DESARROLLO DE UN MECANISMO INTEGRADO DE PROTECCIÓN CONTRA FALLAS EN REDES MPLS (MULTIPROTOCOL LABEL SWITCHING).

LEYLA EUNICE JOAQUÍ CHIMACHANÁ
EDWIN MARCELO BURBANO ANACONA

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2005

DESARROLLO DE UN MECANISMO INTEGRADO DE PROTECCIÓN CONTRA FALLAS EN REDES MPLS (MULTIPROTOCOL LABEL SWITCHING).

LEYLA EUNICE JOAQUÍ CHIMACHANÁ
EDWIN MARCELO BURBANO ANACONA

Monografía para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director
Ing. Esp. OSCAR J. CALDERÓN CORTÉS

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2005

A quien me enseño a nadar contra la corriente, ha sido mi inspiración, gran amiga, compañera y ejemplo en mi vida. Por su inmenso amor, comprensión, ánimo, confianza, apoyo y paciencia para esperar este momento, mi amada madre, Eunice.

A mis hermanas por todo su apoyo, cariño incondicional, juegos, conversaciones y momentos vividos.

A Gustavo, mi querido padre por su apoyo, esfuerzo y preocupación incondicional.

A todas las personas que han creído en mi …

Leyla Eunice Joaquí Chimachaná

Para el Divino Maestro, inspirador de mi vida,
y para toda mi familia,
especialmente para mis adoradas
Viviana Alejandra y Erika.

Edwin Marcelo Burbano Anacona

AGRADECIMIENTOS

Los autores de esta investigación quisieron agradecer a todos quienes de una u otra forma hicieron posible, la realización de este estudio. Específicamente:

A Dios por ser quien nos ha acompañado y guiado a lo largo de nuestras vidas y en cada paso que emprendíamos, especialmente en este que culminamos.

Al ingeniero Oscar J. Calderón Cortes, por su paciencia, apoyo, dirección y entrega para la elaboración de este trabajo.

A todos los profesores que tuvimos durante nuestros estudios de pregrado.

A nuestras familias y a todas aquellas personas que aportaron para hacer posible el cumplimiento de esta meta.

A Todos Ustedes

Muchas Gracias... !!!

Leyla y Marcelo

TABLA DE CONTENIDO

TABLA DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

LISTA DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 5

INTRODUCCIÓN

El crecimiento imparable de Internet durante los últimos años, así como la demanda de nuevos servicios, crean la necesidad de una mayor disponibilidad de recursos, entre ellos ancho de banda, capacidad de procesamiento, etc., por tanto la tecnología ha debido evolucionar y modificarse con respecto a las habituales desarrolladas a mitad de los años 90. En este ambiente de crecimiento acelerado, los Proveedores de Servicio de Internet (ISP: Internet Service Provider) deben encontrar una manera de adaptarse al incremento de tráfico en las redes y al aumento en el número de usuarios que se conectan a la red.

Debido a la necesidad de intercambiar información sin tener en cuenta los requerimientos de ancho de banda, retardo, etc., surgieron las redes IP. Como consecuencia, se desarrollaron una serie de protocolos para facilitar la comunicación entre sistemas heterogéneos, los cuales se conocen como protocolos TCP/IP o protocolos Internet. En las redes IP, los paquetes se procesan y direccionan independientemente en cada nodo, debido a que dichas redes operan en modo no orientado a la conexión, esto ocasiona un bajo rendimiento en la red, ya que no permite satisfacer los requerimientos deseados por los proveedores (mayor ancho de banda, bajo costo en la evolución de las redes, mejores mecanismos para la gestión de tráfico, etc.) y los usuarios (bajo costo, acceso rápido, etc.).

A mediados de los 90 IP fue ganando terreno como protocolo de red respecto a otros protocolos en uso. Por un lado, los backbone IP de los proveedores de servicio estaban constituidos por enrutadores conectados por líneas dedicadas. Por otro lado, el crecimiento explosivo de Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta ante esto fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, se planteaba la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento global del ancho de banda no resultaba efectivo, por lo cual hubo que idear otras alternativas, fundamentalmente en aquellas basadas en mecanismos de ingeniería de tráfico. Como consecuencia, se impulsaron esfuerzos para aumentar el rendimiento de los enrutadores tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los enrutadores IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de red ATM desplegadas por los operadores de telecomunicaciones. Estas redes ofrecían una buena solución a los problemas de crecimiento de los proveedores: por un lado, proporcionaban mayores velocidades (155 Mbps) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó aceptación entre los proveedores, a la vez que facilitó la entrada de un gran número de operadores telefónicos en la provisión de servicios IP y de conexión a Internet.

El modelo IP/ATM presentaba ventajas evidentes en la integración de los niveles 2 y 3, pero tenía sus inconvenientes: debía gestionar dos redes diferentes, una infraestructura ATM y una red IP lógica superpuesta, lo que generaba a los proveedores de servicio mayores costos globales de gestión de sus redes.

Debido a la demanda de nuevos servicios, crecieron las necesidades de interconexión en las redes IP, aumentando los requerimientos en las capacidades de procesamiento y almacenamiento de las tablas de enrutamiento, causadas por los nuevos nodos en la red, lo cual hace necesario la implementación de políticas de enrutamiento adecuadas que permitan a las redes manejar eficientemente su tráfico, previniendo situaciones tales como cuellos de botella, pérdida de paquetes, congestión, etc. Debido a la poca escalabilidad de los protocolos de enrutamiento usados por las redes IP no es posible optimizar el enrutamiento a través de nuevas políticas, por tanto, la implementación de estos es una tarea dispendiosa y costosa para los administradores de red.

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin los inconvenientes señalados anteriormente. Estas técnicas se conocieron como "Conmutación IP" o "Conmutación multinivel". Una serie de tecnologías privadas (IP Switching de Ipsilon Networks, Tag switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba) condujeron finalmente a la definición del actual estándar de Conmutación de Etiquetas Multiprotocolo (MPLS: Multiprotocol Label Switching) por parte del Grupo de Trabajo en Ingeniería de Internet (IETF: Internet Engineering Task Force) en el área de enrutamiento.

La Conmutación de Etiquetas Multiprotocolo, ha surgido como una relativamente nueva e importante herramienta para satisfacer las necesidades de los proveedores de servicios de Internet. MPLS combina una variedad de funciones tanto IP, como de ATM, implementando mejoras a los protocolos de enrutamiento IP, y facilitando comunicaciones orientadas a la conexión, con lo cual estos obtendrán la capacidad de responder ante situaciones de congestión y de fallas. Por esto se considera la evolución natural requerida para que las redes de comunicaciones soporten servicios IP óptimos y predecibles.

MPLS proporciona la capacidad para soportar cualquier tipo de tráfico sobre una gran red IP sin tener que subordinar el diseño de la misma a las limitaciones de los diferentes protocolos de enrutamiento, capas de transporte, y esquemas de direccionamiento. El objetivo del diseño de MPLS fue el incrementar la eficiencia en la transmisión de datos optimizando el procesamiento del encabezado de los paquetes en la red IP. Esta tecnología, se ha consolidado como una solución a los problemas que se presentan actualmente en redes IP, integrando el manejo de ancho de banda con los requerimientos de servicio; además, ofrece un mejor desempeño en cuanto a flexibilidad, escalabilidad, gestión, y combina en una sola plataforma multiservicio el rendimiento y flexibilidad de la conmutación del nivel 2 con el control de nivel 3, convirtiéndose en una alternativa de evolución hacia las redes de siguiente generación. MPLS inicialmente se

enfocó en la optimización del envío de los paquetes IP, pero durante su proceso de desarrollo, se le han adicionado nuevas características que han conducido a la aplicación en la Ingeniería de Tráfico.

Un aspecto importante para contribuir al uso efectivo de los recursos de red y en cierto grado generar garantías a los tráficos que circulan por la red y que tienen especificaciones de Calidad de Servicio (QoS: Quality of Service), es el uso de los métodos de protección, cuyo objetivo es minimizar el riesgo de fallas de conectividad tanto en los enlaces físicos o virtuales como en los nodos de una red y de esta manera poder determinar el comportamiento y las políticas de restablecimiento de las troncales de tráfico bajo condiciones de falla.

Esta monografía introduce los conceptos principales y aspectos técnicos de MPLS; después de ésta sección, se presenta la aplicación en la Ingeniería de Tráfico. Luego se describen los diferentes métodos de protección contra fallas en redes MPLS con sus características más relevantes. Seguidamente se describe el mecanismo integrado de recuperación basado en políticas de restablecimiento y finalmente se presentan las respectivas simulaciones e interpretación de los resultados tanto de los métodos de protección como del mecanismo integrado y consta de 6 capítulos estructurados de la siguiente forma:

Capítulo 1. Conmutación de Etiquetas Multiprotocolo-TE: Descripción y Operación. Define las principales características, componentes y funcionamiento de las redes MPLS; también se analiza la Ingeniería de Tráfico y sus atributos básicos asociados con los recursos de red, específicamente el atributo de restablecimiento.

Capítulo 2. Recuperación de fallas en redes MPLS. Describe detalladamente cada uno de los métodos (Método Global, Método Local y Método Inverso), presentando sus ventajas y desventajas de acuerdo al estado de la red bajo situaciones de falla.

Capitulo 3. Mecanismo Integrado de Protección contra Fallas. Describe el mecanismo integrado de recuperación de fallas basado en políticas, sus componentes de protección y el modelo de red sobre el cual se aplicará este.

Capítulo 4. Herramienta de Simulación de redes MPLS. Describe la herramienta software de simulación seleccionada, la justificación de su elección, muestra detalladamente su funcionamiento y se especifica la interpretación que hace de redes MPLS además de sus ventajas frente a otras.

Capítulo 5. Pruebas y Resultados. Contiene las pruebas y la obtención de resultados, es decir, la simulación de redes MPLS, la visualización de la red y la interpretación de los datos obtenidos por el simulador. Se comparan estos resultados con los obtenidos de simular otras redes (los 3 métodos).

Capítulo 6. Conclusiones y Recomendaciones. Contiene el análisis de los resultados obtenidos explícitos y tangibles de las capacidades del mecanismo integrado en redes MPLS, y posibles trabajos futuros basados en este desarrollo.

1. CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO-TE: DESCRIPCIÓN Y OPERACIÓN

MPLS proporciona la capacidad para soportar cualquier tipo de tráfico sobre una gran red IP sin tener que subordinar el diseño de la misma a las limitaciones de los diferentes protocolos de enrutamiento, capas de transporte y esquemas de direccionamiento. El objetivo del diseño de MPLS fue el incrementar la eficiencia de la transmisión de datos optimizando el procesamiento del encabezado de los paquetes en las redes IP.

Adicionalmente a los avances en enrutamiento, también se han hecho grandes adelantos en la optimización del hardware; debido a factores como el incremento de la capacidad de procesamiento y la disminución de costos de producción, se ha facilitado la construcción de circuitos integrados de aplicación específica que hacen posible la producción en masa de hardware que es capaz de enviar datagramas a altas velocidades.

Este incremento en la capacidad de procesamiento y disminución de costos, en combinación con las mejoras en el enrutamiento, facilita que las redes sean más rápidas y robustas haciendo posible crear una enorme y confiable infraestructura para Internet.

Este capítulo describe las características, componentes y el funcionamiento de MPLS así como sus ventajas y su aplicación en el área de la Ingeniería de Tráfico.

1.1 GENERALIDADES DE MPLS

La Conmutación de Etiquetas Multiprotocolo (MPLS: Multiprotocol Label Switching) es un trabajo realizado y especificado por el Grupo de Trabajo MPLS en el Área de Enrutamiento de la IETF, que surgió como una tecnología que permitía alcanzar un consenso entre las diferentes tecnologías de conmutación multinivel propuestas por varios fabricantes a mitad de los años 90; además, apareció como una solución acorde a las exigencias actuales de Internet [1].

1.1.1 Definición

MPLS constituye un concepto muy amplio, algunos autores lo definen como un protocolo bastante sencillo, pero las implicaciones que supone su implementación real son muy complejas. Otros autores lo definen como una arquitectura, que incluso puede llegar a sustituir al modelo IP/ATM y otros afirman que MPLS se puede explicar simplemente como una técnica para acelerar el envío de paquetes.

En realidad, MPLS unifica todo lo anterior y su aplicación está dada de acuerdo a la

implementación en cada solución particular. MPLS integra los niveles 2 (enlace) y 3 (red), combinando eficazmente las funcionalidades de enrutamiento del nivel de red (control) con la simplicidad y rapidez de la conmutación de nivel de enlace (envío).

MPLS define los parámetros para la asignación eficiente de etiquetas, enrutamiento, envío y conmutación del tráfico que fluye por la red [1]. Esta es una tecnología orientada a la conexión que permite a los proveedores de servicio controlar el flujo de tráfico IP que se transporta por sus redes. Para esto, MPLS define un mecanismo para establecer trayectos virtuales a través de la red, el cual admite que el tráfico sea encaminado dinámica o manualmente [2].

1.1.2 Objetivos

Los objetivos establecidos por el Grupo de Trabajo MPLS de la IETF en la elaboración de este estándar fueron [3]:

- ✓ MPLS debe funcionar sobre cualquier tecnología de transporte, no sólo ATM.

- ✓ MPLS debe funcionar sobre cualquier tecnología de nivel de enlace. Si la tecnología de nivel 2 soporta un campo de etiquetas, éste es utilizado para encapsular la etiqueta MPLS. Si por el contrario, no soporta un campo de etiquetas, una etiqueta MPLS estándar se agrega entre los encabezados de las capas enlace de datos y de red.

- ✓ MPLS debe ser compatible con el Modelo de Servicios Integrados de la IETF, incluyendo el protocolo RSVP. MPLS al ser estandarizado por la IETF, es compatible con los desarrollos realizados por este grupo.

- ✓ MPLS debe facilitar el crecimiento constante de Internet. Por el nuevo enfoque dado por MPLS a la ingeniería de tráfico, redes privadas virtuales y calidad de servicio, brinda un amplio soporte frente a los posibles cambios evolutivos de Internet.

- ✓ MPLS debe ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP. El Grupo de Trabajo de MPLS en el Área de enrutamiento de la IETF hizo un gran esfuerzo en conjunto con varios proveedores y empresas del sector, para estandarizar las tecnologías de conmutación multinivel y así garantizar la interoperabilidad entre cada uno de sus productos.

- ✓ MPLS facilita el ofrecer QoS. Las funcionalidades de MPLS para la ingeniería de tráfico y la reserva de recursos permiten garantizar la transmisión adecuada de todo tipo de tráfico.

1.1.3 Características

MPLS es considerada como la siguiente etapa en la evolución de las redes IP y esto se debe a las siguientes características que la hacen una red multifuncional, multipropósito y flexible:

- ✓ La principal es la adición de una etiqueta de longitud fija a cada uno de los paquetes IP que ingresan al dominio MPLS y el uso de un protocolo de distribución de etiquetas. Además las decisiones de envío de los paquetes son tomadas basadas en la etiqueta MPLS adicionada a la entrada del dominio, y no a la información del encabezado IP. Una vez el paquete abandona el dominio, la etiqueta MPLS es removida.

- ✓ Aprovecha su capacidad de establecimiento de trayectos virtuales para permitir la aplicación de parámetros de ingeniería de tráfico.

- ✓ Aprovecha las ventajas de las tecnologías orientadas y no orientadas a la conexión. En MPLS se establece una conexión virtual entre dos puntos (característica de las redes orientadas a la conexión) sobre una red de datagramas (no orientada a la conexión).

- ✓ Son necesarios menos dispositivos, por lo tanto la fiabilidad se incrementa y se reducen los costos de operación. Adicionalmente, el diseño de la red y su arquitectura se hacen más simples.

- ✓ Los dispositivos MPLS construyen sus propias tablas de direcciones haciendo transparente al nivel de red los procesos de encaminamiento, creando trayectos de extremo a extremo que aseguren la entrega de paquetes al destino.

1.1.4 Funciones y Ventajas

MPLS realiza las siguientes funciones [4]:

- ✓ Especifíca mecanismos para gestionar flujos de tráfico de diferentes tipos (flujos entre diferente hardware, máquinas y aplicaciones).

- ✓ Permanece independiente de los protocolos de la capa de enlace y de la capa de red.

- ✓ Dispone de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.

- ✓ Ofrece interfaces para diferentes protocolos de enrutamiento y señalización.

- ✓ Soporta los protocolos de la capa de enlace, ATM, Frame Relay y Ethernet.

MPLS presenta las siguientes ventajas [5]:

- ✓ MPLS ayuda a realizar Ingeniería de Tráfico, permitiendo la optimización del uso de recursos.

- ✓ MPLS facilita el transporte de servicios con QoS garantizada, permitiendo a los proveedores mantener una baja latencia extremo a extremo para aplicaciones multimedia.

- ✓ MPLS reduce el tiempo de procesamiento en los dispositivos, debido a que estos envían paquetes basados en etiquetas de longitud fija y no en toda la información de cabecera del paquete IP.

- ✓ MPLS proporciona el apropiado nivel de seguridad para hacer a IP tan seguro como Frame Relay en las redes WAN, con lo que se reduce la necesidad de encriptación sobre redes públicas.

- ✓ Las VPNs en MPLS son más escalables que las de los propios usuarios, ya que estas se soportan en las redes de los proveedores, permitiendo a los usuarios disminuir los requerimientos de configuración y gestión de sus redes.

Las anteriores descripciones hacen de MPLS una tecnología muy atractiva para los operadores de red.

1.2 ARQUITECTURA DE MPLS

Un dominio MPLS es un conjunto de dispositivos que soportan funcionalidades MPLS y que están bajo una misma administración, como se observa en la figura 1.1. Estos dispositivos se clasifican en Enrutador de Etiquetas de Frontera (LER: Label Edge Router) y Enrutador de Conmutación de Etiquetas (LSR: Label Switching Router), los cuales soportan enrutamiento de nivel de red, conmutación de nivel de enlace y conmutación por etiquetas. Cada uno de estos tiene funciones específicas para el envío de paquetes dentro del dominio MPLS.

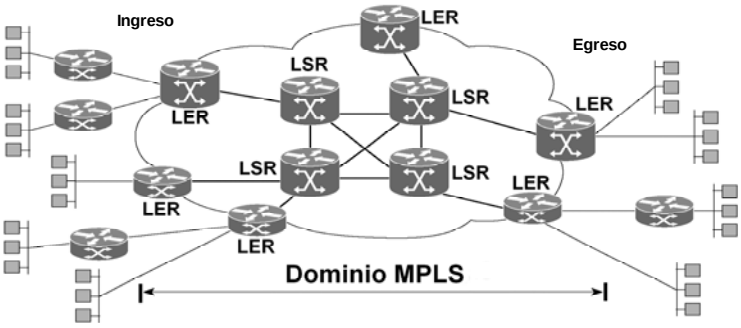


Figura 1.1 Dominio MPLS.

LER: Es un dispositivo de alta velocidad y gran desempeño localizado en la frontera de la red MPLS. El LER es el responsable del procesamiento inicial de los paquetes, de clasificar los paquetes, de asignar y remover etiquetas cuando los paquetes entran o salen de la red. El LER utiliza información de enrutamiento para asignar una etiqueta a un paquete y enviarlo dentro de la red MPLS.

LSR: Este dispositivo provee una alta velocidad de conmutación y opera en el núcleo de la red MPLS. El LSR es el responsable de procesar paquetes etiquetados basándose en la información de

las tablas de envío, tanto de la Base de Información de Envío de Etiqueta (LFIB: Label Forwarding Information Base) la cual envía los paquetes de acuerdo a la etiqueta que se intercambia, como de la Base de Información de Etiqueta (LIB: Label Information Base) que contiene todos los caminos posibles con las etiquetas ya asignadas. Además, los LSR participan en el establecimiento de los Trayectos Conmutados de Etiquetas (LSP: Label Switched Paths).

1.2.1 Conceptos de la arquitectura MPLS

Entre los conceptos básicos de la tecnología MPLS se tienen los siguientes:

1.2.1.1 Etiqueta

Una etiqueta es un identificador corto, de longitud fija, de significado local, el cual es usado para identificar una Clase Equivalente de Envío (FEC: Forwarding Equivalence Class). La etiqueta que es puesta en un paquete en particular representa la FEC a la que ése paquete es asignado. Para tecnologías como PPP y LAN se agrega una cabecera MPLS de 32 bits entre las cabeceras de nivel dos y de nivel tres, como se muestra en la figura 1.2 [6]. En redes ATM o Frame Relay se utilizan los campos VPI/VCI de ATM y el campo DLCI de Frame Relay como etiqueta MPLS.

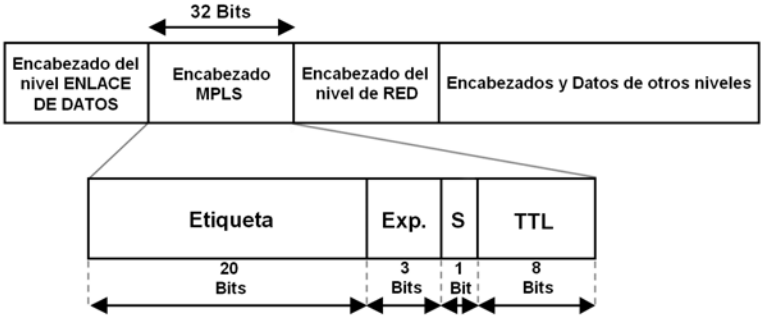


Figura 1.2 Formato Genérico del encabezado MPLS.

El tamaño de este encabezado es de 32 bits y se divide en los siguientes campos:

- ✓ **Etiqueta (20):** Campo de 20 bits que lleva el valor de la etiqueta MPLS.

- ✓ **EXP (3):** Antes se llamaba Clase de Servicio (CoS: Class of Service), ahora se considera un campo experimental para consideraciones de QoS.

- ✓ **S (1):** Se usa para indicar si esta presente una pila de etiquetas (label stack), entonces su valor será uno. Si la etiqueta es la única presente en la pila, entonces su valor será 0.

- ✓ **TTL (8):** El campo Tiempo de Vida (TTL: Time To Live) provee funcionalidad IP TTL. Se usa para indicar el número de nodos MPLS por los que el paquete viajará hasta alcanzar su destino. El valor es copiado del encabezado del paquete cuando se ingresa al LSP, y copiado de vuelta al encabezado del paquete IP cuando sale de la misma [6].

MPLS permite la colocación de múltiples etiquetas a un solo paquete, como consecuencia de ello, MPLS soporta una jerarquía de etiquetas (Pila de Etiquetas-Label Stack), las cuales se organizan en una pila tipo "última en entrar, primera en salir" (LIFO: Last-in, First-out); dicha pila se identifica en el encabezado con la letra S [1]. Si la pila de etiquetas de un paquete es de tamaño m, la última etiqueta se conoce como la etiqueta de nivel 1, a la de arriba de ella, como la etiqueta de nivel 2 y a la etiqueta superior de la pila como la etiqueta de nivel m, como se muestra en la figura 1.3. Los dispositivos MPLS toman decisiones de envío basándose exclusivamente en la etiqueta superior de la pila, debido a esto, el procesamiento de un paquete etiquetado es completamente independiente del nivel de la jerarquía. Uno de los principales usos que se le da a la pila de etiquetas es facilitar la operación de túneles dentro del dominio MPLS.

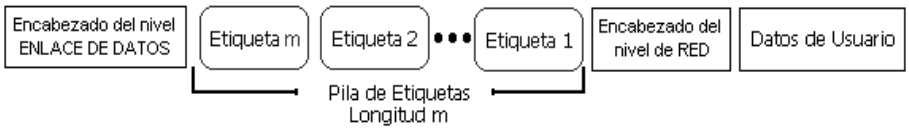


Figura 1.3 Pila de Etiquetas.

Después que la etiqueta superior es procesada, las operaciones que puede realizar un dispositivo MPLS sobre la pila son:

Push: Adiciona una nueva etiqueta en la parte superior de la pila. Si la longitud de la pila es mayor que cero, los campos EXP y TTL de la nueva etiqueta podrían derivarse de la etiquetas de niveles inferiores. En caso contrario, la nueva etiqueta será la primera en la pila y los campos TTL y EXP se derivan de la cabecera del paquete IP.

Pop: Remueve la etiqueta superior de la pila. Si la etiqueta removida es la última en la pila, el valor TTL se copia al encabezado del paquete IP; pero si se tienen múltiples etiquetas, los campos EXP y TTL de la nueva etiqueta podrían derivarse de la anterior.

Swap: Reemplaza el valor de la etiqueta de nivel superior por un nuevo valor. Los bits de EXP y TTL son copiados en la etiqueta anterior, y el campo TTL es copiado y reducido en 1.

Push múltiple: Adiciona múltiples etiquetas (superior a 2) en la parte superior de la pila de etiquetas.

Swap y Push: Reemplaza la etiqueta superior con un nuevo valor, seguido de la adición de una nueva etiqueta en la parte superior de la pila.

1.2.1.2 Clase Equivalente de Envío-FEC

Conjunto de paquetes que comparten unas mismas características para su transporte. Todos los paquetes que pertenecen a la misma FEC recibirán el mismo tratamiento en su camino hacia el destino. La asignación de un paquete a un determinado FEC se produce únicamente cuando este ingresa a la red. Cada FEC puede representar unos requerimientos de servicio para un conjunto

de paquetes o para una dirección fija, o simplemente representa el prefijo de una dirección IP. Los paquetes con la misma FEC son enrutados a través de la red sobre un mismo trayecto.

1.2.1.3 Trayecto Conmutado de Etiquetas-LSP

Es una ruta virtual a través de la cual los paquetes asignados a un misma FEC viajan a lo largo de la red. Cada LSP se crea por la concatenación de uno o más saltos, permitiendo que un paquete sea enviado desde un LSR a otro a través del dominio MPLS. Un LSP es unidireccional ya que los paquetes fluyen en una sola dirección desde el enrutador de ingreso hasta el enrutador de egreso del dominio.

MPLS proporciona dos opciones para establecer un LSP [4]:

- ✓ **Enrutamiento salto-a-salto (hop-by-hop).** Cada LSR selecciona independientemente el siguiente salto para una FEC dada. Esta metodología es similar a la que se usa en redes IP. El LSR usa cualquiera de los protocolos de enrutamiento disponibles, como OSPF, Private Network to Network Interface (PNNI), etc.

- ✓ **Enrutamiento explícito.** El LSR de ingreso especifica la lista de nodos por la cual viaja la trayectoria explícita. Sin embargo, el camino especificado puede no ser óptimo. A lo largo de la trayectoria, los recursos deben ser reservados para asegurar una calidad de servicio para el tráfico de datos, además de facilitar la ingeniería de tráfico.

1.2.2 Modos de distribución de Etiquetas

Que un nodo sea ascendente y otro descendente con respecto a una asociación dada, significa que una etiqueta en particular representa una FEC en los paquetes que viajan desde el nodo ascendente hacia el nodo descendente, como se muestra en la figura 1.4.

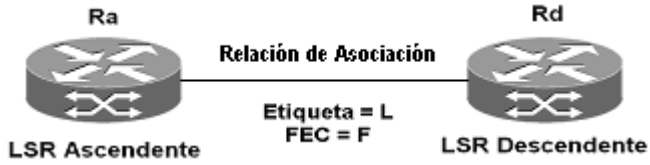


Figura 1.4 LSRs Ascendente y Descendente.

Sean Ra y Rd dos LSRs, los cuales tienen acordado asociar una etiqueta L a la FEC F para los paquetes enviados desde Ra hacia Rd; como resultado de tal acuerdo, L se convierte en la "etiqueta de salida" para Ra y en la "etiqueta de entrada" de Rd representando a la FEC F. En una asociación como esta, se dice que Ra es el "LSR Ascendente" y Rd el "LSR Descendente" [1].

La arquitectura MPLS para el mapeo de la etiqueta en los LSRs, define dos asociaciones descendentes de modos de distribución de etiqueta: descendente sobre demanda y sin solicitud descendente.

- ✓ **Descendente sobre demanda.** La decisión de asociar una etiqueta L a una FEC en particular es efectuada por el LSR que es DESCENDENTE respecto a esa asociación. Luego el LSR descendente informa al LSR ascendente (es quien realiza la solicitud explicita de la etiqueta) de la asociación. De este modo las etiquetas son "asignadas descendentemente" y las asociaciones de etiquetas son "distribuidas ascendentemente"; este proceso se muestra en la figura 1.5 [7].

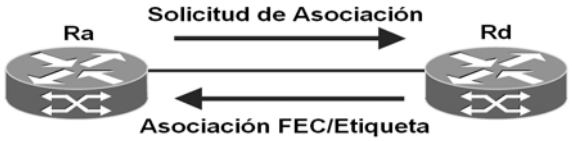


Figura 1.5 Distribución de una asociación FEC/Etiqueta descendente sobre demanda.

- ✓ **Sin solicitud descendente.** La arquitectura MPLS también permite a un LSR distribuir asociaciones de etiqueta a LSRs que no hayan solicitado explícitamente la etiqueta; donde el LSR descendente es el responsable de anunciar el mapeo de la etiqueta al LSR ascendente; este proceso se muestra en la figura 1.6 [7].

Figura 1.6 Anuncio de la etiqueta sin solicitud descendente.

1.2.3 Mecanismos de Señalización en MPLS [4]

- ✓ **Solicitud de Etiquetas (Label Request).** Usando este mecanismo, un LSR hace una solicitud de etiqueta a su vecino descendente, de manera que la pueda asignar a una FEC específica. Este mecanismo puede ser empleado por toda la cadena de LSRs hasta el LER de egreso.

- ✓ **Mapeo de Etiquetas (Label Mapping).** En respuesta a una solicitud de etiqueta, un LSR descendente envía (mapea) una etiqueta al LSR ascendente correspondiente, usando este mecanismo de mapeo.

Los conceptos de señalización se representan gráficamente en la figura 1.7.

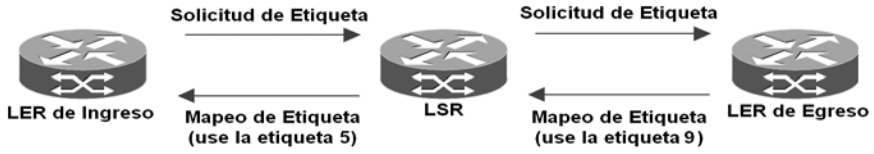


Figura 1.7 Mecanismos de Señalización en MPLS.

1.3 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS [2]

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por medio de los cuales un LSR informa a otro de la asociación etiqueta/FEC que él ha hecho. Dos LSRs que usan un protocolo de distribución de etiquetas para intercambiar información de asignaciones etiqueta/FEC son conocidos como "par de distribución de etiquetas" con respecto a la información de asignaciones que ellos intercambian. Si dos LSRs son pares de distribución de etiquetas, entonces se habla de que existe una "adyacencia de distribución de etiquetas" entre ellos.

La arquitectura no asume que hay un único protocolo de distribución de etiquetas. De hecho, se han estandarizado un número de diferentes protocolos de distribución de etiquetas. Los protocolos existentes han sido extendidos para que la distribución de etiquetas pueda ser transportada dentro de ellos (por ejemplo, BGP y RSVP), también han sido definidos nuevos protocolos para el propósito de distribución explícita de etiquetas (por ejemplo, LDP y CR-LDP).

1.3.1 Protocolo de Distribución de Etiquetas (LDP: Label Distribution Protocol) [8]

LDP es un protocolo definido para la distribución de etiquetas. Este es un conjunto de procedimientos y mensajes por medio de los cuales los LSRs establecen LSPs a través de una red mapeando la información de enrutamiento de la capa de red directamente en caminos conmutados de la capa enlace de datos. Estos LSPs pueden tener punto final en un vecino adjunto (comparable al envío IP salto-a-salto), o en un nodo de egreso de la red, permitiendo la conmutación a través de todos los nodos intermedios. LDP asigna una FEC a cada LSP que crea, la FEC asignada a un LSP especifica cuáles paquetes son "mapeados" a dicho LSP.

Hay cuatro categorías de mensajes LDP [8]:

1. Mensajes de Descubrimiento (Discovery Messages), usados para anunciar y mantener la presencia de un LSR en la red.

2. Mensajes de Sesión (Session Messages), usados para establecer, mantener, y terminar sesiones entre pares LDP.

3. Mensajes de Advertencia (Advertisement Messages), usados para crear, modificar y eliminar mapeos de etiquetas a las FEC.

4. Mensajes de Notificación (Notification Messages), usados para suministrar información de advertencia y comunicar mensajes de error.

Los mensajes de descubrimiento proporcionan un mecanismo por medio del cual los LSRs indican su presencia en la red enviando un mensaje Hello periódicamente. Este es transmitido como un paquete UDP hacia el puerto LDP de "todos los enrutadores de esta subred". Cuando un LSR quiere establecer una sesión con otro LSR aprendido por medio del mensaje Hello, este usa el

procedimiento de inicialización de LDP sobre TCP. Luego de una exitosa finalización del procedimiento de inicialización, los dos LSRs son pares LDP y pueden intercambiar mensajes de advertencia. Solicitar una etiqueta o anunciar un mapeo de etiqueta al par es una decisión local en gran parte hecha por el LSR.

Existen dos diferentes iniciativas para implementar la ingeniería de tráfico en MPLS: RSVP con ingeniería de tráfico y el CR-LDP.

1.3.2 Protocolo de Reservación de Recursos con Ingeniería de Tráfico (TE-RSVP) [9]

El Protocolo de Reservación de Recursos (RSVP: Resource Reservation Protocol) fue diseñado por la IETF en 1997 con el fin de proporcionar el concepto de reserva de recursos antes de la transmisión de datos y que esta contemplado por los requerimientos de calidad de servicio. El protocolo fue diseñado para especificar requerimientos de ancho de banda y de condiciones de tráfico, para una trayectoria definida. Si el ancho de banda requerido esta disponible, entonces se establece el enlace necesario para la transmisión.

El Protocolo de Reservación de Recursos (RSVP: Resource ReSerVation Protocol) fue desarrollado para las redes IP, pero más adelante se le adicionaron nuevas características para que sirviera como protocolo de distribución de etiquetas y más funcionalidades para ingeniería de tráfico de modo que brindara soporte para señalización, establecimiento de niveles de prioridad, re-enrutamiento, re-optimización de los trayectos y detección de bucles. Además, permite especificar requerimientos de ancho de banda y de condiciones de tráfico, para una trayectoria definida. MPLS propone extensiones a este protocolo para la implementación de ingeniería de tráfico, a las que se llama RSVP con Ingeniería de Tráfico (TE-RSVP: Traffic Engineering-RSVP). El usar esta extensión, no significa que deba ser totalmente implementado el protocolo RSVP por los LERs y LSRs con los que cuente la red MPLS. TE-RSVP es un protocolo de estado suave (soft state) que usa datagramas UDP o IP como mecanismo de señalización en el establecimiento de LSPs, incluyendo peticiones de etiquetas, descubrimiento y mapeo.

La figura 1.8 muestra un ejemplo de señalización con TE-RSVP, primero se hace uso del protocolo BGP para descubrir el LER de egreso apropiado y así enviar el tráfico a través del dominio; el LER de ingreso envía un mensaje *PATH* hacia el LER de egreso a través de cada LSR descendente a lo largo del camino. Cada nodo recibe el mensaje *PATH* para recordarle el paso de este flujo, de esta forma se crea una sesión o "estado del camino". El LER de egreso usa el mensaje *RESV* para reservar recursos con los parámetros de tráfico y calidad de servicio en cada LSR ascendente a lo largo del camino; una vez recibido este mensaje en el LER de ingreso, este envía un mensaje *RESVConf* al LER de egreso confirmando el establecimiento del LSP. Para mantener el camino antes establecido y el estado de reserva se deben enviar mensajes de refresco entre los LERs continuamente.

