# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA


MPLS/GMPLS SOBRE LAS REDES ÓPTICAS

**INFORME DE SUFICIENCIA**

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO ELECTRÓNICO**

**PRESENTADO POR:**

**JUAN FREDY HUAMALI NINANYA**

**PROMOCIÓN**
**1998 - II**

**LIMA – PERÚ**
**2006**

# MPLS/GMPLS SOBRE LAS REDES OPTICAS

*Dedico este trabajo a Dios por otorgarme una vida llena de oportunidades y a la UNI por haberme acogido en sus aulas, donde aprendí a consolidarme como un buen profesional.*

## SUMARIO

En estos últimos años se ha producido un incremento exponencial del tráfico de datos, debido principalmente a la proliferación de Redes Privadas Virtuales y a la diversidad de servicios de Internet. Entonces, existe la necesidad de encontrar arquitecturas y protocolos de comunicaciones, que proporcionen una calidad de servicio a las distintas aplicaciones y funciones que faciliten la Ingeniería de Tráfico. Como una solución a este problema y a las necesidades planteadas en el se presenta y analiza el *MultiProtocol Label Switching* (MPLS), que esta ubicado entre la capa de enlace y la capa de red. Sin embargo; los trabajos basados en este protocolo presentan limitaciones de enrutamiento, señalización, distribución de etiquetas, reserva de recursos y gestión del enlace; por esta razón se proponen extensiones que resuelvan estas deficiencias a través del MPLS Generalizado (GMPLS). Estas arquitecturas se describirán en los capítulos I y II y serán enfocadas a las redes ópticas, porque actualmente existe la tendencia al establecimiento de una arquitectura de red de dos capas; la capa de enrutamiento IP y la capa de transmisión óptica; siendo la conexión entre ellas el GMPLS.

## ÍNDICE


**PRÓLOGO** 1

**CAPÍTULO I**
**ARQUITECTURA DEL MPLS** 3
1.1 Introducción 3
1.2. Conceptos básicos del MPLS 5
1.2.1 Etiquetas 5
1.2.2 Protocolo de distribución de etiquetas 6
1.2.3 Pila de etiquetas 7
1.2.4 Trueque de etiquetas 9
1.2.5 Label Switched Path 9
1.2.6 Extrayendo etiquetas en el penúltimo salto (Penultimate Hop Popping) 10
1.2.7 Etiquetas de entrada inválidas 11
1.2.8 Control del LSP: ordenado versus independiente 12
1.2.9 Agregación 13
1.2.10 Selección de una ruta 14
1.2.11 Tiempo de vida (TTL) 15
1.2.12 Codificación de etiquetas 16
1.3 Mezcla de etiquetas 18
1.3.1 LSRs sin mezcla 19
1.3.2. Etiquetas para LSRs con mezcla y sin mezcla 19
1.4 Transporte del protocolo de distribución de etiquetas 20
1.4.1 BGP y LDP 20
1.4.2 Etiquetas y especificaciones de flujo RSVP 21
1.4.3 Etiquetas para LSPs enrutados explícitamente 21

**CAPITULO II**
**ARQUITECTURA DEL GMPLS** 22
2.1 Introducción 22
2.2 Conceptos básicos del GMPLS en las redes ópticas 23

2.2.1 Etiquetas generalizadas 23
2.2.2 Asignaciones de ancho de banda 25
2.2.3 Solicitando etiquetas generalizadas 25
2.2.4 Restringiendo la elección de etiqueta 26
2.2.5 Conjunto de etiquetas 26
2.2.6 Control de etiqueta explícita 27
2.2.7 Control de etiqueta de salida 28
2.3 Tipos de conmutación y jerarquías de envío 28
2.3.1 Interfases capaces de conmutar paquetes (PSC: Packet Switch Capable) 28
2.3.2 Interfases capaces de conmutar en capa 2 (L2SC: Layer 2 Switch Capable) 29
2.3.3 Interfases capaces de multiplexación por división por Tiempo (TDM: Time Division Multiplex Capable) 29
2.3.4 Interfases capaces de conmutar lambdas (LSC: Lambda Switch Capable) 29
2.3.5 Interfases capaces de conmutar fibras (FSC: Fiber Switch Capable) 29
2.4 Modelos de enrutamiento y direccionamiento 30
2.4.1 Direccionamiento de niveles PSC y no PSC 32
2.4.2 Mejoras de escalabilidad GMPLS 32
2.4.3 Extensiones TE para los protocolos de enrutamiento IP 32
2.4.4 Enlaces no numerados 33
2.5 Enlace agrupado 34
2.5.1 Restricciones en los agrupamientos 35
2.5.2 Consideraciones de enrutamiento para el agrupamiento 35
2.5.3 Consideraciones de señalización 36
2.5.4 Enlace agrupado sin numerar 37
2.6 Adyacencias de envío (FA: Forwarding Adjacency) 37
2.6.1 Adyacencias de enrutamiento y envío 38
2.6.2 Adyacencias de enrutamiento y señalización 38
2.7 Bidireccionalidad 39
2.7.1 Confirmando la ruta de envío 39
2.8 Señalización generalizada 41
2.9 Señalización fuera de banda 42

2.9.1 Cálculo del enrutamiento extendido 43
2.9.2 Encapsulación del mensaje de señalización 43
2.9.3 Identificación de la interfase de datos 43
2.9.4 Retardo de señalización 44
2.10 Gestión del enlace 45
2.10.1 Protocolo de gestión del enlace (LMP) 46
2.10.2 LMP para DWDM (OLSs: Optical Line Systems) 51
2.11 Gestión de la red 53
2.11.1 Sistemas de gestión de la red (NMS) 53
2.11.2 Management Information Base (MIB) 54
2.11.3 Herramientas 54
2.11.4 Correlación de fallo entre múltiples niveles 54
2.12 UNI Óptico 55
2.12.1 Modelo puerto 56
2.12.2 Modelo superpuesto 57
2.12.3 Servicios UNI 58
2.12.4 Direccionamiento y encaminamiento 59
2.12.5 Realización de la UNI en los protocolos GMPLS 60

**CAPITULO III**
**IMPLEMENTACION DEL GMPLS** 61
3.1 Mejoras del GMPLS sobre el MPLS-TE 61
3.2 Implementación del G MPLS 62

**CAPITULO IV**
**BENEFICIOS AL IMPLEMENTAR GMPLS** 64
4.1 Técnicas de protección y restauración 64
4.1.1 Mecanismos de protección 65
4.1.2 Mecanismos de restauración 67
4.2 El plano de control de GMPLS 68

**CONCLUSIONES** 70
**GLOSARIO DE ACRÓNIMOS** 72
**BIBLIOGRAFÍA** 75

## GLOSARIO DE ACRÓNIMOS

| | |
|---|---|
| ADM | Add Drop Multiplex |
| APS | Automatic Protection Sonet |
| AS | Autonomous System |
| ATM | Asynchronous Transfer Mode |
| BER | Bit Error Rate |
| BGP | Border Gateway Protocol |
| CLI | Command Line Interfase |
| CR-LDP | Constraint-based Routing LDP |
| CSPF | Constraint-based Shortest Path First |
| DLCI | Data Link Circuit Identifier |
| DWDM | Dense Wavelength Division Multiplexing |
| ERO | Explicit Route Object |
| FA | Forwarding Adjacency |
| FEC | Forwarding Equivalence Class |
| FSC | Fiber Switched Channel |
| FTN | Fec To Nhlfe map |
| GMPLS | Generalized Multi-Protocol Label Switching |
| IGP | Interior Gateway Protocol |
| ILM | Incoming Label Map |
| IP | Internet Protocol |
| IS-IS | Intermediate System to Intermediate System. |
| IETF | Internet Engineering Task Force |
| LDP | Label Distribution Protocol |
| LMP | Link Management Protocol |
| LOL | Loss Of Light |
| LPT | Link Protection Type |
| LSA | Link State Advertisment |
| LSC | Lambda Switched Channel |
| LSP | Label Switched Path |
| LSR | Label Switched Router |

# PRÓLOGO

El presente trabajo tiene por finalidad realizar un estudio de la arquitectura *MultiProtocol Label Switching* y de sus extensiones definidas en el *Generalized MPLS*; porque en la actualidad se requieren tecnologías que proporcionen Calidad de Servicio, Ingeniería de Tráfico y que puedan operar con las redes ópticas de alta velocidad. De esta forma se podrían ofrecer estos servicios a la Internet, que se ha consolidado como el modelo de red pública ya que transporta datos a grandes escalas y sus protocolos TCP/IP se han establecido como estándares. Todos estos requerimientos son resueltos con el GMPLS.

En las redes actuales, el tráfico de datos ha sobrepasado enormemente al tráfico de voz; además existe la necesidad de transportar aún más tráfico, pero de una manera más eficiente en cuanto a los costos de implementación y mantenimiento; por estas razones se plantea una arquitectura de red de datos basada en dos capas; la capa de enrutamiento IP y la capa de transmisión óptica que interactuarán a través del GMPLS; que podría tener ventajas sobre la arquitectura tradicional, que consta de cuatro capas: IP para el transporte de aplicaciones y servicios, *Asynchronous Transfer Mode* (ATM) para Ingeniería de Tráfico, *Synchronous Optical NETwork / Synchronous Digital Hierarchy* (SONET/SDH) para transporte y *Dense Wavelength Division Multiplexing* (DWDM) para la capacidad, es lenta para escalar y transportar los grandes volúmenes de datos, además de que las soluciones planteadas en torno a este esquema son muy costosas.

El transporte efectivo debe optimizar los costos de la multiplexación de datos así como la conmutación de datos sobre un amplio rango de volúmenes de tráfico, estos puntos son tratados por el DWDM, que incrementa la capacidad de transporte y ancho de banda de una sola fibra creando efectivamente múltiples fibras virtuales. Esto permite multiplicar el ancho de banda, manteniendo la misma infraestructura de fibra. Asimismo, dispositivos ópticos como los OXC (*Optical Cross-Connects*), están emergiendo como la opción preferida para la conmutación de flujos de datos ya que se evita el procesamiento electrónico por paquete. Considerando también la hegemonía del TCP/IP es que se plantea la arquitectura de dos capas; consiguiendo así una red más simple, eficiente y de costo moderado.

En el capítulo I se abordará la arquitectura del MPLS, que es un mecanismo de enrutamiento flexible que está basado en la asignación de flujos en rutas de extremo a extremo dentro de un Sistema Autónomo; es decir, suministra enlaces virtuales o túneles a través de la red conectando nodos que se ubican en sus fronteras. Entre las principales características se destacan la división de los planos de control y de envío; el mecanismo de control se encarga básicamente de la creación de rutas, que implica la creación de tablas de enrutamiento, y la señalización de las rutas. El plano de envío es el encargado de la conmutación de paquetes a través del intercambio de etiquetas, que crearán las Trayectorias de Conmutación de Etiquetas (*Label Switching Path*: LSPs). Las etiquetas son insertadas al comienzo del paquete en la entrada de la red MPLS; en cada salto el paquete es enrutado según el valor de la etiqueta y sale por la interfase correspondiente con otro valor de etiqueta; se obtiene una gran rapidez en la conmutación gracias a que las etiquetas son insertadas al principio del paquete y son de longitud fija. Las etiquetas se distribuyen utilizando protocolos de señalización.

El MPLS presenta limitaciones de enrutamiento, señalización, distribución de etiquetas y reserva de recursos cuando opera con redes ópticas de alta velocidad; es por ello que se utilizan extensiones a este protocolo agrupadas por el GMPLS, que se describen en el capítulo II.

En los capítulos III y IV se describen la forma de implementación y los beneficios que se lograrían con el GMPLS; porque establecida la arquitectura de dos capas, GMPLS efectuaría el plano de control sobre estas.

# CAPITULO I
# ARQUITECTURA DEL MPLS

En el presente capítulo se abordarán, los conceptos y técnicas para la construcción de la arquitectura *MultiProtocol Label Switching*. El MPLS [1] fue desarrollado como una tecnología basada en paquetes; actualmente se viene utilizando en las redes troncales y en las redes de voz y datos. El MPLS no sustituye al enrutamiento IP (*Internet Protocol*), sino que puede funcionar al lado de las tecnologías existentes y futuras de enrutamiento, teniendo como finalidad suministrar enrutamiento de datos a muy alta velocidad entre LSRs – Enrutadores de Conmutación de Etiquetas (*Label Switched Routers*) junto con la reserva de ancho de banda para flujos de tráfico con distintos requerimientos de QoS – Calidad de Servicio (*Quality of Service*).

## 1.1. Introducción

Cuando un paquete de un protocolo de nivel de red no orientado a conexión, viaja de un enrutador al siguiente, cada enrutador elige de forma independiente el próximo salto del paquete, basado en el análisis de la cabecera del paquete y en el resultado del empleo del algoritmo de enrutamiento.

En el envío convencional IP, generalmente el enrutador considerará que dos paquetes son de la misma FEC (*Forwarding Equivalence Class*) [1], si tienen el mismo prefijo en la dirección de destino de cada paquete. A medida que el paquete atraviesa la red, en cada salto se reexamina el paquete y se le asigna una FEC.

En MPLS, la asignación de un determinado paquete a una determinada FEC se hace solo una vez y es cuando el paquete entra en la red. La FEC a la cual se asigna el paquete se codifica como un valor corto de longitud fija conocido como etiqueta. Cuando un paquete es enviado a su salto siguiente, la etiqueta es enviada con él; así los paquetes son etiquetados antes de ser enviados.

En los saltos siguientes, no hay más análisis de la cabecera del nivel de red del paquete. Más bien la etiqueta se usa como un índice en la tabla que especifica el próximo salto y la

nueva etiqueta. La etiqueta vieja es sustituida por la nueva y el paquete es enviado al salto siguiente. Todo el envío es dirigido por las etiquetas. Esto tiene ventajas sobre el envío de nivel de red convencional porque:

El envío MPLS puede ser hecho por conmutadores que son capaces de poner etiqueta y sustituirla, pero no son capaces de analizar las cabeceras de nivel de red a la velocidad adecuada.

Desde que un paquete es asignado a una FEC cuando entra en la red, el enrutador de entrada puede usar cualquier información que tiene el paquete, aunque esa información no pueda ser recogida de la cabecera del nivel de red. Por ejemplo, los paquetes que llegan de diferentes puertos se pueden asignar a diferentes FECs. El envío convencional, por otro lado, solo puede considerar la información que viaja con el paquete en la cabecera del paquete.

Un paquete que entra en la red por un enrutador determinado puede ser etiquetado diferentemente si el mismo paquete entra a la red por otro enrutador y como resultado de las decisiones de envío que depende del enrutador de entrada se puede hacer más fácil. Esto no puede ser hecho con el envío convencional, ya que la identidad del enrutador de entrada del paquete no viaja con el paquete.

A veces es deseable forzar un paquete a seguir una determinada ruta, antes de que se elija por el algoritmo de enrutamiento. Esto se puede hacer como un asunto de política o soporte de la Ingeniería de Tráfico. En el envío convencional, esto requiere que el paquete lleve un código de su ruta con él (*source routing*). En MPLS, se puede usar una etiqueta para representar la ruta, por lo tanto, la identidad de la ruta explícita no necesita ser llevada con el paquete.

Algunos enrutadores analizan la cabecera del nivel de red del paquete no solo para elegir el próximo salto del paquete, sino también para determinar la procedencia o clase de servicio del paquete aplicando diferentes umbrales de descarte o disciplinas de programación. MPLS permite (pero no requiere) que la procedencia o la clase de servicio sea completamente o parcialmente inferida de la etiqueta. En este caso, uno puede decir que la etiqueta representa la combinación de una FEC y una procedencia o clase de servicio.

## 1.2. Conceptos básicos del MPLS

A continuación detallamos conceptos acerca de la arquitectura del MPLS.

### 1.2.1 Etiquetas

Una etiqueta es un identificador, de longitud corta y fija que se usa para identificar una FEC. Un paquete es asignado a una FEC en base a su dirección de destino de nivel de red. Sin embargo, la etiqueta nunca es una codificación de esa dirección.

La fig. 1.1 muestra la operación básica del MPLS, se observan dos flujos de datos desde el dispositivo X: uno a Y, el otro a Z, a través de dos LSPs.

