LSRs de tránsito, y los de la frontera enrutadores de etiquetas de frontera (LERs: Label Edge Routers), los cuales tienen la connotación adicional de ingreso o egreso, dependiendo si están al comienzo o final del dominio respectivamente y cuentan con interfaces que permiten su conexión con otro tipo de redes como las basadas en el Modo de Transferencia Asíncrona (ATM: Asynchronous Transfer Mode), Frame Relay, Ethernet, etc. Estos enrutadores encaminan el tráfico proveniente de otras redes y lo direccionan hacia el dominio MPLS, haciendo uso de un protocolo de señalización de etiquetas en el nodo de ingreso, y así mismo se encargan de distribuir el tráfico de vuelta a las redes externas en el nodo de egreso [15]-[16], jugando un papel muy importante en

la asignación y remoción de etiquetas cuando un paquete entra o abandona un dominio MPLS.

Los paquetes transportados a través de un dominio MPLS siguen un camino determinado en el LER de ingreso denominado trayecto conmutado de etiquetas (LSP: Label Switched Path), el cual depende de la Clase Equivalente de Envío (FEC:Forward Equivalence Class) que se le haya asignado en dicho punto. Cuando los paquetes llegan al LSR de ingreso, se clasifican en una determinada FEC, para luego direccionarse en el LSP correspondiente a dicha FEC, actuando como un filtro que define básicamente hacia qué LSPs se deben dirigir los paquetes [14]-[16-18].

MPLS cuenta con una serie de elementos especiales para hacer frente a la ocurrencia de eventos de falla en la red que puedan interrumpir el curso normal de los tráficos transportados. Dichos componentes integran lo que se conoce como dominio de protección MPLS, cuya comprensión es de gran relevancia para abordar los aspectos relacionados asociados con la ocurrencia de fallas y la aplicación de los mecanismos de recuperación en estas redes. A continuación se describen estos componentes.

1.1.2. Componentes del dominio de protección MPLS.

Un dominio de protección MPLS está conformado por un conjunto de LSRs sobre los cuales se despliega un camino activo o de trabajo, por el cual fluye el tráfico en condiciones normales, y por un camino de respaldo el cual direcciona el tráfico en caso de que un evento de falla tenga lugar en la red. Se debe contar adicionalmente con dos nodos con capacidades de protección especiales; un nodo LSR conmutador de rutas (PSL: Path Switch LSR), que conmuta el tráfico entre el camino activo y el de respaldo y otro LSR Combinador de rutas (PML: Path Merge LSR), que combina el tráfico de dichos trayectos [4]-[6-7]. Seguidamente se describe cada uno de estos elementos.

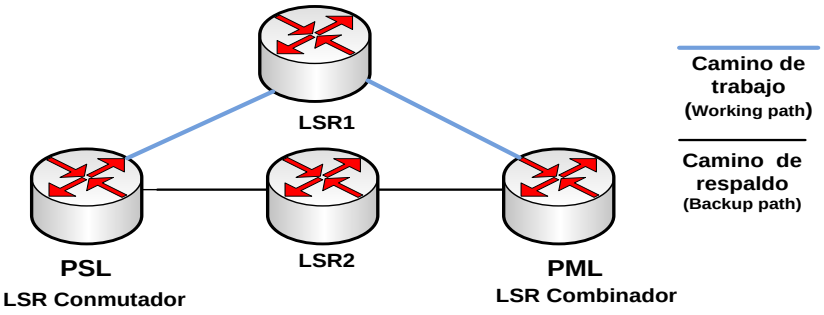


Figura 1-2. Dominio de protección MPLS

- ✓ **Camino de trabajo (WP: Working Path):** El camino activo, de trabajo, o primario, es el trayecto a través del cual fluye el tráfico en condiciones normales de la red. Este camino puede ser un segmento de un LSP o bien un LSP completo que requiere protección.

- ✓ **Camino de respaldo (BP: Backup path):** Es el trayecto hacia el cual se conmuta el tráfico tras la ocurrencia de un evento de falla en una red MPLS. Se conoce también como camino de respaldo, de protección o camino alterno.

- ✓ **LSR Intermedio:** Es cualquier LSR dentro del interior del camino de respaldo o del de trabajo que no es PML o PSL.

- ✓ **LSR Conmutador de Rutas (PSL: Path Switch LSR):** El PSL se encarga de la conmutación entre el camino de trabajo y el camino de recuperación, así como del redireccionamiento del tráfico en caso de falla.

- ✓ **LSR Combinador de Rutas (PML: Path Merge LSR):** El PML se encarga de combinar el tráfico proveniente de los caminos de recuperación y trabajo.

1.2. INCIDENCIA DE FALLAS EN REDES MPLS

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 [16]-[19-20]. 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 de los usuarios [19], repercutiendo también sobre la imagen y credibilidad del operador, sus intereses económicos, y el posicionamiento de sus servicios ofrecidos frente a la competencia.

Para los operadores de red es de gran importancia identificar los factores que conllevan a la aparición de fallas, así como la adopción de medidas preventivas pertinentes con el objetivo de reducir su frecuencia [20-21]. Si la ocurrencia de eventos de falla es inminente y las medidas tomadas no son suficientes, los operadores deben preocuparse por el impacto que estos eventos pueden tener sobre la infraestructura de la red, así como por las consecuencias sobre los tráficos transportados.

Para analizar la ocurrencia de fallas, es posible considerar sus repercusiones en varias capas, lo cual tiene un nivel de complejidad considerable debido a la gran cantidad de procesos de intercambio de información de señalización, protocolos, acciones de

enrutamiento, dispositivos físicos, entre otros que se deben tomar en cuenta para su análisis. Sin embargo en el presente proyecto solo se tienen en consideración eventos de falla en el nivel de infraestructura de red, es decir fallas en los dispositivos físicos como enrutadores y enlaces, y no se abordan problemas que se desencadenen en niveles superiores como los relacionados con protocolos de enrutamiento y el intercambio de mensajes de señalización entre otros. En este orden de ideas, un 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 un evento de falla múltiple involucra el mal funcionamiento de más de uno de estos elementos en la red.

Dentro de la temática de las fallas en redes MPLS, los eventos de falla múltiple se caracterizan por comprometer en mayor grado la infraestructura de la red en comparación con los de falla simple [19]-[21], ya que los primeros no solo pueden afectar los caminos de trabajo por los cuales fluyen los tráficos en condiciones normales de funcionamiento, sino que también afectan los caminos de respaldo empleados por los mecanismos de recuperación para su ejecución, quitándole a la red la capacidad de contrarrestar las consecuencias que acarrean la presencia de las fallas.

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 [19]-[22]. 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 [4][19]-[23]. Los más representativos son el tiempo de restablecimiento, la pérdida y el desorden de paquetes, el retardo y 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 [22-23]. Sin embargo, existen algunas restricciones respecto a los rangos de valores permitidos para estos criterios que permiten garantizar la QoS de servicios y aplicaciones como se describe en la recomendación G.1010 [24].

La mayoría de estudios realizados hasta la fecha sobre el impacto de fallas en redes MPLS se han enfocado en contextos de falla simple, y sobre los cuales se han aplicado mecanismos para la recuperación efectiva de los tráficos comprometidos [12]. Es por tanto de interés realizar un análisis en contextos de falla múltiple en el que se puedan evaluar alternativas de recuperación, así como una valoración del impacto que tiene la ocurrencia de más de un evento de falla sobre distintos tipos de tráfico, en términos de los parámetros de desempeño mencionados.

El presente capítulo define algunos aspectos técnicos de la tecnología MPLS, introduciendo además los elementos que guardan relación con la protección en estas

redes. Adicionalmente se presenta la problemática del proyecto, resaltando la importancia que tiene el análisis de fallas en MPLS, así como la medición del impacto de las mismas sobre la red.

Seguidamente en el capítulo 2 se amplía el panorama de las fallas en las redes MPLS mediante la elaboración de un diagrama conceptual que describe las causas, los actores involucrados, y demás factores relacionados con la ocurrencia de eventos de falla, además de introducir formalmente el concepto de fallas múltiples y su grado de dependencia.

2. ANÁLISIS DE LA OCURRENCIA DE FALLAS EN REDES MPLS.

En los últimos años la demanda de nuevos servicios y aplicaciones basadas en redes MPLS ha crecido de forma significativa, así como los requisitos técnicos y capacidades que estos exigen para su funcionamiento, los cuales llevan constantemente a las redes a sus límites. En estas condiciones, las repercusiones que tiene una interrupción en el servicio debido a una falla en la red son severas, ya que no solo conducen a la pérdida considerable de datos e información, sino que también inciden negativamente sobre los ingresos y la imagen del proveedor de servicios [1][4]-[25-28].

En este capítulo se realiza un estudio sobre el panorama de las fallas en redes MPLS, mediante la elaboración de un marco conceptual que reúne las características más importantes que permiten abordar la problemática desde diferentes puntos de vista, teniendo en cuenta para ello los factores, causas y actores que intervienen en su aparición, y que al mismo tiempo permiten clasificar los diversos tipos de falla que pueden presentarse en la red. Así mismo, se define la forma en que se generan las fallas en el nivel físico y se analiza el grado de dependencia que existe entre ellas. Finalmente se presenta el concepto de confiabilidad y sus atributos.

2.1. MARCO CONCEPTUAL DEL PROBLEMA DE FALLAS EN REDES MPLS.

En la actualidad hay un aumento notable en el número de usuarios que demandan aplicaciones y servicios de nueva generación, así como también se ha incrementado su nivel de sofisticación y requerimientos de recursos de red, exigiendo mayores capacidades hardware y software para su funcionamiento. En estas condiciones la ocurrencia de eventos de falla tiene repercusiones considerables, pues una falla en enlaces de alta velocidad o dispositivos críticos puede conducir a una tasa importante de pérdidas de información, degradando de manera considerable la calidad de los servicios prestados por la red, además de que su proceso de identificación se torna más complejo [21]-[26-29].

A pesar de que las redes MPLS están expuestas a la ocurrencia de eventos de falla, los dispositivos y enlaces que las componen cuentan con un alto grado de robustez [13]-[30], generalmente disponen de altas capacidades de recursos de red y están dotadas con mecanismos de recuperación cuya eficacia ha sido comprobada en contextos de falla simple. Sin embargo, el funcionamiento de la red continúa siendo afectado por diversos tipos de fallas, por lo que es de gran relevancia para los operadores de red identificar los factores relacionados con la ocurrencia de las mismas, los actores involucrados, y las causas, de manera que se puedan adoptar medidas preventivas para preservar la integridad de la red [21]-[32-33].

No hay un consenso entre las propuestas realizadas por algunos autores respecto a la identificación de los factores que están asociados con la ocurrencia de eventos de falla simple y múltiple en MPLS [21]-[28]. La dificultad para realizar dicha identificación radica en la existencia de diversos enfoques que permiten abordar la problemática, y al hecho de que estos pueden presentar elementos en común para su análisis, haciendo difícil la elaboración de una caracterización con base a factores fácilmente reconocibles y excluyentes entre sí, generando en consecuencia incoherencias y problemas de interpretación. Así mismo, es complejo identificar y clasificar plenamente las causas y los tipos de eventos de falla que pueden tener lugar en la red, debido a la multiplicidad de elementos que intervienen en su aparición [21]-[28].

A continuación se propone un marco conceptual, basado en las propuestas realizadas en [21][28-29]-[34], que permite abordar desde diferentes puntos de vista la problemática de las fallas simples y múltiples en redes MPLS, así como los factores relacionados con su ocurrencia. Mediante la elaboración de preguntas específicas se plantea un punto de partida para la determinación de cuatro enfoques como sigue:

2.1.1. Qué produce la falla?

Este enfoque está asociado directamente con las causas que desencadenan eventos de falla en las redes MPLS y para lo cual, de acuerdo con los actores que intervienen en la ocurrencia de las mismas se clasifican de la siguiente forma:

2.1.1.1. Acción del hombre sobre el hardware y software de la red.

A esta categoría pertenecen las actividades u operaciones que ejecuta directamente el hombre y que conducen a la aparición de fallas dentro de la infraestructura de red. En este grupo entran en consideración las acciones llevadas a cabo por el personal que trabaja en la red, así como por individuos ajenos a su operación [21]-[34-35].

Se plantea una distinción de acuerdo a la intención que enmarca la realización de dichas acciones de la siguiente manera:

- ✓ **Voluntarias:** Se refiere a todas las actividades relacionadas con la ejecución de procedimientos de operación y mantenimiento, y en general, a todo tipo de acciones realizadas de manera premeditada y que afectan el desempeño de la red [21]-[28-29].

  Entre los procedimientos más comunes asociados que se llevan a cabo se encuentran:

  - Labores de mantenimiento de los componentes hardware que conforman la infraestructura de red, que incluyen el mantenimiento de los enlaces, LSRs, interfaces de red, etc. Así mismo, implican el reemplazo de componentes

defectuosos o antiguos por otros cuyo rendimiento sea superior.

- Mantenimiento de la(s) fuente(s) de suministro de energía, tales como generadores eléctricos y fuentes de poder ininterrumpidas (UPS: Uninterrumpible Power Supply), así como los procedimientos de análisis de la calidad en el suministro de potencia.

- Rutinas de análisis y medición del desempeño del estado actual de la red, las cuales incluyen la evaluación de los protocolos de enrutamiento, el funcionamiento correcto de los dispositivos, el estudio del comportamiento del tráfico cursante y de las técnicas de ingeniería de tráfico entre otros.

- Trabajos de actualización y reinstalación del software de control y gestión de los dispositivos hardware de la red, los cuales pueden presentar problemas relacionados con la configuración incorrecta de los equipos e incompatibilidades causadas por la instalación incorrecta de actualizaciones entre otros. Cabe resaltar que la mayoría de las fallas asociadas al desempeño del sistema operativo instalado en los enrutadores se deben principalmente a problemas de configuración y no a defectos en el software [36].

- Acciones ejecutadas de manera intencional que atentan contra el correcto funcionamiento del sistema. Los objetivos de estas acciones implican generalmente la interrupción de los servicios soportados por la red, cortes e interrupciones en los nodos y enlaces de la red, la modificación de la configuración del sistema y el acceso a información confidencial de manera no autorizada. Entre estas actividades se distinguen los ataques en el plano de control y de envío, rastreo de paquetes y ataques de denegación del servicio (DoS: Denial of Service). Para ofrecer un buen nivel de confiabilidad y seguridad en redes MPLS, estas se deben equipar con mecanismos o técnicas de defensa apropiadas, tales como el filtrado de paquetes, la instalación de cortafuegos (firewalls), técnicas de detección y prevención de intrusos, autenticación y la encripción de datos [21]-[36].

Es obligación de los operadores de red adoptar medidas efectivas con miras a reducir el impacto negativo que estos procedimientos tienen sobre la red, tales como la notificación con antelación a los usuarios sobre una futura interrupción en el servicio y la programación de los procedimientos en horarios en los cuales el uso de los servicios prestados por la red sea bajo, como en horas nocturnas y en fines de semana, de manera que su grado de afectación sea mínimo [21]-[34].

✓ **Involuntarias:** Se refiere a acciones ejecutadas sin intención y que requieren especial atención por parte del operador de red para minimizar su ocurrencia, especialmente en lo que concierne a la capacitación del personal que trabaja en la empresa y a la

atención oportuna en caso de que estas se presenten [28]-[34]. Pueden afectar tanto componentes hardware como software de la red. Se propone la siguiente clasificación:

- **Accidentales:** Se refiere a acciones no premeditadas que producen fallos en la red y cuya ocurrencia obedece a errores en los procedimientos realizados por el personal de la red y por individuos ajenos a la misma.

- **Por incompetencia:** Comprende las actividades que puedan producir fallos en la red asociadas a la falta de capacitación, profesionalismo, así como negligencia por parte de los operadores de red, quienes no actúan de forma oportuna frente eventos imprevistos que puedan tener repercusiones negativas sobre su normal funcionamiento.

2.1.1.2. Acciones de la naturaleza.

A esta categoría pertenecen los fenómenos de la naturaleza que afectan los componentes de la red. Estos eventos pueden llegar a ser muy violentos y de gran poder destructivo, por lo tanto pueden comprometer significativamente su operación [21].

Es necesario que se tomen medidas preventivas por parte de los operadores de red, de manera que sus componentes más delicados cuenten con la protección necesaria en sus instalaciones y que no resulten expuestos a la ocurrencia de alguno de los fenómenos mencionados. Entre los fenómenos más relevantes se encuentran [27][30]-[37]:

- ✓ Desastres naturales como terremotos, tsunamis, huracanes, tifones, aludes, erupciones volcánicas e inundaciones entre otros, capaces de comprometer en alto grado la mayoría de los elementos que conforman la red como LSRs, enlaces de fibra óptica, interfaces de red y demás infraestructura de transporte.

- ✓ Sobrecargas y daños en los equipos de suministro de energía causados por tormentas eléctricas, que pueden provocar la ocurrencia de transientes de voltaje y picos de energía que pueden afectar gravemente los dispositivos de red si no se cuenta con las medidas de protección adecuadas.

- ✓ Procesos naturales y condiciones ambientales adversas que pueden causar desgaste sobre los componentes de red, tales como la corrosión, humedad, periodos temporales de frío o calor extremo, y presencia de radiaciones entre otros eventos que afectan el tiempo de vida útil de los componentes.

2.1.2. Cómo se presenta la falla en la red ?

Este enfoque hace alusión al nivel de compromiso que existe en la red de acuerdo al número de nodos y enlaces que resulten afectados a raíz de la ocurrencia de eventos de falla. Con base en lo anterior se propone una clasificación como sigue:

2.1.2.1. Fallas individuales.

Se refiere a fallos que afectan únicamente un nodo o enlace en la red MPLS. Generalmente son eventos aislados y su ocurrencia puede deberse a fallos en los componentes electrónicos de los dispositivos, cortes en los enlaces, fallos en las interfaces o bien pueden presentarse a nivel lógico, debido a los procesos de nivel tres que realizan los enrutadores y que están asociados con el funcionamiento propio de la tecnología MPLS [28]-[34].

2.1.2.2. Fallas simultáneas.

A diferencia de las fallas individuales, las fallas simultáneas se refieren a eventos en los cuales resulta afectado más de un componente en la red (LSRs y/o enlaces) y cuya ocurrencia tiene lugar en el mismo momento. En la práctica se considera que dos eventos de falla son simultáneos si su detección ocurre exactamente en un mismo instante de tiempo.

2.1.2.3. Fallas superpuestas.

De manera similar a como ocurre en las fallas simultáneas, las fallas superpuestas se refieren a eventos en los que resulta comprometido más de un componente en la red. Son eventos que comienzan y terminan dentro de una misma ventana de tiempo, que usualmente dura unos pocos segundos. A manera de ejemplo, si se presenta una falla en un nodo compartido por dos enlaces, se producirá en consecuencia una falla en dichos enlaces. Sin embargo la detección de las mismas no ocurre de forma simultánea, debido a que el proceso de notificación de las fallas es complejo e involucra varios temporizadores y mensajes de señalización, que por lo general introducen retardos del orden de los milisegundos [28]-[38].

Lo anterior implica que la ocurrencia de fallas simultáneas es algo conceptual, debido a la complejidad del proceso asociado a la notificación de las mismas.

2.1.3. Qué recursos de la red se afectan ?

Este enfoque es muy general y pretende abarcar mediante la división en dos grupos (hardware y software) los recursos de la red que están expuestos a la ocurrencia de eventos de falla como se presenta a continuación:

2.1.3.1. Hardware.

Se refiere a los eventos de falla que afectan los componentes hardware de la red como fibras, conectores, interfaces, puertos de red y en general todos los componentes físicos de la red [28]-[35].

2.1.3.2. Software.

Describe todas las fallas y errores que comprometen el software de operación, gestión y control de las redes. Obedecen a problemas de enrutamiento, ataques de hackers, problemas de instalación, entre otros [28]. También están asociados con fallas en el plano de control del nivel tres.

2.1.4. Dónde se producen ?

Este enfoque está asociado al lugar donde ocurren las fallas respecto a las fronteras de la red, es decir, si se desarrollan en su interior o bien por fuera de su infraestructura y que tienen repercusiones hacia su interior [34]-[38]. Con base en lo anterior, se tiene la siguiente clasificación:

2.1.4.1. Fallas internas.

Se refiere a aquellas fallas que ocurren en el interior de la red. Pueden estar asociadas a problemas en los nodos o en los enlaces, errores de diseño, defectos en los componentes electrónicos, interrupciones en el fluido eléctrico de las fuentes de potencia, etc. Muchas de las acciones y fallas mencionadas anteriormente entrarían dentro de esta clasificación como por ejemplo fallas en los nodos, en los enlaces, fallas de operación y mantenimiento, entre otras.

2.1.4.2. Fallas externas.

Se generan fuera de la red y sus efectos causan repercusiones sobre el funcionamiento interno de la misma. Pueden propagarse hacia el interior de la red y ocasionar fallos en la infraestructura física. Involucran actos de guerra, vandalismo, terrorismo, accidentes por colisiones de objetos a gran velocidad, fenómenos de la naturaleza, entre otros. Sin

embargo desde la perspectiva de la ingeniería es más interesante el análisis de las fallas internas.

La figura 2-1 presenta el diagrama conceptual propuesto de fallas en redes MPLS.

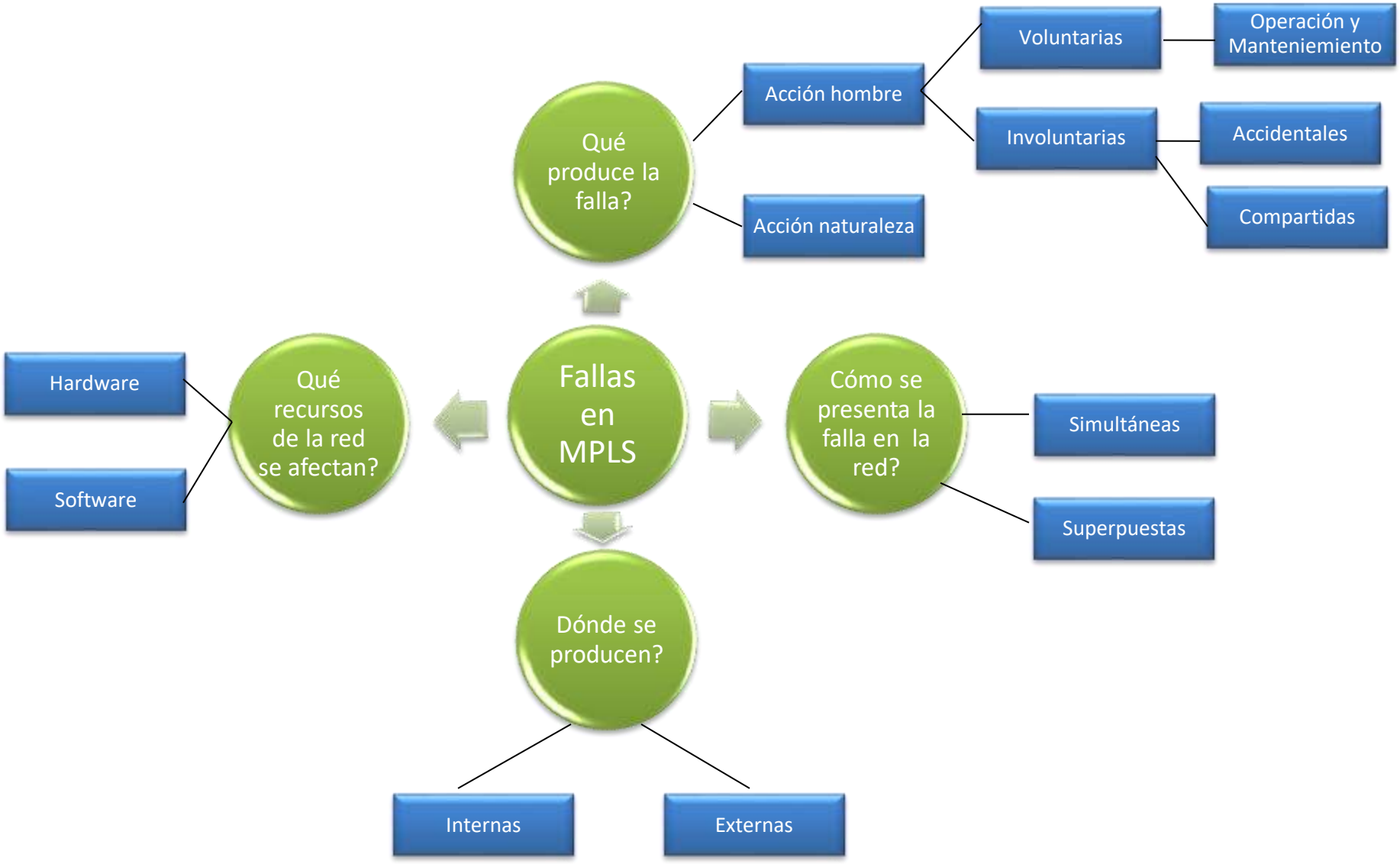


Figura 2-1. Diagrama conceptual de fallas en redes MPLS.