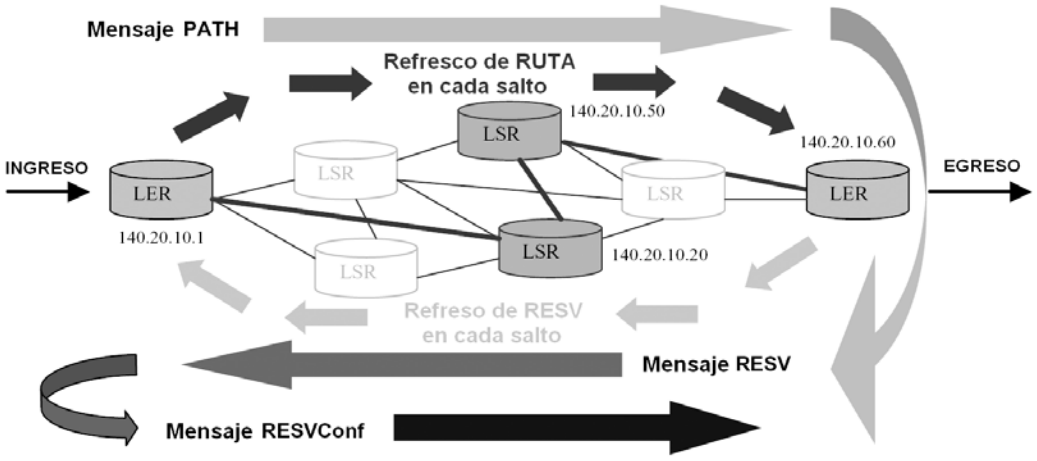


Figura 1.8 Ejemplo del establecimiento de un LSP con TE-RSVP.

1.3.3 Protocolo de Distribución de Etiquetas basado en Restricciones (CR-LDP) [9]

El Protocolo de Distribución de Etiquetas basado en Restricciones (CR-LDP: Constraint-Based Label Distribution Protocol), es un protocolo construido sobre LDP, el cual ya forma parte de MPLS. Usa las estructuras de mensajes existentes, y solo se extiende lo necesario para llevar a cabo implementación de ingeniería de tráfico. Como en RSVP, CR-LDP soporta LSPs enrutados explícitamente. Se usa UDP para descubrir pares MPLS y TCP se usa para control, manejo, peticiones y mapeo (señalización).

La figura 1.9 muestra el proceso de establecimiento de un LSP usando CR-LDP. Para este camino han sido predeterminados tanto el LER de ingreso como el de egreso y se ha limitado a dos LSRs específicos. Las solicitudes de etiquetas han sido enviadas hacia cada LSR descendente hasta el LER de egreso y el mapeo se ha enviado ascendentemente hacia el LER de ingreso. El camino explicito puede ser definido tan preciso como para estipular las direcciones IP a ser usadas por los LER y LSRs. Este procedimiento puede ser muy ventajoso en el caso de un tráfico en particular (como voz o una VPN), ya que se puede seleccionar un camino óptimo para satisfacer las necesidades de ancho de banda y/o de prioridad. Como se observa, se usan los mismos mecanismos de señalización del protocolo LDP para establecer un LSP restringido a pasar por dos LSRs específicos.

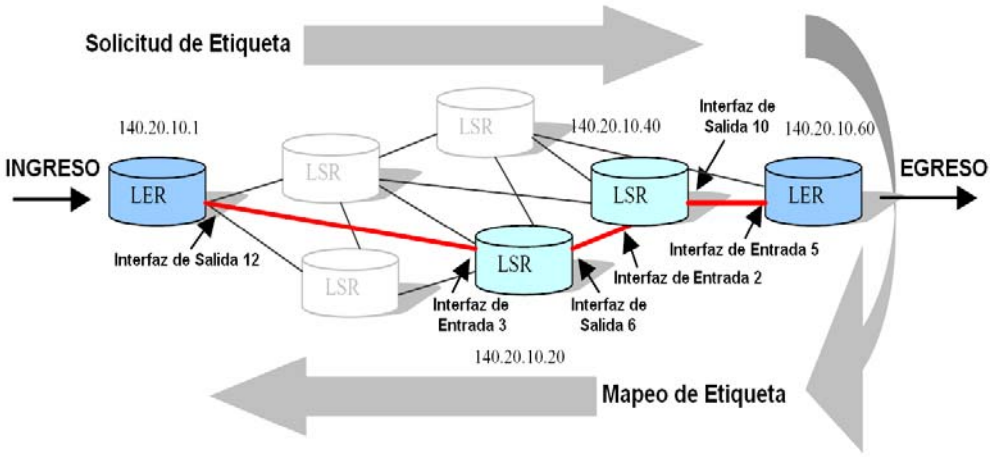


Figura 1.9 Ejemplo de un LSP estricto enrutado por CR-LDP.

1.4 OPERACIÓN DE MPLS

En el enrutamiento efectuado por los tradicionales protocolos de red no orientados a la conexión, cuando un paquete viaja de un enrutador al siguiente, cada enrutador toma una decisión de envío autónoma para ese paquete. Es decir, cada uno analiza el encabezado del paquete, y cada enrutador ejecuta un algoritmo de enrutamiento de nivel de red. Cada enrutador independientemente selecciona el siguiente salto para el paquete, basado en su análisis del encabezado y en los resultados de la ejecución del algoritmo de enrutamiento, además los encabezados de los paquetes contienen mucha más información de la necesaria para seleccionar el siguiente salto. En MPLS la selección del siguiente salto puede conceptualizarse como una labor de dos funciones; la primera divide todo el conjunto de paquetes posibles en un conjunto de FECs y la segunda mapea cada FEC hacia el siguiente salto. Todos los paquetes que pertenecen a una determinada FEC y que viajan desde un determinado nodo seguirán el mismo camino.

En MPLS, la asignación de un determinado paquete a una determinada FEC se hace solo una vez, cuando el paquete entra a la red. La FEC a la cual el paquete es asignado está codificada como un valor de longitud fija y corta conocido como "etiqueta". Cuando un paquete es enviado hacia el siguiente salto, la etiqueta es enviada con él, esto es, los paquetes son "etiquetados" antes de ser enviados. En los siguientes saltos, no hay más análisis del encabezado de la capa de red del paquete. En cambio, se usa la etiqueta como un índice dentro de una tabla que especifica el siguiente salto y la nueva etiqueta. La etiqueta antigua es reemplazada con la nueva, y el paquete es enviado a su siguiente salto.

En el paradigma de envío de MPLS, una vez el paquete es asignado a una FEC, los siguientes enrutadores no hacen más análisis del encabezado; todo el envío es dirigido por las etiquetas. Esto conlleva numerosas ventajas sobre el envío convencional de la capa de red, como son:

- ✓ El envío en MPLS pueden hacerlo los conmutadores capaces de realizar la búsqueda y el reemplazo de la etiqueta, pero cualquiera no es capaz de analizar los encabezados de la capa de red, o no es capaz de analizarlos a una velocidad adecuada, lo que demuestra la relativa sencillez del hardware utilizado en MPLS.

- ✓ Dado que un paquete es asignado a una FEC cuando ingresa a la red, el enrutador de ingreso puede usar, para determinar la asignación, cualquier información que tenga acerca del paquete, aún si esa información no puede ser recopilada del encabezado de la capa de red. Por ejemplo, los paquetes que entran por diferentes puertos pueden ser asignados a diferentes FECs. Por otro lado, en el envío convencional, solamente puede considerarse la información que viaja en el encabezado del paquete.

- ✓ Un paquete que ingresa a la red por un determinado enrutador puede ser etiquetado en forma diferente que el mismo paquete que ingresa a la red por otro enrutador, y como resultado las decisiones de envío que dependen del enrutador de ingreso pueden hacerse más fácilmente. Esto no se puede hacer con el envío convencional, puesto que la identificación del paquete en el enrutador de ingreso no viaja con el.

- ✓ Las consideraciones que determinan como un paquete es asignado a una FEC pueden hacerse aun más y más complicadas, sin ningún impacto en absoluto para los enrutadores que simplemente envían paquetes etiquetados.

- ✓ En ocasiones es deseable que un paquete siga un determinado camino, el cual es explícitamente seleccionado antes o en el momento en que ingresa a la red, en lugar de ser seleccionado por el algoritmo normal de enrutamiento dinámico cuando el paquete viaja a través de la red. Esta selección puede hacerse por medio del requerimiento de políticas, o con el fin de implementar ingeniería de tráfico. En el envío convencional, se requiere que el paquete lleve un código de su camino junto a él. En MPLS puede usarse una etiqueta para representar el camino, así que no es necesario transportar con el paquete un identificador explicito de este [1].

Los paquetes que viajan a través de una red MPLS, en general, deben seguir los siguientes pasos:

1. Creación y Distribución de etiquetas.
2. Creación de tablas en cada LSR.
3. Creación de LSP.
4. Inserción de etiquetas/chequeo de tablas.
5. Envío de paquetes.

En MPLS, no todo el tráfico es transportado por el mismo camino; dependiendo de las características de Ingeniería de Tráfico, se pueden crear diferentes LSPs para paquetes con diferentes requerimientos. La figura 1.10 muestra el proceso de creación de un LSP y el envío de paquetes en una red MPLS [4].

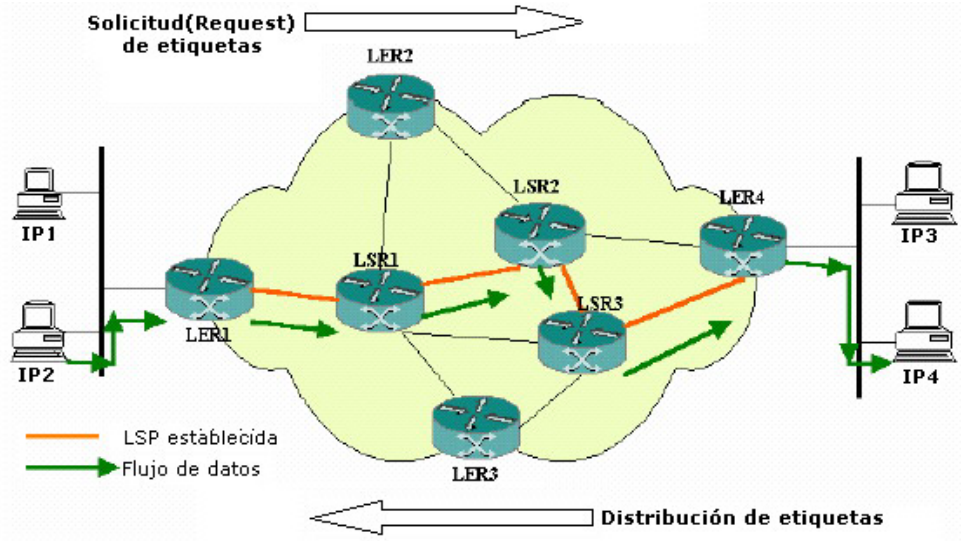


Figura 1.10 Establecimiento y envío de paquetes a través de un LSP.

La tabla 1.1 especifica paso a paso las operaciones que se realizan sobre un paquete que ingresa al dominio MPLS (ver figura 1.10).

OPERACIONES	DESCRIPCIÓN
Creación y Distribución de Etiquetas	Antes de que el tráfico empiece a fluir, los LSRs toman decisiones para asociar una etiqueta a un FEC y construir sus tablas de envío. Haciendo uso de LDP, los enrutadores descendentes inician la distribución de etiquetas y de las asociaciones etiqueta/FEC. Adicionalmente se realizan las negociaciones de las características relacionadas con el tráfico y las capacidades de MPLS usando LDP.
Creación de Tablas	Cuando un LSR recibe las asociaciones de etiquetas, crea nuevas entradas en la LIB, donde se especifica el mapeo entre una etiqueta y una FEC, y también el mapeo entre la tabla de puertos y etiquetas de entrada con la tabla de puertos y etiquetas de salida. Las entradas son actualizadas cada vez que se efectúa una renegociación de las asociaciones etiqueta/FEC.
Creación del LSP	Como se puede ver en la figura 1.10, los LSPs son creados en sentido inverso al de la creación de entradas en las LIBs.
Inserción de Etiquetas/Chequeo de tablas	El LER de ingreso usa la tabla LIB para encontrar el siguiente salto y luego hace una petición de etiqueta para una FEC en particular. Los siguientes LSRs solo usan la etiqueta para encontrar el siguiente salto. Una vez que un paquete llega al LER de egreso, la etiqueta es removida y el paquete es entregado a su destino.
Envío de Paquetes	El LER1 no tiene ninguna etiqueta disponible para el paquete, ya que aún no ha realizado ninguna solicitud, entonces él inicia la solicitud de etiqueta al LSR1. Esta solicitud se propaga a través de la red en dirección al LER4 (egreso). Cada enrutador intermedio recibe una etiqueta de su enrutador descendente, comenzando desde el LER4 y dirigiéndose ascendentemente hasta el LER1. El establecimiento del LSP lo realiza LDP u otro protocolo de señalización. Si se requiere la aplicación de Ingeniería de Tráfico, entonces se hace uso de CR-LDP para realizar el establecimiento del LSP, con el fin de asegurar el cumplimiento de los requerimientos de QoS y de CoS. Ahora el LER1 clasifica el paquete dentro de una de las FEC, consulta su tabla de envío y de acuerdo a la etiqueta del paquete, lo envía hacia el LSR1. Cada LSR siguiente, como los LSR2 y LSR3, examina la etiqueta del paquete, consulta su tabla de envío, reemplaza la etiqueta con una nueva y lo envía hacia el siguiente salto. Cuando el paquete llega al LER4, se remueve la etiqueta ya que aquí el paquete sale de la red MPLS y se entrega a la red destino.

Tabla 1.1 Descripción de la operación de MPLS [4].

La tabla 1.2 muestra un ejemplo de la tabla LIB que se crea en un LSR para permitir la distribución de etiquetas y el envío de paquetes.

Puerto de entrada	Etiqueta de entrada	Puerto de salida	Etiqueta de salida
1	3	3	6
2	9	1	7

Tabla 1.2 Ejemplo de una tabla LIB [4].

Es interesante considerar un ejemplo de dos flujos de paquetes ingresando a un dominio MPLS: un flujo es un intercambio regular de datos entre servidores y el otro es un flujo de video, el cual requiere la aplicación de parámetros de QoS a través de Ingeniería de Tráfico. En el LER, estos dos flujos son clasificados en dos FECs. En el siguiente salto, el LSR consulta su tabla LIB y observa que el mapeo asociado con cada flujo corresponde a las etiquetas 3 y 9 respectivamente, con sus correspondientes puertos de entrada 1 y 2. El LSR ejecuta un intercambio de etiquetas, por lo cual a los paquetes de la FEC1 se les cambia la etiqueta 3 por la 6 y a los paquetes correspondientes a la FEC2 se les cambia 9 por la 7. Finalmente envía los paquetes por los puertos de salida 3 y 2 correspondientes a las dos FECs.

1.5 INGENIERÍA DE TRÁFICO SOBRE MPLS

La Ingeniería de Tráfico (TE: Traffic Engineering) aplicada a MPLS, es un proceso de planeación y optimización, cuyo objetivo es permitir el uso eficiente de los recursos y mejorar el desempeño de la red, además de facilitar la distribución del tráfico de acuerdo con la disponibilidad de los recursos, la carga actual y la esperada [10]; tratando de crear una distribución de tráfico uniforme o diferenciada a través de la red. La idea es equilibrar de forma óptima la utilización de recursos, de manera que no existan algunos que sean sobreutilizados, con posibles puntos con cuellos de botella, mientras otros estén siendo al mismo tiempo desperdiciados.

En las grandes redes IP, no es recomendable para el administrador realizar la configuración manualmente debido al gran esfuerzo necesario para ello. Para solucionar este inconveniente, la IETF introdujo unas herramientas para implementar TE dentro de la red como son los mecanismos de enrutamiento restringido [11], protocolos de señalización y principalmente MPLS; esta integración se conoce como Ingeniería de Tráfico MPLS (MPLS-TE: MPLS Traffic Engineering); con la cual se abordan los problemas de cantidad de tráfico a manejar, mantenimiento del nivel de desempeño, recursos de red que se necesitan y cómo se organizan estos para manejar el tráfico que ingresa a la red [12].

Un concepto fundamental para implementar TE en redes MPLS es la troncal de tráfico, la cual está conformada por un conjunto de flujos unidireccionales de la misma clase (FEC), los cuales están localizados dentro de un mismo LSP (ver figura 1.11) [13]. Esencialmente, una troncal de tráfico es una representación abstracta de tráfico que posee unas características específicas (similares a los circuitos virtuales de ATM y Frame Relay), es decir, una FEC de nivel superior. Además MPLS define un conjunto de atributos básicos asociados con los recursos de la red que

restringen la ubicación de las troncales de tráfico a través de ellos. Los atributos pueden asignarse explícitamente a las troncales por medio de acciones administrativas o implícitamente por los protocolos subyacentes cuando se realiza la clasificación de los paquetes y mapeo de las clases equivalentes a la entrada del dominio MPLS.

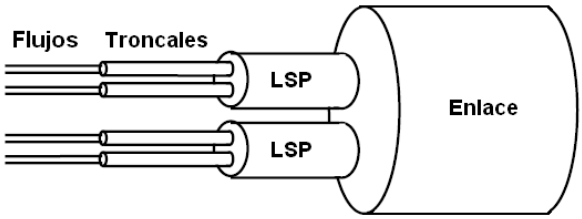


Figura 1.11 Relación entre flujos, troncales, LSPs y Enlace.

Las capacidades funcionales requeridas para un soporte total de Ingeniería de Tráfico sobre MPLS en grandes redes consisten en: *Atributos* y *Enrutamiento Basado en Restricciones*.

1.5.1 Atributos

Por un lado, se tiene un conjunto de atributos asociados con las *troncales de tráfico* que colectivamente especifican sus características de comportamiento. Y por otro lado, están los atributos asociados con los *recursos* que conllevan las restricciones para las troncales de tráfico.

Los atributos [10] básicos de las troncales de tráfico más representativas para la TE son:

- ✓ **Atributos de parámetros de tráfico.** Capturan las características de los flujos (los FEC) para ser transportados a través de las troncales de tráfico. Tales características son la tasa pico, tasa promedio, tamaño de ráfaga permitido, etc. Los parámetros de tráfico son importantes ya que estos indican los requerimientos de recursos de las troncales.

- ✓ **Selección genérica del camino y atributos de mantenimiento.** Define las reglas para la selección de los caminos tomados por la troncal de tráfico así como por los caminos alternos.

- ✓ **Atributos de Prioridad.** Define la importancia relativa de la troncal de tráfico, ya que estos determinan el orden en el cual se realiza la selección de los caminos para cada uno de ellos.

- ✓ **Atributos de Apropiación.** Determina si una troncal de tráfico puede apropiarse de otra troncal perteneciente a un camino dado, o si puede apropiarse de una troncal especifica. La apropiación puede usarse para asegurar que las troncales con alta prioridad sean enrutadas a través de trayectorias relativamente favorables, también se puede usar para implementar varias políticas de restablecimiento ante situaciones de falla.

- ✓ **Atributos de Restablecimiento.** Determinan el comportamiento y las políticas de funcionamiento de las troncales de tráfico bajo condiciones de falla. Por tanto, es necesario

en dichas circunstancias resolver los siguientes problemas: (1) Detección de Fallas, (2) Notificación de Fallas, (3) Recuperación y Restablecimiento.

- ✓ **Atributos de mantenimiento del orden.** Determinan las acciones que deben tomar los protocolos subyacentes cuando una troncal excede los umbrales establecidos al momento de su creación.

Pueden especificarse muchas políticas de restablecimiento de troncales de tráfico cuyos caminos establecidos están afectados por fallas. Los siguientes son ejemplos de esquemas factibles:

1. No re-enrutar la troncal de tráfico.
2. Re-enrutamiento a través de un camino factible con suficientes recursos. Si no hay ninguna disponible, entonces no realizar re-enrutamiento.
3. Re-enrutamiento a través de cualquier camino disponible sin tener en cuenta las restricciones de los recursos.
4. Son posibles otros esquemas, incluyendo algunos que podrían ser combinaciones de los anteriores.

El atributo de Restablecimiento "básico" indica el procedimiento de recuperación que es aplicado a las troncales de tráfico cuyos caminos son afectados por fallas. Específicamente, este atributo es una variable binaria qué determina si la troncal de tráfico designada será re-enrutada cuando fallan segmentos de su trayecto.

Dentro de los atributos de MPLS-TE asociados a los recursos se encuentra:

- ✓ **Multiplicador de Asignación Máximo.** El multiplicador de asignación máximo de un recurso es un atributo administrativamente configurable que determina la proporción de los recursos que están disponibles para la asignación a las troncales de tráfico. Este atributo es principalmente aplicable a los enlaces de Banda Ancha. Sin embargo, también este puede aplicarse a los recursos de almacenamiento en los LSRs.

- ✓ **Atributos de Clase de Recurso.** Estos son parámetros administrativamente asignados, los cuales expresan alguna noción de "Clase" para los recursos. También, pueden ser vistos como "colores" asignados a los recursos tales que el conjunto de recursos con el mismo "color" pertenecen conceptualmente a la misma clase, permitiendo así implementar una variedad de políticas con los recursos de interés claves (enlaces).

1.5.2 Enrutamiento Basado en Restricciones

Una estructura de "enrutamiento basada en restricciones" se usa para seleccionar caminos para los troncales de tráfico sujetas a las restricciones impuestas por los atributos; y usa como entrada:

- Los atributos asociados con las troncales de tráfico.

- Los atributos asociados con los recursos y
- Otra información del estado de la topología.

Acorde a esta información, un proceso de enrutamiento basado en restricción en cada nodo, automáticamente calcula los caminos explícitos para cada troncal de tráfico originada desde el nodo. En este caso, un camino explícito para cada troncal de tráfico es una especificación de un LSP que satisface los requisitos de demanda expresados en los atributos de las troncales de tráfico, sujeto a las restricciones impuestas por la disponibilidad del recurso, las políticas administrativas y otra información del estado de la topología.

Por tanto, el enrutamiento basado en restricciones ayuda en la optimización del funcionamiento de redes operacionales, encontrando automáticamente caminos factibles que satisfagan un conjunto de restricciones para las troncales de tráfico. Esto puede reducir drásticamente la cantidad de configuración administrativa de caminos explícitos y la intervención manual requerida para cumplir los objetivos de la Ingeniería de Tráfico.

Los atributos asociados con las troncales de tráfico y recursos, así, como los parámetros asociados con el enrutamiento, representan colectivamente las variables de control que pueden modificarse a través de su acción administrativa o a través de los agentes automatizados para llevar la red a un estado deseado.

En MPLS, la ingeniería de tráfico se proporciona inherentemente usando LSPs explícitas. Los LSPs son creados independientemente, especificando diferentes trayectorias que se basan en políticas definidas por el usuario. Sin embargo puede ser necesaria una elevada intervención por parte del administrador.

MPLS se consolida como una tecnología que ofrece nuevas capacidades para los ambientes de networking de las redes actuales, entre ellas, las facilidades que tiene para el soporte de funcionalidades de ingeniería de tráfico, la cual busca consolidar procesos de optimización y uso eficiente de los recursos de la red. Un proceso necesario en las redes actuales, dada la tendencia a soportar multiservicios basados en IP, es el de garantizar elevados niveles de confiabilidad; en este aspecto, MPLS ofrece múltiples facilidades, una de ellas son los métodos de protección ante fallas [14], los cuales abordan el problema de reestablecimiento desde una óptica muy particular. Dichos métodos se establecen con el fin de lograr una rápida recuperación de la red ante fallos con lo cual se evita la pérdida de información y se ofrece un adecuado nivel de confiabilidad. El proceso se realiza mediante el establecimiento de Trayectos de Conmutación de Etiquetas (LSPs: Label Switched Paths) redundantes que actúan como caminos de respaldo. Con estos respaldos, el tráfico siempre podrá ser redireccionado en caso de falla.

2. RECUPERACIÓN DE FALLAS EN REDES MPLS

El diseño inicial de una red puede no ser satisfactorio debido a los cambios en la carga ofrecida, las características de tráfico, etc., los cuales no se pueden determinar con absoluta precisión. Los recursos de la red también varían de acuerdo a la reserva de estos y a los cambios en la topología (tales como fallas en los nodos o en los enlaces). Una parte importante al diseñar una red con QoS consiste en brindarle la fiabilidad requerida. Esta fiabilidad puede ser proporcionada por medio de mecanismos de gestión de fallas, aplicados a diferentes niveles de red y escalas de tiempo.

Una vez se ha detectado y localizado la falla, MPLS introduce el Modelo de Protección (Conmutación Protegida) o el Modelo de Restablecimiento (re-enrutamiento) para la recuperación del camino. La diferencia entre protección y restablecimiento se centra en las distintas escalas temporales en las que operan cada uno. La protección requiere recursos preasignados y tiene la facilidad para desarrollar e implementar métodos de protección rápidos para la recuperación de fallas (menos de un par de centenas de milisegundos), por medio del establecimiento de LSPs redundantes, los cuales se usan como caminos de respaldo. Por otra parte, el restablecimiento se basa en el re-enrutamiento y asignación dinámica de recursos y puede llevar un tiempo mayor en orden de magnitud que la conmutación protegida. El restablecimiento también conlleva el cálculo dinámico de caminos, que puede ser computacionalmente costoso si los caminos de respaldo no están precalculados o si los recursos precalculados ya no están disponibles. El objetivo de estos modelos es minimizar el riesgo de fallas de conectividad tanto en los enlaces físicos o virtuales como en los nodos de una red.

Este capítulo presenta las principales características de diseño y aplicación de los métodos de protección (Conmutación Protegida) de MPLS. Primero, se describen los principales componentes y sus funciones, implicados en un dominio de red protegido. Luego se presentan diferentes opciones para clasificar los mecanismos de protección, como son los métodos Global, Local, Inverso y también la utilización de los diferentes tipos de recuperación como es el modelo *m:n*. Finalmente se analiza la notificación de fallas en el ciclo de recuperación y se comparan los principales métodos de protección.

2.1 PROTECCIÓN (CONMUTACIÓN PROTEGIDA)

MPLS proporciona una medida de recuperación ofrecida por la Protección (Conmutación Protegida) para soportar la capacidad de la red y mantener los servicios existentes ante fallas, mediante los diferentes métodos de protección a través del pre-establecimiento de LSPs de respaldo una vez ocurra la falla en el enlace o el nodo de la red, minimizando así la interrupción en el tráfico de datos y logrando mejores tiempos de conmutación protegida que las redes IP.

2.1.1 Arquitectura y funcionamiento de protección en MPLS

El método usual para desarrollar un dominio de protección MPLS involucra un camino de trabajo (camino activo) y un camino de respaldo (camino de recuperación). No siempre un LSP de respaldo se crea en el nodo de ingreso y finaliza en el nodo de egreso, es decir, que un LSP de respaldo puede ser implementado como un LSP de segmento. En este caso para proporcionar ciertas características de protección son necesarias dos clases de nodos [15]: un nodo responsable de la conmutación entre el camino de trabajo y el camino de respaldo, llamado LSR Conmutador de Rutas (PSL: Path Switch LSR) y otro nodo donde el tráfico de los caminos de trabajo y respaldo es combinado, llamado LSR Combinador de Rutas (PML: Path Merge LSR).

Los métodos de protección ante fallas siguen un ciclo, desde la identificación de la falla hasta la recuperación del LSP. Este ciclo involucra varios componentes [16]:

1. Un método de encaminamiento que selecciona caminos de trabajo y de respaldo.
2. Un método de reserva de ancho de banda en ambos caminos.
3. Un método de señalización para configurar (distribuir las etiquetas) en los caminos de trabajo y respaldo (por ejemplo, LDP/RSVP o CR-LDP/RSVP-TE o CR- LDP/RSVP-TE).
4. Un mecanismo de detección y otro de notificación de fallas, todos ellos necesarios para indicar al nodo responsable de tomar las acciones de respuesta a la falla que se ha producido.
5. Un mecanismo para desviar el tráfico desde el camino de trabajo (en el que se ha producido la falla) hasta el camino de respaldo.
6. Un mecanismo de recuperación (opcional), para la conmutación del tráfico hacia el camino de trabajo original, una vez la falla sea corregida o reparada.

La figura 2.1 muestra un dominio de protección MPLS simple, formado por un Trayecto de Conmutación Etiquetas de Trabajo (o segmento del camino de trabajo), que es el segmento protegido y el Trayecto de Conmutación de Etiquetas de Respaldo (o el camino de recuperación) hacia donde el tráfico es conmutado una vez se detecte la falla. Los componentes PSL y PML son dos LSRs con funciones de protección. Todos los componentes implicados en el control de fallas de MPLS serán descritos más adelante en esta sección.

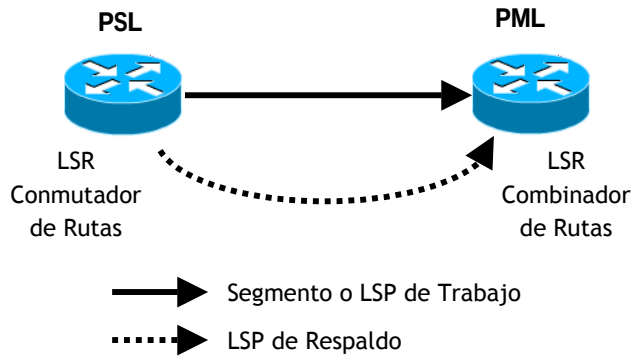


Figura 2.1 Dominio de Protección MPLS.

2.1.2 Conceptos de la arquitectura de protección MPLS

La protección en MPLS introduce algunas definiciones para facilitar el entendimiento de los componentes de gestión de fallas [17]:

2.1.2.1 Dominio de Protección MPLS

Se define como el conjunto de LSRs sobre los cuales, un camino activo y su camino de protección correspondiente son encaminados. En el dominio de protección estos se conocen como el Camino de Trabajo (WP: Working Path) y el Camino de Respaldo (BP: Backup Path) respectivamente.

2.1.2.2 Fallas y señales / mensajes de recuperación

- ✓ **Señal de Indicación de Falla** (FIS: Failure Indication Signal): es una señal que indica que una falla ha sido detectada en un par de LSRs. Esta consiste en una secuencia de paquetes de indicación de falla transmitida desde un LSR descendente a un LSR ascendente, los cuales son transmitidos por cada LSR intermedio a su vecino ascendente, hasta localizar el LSR encargado de desempeñar las funciones de PSL.

- ✓ **Señal de Recuperación de Falla** (FRS: Failure Recovery Signal): es una señal que indica que una falla a lo largo del camino de un LSP ha sido reparada. Esta consiste en una secuencia de paquetes de indicación de recuperación transmitida por un LSR descendente a su LSR ascendente. Nuevamente, como ocurre en la FIS, esta señal es transmitida por cada LSR intermedio a su vecino ascendente, hasta localizar el LSR de protección original.

- ✓ **Mensaje de Verificación** (LM: Liveness Message): mensaje que se intercambia periódicamente entre dos LSRs adyacentes, comprobando la integridad del enlace entre estos y sus vecinos.

- ✓ **Falla del Enlace** (LF: Link Failure): se define como una falla física del enlace entre LSRs adyacentes o un LSR vecino. (En el caso de un enlace bidireccional implementado con dos enlaces unidireccionales, podría significar que se daña cualquiera de los dos o ambos enlaces unidireccionales).

- ✓ **Pérdida de Señal** (LOS: Loss of Signal): esta se produce cuando una señal no es detectada por ninguna interfaz, debido a un deterioro o avería en la capa física.

- ✓ **Pérdida de Paquete** (LOP: Loss of Packet): ocurre cuando se presenta una falla en el enlace o en el LSR local. Esta consiste en el descarte excesivo de paquetes en una interfaz, debido a la incompatibilidad de etiquetas o a errores TTL.

2.1.2.3 Componentes de protección MPLS

- ✓ **Trayecto Conmutado de Etiquetas Activo o de Trabajo.** Es un LSP que se establece para llevar tráfico desde un LSR fuente a un LSR destino en condiciones normales, por ejemplo, en ausencia de fallas. En otras palabras, un camino de trabajo es un LSP que contiene flujos de tráfico que requieren de protección. La parte de un LSP de trabajo que requiere protección se conoce como segmento protegido.

- ✓ **Camino Activo o de Trabajo.** Este camino puede ser un segmento de un LSP o un LSP completo que requiere protección. El camino de trabajo se designa por la secuencia de LSRs que este recorre.

- ✓ **LSR Conmutador de Rutas.** Un PSL es el LSR origen del camino de trabajo y el camino de protección correspondiente. En el caso de una falla, se envía la FIS o su propio mecanismo de detección; la protección realiza la conmutación del tráfico a los LSRs protegidos entre el camino de trabajo y su camino de respaldo.

- ✓ **LSR Combinador de Rutas.** El PML es el LSR donde finaliza el camino de trabajo y el camino de protección correspondiente, y combinan su tráfico solo en el LSP de salida, o, si este es el destino, pasa el tráfico a los protocolos de capa más altos.

- ✓ **LSR Intermedio.** Es un LSR en el camino de trabajo o en el camino de protección que no es el PSL ni el PML.

- ✓ **Trayecto Conmutado de Etiquetas de Respaldo o de Protección.** Es un LSP que se establece para llevar el tráfico del camino de trabajo (o caminos) una vez ha ocurrido la falla sobre este (o sobre uno de los caminos de trabajo, si existe mas de uno), y después realizar la conmutación por el PSL. En la protección del LSP se puede proteger tanto un segmento del camino de trabajo como el camino de trabajo completo.

2.1.3 Tipos de protección

Los tipos de protección para las redes MPLS pueden categorizarse como: protección del enlace, protección del nodo, protección del camino y protección del segmento.

Protección del Enlace. El objetivo es proteger un LSP de una falla en el enlace, mediante un LSP de respaldo (LSP secundario), el cual es disyunto del camino de trabajo (LSP primario) o LSP operacional sobre el cual la protección es requerida. Éste es un método de recuperación local que puede ser rápido y podría ser más apropiado en situaciones dónde algunos elementos de la red a lo largo de un camino dado son menos fiables que otros.

Protección del Nodo. El objetivo es proteger un LSP de una falla en el nodo, mediante un LSP de respaldo disyunto del LSP de trabajo que contiene el nodo a ser protegido. Cuando el nodo falla,

el tráfico del LSP de trabajo es conmutado al LSP de respaldo directamente en el LSR ascendente conectado al nodo que falla.

Protección del Camino. El propósito es proteger un LSP de una falla en cualquier punto a lo largo del camino de trabajo; de esta manera el LSP de respaldo protege completamente al LSP de trabajo de toda posible falla tanto en el enlace como en el nodo, excepto por las fallas que podrían ocurrir en los LSRs de ingreso y egreso del dominio MPLS, o para fallas asociadas que puedan impactar simultáneamente en el funcionamiento del LSP de trabajo como en el LSP de respaldo. Bajo esta condición, el LSP de respaldo está completamente disyunto del LSP de trabajo.

Protección del Segmento. Un dominio MPLS puede ser subdividido en múltiples dominios de protección (subdominios), por lo cual una falla en el subdominio de protección se corrige dentro de ese dominio. En los casos donde un LSP atraviesa los múltiples dominios de protección, el mecanismo de protección dentro de un dominio sólo necesita proteger el segmento del LSP que se encuentra dentro de este dominio (subdominio). Generalmente la protección del segmento es más rápida que la protección del camino dado que la recuperación casi siempre ocurre más cerca de la falla.

2.1.4 Modelo de protección m:n

Probablemente, el modelo de protección m:n es uno de los modelos de clasificación de recuperación de fallas más conocido. Está basado en el número de caminos de respaldo y caminos de trabajo protegidos, donde *m* es el número de LSPs de respaldo usados para proteger los *n* LSPs de trabajo. Los modelos de protección factibles podrían ser:

1:1: un LSP de trabajo es protegido por un LSP de respaldo.

n:1: un LSP de trabajo es protegido por *n* LSPs de respaldo, posiblemente debido a la proporción de la carga. Entre más LSPs de respaldo sean usados, se puede considerar compartir el tráfico a través de los LSPs de respaldo cuando el LSP de trabajo falla, para así satisfacer el requerimiento de ancho de banda de la troncal de tráfico asociada con el LSP de trabajo. Esto puede ser especialmente útil cuando no es factible encontrar un camino que pueda satisfacer el requerimiento de ancho de banda del LSP primario.