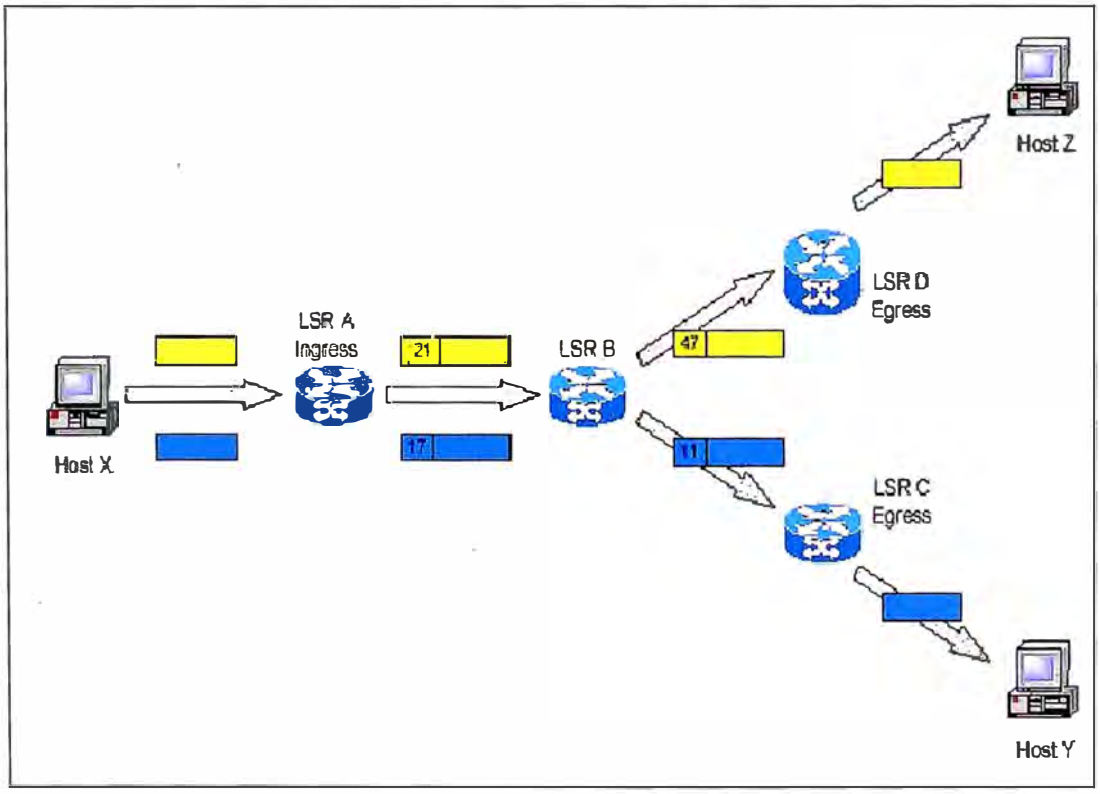


Fig. 1.1: Funcionamiento básico del MPLS

El LSR A es un punto de entrada de la red MPLS para los datos del dispositivo X. Cuando recibe paquetes desde X, el LSR A determina la FEC de cada paquete, deduce el LSP a usar y añade una etiqueta al paquete, después el LSR A envía el paquete a la interfase apropiada del LSP.

El LSR B es un LSR intermedio de la red MPLS. Simplemente toma cada paquete etiquetado y usa el par {interfase de entrada, valor de la etiqueta} para decidir el par {interfase de salida, valor de etiqueta} con el que enviará el paquete. Este procedimiento puede usar una simple tabla de búsqueda y se puede realizar en hardware, junto con el cambio del valor de la etiqueta y el enrutamiento del paquete. Esto permite que las redes MPLS se construyan con el hardware existente de conmutación de etiqueta como el ATM y el *Frame Relay*. Esta forma de enrutar paquetes de datos es potencialmente mucho más rápida que el examinar toda la cabecera del paquete para decidir el próximo salto. En la fig. 1.1, cada paquete con valor de etiqueta 21 será enviado por la interfase hacia el LSR D con el valor de etiqueta 47. Los paquetes con el valor de etiqueta 17 serán reetiquetados con el valor 11 y enviados hacia el LSR C.

El LSR C y el LSR D actúan como LSRs de salida de la red MPLS. Estos LSRs realizan la misma búsqueda que los LSRs intermedios, pero el par {interfase de salida, valor etiqueta} marca el paquete como saliendo por el LSP. Los LSRs de salida eliminan las etiquetas de los paquetes y los envían usando enrutamiento de nivel 3.

Si el LSR A identifica que todos los paquetes son para el destino Z, los enrutará por el LSP de arriba y los etiquetará con el valor 21, ellos serán satisfactoriamente enviados a través de la red.

El formato exacto de una etiqueta y como se añade al paquete depende de la tecnología de enlace de nivel 2 usado en la red MPLS. Una etiqueta podría corresponder a un VPI/VCI (*Virtual Path Identifier / Virtual Circuit Identifier*) de ATM, un DLCI (*Data Link Circuit Identifier*) de *Frame Relay*, una fibra, una longitud de onda DWDM o a una ranura de tiempo TDM (*Time Division Multiplexing*).

Un paquete etiquetado es un paquete codificado, la etiqueta puede residir en la cabecera del nivel de red o del nivel de enlace y dependiendo de la técnica de codificación a usar, debe estar de acuerdo con ambas entidades que codifican y decodifican la etiqueta.

### 1.2.2 Protocolo de distribución de etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un LSR informa a otro de las relaciones etiqueta/FEC que ha hecho. Las tablas de enrutamiento de cada LSR deben ser llenadas con los mapeos de {interfase de entrada,

valor etiqueta} a {interfase de salida, valor etiqueta}. Dos LSRs que usan un protocolo de distribución de etiquetas para intercambiar la información de las relaciones etiqueta/FEC se les conoce como "puertos de distribución de etiquetas". Si dos LSRs son puertos de distribución de etiquetas, diremos que hay una "distribución de etiquetas adyacentes" entre ellos. El protocolo de distribución de etiquetas también abarca las negociaciones de los dos puertos de distribución de etiquetas que necesitan comunicarse con el fin de aprender de las posibilidades MPLS del otro.

La arquitectura no asume que hay solamente un único protocolo de distribución de etiquetas. De hecho, están siendo estandarizados varios protocolos de distribución de etiquetas. Los protocolos existentes han sido ampliados de forma que puedan distribuir etiquetas de forma "*piggybacked*" (Esta técnica consiste en enviar la trama ACK dentro de la trama de datos y no por separado; porque la trama ACK contiene una cantidad mínima de información útil y mas aún, cuando se transmiten datos en ambas direcciones es más eficiente realizar esto, porque se ahorra el envío de una trama); por ejemplo MPLS-BGP [3], MPLS-RSVPTUNNELS [4], MPLS-LDP [5], MPLS-CR-LDP [11].

La arquitectura MPLS permite a un LSR solicitar explícitamente una relación de etiqueta/FEC, desde el salto siguiente de esta FEC; a esto se le conoce como distribución descendente de etiquetas bajo demanda (*downstream-on-demand label distribution*), y cuando el LSR distribuye estas relaciones al LSR que no las ha solicitado explícitamente; a esto se le conoce como distribución descendente de etiquetas sin solicitud (*unsolicited downstream label distribution*).

Un LSR puede recibir información de asociaciones de etiquetas a FECs que no use. Por tanto, un LSR podrá guardar dicha información o descartarla, a esto se denomina modos de retención de etiquetas que se especifican de la siguiente forma: Sí un LSR soporta el "Modo Liberal de Retención de Etiquetas", mantiene las relaciones etiqueta/FEC que son recibidas de los LSRs que no están en el salto siguiente para esta FEC (La ventaja de este modo es cuando ocurre un cambio en la topología, las etiquetas de la nueva topología estarán ya en el LSR, el inconveniente de este modo es que requiere bastante memoria). Si un LSR soporta el "Modo Conservador de Retención de Etiquetas", descarta estas relaciones (La ventaja de este modo es que requiere menos memoria que el modo anterior, pero el inconveniente de este modo es el costo en tiempo en la obtención de nuevas etiquetas ante un cambio en la topología); en conclusión, el Modo Liberal de Retención de Etiquetas permite una adaptación más rápida a los cambios de

enrutamiento, sin embargo el Modo Conservador de Retención de Etiquetas requiere mantener menor número de etiquetas en el LSR.

### 1.2.3 Pila de etiquetas

El modelo más general es que un paquete etiquetado tenga varias etiquetas, organizadas como una pila LIFO (*Last-In, First-Out*), esto es una pila de etiquetas. MPLS soporta una jerarquía de etiquetas, el proceso de un paquete etiquetado es completamente independiente del nivel de la jerarquía. El proceso está basado en la etiqueta superior de la pila, un paquete sin etiqueta es como si fuera un paquete cuya pila de etiquetas está vacía (profundidad de la pila de etiquetas es 0). Si la profundidad de una pila de etiquetas de un paquete es ***m***, nos referimos a la etiqueta del fondo de la pila como etiqueta de nivel 1, a la siguiente como etiqueta de nivel 2 y así hasta llegar a la etiqueta superior que será la etiqueta de nivel ***m***.

Una característica clave del MPLS es que una vez que las etiquetas requeridas para un LSP han sido intercambiadas entre los LSRs que soportan el LSP, los LSRs intermedios que forman parte del LSP no necesitan examinar el contenido de los paquetes de datos que fluyen por el LSP. Por esta razón a menudo los LSPs se consideran que forman túneles a través de toda, o parte, de la red troncal MPLS. Un túnel transporta datos opacos (o paquete tunelado porque son paquetes encapsulados dentro de un paquete de nivel de red cuya dirección destino es el LSR de salida) entre los LSRs de entrada y salida del túnel.

Las pilas de etiquetas ayudan a reducir tanto el tamaño de las tablas de enrutamiento que necesitan ser mantenidas en los LSRs de la red troncal así como la complejidad de gestión del envío de los datos a través de la red troncal. Una pila de etiquetas se organiza con la etiqueta para el túnel más exterior como la de más arriba y la etiqueta para el LSP más interior con la del fondo. En el cable (o fibra) la etiqueta superior (nivel ***m***) se transmite primero y es la única etiqueta usada para enrutar el paquete hasta que es sacada de la pila y es cuando la etiqueta de nivel ***m-1*** se convierte en la etiqueta superior.

La NHLFE (*Next Hop Label Forwarding Entry)* es la etiqueta de entrada a usar para el próximo salto. Se usa cuando se envía un paquete etiquetado, contiene la información siguiente:

1. El próximo salto del paquete.
2. La operación a realizar en la pila de etiquetas del paquete es:
    a) Sustituir la etiqueta en la parte superior de la pila con una etiqueta nueva.
    b) Sacar una etiqueta de la pila.
    c) Sustituir la etiqueta de la parte superior de la pila con una etiqueta nueva, y entonces poner una o más etiquetas nuevas en la pila de etiquetas.
    d) La encapsulación del enlace de datos cuando se transmite el paquete.
    e) La forma de codificar la pila de etiquetas cuando se transmite el paquete.
    f) Cualquier otra información necesaria con el fin de disponer de forma adecuada el paquete.

El ILM (*Incoming Label Map*) mapea cada etiqueta de entrada a un conjunto de NHLFEs. Se usa cuando los paquetes enviados llegan como paquetes etiquetados. Si el ILM mapea una etiqueta concreta a un conjunto de NHLFEs que contiene más de un elemento, entonces el elemento del conjunto se debe elegir antes de enviar el paquete. Si el ILM tiene que mapear una etiqueta del conjunto que contiene más de una NHLFE, se puede realizar el balanceo de cargas sobre múltiples rutas de igual costo.

El FTN (*FEC-To-NHLFE*) mapea cada FEC a un conjunto de NHLFEs, se usa cuando los paquetes enviados que llegan no tienen etiqueta, pero que son etiquetados antes de ser enviados. Si el mapeo FTN mapea una etiqueta a un conjunto de NHLFEs que contiene más de un elemento, exactamente un elemento de este conjunto debe ser elegido antes de enviar el paquete. Si el FTN tiene que mapear una etiqueta del conjunto que contiene más de una NHLFE, se puede realizar el balanceo de cargas sobre múltiples rutas de igual costo.

### 1.2.4 Trueque de etiquetas

Es el uso de procedimientos para enviar un paquete etiquetado. Un LSR examina la etiqueta de la parte superior de la pila de etiquetas; usará el mapeo ILM para mapear esta etiqueta a una NHLFE, usando la información de la NHLFE determina a donde enviar el paquete y realiza una operación en la pila de etiquetas del paquete. Entonces codifica la nueva pila de etiquetas en el paquete y envía el resultado. Cuando se desea enviar un paquete sin etiquetar, el LSR analiza la cabecera de nivel de red para determinar la FEC del paquete; entonces usa el mapeo FTN para mapear ésta a una NHLFE, usando la información de la NHLFE determina a donde enviar el paquete, y

realiza una operación en la pila de etiquetas del paquete. Entonces codifica la nueva pila de etiquetas en el paquete y envía el resultado.

Cuando hay trueque de etiquetas, el salto siguiente siempre es tomado de la NHLFE; en algunos casos esto puede ser diferente de lo que el salto siguiente sería si no se usara el MPLS.

### 1.2.5 Label Switched Path

Un LSP de nivel m para un determinado paquete P es una secuencia de enrutadores, <R1,...., Rn> con las siguientes propiedades:

1. El enrutador $R_1$, que es el enrutador de entrada del LSP, es un LSR que pone una etiqueta en la pila de etiquetas de P, resultando una pila de etiquetas de profundidad **m**.
2. Para todo i, 1<i<n, la pila de etiquetas P tiene una profundidad **m** cuando recibe del LSR $R_i$.
3. En ningún momento durante el tránsito de la pila de etiquetas P desde el enrutador $R_1$ al $R_{n-1}$ la profundidad de la pila de etiquetas es inferior a **m**.
4. Para todo i, 1<i<n: el enrutador $R_i$ transmite la pila de etiquetas P al enrutador $R_{i+1}$ por medio del MPLS.
5. Para todo i, 1<i<n: si un sistema S recibe y envía la pila de etiquetas P después de que la pila de etiquetas P es transmitida por el enrutador $R_i$ pero antes la pila de etiquetas P es recibida por el enrutador $R_{i+1}$ (por ejemplo, los enrutadores $R_i$ y $R_{i+1}$ pueden estar conectados vía una subred a nivel de conmutación de datos, y el sistema S puede ser uno de estos conmutadores), entonces la decisión de envío del sistema S no está basada en la etiqueta de nivel m ó en la cabecera de nivel de red, sino; en la pila de etiquetas a donde se han añadido las etiquetas adicionales en la pila.

Diremos que una secuencia de LSRs es un LSP para una determinada FEC F si es un LSP de nivel **m** para un determinado paquete P cuando la etiqueta de nivel **m** del paquete P es una etiqueta que corresponde a la FEC F.

### 1.2.6 Extrayendo etiquetas en el penúltimo salto (Penultimate Hop Popping)

En el penúltimo LSR del LSP se puede sacar la etiqueta de la pila de etiquetas, en lugar del enrutador de salida del LSP, esto es porque el propósito de la etiqueta de nivel **m** es

llevar el paquete al enrutador $R_n$, una vez que el enrutador $R_{n-1}$ ha decidido enviar el paquete al enrutador $R_n$, la etiqueta no será más utilizada y no necesita ser transportada.

Normalmente cuando el enrutador de salida del LSP recibe un paquete, primero busca en la etiqueta superior y determina como resultado de esta búsqueda si es verdaderamente el enrutador de salida del LSP, entonces debe sacar una etiqueta de la pila y examinar lo que permanece en el paquete. Si hay otra etiqueta en la pila la salida buscará más arriba y enviará el paquete basado en esta búsqueda. Si no hay otra etiqueta en la pila, entonces se envía el paquete de acuerdo a su dirección de destino de nivel de red. Observamos que esto requeriría en la salida hacer dos búsquedas, o dos búsquedas de etiqueta o una búsqueda de etiqueta seguida de una búsqueda de dirección; por esta razón se considera una ventaja sacar la etiqueta en el penúltimo salto. Entonces, el penúltimo nodo saca una etiqueta de la pila y envía el paquete basado en la información obtenida en la búsqueda de la etiqueta que previamente estaba en la parte superior de la pila. Cuando el enrutador de salida del LSP recibe el paquete, la etiqueta que está ahora en la parte superior de la pila será la etiqueta que necesita buscar con el fin de tomar su propia decisión de envío. En caso de que el paquete solo tenía una etiqueta, el enrutador de salida del LSP verá el paquete a nivel de red, que es justamente lo que necesita ver con el fin de tomar su decisión de envío.

Esta técnica permite a la salida hacer una sola búsqueda y también requiere solo una búsqueda para el penúltimo nodo. La creación de la ruta rápida de envío en un protocolo de conmutación de etiquetas puede ser de gran ayuda si se conoce que se requiere una sola búsqueda; con esto, se puede simplificar la codificación si se puede asumir que siempre sólo se necesitará una sola búsqueda y la codificación se puede basar en un presupuesto de tiempo que asume que siempre solo se necesitará una sola búsqueda.