2.2. FALLAS MÚLTIPLES EN REDES MPLS.

Se definen las fallas múltiples en redes MPLS como 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, comprometiendo de esta manera su correcto funcionamiento [1]-[25-26]. La ocurrencia de dichos eventos puede atribuirse a cualquiera de las causas que se presentaron en el marco conceptual [16]-[34-35].

Las fallas múltiples en el nivel de infraestructura en las redes MPLS hacen alusión a eventos de falla que se presenten en los dispositivos físicos que conforman la red, específicamente LSRs y enlaces conforme se presentaron en la sección 2.1.2. La tabla 2-1 describe cómo se pueden presentar estos eventos.

Elementos de red involucrados	Descripción de la falla
LSR-LSR	Este evento de falla múltiple hace relación a dos o más LSRs que fallen en una red MPLS de manera simultánea o en un mismo lapso de tiempo.
Enlace-LSR	En este evento de falla, se ven comprometidos un enlace y un LSR cualquiera dentro de una red MPLS. Lo anterior se extiende para combinaciones entre nodos y enlaces para más de dos evento de falla.
Enlace-Enlace	Se refiere a fallos en dos o más enlaces que conforman la red MPLS.
Enlace/LSR- Nivel superior	A partir de la ocurrencia de una falla en un enlace o en un nodo, podrían resultar afectados procesos que se llevan a cabo en otros niveles, y que son propios del funcionamiento de la tecnología MPLS, como por ejemplo, el intercambio de mensajes de señalización, acciones de enrutamiento, establecimiento de trayectos, entre otros.

Tabla 2-1. Elementos de red involucrados en eventos de falla múltiple en el nivel físico.

A pesar de las diferentes combinaciones de elementos de red que se pueden ver afectados por los eventos de falla, en la práctica es más frecuente que se presenten fallas en los enlaces, debido a que las redes actuales generalmente presentan redundancia en sus nodos y por tanto la probabilidad de que estos fallen es muy baja [21][30]-[34].

2.2.1. Dependencia entre eventos de falla en redes MPLS.

La dependencia de fallas en redes MPLS hace alusión a la relación que existe entre la ocurrencia de dichos fenómenos cuando tienen lugar en la red [39-40]. A partir de la ocurrencia de un primer evento falla, podría inferirse que el desarrollo de fallas subsiguientes guarde alguna relación con este suceso, y por tanto habría algún grado de dependencia, que expresa el nivel de relación entre dichos eventos [21]-[41]. En términos probabilísticos, esto se puede expresar como la probabilidad de que ocurra un fallo en la red dado que otro fallo tuvo lugar en la misma.

Tras la ocurrencia de una falla a nivel físico en la red, podrían resultar afectados algunos de los procesos que se llevan a cabo en otros niveles, y que son propios del funcionamiento de la tecnología MPLS como por ejemplo, el intercambio de mensajes de señalización, acciones de enrutamiento, establecimiento de trayectos, entre otros [41-42]. Bajo estas condiciones se puede decir que hay dependencia entre la falla a nivel físico y los problemas generados sobre dichos procesos. Sin embargo, el análisis de la dependencia desde esta perspectiva se sale del alcance del presente documento, puesto que no describe la relación entre fallas en el nivel físico e involucra procesos que no se desarrollan en dicho nivel [30]-[34].

Para efectos del análisis de la dependencia de fallas a nivel físico, las cuales están asociadas con daños de tipo hardware que pueden ocurrir en la infraestructura de la red, como fallos en los enrutadores, cortes en las fibras, problemas en los puertos e interfaces de red entre otros, se considera que tanto los nodos como los enlaces son independientes entre sí [30]-[34]. Esto implica que tras la ocurrencia de un primer evento de falla en la red, eventos subsiguientes en otros dispositivos no guardan ninguna relación con la ocurrencia del primero.

En general, la dependencia entre dos eventos de falla en la red se puede expresar como la probabilidad de que ocurra un evento X dado que un evento Y tuvo lugar previamente, de acuerdo con la siguiente ecuación [21]-[42-43].

$$P(X|Y) = \frac{P(X \cap Y)}{P(Y)}$$

Ecuación 2-1. Probabilidad condicional entre dos eventos de falla.

La anterior ecuación corresponde a la probabilidad condicional entre las fallas X y Y, y de una manera sencilla permite medir la relación entre dos eventos de falla en la red. Sin embargo, de acuerdo a la consideración que se realizó, se tiene que hay independencia entre la ocurrencia de las mismas. Por lo tanto la ecuación 2-1, se expresa como:

$$P(X|Y) = \frac{P(X).P(Y)}{P(Y)}$$

$$P(X|Y) = P(X)$$

Ecuación 2-2. Probabilidad de falla cuando hay independencia.

Para ilustrar mejor el concepto de independencia entre dispositivos de red, se plantean a continuación tres casos para los cuales se calcula la disponibilidad[2] total del enlace, que se representa como la probabilidad de que la información proveniente del punto A alcance el punto B. Dicha probabilidad se expresa en términos de las disponibilidades de los LSRs como se presenta a continuación [16][30]-[34].

Caso A.

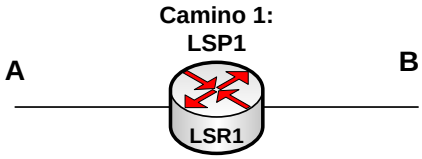


Figura 2-2. Camino de estudio caso A.

En este caso, la disponibilidad de la red se define como la probabilidad de que el LSP1 se encuentre en estado operativo. Esto se puede expresar mediante la ecuación:

$$D = P_{LSP1} = P(LSR1)$$

Donde P_{LSP1} = Probabilidad de que el LSP1 se encuentre en estado operativo.
$P(LSR1)$= Probabilidad de que el LSR1 se encuentre en estado operativo

Caso B.

Considérese el siguiente camino compuesto por dos LSRs de la siguiente manera.

[2] El concepto de disponibilidad define la probabilidad de que un sistema permanezca en estado operativo en un instante de tiempo dado. En la sección 2.3.1.1 se profundiza sobre concepto.

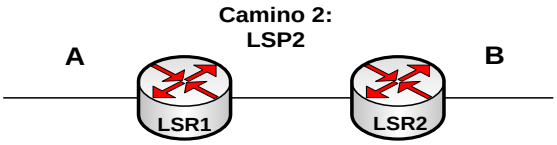


Figura 2-3. Camino de estudio caso B.

La disponibilidad del camino descrito en la figura 2-3, está dada por:

$$D = P_{AB} = P(LSR_1 \cap LSR_2)$$

$$P_{AB} = P(LSR_1).P(LSR_2)$$

Donde P_{AB} = Probabilidad de que el LSP2 se encuentre en estado operativo.

Caso C.

Para este caso se considera la siguiente topología:

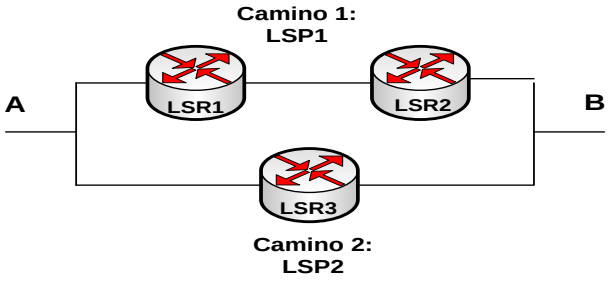


Figura 2-4. Topología caso C.

Usando el complemento se tiene que la probabilidad de que la información llegue del punto A al punto B está dada por:

$$D = P_{AB} = 1 - P_{AB}'$$

La disponibilidad del camino 2 se expresa en función de la indisponibilidad del mismo, es decir, la probabilidad de que la información no llegue de manera exitosa desde el punto A hasta el punto B o la probabilidad de que tanto el LSP1 como el LSP2 no operen de manera adecuada.

$$P_{AB}' = P\{LSP1' \cap LSP2'\},$$

Donde P_{AB}' = Probabilidad de que la información proveniente de A no llegue a B.

Extendiendo la consideración de independencia para los caminos en cuestión se tiene que:

$$P_{AB}' = P\{LSP_1'\}.P\{LSP_2'\}$$

Donde $P\{LSP_1'\}$ = Probabilidad de que el LSP1 se encuentre en estado no operativo.
$P\{LSP_2'\}$ = Probabilidad de que el LSP2 se encuentre en estado no operativo.

Aplicando nuevamente el complemento en la anterior ecuación se tiene:

$$P_{AB}' = [1 - P(LSP_1)].[1 - P(LSP_2)]$$

Con base en los resultados de los casos A y B, se obtiene:

$$P_{AB}' = [1 - P(LSR_1).P(LSR_2)].[1 - P(LSR_3)]$$

Finalmente para calcular la disponibilidad total, se aplica el complemento a la ecuación anterior, obteniendo lo siguiente:

$$P_{AB} = 1 - [1 - P(LSR_1).P(LSR_2)].[1 - P(LSR_3)]$$

A partir de esta expresión se puede deducir que para que la información no llegue desde A hasta B se requiere que fallen ambos trayectos y en tal caso la disponibilidad sería cero. Así mismo, se puede deducir que la probabilidad de falla de un trayecto no tiene nada que ver con la probabilidad de falla del otro, de acuerdo a la consideración realizada.

Este análisis se puede realizar mediante el uso de las disponibilidades individuales de los diferentes nodos o enlaces, o bien usando las probabilidades de fallas de los mismos. En la práctica, es complicado calcular la probabilidad exacta de falla de un enlace o un nodo, por esto, los ISPs asignan estos valores de acuerdo a su propia experiencia haciendo uso de información estadística [21]. Se pueden realizar también aproximaciones con base en características de los enlaces físicos que se estén utilizando, de los nodos de la red, de su distribución geográfica, entre otros [42]-[44-46]

2.3. CONCEPTO DE CONFIABILIDAD EN REDES MPLS.

En una red MPLS, uno de los objetivos primordiales es que los flujos de tráfico que se inyectan a la red a través de los nodos de ingreso puedan atravesarla de manera exitosa siguiendo una ruta o LSP definido, hasta llegar finalmente al LER de egreso, garantizando de esta forma la prestación adecuada de los servicios y aplicaciones soportadas por la red [8]-[47-48].

Para lograr este propósito, es necesario que todos los componentes de la red por los cuales fluye el tráfico se encuentren en óptimo estado de funcionamiento. Dentro de este contexto, para describir la habilidad y propiedades de una red para encaminar el tráfico correctamente y brindar al mismo tiempo servicios y aplicaciones robustas y confiables, se recurre al concepto de confiabilidad [4][30]-[34].

La confiabilidad es un término que define la capacidad de una red para evitar la aparición de fallas y controlar los efectos adversos asociados a su presencia, buscando de esta forma brindar servicios y aplicaciones de alta calidad [21][34]-[46]. La confiabilidad a su vez reúne una serie de atributos usados comúnmente en este contexto, estos son la disponibilidad, la fiabilidad, la mantenibilidad, la integridad y la supervivencia. La disponibilidad se distingue porque es un atributo observable y cuantificable, que puede caracterizarse matemáticamente, mientras que los otros se utilizan para describir el funcionamiento de la red en términos no cuantitativos [21]-[36].

Es de interés conocer de manera precisa cuál es el grado de confiabilidad que en conjunto ofrece una red MPLS [36], debido a que tal información es de utilidad para determinar cuáles dispositivos están más propensos a sufrir averías, permite definir las rutas más seguras a través de las cuales se puede dirigir los tráficos de mayor prioridad o importancia y también porque sirve como referente para adoptar medidas correctivas en aras de aumentar la robustez y seguridad total que ofrece la red. A continuación se explican las características de los atributos mencionados.

2.3.1. Atributos asociados a la confiabilidad en redes.

2.3.1.1. Disponibilidad.

La disponibilidad en redes de telecomunicaciones define la probabilidad de que un sistema o componente permanezca en estado operacional en un instante de tiempo dado o en cualquier instante de tiempo dentro de un intervalo [30][34]-[45].

La disponibilidad de los dispositivos hardware se puede medir mediante la observación detallada de su desempeño, teniendo en cuenta el tiempo que estos equipos permanecen en estado operativo así como el tiempo transcurrido desde que dicho elemento sufre una

avería hasta que vuelve a estar en estado normal de funcionamiento, tomando como referencia para dicho análisis un periodo de tiempo determinado [21]-[30].

Dentro del contexto de un dominio MPLS, dados los valores de disponibilidad de una serie de elementos que conforman un camino o LSP, su disponibilidad total se puede calcular mediante el producto de las disponibilidades individuales de todos los dispositivos y enlaces de red que lo componen [30]-[34], tal como se presenta en la ecuación 2-3:

$$A_n = A_1.A_2.A_3.A_4 \dots A_n$$

Ecuación 2-3. Disponibilidad total de un LSP.

Donde $\mathrm{A_n} =$ Disponibilidad de un LSP como producto de las disponibilidades individuales de los elementos que lo conforman.

A manera de ejemplo, se da el caso de los equipos de red usados en el núcleo de los operadores de red, cuya disponibilidad se ha establecido por el orden de 0.99999, lo cual quiere decir que estos dispositivos deben funcionar normalmente el 99.999% del tiempo.

De forma análoga, se define la indisponibilidad como la probabilidad de que un elemento de red se encuentre en estado no operativo [34]-[39]. Se representa matemáticamente mediante la siguiente expresión.

$$\mathrm{I} = 1 - \mathrm{A}$$

Ecuación 2-4. Indisponibilidad de la red**.**

Donde $\mathrm{I} =$ Indisponibilidad de la red o componente.
$\mathrm{A} =$ Disponibilidad de la red o componente.

Los dispositivos que conforman una red de telecomunicaciones tienen un ciclo de vida en cuya duración pueden experimentar varias fallas, lo cual conlleva a que la condición de los dispositivos este alternándose entre los estados de operación normal y el estado de falla [30][34]-[41]. La indisponibilidad de un elemento de red se puede expresar en términos del tiempo durante el cual este se encuentra en estado operativo así como del periodo de tiempo necesario para corregir la falla una vez se haya producido. Estos valores se usan para obtener el comportamiento temporal de un elemento de red de manera probabilística, cuya definición formal está dada por los siguientes parámetros [30][34]-[49-50]:

- ✓ **Tiempo medio entre fallas (MTBF: Mean Time Between Failures):** Especifica la duración promedio del intervalo de tiempo que transcurre entre dos eventos de falla consecutivos del mismo elemento de red.

- ✓ **Tiempo promedio para reparar (MTTR: Mean Time To Repair):** Describe el tiempo promedio necesario para tomar las medidas correctivas tendientes a la reparación de un elemento de red. Específicamente, el MTTR comprende el tiempo que tardan las operaciones de detección de la falla, el diagnóstico, su posterior reparación y puesta a punto del elemento averiado.

Una vez definidos estos términos, la indisponibilidad de un elemento de red se puede expresar mediante las siguientes ecuaciones [30]-[34]:

$$I = \frac{MTTR}{MTBF + MTTR}$$

Ecuación 2-5. Indisponibilidad de un elemento de red.

En la siguiente expresión se asume que la duración del MTBF es mucho mayor que la del MTTR, lo cual se cumple para la mayoría de los elementos de red [30][34]-[41].

$$I = \frac{MTTR}{MTBF}$$

Ecuación 2-6. Cálculo de la indisponibilidad de un elemento de red cuando MTBF >> MTTR**.**

Luego, a partir de la ecuación 6 la disponibilidad se define mediante la siguiente expresión:

$$A = 1 - \frac{MTTR}{MTBF}$$

Ecuación 2-7. Disponibilidad de un elemento de red cuando MTBF >> MTTR**.**

Esta definición se basa en el comportamiento estadístico de cada componente, cuyos valores son estimados mediante análisis y observaciones previas de su funcionamiento.

Se deduce de la anterior ecuación que si se incrementa el valor del MTBF y se disminuye el MTTR de un componente de red o de un sistema, se obtendrá como resultado un aumento en su disponibilidad. Esto se consigue al aumentar la calidad y robustez de sus componentes software como hardware. De forma similar, al aumentar la disponibilidad de los elementos como los LSRs, enlaces y la infraestructura de transporte en general, se obtiene en consecuencia un incremento en la disponibilidad total de la red [30][34]-[49-51].

2.3.1.2. Fiabilidad.

Se define como la probabilidad de un elemento de red (nodo o enlace) para estar en estado de operación bajo unas condiciones determinadas durante un periodo de tiempo dado. Por lo tanto se considera fiable a una red que se desempeña adecuadamente durante dicho intervalo [34]-[52]. En términos matemáticos, la fiabilidad se puede despejar a partir de la siguiente ecuación:

$$MTBF = \int_0^\infty R(T)dt$$

Ecuación 2-8. MTBF en función de la fiabilidad.

Donde $MTBF =$ Tiempo medio entre fallas.
$R(T) =$ Fiabilidad de un elemento de red en función del tiempo de funcionamiento sin fallas del mismo.

De donde se obtiene:

$$R(T) = e^{(-\frac{T}{MTBF})}$$

Ecuación 2-9. Fiabilidad en función del tiempo de funcionamiento sin fallas.

Donde $T =$ Tiempo en horas en que el componente opera sin ningún tipo de falla.

2.3.1.3. Mantenibilidad.

Es un concepto asociado a los cambios que tienen lugar en las redes de telecomunicaciones, entendiéndose como la capacidad de adaptación de la red a expansiones, renovaciones, reparaciones y actualizaciones a nivel software y hardware que se lleven a cabo en la misma, sin que haya interrupciones apreciables sobre el servicio [21]-[46]. A pesar de que muchos de los cambios que se realizan en la red se llevan a cabo de manera planeada, si no se toman las medidas necesarias por parte de los operadores de red, podría haber interrupciones considerables sobre el servicio prestado [29].

2.3.1.4. Integridad.

Es la habilidad de una red para proporcionar la calidad de servicio (QoS: Quality of Service) deseada a los servicios tanto en escenarios sin presencia de fallas, como en escenarios con presencia de fallas simples y múltiples [29][34]-[46].

2.3.1.5. Supervivencia de red.

Es la habilidad que tiene la red para recuperar el tráfico cuando se presenta un evento de falla, ocasionando pocas o ninguna consecuencia sobre los usuarios [45-46]. Alcanzar la sobrevivencia absoluta en una red MPLS es imposible debido a que estas redes no están exentas a la ocurrencia de fenómenos de gran magnitud como terremotos, explosiones, atentados, entre otros, que podrían afectar significativamente el desempeño de la red.

Para medir la sobrevivencia se usa el concepto de grado de sobrevivencia, que hace referencia al alcance que tiene la red para recuperarse ante eventos de falla simple y múltiple, para lo cual se considera la probabilidad de que cada falla ocurra individualmente [34][46]-[38].

En éste capítulo se presentó un diagrama conceptual de las fallas, a partir de cuatro preguntas que pretenden abordar la problemática desde distintos enfoques, teniendo en cuenta los factores que intervienen en su aparición, los actores involucrados, causas de diversa índole, así como el lugar en el que se desarrollan respecto a las fronteras del sistema. Esto permite ampliar la base conceptual sobre el problema de las fallas simples y múltiples en redes MPLS sirviendo como referencia en especial para los operadores de red, puesto que les permite adoptar medidas preventivas tendientes a minimizar el impacto de dichos fenómenos. Se introdujo posteriormente el concepto de fallas múltiples en el nivel de infraestructura, así como el grado de dependencia entre las mismas. Finalmente se presentó el concepto de confiabilidad y sus atributos asociados en las redes MPLS.

En el capítulo 3 se describen los métodos de protección utilizados en contextos de falla simple, así como los parámetros de desempeño que sirven para determinar el impacto que tiene sobre los tráficos transportados la presencia de fallas simples y múltiples en las redes MPLS.

3. RECUPERACIÓN EN REDES MPLS.

El presente capítulo introduce el concepto de recuperación, así como los modelos de protección y restablecimiento desde los que se puede abordar esta temática. Seguidamente se describe el funcionamiento de los métodos de protección (global, local, inverso) como alternativa de solución en contextos multi-falla. Por último se presentan los parámetros de desempeño que sirven como referente para la medición del impacto ocasionado sobre los tráficos cursantes ante la ocurrencia de fallas simples y múltiples.

3.1. ASPECTOS GENERALES DE 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 permitan mantener las condiciones iniciales del tráfico comprometido por dichas fallas, preservando las características 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 [53-54]. Estos fallos 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, entre otras causas presentadas en el diagrama conceptual descrito en el capítulo 2.

La recuperación en redes MPLS puede abordarse desde dos enfoques distintos a saber:

3.1.1. Modelo de protección (Conmutación protegida)

El modelo de protección 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 [10]-[53]. Para proteger el tráfico usando este modelo se implementan los métodos de protección como estrategia de recuperación en la red.

El funcionamiento de los métodos de protección basa su operación en la ejecución de una serie de etapas que comienzan desde la identificación de la falla en el dominio MPLS, hasta la recuperación del LSP en donde tuvo lugar dicho evento [16]-[31]. A continuación se expone cada una de estas etapas.

- ✓ Un mecanismo de direccionamiento, que permite la selección de los caminos de trabajo y de respaldo.

- ✓ Un método que garantice la reserva de ancho de banda para ambos caminos.
- ✓ Un método de señalización que permita distribuir las etiquetas en los caminos de trabajo y respaldo, haciendo uso de protocolos como LDP/RSVP o CR-LDP/RSVP-TE.
- ✓ Un mecanismo de detección y de notificación de fallas, necesarios para indicar a los nodos dotados con funciones de protección que tomen las acciones necesarias ante la ocurrencia del evento de falla.
- ✓ Un mecanismo para conmutar el tráfico desde el camino donde ocurre la falla hacia el camino de respaldo.
- ✓ Un mecanismo de recuperación para conmutar el tráfico de vuelta hacia el camino de trabajo original una vez se haya reparado la falla.

La figura 3-1 presenta las etapas descritas:

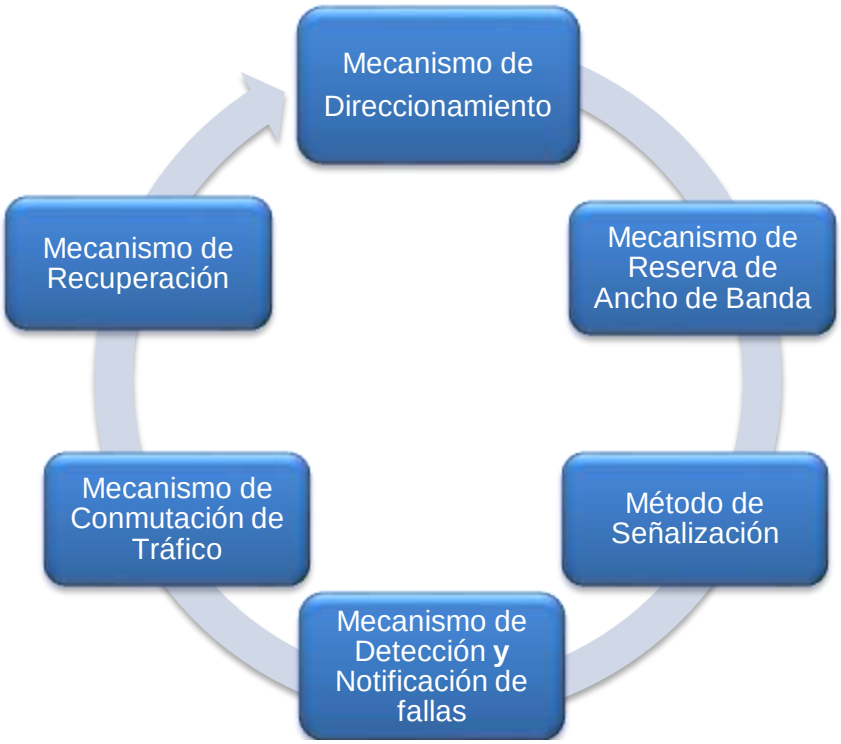


Figura 3-1. Funcionamiento de los métodos de protección.