1:n: un LSP de respaldo se usa para proteger n LPSs de trabajo (respaldos compartidos).

1+1: el tráfico se envía simultáneamente tanto al LSP de trabajo como al LSP de respaldo. En este caso el LSR de egreso selecciona uno de los dos LSPs basado en el proceso de decisión de la totalidad del tráfico local, el cual compara el tráfico recibido del LSP de trabajo y el LSP de respaldo e identifica las diferencias. Este modelo presenta ineficiencia en la utilización de recursos.

2.2 PRINCIPALES MÉTODOS DE PROTECCIÓN DE FALLAS EN MPLS

El método usual para ofrecer protección en los ambientes de MPLS es preestablecer un LSP de respaldo para conmutar el tráfico cuando ocurra la falla. Los diferentes métodos de protección pueden ser tratados dependiendo del origen o de la notificación de la falla/recuperación. La mayoría de estos métodos de protección se han propuesto en los trabajos realizados y especificados por el Grupo de Trabajo MPLS en el Área de Enrutamiento de la IETF [18], [19], [20] o [21].

A continuación se realiza un análisis de los principios fundamentales y una revisión de las ventajas y desventajas de los métodos más comunes de protección MPLS [22].

2.2.1 Método global / respaldo centralizado

En este método, el nodo de ingreso es el responsable de realizar el restablecimiento de la falla cuando la FIS llegue, para lo cual es necesario un camino de respaldo distinto al camino de trabajo [23].

Las acciones de protección siempre se activan en el nodo de ingreso, independientemente de donde ocurra la falla (a lo largo del camino de trabajo). Esto significa que la información de la falla tiene que propagarse desde el nodo donde ésta es detectada hasta el nodo de ingreso. Si no se dispone de ningún LSP inverso, la detección de la falla se tendrá que realizar con otro tipo de mecanismo como la monitorización continua del camino de trabajo.

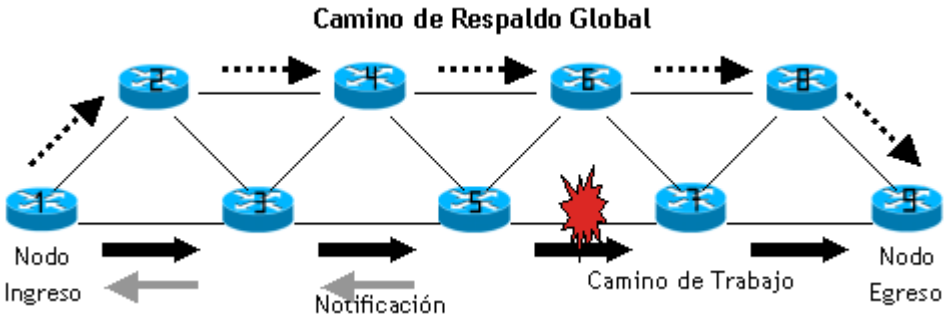


Figura 2.2 Modelo de respaldo Global/Centralizado.

La figura 2.2 muestra un escenario simple formado por nueve LSRs donde el camino de trabajo (LSR1-LSR3-LSR5-LSR7-LSR9) y el camino de respaldo (LSR1-LSR2-LSR4-LSR6-LSR8-LSR9) están preestablecidos. En condiciones normales, el tráfico se transmite desde el nodo de ingreso LSR1 hasta el nodo de egreso LSR9 a través del camino de trabajo. Cuando se detecta una falla en el enlace (por ejemplo entre LSR5 y LSR7) se envía al nodo de ingreso (LSR1) una Señal de Indicación de Falla, el tráfico cambia hacia la ruta de respaldo global.

Este método tiene la ventaja de tener que configurar un único camino de respaldo para cada camino de trabajo y, además, es un método de protección centralizado, lo que significa que un único nodo tiene que ser provisto de las funciones de PSL y otro nodo con los rasgos de PML. Por otro lado, este método presenta un alto costo en términos de tiempo de restablecimiento [24], en particular se utiliza una Prueba de Continuidad del Camino (técnica de monitoreo para detectar las fallas en el enlace o en el nodo) como un método de indicación de falla. Durante este tiempo hay una pérdida de paquetes proporcional al tiempo de recuperación requerido. Además, los paquetes que estaban circulando en el enlace donde ocurre la falla, en el momento de producirse ésta también se perderán. Este es un inconveniente común en todos los modelos de recuperación, aunque, hay actualmente algunas propuestas como aquellas que evitan la pérdida de paquetes en el enlace que tiene la falla mediante la aplicación de etiquetas y técnicas de almacenamiento temporal [25].

2.2.2 Método inverso

Los caminos alternos preestablecidos son esenciales cuando ocurre pérdida de paquetes, debido a fallas indeseables en el LSP. Esto puede tomar un tiempo significativo para detectar una falla distante en el enlace para un dispositivo en el camino de conmutación de etiquetas, los paquetes podrían continuar siendo enviados a lo largo del camino primario. En cuanto los paquetes alcancen al conmutador que esta enterado de la falla, se conmuta al camino de respaldo reenrutándose y así se evita la pérdida de los datos.

La función principal de este método es devolver el tráfico al nodo de ingreso usando un camino de respaldo desde el punto donde se produce la falla. Cuando la falla a lo largo del camino protegido se detecte, el LSR de ingreso del enlace que ha fallado desvía el tráfico entrante. Luego, remite este tráfico al LSP de respaldo que cruza el camino en la dirección inversa del LSP de trabajo (LSP primario). El tráfico y la señal de notificación son enviados al nodo de ingreso. En cuanto la FIS llega, el nodo de ingreso deja de enviar el tráfico al camino de trabajo y cambia el tráfico al camino de respaldo (respaldo global).

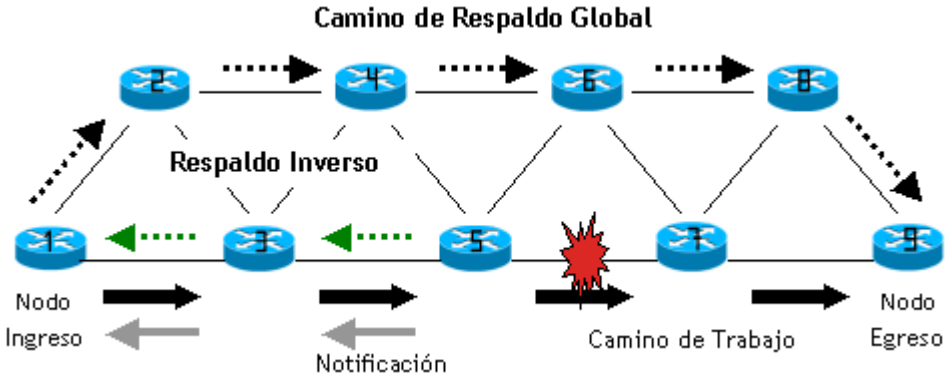


Figura 2.3 Modelo de respaldo Inverso.

La figura 2.3 muestra un ejemplo de utilización del método inverso. Se establecen los caminos de trabajo y respaldo de la misma forma que en el método global y además se añade un camino de respaldo inverso desde LSR5 (LSR5-LSR3-LSR1) hacia el nodo de ingreso. Cuando se detecta una falla en el LSP (LSR5-LSR7), el tráfico se desvía hacia el LSR1 (nodo de ingreso) a través del camino de respaldo inverso; una vez allí, el método se comporta igual que el método global (centralizado).

Este método es sobre todo conveniente en los escenarios de red donde los flujos de tráfico son muy sensibles a pérdidas de paquetes. Por ejemplo, en la transmisión de voz, el retardo es común, pero si un archivo está transmitiéndose, las pérdidas del paquete podrían ser críticas. Si el segmento del enlace o el nodo dónde la falla ocurre esta lejos del nodo de ingreso y la tasa de transmisión es muy rápida, el número de paquetes perdidos puede ser muy alto si se usa respaldo centralizado. La utilización de respaldo inverso permite la recuperación de paquetes cuando la falla ocurre, rescatando paquetes perdidos si se aplica el método centralizado. Otra ventaja consiste en simplificar el mecanismo de notificación de falla, utilizando el LSP de respaldo desde donde ocurre la falla hasta el nodo de ingreso (ver figura 2.3).

La principal desventaja es que tiene un tiempo de restablecimiento igual al del método global. Además, necesita introducir un nuevo camino de respaldo, con lo cual la utilización de los recursos es aún peor que en el método global. A pesar de todo, un respaldo inverso puede ser establecido en asociación con el camino de trabajo, simplemente haciendo que cada LSR a lo largo del camino de trabajo recuerde a su vecino. Otro problema de este esquema es que los paquetes que llegan de la dirección inversa son mezclados con los paquetes entrantes, resultando un desorden de paquetes a través del LSP de respaldo durante el periodo de recuperación.

2.2.3 Método local / respaldo de segmento

En este método el restablecimiento se activa en el mismo punto donde se produce la falla; es, por lo tanto, un método transparente al nodo de ingreso. Su principal ventaja es que ofrece mejor tiempo de restablecimiento que el método global y evita la pérdida de paquetes.

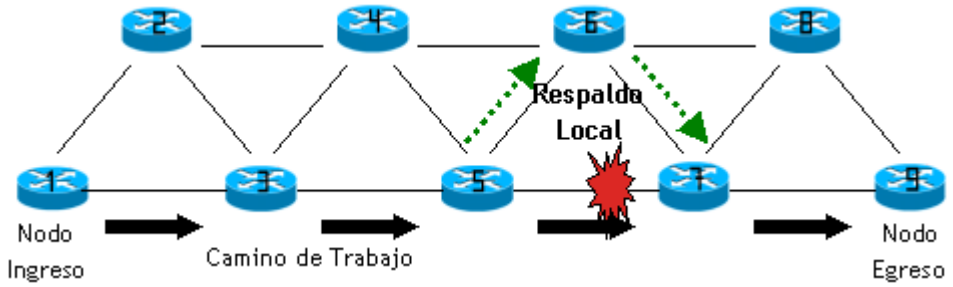


Figura 2.4 Modelo de respaldo Local.

La figura 2.4 muestra el modelo de red de trabajo, donde se tiene un camino principal formado por los nodos (LSR1-LSR3-LSR5-LSR7-LSR9). El camino de respaldo local formado por LSR5-LSR6-

LSR7 es más corto que el camino de recuperación LSP en el método global. Los LSR5 y LSR7 son los nodos con funciones PSL y PML respectivamente. Cuando ocurre una falla en el enlace, el tráfico se cambia (de LSR5-LSR7), que es un segmento del camino de trabajo al camino de respaldo del LSP (LSR5-LSR6-LSR7).

La principal dificultad reside en tener que proveer de funciones PSL (y en su caso PML) a todos los nodos de los segmentos del camino de trabajo que se quiere proteger. Además, se tiene que buscar tantos caminos de respaldo como segmentos a proteger (a diferencia del método global, donde es necesario un único camino de respaldo), lo que significa baja utilización de recursos y una alta complejidad de dirección. Por otro lado, este método ofrece la transparencia al nodo de ingreso, el tiempo de recuperación es más rápido y no se producen pérdidas de paquetes como en el método global [26].

Una solución intermedia podría ser el establecimiento de respaldos locales, pero sólo para segmentos donde requieren un alto grado de fiabilidad, suministrando protección solo para ese segmento de camino. La figura 2.5 muestra este caso, el segmento protegido es formado por LSR5-LSR7-LSR9. Si una falla ocurre (entre LSR7-LSR9) se envía una FIS al nodo PSL (como se observa en este caso el PSL no es el nodo de ingreso). Después de que la FIS llega, el tráfico es recuperado usando el respaldo del segmento alterno (LSR5-LSR6-LSR8-LSR9).

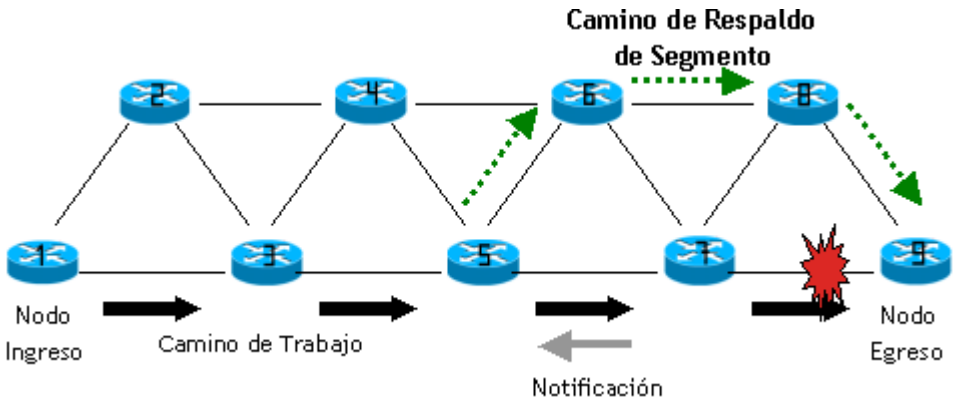


Figura 2.5 Modelo de respaldo del Segmento.

Hay varias versiones del modelo local/segmento, dependiendo de la asignación de los nodos PSL y PML. Por ejemplo el nodo PML, puede corresponder con el nodo de ingreso. Sin embargo la protección del segmento ofrece un mejor tiempo de recuperación que los métodos global/inverso donde hay un tiempo de notificación de fallas y en el caso del ejemplo, la pérdida del paquete puede ocurrir.

2.2.4 Ciclos de protección

Otro modelo de recuperación de fallas es el de ciclos de protección (p-ciclos). Los p-ciclos pueden ser considerados como los ciclos de protección pre-configurados en una red en malla. Un

p-ciclo permite la protección de aquellos enlaces que tienen sus puntos finales en nodos, los cuales pertenecen al mismo p-ciclo. Por lo tanto, los enlaces que pertenecen al p-ciclo (1-2, 2-3, 3-4, y 4-1) como los que no están en éste (enlaces a ambos lados, enlace 1-3) son protegidos, como se muestra en la figura 2.6 (a) y (b).

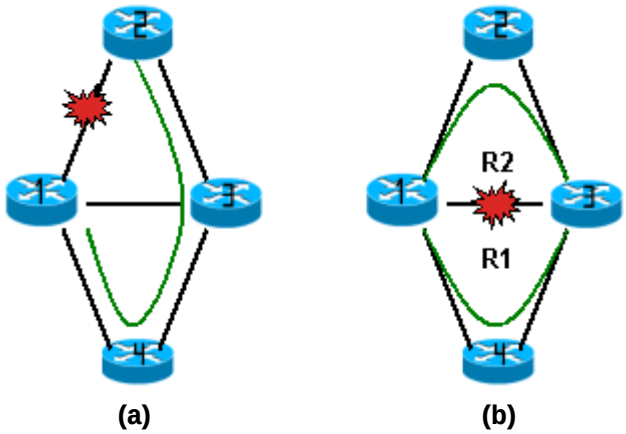


Figura 2.6 Ciclo de protección.

En el primer caso, figura 2.6 (a), el enlace potencial de fallas es protegido por los enlaces restantes del p-ciclo. En el segundo caso, figura 2.6 (b), un enlace a ambos lados puede ser protegido por los dos caminos de respaldo proporcionados por el p-ciclo (R1, R2), por lo tanto, más que un camino de trabajo este comparte el mismo enlace protegido.

En este marco, las decisiones de conmutación protegida pueden hacerse rápidamente porque estas se llevan a cabo en el enlace defectuoso. Nótese que un p-ciclo no puede proteger más de una falla en el enlace al mismo tiempo. Sin embargo, el empleo de múltiples p-ciclos en una red disminuye el impacto de múltiples fallas.

2.3 MÚLTIPLES FALLAS

A pesar de enfocar este trabajo en un esquema de recuperación de fallas simple, es pertinente introducir brevemente el problema de múltiples fallas. A continuación se describen dos esquemas de recuperación múltiple.

2.3.1 Recuperación basada en prioridad

Los esquemas de recuperación de fallas típicamente asumen eventos de falla simple. Sin embargo, múltiples fallas pueden ocurrir en algún intervalo corto de tiempo. La protección contra ocurrencias en escenarios defectuosos requiere cantidades grandes de capacidad de respaldo. Idealmente, la red debe recuperar algunos de los caminos de trabajo en esta situación.

Por ejemplo, se considera la figura 2.7, donde ocurren dos fallas al mismo tiempo. En este caso hay dos caminos de trabajo: WP-LSP1: [1-2-3-4] y WP-LSP2: [7-8-9-10] y sus respectivos caminos de respaldo BP-LSP1: [1-5-6-4] y BP-LSP2: [7-5-6-10].

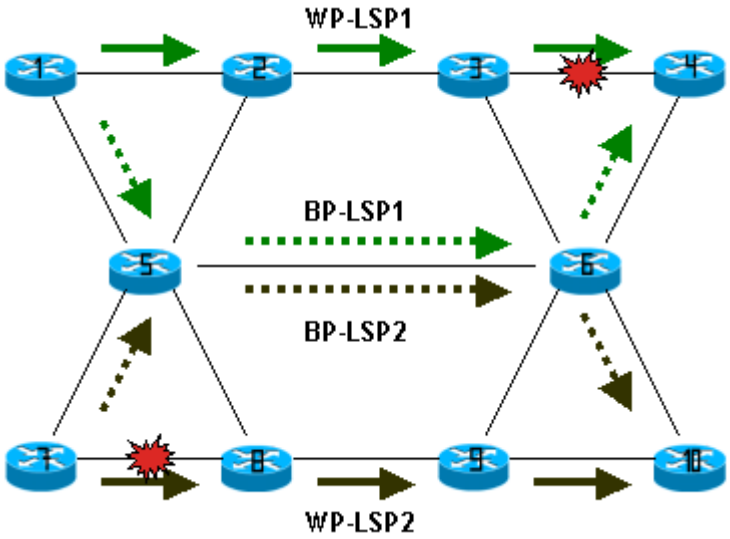


Figura 2.7 Múltiples Fallas: Recuperación basada en prioridad.

Como se puede observar, se presentan dos fallas: una entre los LSRs 3-4, y la otra en el enlace entre los LSRs 7-8. En este ejemplo, LSR3 detecta la falla y envía un mensaje de notificación de falla al nodo de ingreso (LSR1). Casi al mismo tiempo, LSR7 detecta una falla. Si no se usa priorización en LSR6, el camino de recuperación cambia el tráfico de LSR6 a LSR4 porque el mensaje de notificación de falla es para WP-LSP1. Por otro lado, en LSR5, el camino de recuperación cambia el tráfico de LSR5 a LSR6 porque el mensaje de notificación de falla es para WP-LSP2. Como resultado, un camino de recuperación no valido se asigna para seguir (7-5-6-4).

El control basado en prioridades es un método efectivo y recupera los caminos de trabajo específicos bajo condición de múltiples fallas. En el ejemplo anterior, si la prioridad de WP-LSP1 es más alta que WP-LSP2, entonces los mensajes de notificación de falla para WP-LSP1, son priorizados. En otras palabras, el sistema verifica la prioridad del camino de protección y el conjunto de prioridades cambia. En tal caso, la conmutación del tráfico de LSR6 a LSR4 tiene prioridad sobre la conmutación del tráfico de LSR6 a LSR10. Por consiguiente, el camino de recuperación de alta prioridad se activa. La prioridad en general debe asignarse según la política del operador y/o el servicio de la red.

2.3.2 Protección multinivel

La protección multinivel tiene más de un sistema de protección para alcanzar diferentes niveles, dependiendo de la clase de tráfico [27]. Por lo tanto, un escenario de protección multinivel se

establece dinámicamente usando las principales características de calidad de servicio.

En los escenarios de red con un alto grado de requerimientos de protección, la aplicación de gestión de fallas multinivel podría mejorar el desempeño, en comparación con la gestión de nivel simple. No obstante, la construcción del escenario completo es muy costosa (en términos de tiempo y recursos), de esta manera sería mejor construir escenarios multinivel intermedios. Por ejemplo, el dominio protegido podría comenzar únicamente con método global y cuando los requerimientos de protección aumenten (un nodo falla repetidamente), un nuevo camino de respaldo local podría establecerse, de tal manera que proporcione un nuevo nivel de protección.

La figura 2.8 muestra un ejemplo donde el camino de trabajo es (1-3-5-6). Si el enlace (3-5) falla, se utiliza al comienzo el camino de respaldo global (1-2-4-6). Entonces, si el enlace (1-2), que parte del camino de respaldo global, también falla, se usa el camino de respaldo local (3-4-6). Por lo tanto, en este caso de múltiples fallas, el tráfico podría ser enrutado a través del camino (1-3-4-6) evitando que se presente discontinuidad en los segmentos. Si otro enlace (o nodo) fallan pueden superarse las fallas de igual manera.

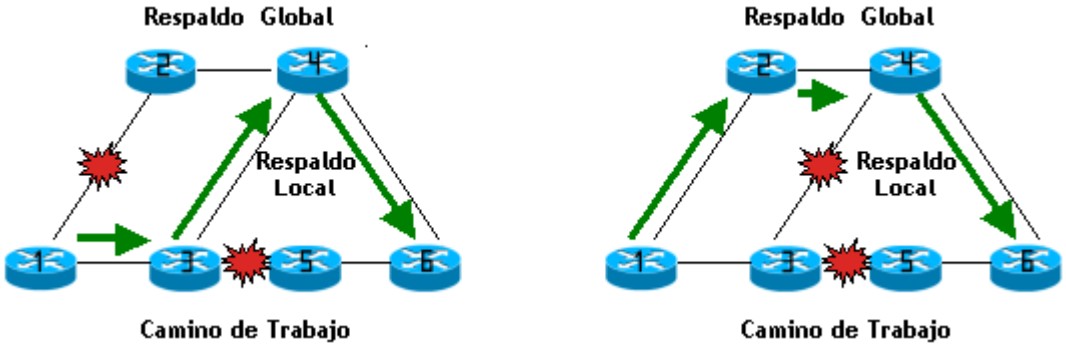


Figura 2.8 Múltiples Fallas: Protección multinivel.

Otra aplicación de la protección multinivel se muestra en la figura 2.8 (b). De nuevo, el camino de trabajo es (1-3-5-6) y el enlace (3-5) es el que falla. En este caso, se usa el inicio del camino de respaldo local (3-4-6). Entonces, si el enlace (3-4) también falla, se aplica otro método de respaldo (respaldo global) y se superan ambas fallas.

2.4 NOTIFICACIÓN DE FALLAS

Uno de los puntos principales en el ciclo de recuperación es la detección y notificación de fallas tanto en el enlace como en el nodo. La detección de la falla puede ser realizada en diferentes capas de la red, dependiendo del tipo de falla y de los protocolos de capa baja. La notificación de la falla, una vez ésta es detectada, puede ser local o centralizada. Si es un método de protección local no usa la notificación de falla, debido a que las acciones de recuperación son efectuadas por el mismo nodo que detecta la falla. Por otro lado, si es un nodo que no es necesariamente el responsable de la detección de la falla, la falla debe ser comunicada desde el

punto donde ocurre ésta hasta el nodo de ingreso o al nodo designado para activar las acciones de recuperación (nodos PSL).

La notificación de fallas presenta varias propuestas, con el objetivo de minimizar el tiempo de restablecimiento dentro del ciclo de recuperación. Entre estas se encuentran:

2.4.1 Notificación Inversa

El Camino de Notificación Inverso (RNT: Reverse Notification Tree), es una propuesta para desarrollar la notificación en un ambiente de protección local (segmento) o global (centralizado). RNT, es un camino punto a multipunto unido al PML a lo largo del cual la FIS o la FRS viajan al PSL, presentando las siguientes ventajas [18]:

- ✓ El RNT se establece en asociación con el camino de trabajo, haciendo que cada LSR a lo largo del camino activo recuerde su vecino ascendente (o el grupo de vecinos ascendentes cuyos caminos de trabajo convergen al LSR). No se requiere enrutamiento multicast.

- ✓ Se requiere un solo RNT para todos los caminos de trabajo que se combinan para formar el camino de transmisión multipunto a punto. El RNT está unido al PML y termina en los PSLs. Todos los LSRs intermedios en la convergencia de los caminos de trabajo comparten el mismo RNT.

Múltiples LSP podrían unirse en un solo LSP. En este caso, se propagaría la notificación de la falla (y la recuperación) hacia los LSPs involucrados en el desarrollo del RNT. En la figura 2.9 se plantea dos escenarios, dependiendo si el dominio de protección es independiente o no. Por ejemplo, el dominio de protección definido por (9-3-4-6-7, 9-10-7) es completamente independiente del dominio definido por (11-13-5-15, 13-14-15). Una vez la falla ocurra, esta no afecta al otro RNT, por consiguiente la detección de falla múltiple podría ser hecha al mismo tiempo.

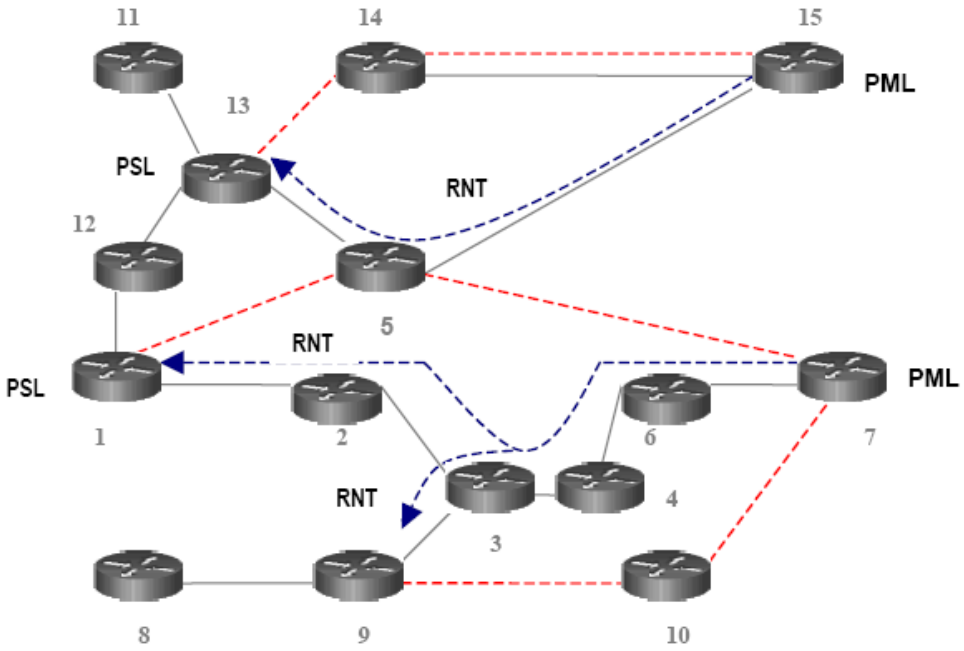


Figura 2.9 Relación entre dominios de protección MPLS.

Si los dominios de protección con diferentes RNTs se superponen, las fallas en los caminos de trabajo de los dos dominios no se verán afectados entre si, debido a que cada RNT trabaja independientemente uno del otro. Sin embargo, las fallas en el camino de protección de un camino puede afectar al camino de trabajo del otro y viceversa. Por ejemplo, el dominio de protección definido por (1-2-3-4-6-7, 1-5-7) no es independiente del dominio definido por (11-13-5-15, 11-13-14-15) dado que el LSR5 se encuentra tanto en el camino de protección del dominio anterior como en el camino de trabajo del siguiente dominio.

2.4.2 Notificación basada en señalización

En el caso de señalización, la recuperación de falla del enlace ocurre como parte de un proceso. En el caso de un nodo que detecta la falla y notifica a las fuentes del LSP, los pasos del proceso son los siguientes [25]:

- ✓ Detecta todos los LSPs que son afectados por una falla en el enlace.
- ✓ Envía un mensaje de indicación de falla a la fuente de cada LSP identificado.
- ✓ Los nodos intermedios que reciben el mensaje lo reenvían sobre el LSP del nodo fuente.

Cuando cada nodo LSP de la fuente recibe el mensaje de indicación de falla, ocurre lo siguiente:

- ✓ El nodo LSP de la fuente envía un mensaje de reconocimiento de falla al nodo de detección.
- ✓ Al recibir dicho mensaje, los nodos intermedios lo envían sobre el nodo de origen.
- ✓ El nodo LSP de origen envía un mensaje de petición de intercambio de extremo a extremo al nodo LSP destino a lo largo del camino de protección, con la información sobre el LSP que debe ser recuperado.
- ✓ El nodo LSP destino envía un mensaje de respuesta de intercambio de extremo a extremo sobre el nodo LSP de origen a lo largo del camino de protección.
- ✓ Al recibir dicho mensaje de respuesta, el nodo LSP de origen comienza a enviar los datos a lo largo del camino de protección.

Este proceso se muestra en la figura 2.10. En este caso una falla ocurre en el enlace 3-4. Después de que la falla se detecta, el nodo 3 envía un mensaje de indicación de falla al nodo de ingreso (nodo 1). Los nodos Intermedios (nodo 2) reciben este mensaje y lo reenvían a los nodos ascendentes. Una vez que el mensaje de indicación de falla llega al nodo de ingreso, el nodo 1 envía un mensaje de reconocimiento de falla al nodo de detección (nodo 3). El nodo de ingreso envía un mensaje de petición de intercambio de extremo a extremo al nodo LSP destino (nodo 6) a lo largo del camino de respaldo (1-7-8-9-10-11-12-6), con la información sobre el LSP que será recuperado. El nodo LSP destino (nodo 6) envía un mensaje de respuesta de intercambio de extremo a extremo hacia el nodo LSP de origen a lo largo del camino de respaldo. Una vez el nodo de ingreso reciba el mensaje de respuesta, el nodo LSP de origen comienza la conmutación.

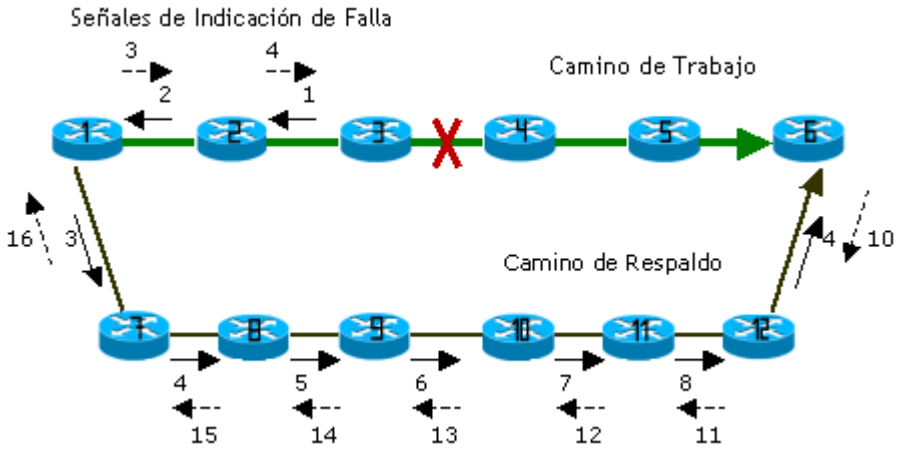


Figura 2.10 Notificación de fallas basada en señalización.

La figura 2.11 muestra el problema de retardo de encolamiento en el caso de usar técnicas basadas en señalización. En este caso hay tres LSPs en el enlace afectado. Después de que la falla es detectada, el nodo 3 envía tantos mensajes de indicación de falla como números de LSPs a sus nodos de ingreso. Cada mensaje llega a las memorias de almacenamiento temporal del nodo

intermedio y se envían a los nodos ascendentes. En el caso de un gran número de LSPs en el enlace afectado, los mensajes de indicación podrían experimentar un alto retraso debido al retardo de encolamiento. Un caso similar ocurre cuando los caminos de respaldo son señalizados antes del intercambio.

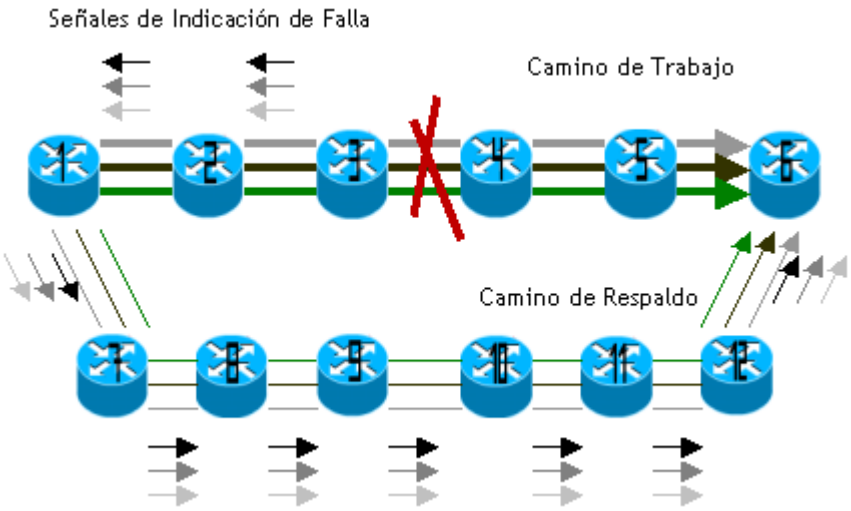


Figura 2.11 Retardo de encolamiento en notificación de fallas basado en señalización.

El peor caso de señalización se muestra en la figura 2.11, cuando todos los LSPs tienen los mismos nodos de ingreso y de egreso. En este caso los mensajes tienen que hacer cola en todos los nodos del camino de respaldo (y también en el segmento del ascendente, entre la detección y los nodos de ingreso).

En tal caso el número de mensajes en la red es proporcional la longitud del camino de notificación y dobla la longitud del camino de respaldo. Y el máximo retardo de encolamiento es proporcional al número de LSPs protegidos en el enlace afectado y al número de mensajes.

2.4.3 Notificación basada en desbordamiento

Una aproximación alterna para manejar el tema de mensajes es mediante el uso de desbordamiento. En vez de enviar la notificación e iniciar la recuperación a través del LSP en cada nodo de origen, el nodo que detecta la falla (por ejemplo, corte de fibra) notifica a todos los nodos de la red. Por lo tanto, hay unos nodos que son afectados con la toma de acciones de recuperación requeridas, mientras los otros envían los mensajes hacia adelante sin la acción suplementaria, pero teniendo conocimiento sobre el orden de la falla, para así mantener un cuadro exacto de la disponibilidad del recurso [28].

La figura 2.12 muestra el proceso de desbordamiento, donde tanto el nodo de detección (en este caso solo el nodo 2) como los nodos intermedios (evitando la reproducción de los mensajes de indicación de falla), envían el mensaje de indicación de falla a sus vecinos. Obviamente, el

mensaje de indicación de falla llega a todos los nodos de ingreso en la red después del camino más corto (en términos de retardo). En la figura 2.12, sin embargo, los desbordamientos pueden seguir sólo el mismo camino que la notificación por señalización.

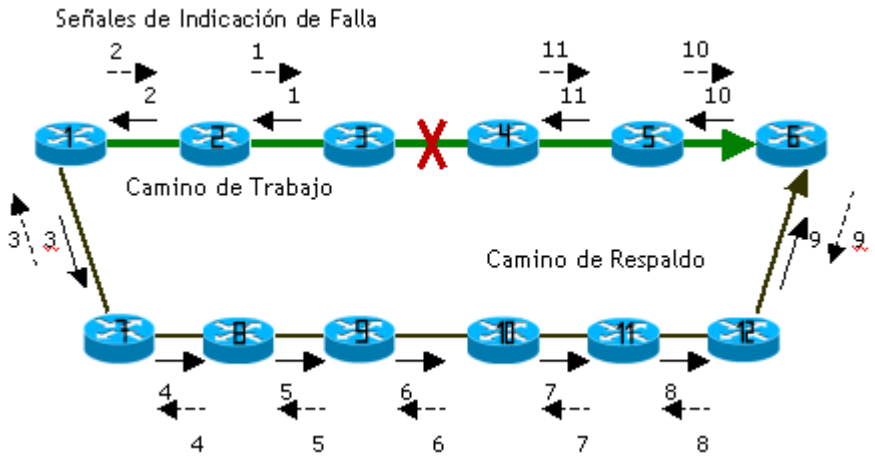


Figura 2.12 Notificación de fallas basada en desbordamiento.