Sin embargo, a veces no es posible sacar una etiqueta de la pila de etiquetas. También hay situaciones en que no es deseable sacar en el penúltimo salto. Por lo tanto el penúltimo nodo saca una etiqueta de la pila de etiquetas solo si es requerido específicamente por el nodo de salida, o si el nodo siguiente del LSP no soporta MPLS; si el nodo siguiente del LSP soporta MPLS, pero no hace esta solicitud el penúltimo nodo no tiene forma de saber cual es el penúltimo nodo.

Las negociaciones iniciales del protocolo de distribución de etiquetas deben permitir a cada LSR determinar si sus LSRs vecinos son capaces de sacar etiquetas de la pila de

etiquetas. Un LSR no debe pedir a un puerto de distribución de etiquetas que saque etiquetas de la pila de etiquetas a menos que sea capaz de hacerlo. Un LSR que es capaz de sacar etiquetas de la pila de etiquetas nunca debe sacar en el penúltimo salto cuando es requerido por el puerto de distribución de etiquetas descendente.

### 1.2.7 Etiquetas de entrada inválidas

¿Qué haría un LSR si recibe un paquete etiquetado con una determinada etiqueta de entrada y no tiene relaciones para esta etiqueta? El LSR asumiría que las etiquetas han sido removidas y el paquete se enviará como paquete IP sin etiqueta; sin embargo, en algunos casos esto causaría un bucle. Sí el LSR ascendente cree que la etiqueta está ligada a una ruta explícita, el LSR descendente no piensa que la etiqueta está ligada a algo y sí el enrutamiento salto a salto del paquete IP no etiquetado regresa el paquete al LSR ascendente; tendremos el bucle.

También es posible que la etiqueta represente una ruta que no puede ser deducida de la cabecera IP. Por lo tanto, cuando un paquete etiquetado es recibido con una etiqueta inválida de entrada debe ser descartada, a menos que se determine de alguna forma que enviarlo sin etiquetar no puede causar ningún daño.

### 1.2.8 Control del LSP: ordenado versus independiente

En el control independiente del LSP, cuando cada LSR tiene que reconocer una determinada FEC, toma una decisión independiente para ligar una etiqueta a esta FEC y distribuir esta ligadura a su puerto de distribución de etiquetas. Esto corresponde a la manera como trabaja el enrutamiento convencional de datagramas IP; cada nodo toma una decisión independiente de como tratar cada paquete y se basa en el algoritmo de enrutamiento para converger rápidamente con el fin de asegurarse de que cada datagrama sea correctamente entregado.

En el control ordenado del LSP, un LSR solo relaciona una etiqueta a una determinada FEC si es el LSR de salida para esta FEC o si ya ha recibido una ligadura de etiqueta para esta FEC de su salto siguiente para esta FEC. Si uno quiere asegurar que el tráfico de una determinada FEC siga una ruta con un conjunto específico de propiedades se debe usar el control ordenado. Con el control independiente, algunos LSRs pueden empezar a etiquetar conmutando un tráfico de la FEC antes de que el LSP esté completamente en funcionamiento, y así algún tráfico de la FEC puede seguir una ruta que no tiene el conjunto específico de propiedades.

El control ordenado también se debe usar si el reconocimiento de la FEC es una consecuencia del establecimiento del correspondiente LSP; el inicio del LSP ordenado puede ser por la entrada o por la salida.

El control ordenado y el control independiente son completamente ínter operables; sin embargo, a menos que todos los LSRs de un LSP estén usando control ordenado, el efecto general sobre el comportamiento de la red es básicamente de control independiente, ya que uno no puede asegurar que un LSP no lo esté usando hasta que está completamente en servicio.

Esta arquitectura permite que la elección entre control independiente y control ordenado sea un asunto local. Ya que los dos métodos interactúan, un determinado LSR necesita soportar solamente el uno u el otro. La elección de control independiente versus ordenado no tiene ningún efecto en los mecanismos de distribución de etiquetas.

### 1.2.9 Agregación

Una forma de dividir el tráfico en FECs es crear una FEC separada para cada prefijo de dirección que aparece en la tabla de enrutamiento. Sin embargo dentro de un determinado dominio MPLS, esto puede hacer que para un determinado conjunto de FECs todo el tráfico relacionado con esta FEC siga la misma ruta. Por ejemplo, un conjunto de prefijos de direcciones diferentes pueden tener el mismo nodo de salida, y el trueque de etiqueta solo se puede usar para sacar el tráfico por el nodo de salida. En este caso, para MPLS la unión de estas FECs es la misma FEC. Esto crea una disyuntiva: ¿O ligar una etiqueta diferente a cada FEC, o ligar una única etiqueta a la unión y aplicar esta etiqueta a todo el tráfico de la unión?

Al procedimiento de ligar una única etiqueta a una unión de FECs que es la propia FEC (dentro del mismo dominio) y aplicar esta etiqueta a todo el tráfico en la unión, se le conoce como **agregación**. La arquitectura MPLS permite la agregación; la agregación puede reducir el número de etiquetas que se necesitan para manejar un conjunto determinado de paquetes y también puede reducir la cantidad de tráfico de control de distribución de etiquetas que se necesita.

Dado un conjunto de FECs que son "agregables" en una única FEC, es posible agregarlos en una única FEC (granularidad más gruesa) ó agregarlos en un conjunto de FECs ó no agregarlos en absoluto (granularidad más fina).

Cuando se usa el control ordenado, cada LSR adoptaría, para un conjunto de FECs, la granularidad usada por el salto siguiente para estas FECs; cuando se usa el control independiente, es posible que haya dos LSR adyacentes, Ru y Rd, que agregarán algún conjunto de FECs diferentemente. Si el enrutador Ru tiene granularidad más fina que el enrutador Rd, esto no es un problema; el enrutador Ru distribuirá más etiquetas para este conjunto de FECs que el enrutador Rd. Esto significa que cuando el enrutador Ru necesita enviar paquetes etiquetados de estas FECs al enrutador Rd, puede necesitar mapear n etiquetas en m etiquetas, donde n > m. Con la opción de que el enrutador Ru pueda retirar un conjunto de n etiquetas que ha distribuido, y entonces distribuir un conjunto de m etiquetas, correspondiendo al nivel de granularidad del enrutador Rd, se consigue una reducción del número de etiquetas distribuidas.

Si el enrutador Ru tiene una granularidad más gruesa que el enrutador Rd (por ejemplo, el enrutador Rd ha distribuido n etiquetas para un conjunto de FECs, mientras que el enrutador Ru ha distribuido m, donde n > m), hay dos opciones:

Puede adoptar un nivel más fino de granularidad del enrutador Rd. Esto requeriría retirar las m etiquetas que ha distribuido y distribuir n etiquetas; esta es la opción preferida.

Puede mapear sus m etiquetas en un subconjunto de n etiquetas del enrutador Rd, si puede determinar que esto producirá el mismo enrutamiento.

En cualquier caso, cada LSR necesita conocer por configuración que granularidad debe usar para las etiquetas que asigna. Donde se use el control ordenado, se requiere que cada nodo conozca solo la granularidad para cada FEC que dejan la red MPLS en este nodo. Para el control independiente, los mejores resultados se pueden obtener asegurando que todos los LSRs estén configurados consistentemente para conocer la granularidad para cada FEC. Sin embargo, en muchos casos esto se puede hacer usando un único nivel de granularidad que se aplica a todas las FECs, tal como "una etiqueta por prefijo IP en la tabla de envío", o "una etiqueta por nodo de salida".

### 1.2.10 Selección de una ruta

La selección de ruta se refiere al método empleado para seleccionar el LSP para una determinada FEC. La arquitectura propuesta para el protocolo MPLS soporta dos opciones para la selección de ruta: enrutamiento salto a salto y enrutamiento explícito.

El enrutamiento salto a salto permite a cada nodo elegir independientemente el próximo salto de cada FEC. Este es el modo habitual hoy en día en las redes IP existentes. Un LSP enrutado salto a salto es un LSP cuya ruta es seleccionada usando el enrutamiento salto a salto. En un LSP con enrutamiento explícito, cada LSR no elige independientemente el próximo salto; más bien un único LSR, generalmente el enrutador de entrada o de salida del LSP, especifica a los LSRs el LSP. Si un único LSR especifica todo el LSP, el LSP es "estrictamente" enrutado y si ese LSR especifica algunos LSRs del LSP, el LSP es "aproximadamente" enrutado.

El enrutamiento explícito puede ser útil para algunos fines, tales como la política de enrutamiento o la ingeniería de tráfico. En MPLS, el enrutamiento explícito necesita ser especificado en el momento en que son asignadas las etiquetas, pero el enrutamiento explícito no tiene que ser especificado con cada paquete IP. Esto hace que el enrutamiento explícito MPLS sea mucho más eficiente que la alternativa del enrutamiento propio de IP.

### 1.2.11 Tiempo de Vida (TTL)

En el envío convencional IP, cada paquete transporta la información de "Tiempo de Vida" (TTL) en su cabecera, cada vez que un paquete pasa a través de un enrutador, su TTL decrementa en 1; si el TTL llega a valer 0 antes de que el paquete haya llegado al destino, el paquete es descartado.

Esto suministra un nivel de protección contra los bucles de envío que puedan existir debido a malas configuraciones o debido a un fallo o a una convergencia lenta del algoritmo de enrutamiento. Esto implica que en MPLS el TTL suprime los bucles o consigue otras funciones, tales como limitar el objetivo de un paquete.

Si el paquete viaja a lo largo de una jerarquía de LSPs, el número total de saltos de LSRs atravesados se debería reflejar en su valor del TTL cuando emerge de la jerarquía de LSPs. La forma en que el TTL es manejado puede variar dependiendo de si los valores de la etiqueta MPLS son transportados en una cabecera "*shim*" específica de MPLS, MPLS-SHIM [20]; o si las etiquetas MPLS son transportadas en una cabecera de la capa 2, tales como una cabecera ATM, MPLS-ATM [7] o una cabecera *Frame Relay*, MPLS-FRMRLY [8].

Si los valores de la etiqueta están codificados en un "*shim*" que está entre las cabeceras del nivel de enlace y el nivel de red, entonces este "*shim*" debe tener un campo TTL que inicialmente carga con el valor del campo TTL de la cabecera de nivel de red, se debería decrementar en cada salto del LSR y se debería copiar en el campo TTL de la cabecera del nivel de red cuando el paquete emerge de su LSP.

Si los valores de la etiqueta son codificados en una cabecera de nivel de enlace, los paquetes etiquetados son enviados por un conmutador de nivel 2 (por ejemplo un conmutador ATM) y el nivel de enlace (como ATM) no tiene el campo TTL, entonces no será posible decrementar el TTL del paquete en cada salto del LSR. Un LSP que consiste de una secuencia de LSRs que no puede decrementar el TTL de un paquete se denominará "LSP sin TTL". Cuando un paquete emerge de un LSP sin TTL, se le debería dar un TTL que reflejara el número de saltos de LSRs que atraviesa. En el caso "*unicast*", esto se puede conseguir propagando una significativa longitud del LSP a los nodos de entrada, permitiendo a su entrada decrementar el TTL antes de enviar los paquetes a un LSP sin TTL. Algunas veces se puede determinar, después del ingreso en un LSP sin TTL, que un determinado TTL de un paquete expirará antes de que el paquete alcance la salida del LSP sin TTL. En este caso, el LSR de entrada del LSP sin TTL no debe conmutar la etiqueta del paquete. Esto significa que se deben desarrollar procedimientos especiales para soportar la funcionalidad del "*traceroute*". Los paquetes "*traceroute*" se pueden enviar mediante el envío convencional de enrutamiento salto a salto.

El TTL no se puede usar para proteger al paquete de posibles bucles, la importancia del control del bucle puede depender del hardware que se usa para el suministro de las funciones del LSR a lo largo del LSP sin TTL.

Por ejemplo, el hardware de un conmutador ATM que se está usando para suministrar las funciones de conmutación MPLS, con la etiqueta transportada en el campo VPI/VCI, no puede decrementar el TTL, no hay protección contra bucles. Si el hardware ATM es capaz de suministrar un buen acceso al buffer de las celdas que llegan transportando diferentes valores VPI/VCI, la posibilidad de bucles no puede tener ningún efecto nocivo en el tráfico y si el hardware ATM no puede suministrar un buen acceso al buffer de este tipo, entonces incluso los bucles de tránsito pueden causar una severa degradación de la rentabilidad total del LSR. Por tanto todos los LSRs que pueden estar conectados a un LSP sin TTL serán requeridos para soportar una técnica común para la detección de bucles; sin embargo, el uso de una técnica de detección de bucles es opcional.

### 1.2.12 Codificación de etiquetas

Con el fin de transmitir una pila de etiquetas junto con el paquete, es necesario definir una codificación concreta de la pila de etiquetas. La arquitectura soporta distintas técnicas de codificación; la elección de la técnica de codificación depende de la clase particular de dispositivo que se use para enviar los paquetes etiquetados.

Puede usarse un hardware y/o un software específico de MPLS para enviar paquetes etiquetados, la forma más obvia de codificar la pila de etiquetas es definir un nuevo protocolo que se usará como un "*shim*" entre las cabeceras de nivel de enlace y de nivel de red. Realmente este "*shim*" sería precisamente una encapsulación de un paquete a nivel de red independiente del protocolo.

Los procedimientos de envío son similares a los de los conmutadores ATM, por esta razón podemos considerar tres formas de codificar las etiquetas en la cabecera de una celda ATM:

**a. Codificación SVC**

Usa el campo VPI/VCI para codificar la etiqueta que está en la parte superior de la pila de etiquetas. Esta técnica se puede usar en cualquier red. Con esta técnica de codificación, cada LSP funciona como un SVC (*Switched Virtual* Circuit) de ATM y el protocolo de distribución de etiquetas es el protocolo de "señalización" de ATM. Con esta técnica de codificación, el ATM-LSR no puede realizar operaciones de poner ni sacar etiquetas de la pila de etiquetas.

**b. Codificación SVP**

Usa el campo VPI para codificar la etiqueta que está en la parte superior de la pila de etiquetas y el campo VCI para codificar la segunda etiqueta de la pila, si existe. Esta técnica tiene algunas ventajas sobre la anterior, porque permite el uso de ATM con conmutación "*Virtual Path*" (VP); los LSPs funcionan como SVPs de ATM; con el protocolo de distribución de etiquetas funcionando como el protocolo de señalización ATM.

Esta técnica no se puede usar siempre. Si la red incluye un VP de ATM a través de una red ATM sin MPLS, entonces el campo VPI no es necesariamente útil para MPLS, cuando se usa esta técnica de codificación, el ATM-LSR a la salida del VP efectivamente hace una operación de sacar la etiqueta.

**c. Codificación multipunto SVP**

Es utilizar el campo VPI para codificar la etiqueta que está en la parte superior de la pila de etiquetas, parte del campo VCI para codificar la segunda etiqueta de la pila y el resto del campo VCI para identificar al enrutador de entrada del LSP. Si se usa esta técnica, las capacidades convencionales de la conmutación VP ATM se pueden usar para suministrar VPs multipunto a punto. Entonces las celdas de diferentes paquetes transportarán diferentes valores VCI. Esta técnica depende de la existencia de una capacidad para asignar los valores VCI de 16 bits a cada conmutador ATM de forma que solo se asigne un valor único VCI a dos conmutadores diferentes. (Si un número adecuado de tales valores se puede asignar a cada conmutador, sería posible también tratar el valor VCI como la segunda etiqueta de la pila), si hay más etiquetas en la pila que pueden ser codificadas en la cabecera ATM, las codificaciones ATM deben ser combinadas con la encapsulación genérica.

La interoperabilidad entre las técnicas de codificación se da por ejemplo si la ruta de los enrutadores <R1, R2, R3> es un LSP, es posible que el enrutador R1 usará una codificación de la pila de etiquetas cuando transmita el paquete P al enrutador R2, pero que el enrutador R2 usará una codificación distinta cuando transmita un paquete P al enrutador R3.

En general, la arquitectura MPLS soporta LSPs con diferentes codificaciones de la pila de etiquetas usadas en diferentes saltos. Los procedimientos para procesar un paquete etiquetado, son términos abstractos de operar en la pila de etiquetas del paquete. Cuando se recibe un paquete etiquetado, el LSR debe decodificarlo para determinar el valor actual de la pila de etiquetas, entonces debe operar en la pila de etiquetas para determinar el nuevo valor de la pila y entonces codificar el nuevo valor apropiadamente antes de transmitir el paquete etiquetado al salto siguiente.