3.1.2. Modelo de restablecimiento (re-enrutamiento dinámico).

El modelo de restablecimiento 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 y por lo tanto se requeriría volver a calcular un nuevo camino de respaldo [31]-[53]. Este modelo cuenta con mayores tiempos de restablecimiento en comparación con el modelo de protección, debido a que el establecimiento de caminos de respaldo toma lugar después de que ocurre algún evento de falla y por esta razón no es muy adecuado para el uso de aplicaciones sensibles al retardo y la pérdida de paquetes [16].

En general, el modelo de protección brinda mejores condiciones para tráficos con altos requerimientos en términos de pérdida de paquetes y tiempos de restablecimiento, ya que el camino de respaldo se calcula antes de la ocurrencia de algún evento de falla, permitiendo por tanto una mayor velocidad de recuperación del tráfico afectado. Para el desarrollo del presente proyecto se hace uso de este modelo y específicamente de los métodos de protección con el objeto de valorar su desempeño cuando se aplican en contextos multi-falla.

3.2. PANORAMA DE LA RECUPERACIÓN ANTE FALLAS MÚLTIPLES EN REDES MPLS.

En la actualidad la gran mayoría de estudios realizados sobre recuperación en redes MPLS se han enfocado en contextos de falla simple [12][16]-[20]. Algunos autores, sin embargo han realizado propuestas en las que se utilizan métodos de restablecimiento en contextos multi-falla. En estas se han desarrollado algoritmos que calculan dinámicamente más de un camino de respaldo por cada camino de trabajo, y en otros casos permiten combinar los métodos de recuperación de acuerdo a las condiciones de falla reportadas mediante la actualización periódica de la información de red [9][11]-[55-56].

En [16]-[22], se aplica el concepto de Protección con QoS (QoSP: QoS Protection) para determinar el mecanismo de restablecimiento más adecuado para establecer los caminos de respaldo. En [12] se presenta una propuesta que permite manejar eventos de falla múltiple para un camino de trabajo protegido, basada en la aplicación de dominios de protección de segmento, mecanismos de recuperación ante falla simple y una extensión de estos mecanismos para la protección del tráfico comprometido. En [20] se proponen

tres algoritmos capaces de establecer más de un camino de respaldo de manera que se puedan afrontar eventos de falla que ocurran tanto en los caminos de trabajo como de respaldo. Exceptuando esta última propuesta, en ninguna de las otras se consideran fallas en el camino de respaldo.

Estas alternativas en general son costosas en términos de consumo de recursos de red y tiempo de procesamiento y no abarcan la problemática desde la perspectiva de la protección, que implica el pre-establecimiento de caminos de respaldo para la recuperación efectiva del tráfico comprometido por las fallas, objeto de estudio del presente proyecto.

3.3. MÉTODOS DE PROTECCIÓN ANTE FALLAS EN REDES MPLS.

A continuación se presentan las características que describen el funcionamiento de los métodos de protección (global, local, inverso) en redes MPLS, cuya eficacia se ha comprobado en contextos de falla simple [12][16]-[20], y que se utilizan en el capítulo 4 para evaluar su desempeño ante la ocurrencia de fallas múltiples.

3.3.1. Método global.

Este método basa su funcionamiento en el uso de dos elementos principales, un nodo de ingreso dotado con funciones PSL y otro nodo de egreso dotado con funciones PML, requiriendo también la presencia de un camino de respaldo por cada camino de trabajo dentro del dominio de protección [57-58].

Después de la ocurrencia y detección de una falla en el trayecto de trabajo mediante el uso de una Señal de Indicación de Falla (FIS: Fault Indication Signal), que debe propagarse desde donde se haya presentado el evento de falla en la red hasta el nodo de ingreso, este último se encarga de realizar el switchover, proceso que consiste en la conmutación del tráfico cursante desde el camino de trabajo hacia el de respaldo. Este método tiene la ventaja de que solamente se requiere configurar un único camino de respaldo por cada camino de trabajo. Además, es un método de protección centralizado, lo que significa que únicamente se requiere contar con dos nodos con funciones PSL y PML respectivamente. Sin embargo, la eficacia de este método depende en gran medida del tiempo de restablecimiento, es decir, el tiempo empleado entre la detección de la falla y el momento en el que los paquetes inician su flujo a través del camino de respaldo, periodo durante el cual se presenta una pérdida de paquetes proporcional a su duración, razón por la cual éste mecanismo no es muy recomendable cuando se está transportando tráfico sensible a pérdidas [16].

La figura 3-2 describe el funcionamiento del método global, la cual está compuesta por siete LSRs, el LSR1 está dotado con funciones de PSL y el LSR7 con funciones de PML.

Se tiene un camino de trabajo, constituido por los nodos LSR1-LSR3-LSR5-LSR7 y el camino de respaldo por los nodos LSR2-LSR4-LSR6. El LSR5 detecta el evento de falla que afecta el camino de trabajo en el enlace LSR5-LSR7, y envía una FIS hacia el LSR1 (PSL). Mientras el mensaje de indicación de falla viaja hasta el PSL, se presenta una pérdida de paquetes proporcional a su tiempo de llegada. Una vez se notifica al PSL del evento de falla, este realiza el proceso de switchover, conmutando el tráfico hacia el camino de respaldo. Finalmente, cuando se recupera el enlace comprometido por la falla, el PSL conmuta el tráfico de vuelta hacia el camino de trabajo, proceso que se conoce como switchback.

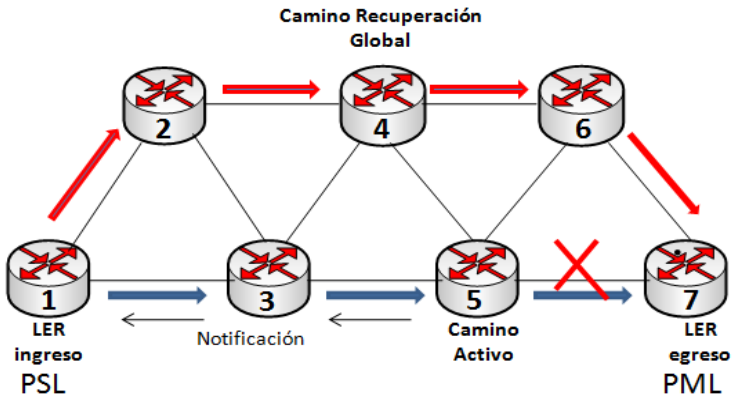


Figura 3-2. Mecanismo de protección global.

3.3.2. Método de recuperación local.

Este mecanismo de protección se caracteriza porque la acción de recuperación se lleva a cabo en el mismo nodo en donde se presenta la falla y por tanto se considera transparente para el nodo de ingreso, obteniendo de esta manera tiempos de restablecimiento menores respecto al mecanismo global, disminuyendo significativamente la pérdida de paquetes relacionadas con su duración [16]-[57-58].

Las ventajas de este método son principalmente el mantenimiento de la integridad de los paquetes de datos transportados por la red debido a la reducida pérdida de paquetes y el bajo tiempo de recuperación, que es considerablemente menor respecto a los otros mecanismos de protección. Por otro lado, la gran desventaja que presenta este mecanismo de recuperación es la de tener que dotar a cada nodo que se requiera proteger con funciones PSL, así como un nodo adicional con funciones PML. Entonces se deben tener tantos caminos de recuperación como segmentos del camino activo se quieran proteger, lo que trae en consecuencia la utilización ineficiente de recursos y el incremento en la complejidad del direccionamiento [13]-[57-58].

La figura 3-3 describe el mecanismo de recuperación local. El camino de trabajo está constituido por los LSRs LSR1-LSR3-LSR5-LSR7 y se presenta una falla en el enlace establecido entre LSR5 y LSR7, nodos dotados con funciones de PSL y PML

respectivamente. Cuando ocurre el evento de falla, el tráfico que fluye por el segmento del camino de trabajo a través de los LSR5 y LSR7 se conmuta hacia el camino de respaldo LSR5-LSR6-LSR7.

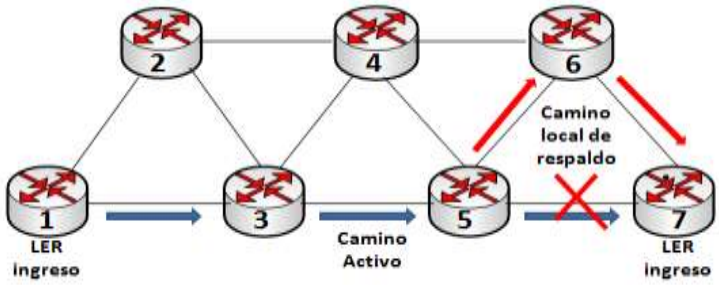


Figura 3-3. Mecanismo de protección local.

3.3.3. Método inverso.

En este mecanismo de protección cuando se presenta una falla en el camino de trabajo, el nodo que detecta la misma envía el tráfico cursante, así como una señal de indicación de falla en dirección inversa hacia el nodo de ingreso a través de un camino de respaldo inverso [13]-[58]. Una vez este nodo recibe dicha señal, deja de cursar el tráfico entrante hacia el camino de trabajo y comienza a redirigirlo hacia el camino de respaldo global, presentándose una pérdida de paquetes mínima en comparación con los otros métodos de recuperación. Por sus características, este método es muy conveniente en los escenarios de red donde el tráfico es muy sensible a la pérdida de paquetes. Además dicho método simplifica el mecanismo de notificación de falla, utilizando el camino de respaldo para tal fin.

La figura 3-4 describe el mecanismo de recuperación inverso. Los caminos de trabajo y respaldo son los mismos que en el mecanismo global. Adicionalmente se agrega un camino de recuperación inverso a partir de LSR5 que es el nodo adyacente al evento de falla, el cual está conformado por los LSRs LSR5-LSR3-LSR1 en dirección al nodo de ingreso. Cuando se detecta la falla en el camino de trabajo (entre los LSR5 y LSR7), el tráfico se re-enruta de vuelta hacia el nodo de ingreso a través del camino de recuperación inverso y una vez se alcanza dicho nodo, el mecanismo funciona igual que el método global, cursando el tráfico hacia el camino de respaldo global conformado por los LSRs LSR2-LSR4-LSR6 hasta que el camino de trabajo vuelva a su estado normal de operación.

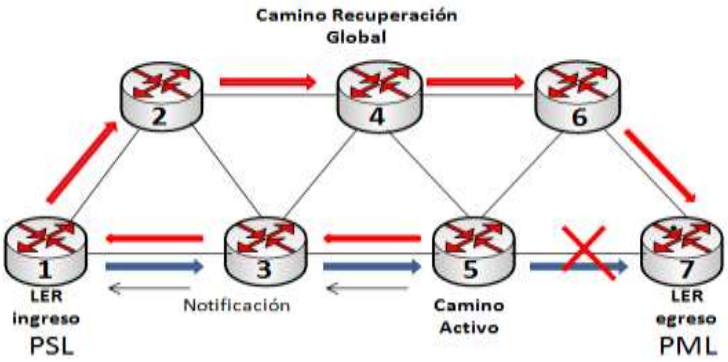


Figura 3-4. Mecanismo de protección inverso.

3.4. PARÁMETROS DE DESEMPEÑO EN REDES MPLS.

Se definen una serie de parámetros que son de utilidad para determinar el desempeño y la efectividad de los mecanismos de recuperación en redes MPLS, cuando se aplican a escenarios con presencia de fallas [6][19][22]-[57]. Además permiten evaluar sus ventajas y desventajas tanto cualitativa como cuantitativamente, de manera que se pueda comparar su efectividad en los contextos mencionados y concluir acerca de cuál es el mejor mecanismo de recuperación para cada caso de falla en particular. A continuación se explica de forma detallada cada uno de ellos, teniendo en cuenta su utilidad para la valoración del impacto sobre los tráficos que fluyen en la red para el escenario de simulación a proponer en el capítulo 4.

3.4.1. Tiempo de restablecimiento.

Es un factor que depende directamente de la cadena de eventos involucrados en la recuperación. Existen básicamente cuatro componentes que afectan el tiempo de restablecimiento, estos son el Tiempo de Detección (DT: Detection Time) de la falla, el Tiempo de Notificación (NT: Notification Time) durante el cual se notifica al nodo responsable de tomar las acciones de conmutación sobre la falla utilizando una señal FIS (Fault Indication Signal) y el tiempo de recuperación del tráfico desde el camino de trabajo hasta el camino de respaldo (ST: Switchover Time). Adicionalmente, si se trabaja con un método de restablecimiento, se debe agregar el tiempo de Re-enrutamiento (RrT: Rerouting Time). El tiempo de restablecimiento está definido por:

$$\mathrm{RT} = \mathrm{DT} + \mathrm{NT} + \mathrm{RrT} + \mathrm{ST}$$

Ecuación 3-1. Tiempo de Restablecimiento.

Donde: DT = Tiempo de Detección.
NT =Tiempo de Notificación.

RrT = Tiempo de Re-enrutamiento.
ST =Tiempo de Switchover.

En la anterior ecuación, el componente más representativo es el Tiempo de Notificación, puesto que por su duración es el responsable de la mayor parte de las pérdidas de paquetes. Existen varios factores que afectan el Tiempo de Notificación, tales como el retardo en la notificación de la falla, el método de notificación y la distancia entre el nodo que detecta la falla y el nodo encargado de iniciar el proceso de conmutación, [16][23]-[44]. Sin embargo, en el método local este factor no es significativo debido a que el nodo que detecta la falla también es responsable del switchover, por lo que la distancia ya no es relevante.

Adicionalmente, para calcular el tiempo de notificación se debe tener en cuenta el Tiempo de Propagación (PT: Propagation Time), el cual caracteriza los retardos concernientes al flujo del tráfico. El Tiempo de Propagación comprende varios parámetros como el Retardo de Enlace (LD: Link Delay), que define la latencia en la propagación sobre los enlaces, el Retardo por Procesamiento del Nodo (NPD: Node Processing Delay) y el Retardo de Procesamiento del Buffer (BPD: Buffer Processing Delay), que representa el tiempo que los paquetes permanecen encolados en los buffers del nodo. Otra condición que influye sobre el tiempo de notificación es la congestión de paquetes causada por la no reservación de ancho de banda en redes con altas cargas de tráfico, lo cual conduce a incrementos en su duración [Protection]. El Tiempo de Propagación esta dado por:

$$\mathrm{PT} = \mathrm{LD} + \mathrm{NPD} + \mathrm{BPD}$$

Ecuación 3-2. Tiempo de Propagación.

Donde: LD = Retardo de Enlace.
NPD = Retardo por Procesamiento del Nodo.
BPD = Retardo de Procesamiento del Buffer.

Luego, el Tiempo de Notificación se puede obtener de forma aproximada a partir de la siguiente expresión:

$$NT: D(i,a) * PT$$

Ecuación 3-3. Tiempo de Notificación.

Donde: D(i,a) = Distancia de notificación (número de saltos) entre el nodo que detecta la falla (nodo a) y el nodo encargado de iniciar el proceso de conmutación (nodo i).
PT = Tiempo de propagación de la señal en cada salto.

La tabla 3-1 indica el grado de protección brindado de acuerdo al tiempo de restablecimiento, el cual varía dependiendo del tipo de tráfico afectado por la falla [6][13]-[19]. Se ha determinado el valor de 50 ms como umbral para el establecimiento de métodos de protección rápidos, sin embargo para experimentar con otros grados de protección, se sugiere no considerar dicho límite. En la práctica es muy importante disminuir la duración de este retardo para reducir de manera notable la pérdida de paquetes asociada y así obtener el nivel de protección requerido para la mayoría de los servicios actuales.

Grado de protección	Tiempo de Restablecimiento (RT)
Muy Bajo	> 1 min
Bajo	200 ms – 1 min
Medio	50 ms – 200 ms
Alto	20 ms – 50 ms
Muy Alto	< 20 ms

Tabla 3-1. Grado de Protección vs Tiempo de Restablecimiento

Para disminuir la duración del tiempo de restablecimiento la principal medida a adoptar es la reducción en la duración de los eventos de cada fase del proceso de recuperación, acción que involucra procesos tales como el uso de técnicas de detección y monitoreo más rápidas, la optimización de los métodos de notificación de fallas, ajustar en un valor adecuado (0-50 ms) el valor del tiempo de retención[3] y minimizar la distancia entre el punto donde ocurre la falla y el nodo encargado de realizar la función de switchover. Existen otras alternativas tales como reducir el tiempo de detección de falla y el tiempo de switchover, sin embargo ellas dependen de la tecnología del nodo por lo cual no se pueden ejecutar de manera sencilla [13][22]-[44].

3.4.2. Pérdida de Paquetes.

La pérdida de paquetes (PL: Packet Loss) es un parámetro crítico para el análisis del impacto de falla y del desempeño de los métodos de recuperación, ya que su efecto posee gran relevancia especialmente en las aplicaciones de nueva generación (VoIp,

[3] El tiempo de retención corresponde al tiempo de espera existente entre la detección del evento de falla y la acción de alguno de los métodos de protección en la red MPLS, cuyo valor es configurable y podría ser incluso cero.

Multimedia, etc.,) donde una pérdida significativa de paquetes puede llegar a interrumpir totalmente la prestación de estos servicios [6][13][17][19]-[23]. La pérdida de paquetes depende del Tiempo de Restablecimiento empleado para superar la falla, específicamente del Tiempo de Notificación y de Re-enrutamiento (en el caso de un método de restablecimiento) y también de la tasa de transmisión de datos asignada en el LSP, siendo el NT el componente más representativo puesto que es el mayor responsable de la pérdida de paquetes. Adicionalmente, se debe considerar la pérdida de paquetes que estaban circulando en el enlace en el instante de la ocurrencia de la falla. La pérdida de paquetes está dada por:

$$\mathrm{PL} = \mathrm{RT} \cdot \mathrm{RB} + \mathrm{LP}$$

Ecuación 3-4. Pérdida de paquetes en función del tiempo de restablecimiento.

Donde: RT = Tiempo de Restablecimiento.
RB = Tasa de transmisión (bits/s).
LP = Pérdida de paquetes que circulan en el enlace en el momento de la falla.

Los métodos de protección introducen una cierta cantidad de pérdidas de paquetes durante la conmutación del camino de trabajo hacia el de respaldo, no siendo posible evitar totalmente la ocurrencia de este fenómeno [6][19][22]-[44].

Los valores de pérdida de paquetes de acuerdo a [24] para diferentes tipos de tráficos y sus servicios asociados se presentan en la tabla 3-2.

Porcentajes de pérdida de paquetes requeridos para diversos tipos de tráfico		
Tipos de tráfico		**Porcentaje de pérdida de paquetes**
Video (Videotelefonía)		< 1%
Datos		0%
Voz	**Voz en dos vías**	< 3%
	Streaming de audio	< 1%

Tabla 3-2. Porcentajes de pérdida de paquetes admitidos según la recomendación ITU-T G.1010 para diversos tipos de tráfico

3.4.3. Duplicación de paquetes.

La duplicación de paquetes es un fenómeno que ocurre en el interior de la red que consiste en la replicación de los paquetes pertenecientes a un flujo de tráfico determinado. La causa principal de la duplicación de paquetes es la aplicación de los métodos de recuperación, que si bien contribuyen a la recuperación efectiva del tráfico, también pueden conducir a la repetición de paquetes de datos. En comparación con el anterior parámetro, es un problema de menor magnitud porque no hay pérdida de información, sin embargo hay un gasto innecesario de ancho de banda por la transmisión de tráfico redundante.

3.4.4. Desorden de paquetes.

El desorden de paquetes es un problema causado por la aplicación de los mecanismos de recuperación en el nodo de ingreso cuando se envía el tráfico por un LSP alternativo después de que este haya regresado por un camino de vuelta al mismo. Dicho fenómeno también se puede presentar cuando los retardos a lo largo de los caminos de trabajo y respaldo son distintos, en cuyo caso el proceso de switchback del tráfico del camino de respaldo hacia el camino de trabajo puede causar que algunos paquetes se sobrepongan unos con otros [16][20]-[58].

Así como ocurre con la pérdida de paquetes, existen tráficos asociados a aplicaciones como el streaming de voz o de video que no toleran el efecto del desorden de paquetes, mientras que existen otras aplicaciones como la transferencia de datos que no se ven afectadas de manera crítica frente a este problema [53]. El desorden de paquetes está estrechamente relacionado a la pérdida de paquetes y al retardo causado por el tiempo de restablecimiento, además de que promueve la aparición de señales erróneas de congestión y una disminución del throughtput de la red [12][13][16]-[44]

Las consecuencias que genera el desorden de paquetes sobre los tráficos cursantes, requieren de la adopción de medidas que permitan re-ordenar los paquetes que han perdido su secuencia. Dichas medidas se desarrollan en niveles superiores, destacándose el uso del Protocolo de Control de Transmisión (TCP: Transmission Control Protocol).

3.4.5. Latencia y Jitter.

La latencia específica la cantidad de tiempo que toma un bit para recorrer la red, por cuanto es útil para medir la calidad de conexión que ésta brinda. Así, entre más baja sea la latencia, la conexión es mejor [6][13]-[16]. Los métodos de protección pueden introducir latencia adicional a la red, como en el caso del establecimiento de un camino de protección que puede ser considerablemente más largo que el camino de trabajo o contar

con más saltos, por lo cual este factor está asociado a los algoritmos de selección de rutas de recuperación.

Otro parámetro importante relacionado con la latencia es el jitter, que define la fluctuación del retardo de la información proveniente de la misma fuente de tráfico. Generalmente se asocia a tareas de procesamiento en los nodos de la red y a la implementación de políticas de enrutamiento aplicadas al transporte de los paquetes. Su análisis reviste importancia especialmente en aplicaciones de tiempo real, donde es conveniente reducirlo al mínimo [6]-[13].

La tabla 3-3 resume los valores de retardo y jitter requeridos para tráficos de video, voz y datos según la recomendación G.1010 de la ITU-T [24].

Retardo y jitter para diversos tipos de tráfico			
Tipos de tráfico		**Retardo**	**Jitter**
Video (Videotelefonía)		**150 ms**	**< 1 ms**
Datos		**-**	**-**
Voz	**Voz en dos vías**	**150 ms**	**< 1 ms**
	Streaming de audio	**< 10 s**	**< < 1 ms**

Tabla 3-3. Valores de retardo y jitter admitidos según la recomendación ITU-T G.1010 para diversos tipos de tráfico

El retardo y el jitter no impactan de manera notable el tráfico de datos, ya que su efecto generalmente no es apreciable por el usuario. Por esta razón, este tipo de tráfico no recibe especial consideración respecto a estos parámetros y por tanto no se definen en la tabla 3-3.

3.4.6. Vulnerabilidad.

Tiempo que el camino de trabajo queda sin respaldo frente a la posible falla de algún componente de la red. En el momento en que el LSP de respaldo transporta el flujo de tráfico del LSP primario, un nuevo LSP se debe establecer para protegerlo [13]-[16].

3.4.7. Calidad de protección.

Es un parámetro propio de los mecanismos de recuperación que define la probabilidad de que una conexión se restablezca ante una falla [6]-[13]. El rango de la calidad de protección se define desde calidad de la protección relativa hasta absoluta. La opción de supervivencia relativa permite asignar diversos niveles de prioridad a diferentes conexiones, para que cuando se presente una falla sea posible restaurarlas basándose en su prioridad relativa. A diferencia de la anterior, en la supervivencia absoluta el tráfico protegido posee garantías explícitas, brindando de esta manera condiciones de protección óptimas para la satisfacción de Acuerdos de nivel de Servicio (SLA: Service Level Agreement) [6][13]-[16].