Los nodos intermedios envían, asincrónicamente, los mensajes de reconocimiento de indicación de fallas. Después que el nodo de egreso (nodo 6) ha recibido el mensaje, no requieren ninguna acción remota (aunque el mensaje de notificación se remite a los nodos restantes). El nodo de ingreso puede empezar enviando el tráfico a los caminos de respaldo (estos nodos pueden saber en qué momento comenzar el intercambio).

2.4.4 Ventajas de la técnica de desbordamiento respecto a las técnicas basadas en señalización

Las ventajas de desbordamiento con respecto a las técnicas basadas en señalización pueden ser resumidas en el retardo de notificación mínimo, debido a lo siguiente:

- ✓ **Retardo del buffer:** El tiempo de encolamiento es cero.

- ✓ **Retardo de procesamiento en el nodo:** Procesamiento de tiempo mínimo en la notificación de mensajes. En la señalización de un mensaje RSVP, el tiempo de procesamiento en el nodo es cerca de unos 100 microsegundos.

- ✓ **Retardo del camino mínimo:** En las técnicas de desbordamiento la notificación de mensajes sigue el camino mínimo inverso (en términos de retardo). Los mensajes son propagados en todas las direcciones a todos los nodos en la red, garantizando un retardo mínimo. Esta propagación completa (en el caso de desbordamiento) también mejora el enrutamiento. De esta manera, todos los nodos son notificados de la falla y esto puede mejorar la evaluación de las futuras respuestas de enrutamiento, evitando las fallas en la señalización.

2.5 COMPARACIÓN DE LAS TÉCNICAS DE PROTECCIÓN DE LSP

La tabla 2.1 proporciona un resumen de algunos de los rasgos principales de las técnicas de protección de LSP, enfocados en [29]:

- ✓ La cantidad de recurso que se debe pre-asignar.
- ✓ La velocidad de restablecimiento.
- ✓ La complejidad de configuración y señalización.
- ✓ El cambio en la distancia de los caminos de trabajo.

Método de Recuperación	Requerimientos de Recurso	Velocidad de Recuperación	Complejidad de Configuración	Complejidad de Señalización	Distancia del Camino de Trabajo
Recuperación Local	No hay pre-asignación. El LSP recuperado usa la misma cantidad de recurso.	Lenta. Depende de la actualización de la tabla de enrutamiento y la señalización adicional.	Ninguna configuración adicional.	Ningún cambio de señalización existente.	El camino recuperado no puede ser el más corto disponible.
Re-enrutamiento a la entrada	Igual que el anterior.	Como el anterior, más notificación de falla a la entrada.	Ninguna configuración adicional.	Ningún cambio de señalización existente.	El camino recuperado es el más corto disponible.
Conmutación Protegida	El LSP de respaldo se pre-asigna, pero puede compartirse entre varios caminos primarios.	La velocidad es limitada por la propagación de la falla.	Deben configurarse los LSP de respaldo a la entrada del dominio.	Ningún cambio en la técnica de señalización, pero se pueden señalizar dos LSPs.	El camino de respaldo es escogido a través de la configuración.
Protección del enlace con Re-enrutamiento rápido	Enlace de respaldo pre-asignado. Necesita un respaldo para cada enlace protegido.	Recuperación rápida en cuanto la falla se detecte.	Los enlaces de respaldo necesitan ser configurados.	Ningún cambio, pero puede limitarse al espacio de la etiqueta global.	El camino de trabajo es extendido por la distancia del camino de respaldo.
Protección del nodo con Re-enrutamiento rápido	Nodo de respaldo preasignado. Necesita un respaldo para cada nodo protegido.	Recuperación rápida en cuanto la falla se detecte.	Los nodos de respaldo necesitan ser configurados.	Requiere información de etiquetas registradas en el enrutamiento. Puede limitarse al espacio de la etiqueta global.	El camino de trabajo es extendido por la distancia del camino de respaldo.
Re-enrutamiento rápido usando los caminos de desvío	Caminos de desvío pre-asignados. Necesita un camino de desvío para cada enlace y nodo protegido.	Recuperación rápida en cuanto la falla se detecte.	Los caminos de desvío se establecen automáticamente sin la configuración adicional.	Exige a la señalización solicitar re-enrutamiento rápido y distingue el camino de desvío.	El camino de trabajo es extendido por la distancia del camino de respaldo.

Tabla 2.1 Comparación de las técnicas de protección de LSP.

En un dominio de protección, se pueden establecer diferentes tipos de respaldo para ofrecer protección MPLS. En algunos casos la topología de la red puede ser forzada a funcionar solamente con un método de respaldo, mientras que en otros se puede pensar en implementar más de un método (mecanismo integrado).

Esta integración, dentro de un mismo modelo, permite la coexistencia de métodos que trabajan a distintas escalas temporales, aprovechando las ventajas que ofrece cada uno por separado, y colocarlos a operar de forma coordinada buscando que trabajen eficientemente y sin afectar los funcionamientos y operaciones individuales de cada uno de los métodos. Para aplicar uno u otro de los anteriores métodos de Protección (conmutación protegida) es necesario tener en cuenta algunos parámetros como velocidad de recuperación, pérdida de paquetes, consumo de recursos, etc., con el fin de garantizar la continuidad del servicio [26]. De tal forma que en caso de presentarse una falla, la red responda de manera rápida restableciendo el tráfico y encaminándolo con éxito hacia el destino, por lo tanto, de la elección adecuada depende el desempeño de la red, lo cual se verá reflejado en el grado de satisfacción de los usuarios.

3. MECANISMO INTEGRADO DE PROTECCIÓN CONTRA FALLAS

Dentro de las características que implementa MPLS, respecto a las facilidades de ingeniería de tráfico se encuentra la capacidad de la red para recuperarse ante fallas mediante los métodos de protección y evitar perder el tráfico que se estaba cursando, sobre todo cuando se está en un ambiente de redes multiservicio que requiere garantías sobre la calidad del servicio que se ofrece. En definitiva, la aplicación de uno u otro método permite obtener una cierta QoS en el tráfico y optimizar el rendimiento global de la red minimizando el riesgo de fallas de conectividad. Estas características y cómo y dónde aplicar un método u otro de protección dependen de las necesidades de la red (este campo es poco explorado en la literatura).

De los argumentos anteriores se plantea un Mecanismo Integrado de Protección contra fallas basado en políticas de restablecimiento, para redes MPLS; con el fin de aclarar y responder preguntas como: ¿Qué sucede si hay una falla en el nodo o en el enlace de la red?, ¿Qué nodo es el responsable de tomar las acciones de respuesta a la falla que se ha producido?, ¿Cuáles son los parámetros a tener en cuenta al seleccionar el camino de respaldo?, ¿Cuál sería el camino más adecuado a tomar en situaciones de falla?, ¿En que momento se debe encaminar por la ruta de respaldo? y ¿Cómo se elige el método adecuado de restablecimiento de fallas? [30]. Para lo cual, no sólo se dispone de un esquema de caminos de respaldo (Globales) para ofrecer protección a los caminos de trabajo (o segmentos del camino de trabajo), sino que existen otros métodos: locales, inversos e híbridos de estos para ofrecer protección; se busca la integración de varios métodos de recuperación hasta ahora empleados de forma independiente en la mayoría de los modelos de red actuales. Esta integración, dentro de un mismo modelo, permite la coexistencia de métodos que trabajan a distintas escalas temporales, aprovechando las ventajas que ofrece cada uno por separado, y colocarlos a operar de forma coordinada buscando que trabajen eficientemente y sin afectar los funcionamientos y operaciones individuales de cada uno de los métodos.

Uno de los problemas principales en el diseño de la red es la optimización de los recursos. Ésta es la razón principal para evaluar la cantidad de recursos de la red al aplicar cada método de protección de falla propuesto en el capítulo 2.

Este capítulo introduce las relaciones entre el impacto de falla y los diferentes métodos de protección en un mismo dominio simple MPLS (mecanismo integrado de protección). Primero, se establecen las políticas de restablecimiento que se ejecutarán en el momento en que ocurra la falla. Luego, se establece el escenario que contiene los tres métodos en un solo dominio. Finalmente, para la selección de uno u otro método se tendrán en consideración los parámetros de tiempo de restablecimiento, pérdida de paquetes, consumo de recursos de respaldo (en términos de ancho de banda), clasificación del tráfico, etc.; lo cual resolverá los problemas planteados anteriormente.

3.1 POLÍTICAS DE RESTABLECIMIENTO

Para el desarrollo del mecanismo integrado de protección es necesario especificar las políticas de restablecimiento de las troncales de tráfico cuyos caminos establecidos están afectados por fallas.

3.1.1 Políticas generales

1. Cuando ocurra una falla se debe realizar la recuperación por medio del Modelo de Protección (Conmutación Protegida).

2. Establecimiento tanto del camino de trabajo como su respectivo camino de respaldo.

3. El método de protección que reacciona cuando se produzca la falla en el enlace o en el nodo de la red, se elegirá de acuerdo a la distancia que exista entre el nodo anterior a la falla y el nodo de ingreso al dominio MPLS.

4. Una vez ocurra la falla en el camino de trabajo, se realiza la conmutación del tráfico al camino de respaldo (camino pre-establecido), independiente del método que se escoja.

5. Después del restablecimiento del camino donde ocurrió la falla, el tráfico es enrutado nuevamente desde el nodo de ingreso por el LSP de trabajo.

3.1.2 Políticas del mecanismo integrado

1. **Método Local.** Este método se ejecutará si la distancia es igual a cero.

2. **Método Global.** El nodo o el enlace donde ocurra la falla debe estar cerca del nodo de ingreso (nodo con funciones PSL).

3. **Método Inverso.** Recibe el mismo tratamiento que el método global y tiene prioridad sobre éste, ya que presenta menor pérdida de paquetes.

3.2 METODOLOGÍA DE EVALUACIÓN DE DESEMPEÑO

3.2.1 Herramienta de simulación

La metodología usada para la evaluación de desempeño en esta tesis es un simulador de red de dominio público, conocido como Network Simulator en su versión 2 (NS-2).

El NS-2 es considerado como la herramienta de simulación estándar usada ampliamente por la comunidad de investigación de redes para validar sus nuevas propuestas. Por consiguiente, el uso

del NS-2 como herramienta de evaluación tiene muchas ventajas:

1. Buena documentación.
2. Mantenimiento y actualizaciones constantes, debido a contribuciones por parte de muchas personas de los diferentes grupos de investigación de redes.
3. Permite calibrar las funciones básicas y parámetros en el simulador.

3.2.2 Criterios de desempeño

Se deben tener en cuenta varios criterios para comparar el desempeño entre diferentes esquemas de recuperación para MPLS, entre los más importantes se encuentran [31]: pérdida de paquetes, latencia, re-ordenamiento, tiempo de restablecimiento, tiempo de restablecimiento completo, vulnerabilidad y calidad de protección.

- ✓ **Pérdida de paquetes.** Los esquemas de recuperación pueden introducir pérdida de paquetes durante la conmutación del tráfico hacia el camino de respaldo. Éste es un parámetro crítico para los métodos de restablecimiento, ya que el rendimiento de las tasas obtenidas por el servicio son seriamente afectadas por la pérdida de paquetes. En las aplicaciones de tiempo real (por ejemplo, VoIP, multimedia, etc.) las pérdidas pueden interrumpir la conexión, es aquí, donde los métodos de protección deben garantizar mínima o ninguna pérdida del paquete durante el período de restablecimiento.

- ✓ **Latencia.** La latencia representa la cantidad de tiempo que toma un bit para recorrer la red. El valor de latencia se usa como un indicador de calidad de conexión de la red: si la latencia es baja la conexión es mejor; también se refiere al retardo extremo a extremo. Para aplicaciones en tiempo real, tales como flujo de video y audio o variación de latencia con el tiempo, éste también es un indicador importante de calidad de la red.

- ✓ **Re-ordenamiento de paquetes.** Los métodos de protección pueden introducir desorden de paquetes. La acción de volver a poner el tráfico en un camino establecido puede introducir re-ordenamiento de paquetes por el nodo de ingreso cuando se envíen los paquetes a través del LSP de respaldo.

- ✓ **Tiempo de restablecimiento.** Tiempo requerido por el camino de respaldo a ser activado y empezar a transmitir el tráfico después de la falla. Este es el tiempo entre la detección de la falla y el tiempo cuando los paquetes inician el flujo a través del LSP de respaldo.

- ✓ **Tiempo de restablecimiento completo.** Tiempo entre la detección de la falla y el tiempo total del tráfico que fluye por el LSP de respaldo.

- ✓ **Vulnerabilidad.** Tiempo que el LSP de trabajo queda sin protección (es decir, sin respaldo) de la posible falla de algún componente de red. Una vez que el LSP de respaldo hace de LSP primario un nuevo LSP puede ser establecido para protegerlo.

- ✓ **Calidad de protección.** La probabilidad de que una conexión se restablezca ante una falla determina la calidad de protección del esquema de recuperación. El rango de la calidad de protección puede ser extendida desde relativa a absoluta.

3.2.3 Modelo de red (escenario de simulación)

La figura 3.1 presenta el escenario de simulación básico del mecanismo integrado de protección, donde se observan los tres métodos en una red simple MPLS. En este, se evalúan los componentes de protección como son el Tiempo de Restablecimiento, Pérdida de paquetes y Consumo de Recursos en el momento en que ocurra la falla y de acuerdo al método que entre en ejecución para la recuperación del tráfico basado en las políticas de restablecimiento.

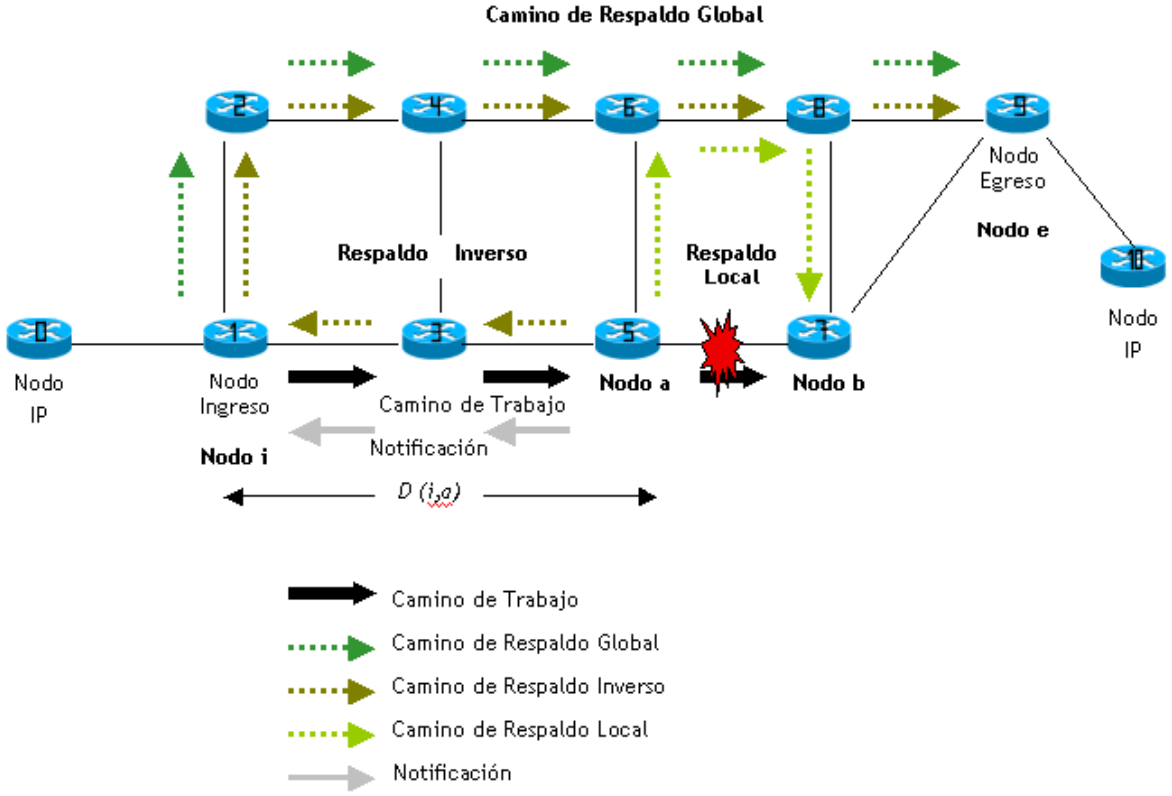


Figura 3.1 Modelo de red integrado.

En la simulación se usará tráfico CBR con un agente UDP generado por el NS-2, permitiendo manejar tráfico multimedia para requerimientos de tiempo real. Además, las fallas sólo se efectuarán en los enlaces de la red, debido a que las redes actuales presentan redundancia en sus nodos y la probabilidad de falla de éstos es mínima. También, es de aclarar que la falla que se presenta en cualquiera de los enlaces es una falla simple, no se tratarán múltiples fallas en los casos de simulación.

Este mecanismo integrado permite que se considere la ejecución de los tres métodos, de acuerdo

a la falla y no limitarse a uno solo en el dominio MPLS como se ha realizado hasta el momento.

3.3. FORMULACIÓN DEL IMPACTO DE FALLA

La calidad de servicio garantizada del tráfico es un aspecto crucial en la evaluación del impacto de falla en el mecanismo integrado. Éste se divide en dos componentes: tiempo de restablecimiento y pérdida de paquetes.

Cada método de protección contra fallas ofrece un tiempo de restablecimiento diferente. La tabla 3.1 muestra la siguiente clasificación [32]:

Requerimientos 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 el establecimiento rápido de los métodos de protección 50 ms es el límite, aunque no se puede descartar trabajar a otros grados de protección. Además, la reducción del tiempo de restablecimiento de falla es uno de los aspectos principales a tomar en cuenta para alcanzar el nivel de protección requerido por muchos de los servicios actuales.

3.3.1 Tiempo de restablecimiento y notificación de falla [32]

El Tiempo de Restablecimiento (RT: Restoration Time) depende de la cadena de eventos involucrados en la recuperación (método de protección, consumo de recursos entre otros). Básicamente son cuatro componentes que afectan el RT. El Tiempo de Detección (DT: Detection Time) de la falla, el Tiempo de Notificación (NT: Notification Time) durante el cual el nodo responsable de hacer las acciones de conmutación es notificado de la falla y el tiempo de recuperación del tráfico desde el camino de trabajo al camino de respaldo y el Tiempo de Switchover (ST: Switchover Time). Si el método de gestión de fallas es dinámico, es decir, que no hay un camino pre-establecido, se adiciona el Tiempo de Re-enrutamiento (RrT: Rerouting Time).

La siguiente formula sintetiza los componentes de *RT*:

$$\mathbf{RT} = DT + NT + RrT + ST \qquad (3.1)$$

Donde:

DT: Tiempo de Detección.

NT: Tiempo de Notificación.
RrT: Tiempo de Re-enrutamiento.
ST: Tiempo de Switchover.

El Tiempo de notificación es considerado el mejor componente ya que este es el responsable de la relación de pérdida de paquetes. Además, NT es directamente afectado por la distancia (*D*), la cual se define como el número de enlaces/nodos entre el nodo donde se identifica la falla y el nodo responsable de hacer las acciones de switchover. En el respaldo local, el nodo que detecta la falla es el responsable del procedimiento del switchover, de esta manera no depende de la distancia. El segundo parámetro es el Retardo del Enlace (LD: Link Delay), o la latencia en la propagación a lo largo de los enlaces, adicionando este al Retardo del procesamiento del Nodo (NPD: Node Processing Delay) y al Retardo del Procesamiento del Buffer (BPD: Buffer Processing Delay) o al tiempo de paquetes que son encolados en los buffers del nodo. La suma del LD, BPD y el NPD es el Tiempo de Propagación (PT: Propagation Time). Para propósitos de comparación de los métodos no se tendrá en cuenta el tiempo en que se detecta falla (DT=0).

Considerando las diferentes estrategias de notificación de acuerdo al método de protección de falla que se aplique dentro del mecanismo integrado, se tiene (ver figura 3.2):

En el método global e inverso esta distancia es igual a D(i,a), dónde el nodo que detecta la falla es el nodo anterior a la falla (nodo a), y el nodo responsable para el switchover es siempre el nodo de ingreso (nodo i).

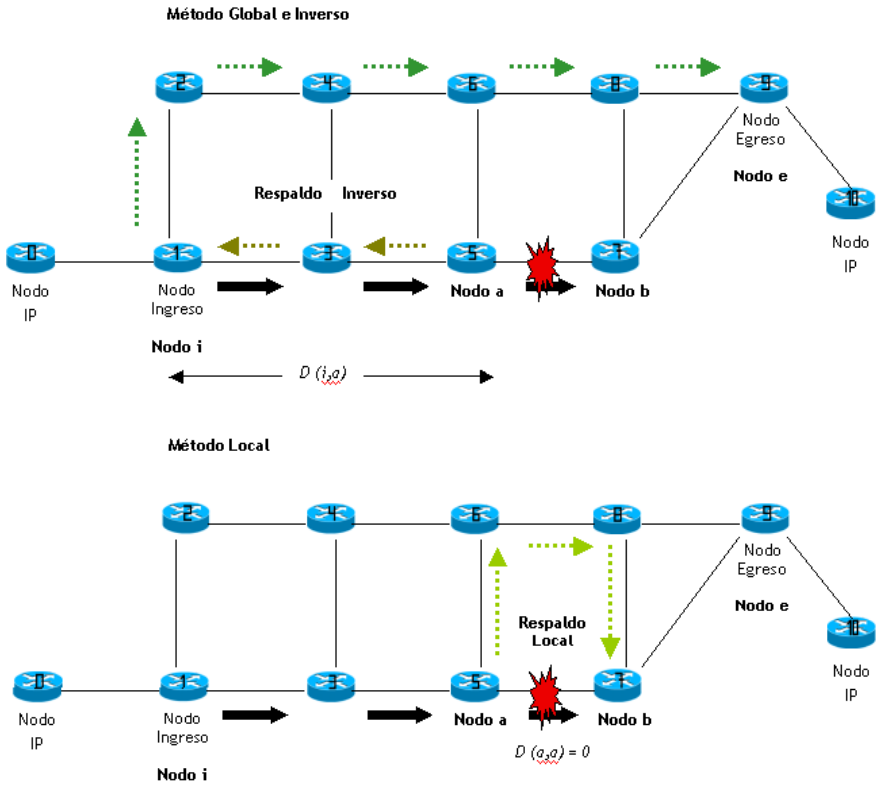


Figura 3.2 Notificación de falla dependiendo del método de protección.

Finalmente, si se usa el respaldo local, la distancia es cero, porque en este caso el nodo que detecta la falla y el nodo responsable del switchover es el mismo nodo (D(a,a)).

Por consiguiente:

$$\mathbf{NT} = D \cdot PT \qquad (3.2)$$

Donde:

D: Distancia de notificación (número de saltos).

PT: Tiempo de propagación de la señal en cada salto.

Esta fórmula es simplemente una aproximación. La distancia y el tiempo requerido a propagar la FIS no es el mismo en cada salto.

3.3.2 Pérdida de Paquetes [32]

La pérdida de paquetes (PL: Packet Loss) depende del Tiempo de Restablecimiento, específicamente de los componentes del Tiempo de Notificación y de Re-enrutamiento (en el caso dinámico) y de la asignación del ancho de banda actual del tráfico en el LSP. El producto de la distancia y la tasa proporcionan un límite superior para la pérdida de paquetes.

$$PL = RT \cdot RB + LP \qquad (3.3)$$

Donde:

RT: Tiempo de Restablecimiento.

RB: Ancho de Banda Reservado (bits/s).

LP: Pérdida de paquetes en el enlace.

3.3.3. Componentes para reducir el tiempo de restablecimiento

La tabla 3.2 presenta los principales aspectos para reducir el tiempo de restablecimiento en cada fase de recuperación de la falla.

Fase de Recuperación	Características	Reducción del Tiempo
Tiempo de Detección (DT)	Depende de la falla.	No se puede reducir.
Tiempo de Notificación (NT)	Depende de la falla, el retardo de notificación y el método de notificación.	Minimizando la falla, distancia de la notificación y optimización del proceso.
Creación del nuevo respaldo	Depende del enrutamiento y el método de señalización aplicado.	Pre-establecimiento del respaldo.

Fase de Recuperación	Características	Reducción del Tiempo
Activación del respaldo	Depende de la distancia del respaldo y el proceso de señalización.	Minimizando la distancia del respaldo y optimizando el proceso.
Tiempo de Switchover (ST)	Depende de la tecnología del nodo.	No puede ser reducido.
Tiempo de recuperación completo	Depende de la distancia de respaldo.	Minimizando la distancia de respaldo.

Tabla 3.2 Ciclo de recuperación y reducción del impacto de falla.

En los escenarios de red con cargas de tráfico altas y ninguna técnica de priorización de paquetes, la no reservación de ancho de banda podría producir un tiempo de notificación grande [32].

Cuando el nivel de protección, en términos de tiempo de restablecimiento, tiene que ser rápido o muy rápido, los caminos de respaldo pre-establecidos y pre-asignados deben usarse. En estos casos la reducción del tiempo de notificación, activación del respaldo, y recuperación completa son probablemente los aspectos más desafiantes a la hora de diseñar los métodos de protección para una red.

Para minimizar estos tiempos, los procesos de notificación de falla y activación del respaldo son cruciales. En este trabajo, el proceso basado en señalización se tiene en cuenta para perfeccionar estas fases.

En el escenario del mecanismo integrado, tanto la pérdida de paquetes como el tiempo de restablecimiento dependen de la distancia D(i,a), donde:

$$PL = D(i,a) \cdot RB \cdot PT\_FIS \qquad (3.4)$$

$$RT = D(i,a) \cdot PT\_FIS \qquad (3.5)$$

3.4 CONSUMO DE RECURSOS EN LOS CAMINOS DE RESPALDO [32]

El Consumo de Recursos (RC: Resource Consumption) en los métodos de protección se evalúa dependiendo del método de recuperación usado. Por simplicidad, se usa la asignación de ancho de banda como la métrica a tener en cuenta. El RC se puede evaluar en un par básico de enlaces, calculando el número de enlaces en el camino y el ancho de banda asignado en cada enlace.

$$RC = NL \cdot RB \qquad (3.6)$$

Donde:

RB : Ancho de Banda Reservado (bits/s).

NL : Número de Enlaces

La formula 3.6 tiene que ser adaptada a los diferentes métodos de camino de respaldo, descritos en el capítulo 2. El consumo de recursos para el método global (RC_G) depende del número de enlaces en el camino de respaldo (NL_G.) El consumo de recursos para el método de protección inverso (RC_R) es la suma del RC_G más los recursos requeridos por el camino inverso ($NL_R \cdot RB$). El consumo de recursos para el método de protección local (RC_L) depende del ancho de banda reservado y el número de enlaces (NL_L). En el caso del respaldo local, debe notarse que se puede crear más de un respaldo para proteger varios enlaces en el camino de trabajo. Por lo tanto, el RC para los diferentes métodos se evalúa por:

$$RC_G = NL_G \cdot RB \qquad (3.7)$$

$$RC_R = RC_G + NL_R \cdot RB \qquad (3.8)$$

$$RC_L = NL_L \cdot RB \qquad (3.9)$$

Donde:

RC_G, RC_R, RC_L Consumo de Recursos (Global, Inverso y Local respectivamente).

NL_G, NL_R, NL_L Número de enlaces (Global, Inverso y Local respectivamente).

Al seleccionar los métodos de protección con asignación de ancho de banda implica una combinación de los diferentes métodos (local, global o inverso) para lograr el nivel de protección requerido con un balance en el costo de consumo de recursos.

La formulación matemática de los principales componentes de protección y restricción para el mecanismo integrado, será analizada y justificada con las diferentes simulaciones y casos de estudio; se hará un análisis de los parámetros de protección (pérdida de paquetes y tiempo de restablecimiento) y consumo de recursos en cada método, realizando una comparación entre ellos. Luego se realiza un análisis de los parámetros y su influencia con respecto a los métodos de protección de la red. Finalmente, se tendrá el mecanismo integrado de protección teniendo en cuenta la relación entre las diferentes clases de tráfico y métodos de protección y así poder determinar qué método de recuperación debe entrar a funcionar cuando ocurra la falla en el dominio MPLS, de acuerdo a las políticas establecidas por los Administradores de red. Para proporcionar esta formulación, se implementarán diferentes simulaciones usando el ns-2 MNS2.0 (Modulo MPLS) para ns2.28. Este modulo será modificado para realizar ciertas funciones, como proveer tráfico (Tasa de Bits Variable) en escenarios de diferente carga de red.

4. HERRAMIENTA DE SIMULACIÓN DE REDES MPLS

Actualmente la simulación de redes, se ha convertido en una herramienta indispensable para la solución de muchos problemas del mundo real, tanto en entornos de investigación como en entornos educativos. Estas simulaciones son usadas para describir y analizar el comportamiento de una red, es decir, dar respuestas a preguntas como "qué sucedería si...”; relacionadas con un sistema real, y de esta manera ayudar en el diseño (modelamiento) de las redes.

Como se planteó en el anterior capítulo de esta monografía, el propósito primordial del trabajo es el simular una red MPLS de prueba para así poder descubrir y constatar con datos, las ventajas de los métodos de protección contra fallas utilizados en las redes MPLS. Para este propósito, se debe contar con una herramienta de simulación que sea confiable, y produzca los datos necesarios para poder observar claramente las ventajas de cada uno de los métodos de protección en el desarrollo del mecanismo integrado contra fallas.

Este capítulo describe la herramienta software de simulación seleccionada, la justificación de su elección, funcionamiento y se especifica la interpretación que hace de redes MPLS, además de sus ventajas frente a otras.

4.1 JUSTIFICACIÓN

La selección del software para las simulaciones se realizó mediante la búsqueda en línea de las principales herramientas existentes, y sobre todo en el constatar que se trata de un sistema que ha sido y sigue siendo muy utilizado en el entorno mundial, debido a que se ha comprobado que es efectivo y no tan complicado de utilizar, teniendo claro, las bases necesarias.

Siguiendo estas disposiciones, se realizaron diferentes pruebas entre el Simulador de Redes de la Universidad Nacional Chiao Tung (NCTUns 2.0: National Chiao Tung University Network Simulator) y el Simulador de Redes (NS-2: Network Simulator), para determinar cual de ellos es el más idóneo para este caso de estudio. De esta manera, se decidió utilizar el *Network Simulator* con su módulo MPLS (MNS), que es un simulador de eventos discretos (procesamiento de una trayectoria de eventos de entrada predecibles, que dependiendo de ésta y sus propias condiciones iniciales, produce una trayectoria de eventos de salida), y que se enfoca totalmente hacia la investigación y análisis del comportamiento de las redes. Este programa fue desarrollado en la Universidad de California con sede en Berkeley (UC at B). Inicialmente fue desarrollado para simular redes IP, pero con el constante surgimiento de nuevas tecnologías, también ha ido evolucionando para soportar las nuevas tecnologías de IP sobre ATM y actualmente un módulo que soporta la simulación de MPLS.

Cabe destacar que para la realización de este estudio y debido a la limitación de recurso existente,

el programa utilizado cumple los requisitos de software gratuito y exento de patentes.

4.2 SIMULADOR DE REDES DE LA UNIVERSIDAD NACIONAL CHIAO TUNG (NCTUns 2.0)

La tecnología de SimReal (la simulación parece real), actualmente cuenta con un simulador/emulador de redes útil y potente, conocido como NCTUns 2.0. Con cinco años de desarrollos, NCTUns 2.0 es ahora una herramienta profesional que compite con el software comercial. Además, con su novedosa metodología de simulación de reingreso al kernel, ofrece ventajas únicas que no pueden lograrse fácilmente con los simuladores y emuladores de las redes tradicionales. NCTUns 2.0 es una valiosa herramienta de planeación e investigación de la red, que cuenta con las siguientes capacidades y característica [33]:

- ✓ **Precisión en los resultados de simulación.** NCTUns usa directamente la pila de protocolos de tiempo real TCP/IP de Linux para generar resultados con alta fidelidad.

- ✓ **Reutilización y extensibilidad de los programas de aplicación.** Todos los programas de aplicación de UNIX existentes o a ser desarrollados, pueden correr sobre una red simulada para generar tráfico real (configuración y monitoreo). La reutilización usada directamente en otras simulaciones, permite ahorrar considerables costos de desarrollo.

- ✓ **Soporte de emulación.** NCTUns puede convertirse en un emulador fácilmente. Por ejemplo, en una emulación, los nodos de la red simulada pueden intercambiar paquetes con dispositivos reales, probando el funcionamiento y desempeño de estos bajo diferentes condiciones de red.

- ✓ **Alta velocidad de simulación.** NCTUns combina la metodología de reingreso al kernel con la simulación de eventos discretos, permitiendo ejecutar simulaciones rápidamente.

- ✓ **Soporte para varias redes.** Puede simular redes alambradas, inalámbricas, celulares (GPRS) y redes ópticas.

- ✓ **Soporte para diferentes dispositivos de red.** NCTUns puede simular varios dispositivos como hubs, switches, routers, hosts, puntos de acceso inalámbricos, interfaces IEEE 802.11 (b), fibras ópticas, anillos de protección, etc.

- ✓ **Soporta diversos protocolos de red.** NCTUns puede simular diversos protocolos como IEEE 802.3, IEEE 802.(b), IP móvil, RIP, OSPF, UDP, TCP, HTTP, FTP, Telnet, DiffServ, etc.

- ✓ **Interfaz amigable.** NCTUns proporciona un entorno integrado y profesional en el que los usuarios pueden realizar fácilmente sus simulaciones de red.

- ✓ **Arquitectura de sistema abierto.** Usa un conjunto de módulos de APIs, que son proporcionados por la máquina de simulación, permitiendo integrar nuevos módulos a ésta.

- ✓ **Arquitectura distribuida.** Usando esta arquitectura, cada componente de NCTUns puede correr sobre una máquina independiente.

4.3 NETWORK SIMULATOR (NS)

NS es un simulador de eventos centrado en la investigación sobre redes. NS dispone simulación para TCP, enrutamiento y multicast sobre redes cableadas o inalámbricas (locales y por satélite).

NS empieza como una variante del Simulador de Redes Extenso y Real (REAL: REalistic And Large) en 1989 y ha evolucionado substancialmente durante los últimos años. En 1995 el desarrollo lo llevaba acabo la Agencia de Proyectos de Investigación para Defensa Avanzada (DARPA) a través del proyecto VINT de LBL, Xerox PARC, UC at Berkeley y USC/ISI. Actualmente el desarrollo de NS lo lleva DARPA junto a SAMAN y otros. NS siempre ha contado con contribuciones de muchos otros desarrolladores, incluyendo código inalámbrico de los proyectos CMU Monach y UCB Daedelus y también de Sun Microsystems [34].

NS se está utilizando tanto en entornos de investigación como en entornos educativos. NS es útil para la investigación ya que permite acceder a simulaciones con elementos a los que no se podrían acceder normalmente en caso de no disponer de un simulador. También permite modificar casi todos los parámetros que influyen en el estado o configuración de una red en tan solo unos segundos mientras que recrear en la realidad este entorno podría tardar días o incluso meses. Además, NS se utiliza en entornos educativos ya que permite simular sencillas redes que van a ayudar a comprender los distintos protocolos, enrutamiento y observar como se produce el envió de paquetes entre nodos, etc.