Los conmutadores ATM no tienen la capacidad para traducir de una técnica de codificación a otra. La arquitectura MPLS por lo tanto requiere para dos conmutadores ATM que estén en sucesivos LSRs a lo largo de un nivel m de un LSP para el mismo paquete, que se use la misma técnica de codificación.

También habrá redes MPLS que contienen una combinación de conmutadores ATM operando como LSRs y otros LSRs operando con una cabecera "*shim*" MPLS. En estas redes puede haber algunos LSRs que tienen interfases ATM así como interfases "MPLS

*Shim*". Es así que un LSR puede cambiar una pila de etiquetas codificada ATM de una interfase de entrada y reemplazarla con una pila de etiquetas codificadas con cabecera "*shim*" MPLS en la interfase de salida.

### 1.3 Mezcla de etiquetas

Es la capacidad de un LSR, que contiene múltiples etiquetas de entrada para una determinada FEC, de enviar los paquetes de esta FEC con una única etiqueta de salida; que se aplica a todos estos paquetes.

Si un LSR es capaz de mezclar etiquetas, puede recibir dos paquetes de diferentes interfases de entrada, y/o con diferentes etiquetas, y enviar ambos paquetes a la misma interfase de salida con la misma etiqueta. Una vez que son transmitidos los paquetes, la información que les llega de diferentes interfases y/o con diferentes etiquetas de entrada se pierde.

Si un LSR no es capaz de mezclar etiquetas, para dos paquetes cualesquiera que llegan de diferentes interfases, o con etiquetas diferentes, los paquetes o deben ser transmitidos por diferentes interfases de salida o deben tener etiquetas diferentes. Los ATM-LSR usando las codificaciones SVC o SVP no pueden realizar mezcla de etiquetas. Con la mezcla de etiquetas el número de etiquetas de salida por FEC necesita ser de solo 1; sin mezcla de etiquetas el número de etiquetas de salida por FEC podría ser tan grande como el número de nodos en la red.

Con una mezcla de etiquetas, el número de etiquetas de entrada por FEC que necesita un LSR determinado nunca es mayor que el número de distribuidores contiguos de etiquetas. Sin mezcla de etiquetas, el número de etiquetas de entrada por FEC que necesita un determinado LSR es tan grande como el número de nodos anteriores que envían tráfico de la FEC al enrutador LSR en cuestión.

La arquitectura MPLS asegura una correcta interoperación entre LSRs con mezcla y sin ella.

#### 1.3.1 LSRs sin mezcla

El procedimiento de envío MPLS es muy similar al procedimiento de envío usado por tecnologías como ATM y *Frame Relay*. Es decir, llega una unidad de datos, se busca una etiqueta (VPI/VCI o DLCI) en la tabla "*cross-connect*" y en base a esta búsqueda, se elige

un puerto de salida y se reeescribe el valor de la etiqueta. También, se puede usar un protocolo de distribución de etiquetas como el "protocolo de señalización" para el establecimiento de las tablas "*cross-connect*".

Estas tecnologías no soportan mezcla de etiquetas; MPLS contiene procedimientos que permiten el uso de LSRs sin mezcla y también soportará procedimientos que permitan a ciertos conmutadores ATM funcionar como LSRs con mezcla.

### 1.3.2. Etiquetas para LSRs con mezcla y sin mezcla

Un LSR ascendente que soporta mezcla de etiquetas, necesita solo enviar una etiqueta por FEC. Un vecino anterior que no soporta mezcla de etiquetas, necesita enviar múltiples etiquetas por FEC. Sin embargo no hay forma de saber a priori cuantas etiquetas se necesitan.

En la arquitectura MPLS, si un determinado vecino ascendente no soporta mezcla de etiquetas, no envía ninguna etiqueta para una determinada FEC a menos que explícitamente se pida una etiqueta para esta FEC. El vecino ascendente puede hacer múltiples solicitudes, y se da una nueva etiqueta cada vez. Cuando un vecino descendente recibe la solicitud del anterior y este no soporta por si mismo mezcla de etiquetas, entonces por turno debe pedir al vecino descendente otra etiqueta para la FEC en cuestión.

Es posible que pueden haber algunos nodos que soporten mezcla de etiquetas, pero que solo puedan mezclar un número limitado de etiquetas de entrada en una única etiqueta de salida. Por ejemplo debido a alguna limitación de hardware un nodo es capaz de mezclar cuatro etiquetas de entrada en una única etiqueta de salida. Sin embargo este nodo tiene seis etiquetas de entrada que le llegan para una determinada FEC. En este caso este nodo puede mezclarlos en dos etiquetas de salida.

## 1.4 Transporte del protocolo de distribución de etiquetas

Se usa un protocolo de distribución de etiquetas entre nodos de una red MPLS para establecer y mantener las ligaduras de las etiquetas. Con el fin de operar correctamente el MPLS, la información de distribución de etiquetas necesita ser transmitida con fiabilidad y los mensajes del protocolo de distribución de etiquetas que pertenecen a una determinada FEC necesitan ser transmitidos en secuencia. También es deseable el control de flujo, como es la capacidad de transportar múltiples mensajes de etiquetas en

un único datagrama, una forma de cumplir estos objetivos es usar TCP (*Transmission Control Protocol*) como transporte, como se hace en MPLS-LDP y MPLS-BGP.

Esta arquitectura no establece reglas duras y rápidas en la elección de que protocolo de distribución de etiquetas usar y en que circunstancias. Sin embargo es posible señalar algunas consideraciones:

### 1.4.1 BGP y LDP

Muchas veces es deseable ligar las etiquetas a las FECs que se pueden identificar con rutas a prefijos de direcciones. Si hay un estándar, el algoritmo de enrutamiento ampliamente desplegado que distribuye estas rutas, puede ser lo mejor para la distribución de etiquetas usando "*piggybacking*" para distribuir las etiquetas y las rutas.

Por ejemplo el BGP (*Border Gateway Protocol*) distribuye estas rutas, y si un portavoz BGP necesita también distribuir etiquetas a sus puertos BGP, tiene ventajas el usar BGP para hacer la distribución de etiquetas. En particular permite a los reflectores de la ruta BGP distribuir etiquetas, suministrando así una ventaja de escalabilidad sobre LDP (*Label Distribution* Protocol) para distribuir etiquetas entre puertos BGP.

### 1.4.2 Etiquetas y especificaciones de flujo RSVP

Cuando se usa RSVP [9] para establecer las reservas de recursos para unos determinados flujos, puede ser deseable etiquetar los paquetes de estos flujos, así que las especificaciones de filtro de RSVP no necesitan ser aplicadas en cada salto. Se puede argumentar que teniendo el RSVP para distribuir etiquetas como parte del proceso de establecimiento de la ruta/reserva es el método más eficiente de distribuir etiquetas.

### 1.4.3 Etiquetas para LSPs enrutados explícitamente

En algunas aplicaciones de MPLS, particularmente las relacionadas con la ingeniería de tráfico, es deseable establecer un enrutamiento explícito, de entrada a salida. También, es deseable aplicar reservas de recursos a lo largo de la ruta. Entonces uno puede imaginar dos propuestas: Empezar con un protocolo existente que es usado para establecer reservas de recursos y ampliarlo para soportar enrutamiento explícito y distribución de etiquetas, ó empezar con un protocolo existente que es usado para distribuir etiquetas y ampliarlo para soportar enrutamiento explícito y reservas de recursos. La primera propuesta es el protocolo especificado como MPLS-RSVP-TUNNELS, el segundo especificado como MPLS-CR-LDP.

# CAPITULO II
# ARQUITECTURA DEL GMPLS

El *Generalized* MPLS (GMPLS) es una arquitectura que surge con la finalidad de contemplar múltiples niveles de conmutación. Además de proveer recursos dinámicamente y de lograr un funcionamiento de la red con garantías, usando para ello técnicas de restauración y protección.

En el presente capítulo trataremos las características de la arquitectura del GMPLS [10], por las cuales es considerado el planteamiento más prometedor para la consolidación de las redes troncales.

## 2.1 Introducción

El protocolo GMPLS amplía el protocolo MPLS por que maneja la conmutación por división de tiempo, por longitud de onda y por espacio (por ejemplo: puerto/fibra de entrada a puerto/fibra de salida). El objetivo principal del protocolo GMPLS está en el plano de control de estos niveles; desde cada uno de los cuales se puede usar físicamente distintos planos de datos y envío.

La arquitectura GMPLS cubre los principales bloques constructivos de señalización y enrutamiento necesarios para construir un plano de control. No restringe la forma en que estos niveles trabajan juntos. Se pueden aplicar diferentes modelos como el superpuesto, aumentado o integrado. Por otra parte, cada par de niveles contiguos pueden trabajar conjuntamente de formas distintas, resultando de ello varias posibles combinaciones, en función de las decisiones de los fabricantes y operadores.

Esta arquitectura separa claramente el plano de control y el plano de envío. Además separa el plano de control en dos partes, el plano de señalización y el plano de enrutamiento con sus respectivos protocolos.

## 2.2 Conceptos básicos del GMPLS en las redes ópticas

Podemos definir los siguientes:

### 2.2.1 Etiquetas generalizadas

Recordemos que en el MPLS no generalizado, una etiqueta es un número (de hasta 32 bits) que se escribe en los campos de la cabecera del protocolo de los paquetes de datos que viajan por un enlace. Pero, el valor de etiqueta acordado, no implica necesariamente una relación a la asignación de ancho de banda ni calidad de servicio para el correspondiente flujo de datos. Los protocolos de distribución de etiquetas de Ingeniería de Tráfico (tales como RSVP y CR-LDP) son los que facilitarán la calidad de servicio y la negociación del ancho de banda como parte del intercambio de etiqueta.

En GMPLS la etiqueta generalizada amplía la etiqueta tradicional MPLS permitiendo la representación de no solo etiquetas que viajan *in-band* con paquetes de datos asociados, sino también etiquetas que identifican ranuras de tiempo, longitudes de onda, posiciones multiplexadas por división de espacio, etiquetas genéricas MPLS, etiquetas *Frame Relay*, o etiquetas ATM (VCI/VPI). El formato de una etiqueta puede ser tan simple como un valor entero de una etiqueta de longitud de onda o ser más elaborado como una etiqueta SDH/SONET o G.709.

Una etiqueta generalizada solo transporta un solo nivel de etiqueta. Cuando se solicitan múltiples niveles de etiquetas (LSPs dentro de LSPs), cada LSP se debe establecer separadamente.

La premisa del GMPLS es que la idea de una etiqueta se puede generalizar como algo que es suficiente para identificar un flujo de tráfico. Por ejemplo, en una fibra óptica cuyo ancho de banda es dividido en longitudes de onda, el conjunto de una longitud de onda puede ser asignado a un flujo solicitado; los LSRs en cualquier extremo de la fibra tienen simplemente que estar de acuerdo con la frecuencia a usar. A diferencia de las etiquetas no generalizadas, los datos dentro del flujo solicitado no necesitan ser marcados con un valor de etiqueta; el valor etiqueta es implícito por el hecho de que los datos están siendo transportados con la banda de frecuencia acordada. Por otro lado, se necesita alguna representación del valor etiqueta en el protocolo de señalización de forma que los mensajes de control entre los LSRs puedan acordar el valor a usar.

El GMPLS extiende la representación de una etiqueta desde un solo número de 32 bits a un conjunto de octetos de longitud arbitraria e introduce el objeto *Generalized Label* (en RSVP) y el *Generalized Label TLV* (en CR-LDP) para transportar la propia etiqueta y la información relacionada con ella.

Entre los principales tipos de etiquetas tenemos:

**a) Etiquetas de toda una fibra**

Un enlace entre LSRs puede consistir de una agrupación de fibras ópticas. Los LSRs pueden elegir la asignación de toda una fibra a un flujo de datos y así simplemente necesitan acordar que fibra usar. En este caso el valor de la etiqueta es el número de la fibra seleccionada dentro de la agrupación. La interpretación de los números fibra/puerto es un asunto local para los LSRs del enlace. Los dos LSRs usan diferentes esquemas de numeración, el LMP (*Link Managment Protocol*) suministrará un mecanismo a los LSRs para intercambiar y correlacionar la información de numeración.

**b) Etiquetas de longitud de onda**

Cuando el ancho de banda de una fibra óptica se subdivide con WDM (*Wavelength Division Multiplexing*), un LSR óptico puede elegir en asignar una sola longitud de onda (o lambda) a un flujo de datos solicitado. En este caso el valor de la etiqueta es la longitud de onda seleccionada.

**c) Etiquetas waveband**

Si se agrupan longitudes de onda consecutivas en una *waveband*, de forma que todas se conmuten de la misma forma, la etiqueta es un ID de la *waveband* y un par de números (identificadores de canal) que indican las longitudes de onda inferior y superior de la *waveband* seleccionada.

**d) Etiquetas de ranuras de tiempo**

Cuando el ancho de banda de una fibra óptica se subdivide en ranuras de tiempo por TDM, un conmutador óptico puede satisfacer una determinada solicitud de flujo de datos asignando una o más ranuras de tiempo en este flujo. Por lo tanto en general un valor de etiqueta TDM debe ser suficiente para especificar la ranura(s) de tiempo asignada. Los detalles exactos de la representación de una etiqueta TDM dependen de la jerarquía TDM en uso.

**e) Etiquetas SONET/SDH**

SDH y SONET definen cada uno de ellos una estructura multiplexada; estas, se usarán como árboles con nombres para crear etiquetas únicas. Esta etiqueta identificará la posición exacta (ranura(s) de tiempo) de una señal de estructura multiplexada. Una etiqueta SONET/SDH se representa como una secuencia de cinco números, conocidos como S, U, K, L y M, que seleccionan ramas de la jerarquía TDM SONET/SDH.

### 2.2.2 Asignaciones de ancho de banda

Para todos los tipos de etiquetas del GMPLS descritos aquí, el valor etiqueta implica directamente el ancho de banda que está disponible para el correspondiente flujo de datos. Por ejemplo, si una etiqueta denota una sola ranura de tiempo SONET VT-6, el ancho de banda disponible es el de una ranura VT-6; similarmente para las otras etiquetas TDM, lambda, `waveband` o fibra. Esto es completamente diferente del caso de las etiquetas no generalizadas y es un reflejo fundamental de la naturaleza de las redes ópticas.

### 2.2.3 Solicitando etiquetas generalizadas

El GMPLS generaliza el mensaje de la solicitud del establecimiento por dos razones:

Distinguirlo de una solicitud de establecimiento no generalizado y,
Permitirle transportar con más detalle los parámetros adicionales que especifican la solicitud.

En RSVP esto se hace usando un objeto solicitud de etiqueta generalizada en lugar de una solicitud de etiqueta en el mensaje *Path*, y en CR-LDP añadiendo una *Generalized Label Request* TLV al mensaje solicitud de etiqueta. En el nivel más básico, ambos LSRs conocen que el enlace debe ser generalizado, porque conocen que el enlace al que se aplica la solicitud es un enlace óptico generalizado. Por lo tanto, esta información no es explícita en el mensaje de solicitud.

Sin embargo, dado que un enlace óptico puede consistir de una agrupación de fibras, y los conmutadores pueden soportar más de un tipo de multiplexación en estas fibras, es necesario para el LSR ascendente especificar el tipo de codificación del LSP que quiere para el flujo de datos que se está estableciendo; entonces este tipo de codificación determina si la etiqueta acordada estará basada en ranura de tiempo o en longitud de onda. Así la Solicitud de Etiqueta Generalizada especificada por el GMPLS transporta un

campo del tipo de codificación del LSP. Los valores normalmente soportados para este campo que son relevantes en las redes ópticas son: ANSI PDH, ETSI PDH, SDH, SONET, *Digital Wrapper*, Lambda, Fibra.

Dado que algunos enlaces pueden mostrar (a través del IGP) la capacidad de soportar más de un tipo de conmutación, el Objeto Solicitud de Etiqueta Generalizada/TLV contiene un campo que indica el modo de conmutación a ser aplicado en un determinado LSP. Esto permite que un conmutador sea capaz de conmutar fibras enteras, *wavebands* o lambdas individuales. La opción de como conmutar para cualquier LSP en particular, se hace cuando se establece el LSP. Esto incrementa la flexibilidad de como se pueden usar los recursos de la red. Para las etiquetas basadas en fibra y en longitud de onda, no se necesita nada más. Cuando se solicita etiquetas SONET y SDH, puede ser necesario solicitar que el ancho de banda total para el LSP se debería dividir en múltiples ranuras de tiempo. Por lo tanto, cuando el tipo de codificación del LSP es SONET o SDH, la solicitud de etiqueta generalizada transporta campos adicionales que especifican cuantas ranuras de tiempo se podrían combinar para cumplir la solicitud (campo número de componentes) y como estas ranuras de tiempo estarían concatenadas, incluido si son requeridas que sean contiguas (campo tipo de agrupación solicitado).