3.4.8. Tiempo de restablecimiento completo.

Tiempo transcurrido entre la detección de una falla y el instante donde todo el tráfico recuperado comienza a fluir a través de los caminos de respaldo que sirven de soporte en el proceso de restablecimiento del tráfico. El tiempo de restablecimiento completo puede ser equivalente o diferente al tiempo de restablecimiento, dependiendo de si se utilizan trayectos de respaldo con igual o diferente capacidad de recursos que los trayectos de trabajo [6][13]-[16].

3.4.9. Ancho de banda garantizado.

Describe la capacidad de algunos mecanismos de recuperación para garantizar que la totalidad del ancho de banda del tráfico afectado se reasigne en los caminos de respaldo. Otros mecanismos de recuperación no ofrecen ninguna garantía de este tipo, es decir, puede o no haber suficiente capacidad de ancho de banda de respaldo para conmutar el tráfico afectado, degradando en consecuencia las características de las aplicaciones soportadas por ellos.

3.4.10. Escalabilidad.

Un mecanismo de recuperación se considera escalable si su rendimiento no depende en gran medida del tamaño de la red y del tráfico transportado a través de ella, el cual está sujeto a cambios debido al incremento de los mensajes de señalización y difusión de estado [4][13]-[16]. Se suman a estos factores el tiempo de recuperación y la capacidad de respaldo, que también se ven influenciados por el tamaño del tráfico y la red. Su consideración es importante porque dicho parámetro está ligado al aseguramiento de las condiciones de funcionamiento de la red hacia futuro.

3.4.11. Estabilidad.

Al configurar y poner en funcionamiento un mecanismo de recuperación, normalmente es posible modificar una serie de parámetros temporales (por ejemplo, el tiempo entre dos mensajes consecutivos, los tiempos de retención, etc.,) dentro de un cierto rango de valores. Aunque el ajuste de valores pequeños para dichos parámetros suele acelerar el proceso de recuperación, su configuración puede impactar la estabilidad de la red. Por ejemplo, en el caso de un enlace que presenta fallas recurrentes, la configuración del tiempo de retención empleando valores de esta magnitud puede conducir a un ciclo sin fin de conmutación entre los caminos de trabajo y respaldo, incidiendo negativamente sobre los tráficos que fluyen en la red [6]-[13].

3.4.12. Noción de la clase de recuperación.

Algunos mecanismos de recuperación brindan la posibilidad de distinguir entre varias clases de tráfico y adoptar las medidas de recuperación apropiadas para cada una de ellas [4]. Esta característica es muy útil, ya que cada clase de tráfico demanda un nivel de protección distinto. Por ejemplo, una clase de tráfico puede requerir un esquema de recuperación muy rápido con garantías de ancho de banda, mientras que para otra clase puede ser suficiente implementar un mecanismo de recuperación poco exigente a un bajo costo [13]. Lo anterior también se aplica en la práctica con el objetivo de optimizar la utilización de recursos de red, evitando por ejemplo el desperdicio o asignación ineficaz de ancho de banda en caminos de respaldo que no lo requieran [2].

3.4.13. State Overhead.

En el interior de la red, la información de estado requerida para el mantenimiento de sus componentes aumenta a medida que el número de caminos de respaldo se incrementa. El encabezado de estado transmitido a través de la red depende no sólo del número de caminos de respaldo, al cual es proporcional, sino también de la cantidad de mensajes de estado particulares asociados al funcionamiento de los mecanismos de recuperación [2][6]-[13].

Para llevar a cabo el estudio del impacto de los eventos de falla simple y múltiple en los tráficos que fluyen en el escenario de red a plantear en el capítulo 4, así como el análisis de la adaptación de los métodos de protección ante falla simple en contextos multi-falla, se hará uso de algunos de los parámetros de desempeño previamente descritos, de acuerdo a las capacidades del simulador para analizarlos, así como también a la relevancia de la información que se pueda obtener a partir de ellos. Con base en lo anterior, los parámetros de desempeño a considerar dentro de la simulación son los siguientes: pérdida de paquetes, tiempo de restablecimiento, desorden de paquetes,

retardo y el jitter[16][20]-[44].

Este capítulo presentó una breve descripción de las propuestas actuales de recuperación ante eventos de falla múltiple en redes MPLS. Posteriormente se describieron los métodos de protección utilizados en contextos de falla simple, así como los parámetros de desempeño que sirven como referente para la valoración del impacto de los eventos de falla que ocurran dentro de un escenario de red MPLS.

El capítulo 4 presenta la descripción de la herramienta de simulación, el plan de pruebas a realizar y los resultados del mismo. Se determina el impacto que tienen los eventos de falla simple y múltiple con base en los resultados obtenidos para los parámetros evaluados, cuando no se aplican alternativas de recuperación así como cuando se aplican los métodos de protección sobre la topología a proponer.

4. SIMULACIÓN, PRUEBAS Y RESULTADOS.

Este capítulo presenta los resultados obtenidos tras la realización de un conjunto de pruebas dividido en dos casos a partir de los que se analiza la respuesta que tiene la ocurrencia de eventos de falla simple y múltiple sobre los tráficos de voz, video y datos que fluyen a través de la red, en términos del throughput, pérdida y desorden de paquetes, retardo, jitter y tiempos de restablecimiento.

Finalmente, se plantea una evaluación del impacto mediante la definición de unos rangos que permitan clasificar los valores de los parámetros obtenidos en las diferentes pruebas realizadas y que permitan concluir sobre qué tan afectados resultan los tráficos cursantes ante eventos de falla.

La metodología de simulación adoptada para llevar a cabo el plan de pruebas está basada en los trabajos de [4][12]-[20], la cual consta de los pasos que se describen a continuación.

- ✓ Planteamiento del escenario de simulación.
- ✓ Definición de las características de los enlaces y tráficos de simulación.
- ✓ Definición de los parámetros de desempeño usados para evaluar el impacto ocasionado a los tráficos cursantes en la red.
- ✓ Descripción de los enlaces involucrados en la ocurrencia de fallas y en las acciones de recuperación.
- ✓ Ejecución de las pruebas de simulación.
- ✓ Análisis de resultados.

4.1. DESCRIPCIÓN DE LA HERRAMIENTA DE SIMULACIÓN.

4.1.1. NS-2 (Network Simulator V2.0).

Para la realización de las pruebas de simulación en donde se programarán eventos de fallas simples y múltiples sobre el escenario de red establecido se usará el simulador NS-2 (Network Simulator 2.0) en su versión 2.26, la cual funciona sin problemas con el módulo de simulación de redes MPLS MNS v2.0.

NS-2 es una reconocida herramienta de simulación de software libre usada tanto en ambientes académicos como en entornos de investigación para realizar validaciones de pruebas de protocolos y aplicaciones de red (Simulación para TCP/UDP, enrutamiento y multicast sobre redes cableadas o inalámbricas, interacciones multiprotocolo tales como protocolos de transporte, sesión, aplicación, algoritmos de encaminamiento y control de congestión, redes satelitales, entre otros) [59-60]. El simulador está implementado en lenguaje C++, sin embargo, este usa otro lenguaje interpretado llamado OTcl, el cual se

utiliza para escribir los scripts que sirven para definir la topología de red, los elementos que la componen, su configuración y funcionamiento. Adicionalmente, permite una visualización sencilla de las topologías de red a simular, del flujo de tráfico entre nodos, de la información de señalización, así como del comportamiento de los parámetros y métricas de desempeño de la red.

El simulador NS-2 ha recibido grandes contribuciones por parte de desarrolladores e investigadores, quienes han creado módulos adicionales y actualizaciones de acuerdo a sus necesidades específicas de simulación. Para el caso de la simulación de redes MPLS, se implementó el módulo MPLS Network Simulator (MNS) [61-62], el cual permite el diseño y análisis de topologías de red con esta tecnología, permitiendo también para este proyecto la realización del análisis de la incidencia de eventos de falla en dichas redes.

La versión de NS actualmente en desarrollo es la 3, sin embargo ésta aún no es compatible con el módulo MNS v2.0, por lo cual se utiliza la versión 2.26 que funciona adecuadamente con dicho módulo. Cabe destacar que el principal cambio que aplicó la versión 2 en comparación con la versión 1 es que incorpora una mejor subdivisión de las clases de objetos que componen el núcleo del simulador, lo cual permite un mejor desarrollo del mismo.

El simulador está diseñado para ejecutarse en cualquier distribución de Linux, pero también existe una versión compatible con el sistema operativo Windows 9x/ME/2000/XP. Sin embargo, esta última versión no está tan depurada como las versiones disponibles para sistemas Linux, por lo que puede contener errores de funcionamiento. Debido a ello, se opta por trabajar con el sistema operativo Linux.

El anexo adjunto a la monografía contiene la información referente a la instalación de ésta herramienta así como del módulo de MPLS MNSv2.0.

4.2. PLANTEAMIENTO DEL ESCENARIO DE SIMULACIÓN.

4.2.1. Generalidades del escenario de simulación.

Dentro de la metodología de simulación a abordar se plantea un escenario de red caracterizado por la disposición asimétrica de los enlaces, así como por el uso de varios LSPs que facilitan la realización del análisis de la incidencia de eventos de falla simple y múltiple sobre la red.

La figura 4-1 muestra el escenario de simulación propuesto. Este consta de catorce LSRs, dos nodos LER de ingreso y egreso respectivamente que delimitan el dominio MPLS y dos nodos IP que representan los puntos donde se generan y reciben los flujos de tráfico que van a fluir a través de la topología de red. Se definen en la topología tal número de LSRs y LERs con el objetivo de que sus características se asemejen a las de las redes

reales [1][17][25]-[32], logrando de esta manera una aproximación más precisa en la obtención de los resultados. Así mismo, este número de nodos permite el establecimiento de suficientes enlaces que faciliten la programación de múltiples fallas en la red sin quitarle a esta la capacidad de poder recuperarse ante su ocurrencia. Adicionalmente se introdujeron diferentes distancias representadas en términos de distintos valores de retardo en los enlaces que componen cada uno de los caminos, de tal manera que se tenga una relación asimétrica en los mismos.

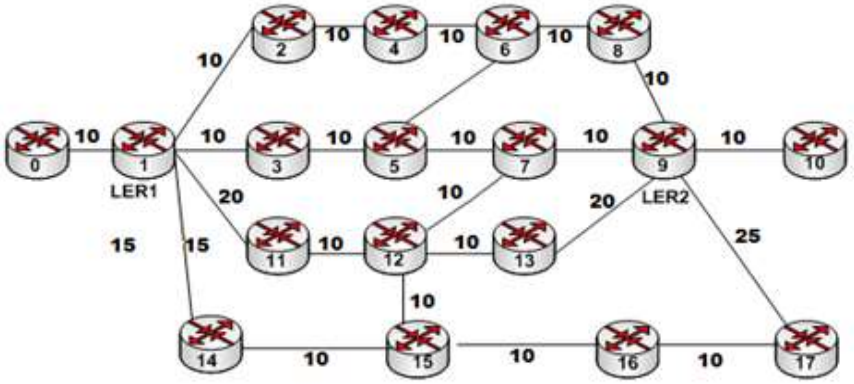


Figura 4-1. Escenario general de simulación.

Los caminos establecidos para el escenario de simulación deben contar con un ancho de banda suficiente para soportar dos y en ocasiones los tres tráficos fluyendo a través de ellos. Por esta razón y debido a que el consumo de ancho de banda no es un parámetro de interés en el presente proyecto, se han dimensionado los enlaces con un valor de ancho de banda de 6 Mbps, de tal forma que en ningún caso se presenten problemas de pérdidas de paquetes causados por congestión o falta de este recurso en la red.

4.2.2. Características del tráfico de simulación

Para la realización de las pruebas se establecen tres tipos de tráfico (voz, video y datos) que fluyen a través de los caminos de trabajo y respaldo dispuestos en la topología planteada, cuyo comportamiento y grado de afectación ante la presencia de eventos de falla simple y múltiple programados en diferentes puntos de la red será evaluado con base en los parámetros de desempeño descritos anteriormente.

Para trabajar con los tráficos mencionados en el simulador NS-2, se deben establecer las características propias de los mismos, definiendo para ello el tipo de tráfico, el tamaño del paquete y la tasa de datos de la siguiente manera [63-65].

Tipo de Tráfico	Video Streaming (CBR/UDP)	Datos-FTP (VBR/TCP)	Voz (CBR/UDP)
Tamaño de Paquete (Bytes)	1500	1500	80
Tasa de Datos (Kbps)	1400	800	256

Tabla 4-1. Características de los tráficos de simulación.

4.2.3. Características generales del plan de pruebas.

Las características del escenario de simulación mostradas a continuación, así como de los tráficos y las fallas a programar sobre el simulador NS2 permanecen invariantes en todos los casos, con el propósito de lograr coherencia en los resultados y análisis a presentar.

- ✓ La topología de red es exactamente la misma para todas las pruebas a realizar.
- ✓ Para todos los casos simulados habrá tres tipos distintos de tráfico fluyendo a través de la red, el tráfico de video, de datos y el tráfico de voz.
- ✓ Se considera en todos los casos de múltiples fallas independencia entre la ocurrencia de dichos eventos en el nivel físico [13][39]-[43].
- ✓ Las colas establecidas en los nodos que componen el escenario de red planteado son de tipo Droptail, que descartan los paquetes que sobrepasan el límite establecido para la cola.
- ✓ Para todos los casos se analizan los mismos parámetros de desempeño a saber: pérdida de paquetes, desorden de paquetes, tiempo de restablecimiento, retardo y jitter.

4.2.4. Localización e instantes de ocurrencia de eventos de falla

En la realización de las pruebas se consideraron contextos de hasta tres fallas, debido a que la probabilidad de que ocurran en la práctica un mayor número de estos eventos es muy baja [13][32]-[45], además de que de acuerdo al tamaño de la topología propuesta se podría impedir completamente el flujo de tráficos por cualquiera de los LSPs que la constituyen. La tabla 4-2 describe los instantes del tiempo de simulación en donde tienen lugar los eventos de falla.

Instantes de tiempo para los eventos de falla en la simulación			
Enlaces donde ocurren fallas en la red	**1 Falla**	**2 Fallas**	**3 Fallas**
LSR7-LSR9	0.8	0.8	0.8
LSR12-LSR13	--	0.9	0.95
LSR6-LSR8	--	--	0.9

Tabla 4-2. Instantes de tiempo donde ocurren los eventos de falla en la simulación

4.3. ANÁLISIS DE LOS RESULTADOS DEL PLAN DE PRUEBAS.

Para la realización de la simulación donde se llevan a cabo las pruebas con eventos de falla simple y múltiple en la topología de red planteada, se proponen a continuación dos casos de pruebas que sirven como referente para el análisis de los parámetros de desempeño a partir de los cuales se evalúa el impacto que presentan los tráficos afectados ante la ocurrencia de dichos eventos de falla, los cuales se analizan a continuación.

4.3.1. Caso 1: Simulación del escenario de red con presencia de eventos de falla sin aplicar mecanismos de recuperación.

En las pruebas correspondientes al caso 1 se programan eventos de una, dos y tres fallas con el objetivo de analizar el impacto de ellos cuando no se aplica ninguna alternativa de recuperación. La tabla 4-3 presenta los caminos por los cuales circulan los tráficos establecidos dentro del escenario de simulación correspondiente a este caso.

DEFINICIÓN DE LOS LSPs PARA EL CASO 1			
LSPs para los tres tráficos	**LSP1 (Tráficos de Video y datos)**	LSR1-LSR3-LSR5-LSR7-LSR9
	LSP2 (Tráfico de Voz)	LSR1-LSR2-LSR4-LSR6-LSR8-LSR9

Tabla 4-3. Definición de los LSPs para el caso 1.

La tabla 4-4 describe la localización de los eventos de falla así como la descripción de los sucesos asociados a las mismas para el caso 1.

Localización de evento(s) de falla en la red	Descripción del evento
LSR7-LSR9 (1 falla)	Los paquetes asociados a los tráficos de video y datos se descartan debido a la ocurrencia de la falla en el WP1. Sin embargo el tráfico de voz no se ve afectado por este evento. Este suceso ocurre hasta que el enlace vuelva a su estado operativo.
LSR7- LSR9 / LSR12-LSR13 (2 fallas)	El evento de falla en el enlace LSR12-LSR13 compromete un camino por el cual no fluyen los tráficos, por lo tanto su efecto es nulo, presentándose descarte de paquetes de datos y video asociados con la primera falla.
LSR7-LSR9 / LSR6-LSR8 / LSR12-LSR13 (3 fallas)	Se presenta descarte de paquetes para los tres tráficos puesto que resultan comprometidos los caminos WP1 (LSR7-LSR9) y WP2 (LSR6-LSR8). El tercer evento de falla no afecta los tráficos que fluyen por la red.

Tabla 4-4. Localización de las fallas y descripción de los sucesos asociados a ellas para el caso 1.

4.3.1.1. Análisis de throughput y pérdida de paquetes para el caso 1 del plan de pruebas.

El throughput se define como la tasa efectiva a la cual un nodo de red transmite o recibe información, cuya medida es útil porque permite conocer la capacidad de un enlace de comunicaciones [7]. Su valor se mide usualmente en bits por segundo (bit/s). Dentro del simulador NS2, el análisis del throughput de la red se lleva a cabo utilizando el comando xgraph, con el cual se puede analizar el comportamiento de los tráficos cuando los eventos de falla tienen lugar, así como cuando se intenta su recuperación por medio de la acción de alguno de los métodos de protección.

Por otro lado, la pérdida de paquetes que experimentan los tráficos que circulan en la red en el momento en que ocurren las fallas se calcula porcentualmente usando la siguiente fórmula:

$$\%\mathrm{PL} = (1 - \frac{\mathrm{RP}}{\mathrm{SP}}) * 100$$

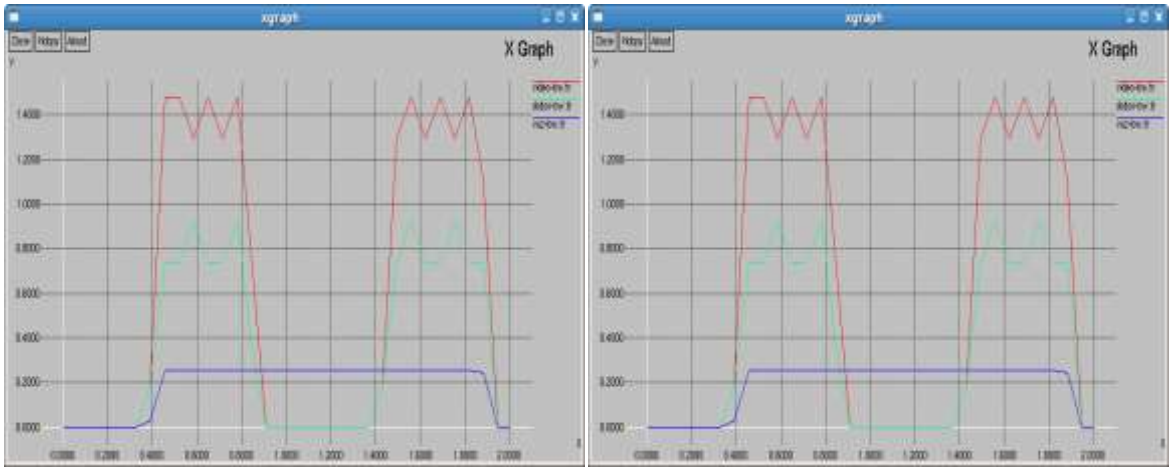
Ecuación 4-1. Cálculo de la pérdida de paquetes.

En las gráficas de pérdida de paquetes, el eje horizontal describe el caso al cual corresponde el contexto de falla específico a analizar, mientras que el eje vertical presenta el porcentaje de pérdida de paquetes ocasionado a los tráficos cursantes en el escenario de red propuesto.

La figuras 4-2a y 4-2b presentan las gráficas de throughput de los tres tráficos estudiados correspondientes a uno y dos eventos de falla respectivamente cuando no se aplican mecanismos de recuperación tal como se describió en las pruebas pertenecientes al caso 1 (ver tabla 4-4). Estos fluyen normalmente alrededor de su tasa de transmisión hasta el instante 0.8, donde se evidencia claramente una caída total del throughput de los tráficos de video y datos debida a la falla en el enlace LSR7-LSR9, que se extiende hasta el instante 1.4 del tiempo de simulación, momento en que el enlace afectado vuelve a su estado de operación normal. Adicionalmente, el tráfico de voz no se ve afectado, ya que el camino de trabajo por el cual fluye (WP2) no sufre ninguna falla y por tanto su throughput permanece casi constante durante el transcurso de la simulación.

Por otra parte, el segundo evento de falla tiene lugar en el enlace LSR12-LSR13 conforme se describió en la tabla 4-4, sin embargo no hay tráficos fluyendo a través del mismo por lo cual el throughput no resulta afectado, y su comportamiento por tanto es muy similar al mostrado en la figura 4-2a.

La figura 4-2c describe el throughput de los tres tráficos cuando ocurren tres fallas en la red. Además de la caída severa en el throughput de los tráficos de video y datos como consecuencia del primer evento de falla en 0.8, el tráfico de voz también la sufre debido a la falla que se presenta en el enlace LSR6-LSR8 tal como se observa en la figura. Sobre el instante 1.4 los enlaces afectados regresan a su estado operativo.



a) **b)**

c)

Figura 4-2. Throughput para eventos de una, dos y tres fallas para el caso 1.

La figura 4-3 muestra una comparación de la pérdida de paquetes producida cuando ocurre una, dos y tres eventos de falla. Se aprecia en general un volumen considerable de pérdida de paquetes cuando no se aplica ningún mecanismo de recuperación, lo cual se vio reflejado en las caídas del throughput descritas anteriormente. Para los eventos de una y dos fallas, la pérdida de paquetes que sufren los tráficos de video y datos es la misma (40.8 y 40% respectivamente), mientras que la pérdida de paquetes del tráfico de voz alcanza el 34% cuando se presentan tres fallas, lo cual se ve reflejado en la degradación de las características de los tráficos cursantes de acuerdo a los valores permitidos según [24], comprometiendo finalmente la QoS de las aplicaciones y servicios prestados por la red.

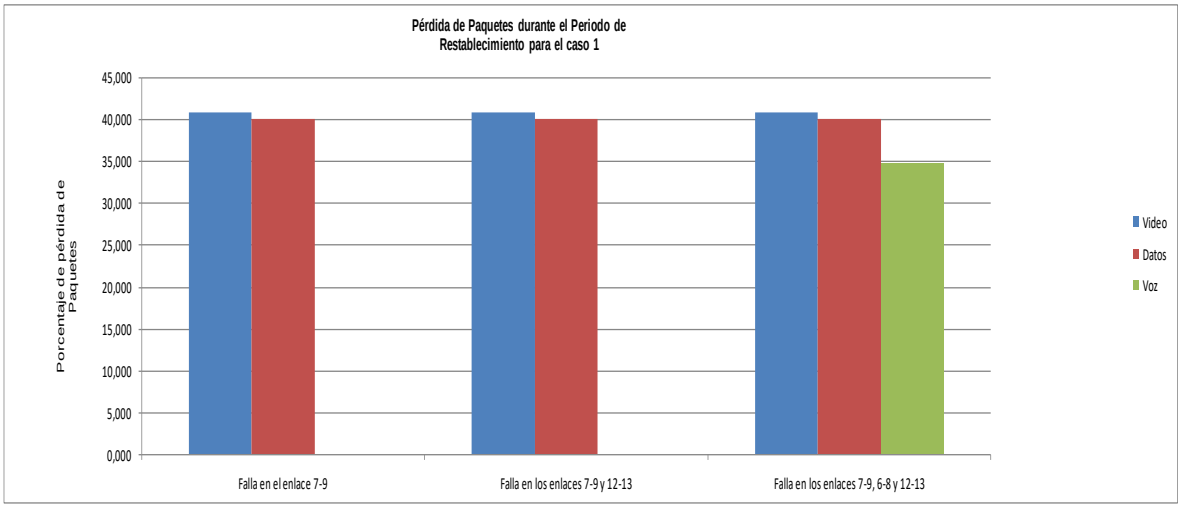


Figura 4-3. Pérdida de paquetes correspondiente a eventos de una, dos y tres fallas para el caso 1.