Para definir una simulación en NS se utiliza un lenguaje de script llamado Tcl, el cual permite definir los distintos elementos de la red y como deben comportarse. Una vez terminado el script se pasa al NS y este irá realizando la simulación.

NS dispone de una interfaz gráfica para visualizar las simulaciones llamado Animador de Red (NAM: Network Animator). NAM también dispone de un editor gráfico, que permite no tener que usar código Tcl para crear las animaciones. Se puede crear la topología de red y simular varios protocolos y fuentes de tráfico mediante el uso del ratón.

NS implementa protocolos de red tales como TCP y UDP; comportamiento de fuentes de tráfico como FTP, Telnet, Web, CBR y VBR; mecanismos de manejo de colas en enrutadores como *Drop tail,* RED y CBQ; algoritmos de enrutamiento como Dijkstra, y más. NS también implementa protocolos de *multicasting* y algunos de los protocolos de la capa MAC para simular LAN's.

Como se observa en la figura 4.1, NS es un intérprete de scripts del lenguaje Tcl Orientado a Objetos, el cual tiene un planificador de eventos de simulación, librerías de objetos de componentes de red y librerías de módulos de instalación de red *(plumbing).* En otras palabras, para usar NS, se programa en lenguaje de scripts OTcl. Para establecer y correr una simulación de red, el usuario debe escribir un script OTcl que inicialice el planificador de eventos, que establezca la topología de la red usando los objetos de red y las funciones de las librerías, y diga a las fuentes de tráfico cuando empezar y dejar de transmitir paquetes a través del planificador de eventos.

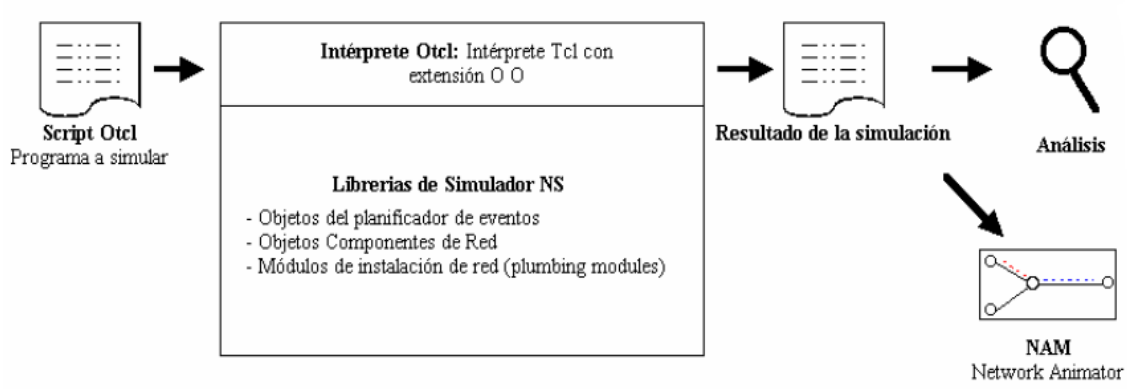


Figura 4.1 Esquema de simulación en NS [35].

El término *"plumbing"* (explorar) se usa para establecer las características de la red, ya que establecer una red, es explorar las posibles trayectorias entre objetos de la red, direccionando correctamente el apuntador de un objeto vecino a otro. Cuando el usuario quiere crear un nuevo objeto de red, lo puede hacer escribiendo un nuevo objeto o creando un objeto compuesto de las librerías existentes y explorando la trayectoria de datos a través del dato. Esto puede sonar como un trabajo complicado, pero en realidad los módulos *plumbing* del OTcl hacen que el trabajo sea muy sencillo. El poder del NS viene de esta función [35].

Un importante componente del NS a parte de los objetos de red, es el Planificador de Eventos o *event scheduler*. En NS, un evento es el Identificador (ID) que es único para cada paquete cuyo tiempo y apuntador están programados a un objeto que maneja el evento. Un planificador de evento mantiene la pista del tiempo de simulación y dispara todos los eventos programados en sus respectivos momentos al invocar los componentes de red apropiados, y los deja realizar la acción asociada con el paquete apuntado por el evento. Los componentes de la red se comunican entre si al pasarse los paquetes; sin embargo, esto no consume tiempo de simulación real. Todos los componentes de red que necesitan gastar cierto tiempo de simulación manipulando un paquete (por ejemplo un retardo), usan el planificador de eventos; esto, atribuyendo un evento al paquete, y esperando a que el evento sea disparado por sí mismo, antes de hacer cualquier acción de manipulación del paquete. Por ejemplo, un componente de conmutación de red que simula un conmutador con 20 microsegundos de retraso en la conmutación, produce un evento en el cual el paquete será conmutado 20 microsegundos después. El planificador, después de 20 microsegundos, saca de la cola al evento y lo dispara hacia el componente de conmutación, el cual a su vez pasa el paquete hacia el componente de salida apropiado.

Otra aplicación para el planificador de eventos es el del *timer*. Por ejemplo, TCP necesita un *timer* para mantener el control del tiempo de transmisión de un paquete para su retransmisión (transmisión de un paquete con el mismo número del paquete TCP, pero con diferente ID de paquete para NS).

NS está escrito, no sólo en OTcl, sino también en C++. Por razones de eficiencia, NS separa la

implementación de trayectoria de datos de las implementaciones de las trayectorias de control. Para reducir el tiempo de proceso de paquetes y eventos (no el tiempo de simulación), el planificador de eventos y los objetos de componentes básicos de red en la trayectoria de datos, están escritos y compilados en C++. Estos objetos compilados están disponibles al intérprete OTcl a través de un acoplamiento OTcl, el cual crea un objeto OTcl compatible para cada uno de los objetos C++, y hace que las funciones de control y las variables configurables (especificadas por el objeto C++) actúen como funciones y variables asociadas del correspondiente objeto OTcl. De esta misma manera, los controles del objeto C++, se dan a OTcl. También es posible agregar funciones y variables asocidas al objeto OTcl enlazado con C++. Los objetos C++ que no necesitan ser controlados en una simulación o internamente ser utilizados por otro objeto, no necesitan ser enlazados a OTcl. Asimismo, un objeto (que no esta en la trayectoria de datos) puede ser totalmente implementado en OTcl. La figura 4.2, muestra el ejemplo de la jerarquía en un objeto, en C++ y OTcl, donde cada objeto C++ tiene un enlace OTcl (formando una jerarquía), existe una jerarquía de objeto OTcl correspondiente y muy similar.

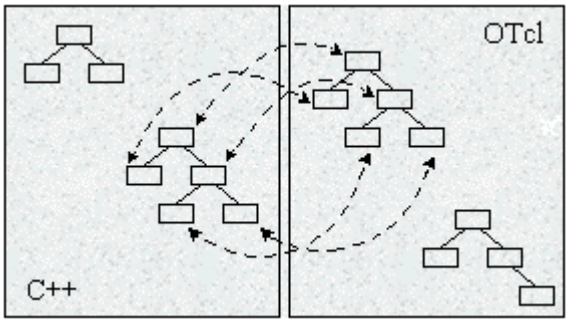


Figura 4.2 La dualidad: C++ y OTcl [35].

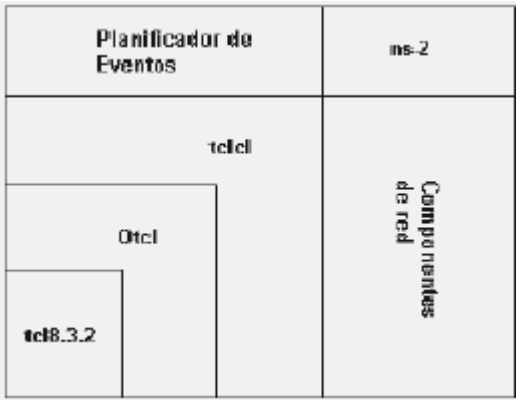


Figura 4.3 Arquitectura de NS [35].

La figura 4.3 muestra la arquitectura general del NS. En esta figura, un usuario general (no un desarrollador) se puede considerar colocando en la esquina inferior izquierda, diseñando y corriendo las simulaciones en Tcl, usando objetos del simulador existentes en las librerías OTcl.

Los planificadores de eventos y la mayoría de los componentes de red están implementados en C++, y a su vez, están disponibles para OTcl, a través de un enlace OTcl que es implementado usando TclCL (paquete conocido como lib TCl). Todos estos elementos en conjunto forman el Network Simulator, el cual es un intérprete Tcl orientado a objetos con librerías de simulación de redes.

4.4 REQUERIMIENTOS DE INSTALACIÓN

Network Simulator es una herramienta creada por usuarios del sistema Unix, y está escrito en C++, por lo que su principal forma de distribución (gratuita) es a través de su código fuente, el cual debe ser descargado de la página: http://www.isi.edu/nsnam/ns/ns-build.html.

De esta página se puede descargar la versión más actualizada con la que se cuente, actualmente se encuentra disponible la versión *NS 2.28.* Para el correcto funcionamiento del NS, es necesario tener también instalados los siguientes paquetes en sus versiones actuales:

- ✓ Tcl-8.4.5
- ✓ Tk-8.4.5
- ✓ otcl-1.10
- ✓ TclCL-1.17
- ✓ ns-2.28

Todos estos componentes deben ser compilados e instalados independientemente, por lo que es necesario contar con un sistema Unix (Linux o cualquier equivalente), o un sistema Windows con la paquetería de Microsoft Visual C++ 5.0 (0 mayor). Otra forma de instalarlo en un PC, es a través de un programa de emulación de Linux, este programa llamado *Cygwin* contiene los paquetes y herramientas de compilación necesarios para la instalación del NS. Sin embargo, estos modos de instalación, tienen un sin número de inconvenientes al momento de la compilación, debido a que la versión de cada paquete debe tener una correspondencia con la versión del compilador y la del sistema en que se este trabajando. Para mayor información sobre descarga e instalación del *Network Simulator*, revisar bibliografías [34] y [36].

La página de distribución del código NS, también incluye la opción de descargar archivos binarios precompilados de NS. La opción de descargar estas versiones, resulta lo más adecuado para el caso de este trabajo de tesis, ya que son archivos ejecutables y no necesitan de procesos anteriores a su utilización. Todas las simulaciones que se realizan en este trabajo se realizan con la versión de ns-2.28. una guía sencilla para la descarga y utilización de estos archivos se incluye en el Anexo.

Para lo que respecta a la visualización de resultados también es necesario descargar el NAM, el cual es una herramienta de interfaz muy sencilla de utilizar. Al igual que NS, NAM se puede descargar en sus diferentes versiones precompiladas de la misma forma. Para este caso de estudio, se trabaja con la versión 1.11 del NAM.

4.5 DISEÑO E IMPLEMENTACIÓN DE MPLS EN EL NETWORK SIMULATOR (MNS) [37]

El MPLS Network Simulator (MNS) fue implementado como una extensión del NS por Gaeil Ahn, y está incluido en el simulador a partir de la versión 2.1b5 [38]. El principal propósito del MNS es simular varias aplicaciones sin construir una red MPLS real. El MNS esta diseñado bajo las siguientes consideraciones [39]:

1. **Extensibilidad**: sigue fielmente el concepto orientado a objeto, de esta manera podrá soportar varias aplicaciones de MPLS.

2. **Usabilidad**: el diseño permite a los usuarios que puedan fácilmente aprender y manejar el simulador.

3. **Portabilidad**: minimiza la modificación del código de NS, de manera que no se subordine para una versión específica.

4. **Reusabilidad**: diseño para soportar el desarrollo de una conmutación de LSR real.

El alcance de la implementación del MNS está definido por los siguientes puntos:

- ✓ Conmutación de paquetes en MPLS: operación de intercambio por etiquetas, decremento TTL y obtención del penúltimo salto.
- ✓ LDP: manejo de mensajes LDP (Petición, Mapeo, Extracción, Liberación y Notificación).
- ✓ CR-LDP: manejo de mensajes CR-LDP (Petición y Mapeo).

La capacidad del MNS relacionada al establecimiento de LSPs es la siguiente:

- ✓ En cuanto a la Estrategia de Disparo de un LSP: soporta ambos, disparo manejado por datos y manejado por control.
- ✓ En Asignación de Etiquetas y Esquema de Distribución: soporta solo un esquema descendente para disparo manejado por control, y los dos esquemas (ascendente y descendente) para disparo manejado por datos.
- ✓ En el Modo de Control para la Distribución de Etiquetas: soporta solo modo independiente en disparo manejado por control, y tanto modo independiente como modo ordenado en disparo manejado por datos.
- ✓ En Modo de Retención de Etiquetas: soporta solo modo conservativo.
- ✓ ER-LSP basado en CR-LDP: establecido, y se basa en la información del camino predefinido por el usuario (enrutamiento explícito).
- ✓ CR-LSP basado en CR-LDP: establecido, y se basa en los parámetros como rango de tráfico, tamaño de buffer (enrutamiento dependiente).

- ✓ En Priorización de recursos (resource preemption): priorizar el recurso del CR- LSP existe con prioridad establecida (setup-priority) o prioridad restringida (holding-priority).
- ✓ Agregación de flujo: agrega buenos flujos a flujos más ordinarios.

4.5.1 Arquitectura del nodo MPLS

MNS es la extensión del NS, que es un simulador basado en IP. En NS, un nodo esta constituido por agentes y clasificadores. Un agente es el objeto transmisor/receptor del protocolo, y un clasificador es el objeto que es responsable de la clasificación del paquete requerida para el envío de paquetes al siguiente nodo. Para crear un nuevo nodo MPLS de un nodo IP, se insertan un 'Clasificador MPLS' y un 'Agente LDP' dentro del nodo IP.

La figura 4.4 muestra la arquitectura de un nodo MPLS dentro de MNS. 'Nodo de Entrada' retorna un punto de entrada al nodo. Este es el primer elemento que maneja paquetes que llegan al nodo. La variable de instancia de nodo 'entry_', almacena la referencia para este elemento. Ya que en principio no se soporta el *multicasting*, la variable debe ser referida al 'Clasificador MPLS', el cual debe primero clasificar al paquete entrante en etiquetado o no etiquetado. Si se trata de un paquete no etiquetado, éste se trata en la manera convencional. Para un paquete etiquetado, el clasificador MPLS es responsable del intercambio de etiquetas y de la conmutación de paquetes. La variable de instancia 'classifier_' almacena la referencia hacia otro nodo o hacia el 'Clasificador de dirección'. Este elemento se encarga del envío de paquetes basado en la dirección IP de destino, el 'Clasificador de Puerto' es responsable de la selección de agentes.

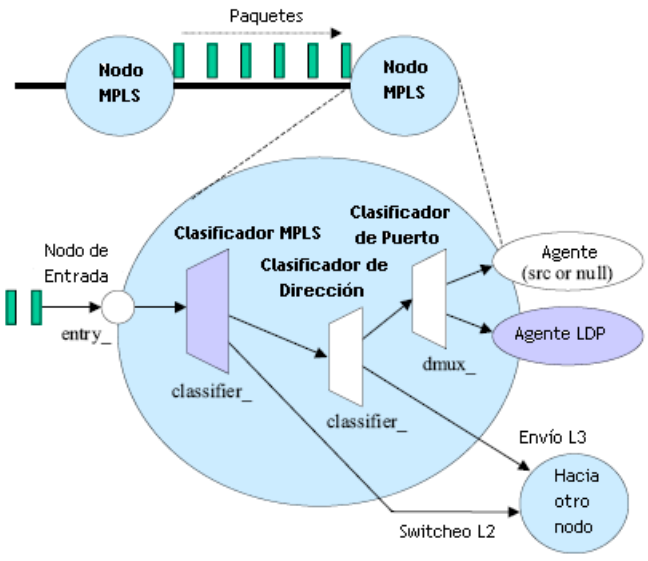


Figura 4.4 Arquitectura del nodo MPLS [37].

Cuando se recibe un paquete, un nodo MPLS opera de la siguiente manera:

1. El 'Clasificador MPLS' determina si el paquete recibido tiene o no etiqueta. En el caso

de un paquete etiquetado, el 'Clasificador MPLS' ejecuta la conmutación de capa 2 (L2) que lo envía directamente al siguiente nodo, después de haber efectuado el intercambio de etiquetas. Si se trata de un paquete que no tiene etiqueta, pero se tiene preparado un LSP para el paquete, el clasificador ejecuta la conmutación como si fuera un envío de paquetes etiquetados. De otra forma, el paquete se envía al 'Clasificador de dirección'.

2. El 'Clasificador de dirección' ejecuta el envío de paquetes (L3) una vez examinada la dirección destino del paquete.

3. Si el siguiente salto del paquete es él mismo, el paquete se envía al 'Clasificador de Puerto'.

Un nodo MPLS cuenta con tres tablas para manejar la información relacionada al LSP:

- ✓ Tabla de Envío Parcial (PFT: Partial Forwarding Table): es una parte de la tabla de envío, y se usa para mapear un paquete IP dentro de un LSP. Consta de la FEC, PHB (Per-Hop-Behavior) y un apuntador LIBptr.

- ✓ Base de Información de Etiquetas (LIB: Label Information Base): contiene información para el LSP establecido, y se usa para conmutar los paquetes etiquetados. Consta de las etiquetas de entrada y salida, y de las interfaces de entrada y salida.

- ✓ Base de Información de Enrutamiento Explícito (ERB: Explicit Routing information Base): contiene información sobre el camino predefinido por el usuario. Consiste de un LSPID, FEC y también cuenta con un apuntador LIBptr.

La figura 4.5 muestra la estructura de estas tablas, así como el algoritmo simple que se usa para el envío de paquetes.

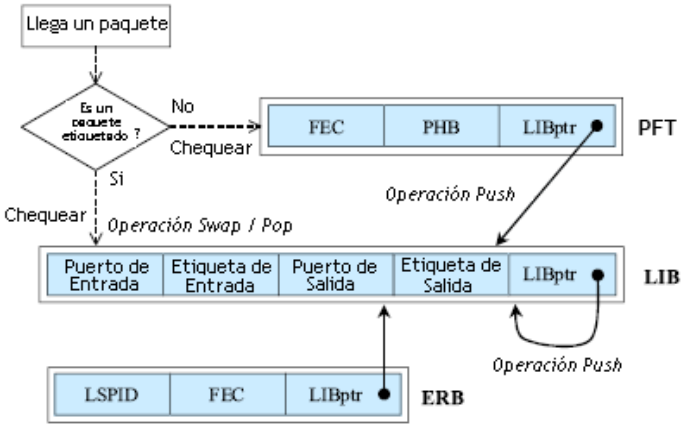


Figura 4.5 Algoritmo para el envío de paquetes [37].

Cuando un nodo MPLS recibe un paquete (etiquetado o no etiquetado), se ejecuta la revisión de

las tablas PFT/LIB. En el caso de un paquete no etiquetado, el nodo MPLS busca en la tabla PFT por una entrada (que es como una fila dentro de una tabla) que contenga la FEC del paquete (o sea, la dirección de destino del paquete). Si el apuntador LIBptr de la entrada encontrada indica NULL, entonces el nodo ejecuta el envío del paquete, usando el esquema de envío de capa 3 (L3). De otra forma, el nodo ejecuta una operación de *push* de etiqueta para el paquete. Esto significa que agrega al paquete la etiqueta de salida de la entrada en la LIB a la que apunta el LIBptr de la entrada PFT. Después habrá un ciclo en el que se repetirá el proceso de *push* de etiqueta (ó sea una operación de pila de etiqueta), hasta que el LIBptr de la tabla LIB indique NULL. Después de que se termina la operación de agregar la etiqueta, el paquete se envía directamente al siguiente nodo indicado por la interfaz de salida de la entrada LIB.

En el caso de un paquete etiquetado, el nodo MPLS fácilmente reconoce la entrada LIB correspondiente, usando la etiqueta que tiene insertada como un índice de la tabla LIB. Entonces, el nodo ejecuta la operación de intercambio (*swap*) de etiquetas que reemplaza la etiqueta del paquete con la etiqueta de salida que marca la tabla. Si la etiqueta de salida es una etiqueta NULL, lo que quiere decir que el nodo es el penúltimo salto dentro de la trayectoria, el nodo MPLS realiza una operación de *pop* de etiqueta (remover la etiqueta), en vez de la operación de intercambio. Después el nodo ejecuta la misma operación de pila para el paquete, hasta que el LIBptr de la LIB sea NULL. Finalmente, el paquete es enviado directamente al siguiente nodo, indicado por la interfaz de salida de la entrada LIB.

La tabla ERB se usa para mantener solamente la información sobre el ER-LSP. Así que no participa directamente en el proceso de envío del paquete. Si se necesita para mapear un flujo dentro de un ER-LSP previamente establecido, se insertará una nueva entrada dentro de la tabla PFT, que tenga el mismo LIBptr que tiene la entrada ERB.

4.5.2 APIs (Application Programming Interface) para LDP y CR-LDP

Cuando un agente LDP recibe un mensaje LDP, debe manejar este mensaje, seleccionar el siguiente nodo, crear un nuevo mensaje LDP, y enviarlo a un agente vinculado al siguiente nodo. Una secuencia de la invocación API para esto se observa la figura 4.6.

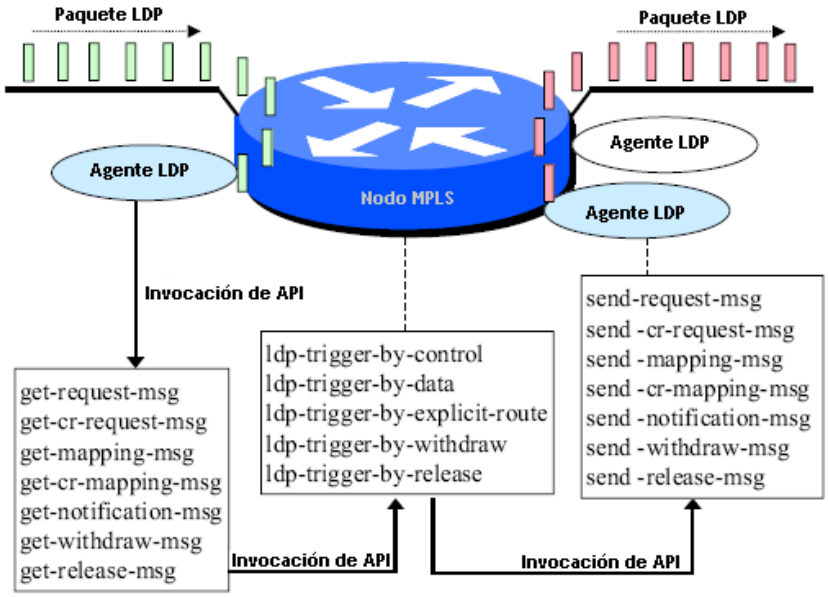


Figura 4.6 Invocación de APIs para la creación de una red MPLS manejando LDP [37].

Cuando un agente LDP recibe un mensaje LDP, su API *get-*-msg* es requerida. Después de manejar este mensaje, el agente LDP llama a la API *ldp-trigger-by-**, que pertenece al nodo MPLS, de manera que éste seleccione el siguiente nodo que recibirá un mensaje LDP. Una vez que se ha determinado el siguiente nodo, el nodo MPLS llama a una API *send-*-msg* de su agente, correspondiente a un agente del siguiente nodo, para así crear un nuevo mensaje LDP y enviarlo al siguiente nodo.

Es así, como NS, es una herramienta muy potente dentro del campo de la simulación de redes. Es a la vez muy flexible dada la posibilidad de trabajar con scripts Otcl, los cuales permiten agregar toda la potencia de un lenguaje de programación a los propios elementos de la simulación. Además dispone de un entorno gráfico que simplifica el trabajo del diseño de la simulación al tiempo que da la posibilidad de observar los resultados de la simulación de una forma gráfica fácilmente comprensible.

Todo ello hace de NS una ayuda inestimable en el campo de la investigación y del aprendizaje de redes, y particularmente en el caso de estudio de los métodos y el desarrollo del mecanismo integrado de protección contra fallas en redes MPLS; permitiendo comparar los resultados teóricos mediante la simulación del modelo de red, de manera más real.

5. PRUEBAS Y RESULTADOS

Este capítulo presenta los resultados de varias pruebas analíticas y experimentales llevadas a cabo para verificar el desempeño de los métodos de protección y el mecanismo integrado propuesto en este trabajo. El capítulo esta organizado en secciones para cada uno de los dos conjuntos de prueba. El primer conjunto de experimentos contiene los tres casos de estudio de los métodos de protección global, local e inverso, los cuales se llevaron a cabo en una topología de malla simple que evalúa la conducta de algunos parámetros de red, que afectan el tiempo de restablecimiento de falla y, por consiguiente, la pérdida de paquetes. Este conjunto de experimentos es realizado usando el simulador NS-2.

El segundo conjunto de experimentos es para el mecanismo integrado de protección (descrito en el capítulo 3), el cual es implementado y ejecutado en el mismo escenario de red (con diferentes distancias, de acuerdo a las políticas de restablecimiento). Varios resultados analíticos se explican, mientras se indica cual de los métodos de respaldo es el más conveniente para lograr el nivel de protección requerido. Sin embargo, el mecanismo integrado de respaldo involucra un proceso costoso (en términos de tiempo de cálculo). Por otro lado, algunos parámetros, para cada una de las clases de tráfico, tienen que ser sincronizados para lograr resultados más exactos.

Este conjunto de experimentos se llevó a cabo en ambientes estáticos, donde se consideran LSPs de larga vida (los LSPs no se anulan durante el experimento). También se compararon los métodos respecto al impacto de falla (en términos de tiempo de restablecimiento y pérdida de paquetes), el consumo de recursos, las diferentes notificaciones de falla y la activación del método de respaldo adecuado dependiendo de donde ocurra la falla (distancia).

5.1 CONDICIONES DE SIMULACIÓN

Para tener una correcta interpretación de los resultados obtenidos, hay que tener en cuenta que NS puede generar tres tipos de archivos de salida: un archivo de trazo (*trace file*), un archivo NAM (*nam file*), y archivos de datos generados por el usuario. El archivo trace file (*.tr) contiene la información referente a los paquetes que viajan por la red en el tiempo que transcurre la simulación. En el nam file (*.nam) se escribe la información que se podrá interpretar para la visualización del modelo de red generado. El tercer tipo de archivo lo genera el usuario y su implementación depende de las necesidades que este tenga.

Para la visualización de los archivos simulados se utiliza el NAM en su versión 1.11. El NAM es una herramienta de animación basada en tcl/tk para la visualización de redes; también hace parte del proyecto VINT que desarrolló el NS. Su funcionamiento es sencillo y muy gráfico. Como se

había mencionado en el capítulo anterior, el NAM se puede descargar, en su versión binaria, de la misma página de descarga del NS.

La figura 5.1 muestra una ventana del NAM y la función de cada elemento de la interfaz gráfica.

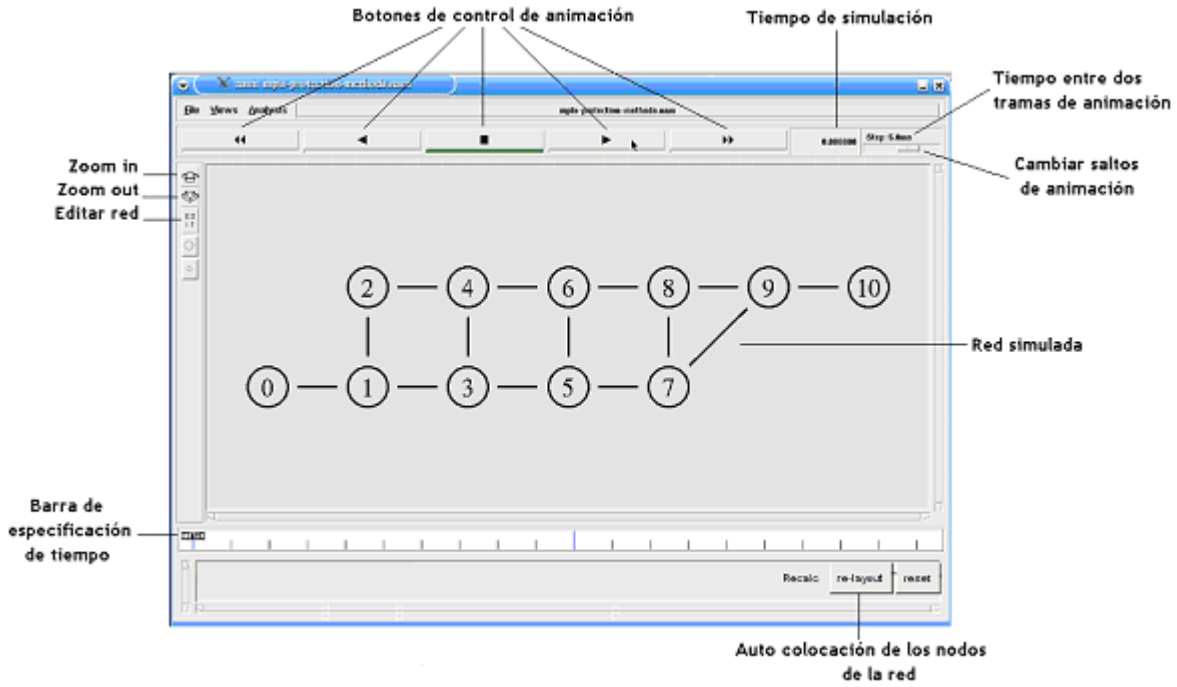


Figura 5.1 Interfaz gráfica del NAM y sus funciones.

5.2 REQUERIMIENTOS DE COMPARACIÓN

A continuación se plantean diferentes casos de estudio (global, inverso, local e integrado), cada uno con la misma topología; cada ejemplo esta compuesto por nodos IP (entrada y salida) y nodos MPLS (LSRs). Para realizar la comparación entre dichos escenarios, se plantean los siguientes puntos:

- ✓ Todos los escenarios de red deben tener la misma topología (número y posición de nodos).
- ✓ Los enlaces correspondientes entre nodos, serán de la misma capacidad.
- ✓ En todos los casos de estudio, sobre la red utilizada para llevar a cabo las respectivas pruebas y con el fin de demostrar la funcionalidad tanto de los métodos de protección como del mecanismo integrado, se establecen dos tipos de flujo de tráfico (fuentes), uno tipo de Tasa de Bit Constante (CBR: Constant Bit Rate) y otro tipo de Tasa de Bit Variable

(VBR: Variable Bit Rate), a través de UDP (User Datagram Protocol). El primero permite simular el tráfico al cual se le ofrece QoS, a través de los diferentes métodos de protección de MPLS; mientras que el segundo proporciona un tráfico de fondo que permite simular un escenario más cercano a la realidad, y dependiendo de la variación de la tasa de tráfico es posible simular diferentes cargas sobre la red. Las tablas 5.1, 5.2 y 5.3 muestran una lista detallada de los parámetros usados en la red y en cada uno de estos tipos de flujo de tráfico.

Parámetros de Red
BW del enlace: 2Mb/seg
Retardo en el enlace: variable {1,2,3,…,20 mseg}
Tipo de cola en los LSR: DropTail
Carga de la red: variable { 0, 10, … , 50% }
Distancia D(i,a): variable { 0,1,2,3,4 saltos }

Tabla 5.1 Parámetros de red.

Fuente de Tráfico: Constant Bit Rate (UDP)
Velocidad: variable { 0.25Mb/seg,…,0.5Mb/seg }
Intervalo entre paquetes: 10 mseg (1000 paquetes/seg)
Tamaño del paquete: 500 bytes

Tabla 5.2 Fuente de tráfico.

Fuente de tráfico de fondo: Variable Bit Rate (UDP)
Velocidad: variable { 0.25Mb/seg,…,0.5Mb/seg }
Duración de la ráfaga: 500 mseg
Tamaño del paquete: 500 bytes

Tabla 5.3 Fuente de tráfico de fondo.

- ✓ En todos los casos de estudio se generan tres archivos de salida, un trace file, un nam file, y un archivo para la graficación.

Además, se utiliza un agente de monitoreo que tiene el NS, llamado "Loss-Monitor" Agent/LossMonitor, el cual es una subclase de agentes que contiene un sumidero (*sink*) de tráfico que permite dar estadísticas sobre los datos recibidos. Las variables de estado que maneja son:

*nlost_* Número de paquetes perdidos.

*npkts_* Número de paquetes recibidos.

*bytes_* Número de bytes recibidos.

*lastPktTime_* Instante en el que se recibió el último paquete.

*expected_* Número de secuencia esperado del paquete que debe llegar a continuación.

5.3 SIMULACIONES

5.3.1 Caso de estudio: Método de protección global

5.3.1.1 Modelo de red

La topología planteada para el método de respaldo global, se puede observar en la figura 5.2.

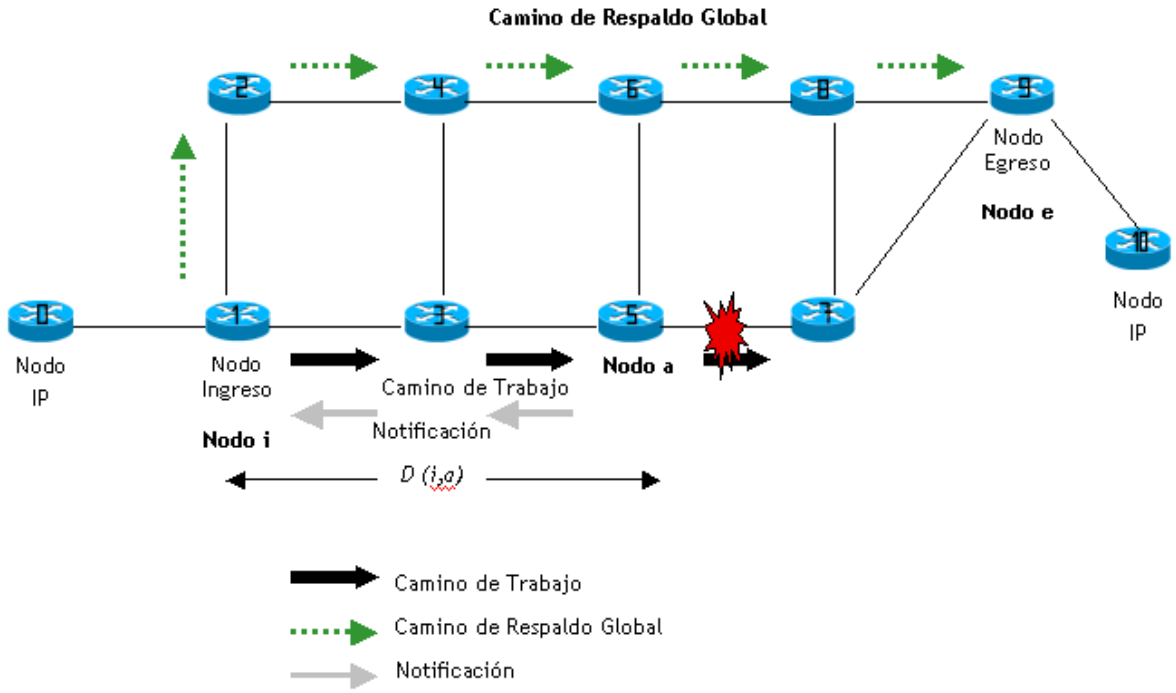


Figura 5.2 Escenario de red del método global.

La red esta formada por 10 nodos, 2 nodos IP (n0 y n10) que funcionan como fuente y destino de tráfico respectivamente, y 9 nodos MPLS (LSR1, LSR2, LSR3, LSR4, LSR5, LSR6, LSR7, LSR8 Y LSR9) que conforman el núcleo del dominio MPLS.

Todos los enlaces entre nodos deben ser definidos en el NS; en este caso, se trata de enlaces unidireccionales con un retardo de propagación variable (ver tabla 5.1). El ancho de banda definido para cada enlace es variable tanto para los nodos externos al dominio MPLS, como para los enlaces LSR1, LSR2, LSR3, LSR4, LSR5, LSR6, LSR7, LSR8 Y LSR9; para poder así observar el funcionamiento de la cola en el NS. Al definir un enlace, también se define el tipo de cola que manejará. En todos los casos de estudio de este trabajo se utiliza la cola *DropTail*, que como su nombre lo dice, descarta los paquetes que se pasen del límite. No se definió límite de paquetes que puede mantener la cola. Al mismo tiempo se tienen que definir los pares LDP, es decir, inicializar una señalización LDP para cada par de LSRs que tenga un enlace entre sí.