### 2.2.4 Restringiendo la elección de etiqueta

La etiqueta para cada enlace es normalmente dado por el nodo descendente de este enlace. En GMPLS, donde las etiquetas están directamente relacionadas con los recursos de la red, esto puede llevar a conflictos durante el establecimiento del LSP. Por ejemplo, un conmutador óptico basado en microespejos puede conmutar una longitud de onda recibida desde un puerto de entrada a un puerto de salida, pero no puede modificar la longitud de onda. Hay por lo tanto una necesidad de permitir que los OXCs a lo largo de la ruta puedan restringir y/o influir en la elección de etiquetas apropiadas.

### 2.2.5 Conjunto de etiquetas

El GMPLS introduce el concepto de un conjunto de etiquetas. Un LSR ascendente incluye un conjunto de etiquetas en su solicitud de señalización para restringir la elección de la etiqueta del LSR descendente para el enlace entre ellos. El LSR descendente debe seleccionar una etiqueta dentro del conjunto de etiquetas, o de lo contrario debe fallar el establecimiento del LSP, esto es útil en el dominio óptico cuando:

Un LSR es incapaz de convertir longitudes de onda.

Un LSR solo puede generar y recibir un subconjunto de las longitudes de onda que pueden ser conmutadas por los LSRs vecinos.

Es deseable para un LSR limitar la cantidad de conversiones de longitudes de onda que tiene que realizar, con el fin de reducir la distorsión de las señales ópticas.

El conjunto de etiquetas se construye incluyendo y/o excluyendo un número arbitrario de listas y/o rangos de etiquetas. Si no se incluye ninguna etiqueta explícitamente, el conjunto consiste de todas las etiquetas no excluidas explícitamente. Si no hay presente un conjunto de etiquetas, el LSR descendente no está restringido en su elección de etiqueta. A medida que el conjunto de etiquetas se propaga con el mensaje *Path*, cada LSR puede generar un nuevo conjunto de etiquetas de salida, basado en sus capacidades de *hardware* y posiblemente del conjunto de etiquetas de entrada.

### 2.2.6 Control de etiqueta explícita

El GMPLS también introduce el control de etiqueta explícita. Esto mejora el concepto del MPLS de una ruta explícita permitiendo al LSR de entrada especificar la(s) etiqueta(s) a usar en uno, algunos o todos los enlaces enrutados explícitamente para la ruta de ida y/o vuelta. Es útil cuando el LSR de entrada quiere insistir en que la longitud de onda usada es la misma a lo largo de todo el LSP; esto puede ser deseable con el fin de evitar distorsión de la señal óptica.

También, puede ser útil en la Ingeniería de Tráfico donde la ruta tiene conocimiento de las etiquetas en uso en la red y las capacidades de conmutación de los LSRs. En este caso, la ruta puede incluir las etiquetas específicas a ser usadas en cada salto. Las etiquetas explícitas son especificadas por el LSR de entrada como parte de la ruta explícita.

En cada LSR a lo largo de la ruta, cualquier etiqueta explícita que es especificada en la ruta explícita para el salto siguiente es eliminada y convertida en un objeto conjunto de etiquetas, conteniendo una única etiqueta para el salto siguiente. El LSR que recibe este conjunto de etiquetas usa esta etiqueta para este salto (y debe fallar el establecimiento si esta etiqueta no está disponible localmente).

### 2.2.7 Control de etiqueta de salida

Cuando un administrador de la red inicia el establecimiento de un LSP, es libre de especificar la ruta del LSP y opcionalmente los valores de las etiquetas a usar en los enlaces que el LSP atraviesa.

A veces el administrador de la red puede tener información adicional sobre el enrutamiento del tráfico de datos en cuanto emerge en el extremo más lejano del LSP. Por ejemplo, puede saber que solo el tráfico de telefonía de voz será inyectado en este LSP; y que a la salida del LSP, todo este tráfico será enrutado vía una pasarela telefónica a una dirección conocida.

El mecanismo para conseguir esto se llama control de etiqueta de salida. El administrador añade simplemente objetos adicionales de etiqueta a la ruta explícita después del último salto, cuando el LSR de salida recibe el mensaje de establecimiento del LSP, anuncia las etiquetas adicionales al extremo de la ruta explícita y las interpreta de forma que lo encuentre útil.

## 2.3 Tipos de conmutación y jerarquías de envío

El GMPLS difiere del MPLS en que soporta múltiples tipos de conmutación, el soporte para los tipos adicionales de conmutación ha llevado al GMPLS a ampliar determinadas funciones básicas del MPLS y en algunos casos, a añadirles funcionalidad. Estos cambios y adiciones impactan en las propiedades básicas del LSP, en las formas de solicitud y comunicación de las etiquetas, en la naturaleza unidireccional de los rutas LSP, en como se propagan los errores y la información suministrada para la sincronización de los LSRs de entrada y salida.

La arquitectura MPLS se definió para soportar el envío de datos basados en una etiqueta. En GMPLS se asume que los LSRs tienen un plano de envío que es capaz de reconocer el inicio y final de los paquetes o celdas, y poder procesar sus cabeceras. Específicamente estos LSRs incluyen dispositivos donde la decisión de envío se basa en ranuras de tiempo, longitudes de onda o puertos físicos. Así el nuevo conjunto de LSRs, o con más precisión las interfases de estos LSRs [12], se pueden subdividir en:

### 2.3.1 Interfases capaces de conmutar paquetes (PSC: Packet Switch Capable)

Son las interfases que reconocen los extremos del paquete y pueden enviar datos basados en el contenido de la cabecera del paquete. Por ejemplo, las interfases de los

enrutadores que envían datos basados en el contenido de la cabecera IP y las interfases de los enrutadores que envían datos basados en el contenido de la cabecera "*shim*" de MPLS.

### 2.3.2 Interfases capaces de conmutar en capa 2 (L2SC: Layer 2 Switch Capable)

Son las interfases que reconocen los extremos de la trama/celda y pueden enviar datos basados en el contenido de las cabeceras de trama/celda. Por ejemplo, las interfases de los puentes *Ethernet* que envían datos basados en el contenido de la cabecera MAC y las interfases de los LSRs de ATM que envían datos basados en los VPI/VCI de ATM.

### 2.3.3 Interfases capaces de multiplexación por división por tiempo (TDM: Time Division Multiplex Capable)

Son las interfases que envían datos basados en la ranura de tiempo de datos en un ciclo repetitivo. Por ejemplo, las interfases de un *Cross-Connect* (XC) SDH/SONET, un *Terminal Multiplexer* (TM), un Multiplexador *Add-Drop* (ADM) y el *Digital Wrapper* (que provee capacidades TDM).

### 2.3.4 Interfases capaces de conmutar lambdas (LSC: Lambda Switch Capable)

Son las interfases que envían datos basados en la longitud de onda. Por ejemplo, las interfases de un *Cross-Connect Photonic* (PXC) o un *Cross-Connect Optical* (OXC) que pueden operar a nivel individual de longitud de onda y las interfases de los conmutadores ópticos PXC que pueden operar a nivel de un grupo de longitudes de onda.

### 2.3.5 Interfases capaces de conmutar fibras (FSC: Fiber Switch Capable)

Son las interfases que envían datos basados en la posición de los datos en los espacios físicos (puertos). Una interfase de este tipo es la de un conmutador óptico PXC/OXC que puede operar a nivel de una sola fibra o múltiples fibras.

Solo se puede establecer un circuito entre las interfases del mismo tipo; para GMPLS estos circuitos se nombran como LSPs.

El concepto de LSP anidado (LSP dentro de otro LSP), ya disponible en MPLS, facilita la construcción de la jerarquía de envío. Esta jerarquía de LSPs puede estar en una misma interfase o entre distintas interfases.

Se puede construir una jerarquía [13], si una interfase es capaz de multiplexar varios LSPs de la misma tecnología (nivel).

El anidado también puede ocurrir entre interfases. En la parte alta de la jerarquía están las interfases FSC, seguidas por LSC, TDM, L2SC y finalmente por interfases PSC. En la fig. 2.1, por ejemplo, un LSP que empieza y acaba en una interfase PSC se puede anidar (junto con otros LSPs) en un LSP de tipo TDM que empieza y acaba en una interfase TDM, este LSP se puede anidar (junto con otros TDM-LSPs) en un LSP que empieza y acaba en una interfase LSC, y finalmente en una interfase FSC.

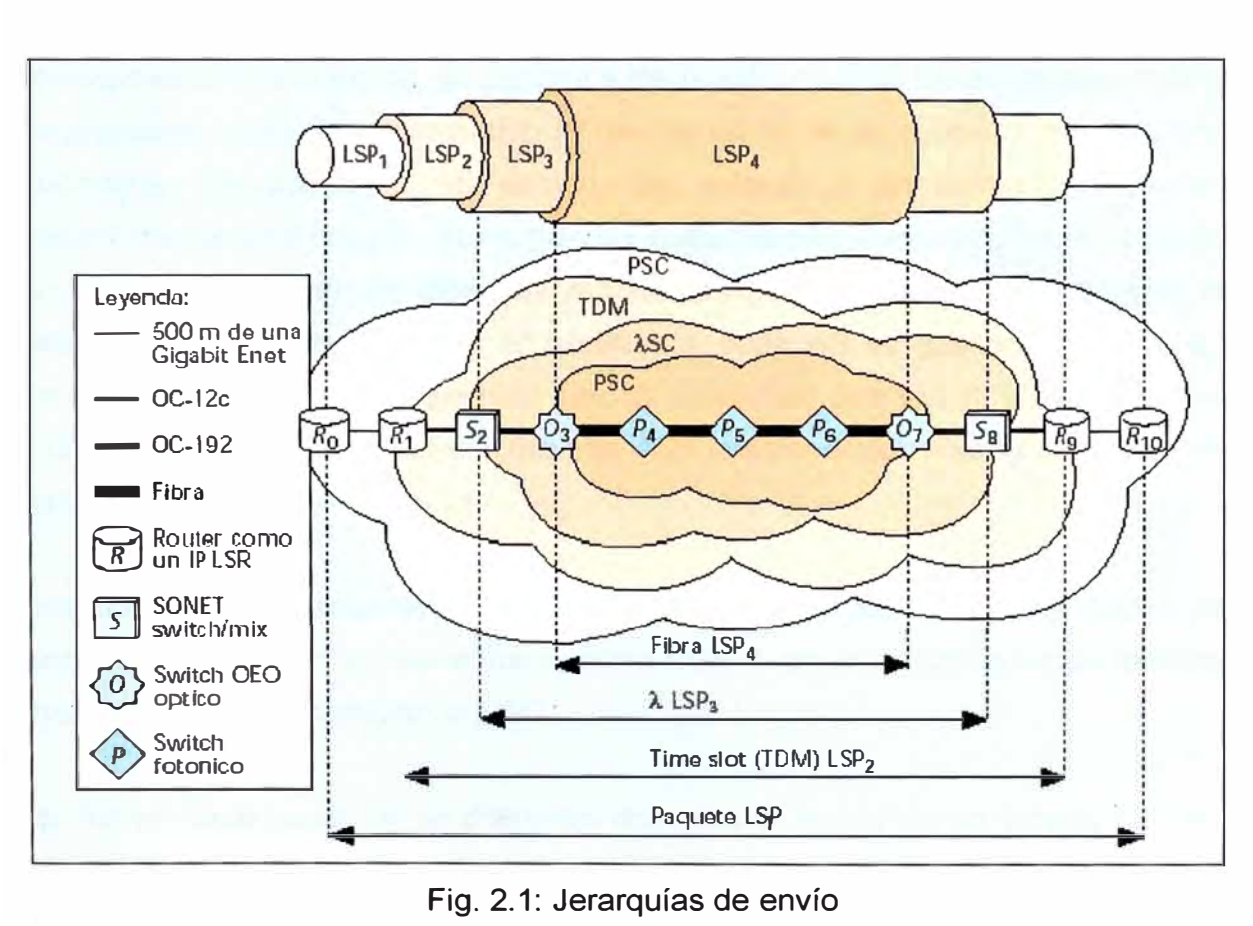


Fig. 2.1: Jerarquías de envío

## 2.4 Modelos de enrutamiento y direccionamiento

El GMPLS está basado en modelos de enrutamiento y direccionamiento IP. Esto hace que se usen las direcciones IPv4 y/o IPv6 para identificar las interfases y que también se reusen los tradicionales protocolos de enrutamiento IP.

Como los planos de control y datos están desacoplados en GMPLS, los vecinos del plano de control no tienen porque ser vecinos en el plano de datos, por lo tanto los mecanismos

como el protocolo LMP necesitan asociar los enlaces de Ingeniería de Tráfico (TE) con los nodos vecinos.

Las direcciones IP no solo se usan para identificar las interfases de los dispositivos y enrutadores, sino de forma general para identificar cualquier interfase PSC y no PSC. Similarmente los protocolos de enrutamiento IP se usan para encontrar rutas para datagramas IP con un algoritmo SPF (*Shortest Path First*) y también se usan para encontrar rutas para circuitos no PSC usando un algoritmo CSPF (*Constraint-based Shortest Path First*). Sin embargo se necesitan algunos mecanismos adicionales para aumentar la escalabilidad de estos modelos y para tratar con determinados requerimientos de ingeniería de tráfico de los niveles no PSC. Reusando los protocolos de enrutamiento IP existentes, se permite a los niveles no PSC tomar los desarrollos que se implantaron para el enrutamiento IP, en particular en el contexto del enrutamiento intra-dominio (enrutamiento del estado del enlace) y enrutamiento inter-dominio (enrutamiento de políticas). En un modelo de superposición, cada nivel no PSC puede ser visto como un conjunto de Sistemas Autónomos (AS) interconectados de una forma arbitraria. Similar al enrutamiento IP tradicional, cada AS es gestionado por una sola autoridad administrativa. Por ejemplo, un AS puede ser una red SDH/SONET operada por un *carrier* determinado. El conjunto de ASs interconectados sería una *Internetwork* SDH/SONET.

El intercambio de la información de enrutamiento entre ASs se puede hacer vía un protocolo de enrutamiento inter-dominio como BGP-4, por sus facilidades de reutilización y enrutamiento en un contexto no PSC.

Cada AS se puede subdividir en diferentes dominios de enrutamiento, y cada uno de ellos puede correr un protocolo de enrutamiento intra-dominio diferente. Así sucesivamente cada dominio de enrutamiento se puede dividir en áreas. Un dominio de enrutamiento está hecho de nodos dotados de GMPLS. Estos nodos pueden ser nodos frontera (dispositivos, LSRs de entrada o de salida), o LSRs internos. Un ejemplo de dispositivos no PSC es un SDH/SONET *Terminal Multiplexer*, una tarjeta SDH/SONET dentro de un enrutador IP o un conmutador ATM.

La TE dentro del dominio requiere el uso de protocolos de enrutamiento de estado de enlace como OSPF o IS-IS. El GMPLS define las extensiones para estos protocolos.

Estas extensiones se necesitan para distribuir determinadas características estáticas y dinámicas TDM, LSC y FSC a los nodos y enlaces.

### 2.4.1 Direccionamiento de niveles PSC y no PSC

Al usar las direcciones IPv4 y/o IPv6, no implica en absoluto que deberían estar asignadas en el mismo espacio de direccionamiento que las direcciones públicas IPv4 y/o IPv6 usadas en Internet. Se pueden usar las direcciones IP privadas si no requieren ser intercambiadas con otro operador, pero de no ser así se requieren direcciones IP públicas. Sí se usa un modelo integrado, dos niveles pueden compartir el mismo espacio de direcciones. Notemos que es beneficioso el uso de direcciones públicas IPv4 y/o IPv6 de Internet para los niveles no PSC si se tiene un modelo integrado con el nivel IP. Los espacios de direccionamiento IPv4 (32 bits) e IPv6 (128 bits) son más que suficientes para acomodar cualquier nivel no PSC.

### 2.4.2 Mejoras de escalabilidad GMPLS

Los niveles TDM, LSC y FSC introducen nuevas restricciones en los modelos de direccionamiento y enrutamiento IP, ya que ahora los enlaces físicos paralelos pueden conectar dos nodos. La mayoría de los *carriers* ya tienen hoy decenas de longitudes de onda por fibra entre dos nodos. La nueva generación de sistemas DWDM permitirá centenares de longitudes de onda por fibra. Llega a ser poco práctico asociar una dirección IP a cada extremo de cada enlace físico; representar cada enlace como una adyacencia separada de enrutamiento y mantener los estados del enlace para cada uno de estos enlaces. Con este fin el GMPLS mejora los modelos de enrutamiento y direccionamiento MPLS para incrementar su escalabilidad.