El porcentaje de desorden de paquetes ocasionado a los tráficos de voz, video y datos en las pruebas realizadas es de cero, debido a que no se aplica ningún mecanismo de recuperación cuya ejecución implique la conmutación de los mismos por caminos de respaldo que introduzcan mayor retardo que los de trabajo, lo cual hace que dichos paquetes pierdan su secuencia (Los paquetes del WP llegan antes al destino que los enviados a través del BP) respecto a los que fluyen nuevamente por los caminos de trabajo cuando la función de los enlaces se restablece y la red vuelve a su estado operativo.

A partir de los resultados obtenidos anteriormente se puede concluir que cuando no se aplican mecanismos de recuperación en la red, la ocurrencia de eventos de falla afecta de manera considerable el rendimiento de la red, en términos de los grandes porcentajes de pérdida de paquetes presentados, que alcanzan valores inadmisibles reflejados en las caídas críticas del throughput para los diferentes tráficos que circulan por la red.

4.3.2. Caso 2: Simulación del escenario de red con presencia de eventos de falla al aplicar mecanismos de recuperación.

El caso 2 incorpora un conjunto de pruebas para eventos de una, dos y tres fallas en donde se aplica recuperación a través del enfoque de protección. Para ello se emplean los métodos de protección (cuya eficacia se ha comprobado efectiva en situaciones de falla simple) [16]-[66] como alternativa de solución en contextos de múltiples fallas. Estas pruebas se dividen a su vez en dos casos denominados caso 2a y caso 2b. En el primero de ellos los caminos de respaldo establecidos se ven afectados por la presencia de fallas, mientras que en el segundo se utilizan caminos de respaldo distintos de manera que no resultan comprometidos por ellas.

La tabla 4-5 presenta los caminos de trabajo y respaldo por los cuales circulan los tráficos establecidos dentro del escenario de simulación correspondiente a este caso.

CARACTERÍSTICAS DEL ESCENARIO DE SIMULACIÓN PARA EL CASO 2.			
2	**Caminos de trabajo (Working Path)**	**WP1**	LSR1-LSR3-LSR5-LSR7-LSR9
		WP2	LSR1-LSR2-LSR4-LSR6-LSR8-LSR9
3	**Caminos de respaldo (Backup Path)**	**BP1 (Caso 2a)**	LSR1-LSR11-LSR12-LSR13-LSR9
		BP2 (Caso2b)	LSR1-LSR14-LSR15-LSR16-LSR9

Tabla 4-5. Características del escenario de simulación.

La tabla 4-6 describe la localización de los eventos de falla programados para los casos 2a y 2b del plan de pruebas, así como las acciones de recuperación asociadas a los métodos de protección para cada una de ellas. Para el evento de falla simple solo se describe la acción de recuperación correspondiente al caso 2a, puesto que su camino de respaldo no se ve afectado por fallas y en consecuencia no hace falta considerar rutas de respaldo distintas.

		Método de Protección / Acción de Recuperación		
Localización de evento(s) de falla en la red	**Casos de Pruebas**	**Método global**	**Método inverso**	**Método Local**
LSR7-LSR9 (1 falla)	**Caso 2a**	Los tráficos afectados (video y datos) se conmutan hacia el BP1 por el PSL (LSR1) y se recuperan de manera efectiva.	Los tráficos que fluyen por el WP1 se re-enrutan por el camino inverso hacia el PSL (LSR1) quien posteriormente los conmuta hacia el BP1. El tráfico de voz no resulta afectado.	Se re-enrutan los tráficos afectados por el camino local LSR7-LSR12-LSR13-LSR9 llegando a su destino exitosamente.
LSR7- LSR9 / LSR12-LSR13 (2 fallas)	**Caso 2a**	Se usa BP1 para recuperar los tráficos afectados, sin embargo el segundo evento de falla (LSR12-LSR13) afect este camino de respaldo y no permite que los flujos de datos y video se recuperen exitosamente	El LSR1 conmuta los tráficos de video y datos, hacia el BP1, sin embargo la segunda falla no permite la recuperación de los mismos. Los eventos de falla no afectan el tráfico de voz.	El camino de recuperación local (LSR7-LSR12-LSR13-LSR9) por el cual se re-enrutan los tráficos tras el primer evento de falla se ve afectado por la falla en LSR12-LSR13 y por tanto no se recuperan los tráficos efectivamente.
	Caso 2b	La acción de recuperación que se toma en este caso utiliza el BP2 como alternativa de enrutamiento, por lo tanto la segunda falla no compromete la integridad de este último camino y los tráficos se recuperan exitosamente. El tráfico de voz fluye normalmente por WP2.	El LSR1 conmuta los tráficos que fluyen por el camino de recuperación inverso hacia el BP2, y por tanto los tráficos llegan exitosamente al nodo de egreso.	En este caso el camino de recuperación local que se emplea tras la ocurrencia de la primera falla está conformado por LSR7-LSR12-LSR15-LSR16-LSR17-LSR9 y por tanto se evita que la falla en LSR12-LSR13 impida la recuperación efectiva de los tráficos. El tráfico de voz no se ve afectado.

LSR7-LSR9 / LSR6-LSR8 / LSR12-LSR13 (3 fallas)	**Caso 2a**	Los tráficos que fluyen por WP1 y WP2 resultan afectados por los dos primeros eventos de falla y la acción de recuperación tomada los re-enruta hacia el BP1. Sin embargo no se recuperan de manera efectiva puesto que este último camino resulta afectado por la tercera falla.	El LSR1 conmuta hacia BP1 los tráficos afectados por los dos primeros eventos de falla. La última falla en BP1 no permite completar la acción de recuperación.	Se utilizan dos caminos de recuperación locales. El primero conformado por LSR7-LSR12-LSR13-LSR9 re-enruta los tráficos de video y datos afectados por la primera falla. El segundo conformado por LSR6-LSR5-LSR7-LSR12-LSR13-LSR9 permite el flujo del tráfico de voz afectado por la segunda falla. El tercer evento de falla, afecta ambos caminos de respaldo.
	Caso 2b	Se adopta el camino BP2 como alternativa de recuperación para los tráficos comprometidos por fallas en los WP1 y WP2. El LSR1 realiza la conmutación de los tráficos y alcanzan el destino de manera exitosa, sin verse afectados por el tercer evento de falla.	Los tres tráficos afectados por los dos primeros eventos de falla, se conmutan por el LSR1 hacia el BP2, llegando exitosamente a destino.	Los caminos de recuperación local que se utilizan ahora son: LSR6-LSR5-LSR7-LSR12-LSR15-LSR16-LSR17-LSR9 para el tráfico de voz y LSR7-LSR12-LSR15-LSR16-LSR17-LSR9 para los tráficos de video y datos que se afectan por la falla en LSR7-LSR9. De esta manera la acciones de recuperación no se ven afectadas por el tercer evento de falla y se logra la recuperación efectiva de los tráficos.

Tabla 4-6. Descripción de los eventos de falla y de las acciones de recuperación cuando se aplican los métodos de protección (Caso 2a y 2b)

A continuación se describen los eventos asociados con una de las pruebas realizadas en el caso 2a para el método global cuando se programan tres fallas, con el fin de ilustrar de manera clara cuales son los eventos que toman lugar en el proceso de simulación y que en general ocurren en todos los casos planteados. Se presenta la interfaz NAM del simulador NS-2 que permite visualizar la topología diseñada así como los eventos de falla en la red y las acciones de recuperación adoptadas para contrarrestarlas.

Inicialmente se tiene el escenario de simulación propuesto en la interfaz NAM del simulador NS-2 en donde se observan los caminos de trabajo y respaldo designados. Sobre la parte superior se despliega el panel de control de la reproducción de la simulación, a la derecha se observa el control del paso de la simulación con el cual se puede acelerar o reducir su velocidad y en la izquierda se despliegan las opciones de visualización que permiten agrandar o reducir la presentación de la topología.

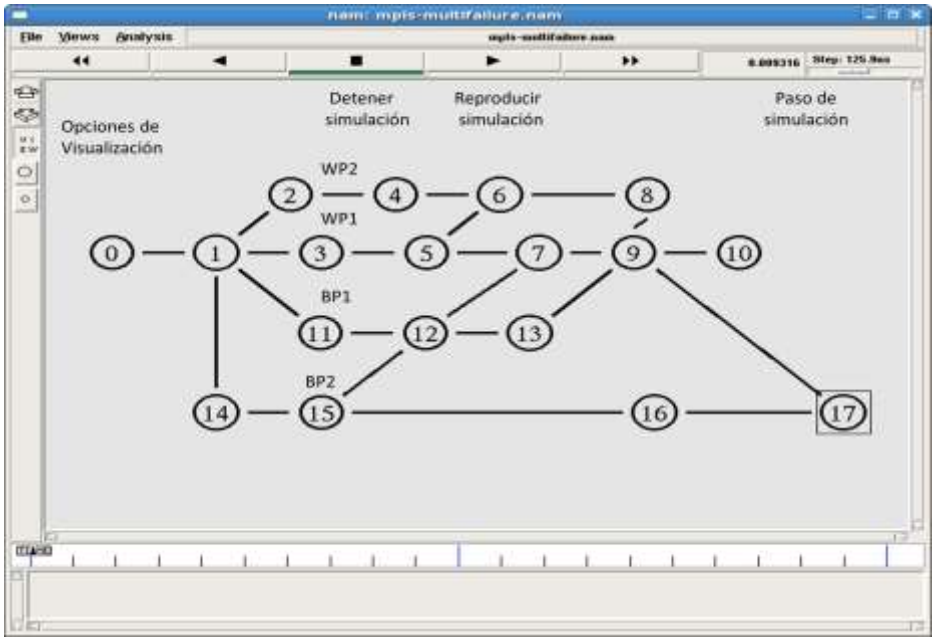


Figura 4-4. Escenario de simulación.

Al inicio de la simulación se establecen los LSPs por los cuales circulan los tráficos, mediante el uso de mensajes LDP hacia los diferentes trayectos que conforman la topología, tal como se muestra en la figura 4-5.

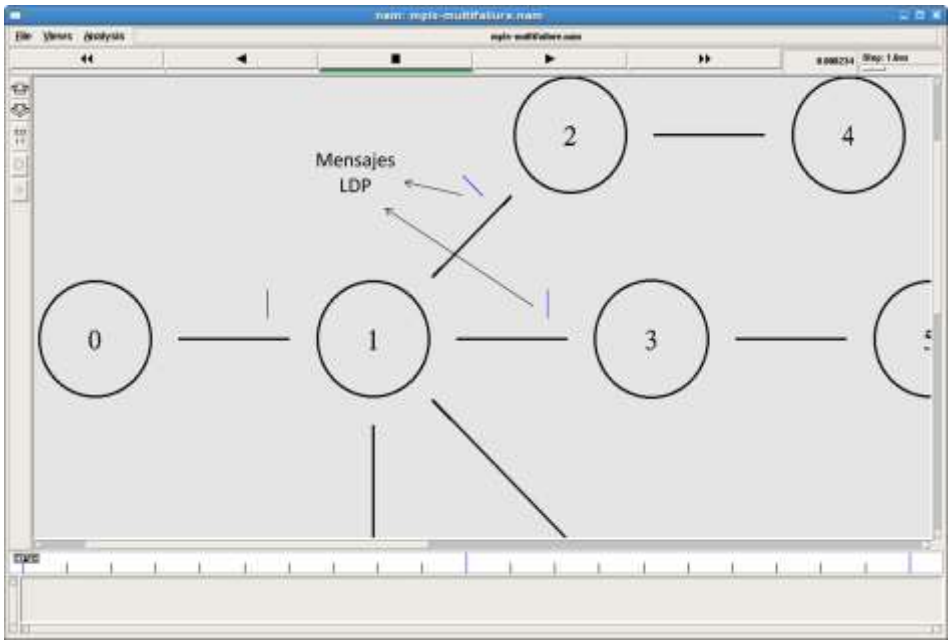


Figura 4-5. Establecimiento de los LSPs

La figura 4-6 muestra los tres tráficos fluyendo a través de los WPs establecidos, en donde el tráfico de video se representa con color magenta, el de datos con azul y el de voz con color naranja.

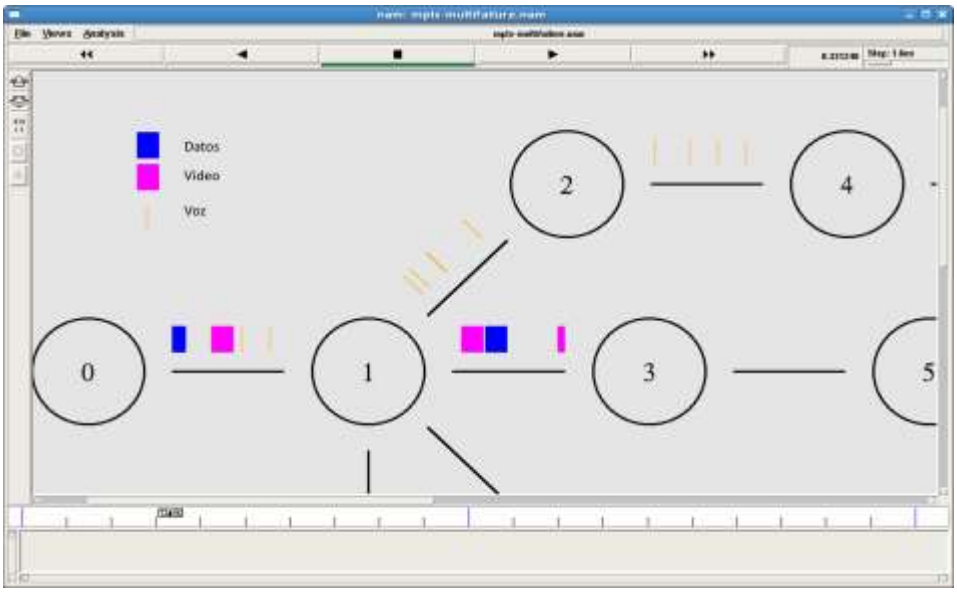


Figura 4-6. Tráficos fluyendo por los WPs definidos.

En el instante 0.8 de simulación ocurre el primer evento de falla que afecta el enlace LSR7-LSR9. Se puede ver como se descartan algunos paquetes pertenecientes a los

tráficos de video y datos en el momento en que ocurre la falla, prolongándose dicha pérdida hasta tanto se tome alguna acción de recuperación. Inmediatamente ocurre la falla, el LSR7 envía una señal FIS hacia el nodo LSR1 como se observa en la figura 4-7.

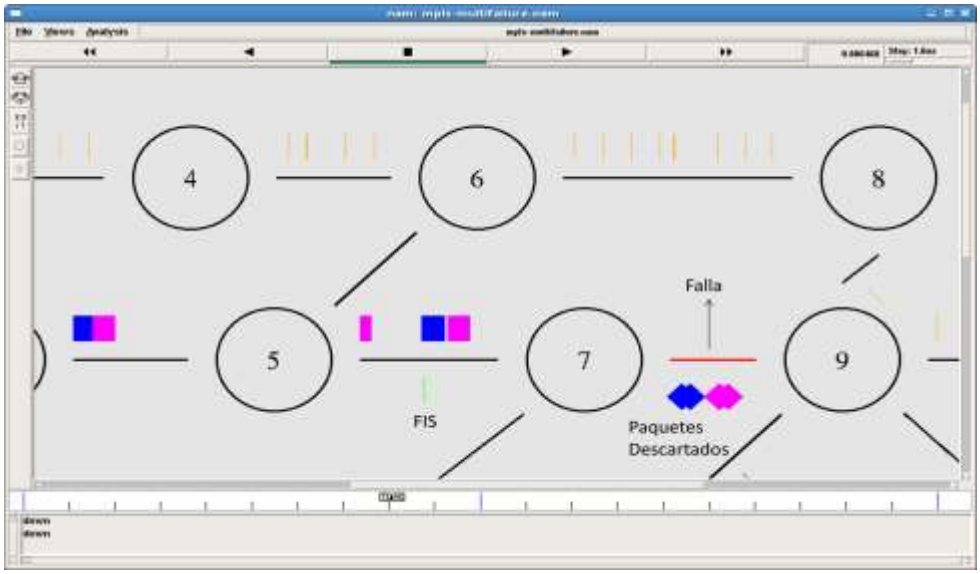


Figura 4-7. Primer evento de falla

Una vez se recibe la señal FIS, el PSL (LSR1) conmuta los tráficos de video y datos hacia el BP1, como se observa en la figura 4-8.

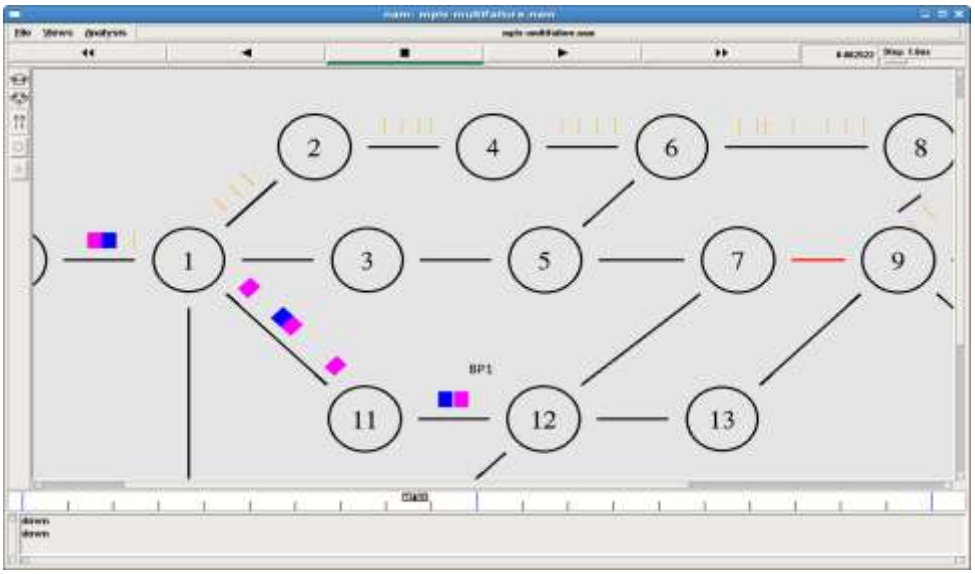
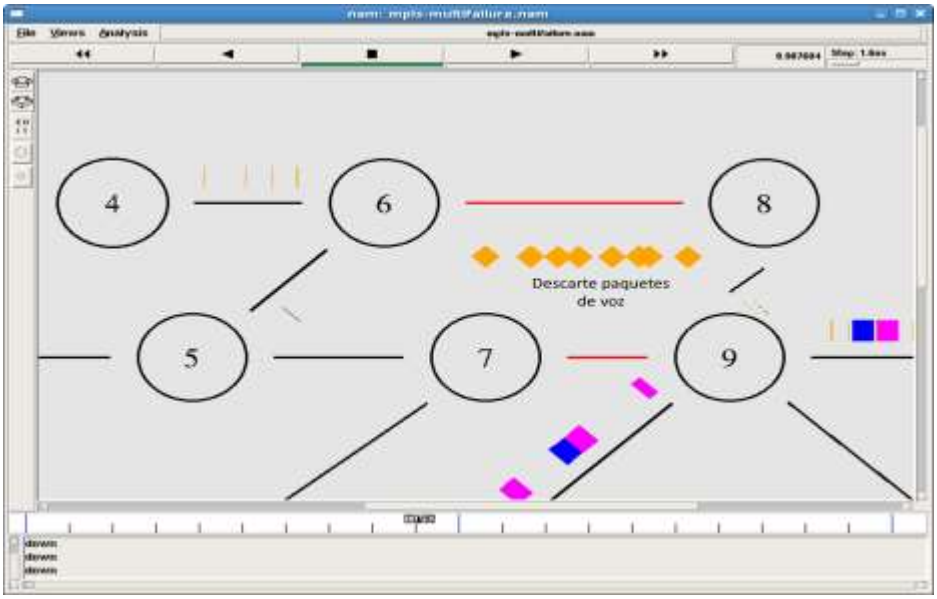


Figura 4-8. Acción de recuperación para la primera falla

En el instante 0.9 de la simulación se presenta el segundo evento de falla, afectando el

enlace LSR6-LSR8 y por tanto al tráfico de voz. De manera similar al anterior caso, hay pérdida de paquetes tanto en el momento en que ocurre la falla así como en el periodo de tiempo previo a la llegada de la señal FIS al nodo LSR1.



.

Figura 4-9. Segundo evento de falla.

La acción de recuperación del método global, conmuta el tráfico de voz hacia el BP1, de manera similar a como ocurrió con la primera falla, como se observa en la figura 4-10.

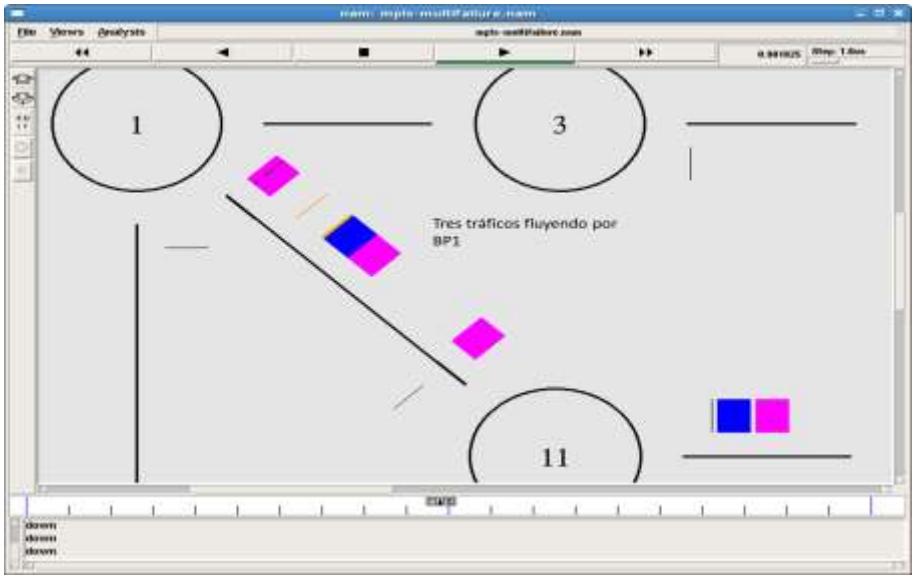


Figura 4-10. Acción de recuperación para el segundo evento de falla.

En el instante 0.95 de simulación conforme se describió en la tabla 4-2, ocurre el tercer evento de falla, afectando el enlace LSR12-LSR13 y por tanto el BP1. Este evento no permite que las acciones de recuperación adoptadas para las otras dos fallas se lleven a cabo de manera exitosa.

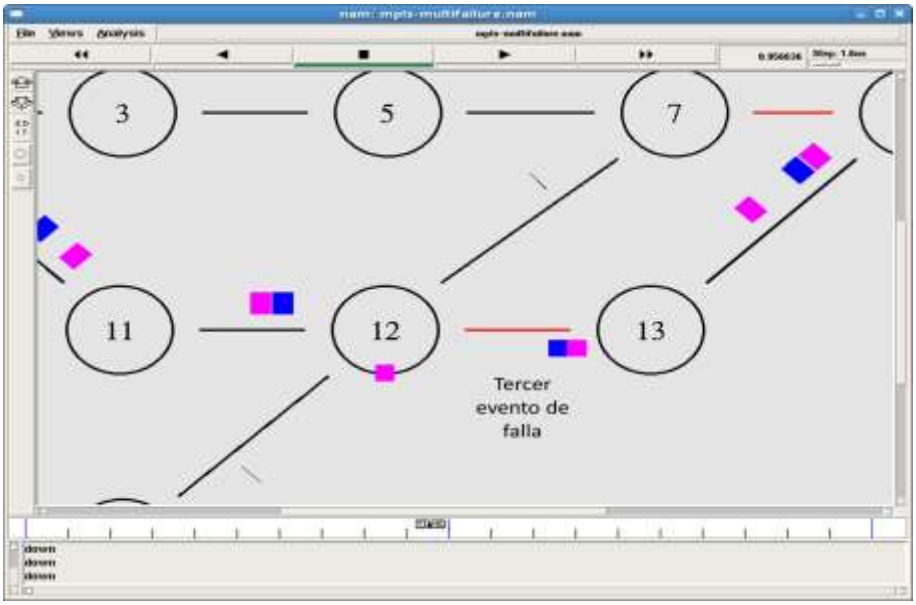


Figura 4-11. Tercer evento de falla.