Se define un tipo de tráfico CBR a través de UDP que envía paquetes de n0 a n10; para este tráfico se define su tamaño= 500 y su tasa variable. Para mayor referencia de cómo definir estos parámetros, revisar el manual del NS [36].

Para la programación de eventos se tiene en cuenta la definición de un camino explícito de protección como base para definir el método de respaldo global para el óptimo restablecimiento de los caminos. Utilizando este modelo MPLS, se compararán los tres métodos de protección utilizando el mismo escenario de red.

En el script de este método se abarca la programación de eventos de la siguiente manera:

- ✓ En el instante 0.0 se inicia el procedimiento *record* para el monitoreo de la ocurrencia de la falla, la conmutación al camino de respaldo y su restablecimiento.

- ✓ En el instante 0.1 se envían los mensajes de petición y mapeo tanto por el camino de trabajo como por el camino de respaldo (pre-establecido) desde el nodo de ingreso hasta el nodo de egreso en el dominio MPLS.

- ✓ En el instante 0.3 inicia el tráfico de paquetes CBR saliendo del n0 (nodo IP de entrada). También en este instante se crea el camino explícito y se le asigna el identificador de flujo.

- ✓ En 0.8 ocurre la falla (se cae el enlace), seguidamente se envía el mensaje de notificación de falla al nodo de ingreso (nodo con funciones PSL); luego se realiza la conmutación del tráfico al camino de respaldo global.

- ✓ En 1.3 se restablece el camino de trabajo y se envía un mensaje de notificación al nodo PSL para enrutar de nuevo el tráfico a éste camino.

- ✓ En el instante 1.8 se finaliza el flujo del tráfico y también se cierran los archivos de salida generados.

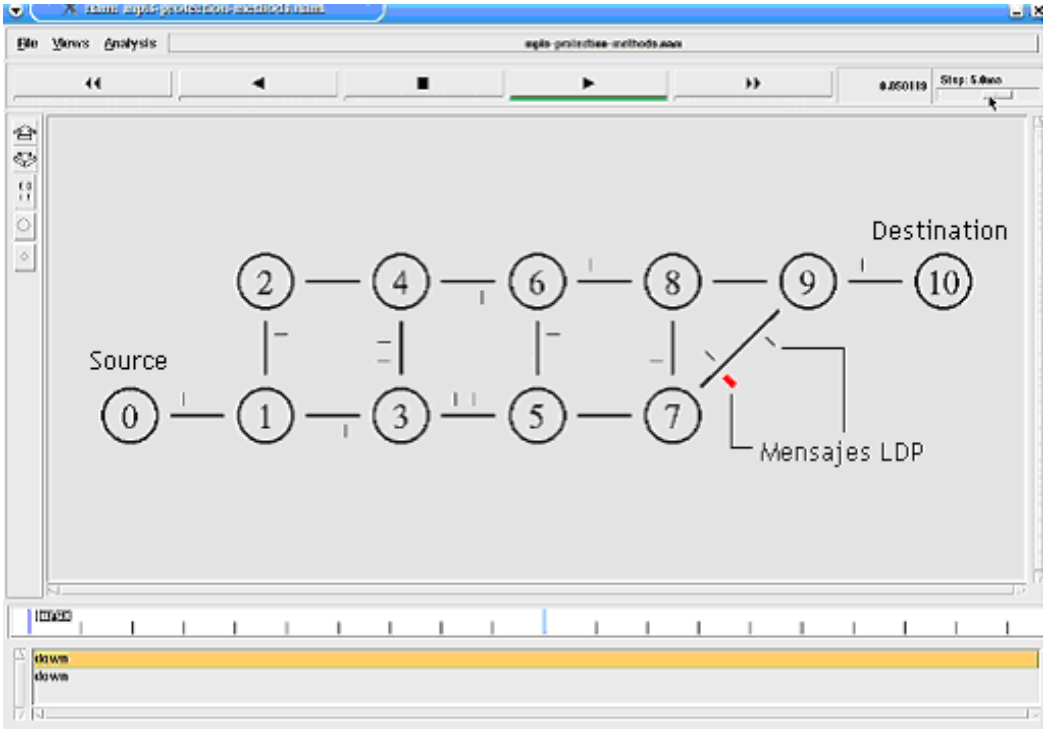
Una vez definida la topología de red dentro del script, se corre la aplicación NS, y se generan los resultados.

5.3.1.2 Sucesión de eventos

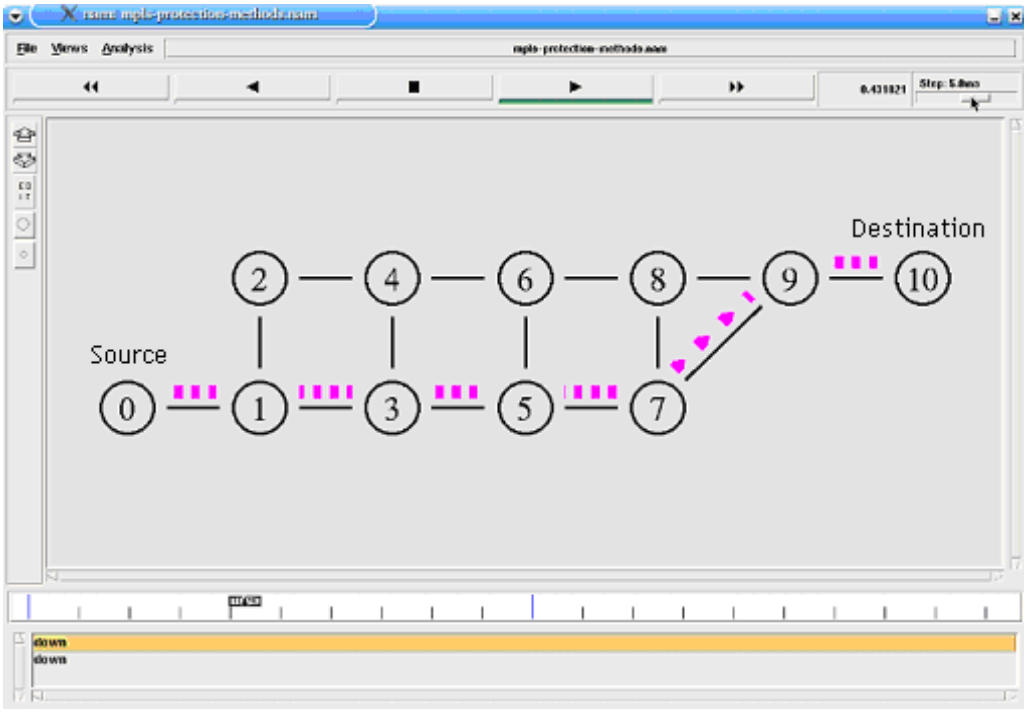
Estos escenarios de red para los métodos de protección son muy representativos dentro de las características de TE que ofrece MPLS.

Al correr el archivo mpls-protection-methods.tcl, que corresponde al método global, automáticamente se abre el NAM con la topología creada, lista para visualizar.

El primer evento visible dentro del NAM, es el mecanismo de señalización con que LDP establece los caminos de trabajo y de respaldo (ver figura 5.3a). Luego se inicia el flujo CBR de n0 a n10, pasando por cada uno de los LSRs del camino de trabajo (LSR1-LSR3-LSR5-LSR7-LSR9) del dominio MPLS. La figura 5.3b muestra este evento y además se observa en la figura, el flujo de paquetes que se distingue por el color fucsia.



(a) Establecimiento del camino de trabajo y de respaldo.



(b) Flujo de tráfico por el camino de trabajo.

Figura 5.3 Método global, evento 1.

Después del instante 0.8 ms, se produce la falla en el enlace entre el LSR3 y LSR5; se envía la señal de indicación de falla al nodo de ingreso (PSL) y se inicia el descarte de paquetes, desechando los paquetes del fondo de la pila. Este evento se observa en la figura 5.4.

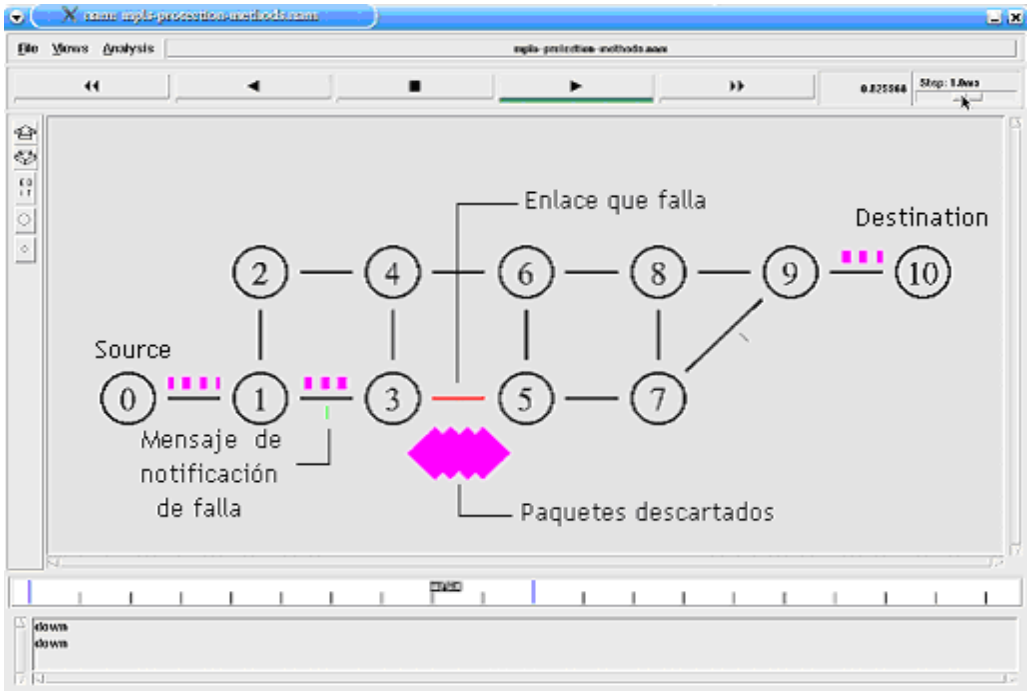


Figura 5.4 Método global - Falla en el enlace, evento 2.

Una vez ocurre la falla se conmuta el tráfico del camino de trabajo al camino de respaldo pre-establecido hasta que se restablezca nuevamente el enlace que ha fallado, como se observa en la figura 5.5.

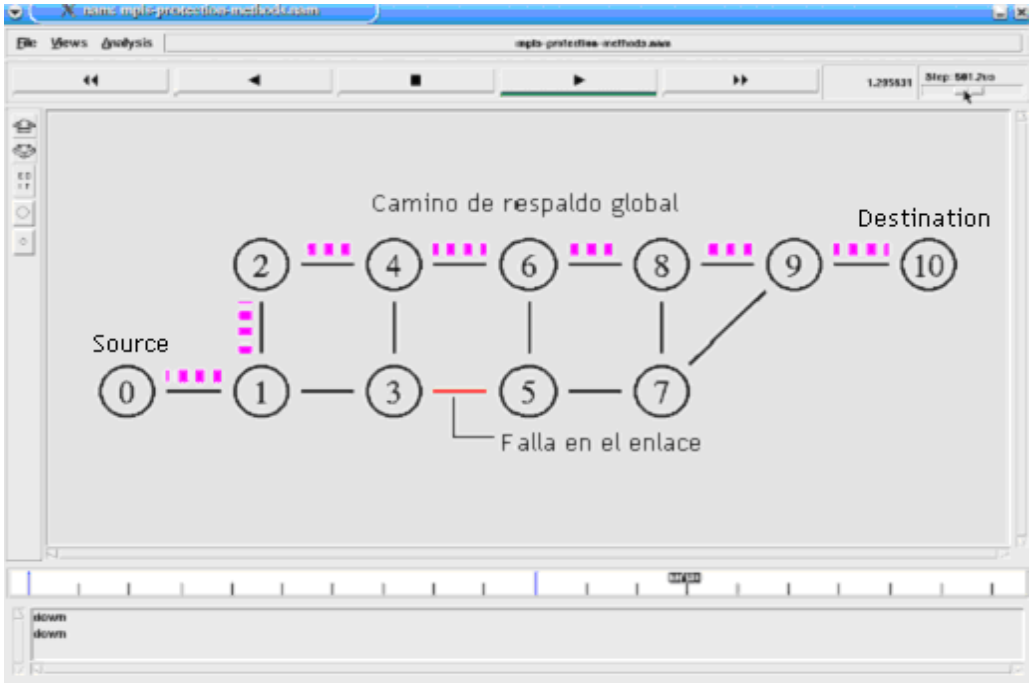


Figura 5.5 Método global – Tráfico sobre el respaldo, evento 3.

La figura 5.6 muestra el envío de mensajes de restablecimiento del camino de trabajo en el instante 1.3 ms tanto al nodo PSL como a los LSRs intermedios, para que se reanude el flujo de tráfico por éste camino. Los datos que van por el camino de respaldo continúan hasta llegar al nodo de ingreso sin inconvenientes en su trayectoria.

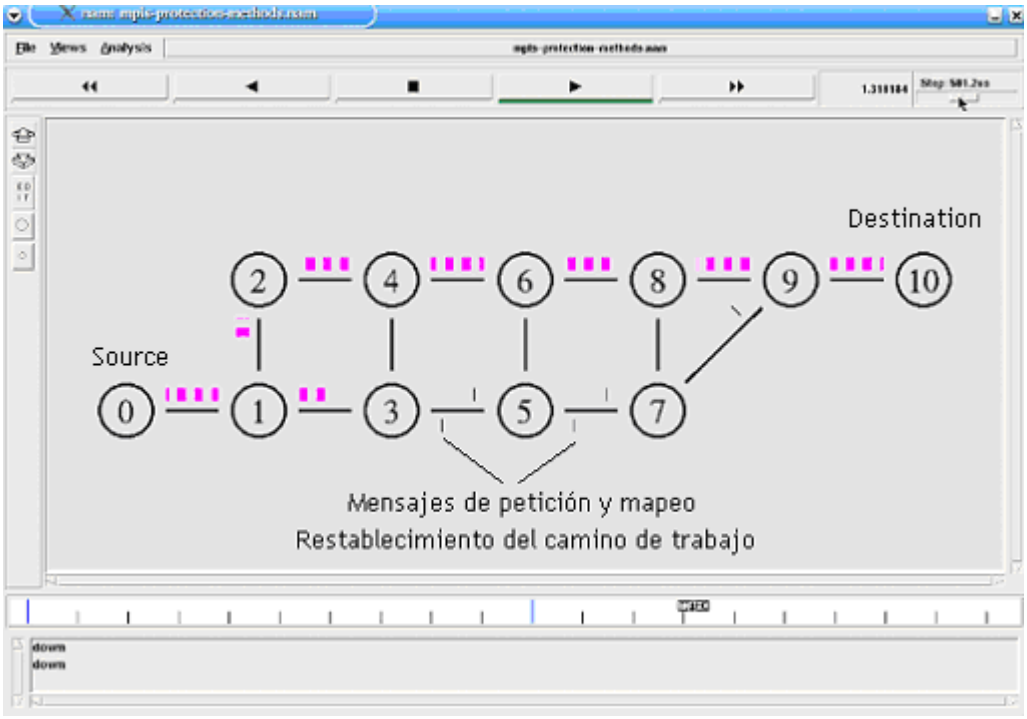


Figura 5.6 Método global – Restablecimiento del camino de trabajo, evento 4.

En la figura 5.7, se observa que el flujo de paquetes CBR, circula nuevamente a través del camino de trabajo y los pocos paquetes que quedan del camino de respaldo se encolan en el enlace con los que proceden de éste camino, pero no se descarta ningún paquete. Instantes después, se detiene el envío de paquetes, con lo cual se termina la simulación.

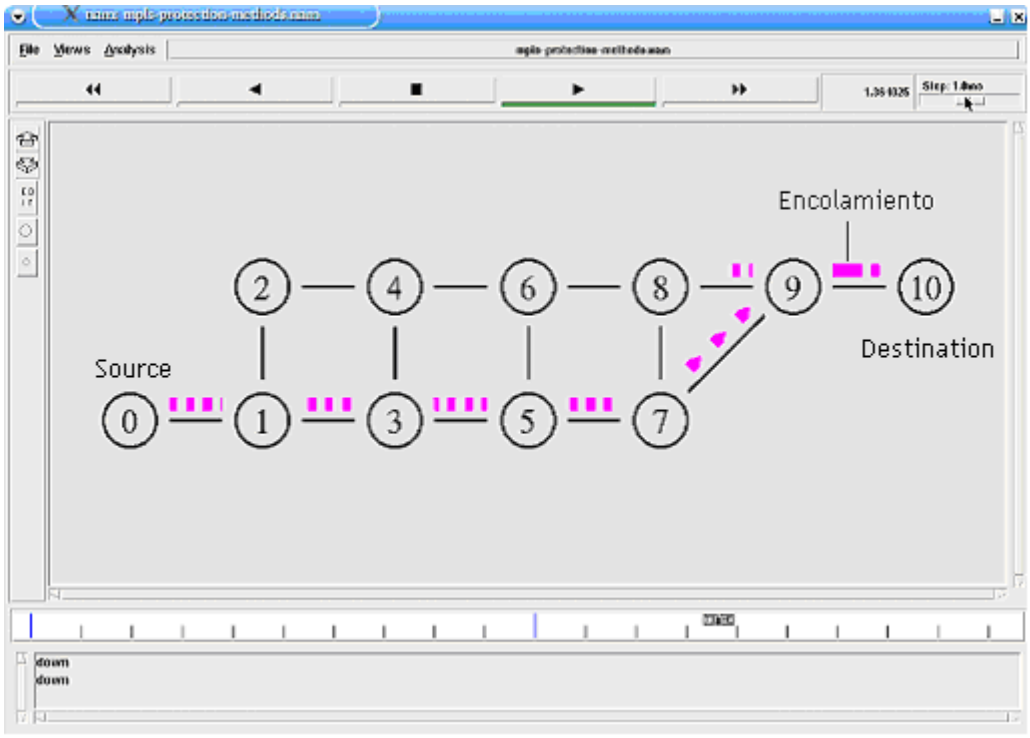


Figura 5.7 Método global, evento 5.

5.3.1.3 Resultados

Sin duda la visualización en el NAM deja una perspectiva clara de lo que sucede en la red simulada; pero para tener una mejor interpretación de los resultados, se utiliza el comando *xgraph* para generar la gráfica del ancho de banda en función del tiempo de simulación cuando ocurre la falla y reacciona el método de protección, como se observa en la figura 5.8. Aquí se puede observar el desempeño de la red cuando ocurre la falla, y de acuerdo a los valores del ancho de banda para ver su estabilidad, instantes después de que se ha caído el enlace. Este método presenta mayor pérdida de paquetes y tiempo de restablecimiento.

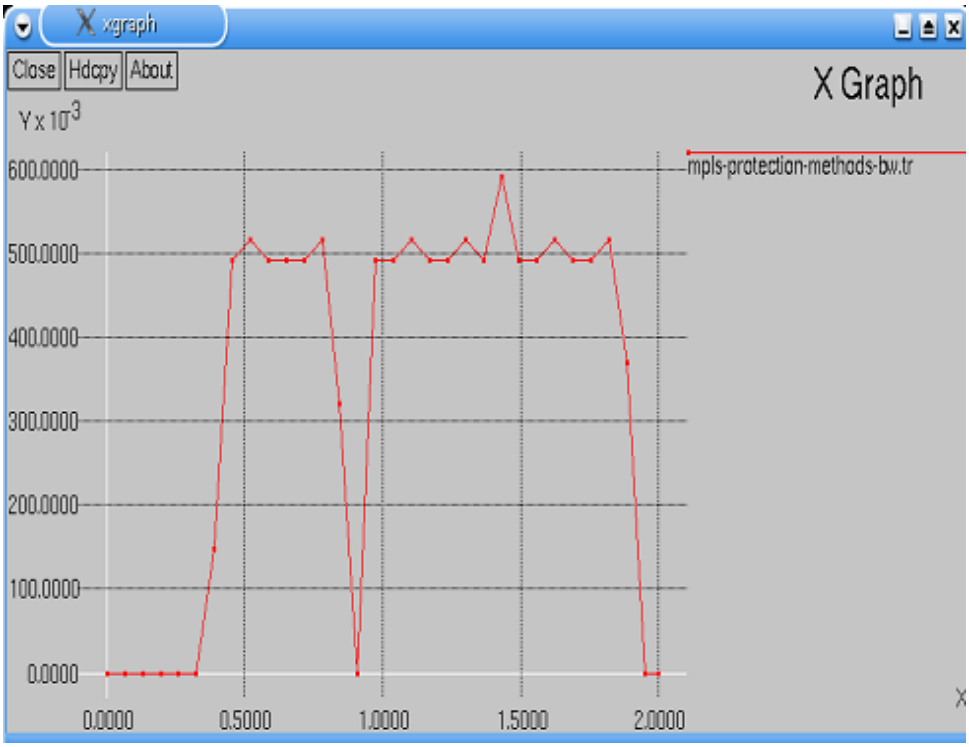


Figura 5.8 Resultado del método de protección global.

Como se observa el ancho de banda en el LSR3 oscila entre 0.2 Mbits/seg y 0.5 Mbits/seg. También se observa que instantes después de que ocurre la falla (0.8 ms) el ancho de banda empieza a caer constantemente, pero no llega a cero debido a que se efectúa el método de protección permitiendo así que los nuevos paquetes sean enviados por el camino de respaldo mientras los paquetes que se encontraban en el camino de trabajo son descartados (pérdida de paquetes).

5.3.2 Caso de estudio: Método de protección inverso

5.3.2.1 Modelo de red

En este escenario se plantea la misma topología de red que en el caso de estudio para el método global, e igualmente la falla ocurre en el enlace formado por el LSR3 y LSR5. En la figura 5.9 se muestra esta topología.

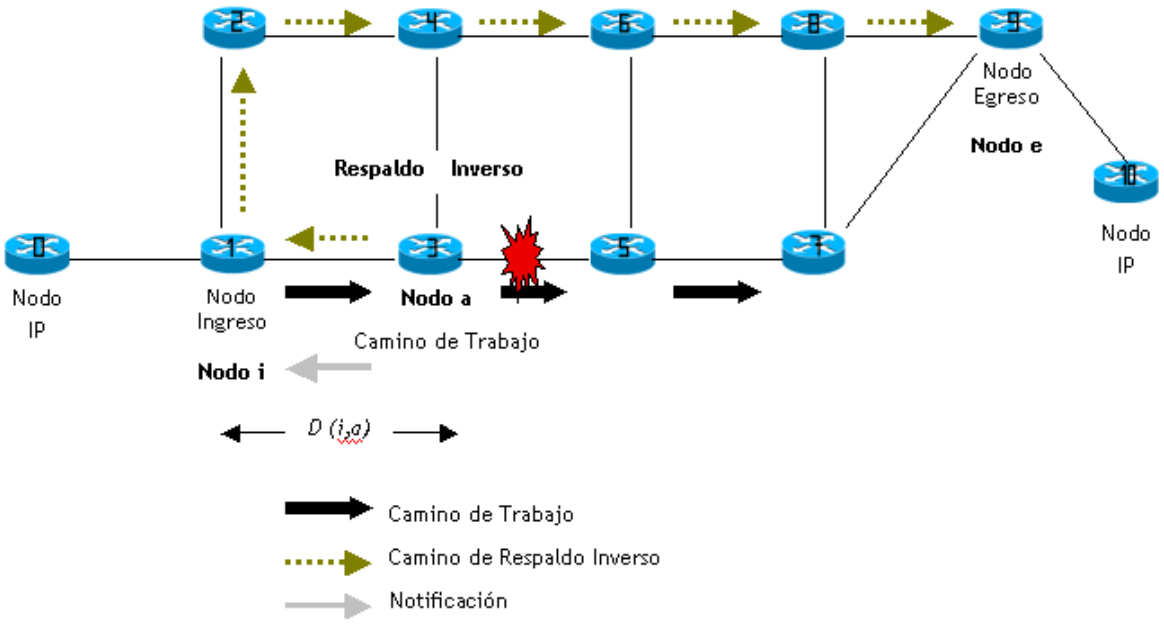


Figura 5.9 Escenario de red del método inverso.

Se conservan los parámetros del primer escenario (método global) para la comparación. Cada enlace tiene las mismas especificaciones, el mismo ancho de banda, el mismo retardo y el mismo tipo de cola (*DropTail*). También se envían los mimos flujos de tráfico, se monitorea el mismo enlace donde se producirá la falla y también se incluyen las mismas rutinas para generar el método de protección.

A diferencia del anterior método la señalización LDP se realiza utilizando el mismo respaldo inverso. La programación de eventos también es la misma que para el caso de estudio del método global.

5.3.2.2 Sucesión de eventos

Una vez que se corre la simulación del archivo mpls-protection-methods.tcl, que corresponde al método inverso, se genera la topología y se visualiza en el NAM. La sucesión de eventos es prácticamente la misma. El primer evento es igual que el del método global, donde se realiza el envío de mensajes LDP para establecer los caminos tanto de trabajo como de respaldo.

Como la programación de eventos es diferente, debido a que éste método necesita de dos caminos de respaldo una vez ocurra la falla, se presentan varios cambios en su visualización. La figura 5.10 muestra la situación de los paquetes cuando ocurre la falla en el enlace formado por el LSR3 y LSR5. En el instante de la falla el nodo afectado notifica (proceso de señalización) al nodo PSL e inmediatamente se realiza la notificación a través de uno de los caminos de respaldo hasta llegar al nodo de ingreso quien se encargará de realizar la conmutación del tráfico al otro camino de respaldo.

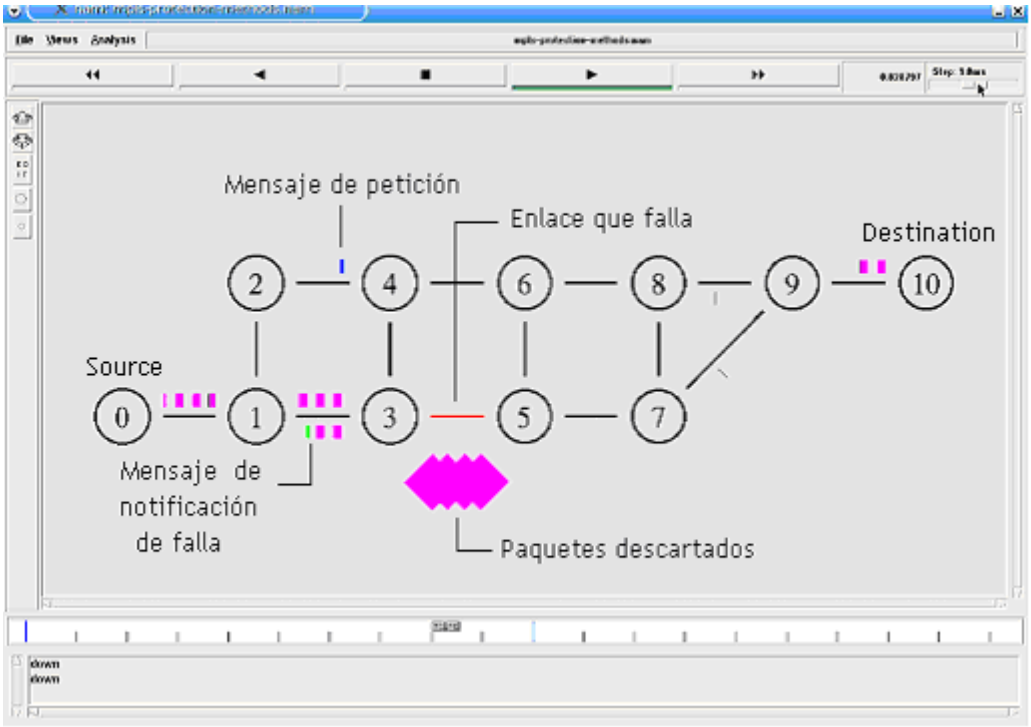


Figura 5.10 Método inverso – Falla en el enlace, evento 2.

Una vez los paquetes que provienen en sentido inverso al camino de trabajo llegan al nodo de ingreso, estos se enrutan junto con el flujo que proviene del nodo IP por el camino de respaldo. Este método a diferencia del método global tiene menor pérdida de paquetes en el enlace afectado. Este evento se muestra en la figura 5.11, donde también se observa encolamiento en el enlace congestionado debido a la acumulación de paquetes, pero no se produce descarte de paquetes, en el nuevo camino de respaldo una vez se conmuta el tráfico (ver figura 5.11).

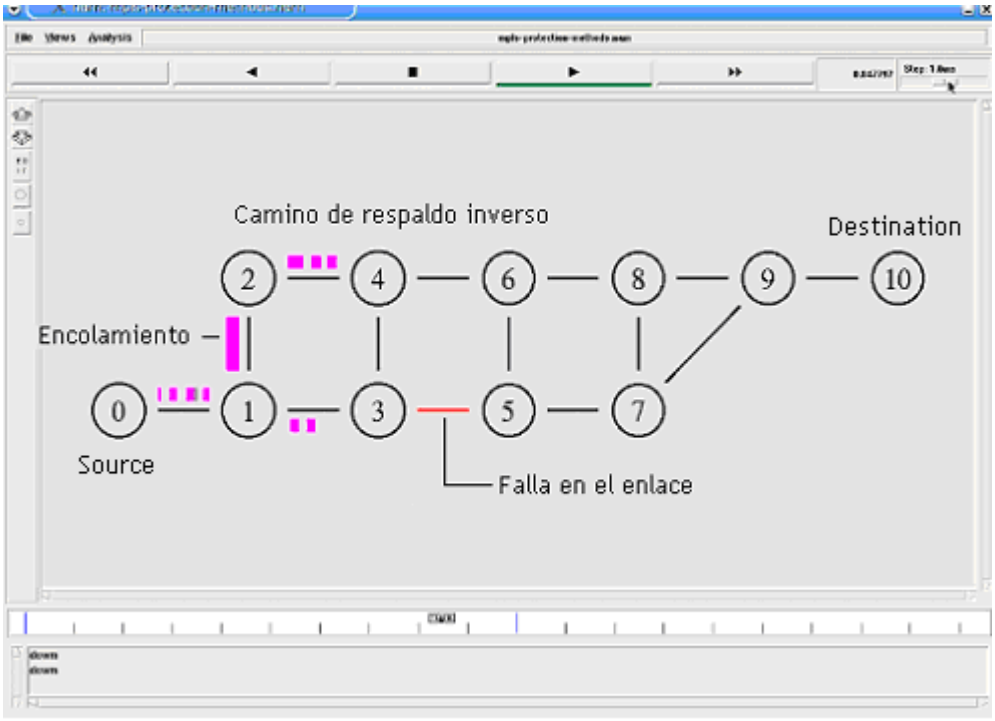


Figura 5.11 Método inverso – Conmutación del tráfico, evento 3.

Mientras permanezca la falla en el enlace el método inverso se comporta como el método de respaldo global (ver figura 5.12), hasta que re restablezca nuevamente el camino de trabajo.

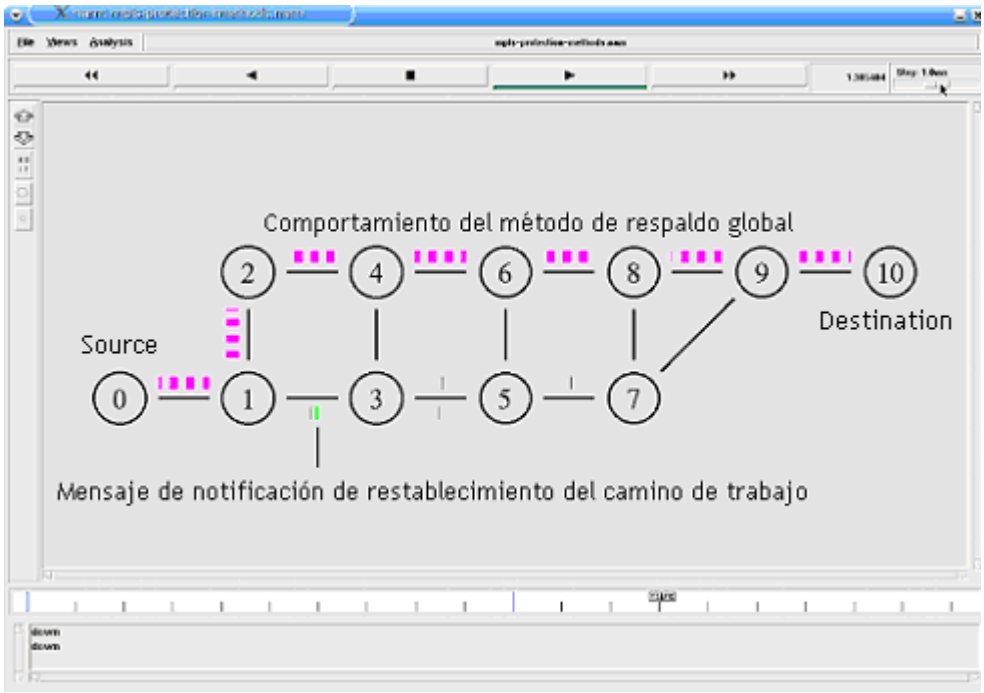


Figura 5.12 Método inverso – Restablecimiento del enlace , evento 4.

Por último, la figura 5.13 muestra el flujo de los últimos paquetes a través del camino de respaldo y el restablecimiento total del camino de trabajo en el instante 1.3 segundos.

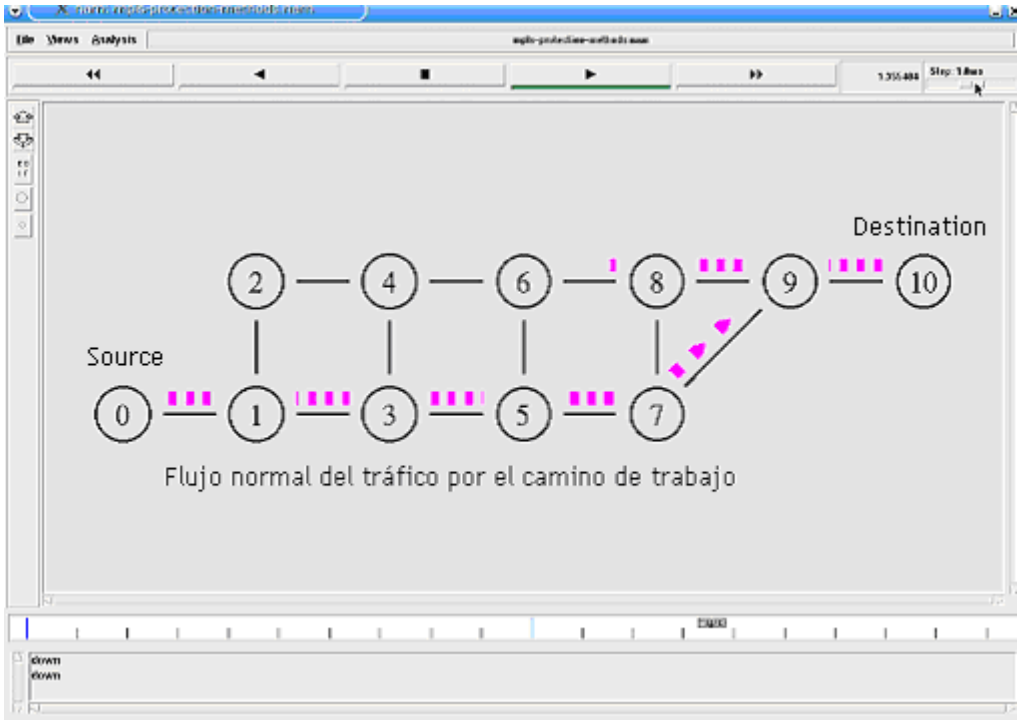


Figura 5.13 Método inverso – Restablecimiento del camino de trabajo, evento 5.