Se pueden usar dos mecanismos para incrementar la escalabilidad del direccionamiento y el enrutamiento; los enlaces no numerados y los enlaces agregados ó también una combinación de estos. Ellos requieren extensiones para los protocolos de señalización RSVP-TE y CR-LDP [9,11], y enrutamiento OSPF-TE e IS-IS-TE [14].

### 2.4.3 Extensiones TE para los protocolos de enrutamiento IP

Generalmente un enlace TE se considera como un accesorio a un enlace "regular" OSPF o IS-IS y cuando el enlace se activa, entonces se observan las propiedades regulares IGP del enlace; básicamente la métrica SPF y las propiedades TE del enlace; sin embargo GMPLS propone:

Primero, los enlaces que son no PSC pueden tener aún propiedades TE; sin embargo una adyacencia OSPF no se puede instalar directamente en estos enlaces.

Segundo, un LSP se puede anunciar como un enlace TE punto a punto en el protocolo de enrutamiento, como una Adyacencia de Envío (FA); así un enlace TE anunciado no necesita serlo entre dos vecinos OSPF adyacentes.

Tercero, se pueden anunciar un número de enlaces como un único enlace TE; por ejemplo, para mejorar la escalabilidad, así no habrá una asociación uno a uno de una adyacencia regular y un enlace TE.

Un enlace TE es un enlace lógico que tiene propiedades TE, algunas de las cuales se pueden configurar en un LSR de anuncios, otras se pueden obtener de LSRs por medio de algún protocolo y también deducir de los componentes de un enlace TE. Una propiedad importante de un enlace TE está relacionada con la contabilidad del ancho de banda para este enlace. GMPLS definirá distintas reglas contables para diferentes niveles no PSC. Sin embargo, los atributos genéricos del ancho de banda están definidos por extensiones TE para enrutamiento y por el GMPLS, tales como el ancho de banda sin reserva, el máximo ancho de banda reservable y el máximo ancho de banda del LSP.

En un entorno dinámico se espera tener frecuentes cambios de información contable del ancho de banda. Se puede implementar una política flexible para disparar la actualización del estado de enlace basado en unos umbrales de ancho de banda y un mecanismo de moderación del enlace.

También, las propiedades TE asociadas a un enlace capturarían las características relacionadas con la protección y la restauración. Un enlace TE entre un par de LSRs no implica la existencia de una adyacencia IGP entre estos LSRs. Un enlace TE debe tener algunos medios por los cuales el LSR de anuncios de ha conocer su tiempo de vida. Cuando un LSR se entera de que un enlace TE se ha activado y además que pueda determinar las propiedades del enlace TE, entonces este LSR puede anunciar este enlace a sus vecinos del OSPF mejorado o del IS-IS de GMPLS usando los TE objects/TLVs. Las interfases sobre las que se establecen las adyacencias del OSPF mejorado o del IS-IS de GMPLS se llaman "canales de control".

### 2.4.4 Enlaces no numerados

Los enlaces no numerados (o interfases) son enlaces que no tienen direcciones IP. El uso de estos enlaces conlleva a dos posibilidades:

A. La posibilidad de especificar enlaces no numerados en la señalización MPLS TE. La señalización MPLS TE no provee soporte para los enlaces no numerados, porque no provee una forma de indicar un enlace no numerado. El GMPLS define extensiones simples para indicar un enlace no numerado utilizando dos objetos/TLV: *Explicit Route Object* (ERO) y *Record Route Object* (RRO).

   Dado que los enlaces no numerados no están identificados por una dirección IP; para el propósito MPLS TE, cada extremo necesita algún tipo de identificador local para el LSR que pertenece al enlace. Los LSRs en los dos puntos extremos de un enlace no numerado intercambian los identificadores que ellos asignan al enlace; el intercambio de los identificadores se puede conseguir por configuración, por medio de un protocolo como el LMP, por medio de RSVP/CR-LDP o por medio de las extensiones IS-IS u OSPF.

B. La posibilidad de transportar información TE sobre los enlaces no numerados en las extensiones IGP-TE de ISIS-TE (TLV de alcanzabilidad extendido de IS) y OSPF-TE (TE LSA: LSA opaco).

**2.5 Enlace agrupado**

El concepto de enlace agrupado es esencial en ciertas redes que emplean el plano de control del GMPLS. Un ejemplo típico, es una red mallada óptica donde los *cross-connects* ópticos adyacentes (LSRs) están conectados por varios centenares de longitudes de onda paralelas. En esta red, consideramos la aplicación de los protocolos de enrutamiento del estado de enlace como OSPF o IS-IS, con extensiones adecuadas para el descubrimiento del recurso y la computación dinámica de la ruta.

Cuando un par de LSRs están conectados por múltiples enlaces, es posible anunciar varios (o todos) de estos enlaces como un solo enlace en OSPF y/o IS-IS; a este proceso se llama enlace agrupado o solo agrupación. El enlace lógico resultante se llama enlace agrupado y a los enlaces físicos enlaces componentes (que son identificados por índices de interfase). La combinación de los tres identificadores (identificador del enlace (agrupado), identificador del enlace componente, etiqueta) son suficientes para identificar sin ambigüedad los recursos usados por un LSP.

El propósito del enlace agrupado es mejorar la escalabilidad del enrutamiento, reduciendo la cantidad de información que maneja el OSPF y/o IS-IS. Esta reducción se consigue realizando la agregación/abstracción de la información; pero el resultado es la pérdida de alguna información. Para limitar la cantidad de pérdidas se necesita restringir el tipo de información que se puede agregar/abstraer.

### 2.5.1 Restricciones en los agrupamientos

Todos los enlaces componentes de un agrupamiento deben empezar y acabar en el mismo par de LSRs y compartir algunas características o propiedades comunes definidas en OSPF-TE e ISIS-TE [14]; por ejemplo deben tener el mismo tipo de enlace como punto a punto o multi-acceso, la métrica de la TE (el costo administrativo), el conjunto de las clases de recursos en cada extremo del enlace (colores). Una FA también puede ser un enlace componente; de hecho un agrupamiento puede consistir en una mezcla de enlaces punto a punto y FA, pero todos compartiendo algunas propiedades comunes.

### 2.5.2 Consideraciones de enrutamiento para el agrupamiento

Un enlace agrupado es solo otra clase de enlace TE. El tiempo de vida del enlace agrupado se determina por el tiempo de vida de cada uno de sus enlaces componentes; un enlace agrupado tiene vida sí al menos uno de sus enlaces componentes está con vida. El tiempo de vida de un enlace componente se puede determinar a través de:

*Hellos* IS-IS u OSPF sobre el enlace componente.
*Hellos* RSVP (salto local).
*Hellos* LMP (enlace local).
Indicaciones de la capa 1 o capa 2.

De acuerdo con la especificación del RSVP-TE *Tunnel* se intenta usar el mecanismo *Hello* RSVP, cuando la notificación de fallos del nivel de enlace no es adecuada y no se usan enlaces no numerados, o cuando los mecanismos de detección de fallos del nodo, suministrados por el nivel de enlace, no son suficientes. Una vez que se determina que un enlace agrupado tiene vida, se puede anunciar como un enlace TE y se puede enviar la información TE. Sí los *Hellos* IS-IS/OSPF están corriendo sobre enlaces componentes, el flujo IS-IS/OSPF se puede restringir a sólo un enlace componente. Anunciar un enlace (agrupado) TE entre un par de LSRs, no implica que haya una adyacencia IGP entre estos; sólo están asociados a este enlace.

Crear un enlace agrupado consiste en agregar los parámetros TE idénticos de cada enlace componente individual para producir parámetros TE agregados. Un enlace TE tiene muchos parámetros y se deben definir adecuadas reglas de agregación para cada uno de ellos. Algunos parámetros pueden ser sumas de características de componente, como el ancho de banda sin reservar y el máximo ancho de banda reservable. Un nodo GMPLS con enlaces agrupados debe aplicar el control de admisión en base al enlace por componente.

### 2.5.3 Consideraciones de señalización

En una ruta explícita de un LSP se elige el enlace agrupado que deberá utilizar el LSP, pero no el/los enlace(s) componente; porque la información sobre el enlace agrupado se anuncia, pero la información sobre los enlaces componentes no. La elección del enlace componente a utilizar la realiza el nodo ascendente. Si el LSP es bidireccional, el nodo ascendente elige un enlace componente en cada dirección. Para comunicar esta elección al nodo descendente hay tres mecanismos posibles:

**a) Mecanismo 1: Indicación Implícita**

Este mecanismo requiere que cada enlace componente tenga un canal de señalización dedicado. El nodo ascendente le dice al receptor qué enlace componente debe utilizar para enviar el mensaje sobre el canal de señalización dedicado del enlace componente. Este canal de señalización puede ser *in-band* u *out-of-band*; en este último caso, la asociación entre el canal de señalización y este enlace componente necesita ser configurado explícitamente.

**b) Mecanismo 2: Indicación Explícita por ID de interfase numerada**

Este mecanismo requiere que el enlace componente tenga una única dirección IP remota.

**c) Mecanismo 3: Indicación Explícita por ID de interfase sin numerar**

Con este mecanismo, a cada enlace componente no numerado se le asigna un único Identificador de Interfase (valor de 32 bits). Este objeto/TLV transporta la identificación ID de la interfase del componente en la dirección descendente para un LSP unidireccional y en la dirección ascendente para un LSP bidireccional.

Los dos últimos mecanismos no requieren que cada enlace componente, ni enlace completo (agregado) tengan su propio canal de control.

### 2.5.4 Enlace agrupado sin numerar

Un enlace agrupado puede estar numerado o no numerado independientemente de si los enlaces componentes están numerados o no. Esto afecta a cómo es anunciado un enlace agrupado en IS-IS/OSPF y al formato ERO del LSP que atraviesa el enlace agrupado. Además, los identificadores de las interfases sin numerar para todos los enlaces de salida no numerados de un determinado LSR (ya sean enlaces componentes, FAs o enlaces agrupados) deben ser únicos en el contexto de este LSR.

## 2.6 Adyacencias de envío (FA: Forwarding Adjacency)

Para mejorar la escalabilidad de MPLS TE (y GMPLS), puede ser útil agregar múltiples LSPs TE dentro de un LSP TE mayor. Los nodos intermedios solo ven el LSP externo, no necesitan mantener los estados de envío de los LSPs internos, intercambian menos mensajes de señalización y el LSP externo se puede proteger en lugar de los LSPs internos. Esto puede aumentar considerablemente la escalabilidad de la señalización.

Para crear una agregación se realiza el siguiente procedimiento:

a) Un LSR crea un LSP TE.
b) El LSR conforma una adyacencia de envío a partir de dicho LSP (anunciando este LSP como un enlace TE en IS-IS/OSPF).
c) Se permite a otros LSRs utilizar las FAs para el cálculo de sus rutas.
d) Se anidan los LSPs originados por otros LSRs en el primer LSP.

Un LSR puede (bajo su control local de configuración) anunciar un LSP como un enlace TE en IS-IS/OSPF; cuando este enlace es anunciado en la misma instancia del IS-IS/OSPF como la que determina la ruta tomada por el LSP, llamaremos a este enlace "Adyacencia de Envío LSP". Notemos que desde que la entidad anunciada es un enlace en IS-IS/OSPF, ambos extremos de los LSRs del FA-LSP deben pertenecer al mismo nivel IS-IS o área OSPF.

En general, la creación/terminación de una FA y su FA-LSP se puede dirigir por mecanismos dentro y fuera del MPLS.

El IS-IS/OSPF extiende la información de las FAs de la misma forma que extiende la información de otros enlaces. Como resultado de extender esta información, el LSR tiene en la base de datos el estado del enlace TE, la información de los enlaces convencionales y la FAs.

Cuando un LSR realiza el cálculo de la ruta utiliza enlaces convencionales y FAs. Una vez definida la ruta, el LSR usa RSVP-TE/CR-LDP para establecer la ligadura de la etiqueta a lo largo de la ruta. Las FAs necesitan extensiones simples para los protocolos de señalización y enrutamiento.

### 2.6.1 Adyacencias de enrutamiento y envío

Las FAs se pueden representar como enlaces numerados o no numerados. También una FA puede ser un grupo de LSPs entre dos nodos. Cuando una FA se crea dinámicamente, sus atributos TE son heredados del FA-LSP que indujo a su creación. El ancho de banda FA debe ser mayor que la del FA-LSP que lo indujo; pero puede ser mayor si sólo están disponibles anchos de banda discretos para el FA-LSP. En general, para las FAs generadas dinámicamente, puede ser necesario un mecanismo basado en políticas para asociar atributos a las FAs.

Un anuncio FA puede contener la información de la ruta tomada por el FA-LSP asociada con esta FA. Otros LSRs pueden usar esta información para el cálculo de la ruta. Esta información es transportada en un nuevo OSPF e IS-IS TLV llamado *Path* TLV.

Es posible que la información fundamental de la ruta pueda cambiar más adelante por las actualizaciones de configuración o las modificaciones de las rutas dinámicas; teniendo como resultado el cambio de este TLV.

Si las FAs se agrupan (por agrupamiento del enlace) y si el enlace agrupado resultante lleva un *Path* TLV; la ruta principal seguida por cada FA-LSP que conforman los enlaces componentes debe ser el mismo.

### 2.6.2 Adyacencias de enrutamiento y señalización

Por definición, dos nodos tienen una adyacencia de enrutamiento si son vecinos en el sentido IS-IS/OSPF. También dos nodos tienen una adyacencia de señalización si son vecinos en el sentido RSVP-TE/CR-LDP. Los nodos A y B son vecinos RSVP-TE si intercambian directamente mensajes RSVP-TE. La relación de vecindario incluye el intercambio de *Hellos* RSVP-TE.

Por definición, una FA es un enlace TE entre dos nodos GMPLS cuyas rutas transitan varios nodos GMPLS en la misma instancia del plano de control de GMPLS. Si dos nodos tienen uno o más enlaces TE sin FA entre ellos, se espera (aunque no es requerido) de

que estos nodos tengan una adyacencia de enrutamiento. Si dos nodos no tiene ningún enlace TE sin FA entre ellos, se espera (aunque no es requerido) que estos nodos no tengan una adyacencia de enrutamiento. Sí los enlaces TE entre dos nodos se usan para establecer LSPs, los nodos deben tener una adyacencia de señalización.
Si uno quiere establecer adyacencia de enrutamiento y/o señalización entre dos nodos, debe haber una ruta IP entre ellos. Esta ruta IP puede ser por ejemplo, un enlace TE con una capacidad de conmutación

## 2.7 Bidireccionalidad

Los enlaces a través de la red troncal óptica necesitan a menudo ser bidireccionales; es decir, necesitan ser capaces de transportar datos en ambas direcciones.

En la especificación original del MPLS las conexiones bidireccionales requieren el establecimiento de dos LSPs unidireccionales y por lo tanto la coordinación entre los puntos extremos. Esto requería que los mensajes de gestión fueran enviados a ambos extremos del LSP, solicitando que las dos direcciones sean señalizadas por los dos nodos de entrada. Esto tiene el inconveniente de necesitar dos protocolos de señalización (uno para el MPLS y otro para los mensajes de gestión) y podría pasar que las dos direcciones del LSP siguieran rutas diferentes a través de la red. También deja a los extremos con la necesidad de tener una ruta de identificación y coordinación de los dos LSPs unidireccionales para construir un único LSP bidireccional.

El GMPLS tiene extensiones del MPLS para resolver todas estas cuestiones y permitir el establecimiento de un LSP bidireccional usando un único intercambio de mensajes; esto tiene la ventaja de requerir menos señalización y además se consigue una coordinación inmediata entre las direcciones del flujo. Los extremos del LSP son definidos como iniciador y terminador; en un LSP unidireccional la entrada es el iniciador y la salida el terminador. En un LSP bidireccional los conceptos de entrada y salida, hacia arriba y hacia abajo no están claros dado que los datos fluyen en ambas direcciones; pero como el LSP se solicita originalmente desde un lugar y responden desde el otro, podemos usar los términos iniciador y terminador sin ambigüedad.

### 2.7.1 Confirmando la ruta de envío

Una Etiqueta Ascendente es un objeto introducido en las solicitudes de establecimiento del LSP por GMPLS. Permite que un LSR ascendente señalice la etiqueta que será

usada por el LSR adyacente descendente para enviar datos desde el terminador hacia el iniciador.