4.3.2.1 Análisis de Throughput y pérdida de paquetes aplicando mecanismos de recuperación para los casos 2a y 2b.

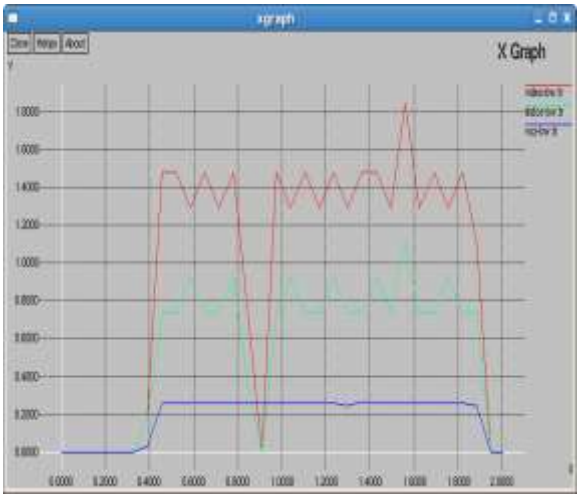
La figura 4-12 presenta las gráficas de throughput para los tres tráficos que corresponden a un único evento de falla (enlace LSR7-LSR9) en donde se aplican los tres métodos de protección (figuras 4-12a, 4-12b y 4-12c). Se evidencia en todas las figuras que los tráficos fluyen normalmente alrededor de su tasa de envío de información hasta el instante 0.8, donde se observa una caída parcial del throughput de los tráficos de video y datos, cuya magnitud varía de acuerdo al método de protección empleado, siendo más pronunciada para los métodos global e inverso (figuras 4-12a y 4-12b) en comparación con el método local (figura 4-12c), en donde la acción de recuperación toma lugar en el nodo contiguo al lugar de la falla y por tanto se evita la pérdida de tiempo asociada con la notificación de la FIS al nodo dotado con funciones PSL como sucede en los primeros dos métodos.

En la figura 4-12b se destaca la presencia de un pico que alcanza los 2500 Kbps en el instante de la conmutación de los tráficos al camino de respaldo, ocasionado porque el tráfico que se re-enruta por el camino de recuperación inverso y el proveniente del nodo 0

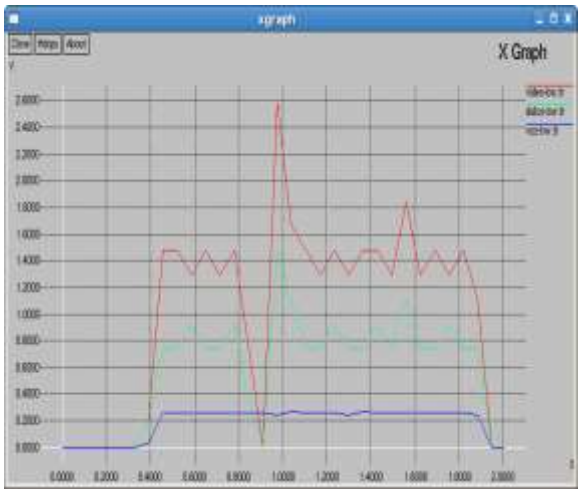
se encuentran en el LSR1 y se direccionan a través del BP1, lo cual genera en el destino un incremento momentáneo en la tasa de información transmitida. Posteriormente, en el instante 1.4 cuando el enlace afectado vuelve a su estado operativo, se observa un nuevo pico en todas las gráficas de throughput de los métodos de protección que sobrepasa los 1800 Kbps, el cual tiene lugar debido al encolamiento de paquetes sobre el LSR9 cuando los tráficos provenientes del BP1 y del WP1 se encuentran. El tráfico de voz no resulta afectado por la falla y por tanto se mantiene casi constante sobre su tasa de transmisión de datos de 256Kbps en todas las gráficas presentadas (tráfico azul).

La figura 4-12d muestra una comparación del porcentaje de pérdida de paquetes en presencia de una falla cuando se aplican los métodos de protección. Se aprecia una notable mejoría en comparación con los resultados obtenidos en la sección 4.3.1.1, alcanzando niveles del 5% aproximadamente para los tráficos de video y de datos en el método global, alrededor del 1% para el inverso y casi del 0% para el método local, resultados que son coherentes respecto al comportamiento descrito en las gráficas de throughput, demostrando así que para escenarios con presencia de una falla el uso de estos mecanismos es muy efectivo.

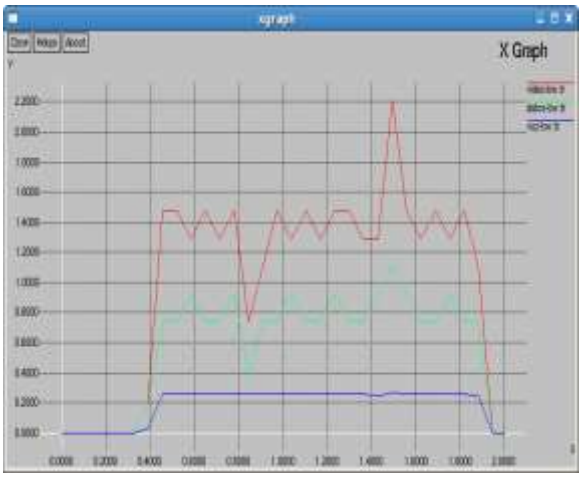
A partir de los resultados obtenidos se concluye que la aplicación de los métodos de protección en contextos de falla simple recupera de manera efectiva los tráficos afectados, razón por la cual no se requiere la adopción de caminos de respaldo distintos a los utilizados en esta sección, no siendo necesario su estudio en las pruebas realizadas en el caso 2b.



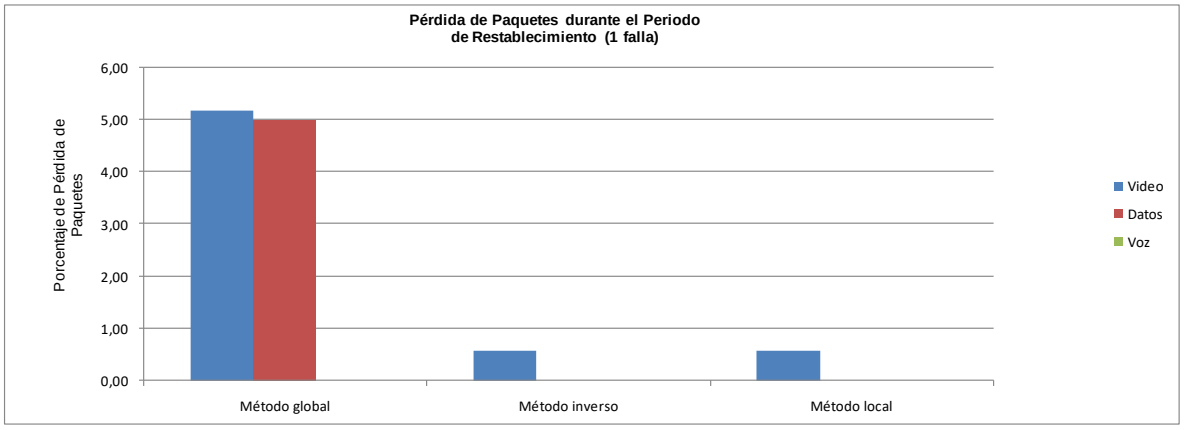
a) Método global



b) Método inverso



c) Método local



d) Pérdida de paquetes para el evento de falla simple

Figura 4-12. Throughput y pérdida de paquetes para el evento de falla simple aplicando los métodos de protección.

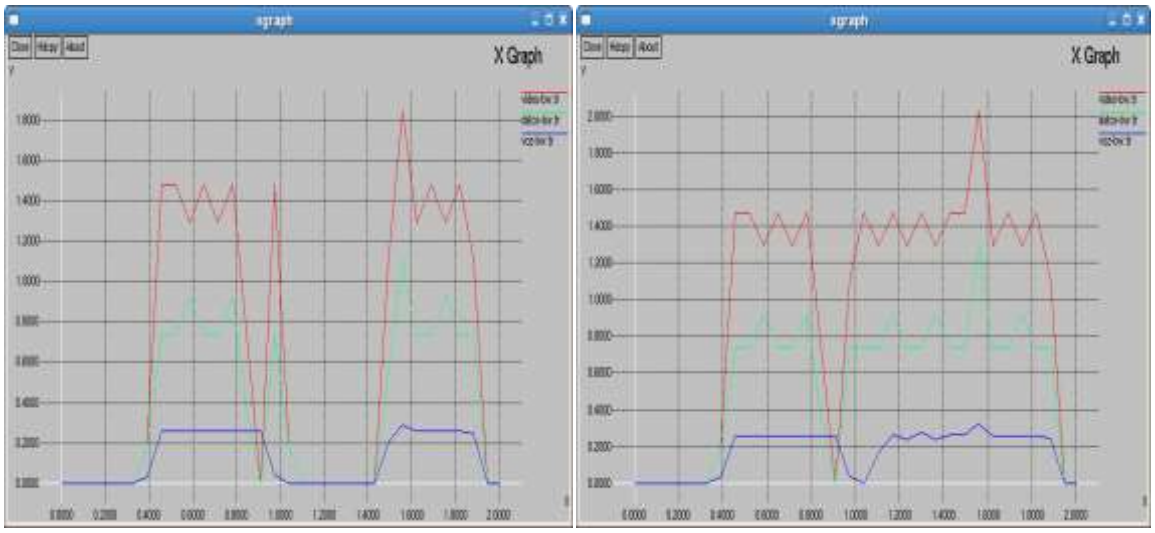
Dentro del análisis del throughput y pérdida de paquetes correspondiente a los casos de falla múltiple en los que se aplican los métodos de protección (casos 2a y 2b del plan de pruebas), se analizan únicamente los eventos de tres fallas, puesto que los resultados de estos en comparación con los obtenidos cuando hay dos fallas son muy semejantes, siendo la única diferencia el comportamiento del tráfico de voz, el cual resulta comprometido solo cuando ocurren tres fallas. Además de lo anterior, el análisis del escenario de red con presencia de tres fallas reviste mayor interés porque afecta todos los tráficos cursantes en la red.

Al aplicar los métodos de protección para el caso 2a, se evidencia que las gráficas de

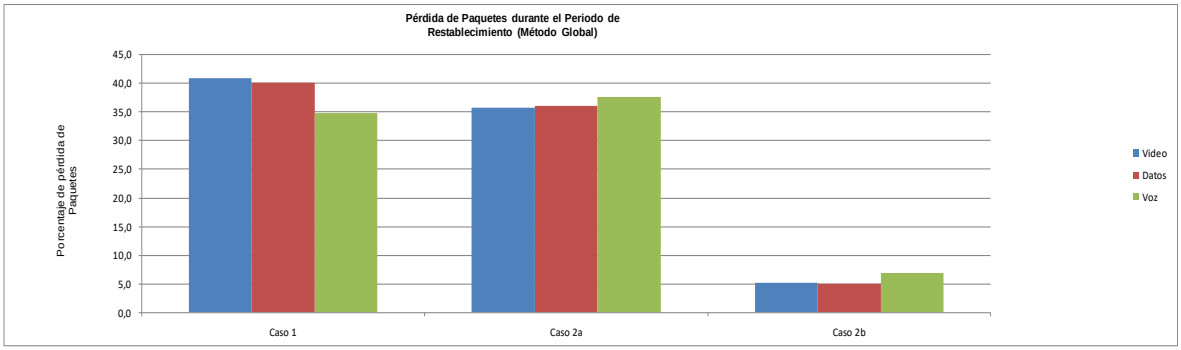
throughput (figuras 4-13a, 4-14a y 4-15a) presentan un comportamiento similar, debido a que las acciones de recuperación adoptadas conforme a la tabla 4-6 no logran la recuperación efectiva de los tráficos, y por tanto se evidencia una caída de throughput menos pronunciada en comparación con la registrada en la figura 4-2 para el caso de tres fallas, además de un pico momentáneo alrededor del instante 0.9 del tiempo de simulación. Estos hechos obedecen a la acción parcial de los métodos que si bien no recuperan de manera efectiva los tráficos comprometidos por fallas, permiten que algunos paquetes alcancen su destino hasta que la ocurrencia de otro evento de falla interrumpa dicho proceso al comprometer los caminos de respaldo empleados. Por esta misma razón, en la pérdida de paquetes asociada al caso 2a para los tres métodos (figuras 4-13c, 4-14c y 4-15c) se observa una leve mejoría en sus porcentajes en comparación con el caso 1, los cuales alcanzan valores comprendidos entre el 30 y 37%.

Las gráficas de throughput correspondientes a la aplicación de los métodos de protección para el caso 2b muestran un comportamiento similar al presentado en el contexto de falla simple expuesto al comienzo de esta sección. En general la caída del throughput no es total para los tráficos afectados cuando los caminos de respaldo asociados a los métodos de protección no se ven comprometidos por eventos de falla conforme se describió en la tabla 4-6, extendiéndose por un periodo de tiempo significativamente menor en contraste con las presentadas en el caso 2a. Los picos en las gráficas que se presentan en el caso 2b en el instante 1.4 obedecen al encolamiento que se genera debido a la confluencia de paquetes provenientes del BP2 y paquetes del WP1 sobre el LSR9, tal como se describió anteriormente. Respecto a la pérdida de paquetes, la mejora porcentual que se obtiene en el caso 2b es muy significativa, puesto que se pasa de valores alrededor del 40% y 35% para los casos 1 y 2a respectivamente, a valores alrededor del 2.5%.

A partir de los resultados obtenidos para el caso 2b, se concluye que la aplicación de los métodos de protección en contextos múlti-falla cuando se escogen caminos de respaldo para el proceso de recuperación que no resulten afectados por eventos de falla, permite la recuperación exitosa de los tráficos, lo cual se ve reflejado en el comportamiento de las gráficas de throughput así como en los bajos porcentajes de pérdida de paquetes obtenidos. Por lo tanto, de la misma manera en que los métodos de protección son efectivos para la recuperación en contextos de falla simple, también se consolidan como una alternativa útil de cara a la problemática de fallas múltiples.

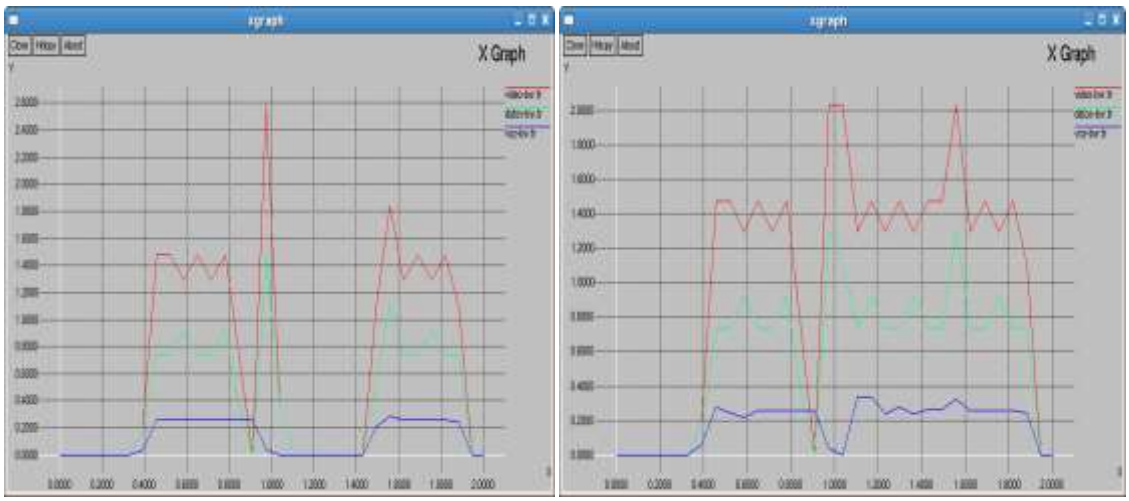


a) Caso 2a **b) Caso 2b**

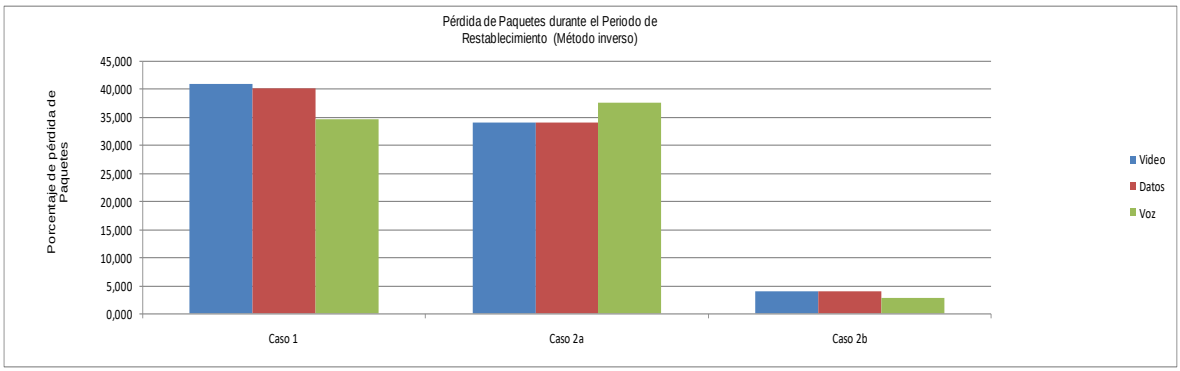


c)

Figura 4-13. Throughput y pérdida de paquetes para el evento de tres fallas en los casos del plan de pruebas usando el método de protección global.

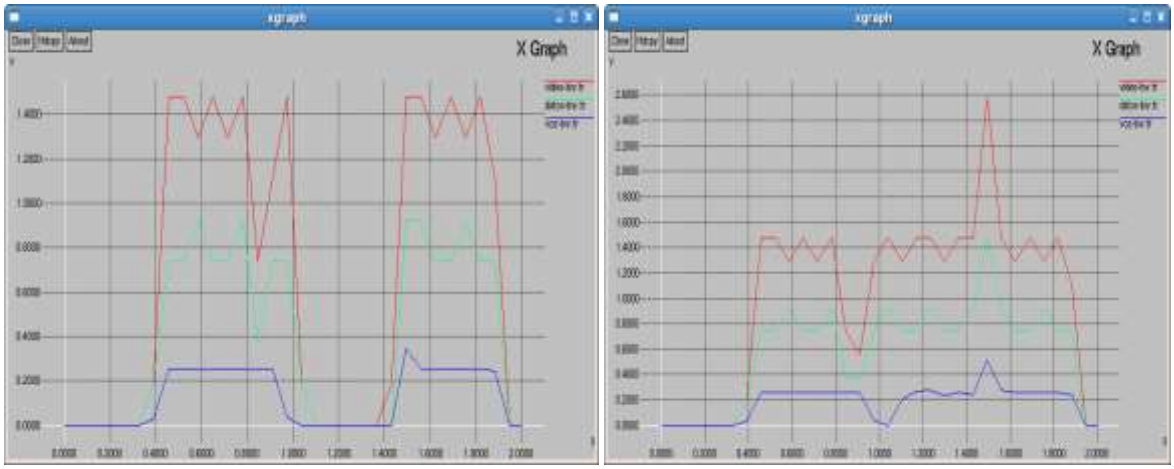


a) Caso 2a **b) Caso 2b**

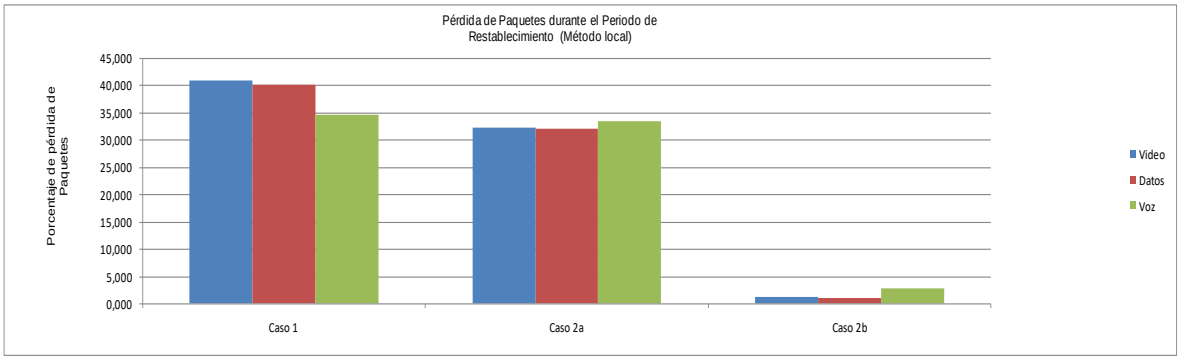


c)

Figura 4-14. Throughput y pérdida de paquetes para el evento de tres fallas en los casos del plan de pruebas usando el método de protección inverso.



a) Caso 2a **b) Caso 2b**



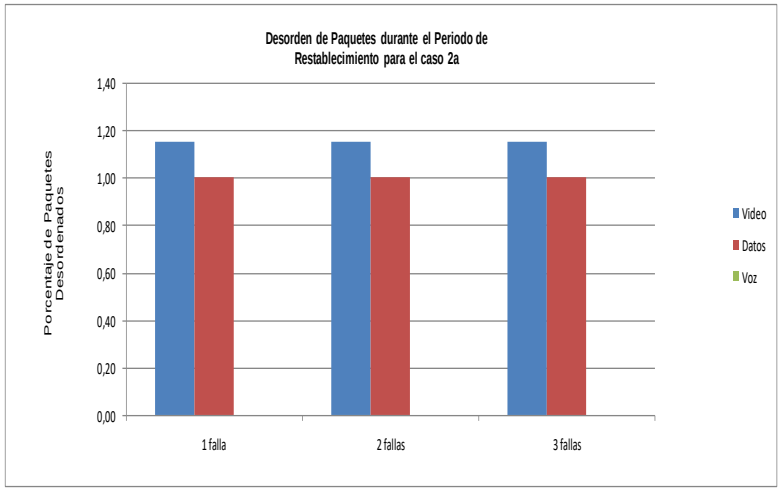
c)

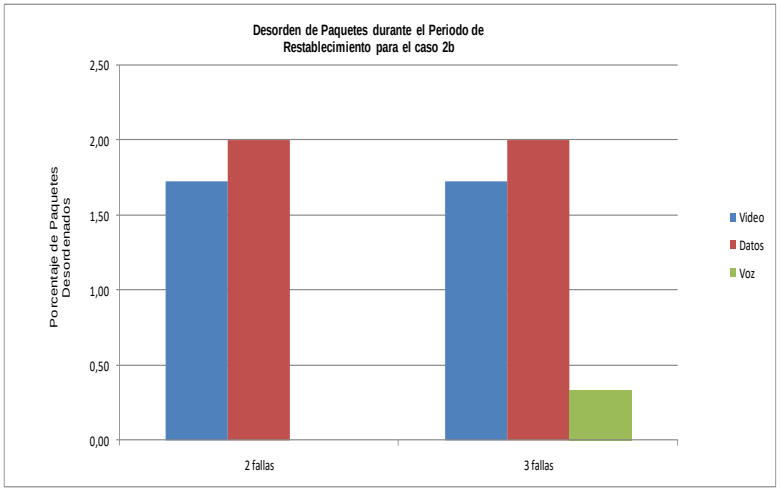
Figura 4-15. Throughput y pérdida de paquetes para el evento de tres fallas en los casos del plan de pruebas usando el método de protección local

4.3.2.2. Análisis del desorden de paquetes.

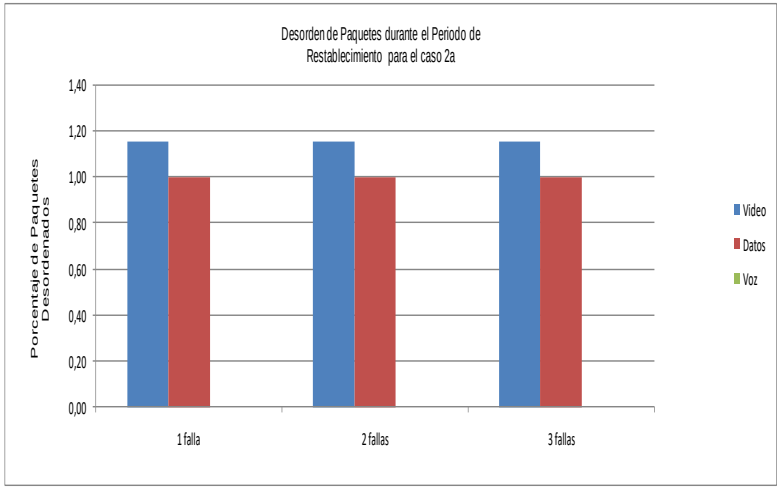
La figura 4-16 muestra el porcentaje de desorden de paquetes cuando se aplican los métodos de protección en los casos 2a y 2b. Para las pruebas correspondientes al caso 2a se evidencia un nivel de desorden similar en los métodos global e inverso, que varía entre el 1 y 1.2% para los tráficos cursantes en todos los eventos de falla programados. Por otra parte, en el método local este porcentaje aumenta a alrededor del 2% para el evento de falla simple, mientras que para los eventos de múltiples fallas su valor varía entre 0.5 y 1.25%. Estos porcentajes en general son muy bajos debido a que las acciones de recuperación se llevan a cabo de manera parcial, lo cual implica que el flujo de paquetes que se conmuta hacia los caminos de respaldo solo experimenta por un corto instante de tiempo el retardo asociado a los mismos, cuyo valor es diferente al de los caminos de trabajo.