5.3.2.3 Resultados

El resultado que arroja éste método respecto al ancho de banda vs el tiempo de simulación se observa en la figura 5.14, donde se puede observar que este método de protección tiene un desempeño igual al método global en cuanto a tiempo de restablecimiento, pero su diferencia radica en la pérdida de paquetes debido a que ésta es mínima, instantes después de que se ha caído el enlace. Este método presenta desorden de paquetes a diferencia del método global y utiliza un camino de respaldo para realizar la notificación de la falla.

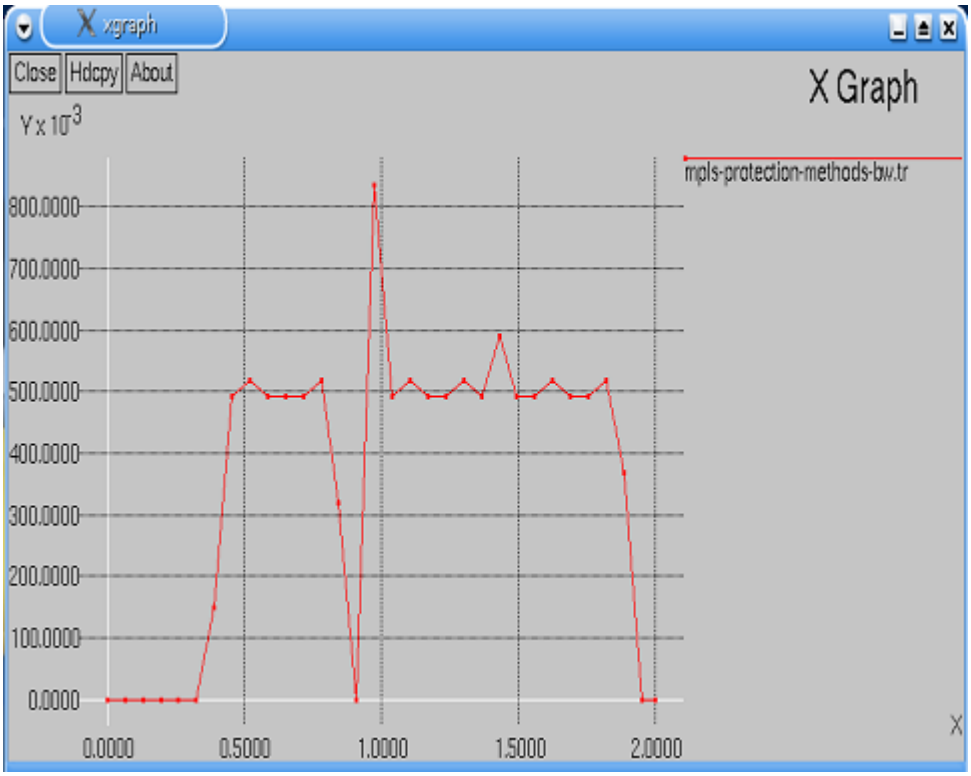


Figura 5.14 Resultado del método de protección inverso.

5.3.3 Caso de estudio: Método de protección local

5.3.3.1 Modelo de red

Este escenario presenta la misma topología de red que para los casos de estudio global e inverso, con la diferencia que la falla ocurre es en el enlace formado por el LSR5 y LSR7. La figura 5.15 muestra esta topología.

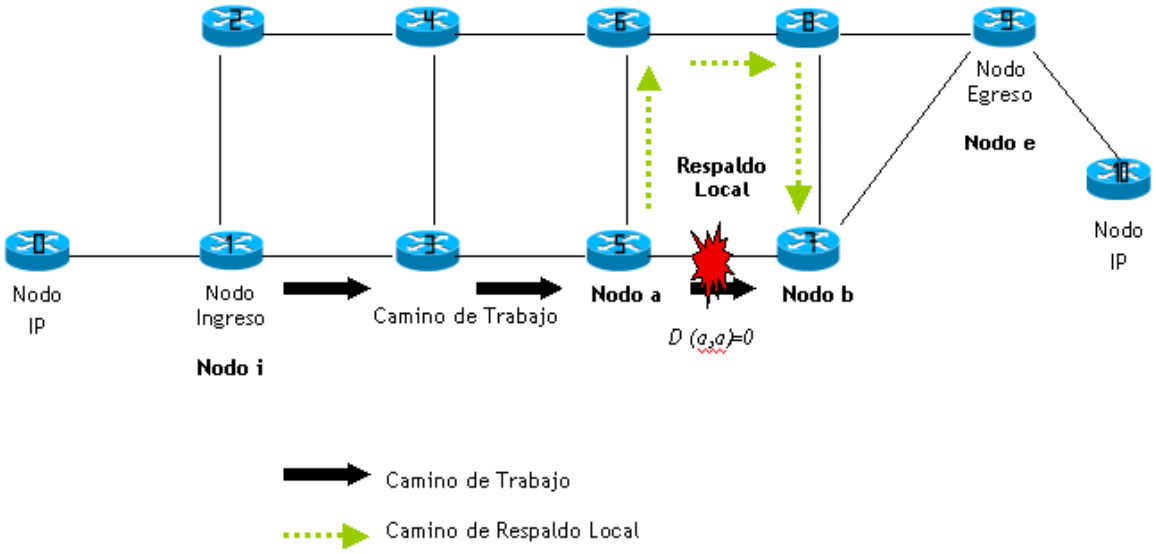


Figura 5.15 Escenario de red del método local.

Igual que el anterior método se conservan los parámetros del primer escenario (método global) para la comparación. Cada enlace tiene las mismas especificaciones, el mismo ancho de banda, el mismo retardo y el mismo tipo de cola (*DropTail*). También se envían los mimos flujos de tráfico, y a diferencia de los anteriores se monitoreará otro enlace (LSR5-LSR7) donde se producirá la falla, y se establece el mismo límite en la cola. Las rutinas para generar el método de protección son un poco diferentes ya que se deben asignar funcionalidades PSL y PML a cada LSR del camino de trabajo y no al nodo de ingreso y egreso respectivamente, como para los métodos global e inverso.

A diferencia con los otros dos métodos se simplifica la señalización LDP. La programación de eventos es diferente en comparación al caso de estudio del método global e inverso.

5.3.3.2 Sucesión de eventos

Luego de simular el archivo mpls-protection-methods.tcl, que corresponde al método local, se genera la topología y se visualiza en el NAM. La sucesión de eventos es prácticamente la misma. El primer evento trascendente, donde se realiza el establecimiento del camino de trabajo y de respaldo se observa en la figura 5.16.

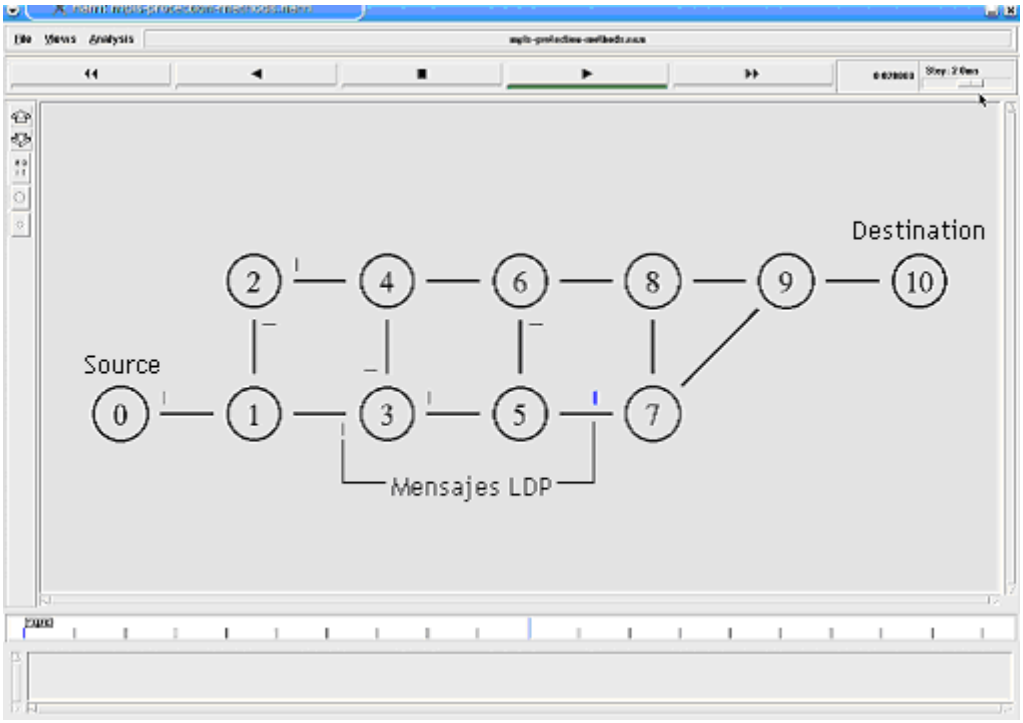


Figura 5.16 Método local – Preestablecimiento de caminos, evento 1.

La programación de eventos es diferente, debido a que éste método de respaldo sólo protege un segmento del dominio MPLS. Una vez ocurra la falla, el nodo anterior a ésta (nodo PSL) conmuta el flujo de tráfico al camino de respaldo pre-establecido para ese segmento, sin necesidad de enviar notificación al nodo de ingreso. El tiempo de restablecimiento y la pérdida de paquetes es menor que los dos anteriores métodos, excepto que consume más recursos debido a que todos los LSRs deben tener funcionalidades PSL y PML (ver figura 5.17).

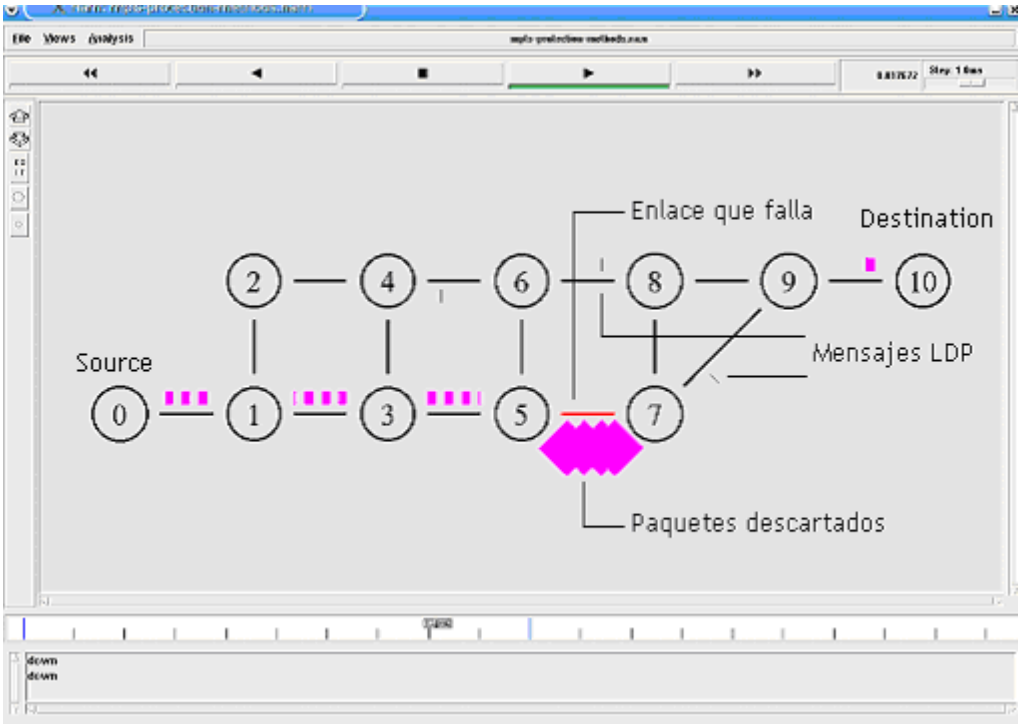


Figura 5.17 Método local – Falla en el enlace, evento 2.

Una vez ocurre la falla se conmuta el tráfico del camino de trabajo al camino de respaldo pre-establecido hasta que se restablezca nuevamente el enlace que ha fallado, como se observa en la figura 5.18.

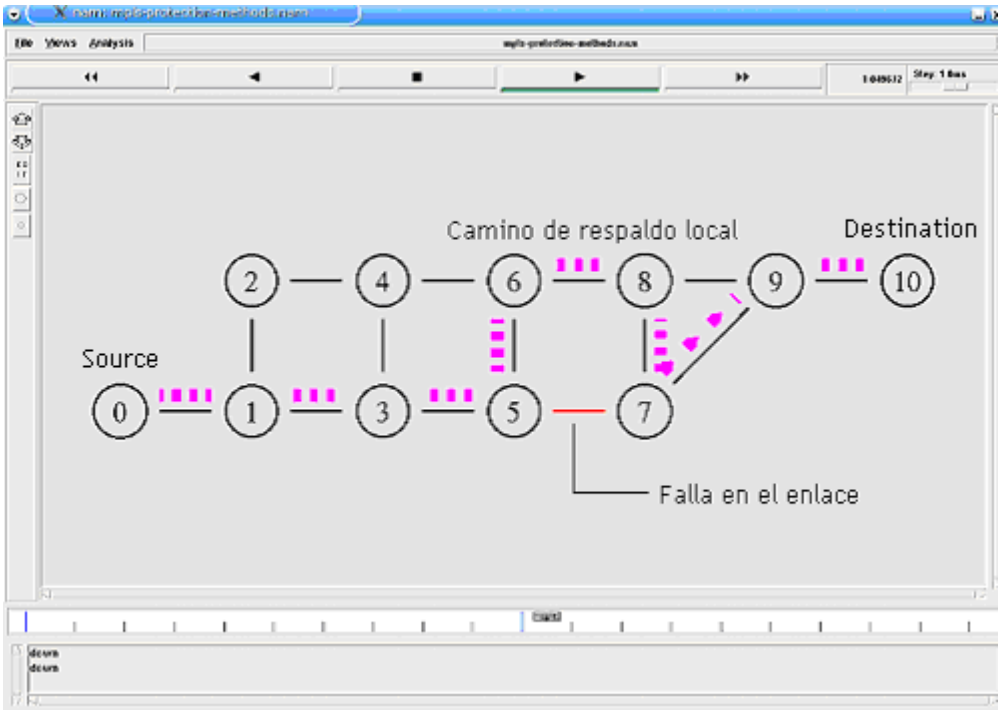


Figura 5.18 Método local – Conmutación al camino de respaldo, evento 3.

Por último, la figura 5.19 muestra el flujo de los últimos paquetes a través del camino de respaldo local y el envío de mensajes LDP cuando ocurre el restablecimiento total del camino de trabajo en el instante 1.3 ms.

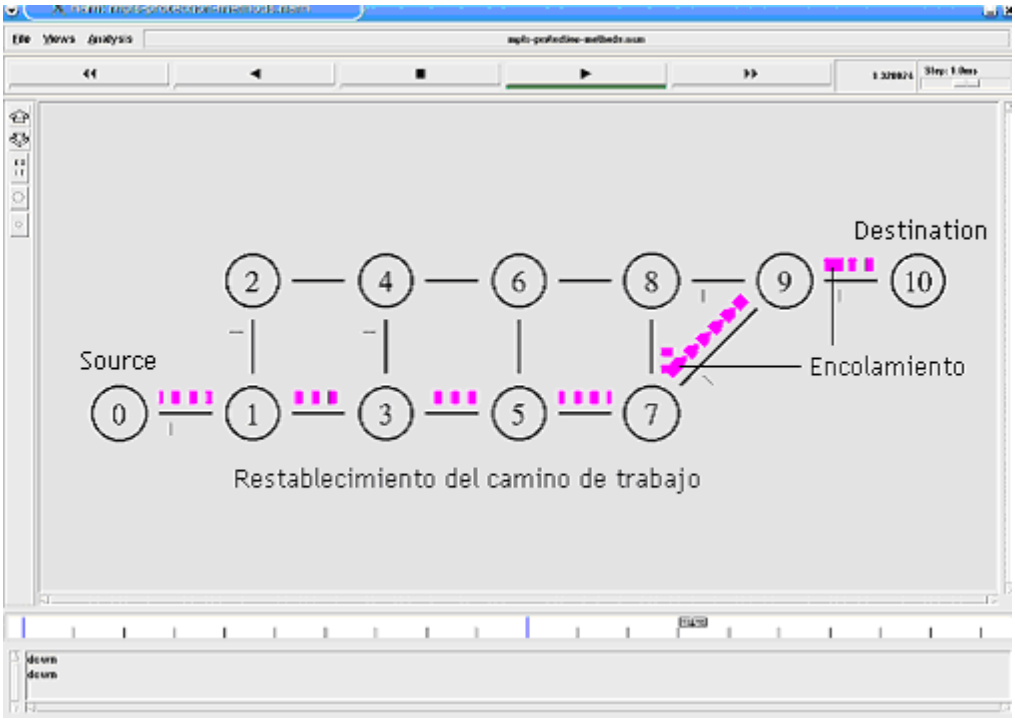


Figura 5.19 Método local – Restablecimiento del camino de trabajo, evento 4.

5.3.3.3 Resultados

El resultado que arroja la graficación se observa en la figura 5.20, donde se puede observar que este método de protección tiene un desempeño más estable que el presentado por los anteriores métodos, además la pérdida de paquetes es mínima, instantes después de que se ha caído el enlace, debido a que este método de respaldo es transparente al nodo de ingreso. Este método presenta menor tiempo de restablecimiento.

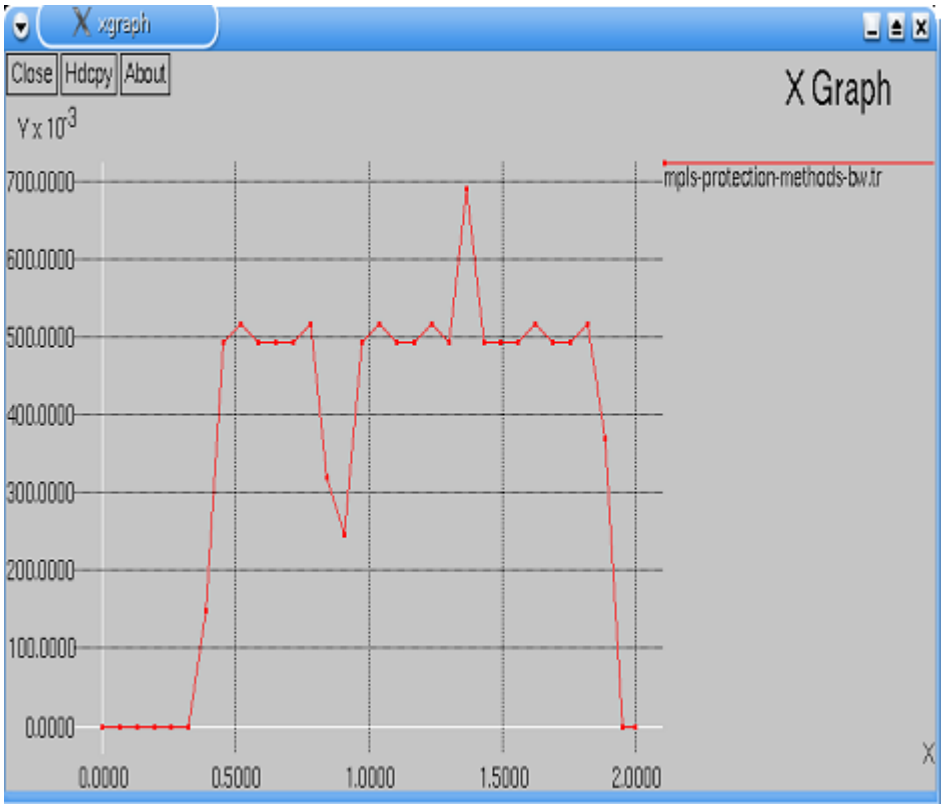


Figura 5.20 Resultado del método de protección local.

En los anteriores casos de estudio cuando ocurre la falla y reacciona determinado método (independiente de cual sea), la protección se efectúa y no permite que caiga del todo el enlace, es decir, que de esta manera la pérdida de paquetes no es tan drástica en comparación a que no se presente ningún tipo de respaldo o se anule el enlace y no permita que éste se recupere.

5.4 EVALUACIÓN DE DESEMPEÑO DE LOS MÉTODOS DE PROTECCIÓN MPLS

Los factores básicos que afectan el desempeño de los métodos de protección son la pérdida de paquetes, el tiempo de restablecimiento, y el consumo de recursos aunque también se debe tener en cuenta el desorden de paquetes. Estos parámetros de medida de desempeño se usaron para comparar los métodos de protección de MPLS cuando ocurre una falla en el enlace y determinar cual es el más adecuado en reaccionar dependiendo de las políticas de restablecimiento. Otros parámetros serán considerados más adelante en el mecanismo integrado.

La evaluación de desempeño para cada uno de los métodos está basada en los modelos de red de la figuras 5.2, 5.9 y 5.15, para los cuales se presenta un mismo modelo de red de prueba.

Las figuras 5.21 y 5.22 presentan la comparación del comportamiento de los tres métodos: global, inverso y local con caminos de respaldo pre-establecidos. Los resultados sólo se refieren al

período de restablecimiento y muestra el porcentaje (%) de pérdida de paquetes y el de los paquetes que sufren desorden al aplicar el método escogido. El eje horizontal presenta la posición del LSR que detecta la falla dentro del LSP protegido respecto al nodo de ingreso.

5.4.1 Pérdida de paquetes

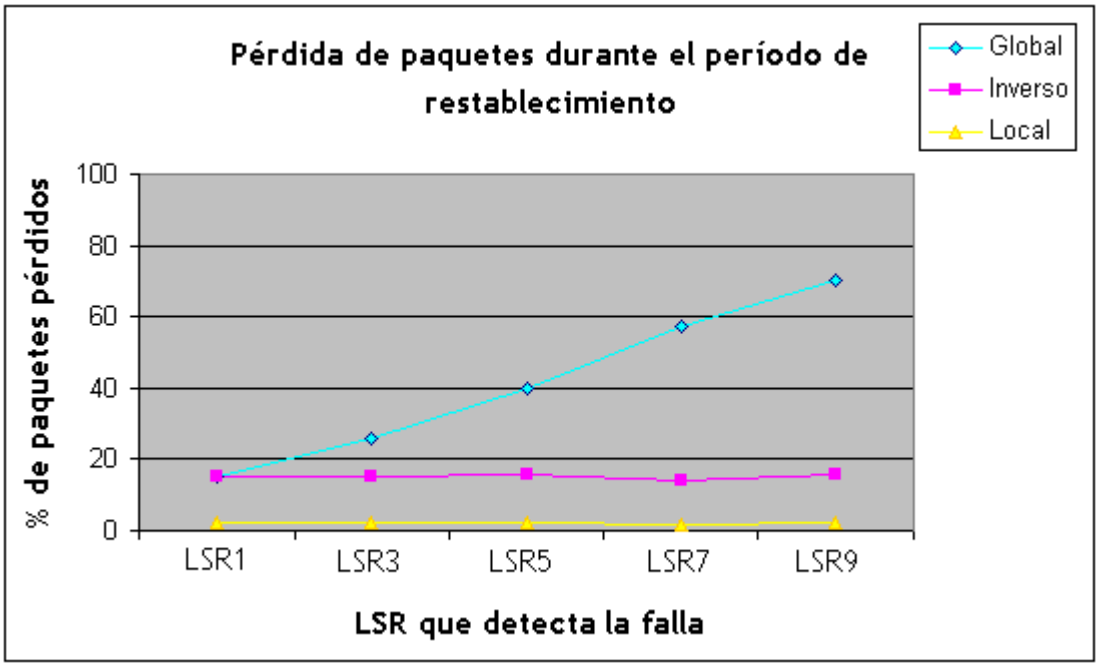


Figura 5.21 Comparación de la pérdida de paquetes entre los métodos de protección en redes MPLS.

La figura 5.21 muestra la comparación de los métodos en cuanto a pérdida de paquetes se refiere. Para el método global la pérdida de paquetes aumenta en proporción a la distancia entre el LSR de ingreso y el LSR que detecta la falla, debido al tiempo que toma el mensaje de notificación de falla. Por otro lado, tanto para el método inverso como para el local la pérdida de paquetes sólo se da en el enlace que ha fallado o en el enlace adyacente al LSR que falla, por esta razón es mínima la pérdida de paquetes. Sin embargo, el que presenta menor pérdida de paquetes es el método local, debido a que sólo protege el segmento, y los tiempos de recuperación y desviación de paquetes son menores.

5.4.2 Re-ordenamiento de paquetes

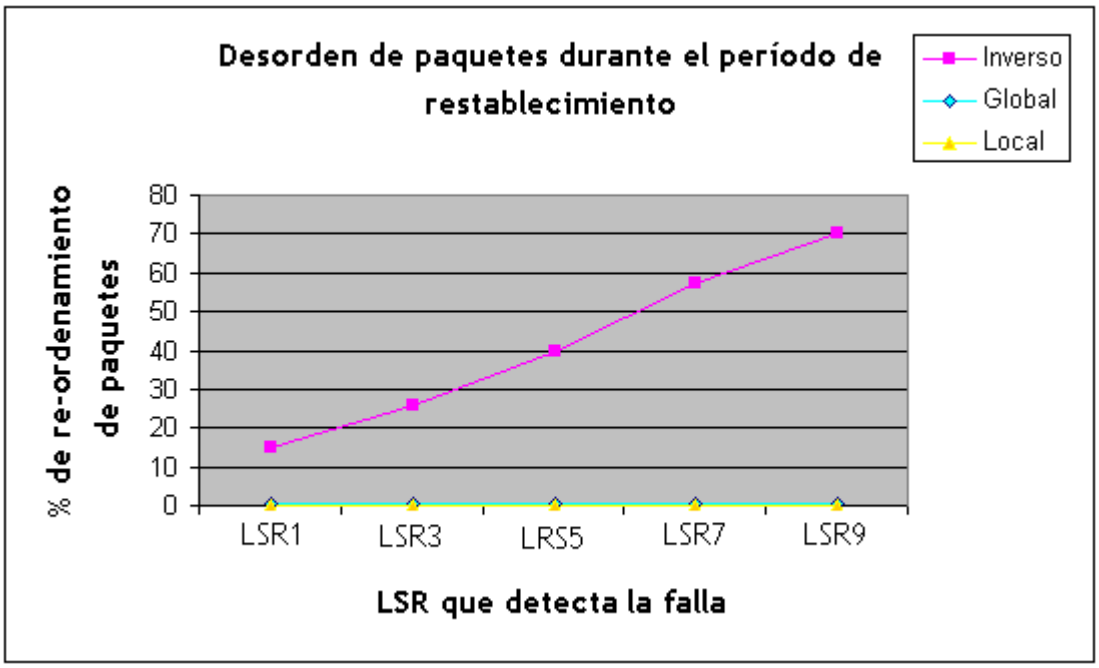


Figura 5.22 Comparación de desempeño en el desorden de paquetes entre los métodos de protección en redes MPLS.

La figura 5.22 presenta el resultado del desorden de paquetes cuando ocurre la falla para éstos métodos. En el método Inverso el desorden de paquetes aumenta en proporción a la distancia entre el LSR de ingreso y el LSR que detecta la falla. Nótese que el desorden de paquetes que se considera aquí es el desorden producido durante el período de restablecimiento que no incluye el desorden producido por la retransmisión de paquetes perdidos por un protocolo de nivel alto (es decir, TCP).

Tanto el método Global como el Local no introducen desorden de paquetes, aunque el método global causa más pérdida de paquetes.

Basado en la argumentación de este capítulo se restringe a la combinación de las acciones de los métodos de protección global, inverso y local con LSP de respaldo pre-establecido. La acción del método local se usa debido a su ventaja en términos de velocidad para la conmutación del tráfico desde el camino de trabajo al camino de respaldo comparado con la acción de recuperación global. También es de notar que la recuperación local puede llevar al uso más alto de recursos debido a la longitud del camino de la protección resultante. Por esta razón se usa el método de protección global que proporciona el camino óptimo disponible. Además se escogió el método inverso porque, al igual que el método local reporta una pérdida de paquetes mínima. Sin embargo, el método local es diferente, en el método inverso los recursos se usan sólo durante el tiempo de restablecimiento que es relativamente corto y puede usarse por el tráfico de prioridad baja, mientras que en el método local el consumo de recursos es mayor.

5.4.3 Consumo de recursos

La comparación del porcentaje de recursos usado por los tres métodos de protección pre-establecidos se muestra en la figura 5.23. Como era esperado, los resultados muestran que el respaldo inverso consume más recursos y que el más pequeño porcentaje lo obtiene el respaldo local. En este caso, sólo el 20% de los enlaces de la red son protegidos. Sin embargo, si el porcentaje de protección de la red aumenta, los respaldos locales pueden consumir más recursos que los respaldos globales o inversos (aproximadamente 0.15 para los respaldos inversos y 0.1 para los respaldos globales y locales). Los resultados también muestran que los respaldos inversos siempre usan más recursos que los respaldos globales, debido a su doble camino de respaldo. En cada prueba hay sin embargo, una proporción diferente entre los respaldos globales y locales. Esto se debe a que el establecimiento de los respaldos inversos empieza en el último nodo que es protegido, minimizando el consumo de recursos cuando este nodo está cerca al nodo de ingreso.

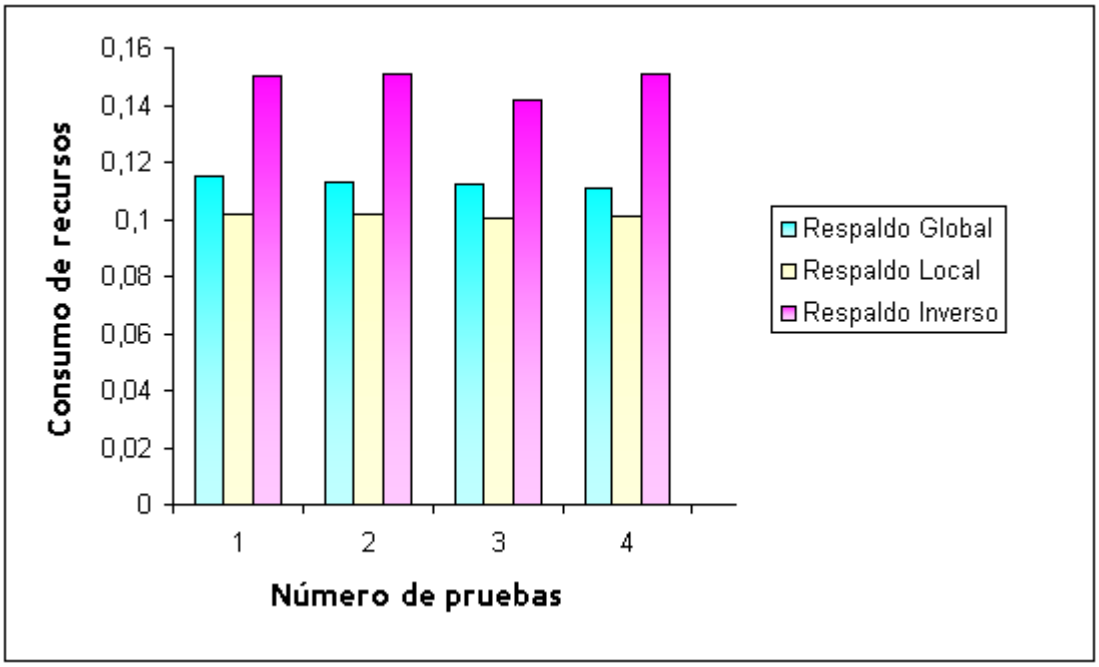


Figura 5.23 Comparación del consumo de recursos de los métodos de respaldo.

5.5 RESULTADOS EXPERIMENTALES DEL MECANISMO INTEGRADO

Las fallas son introducidas en diferentes segmentos de la red para simular la influencia de la distancia D (i,a), entre el nodo que detecta la falla y el nodo encargado de ejecutar las acciones de conmutación del tráfico al camino de respaldo, teniendo en cuenta las políticas de restablecimiento. La figura 5.24 muestra el modelo de red de prueba utilizado para la realización tanto de los casos de estudio de cada uno de los métodos de protección como del mecanismo integrado.

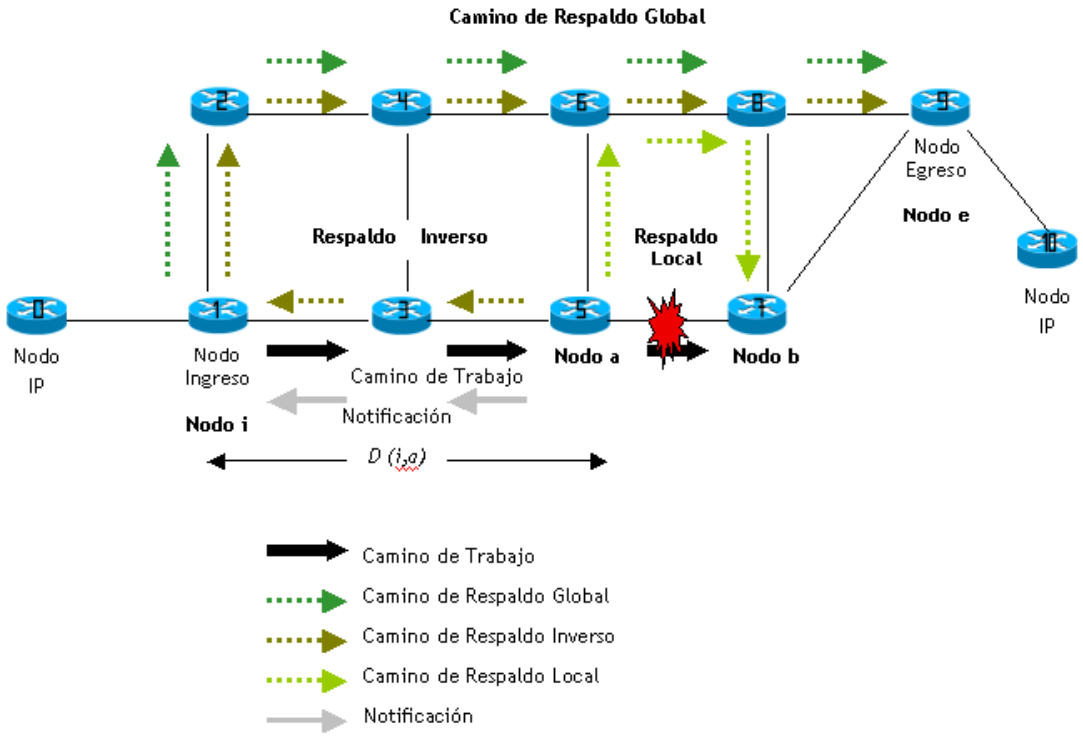


Figura 5.24 Escenario de red integrado.

5.5.1 Tiempo de restablecimiento

Se llevaron a cabo dos pruebas con el fin de comprobar en el simulador la fórmula del tiempo de restablecimiento (RT),

a). Tiempo de Restablecimiento y Tiempo de Propagación vs Distancia

El objetivo de esta prueba es comprobar que el tiempo de restablecimiento está influenciado directamente por la distancia, entre el nodo que detecta la falla y el nodo encargado de la conmutación del tráfico al camino de respaldo, y por el tiempo de propagación de la señal de indicación de falla (FIS), esta última depende de la latencia en los enlaces.

La tabla 5.4 muestra diferentes escenarios de prueba, en los cuales se aprecia que el tiempo de propagación afecta linealmente (especialmente el retardo en los enlaces) al tiempo de restablecimiento, además de que la distancia es otro factor determinante en estas pruebas.