Las especificaciones de GMPLS establecen que cuando la solicitud del establecimiento del LSP (mensaje *Path*) llegan al terminador, la ruta de datos en el sentido contrario debe ser considerada como establecida y los datos pueden empezar a fluir inmediatamente.

Con la finalidad de garantizar esto, cada LSR de la ruta debe esperar hasta que su conmutador este completamente programado antes de enviar la solicitud de establecimiento del LSP hacia el terminador. Esto tardaría el establecimiento del LSP ya que cada conmutador puede tomarse una cantidad de tiempo considerable de estabilización. Esto se puede tratar realizando el siguiente procedimiento:

> Antes de enviar datos el LSR terminador debe esperar un tiempo para que los otros LSRs se programen satisfactoriamente. Este tiempo debe ser no mayor que el tiempo que toma el propio conmutador para su programación; pero podría ser mayor en una red compuesta por conmutadores de distintos fabricantes.
> La identificación de errores en los LSRs de tránsito deben ser inmediatamente informados como fallos del LSP y el LSR terminador debe estar preparado para manejar estas notificaciones aún si estas llegan antes que la solicitud original.

Esta propuesta permite que el tiempo de establecimiento del LSP converja con el tiempo de establecimiento de un LSP unidireccional, pero requiere conocimiento compartido y cooperación entre los conmutadores de los LSRs en tránsito.

Una solución más segura está disponible en RSVP-TE y usa el mensaje *ResvConf*. Este mensaje fluye en la misma dirección que un mensaje *Path* y confirma la recepción en el iniciador con el mensaje *Resv*. Se solicita por el terminador con un *flag* en el mensaje *Resv*.

El terminador puede usar este mensaje para confirmar que los conmutadores en los nodos de tránsito han sido programados satisfactoriamente. Cualquier LSR no debe propagar el *Resv* hacia el iniciador hasta que su conmutador este correctamente programado. Cuando el *Resv* llega al iniciador, este envía un *ResvConf* al terminador (salto a salto) y los datos pueden fluir en ambas direcciones.

Esta solución incrementa el número de intercambios de señalización, pero incrementa la estabilidad de la señalización. En general se elige esta opción para el LSR terminador y no requiere más adiciones al protocolo RSVP.

**2.8 Señalización generalizada**

La señalización GMPLS amplía algunas funciones básicas de la señalización RSVP-TE y CR-LDP y en algunos casos añade funcionalidad. Estos cambios y adiciones impactan en las propiedades básicas del LSP, en como las etiquetas son solicitadas y comunicadas, en la naturaleza unidireccional del LSP, en como se propagan los errores y en la información suministrada por la sincronización de entrada y salida.

Por estas razones la señalización GMPLS define los siguientes bloques constructivos en la parte alta de MPLS-TE:

1. Un nuevo formato genérico de solicitud de etiqueta.
2. Etiquetas para las interfases TDM, LSC y FSC; conocidas como Etiquetas Generalizadas.
3. Soporte de conmutación de longitud de onda.
4. Sugerir la etiqueta ascendentemente con fines de optimización.
5. Restricción de etiqueta ascendentemente para soportar algunas restricciones ópticas.
6. Establecimiento bidireccional del LSP.
7. Extensiones de notificación rápida de fallo.
8. Información de la protección normalmente enfocada en la protección del enlace, más la indicación primaria y secundaria del LSP.
9. Enrutamiento explícito con control de etiqueta explícita para un grado fino de control.
10. Parámetros específicos de tráfico por tecnología.
11. Manejo del estado administrativo del LSP.

El GMPLS es altamente genérico y tiene muchas opciones. Solamente los bloques constructivos 1, 2 y 10 son obligatorios dentro del formato específico que se necesita. Normalmente se deberían implementar los bloques constructivos 6 y 9. Los bloques constructivos 3, 4, 5, 7, 8 y 11 son opcionales.

Por ejemplo, en una red típica de conmutación SDH/SONET se debería implementar los bloques constructivos: 1, 2 (la etiqueta SDH/SONET), 6, 9, 10 y 11. Los bloques constructivos 7 y 8 son opcionales ya que la protección/restauración se puede conseguir usando los octetos de la cabecera SDH/SONET.

En una red típica de conmutación de longitud de onda se debería implementar los bloques constructivos: 1, 2 (formato genérico), 4, 5, 6, 7, 8, 9 y 11. El bloque constructivo 3 solo se necesita en el caso particular de conmutación de longitud de onda. Una red de conmutación de fibra debería implementar los bloques constructivos: 1, 2 (formato genérico), 6, 7, 8, 9 y 11.

Una red típica MPLS-IP no debería implementar ninguno de estos bloques constructivos, ya que la ausencia del bloque constructivo 1 indicaría MPLS-IP normal. Sin embargo, los bloques constructivos 1 y 8 se pueden usar para señalizar MPLS-IP por que beneficiaría el tipo de protección del enlace (no disponible en CR-LDP, de una forma muy básica está disponible en RSVP-TE). El bloque constructivo 2 es aquí una etiqueta MPLS normal y no se requiere un nuevo formato de etiqueta.

El GMPLS no especifica ningún perfil para las implementaciones RSVP-TE y CR-LDP que tienen que soportar GMPLS; excepto para el que está directamente relacionado a los procedimientos GMPLS. Es el fabricante el que tiene que decidir cuáles son los elementos opcionales y los procedimientos de RSVP-TE y CR-LDP que necesitan ser implementados.

### 2.9 Señalización fuera de banda

Los protocolos de señalización del MPLS no Generalizado suponen que el tráfico de datos en un LSP seguirá la misma ruta que los mensajes de señalización. Hacer esto en las redes ópticas, sería derrochar parte del ancho de banda total (ranura de tiempo o longitud de onda) al considerar este como un canal de señalización. Por estas razones la señalización sigue una ruta fuera de banda; vía un canal de control que es físicamente distinto del canal de datos. Esto simplifica la tecnología que un conmutador óptico necesitará para la implementación de su plano de datos; el plano de datos no necesita entender los protocolos sobre los que se basan los mensajes de señalización.

La señalización fuera de banda considera tres cuestiones claves para la aplicación del GMPLS en las redes ópticas:

El enrutamiento que un LSR óptico realiza durante el establecimiento del LSP debe ser extendido para calcular las distintas direcciones IP disponibles para el próximo salto y las interfases de salida para los datos y la señalización.

Los mensajes de señalización pueden necesitar ser encapsulados para asegurar que lleguen satisfactoriamente al LSR deseado del próximo salto.

Dado que los mensajes de señalización ya no van más "*in band*", necesitan una manera para indicar a la interfase de datos a la que ellos se refieren.

### 2.9.1 Cálculo del enrutamiento extendido

Cuando un LSR intenta enrutar el establecimiento del LSP en las rutas de datos y señalización primero debe calcular dos rutas de salida en el próximo salto, una para cada una de ellas. La ruta de datos debe ser evaluada y después se debe encontrar la ruta de señalización que acceda al próximo salto de la ruta de datos.

Las topologías para las redes de señalización y datos son diferentes; por lo que la decisión de enrutamiento es complicada. Cuando se han distribuido los datos, cada LSR tiene la información que necesita para calcular las rutas requeridas para la señalización fuera de banda del GMPLS.

### 2.9.2 Encapsulación del mensaje de señalización

Realizar esto requiere una función sencilla adicional en el LSR receptor, para reconocer que es el destino del paquete IP. El método requiere que el paquete IP se envíe doblemente encapsulado con una cabecera extra IP. La cabecera exterior se dirige al salto siguiente de la ruta de datos y se muestra al protocolo de datos como un IP encapsulado; mientras que la cabecera interior es la cabecera normal para un paquete RSVP.

### 2.9.3 Identificación de la interfase de datos

Un LSR puede recibir los mensajes de señalización fuera de banda en una interfase diferente de la que estaba usando para transportar los datos. Esto se puede explicar de la siguiente manera:

1) Cuando se recibe un mensaje *Path*: ¿Cómo sabe el LSR que interfase de datos se usa para señalización? Se tienen las siguientes opciones:

   En lugar de una dirección de red (IPv4 o IPv6), se puede especificar una ruta explícita como un objeto de enlace sin numerar. El ID de un enlace sin numerar en este objeto es suficiente para identificar la interfase de datos a la que se refiere el mensaje de señalización.

Se puede especificar una ruta explícita con la etiqueta del salto. Es posible que el valor de la etiqueta también podría codificar el índice de la interfase a la que se aplica la etiqueta. Por ejemplo, la etiqueta podría transportar el ID del puerto en los 16 bits más altos y el ID de la lambda en los 16 bits restantes.
La interfase de datos puede ser comunicada a través de un objeto del protocolo de señalización.

2) El LSR necesita procesar reglas para controlar su ruta explícita; así que es aceptable para el último salto referirse a la ruta de datos y no a la ruta de señalización.

### 2.9.4 Retardo de señalización

Las características del rendimiento de las redes ópticas son a menudo completamente diferentes de las redes electrónicas de conmutación de paquetes para las que se desarrolló originalmente el MPLS; entre ellas podemos citar:

El tiempo necesario para establecer un LSP óptico puede ser mayor que el correspondiente a un LSP de conmutación de paquetes, debido a la mecánica del hardware del conmutador óptico.
Las redes ópticas son particularmente estables, una vez que se ha establecido un LSP a través de una red óptica, es probable que permanezca establecido durante mucho tiempo.

Los conmutadores ópticos pueden ser relativamente lentos de programar; aunque el tiempo de seleccionar y ajustar los componentes de conmutación puede ser muy rápido, el tiempo tomado por los componentes para instalarse después de la programación puede ser mucho mayor, medido en milisegundos. Por ejemplo, un microespejo puede ser programado rápidamente, pero el espejo puede necesitar decenas de milisegundos para estabilizarse y parar la vibración después de que ha sido ajustado. No es seguro para un LSR enviar una respuesta de señalización a su vecino ascendente mientras que el espejo aún este vibrando, porque la entrada podría prematuramente enviar datos y estos se perderían o se conmutarían incorrectamente.

La solicitud de señalización progresa a través de la red salto a salto desde la entrada a la salida, después la respuesta de señalización viaja de la salida a la entrada haciendo que el conmutador se programe de acuerdo con ella. Cuando la respuesta alcanza la entrada,

se programa todo el LSP y a continuación los datos pueden empezar a fluir inmediatamente.

El tiempo tomado para establecer un LSP que atraviesa n LSRs ópticos es:

$$2*(tse) + n*(tpe) \qquad 2.1$$

Donde:

tse: Es el tiempo de señalización de extremo a extremo.

tpe: Es el tiempo de programación y establecimiento del conmutador.

En conclusión; la combinación de conmutadores ópticos y el MPLS convencional provoca un retardo considerable en el establecimiento del LSP.

Para reducir el retardo del establecimiento del LSP, GMPLS introduce el concepto de Etiqueta Sugerida. Cada LSR selecciona una etiqueta que cree que estará disponible para su uso en el enlace entre el mismo y su LSR descendente. Señala esta etiqueta en la ruta de envío de señalización e inmediatamente empieza a programar su propio conmutador con la seguridad de que esta etiqueta es la que será acordada. Cuando la respuesta de señalización vuelve al LSR, el mensaje transporta una etiqueta. Si esta etiqueta confirma la opción sugerida en la solicitud, no se hace nada más porque el conmutador ya está programado. Una vez que la programación del conmutador se haya realizado, la respuesta de señalización puede ser enviada de inmediato en forma ascendente. Si la etiqueta es diferente de la sugerida en la solicitud de señalización, el conmutador debe ser reprogramado; pero nada se pierde comparado con el caso básico donde no fue sugerida ninguna etiqueta.

### 2.10 Gestión del enlace

En el contexto del GMPLS, dos nodos se puede conectar por decenas de fibras y cada fibra se puede usar para transmitir centenares de longitudes de onda si se usa DWDM. Estas fibras y/o longitudes de onda también se pueden combinar en uno o más enlaces agrupados con fines de enrutamiento. Para esto se deben establecer canales de control para permitir la comunicación entre nodos a efectos de enrutamiento, señalización y gestión del enlace.

La gestión del enlace es un conjunto de procedimientos útiles para los nodos adyacentes que proveen servicios locales tales como la gestión del canal de control, la verificación de

la conectividad del enlace, la correlación de la propiedad del enlace y la gestión de los fallos. Entonces, se define el protocolo LMP para realizar estas operaciones. La gestión del canal de control y la correlación de la propiedad del enlace son procedimientos obligatorios para el protocolo LMP; la verificación de la conectividad del enlace y la gestión de fallos son procedimientos opcionales.

### 2.10.1 Protocolo de gestión del enlace (LMP)

Cuando se usa el GMPLS para señalizar los LSPs a través de las redes troncales ópticas, se debe tener en cuenta las siguientes consideraciones:

La mayoría de los conmutadores de una red óptica son fotónicos y por lo tanto no pueden detectar automáticamente el "*Loss of Light*"; entonces ¿cómo se puede precisar la localización de un fallo?

El enlace entre dos conmutadores consta de una agrupación numerosa de fibras ópticas, ¿cómo se puede proteger el protocolo de enrutamiento para no tener que anunciar este gran número de enlaces?

Con el gran número de fibras ¿cómo pueden acordar los dispositivos vecinos para direccionar estos enlaces sin configurar manualmente cada nodo con el esquema de numeración de enlace del otro dispositivo?

Para resolver estos puntos se utiliza el LMP [15], es así que entre dos nodos de una red óptica, puede haber múltiples enlaces paralelos ópticos transportando tráfico de datos. Estos enlaces de datos pueden ser:

Terminados eléctricamente en un nodo, en cuyo caso el nodo está siempre informado del flujo de datos.

Transparentes, en cuyo caso el nodo no puede normalmente ver los datos que fluyen (aunque en muchos dispositivos ópticos se puede usar una llave óptica para verificar el flujo de datos cuando es necesario).

En el caso general, hay un canal exclusivo de control que se usa para el intercambio de protocolo (fuera de banda), aunque también es posible que el intercambio de protocolo se realice a través de uno o más enlaces de datos (dentro de banda).

La función del LMP es verificar el cableado de los enlaces entre nodos adyacentes, verificar la operatividad del enlace de datos y localizar fallos. Por lo tanto, el intercambio

del protocolo LMP solo se requiere entre nodos adyacentes que están directamente conectados por enlaces de datos.

La gestión del enlace a través del LMP proporciona los siguientes servicios:

**a) Gestión del canal de control**

La gestión del canal de control se usa para establecer y mantener los canales de control entre dos nodos. Una "adyacencia LMP " está formada entre dos nodos que soportan las mismas capacidades del protocolo LMP, en donde los canales de control se pueden activar simultáneamente para cada adyacencia. Un canal de control puede ser configurado explícitamente o seleccionado automáticamente; usualmente el protocolo LMP asume que los canales de control son configurados explícitamente, mientras que la configuración de las capacidades del canal de control se puede negociar dinámicamente. Los canales de control entre dos nodos son físicamente distintos de los enlaces de datos; por lo tanto se han desarrollado nuevos mecanismos en el protocolo LMP para gestionar los enlaces, ambos en términos de aprovisionamiento del enlace y aislamiento de fallas.

Cada canal de control negocia individualmente sus parámetros y mantiene la conectividad usando un protocolo *Hello*. Estos últimos se requieren si los mecanismos de bajo nivel no están disponibles para detectar los fallos del enlace. El protocolo *Hello* del LMP se intenta que sea un mecanismo que reaccione rápidamente ante los fallos del canal de control, de forma que los IGP *Hellos* no se pierdan y las adyacencias asociadas del estado de enlace tampoco se borren innecesariamente. El protocolo *Hello* consta de dos fases; una fase de negociación que permite la negociación de algunos parámetros básicos del protocolo *Hello* (por ejemplo la frecuencia) y una fase "*keep-alive*" que consta de un intercambio rápido, ligero y bidireccional de mensajes *Hellos*.

La gestión del canal de control se refiere a la negociación y al mantenimiento de la propia sesión del LMP. Los mensajes *Hellos* del LMP se usan para confirmar que la sesión está aún funcionando. Es necesaria la negociación de los parámetros con el fin de acordar los valores de los parámetros por sesión, tales como los períodos de temporización del *Hello*, nivel soportado del protocolo y soporte para características opcionales del protocolo.

La negociación de los parámetros permite que un par de nodos LMP, converjan en un conjunto mutuo de parámetros de configuración. El intercambio del protocolo implica tres mensajes (*Config*, *ConfigAck*, *ConfigNack*) cada uno de los cuales puede contener un

número variable de subobjetos describiendo determinados parámetros (tales como valores de temporización y soporte de elementos opcionales del protocolo).