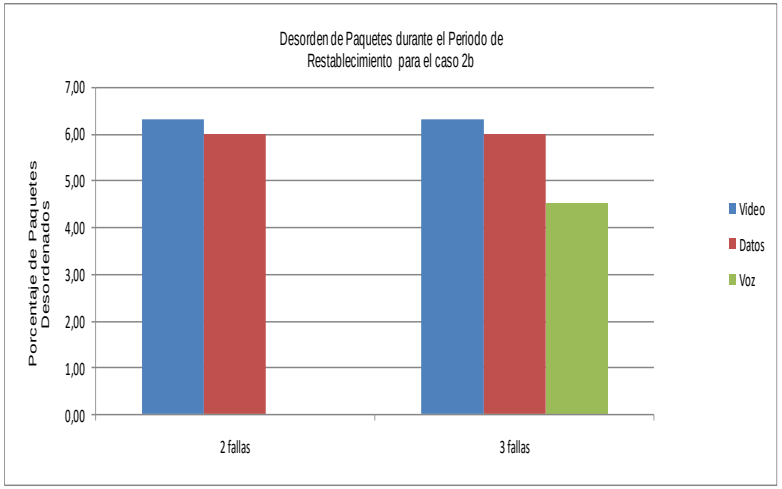
Por otro lado, en los gráficos de porcentajes de desorden del caso 2b se observa un incremento en el desorden introducido a los tráficos recuperados, variando entre el 2 y el 6.5% para todos los eventos de falla cuando se aplican de forma efectiva los métodos de protección. Esto implica que los tráficos afectados deban fluir por periodos de tiempo mayores a través de caminos de respaldo conformados por enlaces que en conjunto suman un valor de retardo mayor al registrado por los caminos de trabajo, en comparación a los del caso 2a, lo cual sumado al encolamiento de paquetes sobre el nodo LSR9 cuando se encuentran los tráficos recuperados por los caminos de respaldo con los tráficos que fluyen nuevamente por el WP1 y WP2, genera un mayor volumen de paquetes desordenados.



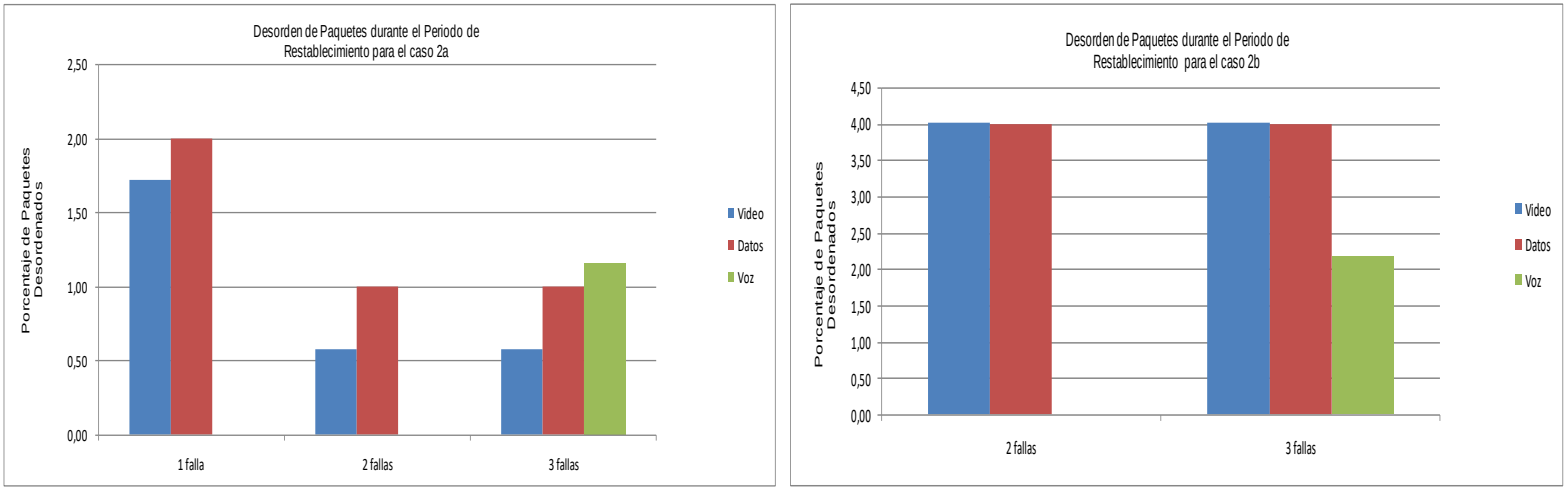


a) Método global





b) Método inverso



c) Método local

Figura 4-16. Porcentaje de desorden de paquetes para los métodos de protección en el caso 2a y 2b del plan de pruebas

4.3.3. Análisis del tiempo de restablecimiento para los tres métodos de protección.

Para la interpretación de los resultados arrojados por el simulador correspondiente al tiempo de restablecimiento se deben tener en cuenta algunas consideraciones que se exponen a continuación:

1. Cuando ocurre una falla en un enlace a través del cual no fluye ningún flujo de tráfico, el tiempo de restablecimiento se define como cero (no se incluye en la tabla).

2. El tiempo de restablecimiento se define como cero en caso de que una falla afecte un flujo de tráfico y no se aplique ningún método de protección para afrontar el problema, o bien cuando la acción de recuperación adoptada para contrarrestar el efecto de uno o varios eventos de falla no se lleva a cabo de manera exitosa, tal como ocurre en los contextos de falla descritos en el caso 1 y 2a del plan de pruebas respectivamente.

El tiempo de restablecimiento en todos los métodos de protección presenta un comportamiento estable ante la presencia de una sola falla. Se evidencia que el tiempo de restablecimiento de RT=34.85 ms es igual en el mecanismo global y el inverso debido a que el enlace afectado por la falla, así como el nodo que la detecta y el nodo encargado de la conmutación del tráfico hacia el camino de respaldo son los mismos, y también por la similitud en el manejo de la señal FIS en dichos métodos. El tiempo de restablecimiento del método local disminuye en forma considerable en comparación con los otros métodos debido a que la distancia D(i,a)=0, por lo que el volumen de pérdida de paquetes es menor. Este método cuenta con el tiempo de restablecimiento más óptimo de todos, sin embargo su principal desventaja es la ineficiencia en el consumo de recursos y la dificultad para establecer cuál enlace es más propenso a sufrir fallas y así determinar qué nodos deben dotarse con funciones de PML y PSL respectivamente.

Por tanto, las características de los tráficos de video y datos que fluyen a través de WP1 no resultan demasiado afectadas debido a la respuesta rápida de los métodos mencionados, cuya eficacia está comprobada en contextos de falla simple.

De acuerdo a la tabla 4-7, en los eventos de falla estudiados no todas las fallas de enlace tienen asignado un valor de tiempo de restablecimiento, debido a que no hay tráficos fluyendo por estos enlaces que se ven comprometidos por fallas, así como se da el caso de que en ellos sí se afecta los flujos de tráfico pero no se adoptan estrategias de recuperación. Por tanto, solamente se presentan los casos en los que se ven afectados los tráficos y además se aplican los métodos de protección para tratar de recuperarlos. Tal es el caso de la falla presente en el enlace LSR12-LSR13 en todos los métodos de protección estudiados en el caso 2a y 2b del plan de pruebas

El tiempo de restablecimiento obtenido por el simulador es de 41.55 ms cuando el LSR7 detecta la falla en todos los casos de falla estudiados en el caso 2a y 2b del plan de

pruebas, valor que supera el resultado calculado de forma analítica. Dicho incremento se debe a que el nodo de ingreso LSR1 procesa más de una FIS debido a la ocurrencia de más de un evento de falla en el modelo de red planteado, lo cual torna más lento el proceso de detección de falla y posterior conmutación del tráfico al camino de respaldo preestablecido. El tiempo de restablecimiento al aplicar el método de protección local es de 4.8 ms en el caso de un único evento de falla y toma valores de 3.5 y 4.8 ms en las demás pruebas realizadas con dos y tres fallas, ya que la distancia d(i,a)=0. Lo anterior hace que el método local sea el más indicado para la recuperación de tráficos cuyos requerimientos de protección sean altos y por tanto exijan tiempos de restablecimiento muy pequeños tales como el streaming de video y audio, de acuerdo a la tabla 3-1.

Finalmente, al evaluar el tiempo de restablecimiento para los métodos global e inverso cuando se simulan eventos de tres fallas, se evidencia un incremento en su valor que supera el cálculo realizado en forma teórica (RT(LSR6)=30.112 ms y RT(LSR7)=30.34 ms y) en contraste con los resultados obtenidos por el simulador ((LSR6)=54.23 ms y RT(LSR7)=37.71 ms), cuya causa reside en la carga adicional que debe soportar el nodo de ingreso al procesar la señal FIS asociada a la ocurrencia de la tercera falla, incidiendo negativamente en el porcentaje de pérdida de paquetes de todos los tráficos, debido a que las fallas comprometen los dos caminos de trabajo. De acuerdo a los resultados arrojados por el simulador en el caso de 3 fallas, el método local nuevamente se consolida como el más optimo de los mecanismos de protección en lo que respecta al tiempo de restablecimiento, ya que la distancia de notificación de fallas es cero, y además cada LSR realiza el proceso de switchover de manera independiente.

Caso 2a			
Número de fallas/ (Nodo(s) que toman la acción de recuperación)	**Global**	**Local**	**Inverso**
1 falla/ (LSR7)	34,85 ms	4.8 ms	34,85 ms
2 fallas/ (LSR7)	41,55 ms	4.8 ms	41,55 ms

	3 fallas/ (LSR6/LSR7)	54,23 ms/37,71 ms	30.17 ms/3,7 ms	54,23 ms/38.2 ms
	Caso 2b			
	2 fallas/ (LSR7)	34,85 ms	4,8 ms	34,85 ms
	3 fallas/ (LSR6/LSR7)	54,23 ms/37,71 ms	30.17 ms/4.8 ms	54,23 ms/38.2 ms

Tabla 4-7. Tiempo de restablecimiento para el caso 2a y el caso 2b del plan de pruebas.

4.3.4. Análisis de retardo y jitter para los tres métodos de protección.

De acuerdo a la recomendación G.1010 de la ITU-T [24], el retardo máximo admitido en aplicaciones que requieran la transmisión de audio y video en tiempo real para asegurar las condiciones óptimas de QoS es de 150 ms, específicamente para servicios de voz de dos vías y videotelefonía que están enmarcados dentro de un entorno conversacional. Por otro lado, aplicaciones como el streaming de audio y video en una vía no son tan restrictivas respecto al retardo, tolerando valores de hasta 10 s.

Además del retardo extremo a extremo, otro parámetro que reviste importancia en aplicaciones de tiempo real es el jitter o variación de retardo entre paquetes, el cual es capaz de alterar la calidad y fluidez de las aplicaciones de video y sonido si su valor es muy grande. Según [24] se requiere un valor de jitter menor a 1ms para el servicio de voz en dos vías, ya que en la práctica el oído humano es muy sensible ante la variación del retardo de la voz. El streaming de audio no es exigente en lo que respecta al retardo, sin embargo requiere un jitter << 1 ms puesto que se espera que este servicio ofrezca mejor calidad que la telefonía convencional. Con respecto al tráfico de video, se toman en consideración los mismos valores de jitter correspondientes a las aplicaciones de voz mencionados anteriormente. El retardo y el jitter no impactan de manera notable el tráfico de datos, ya que su efecto generalmente no es apreciable por el usuario. Por esta razón, este tipo de tráfico no recibe especial consideración respecto a estos parámetros.

Cabe aclarar que en la tabla 4-8 solo se definen valores de retardo y jitter cuando se logra la recuperación efectiva de los tráficos comprometidos por los eventos de falla, por lo cual no se incluyen las pruebas para dos y tres fallas del caso 2a, ya que cuando las acciones de recuperación no se completan de manera exitosa, el simulador no puede calcular estos parámetros de manera precisa.

Al contrastar los tres métodos de protección en la tabla 4-8, se observa que los valores de retardo para los tráficos de video, voz y datos cuando se aplican los métodos de protección global e inverso son similares, variando entre 46,66 y 66,66 ms, y entre 48,33 y 66,86 ms respectivamente para dichos métodos, siendo menores por un pequeño margen los correspondientes al método inverso. En general los retardos asociados al tráfico de voz son menores, puesto que en las pruebas con una y dos fallas no resulta afectado el camino WP2 por el cual este fluye normalmente, y por tanto no se conmuta hacia un camino de respaldo que pueda introducirle mayores retardos. Los valores más altos de retardo para los tres tráficos se obtienen al aplicar el método local, debido a que la longitud del camino de recuperación para éste método es mayor en comparación a la del camino de respaldo de los métodos global e inverso. Sus valores varían entre 46,66 y 94,33 ms, siendo los más altos los correspondientes a los eventos de 3 fallas, puesto que los tres tráficos se re-enrutan por caminos de respaldo.

Ninguno de los valores de retardo sobrepasa el valor 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 y por tanto las aplicaciones soportadas por los mismos no se verían afectadas. Para el tráfico de datos dichos valores son mayores y varían entre 3,05 y 3,34 ms, aunque la restricción de ITU-T no aplica para este tráfico, por lo que no se considera que afecten el desempeño del mismo.

Valores de retardo y jitter para los 3 métodos de protección

Métodos de protección							
Tipos de Tráfico	No de fallas	Global		Inverso		Local	
		Retardo	Jitter	Retardo	Jitter	Retardo	Jitter
Video	1 falla	60,60	0,23	57,80	0,23	63,58	0,23
	2 fallas	66,62	0,23	63,54	0,23	86,70	0,21

		3 fallas	66,66	0,25	63,58	0,24	87,20	0,21
	Datos	**1 falla**	52,63	3,30	50	3,30	70	3,34
		2 fallas	63,15	3,21	60	3,19	80	3,05
		3 fallas	63,18	3,26	60.6	3,21	80,80	3,05
	Voz	**1 falla**	46,66	0,52	48,33	0,52	46,66	0,52
		2 fallas	48,33	0,52	46,66	0,52	46,66	0,52
		3 fallas	57,24	0,56	63.86	0,56	94,33	0,56

Tabla 4-8. Valores de retardo y jitter para los tres métodos de protección.

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

Con base en el análisis de los resultados realizado previamente, se presenta a continuación un análisis del impacto que los eventos de falla (simple y múltiple) ocasionan a los tráficos establecidos para las pruebas de simulación en términos de los parámetros de desempeño evaluados, entendiéndose este como el grado de afectación que tiene sobre la red la ocurrencia de dichos eventos [16][19][22]-[66]. Cabe aclarar que el análisis presentado 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 aplicar a otras topologías distintas con presencia de múltiples fallas y donde fluyan tráficos de diferentes tipos.

4.4.1. Convenciones para la valoración del impacto.

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 [24] y a los resultados arrojados por la simulación, los cuales se presentan en la tabla 4-9. Debido a que 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, no se tienen en cuenta en la siguiente tabla.

Tipo de tráfico	Porcentaje de pérdida de paquetes (%)			Desorden de paquetes (%)			Tiempo de Restablecimiento (ms)			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

Tabla 4-9. Rangos de valores para la valoración del impacto de los eventos de falla

4.4.2. Impacto ocasionado por eventos de falla simple y múltiple sin la aplicación de mecanismos de recuperación (Caso 1 del plan de pruebas).

La tabla 4-10 muestra el impacto ante la ocurrencia de una, dos y tres fallas que experimentan los tráficos transportados por la red cuando no se aplica ningún mecanismo de recuperación. En el análisis del impacto presentado a continuación solo se considera el comportamiento de la pérdida y el desorden de paquetes de entre los cinco parámetros de desempeño establecidos para evaluar el impacto ocasionado en los tráficos cursantes, puesto que al no aplicarse ninguna estrategia de recuperación no se tiene en cuenta el tiempo de restablecimiento, además de que el valor de retardo y jitter experimentado por los tráficos afectados en los casos de falla mencionados no se puede determinar con precisión por el simulador y por tanto no se define.

El impacto ocasionado a los tráficos en términos del porcentaje de pérdida de paquetes es alto en todos los casos de falla estudiados como se aprecia en la tabla 4-10, 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 el impacto ocasionado al tráfico de voz en términos de la pérdida y desorden de paquetes es bajo.

A raíz de lo anterior, la calidad de servicio de las aplicaciones y servicios soportados por estos tráficos se verá degradada de manera crítica, hecho que inevitablemente perjudicara la experiencia de uso de los usuarios finales y por ende redundara en la disminución de la credibilidad del operador de servicios. Lo anterior se evidencia claramente en las caídas del throughput correspondientes al caso 1 y en las gráficas de porcentajes de paquetes perdidos, analizadas anteriormente en la sección 4.3.1.1.

Por otro lado, el impacto que tiene el desorden de paquetes en los diferentes casos de falla es bajo, puesto que no se aplican acciones de recuperación y por ende las causas de desorden asociadas al funcionamiento de los mismos 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.

Impacto ocasionado en los tráficos cursantes sin la aplicación de mecanismos de protección (caso1)			
Número de eventos de falla	Tipos de tráfico	Pérdida de paquetes	Desorden de paquetes
Una falla	Video	Alto	Bajo
	Datos	Alto	Bajo
	Voz	Bajo	Bajo
Dos fallas	Video	Alto	Bajo
	Datos	Alto	Bajo
	Voz	Alto	Bajo
Tres fallas	Video	Alto	Bajo
	Datos	Alto	Bajo
	Voz	Alto	Bajo

Tabla 4-10. Valoración cualitativa del impacto ocasionado a los tráficos cursantes para uno, dos y tres eventos de falla sin la aplicación de mecanismos de protección.

4.4.3. Impacto ocasionado por eventos de falla simple y múltiple al aplicar los métodos de protección (Caso 2a y 2b del plan de pruebas).

4.4.3.1. Impacto ocasionado por eventos de falla simple en los tráficos cursantes.

La tabla 4-11, presenta el impacto en términos de los parámetros de desempeño que experimentan los tráficos cursantes ante la ocurrencia de un único evento de falla en la red cuando se aplican los métodos de protección. La estimación del impacto en el caso de una falla para los diferentes tráficos se realiza con base en el evento de falla programado

en el enlace LSR7-LSR9 para cada uno de los métodos de protección. En dichos casos se afectan los tráficos de video y datos respectivamente, y en ninguno de ellos resulta afectado el tráfico de voz puesto que el WP2 no se ve comprometido.

El impacto asociado con la pérdida de paquetes para el método de protección global es alto, debido al tiempo de que toma la señal FIS para alcanzar el PSL, durante el cual hay descarte de paquetes. Para los métodos local e inverso, se registra una pérdida nula de paquetes por lo que el impacto asociado es bajo, a pesar de que se evidencia una caída en el throughput para los tráficos comprometidos.

En cuanto al desorden de paquetes el impacto es bajo para todos métodos de protección, debido a que solo dos de los tres tráficos se ven comprometidos por fallas y además el retardo de BP1 usado como camino de respaldo, es similar al retardo del WP1 por lo que los paquetes no pierden su secuencia al alcanzar el destino.

En términos del tiempo de restablecimiento se tiene un impacto bajo para el método local debido a las acciones rápidas de re-enrutamiento que se toman por los enrutadores contiguos a los enlaces afectados por la falla, y por lo tanto no se tiene en cuenta el tiempo de notificación de la señal FIS, la cual viaja hacia el nodo de ingreso encargado de conmutar los tráficos afectados al BP1, el cual si se considera en los métodos global e inverso, quienes presentan tiempos de restablecimiento mayores y en consecuencia un impacto medio.

El impacto relacionado con el retardo es bajo para todos los mecanismos de acuerdo a los valores definidos en la tabla 4-11, y por tanto su influencia sobre las aplicaciones asociadas a los tráficos que fluyen a través de la red no es relevante. De igual manera, el impacto ocasionado por el jitter es bajo para el tráfico de video y voz en todos los métodos analizados, por lo cual no repercute de manera significativa sobre los servicios prestados.

En comparación con los resultados obtenidos en la sección 4.3.2.1 referentes a la pérdida y al desorden de paquetes en el caso de falla simple, se evidencia que cuando se aplican los métodos de protección en estos contextos, se obtiene una mejora significativa del porcentaje de pérdida de paquetes, logrando un impacto bajo en los tráficos afectados. Sin embargo, no ocurre lo mismo con el desorden de paquetes introducido, cuyo impacto si bien es bajo en los dos casos, es un poco mayor cuando se aplican los métodos de protección por las razones descritas previamente.

Impacto ocasionado en los tráficos cursantes por un evento de falla simple.						
Métodos de protección	**Tipos de tráfico**	**Pérdida de paquetes**	**Desorden de paquetes**	**Tiempo de Restablecimiento**	**Retardo**	**Jitter**
Método Local	**Video**	**Bajo**	**Bajo**	**Bajo**	**Bajo**	Bajo
	Datos	**Bajo**	**Bajo**	**Bajo**	**NA**	**NA**
	Voz	**-**	**-**	**-**	**Bajo**	Bajo
Método Reverse	**Video**	**Bajo**	**Bajo**	Medio	**Bajo**	Bajo
	Datos	**Bajo**	**Bajo**	Medio	**NA**	**NA**
	Voz	**-**	**-**	-	**Bajo**	Bajo
Método Global	**Video**	Alto	Bajo	Medio	Bajo	Bajo
	Datos	Alto	Bajo	Medio	**NA**	**NA**
	Voz	-	-	-	Bajo	Bajo

Tabla 4-11. Valoración cualitativa del impacto ocasionado a los tráficos cursantes en contextos de falla simple.

4.4.3.2. Impacto ocasionado por múltiples fallas en los tráficos cursantes (Caso 2a del plan de pruebas).

En este análisis solo se tienen en cuenta tres de los cinco parámetros de desempeño establecidos para evaluar el impacto ocasionado en los tráficos cursantes (pérdida de paquetes, desorden de paquetes y tiempo de restablecimiento), puesto que el valor de retardo y jitter experimentado en los casos de falla donde no hay recuperación efectiva del tráfico no se puede determinar con precisión por el simulador y por tanto no se define. Por otro lado, el tráfico de voz solo resulta comprometido en los casos con presencia de tres fallas, por lo que la valoración del impacto ocasionado sobre este se realiza con base en estos casos.