Retardo en el enlace (ms)	D(i,a)=0	D(i,a)=1	D(i,a)=2	D(i,a)=3	D(i,a)=4
	RT	RT	RT	RT	RT
0	0.2	0.48	0.51	0.54	0.81
2	0.2	2.47	4.51	6.54	8.81
4	0.2	4.48	8.51	12.54	16.81
6	0.2	6.46	12.51	18.54	24.81
8	0.2	8.46	16.51	24.54	32.81
10	0.2	12.46	20.51	30.54	48.16
20	0.2	20.46	40.21	60.41	80.74

Tabla 5.4 Tiempo de Restablecimiento Vs Distancia.

b). Tiempo de Restablecimiento Vs Carga de la red y Métodos de protección MPLS

La tabla 5.5 muestra la importancia del método de protección seleccionado con respecto al tiempo de restablecimiento. En este caso se utiliza una red mas aproximada a la realidad al introducir un tráfico de fondo; los resultados demuestran que los métodos de respaldo Global e Inverso tienen un comportamiento similar con respecto al tiempo de restablecimiento, mientras que el método local no lo afecta. Por otra parte, se puede observar que una red muy cargada puede afectar negativamente el tiempo de restablecimiento, excepto en el caso de hacer uso de respaldos locales.

Carga de la red (%)	Local	Global	Inverso
	RT	RT	RT
0	0.40	0.40	0.40
10	0.40	1.69	1.53
20	0.40	2.00	2.01
30	0.40	2.06	2.12
40	0.40	2.28	2.25
50	0.40	2.5	2.38

Tabla 5.5 Tiempo de Restablecimiento Vs Carga de la red en cada método de protección MPLS.

5.5.2 Pérdida de paquetes

Se llevaron a cabo dos pruebas para comprobar la fórmula de pérdida de paquetes:

a). % de pérdida de paquetes Vs Carga de la red y método de protección

En esta prueba se analiza la influencia que existe entre el número de paquetes perdidos y el método de protección seleccionado en un escenario con diferente carga de red. La tabla 5.6 muestra los resultados de esta prueba.

Carga de la red (%)	Local (D(i,a)=0)	Inverso (D(i,a)=3)	Global (D(i,a)=3)
	PL	PL	PL
50	13.1	16.5	25.8
40	11.3	13.3	20.7
30	10.2	10.6	16.3
20	5.25	5.6	13.4
10	2.4	2.6	7.6
0	1.2	1.2	5.9

Tabla 5.6 % de pérdida de paquetes Vs Carga de la red en cada método de protección.

b). Pérdida de paquetes Vs Tasa y Distancia

El objetivo de esta prueba es demostrar que el segundo parámetro que más afecta a la pérdida de paquetes, es la tasa (velocidad) del tráfico (bytes/seg) en el camino de trabajo. Se llevaron a cabo varias pruebas con diferentes tasas (paquetes/seg) y el tamaño de los paquetes se fijo a 250 bytes. Nuevamente, la distancia y el método de protección son factores determinantes para minimizar la pérdida de paquetes. En la tabla 4.7 se observan los resultados.

Tasa (paquetes/seg)	Inverso-Local	Global(D(i,a)=3)	Global(D(i,a)=2)
	PL	PL	PL
800	6	78	62
641	5	63	50
542	4	60	48
458	4	44	37
400	3	39	31
356	3	35	28
319	2	29	23

Tabla 5.7 Pérdida de paquetes Vs Tasa teniendo en cuenta la distancia.

5.5.3 Tiempo de restablecimiento y pérdida de paquetes Vs Tasa de tráfico y distancia

El objetivo de esta prueba es permitir comprobar las fórmulas de tiempo de restablecimiento y pérdida de paquetes bajo las siguientes condiciones: retardo en el enlace= 10 ms, diferentes tasas de trafico en el camino de trabajo y distintas distancias D(i,a). En la tabla 4.8 se tienen los resultados de esta prueba.

Tasa de tráfico (paquetes/seg)	D(i,a)=0		D(i,a)=2		D(i,a)=3		D(i,a)=4	
	RT	PL	RT	PL	RT	PL	RT	PL
50	0.25	1	20.1	2	30.2	4	40.38	8
100	0.25	1.1	20.1	5	30.2	8	40.38	15
125	0.25	1.2	20.1	7	30.2	10	40.38	17
250	0.25	2.5	20.1	15	30.2	17	40.38	35
500	0.25	5	20.1	30	30.2	40	40.38	70

Tabla 5.8 Tiempo de restablecimiento y pérdida de paquetes Vs Tasa de tráfico y distancia.

5.5.4 Tiempo de Restablecimiento y pérdida de paquetes Vs Retardo en el enlace y distancia

En la tabla 5.9, se muestra la influencia de la distancia de notificación para las diferentes tasas de tráfico. El objetivo de este análisis es indicar que la distancia de notificación también es un aspecto crucial al seleccionar el método de protección en los escenarios con tasas de tráfico diferente. Una distancia igual a cero significa que se escoge el método local; por otro lado el método global o inverso pueden ser seleccionados. Los resultados revelan que el tiempo de restablecimiento (RT) es directamente proporcional a la distancia.

Retardo en el enlace (ms)(PT)	D(i,a)=0		D(i,a)=2		D(i,a)=3		D(i,a)=4	
	RT	PL	RT	PL	RT	PL	RT	PL
20	0.2	2.3	40.21	11	60.41	15	80.74	26
10	0.2	1.4	20.51	6	30.54	9	48.16	14
8	0.2	1.2	16.51	4.3	24.54	7	32.81	11
2	0.2	0.2	4.51	1.2	6.54	1.5	8.81	3

Tabla 5.9 Tiempo de Restablecimiento y pérdida de paquetes Vs Retardo en el enlace y distancia.

La misma tasa de tráfico ha sido considerada para todos los experimentos. En este escenario, para las distancias de notificación grandes (por ejemplo D(i,a)=4) el tiempo de la propagación entre todos los enlaces se manifiesta como un aspecto crucial. Por ejemplo, cuando se incrementa el tiempo de propagación en el enlace de 2ms a 20ms, el tiempo de restablecimiento empeora casi 100% (ver tabla 5.9). Lo mismo ocurre con la pérdida de paquetes. Hay 26 paquetes perdidos para el retardo del enlace de 20 ms comparados a 3 paquetes para el retardo de 2 ms.

Como se ha mostrado para los experimentos anteriores, la reducción del tiempo de restablecimiento (y también de la pérdida de paquetes) sólo puede lograrse reduciendo la distancia (D(i,a)). Otros componentes, como el tiempo de propagación, dependen de la tecnología física del enlace y no puede reducirse.

El caso óptimo es el uso del método de respaldo local (D(i,a) = 0). Sin embargo, su principal desventaja es que la distancia D(i,a) no se percibe de antemano, porque el enlace qué va a fallar no se conoce todavía.

5.6 APLICACIÓN DEL MECANISMO INTEGRADO DE PROTECCIÓN PARA REDES MPLS

Una aplicación del mecanismo integrado se puede realizar dependiendo de la clase de servicios definidos en el RFC 3270 de la IETF [40], el cual presenta la clase de Envío Acelerado (EF: Expedited forwarding), que se define para transportar el tráfico en tiempo real; dos clases de Envío Asegurado (AF1 y AF2: Assured Forwarding), que se usan para el tráfico con diferentes pérdidas, y como es usual, una clase del Mejor Esfuerzo (BE: Best Effort) para el tráfico sin requerimientos de QoS.

Para realizar las siguientes pruebas de esta aplicación en el mecanismo integrado, se tuvo en cuenta algunas clases de servicio y la formulación de Protección de Calidad de Servicio (QoSP: Quality of Service Protection) [41].

La función general para QoSP se expresa como:

$$QoSP = f(PL, RT, RC) \qquad (5.1)$$

Y una combinación de acuerdo a los parámetros de protección más específica sería [41]:

$$QoSP = \alpha \cdot PL^N + \beta \cdot RT^N + \lambda \cdot RC^N \qquad (5.2)$$

La tabla 5.10 muestra los requerimientos de protección de las diferentes clases de tráfico y sus respectivos ponderados:

Clase de tráfico	Requerimientos de QoS	α	β	λ
EF	PL y RT muy altos	0.5	0.45	0.05
AF1	PL muy alta	0.5	0.3	0.2
AF2	PL baja	0.33	0.33	0.33
BE	No tiene	0.05	0.05	0.9

Tabla 5.10 Clases de tráfico y sus ponderados.

Las siguientes pruebas pretenden demostrar el correcto funcionamiento del mecanismo integrado de protección, para ello se evaluará la función QoSP en cada uno de los casos que se plantearan con el fin de permitir observar cual es el método mas adecuado a aplicar de acuerdo a la clase de tráfico.

Seleccionar el mejor método de protección consiste simplemente en aplicar la métrica QoSP a cada uno de los tres métodos y seleccionar cual de ellos es el que tiene menores requerimientos de QoSP.

A continuación se consideran diferentes escenarios de red en los cuales se tiene en cuenta los siguientes aspectos:

1. Clases de tráfico: EF, AF1, AF2 y BE; los valores para estos se encuentran en la tabla 5.10.
2. Anchos de banda para los LSPs.
3. Número de segmentos a proteger del camino de trabajo.
4. Distancia D(i,a).

5.6.1 Caso 1: QosP e influencia del ancho de banda

Los parámetros de esta prueba son los siguientes:

- ✓ Clase de tráfico: EF.
- ✓ Número de enlaces a proteger: 6.
- ✓ D(i,a)=2.
- ✓ C= variable, ancho de banda necesario para la solicitud de LSP.

La figura 5.25 se muestra los resultados para esta prueba, a partir de ellos se puede ver que se le da prioridad al método local, el cual permite asegurar que se satisfagan los requerimientos de PL y RT. La segunda opción es el método inverso, aunque la diferencia entre los dos se eleva al incrementar el ancho de banda necesario para la solicitud de LSP, dado que éste afecta la pérdida de paquetes como se pudo observar en las pruebas de los métodos de protección. Entre mayor sea el ancho de banda mucho mayor es la perdida de paquetes.

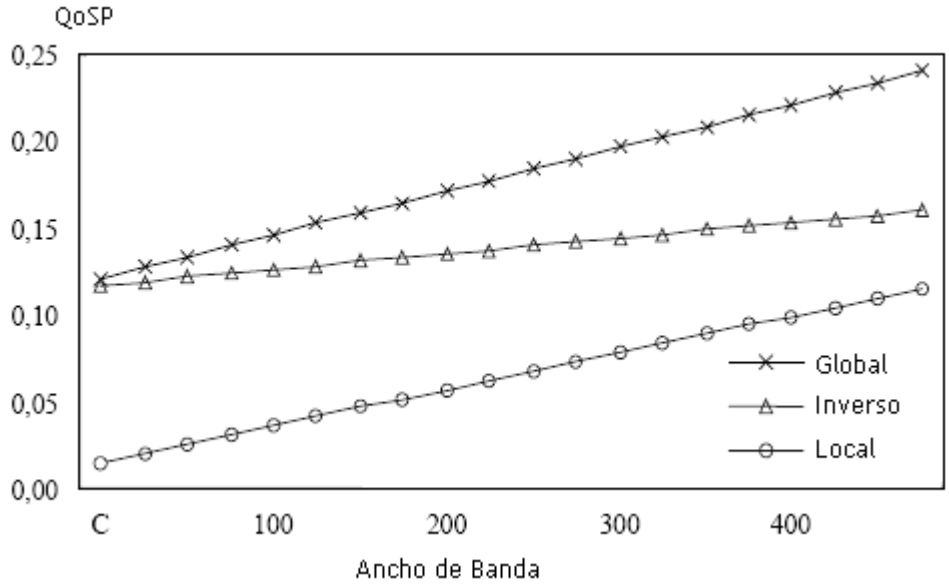


Figura 5.25 QoSP vs Ancho de Banda para tráfico EF.

5.6.2 Caso 2: QoSP e influencia de la distancia

Los parámetros de esta prueba son los siguientes:

- ✓ Clase de tráfico: EF.
- ✓ Número de enlaces a proteger: 2.
- ✓ D(i,a)= variable.
- ✓ C= 400MB

Los resultados están consignados en la figura 5.26, de la cual se puede observar que se selecciona el método local como la primera opción que mejor se adecua a los requerimientos del tráfico EF. Lo interesante está en que la segunda opción varía de acuerdo a la distancia, para distancias cortas un respaldo global es la mejor opción con menor consumo de recursos que el método inverso. Para distancias mas grandes, mayores que 2, el respaldo inverso es mejor. Esto es debido a que en el caso del tráfico EF los parámetros de RT y PT son cruciales en comparación al consumo de recursos.

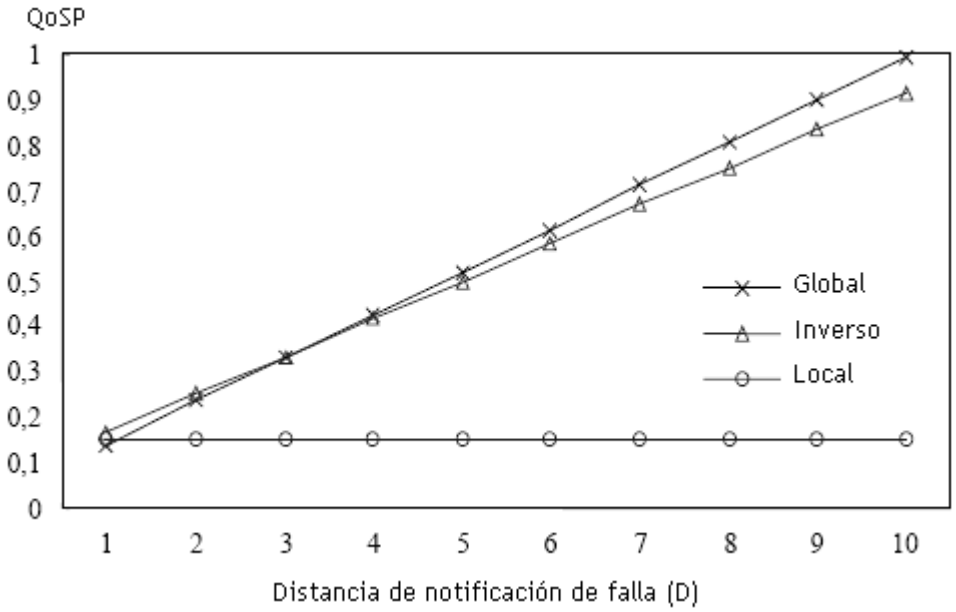


Figura 5.26 QoSP vs Distancia de notificación de falla para tráfico EF.

5.6.3 Caso 3: QoSP e influencia de la distancia

Los parámetros de esta prueba son los siguientes:

- ✓ Clase de tráfico: AF2.
- ✓ Número de enlaces a proteger: 5.
- ✓ D(i,a)= variable.
- ✓ C= 400MB.

En la figura 5.27 se observan los resultados de esta prueba, a partir de ellos se puede observar la influencia de la distancia cuando se tiene un alto número de enlaces a proteger. Para distancias cortas, se selecciona el método global, el cual proporciona una completa protección del camino de trabajo con valores de PL y RT relativamente adecuados. Sin embargo, para distancias grandes (D≥4) se selecciona el método local (pérdida de paquetes y tiempo de restablecimiento bajos). Si la distancia es mayor que 5, se observa que la elección del respaldo inverso y el global es el peor.

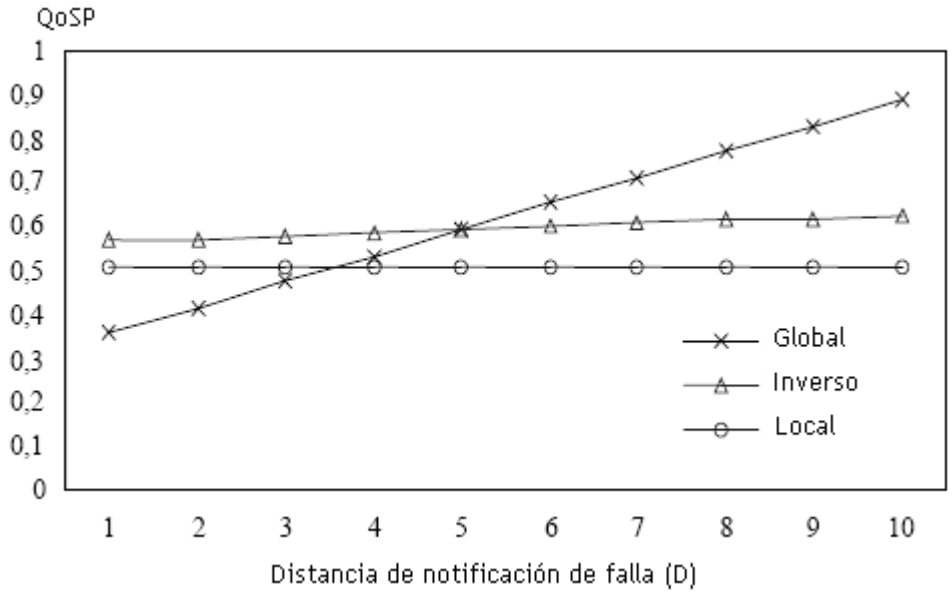


Figura 5.27 QoSP vs Distancia de notificación de falla para tráfico AF2.

Se ha completado la simulación de los casos de estudio tanto de los métodos como del mecanismo integrado de protección y se han obtenido resultados relevantes que han sido analizados. Conclusiones globales del trabajo realizado se formulan en el siguiente capítulo.

6. CONCLUSIONES Y RECOMENDACIONES

Los objetivos propuestos para este trabajo de grado se han alcanzado y al mismo tiempo se ha realizado un estudio a fondo del nivel de protección de la red. Se presentaron y probaron diversos métodos y una nueva propuesta para evaluar y mejorar la protección actual y futura de las redes MPLS.

Durante el desarrollo, se realizaron tres tareas muy concretas e importantes: Primero, se realizó la descripción y operación de MPLS, y la presentación de los argumentos que han llevado a los desarrolladores de redes de comunicaciones a señalar a esta tecnología como la más adecuada para confrontar los problemas en las redes actuales. Segundo, se enfocó en el análisis de los métodos y el desarrollo del mecanismo integrado de protección MPLS, capaces de proveer el restablecimiento confiable y rápido de los componentes de red cuando ocurre una falla, basados en políticas de restablecimiento. Y tercero, se han implementado y simulado los métodos de protección MPLS en diferentes casos de estudio y el mecanismo integrado, comparando sus resultados con topología similar; todo esto utilizando el *Network Simulator* como herramienta de simulación.

CONCLUSIONES

Respecto al trabajo mismo.

Lo que se ha discutido en este análisis, es la desventaja que puede proporcionar a la tecnología MPLS, la ocurrencia de una falla en la red si no se tiene un método de respaldo adecuado para solucionar este problema, ya que se ve afectado el tiempo de restablecimiento y la pérdida de paquetes.

Las fallas en los enlaces son una causa común de ruptura del servicio en las redes. Éstas pueden darse en enlaces de alta capacidad o entre enrutadores del backbone, afectando tanto los servicios de aplicación en tiempo real como los protocolos. Para tratar este problema se adoptaron los métodos de protección como una solución a la recuperación de los enlaces y a la integración de éstos en un solo mecanismo, para optimizar los recursos.

Se desarrolló un mecanismo de protección que integra varias de las características de los métodos de recuperación hasta ahora empleados de forma independiente en la mayoría de los modelos de red actuales, además se plantearon políticas de restablecimiento que fueron aplicadas al modelo de prueba, logrando un mejoramiento de los métodos contra fallas de acuerdo a los parámetros y a la formulación de los componentes de protección por medio de simulaciones. Para el logro de este mecanismo se definió un modelo de red MPLS de prueba a ser usado en la simulación de acuerdo a parámetros como tiempo de restablecimiento, pérdida de paquetes, consumo de recursos, entre otros; determinando así la incidencia de los métodos de protección de fallas en

redes MPLS en el desempeño de la red.

El mecanismo propuesto puede usarse para provisión de calidad de servicio, ya que este tiene criterios de desempeño que se efectúan cuando ocurre la falla y de esta manera se activa el método de respaldo. Este mecanismo se ha evaluado a través de la simulación y los resultados tiene una mejora en el retardo del paquete.

Se expuso la propuesta de este trabajo en las Jornadas de Investigación y desarrollo en Electrónica, Telecomunicaciones, Informática y Pedagógicas del 5º Encuentro TECNOCOM 2005.

Respecto a la tecnología y la protección de redes.

MPLS hace posible conmutar el tráfico a través de enrutadores IP que siempre han tenido que procesar la cabecera IP para enviar los datos con la consiguiente sobrecarga en ellos. Esto se consigue a través de la etiqueta que se ha insertado, la cual corresponde a un camino establecido.

MPLS integra las propiedades de las tecnologías orientadas a la conexión con la flexibilidad del enrutamiento de IP, lo cual permite aprovechar al máximo la capacidad en las redes actuales.

El hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte —no sólo sobre infraestructuras ATM— posibilitará de modo significativo la migración para la próxima generación de Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

MPLS es la evolución natural de las redes existentes que quieren converger en sistemas de comunicaciones que puedan soportar las capacidades necesarias que el impresionante crecimiento de Internet implica; y al mismo tiempo, que permitan a los administradores de redes controlar el tráfico en un nivel mucho más granular o especifico. El hecho de simplemente intercambiar etiquetas, en vez de la interpretación y el procesamiento de todo un encabezado IP en cada salto, provee una mejor manera de enviar paquetes, lo que al mismo tiempo ofrece la oportunidad de enviar flujos de tráfico a una mayor velocidad.

La red MPLS es una red bastante segura ya que no se permite que los datos entren o salgan del LSP por lugares que no han sido establecidos por el administrador de la red, además, cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores más que por el módulo de envío MPLS, que intercambiará la etiqueta conforme a la tabla de envío del LSR, lo que impide en gran medida que usuarios malintencionados "husmeen" la información.

Dentro de las características que implementa MPLS, respecto a las facilidades de ingeniería de tráfico se encuentra la capacidad de la red para recuperarse ante fallos y evitar perder el tráfico que se estaba cursando, por tal razón se debe considerar la selección de uno u otro método de respaldo para garantizar la demanda de Calidad de Servicio sobre todo cuando se esta en un ambiente de redes multiservicio.

El tener una visión integral sobre el problema de restablecimiento ante fallas en redes MPLS, permitirá comprender los efectos de las fallas en las redes en general y como se afectan los servicios y el tráfico que se cursa por dicha red.

La carga en la red es un aspecto importante para considerar la selección del método de respaldo, ya que cuando la carga de tráfico es baja es innecesaria la asignación de ancho de banda, sin embargo cuando la carga de la red incrementa, estos respaldos se deben hacer para garantizar la demanda de Calidad de Servicio.

Se analizaron y compararon los diferentes métodos de protección de MPLS. Los cuales preestablecen los caminos de respaldo para recuperar el tráfico después de un falla. MPLS permite la creación de diferentes tipos de respaldo debido a sus propias características, igualmente MPLS es un método conveniente para soportar ingeniería de tráfico en las redes. La creación de un LSP involucra una fase de asignación de caminos tanto de trabajo como de respaldo dónde los aspectos de QoS, (para lograr confiabilidad en la red red), deben aplicarse.

Se realizó una revisión de las técnicas principales de notificación de falla, ya que la técnica basada en señalización es la que se usa actualmente.

Respecto a la simulación y las herramientas.

A la hora de diseñar un modelo de red se debe realizar previamente un análisis de confiabilidad de ésta, ya que éste estudio es crucial para optimizar el diseño de la red ofreciendo una adecuada protección dependiendo del impacto de la falla. Se propuso un mecanismo integrado de protección en un escenario estático para evaluar el desempeño de cada uno de los métodos basado en políticas de restablecimiento de acuerdo a la distancia donde ocurra la falla en el enlace.

Se analizaron en profundidad todos los pasos para la recuperación del tráfico, desde que ocurre la falla y se realiza la conmutación al camino de respaldo hasta el restablecimiento del camino de trabajo.

Se simularon tres casos de estudio y el mecanismo integrado en los que se plantearon los diferentes métodos de protección en un dominio MPLS, con un mismo escenario. Los resultados fueron analizados y comparados, por lo que se puede concluir que:

Independiente de la técnica de notificación de falla, los resultados han demostrado que el método de respaldo local mejora los tiempos de restablecimiento y reduce al mínimo el impacto de falla (retardo y pérdida de paquetes) y optimiza el consumo de recursos de la red (para un solo segmento protegido).

La señal de indicación de falla y los mensajes de activación del camino de respaldo se deben enviar tan rápido como sea posible para reducir el tiempo de restablecimiento de falla. En este caso para los enlaces, éstos adicionan un retardo proporcional al tiempo de propagación y al

tiempo de transmisión.

En este estudio se le ha dado prioridad tanto al tiempo de restablecimiento como a la pérdida de paquetes, ya que la distancia, número de los saltos (enlaces), en las políticas de restablecimiento determinan el método de protección que se ejecutará en el mecanismo integrado cuando ocurra una falla.

Cada caso de estudio fue analizado con diversas variables de comparación, las cuales permitieron observar el desempeño de cada método por separado y del mecanismo integrado. Lo cual permitió ver como la protección no permite que el enlace se anule, ya que sólo se cae durante un determinando tiempo mientras se restablece nuevamente éste.

En las redes futuras el tiempo de restablecimiento espera ser reducido y el ancho de banda del enlace ampliado, reduciendo el tiempo de transmisión. Sin embargo, en redes grandes los ISPs, con grandes enlaces (centenares de kilómetros), el tiempo de la propagación es el único aspecto que no puede ser reducido. En este caso la protección del segmento (respaldo local) se elige como la técnica más conveniente de protección, a pesar de que su implementación sea mucho más costosa que los otros dos respaldos (global e inverso).

Nuestra propuesta mejora la confiabilidad de la red y reduce el impacto de falla, aplicando en un mismo dominio MPLS los diferentes métodos de protección. Sin embargo, no todos los servicios actuales y futuros del tráfico requerirán el mismo nivel de protección. Por otra parte, en algunos casos mejorar el nivel de protección implica que los métodos sean más costosos en el restablecimiento de la falla (en términos del consumo de recursos) que no se pueden desplegar en toda la red. Los resultados han demostrado que se puede obtener un alto nivel de protección con un consumo de recursos racional usando clasificación de servicios.

El uso del NCTUns 2.0 no fue posible debido a que este simulador no tiene un módulo MPLS y después de un tiempo intentando trabajar con él, se concluyó que la implementación de éste modulo sería tema para todo un proyecto.

Se uso el NS como herramienta de simulación para MPLS debido a las posibilidades que este programa ofrece, ya que se ha ido mejorando y ampliando poco a poco, no solo por los desarrolladores, sino por todo tipo de usuarios. Es por esto que NS con su modulo MNS resulta ser una buena herramienta para la simulación de redes MPLS.

Los Operadores de Red y los Proveedores de Servicio de Internet pueden usar esta metodología para evaluar el desempeño de sus redes desde el punto de vista de protección. Sin embargo la propuesta y la formulación de esta, les permitirá a los proveedores analizar el grado de protección de sus redes y encontrar la estrategia mas adecuada en términos de requerimientos de protección.

RECOMENDACIONES

El uso del NS deja la puerta abierta a un sin fin de aplicaciones. El NS es muy interesante para fines didácticos, por lo que se puede sugerir algún trabajo futuro que se enfoque enteramente a la utilización de NS. Para esto, sería necesario instalar la versión no compilada, con lo que se tiene la posibilidad de aplicar todas las extensiones con que cuenta NS: RSVP, ATM, DiffServ, QoS, wireless, etc.

Este trabajo comienza con la tecnología basada en MPLS. Sin embargo, un análisis profundo de la tecnología de red óptica actual y futura (GMPLS) se debe considerar para un trabajo futuro, considerando las arquitecturas ópticas del nodo para calcular el tiempo de restablecimiento de falla. También debe ser incluido un estudio más detallado de GMPLS.

En el capítulo 3 se presenta un mecanismo integrado para reducir el impacto de falla dependiendo de la distancia en un escenario estático y con falla simple en los enlaces. Sin embargo, este mecanismo se basa en un modelo de red de prueba. Un análisis profundo de este mecanismo con un escenario dinámico y con múltiples fallas tanto en enlaces como en los nodos para la tecnología de red actual se debe considerar para un trabajo futuro.

Otras áreas que emergen en la protección de la red, tal como p-ciclos y grupos de riesgo compartidos (nodos y enlaces), no se han considerado en este trabajo. Sin embargo, muchos de los escenarios propuestos y de la evaluación del nivel de protección de la red pueden ser aplicadas fácilmente.

Trabajar con algunos algoritmos actuales de enrutamiento con QoS para ofrecer una mejor protección de la red y optimización de recursos.

Que este trabajo de grado se tome como un módulo de gestión de las FCAPS, en este caso particular se tendría el módulo de Falla; quedando como trabajo futuro implementar los módulos restantes, buscando como finalidad integrarlos y poder trabajar con éste en las materias relacionadas con este tema.

Trabajar sobre la posible implementación de un pequeño laboratorio donde los estudiante puedan manipular tanto el simulador NS2 como los scripts que se han implementado en este trabajo de grado.

BIBLIOGRAFÍA

[1] Rosen, E. et al., "Multiprotocol Label Switching Architecture". RFC 3031. Enero, 2001.

[2] Martin, P. et al., "Summary of MPLS". White paper, 2004.

[3] Barberá, J., "MPLS: Una arquitectura de backbone para la Internet del siglo XXI". Febrero, 1999. http://www.aui.es/biblio/libros/mi2000/Jose%20Barbera.

[4] International Engineering Consortium. "MPLS Tutorial", 2003, http://www.iec.org/online/tutorials/mpls/. 2003.

[5] Ixia, "Multi-Protocol Label Switching (MPLS) Conformance and Performance Testing". White paper, 2004.

[6] Gallaher, R., "An introduction to MPLS". 1999, http://www.convergedigest.com/Bandwidth/archive/010910TUTORIALrgallaher1.htm.

[7] Holness, F., "Congestion Control Mechanisms within MPLS Networks", Septiembre, 2000.

[8] Andersson, L. et al., "LDP Specification", RFC 3036. Enero, 2001.

[9] Pulley, R. et al., "A Comparison of MPLS Traffic Engineering Initiatives". NetPlane Systems, Inc. 2000.

[10] Awduche, D. et al., "Requirements for Traffic Engineering over MPLS", RFC 2702, Septiembre, 1999.

[11] Butenweg, S., "Two distributed reactive MPLS Traffic Engineering mechanisms for throughput optimization in Best Effort MPLS networks". White paper, 2003.

[12] Chung, J., "Analysis of MPLS Traffic Engineering". White paper, 2000.

[13] Praveen, B. et al., "Quality of Service using Traffic Engineering over MPLS: An Analysis". Marzo, 1999.

[14] Sharma, V. et al., "Framework for MPLS-based Recovery ". Internet Draft draft-ietfmpls-recovery-frmwrk-02.txt, IETF. 2001.

[15] Calle, E. et al., "A Dynamic Multilevel MPLS Protection Domain". Budapest. Tibor Cinkler. 2001.

[16] Banimelhem, O. et al., "Resiliency Issues in MPLS Networks". Montreal. IEEE. 2003.

[17] Makam, S. et al., "Protection/Restoration of MPLS Networks" (work in progress). Internet Draft draft-makam-mpls-protection, Octubre, 1999.

[18] Huang, C. et al., "A Path Protection/Restoration Mechanism for MPLS Networks" (work in progress). Internet Draft draft-chang-mplspath-protection, Julio, 2000.

[19] Kini, S. et al., "Shared backup Label Switched Path restoration" (work in progress). Internet Draft draft-kini-restorationshared-backup, Octubre, 2000.

[20] Haskin, D. et al. "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute" (work in progress). Internet Draft draft-haskin-mpls-fastreroute, Noviembre, 2000.

[21] Krishnan, R. et al. "Extensions to RSVP to Handle Establishment of Alternate Label-Switched-Paths for Fast Reroute" (work in progress). Internet Draft draftkrishnan-mpls-reroute-resvpext-00.txt, Junio, 1999.

[22] Bartos, R. et al., "A Heuristic Approach to Service Restoration in MPLS Networks". Durham. CNRG.2003.

[23] Huang, Ch. et al., "Building reliable MPLS Networks using a path protection mechanism", IEEE Communications Magazine, Marzo, 2002.

[24] Autenrieth, A., "Recovery Time Analysis of Differentiated Resilience". White paper, 2003.

[25] Berger, L. (Editor) et al., "Generalized MPLS Signaling-RSVP-TE Extensions", IETF RFC 3473. Enero, 2003.

[26] Foo, J., "A Survey of Service Restoration Techniques in MPLS Networks". White paper, 2003.

[27] Marzo, L. et al., "QoS On-Line Routing and MPLS Multilevel Protection: a Survey". IEEE Communications Magazine, Octubre, 2003.

[28] Rabbat, R. et al., "Extensions to LMP for Floodingbased Fault Notification," Internet Draft (work in progress), Junio, 2003.

[29] Harrison, A. et al., "Protection and Restoration in MPLS Networks". Data Connection Limited, Octubre, 2001.

[30] Joaquí, L. Et al., "MPLS y sus Métodos de Protección contra Fallas". Medellín. JIDTEL-Tecnocom. 2005. ISBN 958-655-887-8.

[31] Sharma, V. et al., "Framework for MPLS-based Recovery". Work in progress, internet draft <draft-ietf-mpls-recovery-frmwrk-08.txt>. October 2002.

[32] Calle, E. et al., "Protection Performance Components in MPLS Networks". Girona. IEEE. 2003.

[33] Wang, S., "The GUI User Manual for the NCTUns 2.0 Network Simulator and Emulator". Taiwan. Enero, 2005.

[34] Network Simulator Homepage, URL: http://www.isi.edu/nsnam/ns/ns-build.html

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

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

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

[38] UCB/LBNL/VINT, "ns manual", URL: http://www-mash.es.berkeley.edu/ns/ns-nam.html

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

[40] Facheur, F. et al., "Requirements for support of Diff-Servaware MPLS traffic engineering". IETF RFC 3270. Mayo, 2002.

[41] Marzo, L. et al. "Adding QoS Protection in Order to Enhance MPLS QoS Routing". Anchorage, Alaska (USA). IEEE 2003.

REREFENCIAS WEB

[42] Página de ns-2: http://www.isi.edu/nsnam/ns/
[43] Manual de ns: http://www.isi.edu/nsnam/ns/doc/index.html
[44] Tutorial de ns de Marc Greis: http://www.isi.edu/nsnam/ns/tutorial/index.html
[45] NS by Example: http://nile.wpi.edu/NS/
[46] Congestion Control Research Group: http://perform.wpi.edu/cc/
[47] VINT Project Home Page: http://www.isi.edu/nsnam/vint/
[48] Instalación NS: http://www.isi.edu/nsnam/ns/ns-build.html
[49] Documentación NS: http://www.isi.edu/nsnam/ns/ns-documentation.html
[50] Historia NS CVS (estructura del directorio): http://www.isi.edu/cgi-bin/nsnam/cvsweb
[51] Jerarquía de Clases NS: http://www-sop.inria.fr/rodeo/personnel/Antoine.Clerget/ns
[52] Tutorial/workshop 5th VINT/NS Simulator http://www.isi.edu/nsnam/ns/ns-tutorial/ucb-

tutorial.html
[53] Guia de referncia rápida Tcl/Tk: http://www.slac.stanford.edu/~raines/tkref.html
[54] Tutorial OTcl (Versión Berkeley): http://bmrc.berkeley.edu/research/cmt/cmtdoc/otcl
[55] Tutorial OTcl (Versión MIT): ftp://ftp.tns.lcs.mit.edu/pub/otcl/README.html
[56] XGraph: http://jean-luc.ncsa.uiuc.edu/Codes/xgraph
[57] Network Animator (NAM): http://www.isi.edu/nsnam/nam/
[58] NCTUns 2.0: http: //nsl10.csie.nctu.edu.tw

ANEXO

ANEXO A - NETWORK SIMULATOR (NS-2)