En la tabla 4-12 se puede apreciar que el impacto sufrido por los tráficos en términos del número de paquetes perdidos es alto en todos los métodos de protección, debido a que

no se logra su recuperación efectiva, lo cual trae como consecuencia una notable degradación de las características de los tráficos y de las aplicaciones soportadas por ellos. Este comportamiento se evidencia en las caídas del throughput correspondientes a cada método así como en las gráficas de porcentajes de paquetes perdidos descritas en la sección 4.4.2.

El impacto que tiene el desorden de paquetes en los diferentes casos es bajo, puesto que la acción de los métodos de protección se completa de forma parcial y por tanto las causas de desorden relacionadas al funcionamiento de los mismos 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 son significativas.

Si bien en el caso 2a del plan de pruebas los métodos de protección no recuperan el tráfico de manera efectiva ante la presencia de fallas múltiples, se considera el impacto relacionado con el tiempo de restablecimiento, debido a que en todos los casos de falla analizados los métodos de protección alcanzan a realizar la conmutación de los tráficos afectados hacia un camino de respaldo preestablecido. Según la tabla 4-12, se observa que el método local presenta el impacto más bajo respecto al tiempo de restablecimiento, mientras que el impacto para los otros mecanismos es alto, lo cual se debe al funcionamiento propio de cada uno de los métodos de protección y a la distancia que existe entre el punto donde ocurre la falla y el nodo encargado de la acción de recuperación, teniendo en cuenta que para los mecanismos inverso y global una distancia mayor implicaría un mayor tiempo de notificación de la FIS y por ende un mayor tiempo de restablecimiento.

Respecto a la valoración del impacto para el conjunto de experimentos descrito en la sección 4.3.1.1 para los casos de más de dos fallas, se observa que tanto en esas pruebas así como las correspondientes al caso 2a las repercusiones sobre el tráfico transportado en términos de la pérdida de paquetes son críticas, sin embargo cuando se aplican los métodos de protección en presencia de fallas sobre los caminos de respaldo para la recuperación de los tráficos, se obtiene una leve mejora sobre los resultados entregados ya que ellos son capaces de recuperar algunos paquetes comprometidos por los eventos de falla. Por otro lado, el impacto causado por el desorden de paquetes es bajo en los dos conjuntos de pruebas analizados, siendo ligeramente mayor cuando se aplican los métodos de protección conforme se ha descrito previamente.

A partir de lo anterior se puede concluir que la recuperación es beneficiosa bajo todo punto de vista porque permite mejorar las condiciones de los tráficos afectados por la presencia de fallas en cualquier punto de la red, siendo siempre preferible su uso en lugar de dejar la red completamente desprotegida.

	Impacto ocasionado en los tráficos cursantes en contextos multifalla (Caso 2a)				
	Métodos de protección	**Tipos de tráfico**	**Pérdida de paquetes**	**Desorden de paquetes**	**Tiempo de Restablecimiento**
	Método Local	**Video**	**Alto**	**Bajo**	**Bajo**
		Datos	**Alto**	**Bajo**	**Bajo**
		Voz	**Alto**	**Bajo**	**Bajo**
	Método Reverse	**Video**	**Alto**	**Bajo**	Alto
		Datos	**Alto**	**Bajo**	Alto
		Voz	**Alto**	**Bajo**	Alto
	Método Global	**Video**	**Alto**	Bajo	Alto
		Datos	**Alto**	Bajo	Alto
		Voz	**Alto**	Bajo	Alto

Tabla 4-12. Valoración cualitativa del impacto ocasionado a los tráficos cursantes en contextos multifalla (Caso 2a del plan de pruebas).

4.4.3.3 Impacto ocasionado por múltiples fallas en los tráficos cursantes (Caso 2b del plan de pruebas).

Según los resultados de la tabla 4-13, se puede observar una notable mejora del impacto ocasionado a los tráficos de video, datos y voz que fluyen a través de la red planteada tras la ocurrencia de múltiples fallas. Se evidencia que el método de protección global es el que registra el impacto más alto en término del número de paquetes perdidos en comparación con los demás métodos para los tres tipos de tráfico, sin embargo el impacto del desorden de paquetes introducido es el más bajo de todos, puesto que no hay combinación de tráficos que fluyan en distintos sentidos en un mismo LSP como sucede en el método inverso, que registra el impacto más alto según la tabla.

El método local es el que registra el impacto más bajo en cuanto a la pérdida de paquetes, ya que ofrece el menor tiempo de restablecimiento debido a que la conmutación del tráfico afectado por la falla toma lugar en el mismo nodo que detecta su aparición, hecho que lo diferencia de los demás métodos donde este proceso ocurre en el

nodo de ingreso al dominio MPLS. En este sentido, el método local 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 [13][16]-[20].

En todos los métodos analizados, se cumplió con las restricciones de retardo y jitter requeridas para el correcto funcionamiento de las aplicaciones y servicios asociados a los tráficos de voz, video y datos, gracias en parte al bajo retardo introducido por los enlaces que componen los caminos de trabajo y de respaldo. Teniendo en cuenta lo anterior, 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, para que de esta forma su efecto no perjudique la calidad de las aplicaciones soportadas por la red. Por otro lado, 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 [16]-[20].

Finalmente se concluye que 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 comprobado en 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 ante la presencia de fallas. No obstante, su principal desventaja reside en la utilización ineficiente de recursos que realiza, además de la necesidad de dotar a la red con tantos pares de nodos PSL y PML como enlaces se desee proteger.

De igual forma, se evidencia claramente que 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**

Tabla 4-13. Valoración cualitativa del impacto ocasionado a los tráficos cursantes en contextos multifalla (Caso 2b del plan de pruebas).

Este capítulo presentó un análisis detallado del desempeño que tienen los métodos de protección cuando se aplican en contextos de falla simple y múltiple, para lo cual se tuvieron en cuenta algunos parámetros de desempeño (pérdida y desorden de paquetes, tiempo de restablecimiento, retardo y jitter). De igual manera se utilizaron estos parámetros para la realización de una valoración del impacto ocasionado sobre los tráficos cursantes con base en los rangos establecidos por la ITU-T y los resultados arrojados por la simulación, determinando el grado de afectación para cada uno de los parámetros cuando se aplican los métodos de protección en los tres casos que componen el plan de pruebas.

El capítulo 5, presenta las conclusiones del proyecto, recomendaciones y trabajos futuros a implementar referentes a esta temática.

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En este capítulo se presentan las conclusiones obtenidas a partir de la realización del proyecto con base en los objetivos planteados, los resultados del plan de pruebas y el contenido de los diferentes capítulos. Adicionalmente se presentan recomendaciones y trabajos futuros relacionados con la problemática de fallas en redes MPLS con miras a continuar la investigación y el desarrollo de otros proyectos relacionados con esta temática.

5.1. CONCLUSIONES

Respecto a la problemática de fallas:

- ✓ Las redes MPLS están propensas a sufrir el impacto de diversos tipos de fallas que afectan el desempeño de los tráficos transportados.

- ✓ El estudio matemático y teórico realizado sobre la ocurrencia de eventos de falla en la red indica de forma clara que existe independencia entre dichos eventos, lo cual hace menos complejo el desarrollo de las pruebas de simulación.

- ✓ 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.

Respecto al desarrollo de la simulación:

- ✓ 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 planteamiento de un escenario de simulación con características que se asemejan a las encontradas en las redes reales permitió el desarrollo de un análisis a partir del cual se obtuvieron resultados relevantes.

Respecto al análisis de los resultados de la simulación:

- ✓ 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.

- ✓ El impacto que sufren los tráficos cuando no se implementan mecanismos de recuperación es tan severo como cuando su ejecución no se completa de manera exitosa.

- ✓ La ocurrencia de fallas en los caminos de respaldo afecta de manera sustancial el desarrollo de las acciones de recuperación, imposibilitando que los tráficos inyectados a la red lleguen de manera exitosa a su destino.

- ✓ 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.

5.2. RECOMENDACIONES.

Algunos aspectos relevantes que enmarcaron el desarrollo del proyecto y que se pueden tener en cuenta para el estudio de otros trabajos sobre la temática en cuestión son:

- ✓ Se recomienda que la Universidad del Cauca destine más recursos para adquirir licencias de herramientas de simulación más completas, que cuenten con interfaces gráficas amigables y de manipulación intuitiva, de manera que se incentive el desarrollo de proyectos de mayor envergadura que aporten a la línea de investigación del GNTT.

- ✓ Seguir de manera detallada los pasos de instalación para la herramienta de simulación NS-2, así como la de los módulos adicionales, teniendo en cuenta la distribución de Linux sobre la que se lleva a cabo, puesto que no todas son compatibles o bien pueden generar problemas en el correcto funcionamiento del simulador.

- ✓ Para practicas de simulación que impliquen la ejecución de muchas pruebas se recomienda el desarrollo de scripts tcl por separado, puesto que la capacidad de procesamiento que exige el simulador NS-2 para la compilación de los mismos es alta y por tanto la integración de ellas en un único script sería ineficiente.

- ✓ Definir adecuadamente las características de los escenarios de red donde se llevan a cabo las pruebas de simulación, tales como retardos, anchos de banda para los enlaces, características de los tráficos cursantes, etc., pues si no se dimensionan

adecuadamente los resultados obtenidos relacionados con los parámetros de observación analizados no serán confiables.

5.3. TRABAJOS FUTUROS.

La recuperación en redes MPLS es una temática amplia, la cual comprende una gran variedad de tópicos y aspectos de interés que no se contemplaron en el desarrollo del presente proyecto. A continuación se proponen algunas ideas sobre trabajos futuros a desarrollar relacionados con esta línea de investigación.

- ✓ Realizar una integración de los métodos de protección junto con técnicas de restablecimiento para afrontar de manera más óptima la problemática de la recuperación ante eventos de falla.

- ✓ Se propone el análisis y utilización del protocolo RSVP-TE para la realización de trabajos futuros en esta línea de investigación, puesto que en la actualidad es el protocolo de distribución de etiquetas más usado, además de que brinda varias ventajas en comparación a LDP.

- ✓ Se propone realizar un estudio de la problemática de fallas para redes basadas en la Conmutación de Etiquetas Multi-Protocolo Generalizado (GMPLS: Generalized Multi Protocol Label Switching), así como realizar la simulación de su funcionamiento en NS u otro simulador que disponga de un módulo adecuado para dicho propósito.

BIBLIOGRAFÍA.

[1]Barakovic, J, Bajric, H, Husic, A., "Multimedia Traffic Analysis of MPLS and non-MPLS Network," Multimedia Signal Processing and Communications, 48th International Symposium ELMAR-2006 basado en, vol, no, pp.285-288, Junio 2006.

[2] Autenrieth, A, Kirstadter, A., "Engineering End-to-End IP Resilience Using Resilience Differentiated QoS". Communications Magazine, IEEE, vol 40, pág 50-57, Enero 2002.

[3] itage, G., "MPLS: The magic behind the myths [multiprotocol label switching] " Communications Magazine, IEEE , vol.38, no.1, pp.124-131, Enero de 2000.

[4] Olof Peterson, J.M., "MPLS Based Recovery Mechanisims" Tesis de Maestría, Universidad de Oslo, Noruega, 2005.

[5] Lawrence,Jeremy., "Designing Multiprotocol Label Switching Networks". Artículo Communication Magazine, Julio 2001.

[6] Sharma, V, Hellstrand, F., "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery" IETF 3469, Febrero 2003.

[7] R, Cohen, G, Nakibly., "Maximizing restorable throughput in MPLS networks". Instituto de Tecnología Technion, Israel, Junio 2007.

[8] Calle, E, L Marzo, J, Urra, A, Vila, P., "Enhancing MPLS QoS routing algorithms by using the Network Protection Degree paradigm". Instituto de Informática y Aplicaciones, Universidad de Girona, España, Diciembre 2003.

[9] G, Bal´azs, Orincsay, D, Kern, Andr´as., "Surviving Multiple Network Failures Using Shared Backup Path Protection". HSNLab, Universidad de Tecnología y Economía de Budapest, Budapest, Hungría, Julio 2003.

[10] Banimelhem, O, Agarwal, A, Atwood, J., "A tree division approach to support local failure recovery for multicasting in MPLS networks". Systems Communications, 2005. Proceedings, basado en vol no, pp. 249-254, 14-17, Agosto 2005.

[11] Changcheng Huang Minzhe Li, Srinivasan, A, "A Scalable Path Protection Mechanism for Guaranteed Network Reliability". Reliability, IEEE Transactions on, vol 56, ed 2, pág 254-267, Junio 2007.

[12] Hundessa, G.L, Domingo-Pascual, J., "Optimal and guaranteed alternative LSP for multiple failures", Computer Communications and Networks, ICCCN 2004. Proceedings. 13th International Conference on, 2004, Pág 59-64.

[13] Vasseur, J, Pickavet, M, Demeester, P., "Network Recovery- Protection and Restoration of Optical, SONET-SDH, IP and MPLS",The Morgan Kaufmann Series in Networking, 2004

[14] Rosen, E, Viswanathan, A, Callon, R., "Multiprotocol Label Switching Architecture (RFC 3031)", IETF RFC 3031, Enero 2001.

[15] Canalis, María Sol., "MPLS: Multiprotocol Label Switching: Una Arquitectura de Backbone para la Internet del Siglo XXI", Departamento. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina, 2006.

[16] Hundessa, G.L., "Enhanced Fast Rerouting Mechanisms for Protected Traffic in MPLS Networks". Tesis Doctoral, Departamento de Arquitectura de Computadores, Universidad Politécnica de Cataluña, España, 2003.

[17] Rahman, M.A, Kabir, A.H, Lutfullah, K.A.M, Hassan, M.Z., Amin, M.R., "Performance analysis and the study of the behavior of MPLS protocols," Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on , vol., no., pp.226-229, 13-15, Mayo 2008.

[18] Alwayn, V, "Advanced MPLS design and implementation", Cisco Press, Indianapolis, USA, 2002

[19] Calle, E, Marzo, J.L, Urra, A., "Protection Performance Components in MPLS Networks". Instituto de Informática y Aplicaciones, Universidad de Girona, España, 2003.

[20] Hadjiona, Maria, Georgiou, Chryssis, Vassiliou, Vasos., "A Hybrid Fault-Tolerant Algorithm for MPLS Networks", Departamento de Ciencias de la Computación, Universidad de Chipre, Diciembre 2007.

[21] Avizienis, A, Laprie, J, Randell, B, Landwehr, C., "Basic concepts and taxonomy of dependable and secure computing," Dependable and Secure Computing, IEEE Transactions on , vol.1, no.1, pp. 11-33, Jan, Marzo, 2004.

[22] Marzo, J, Calle, E, Scoglio C, Trincha, A., "Adding QoS Protection in Order to Enhance MPLS QoS Routing", Instituto de Informática y Aplicaciones, Universidad de Girona, España, 2003.

[23] Harrison, E, Farrel, A, Miller, B., "Protection and Restoration in MPLS Networks version 2", Data Connection Limited, Enfield, Reino Unido, 2006.

[24] 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”. Publicado en Noviembre 1, 2001.

[25] Sahel Alouneh; Anjali Agarwal; Abdeslam En-Nouaary, "A Novel Approach for Fault Tolerance in MPLS Networks," Innovations in Information Technology, 2006 , vol., no., pp.1-5, Nov. 2006.

[26] Banimelhem, O, Agarwal, A, Atwood, J.W.,“A New MPLS-based Local Failure Recovery for Multicast Communication,” Computer Systems and Applications, 2006. IEEE International Conference on, basado en Vol, no, pp 228-231, Marzo 2006.

[27] Autenrieth, A., “Recovery time analysis of differentiated resilience in MPLS”, Design of Reliable Communication Networks, 2003. (DRCN 2003). Proceedings. Fourth International Workshop on, basado en vol, no, pp 333-340, Octubre 2003.

[28] Markopoulou, A, Iannaccone, G, Bhattacharyya, S,. Chen-Nee, Chuah; Diot, C., "Characterization of failures in an IP backbone," INFOCOM 2004. Twenty-third AnnualJoint, Conferencia de IEEE Computer and Communications Societies , vol.4, no., pp. 2307-2317 vol.4, 7-11, Mazo, 2004.

[29] Avizienis, A, Laprie, Jean-Claude, Randell, Brian., “Fundamental Concepts of Dependability”, Departamento de Ciencias de la Computación, Universidad de Newcastle, Reino Unido, 2003.

[30] Hussain, I., “Fault-Tolerant IP and MPLS networks”. Cisco Press, Indianapolis, USA, 2005.

[31] Banimelhem, O, Atwood, W, Agarwal, A., “Resiliency issues in MPLS networks,” Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on, basado en Vol 2, no, pp 1039-1042, Marzo 2003.

[32] Iannaccone, G, Chuah, C, Mortier, R, Bhattacharyya, C, Diot, C., “Analysis of link failures in an IP backbone” Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement, pp. 237-242, Marsella, Francia, 2002.

[33] Kuhn, Richard., “Sources of Failure in the public switched telephone network”, National Institute of Standards and Technology, 1997.

[34] Vasseur, J, Pickavet, M, Demeester, P, “Network Recovery- Protection and Restoration of Optical, SONET-SDH, IP and MPLS“,The Morgan Kaufmann Series in Networking, 2004.

[35] "Carrier IP Network Design for Performance and Dependability"., White paper, Nortel Networks 2004.

[36] Ahola, Kimmo, Myötyri, Eija, Norros Ilkka , Norros, Leena, Pulkkinesn, Urho , Raatikainen, Pertti, Suihko, Tapio,. "The dependability of an IP network – what is it?", VTT-Centro de investigación técnico de Finlandia, paper, 2006.

[37] Kanoun, K., "DBench Dependability Benchmarks," DBench, Project IST-2000-25425, eds., pp. 233, Mayo 2004.

[38] Urra Fabregas, Anna., "Multi-layer survivability: routing schemes for GMPLS-based networks". Tesis Doctoral. Instituto de Informatica y Aplicaciones, Universidad de Girona, España, 2006.

[39] Whaley, A, Boring, R, Blackman, H, McCabe, P, Hallbert, B., "Lessons Learned from Dependency Usage in HERA: Implications for THERP-Related HRA Methods", Joint 8th Annual Conference on Human Factors and Power Plants and the 13th Annual Workshop on Human Performance", Agosto 2007.

[40] Krishnaswamy, Shonali, Wai Loke, Seng, Zaslavsky, Arkady., "Estimating Computation Times of Data-Intensive Applications". IEEE DISTRIBUTED SYSTEMS ONLINE. IEEE Computer Society, 2004.

[41] Lepropre, Jean, Leduc, Guy,. "Inferring Groups of Correlated Failures"., Universidad de Liege, Belgica, 2006

[42] Weidong, Cui, Stoica,Ion, Katz, Randy., "Backup Path Allocation Based On A Correlated Link Failure Probability Model In Overlay Networks". Departamento de Ingeniería Eléctrica y Ciencias de Computación. Universidad de Berkeley. Estados Unidos, 2004

[43] Haque, Anwar, Ho, Pin-Han, Boutaba, Raouf., "Group shared protection for spare capacity reconfiguration in optical networks". Universidad de Waterloo, Canada, 2005.

[44] Calle Ortega, Eusebi, "Enhanced fault recovery methods for protected traffic services in GMPLS networks". Tesis Doctoral, Departamento de Electrónica, Informática y Automática, Universidad de Girona, España, 2004.

[45] Meyers, P, Degrande, N, Van den Bosch, S., "High Availability In MPLS-Based Networks," Alcatel Telecommunications Review, Septiembre de 2004.

[46] Bhagwan, Ranjita, Savage Stefan, Voelker, Geoffrey., "Understanding Availability". Universidad de California, San Siego, Estados Unidos, 2004

[47] Seppänen, Kari, “Dependability of All IP Networks: Resiliency in Ethernet Based Transport”,. VTT- Centro de investigación técnico de Finlandia, 2006.

[48] Semeria, Chuck., “IP Dependability: Network Link and Node Protection”. White paper, Juniper Networks, 2002.

[49] Klymash, M, Pavlyuk, R., “The Methodology of Determination of SDH-Network Structural Reliability”, Modern Problems of Radio Engineering, Telecommunications, and Computer Science, TCSET 2006 International Conference, pp. 582-584, Lviv-Slavsko, Febrero 2006.

[50] Al-Khateeb, W.F, Al-Irhayim, S, Al-Khateeb, K.A.,“Reliability objectives in next-generation Internet”. Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on, basado en Vol 1, No 21-24, pp. 192-197, Septiembre 2003.

[51] Tapolcai, J, Cholda, P, Cinkler, T, Wajda, K.O, Jajszczyk, A, Verchere, D., “Joint Quantification of Resilience and Quality of Service”. Communications, 2006. ICC apos 06, IEEE International Conference on, basado en vol 2, no, pp. 477-482, Junio 2006.

[52] Recomendación de la ITU-T E.800, “Terms and definition related to QoS and network performance including dependability”, Agosto de 2004.

[53] Amin, M, Kin-Hon, Ho, Pavlou, G, Howarth, M., "Improving survivability through traffic engineering in MPLS networks," Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on , vol., no., pp. 758-763, 27-30 Junio 2005.

[54] Menth, Michael, Martin, Ruediger, Spoerlein, Ulrich., "CAM05-1: Impact of Unprotected Multi-Failures in Resilient SPM Networks: a Capacity Dimensioning Approach," Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE , vol., no., pp.1-6, Noviembre 2006.

[55] She, Qingya, Huang, Xiaodong, Jue, Jason P., "Survivable Routing for Segment Protection under Multiple Failures,". Optical Fiber Communication and the National Fiber Optic Engineers Conference, 2007. OFC/NFOEC 2007. Conference on , vol., no., pp.1-3, 25-29, Marzo 2007.

[56] Fumagalli, A, Tacca, M, Wu, K, Vasseur, J.-P., "Local recovery solutions from multi-link failures in MPLS-TE networks with probable failure patterns,". Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE , vol.3, no., pp. 1490-1494, Vol.3, 29, Diciembre 2004.

[57] J. L Marzo, E. Calle, C. Scoglio, T. Anjali "QoS On-LineRouting and MPLS Multilevel Protection: a Survey", Communications, 2003, IEEE International Conference on, Volume 3, 2003, pages: 1973 – 1977.

[58] Jafari, Fahimed, Yaghmae, Mohammad.," A New Fault Tolerant Routing Algorithm For GMPLS/MPLS Networks" Artículo Universidad de Mashhad, Iran, 2004.

[57] K, Sharma, V, Oommen, M., ''Network survivability considerations for traffic engineered IP networks,''. Internet draft: draft-owens-te-network-survivability, Mayo de 2002.

[58] Feng, Jie, Ouyang, Zhipeng, Xu, Lisong, Ramamurthy, Byrav., "Packet reordering in high-speed networks and its impact on high-speed TCP variants". Computer Communications, vol 32, Ed, 1, pág 62-68, Enero 2009.

[59] Fall, K., "The NS Manual". VINT Project. URL: http://www.isi.edu/nsnam/ns/ns-documentation. Diciembre 2003.

[60] Chung, C., "NS by Example". Worrester Polytechnic Institute. 2001.

[61] Ahn, G. et al., "Design and Implementation of MPLS Network Simulator". Chungnam National University. Korea, febrero 2001.

[62] Ahn, G. et al., " Architecture of MPLS Network simulator (MNS) for the setup of CR-LSP". Chungnam National University. Korea, 2001.

[63] Meeneghan, Paul, Delaney, Declan., "An Introduction to NS, Nam and OTcl scripting", Universidad Nacional de Irlanda, Maynooth, 2005.

[64] Masalías, Alejandro.," Adaptación y test del protocolo 802.11e al simulador ns-2.28". Ingeniería de Telecomunicaciones, Universidad Politécnica de Cataluña, España, 2006.

[65] Moodley, P.V, Hanrahan, H.E., "Investigation into Performance Metrics for Connection Admission Control in an MPLS Simulated Network" Universidad de Johannesburgo, Sur Africa, 2008.

[66] Hadjiona, Maria, Georgiou, Chryssis, Vassiliou, Vasos., "A Hybrid Fault-Tolerant Algorithm for MPLS Networks". Proceeding of the 6th International Conference on Wired/Wireless Internet Communications (WWIC 2008), pp. 41-52, Tampere, Finlandia, 2008.