El mantenimiento del canal de control implica un continuo intercambio de mensajes *Hello* entre un par de nodos LMP, con la finalidad de confirmar que el canal de control aún esta operando. Durante la transferencia de operaciones LMP a un canal de control de reserva, se puede producir un fallo en el canal de control. Si ningún canal de control LMP está activo, es imposible estar seguro del estado de los enlaces de datos y el LMP no puede recoger ninguna información adicional.

**b) Correlación de la propiedad del enlace**

Como parte del protocolo LMP, se define el intercambio de correlación de la propiedad del enlace. El intercambio se usa para agregar múltiples enlaces de datos a un enlace agrupado e intercambiar, correlacionar o cambiar los parámetros de ingeniería de tráfico del enlace. El intercambio de la correlación de la propiedad del enlace se puede hacer en cualquier momento mientras funcione el enlace y no en el proceso de verificación. Permite entre otras cosas, añadir enlaces de componente a un enlace agrupado, cambiar los mecanismos de protección de un enlace, cambiar los identificadores del puerto o cambiar los identificadores del componente en un agrupamiento.

Los resultados del proceso de correlación de la propiedad del enlace son:

Confirmación de que los mapeos entre los IDs de las interfases locales y remotas son consistentes entre nodos LMP.

Confirmación de que la agregación de los enlaces de datos en los enlaces TE es consistente entre nodos LMP adyacentes.

Acuerdos sobre las propiedades y capacidades de los canales de datos.

También se define el concepto, resumen de la propiedad del enlace como una función para descubrir y acordar entre dos nodos LMP adyacentes los mapeos de los IDs de interfase y las propiedades de los enlaces de datos; esto se consigue con el intercambio de mensajes *LinkSummary / LinkSummaryAck / LinkSummaryNack*, cada uno de los cuales contiene múltiples subobjetos:

Los subobjetos del enlace TE indican los mapeos entre los IDs de los enlaces TE local y remoto, junto a otras informaciones sobre los enlaces TE (tales como la

protección y la capacidad de multiplexación). Cada enlace TE agrega múltiples enlaces de datos, indicados por los subsiguientes subobjetos del enlace de datos.

Los subobjetos del enlace de datos indican los mapeos entre los IDs de las interfases local y remota (como se determinó con la verificación del enlace o con la configuración manual) junto con la información sobre el tipo de enlace.

**c) Verificación de la conectividad del enlace**

La verificación de la conectividad del enlace tiene dos finalidades:

La verificación de la conectividad de los datos en determinados enlaces de datos.

La determinación automática del mapeo entre los IDs de las interfases local y remota; tanto para los enlaces de datos como para los enlaces TE.

En el GMPLS, los mapeos del ID de interfase determinados por la verificación de enlace del LMP, son utilizados por los LSRs para señalizar exactamente que fibra de un enlace TE es el objetivo para un LSP.

El procedimiento para la verificación del enlace implica los siguientes pasos:

El intercambio de mensajes *BeginVerify* / *BeginVerifyAck* / *BeginVerifyNack* entre los nodos LMP para iniciar la verificación del enlace. El mensaje *BeginVerify* enviado por el nodo iniciador incluye el ID del enlace TE cuyas fibras se intentan comprobar.

El envío de mensajes *Test* hacia los enlaces a comprobar, junto con el procesamiento temporizador/reintentos. Este mensaje es transmitido sobre el propio enlace de datos que está siendo verificado, no es enviado vía el canal de control normal IP. El nodo receptor comprueba si hay luz en cada una de las fibras que cree son sus extremos del enlace TE especificado.

El intercambio de mensajes *TestStatusFail* / *TestStatusSuccess* / *TestStatusAck*; para informar de los resultados de las comprobaciones del enlace de datos.

El intercambio de mensajes *EndVerify* / *EndVerifyAck*.

Los resultados del proceso de verificación del enlace son:

Determinación de que enlaces de datos han sido comprobados satisfactoriamente.

Mapeos entre los IDs de las interfases local y remota de los enlaces de datos.

Mapeos entre los IDs de las interfases local y remota de los enlaces TE.

**d) Gestión de fallos**

La gestión de fallos es un requerimiento importante desde el punto de vista operacional. La gestión de fallos incluye la detección, localización y notificación del fallo. También la localización del fallo se puede usar para soportar mecanismos específicos y locales de protección/restauración.

En las nuevas tecnologías tales como la conmutación fotónica, muchos conmutadores ópticos fotónicos son transparentes, en el sentido de que propagan la señal de la luz sin ninguna interferencia. Pueden conmutar datos por fibra, longitud de onda o ranura de tiempo sin necesidad de examinar en absoluto la señal actual. En consecuencia, si la señal desaparece debido a un fallo de algún sitio ascendente, el conmutador puede simplemente no enterarse. En el peor caso (típico), la ausencia de la señal solo es detectada cuando se necesita volverla a convertir en forma electrónica para enviarla sobre una red conmutada de paquetes. Entonces la única información, es que hay un fallo en uno de los enlaces ópticos en algún lugar del LSP a través del cual se esperaba la llegada de paquetes. La detección del fallo LMP se usa en este caso para localizar el enlace en que ocurrió el fallo y se procede de la siguiente forma:

El proceso se inicia en el nodo descendente que detectó primero el fallo en el enlace de datos.

Este nodo envía un mensaje *Channel Failure* a su vecino ascendente de este enlace.

El nodo ascendente determina que enlace(s) de datos entrante/ascendente se conecta al enlace de datos fallado saliente/descendente.

Si el correspondiente enlace de datos entrante también ha fallado, entonces el nodo ascendente responde con un mensaje *ChannelFailureAck* y propaga el proceso de detección del fallo enviando un nuevo mensaje *ChannelFailure* al nodo siguiente ascendente. Alternativamente, este nodo puede haber notado el LOL por si mismo y así ya ha propagado el *ChannelFailure* ascendentemente.

Si el correspondiente enlace de datos entrante no ha fallado; entonces el nodo ascendente ha localizado el fallo, responde al nodo descendente con un mensaje *ChannelFailureNack* y reporta el error localmente.

Los resultados del proceso son:

Una notificación de que ha fallado un determinado enlace de datos.

Una notificación del nodo que ha localizado el fallo, al enlace descendente a este nodo.

El LMP también incluye un mecanismo para los nodos; para indicar cuando determinados enlaces de datos se recuperan otra vez, vía el intercambio de mensajes *ChannelActive* / *ChannelActiveAck*.

En la fig. 2.2, las líneas azules y rosadas representan los LSPs primarios a través de la red. Cuando el enlace que comparten falla, los datos son redirigidos para que fluyan por los LSPs de reserva (líneas verdes).

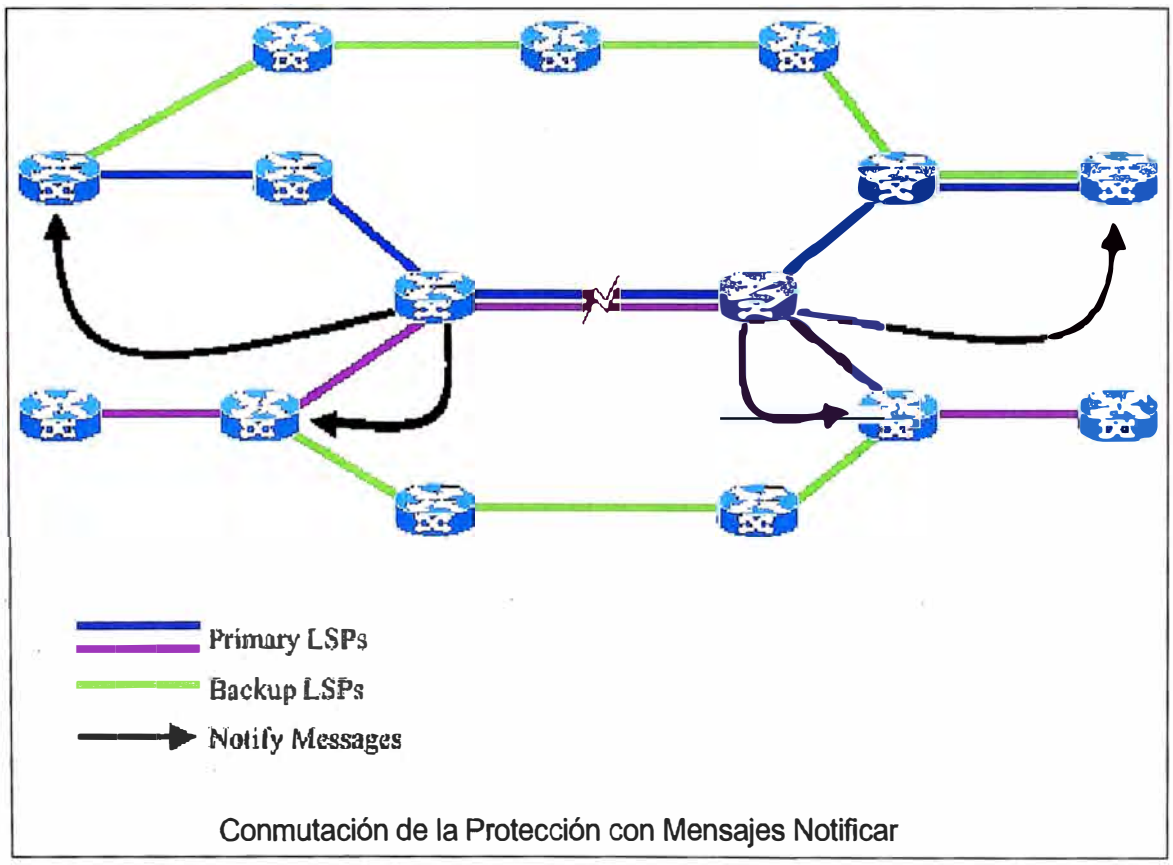


Fig. 2.2: Protección del enlace

### 2.10.2 LMP para DWDM (OLSs: Optical Line Systems)

En los entornos ópticos, el protocolo LMP se enfoca en las comunicaciones de los puertos (como por ejemplo de OXC a OXC). Muchas transacciones de información acerca de un enlace entre dos OXCs son conocidas por el OLS (OLS or TM-WDM). Presentando esta información al plano de control, se puede mejorar el uso de la red

reduciendo la configuración manual requerida y también mejorando sustancialmente la detección y la recuperación de fallos.

La detección del fallo es muy difícil cuando la red está usando conmutadores fotónicos (PXC). Una vez establecida una conexión, los PXCs solo tienen visibilidad limitada de la conexión. Aunque el PXC es todo óptico, normalmente los OLSs de larga distancia terminan los canales eléctricamente y los regeneran óptimamente, esto permite la monitorización del canal entre PXCs. Entonces el LMP-WDM se puede usar por el OLS para suministrar esta información al PXC.

Además de la información del enlace conocida por el OLS que es intercambiada a través del LMP-WDM, también se puede intercambiar alguna información conocida del OXC con el OLS a través del LMP-WDM. Esta información es útil para la gestión de las alarmas y la monitorización del enlace (por ejemplo: monitorización de la señal). La gestión de alarmas es importante porque el estado administrativo de una conexión, conocido al OXC, se puede usar para eliminar las alarmas espúreas. Por ejemplo el OXC puede conocer que una conexión está activa, caída, en modo de prueba o siendo borrada. El OXC puede usar esta información para inhibir el informe de las alarmas del OLS cuando una conexión está caída, en pruebas, o siendo borrada.

Es importante resaltar que un OXC puede estar conectado a uno o más OLSs y un OLS puede conectarse a uno o más OXCs. Aunque hay muchas similitudes entre una sesión OXC-OXC LMP y una sesión OXC-OLS LMP (en particular para la gestión del control y la verificación del enlace); también hay algunas diferencias. Estas diferencias se puede atribuir a la naturaleza de un enlace OXC-OLS y al propósito de las sesiones OXC-OLS LMP. Los enlaces OXC-OXC se pueden usar para proveer la base de la señalización del GMPLS y el enrutamiento a nivel óptico. La información intercambiada sobre sesiones LMP-WDM, se usa para aumentar el conocimiento acerca de los enlaces entre OXCs.

En cuanto a la información intercambiada sobre sesiones OXC-OLS LMP a ser usada por la sesión OXC-OXC, la información debe ser coordinada por el OXC. Sin embargo las sesiones OXC-OXC y OXC-OLS LMP corren de forma independiente y se deben mantener separadamente. Un requerimiento crítico cuando corre una sesión OXC-OLS LMP es la posibilidad del OLS de hacer transparente un enlace de datos cuando no hay procedimiento de verificación. Esto es porque el mismo enlace de datos se puede verificar entre OXC-OLS y entre OXC-OXC. El procedimiento de verificación del protocolo

LMP se usa para coordinar el procedimiento *Test* (y por lo tanto la transparencia/opacidad de los enlaces de datos). Para mantener la independencia entre las sesiones, las sesiones LMP se deben poder activar en cualquier orden. En particular debe ser posible activar una sesión OXC-OXC LMP sin que una sesión OXC-OLS LMP esté activada y viceversa.

### 2.11 Gestión de la red

Los proveedores de servicios (SPs) usan intensivamente la gestión de la red para configurar, monitorizar y aprovisionar los distintos dispositivos de su red. Es importante notar que el equipamiento de un SP se puede distribuir a través de distintos sitios separados geográficamente, haciendo gestión distribuida que aún es más importante. El SP utilizaría los NMS (*Network Management Systems*) y los protocolos de gestión estándar tales como SNMP (*Simple Network Managment* Protocol) y sus asociadas MIBs como interfases estándar para configurar, monitorizar y aprovisionar dispositivos en distintas ubicaciones. Este SP también puede usar el CLI (*Command Line Interface* ) suministrado por los fabricantes de dispositivos, pero a pesar de esto, no es una solución estándar ni recomendada debido al hecho de que no hay un lenguaje estándar CLI ni una interfase, con lo que resulta que hay N diferentes CLIs en una red con dispositivos de N fabricantes diferentes. En el contexto del GMPLS, es muy importante para las interfases estándares de los dispositivos del SP que existan debido a la propia naturaleza de la tecnología; ya que el GMPLS comprende muchos niveles de la tecnología del plano de control y del plano de datos, es importante para las interfases de gestión en esta área que sean lo suficientemente flexibles para permitir gestionar el GMPLS fácilmente y de una forma estándar.

#### 2.11.1 Sistemas de gestión de la red (NMS)

Los NMS debe mantener la información colectiva de cada dispositivo del sistema. Los NMS actualmente puede estar compuestos por varias aplicaciones distribuidas (por ejemplo: agregadores de alarmas, consolas de configuración, aplicaciones de *polling*, etc.) que colectivamente comprenden los NMS de los SPs. De esta forma, se pueden tomar decisiones de aprovisionamiento y mantenimiento con un conocimiento completo de toda la red del SP. La información de configuración o aprovisionamiento (por ejemplo: solicitudes de nuevos servicios) se puede introducir en el NMS y posteriormente distribuirlo vía SNMP a los dispositivos remotos, haciendo el trabajo de los SPs de gestión de la red mucho más compacto y con menos esfuerzo que tener que gestionar cada dispositivo individualmente. El control de la seguridad y el acceso se puede

conseguir a través del uso del SNMPv3 y el *View Access Control Model*, SNMPv3VACM [6]. Esta propuesta se puede usar muy efectivamente dentro de una red de un SP, ya que el SP tiene acceso y control sobre todos los dispositivos dentro de su dominio. Las MIBs estandarizadas deberán ser desarrolladas antes de que esta propuesta se pueda usar con fiabilidad para aprovisionar, configurar y monitorizar los dispositivos en redes heterogéneas o a través de las fronteras de los SPs.

### 2.11.2 Management Information Base (MIB)

En el contexto del GMPLS, es extremadamente importante para las interfases estándares de los dispositivos que existen debido a la naturaleza de la propia tecnología. Ya que el GMPLS comprende muchos niveles de tecnología en el plano de control, es importante que las MIBs del SNMP sean lo suficientemente flexibles para permitir gestionar todo el plano de control. Esto sería a través de un conjunto de MIBs que puedan cooperar, o a través de MIBs más generalizadas que agreguen algunas de las acciones deseadas y enviar estos detalles a los dispositivos. Es importante notar que en determinadas circunstancias, puede ser necesario duplicar algún subconjunto de objetos gestionables en nuevas MIBs para una gestión más conveniente. También, las MIBs existentes pueden necesitar ser ampliadas para facilitar algunas de las nuevas funcionalidades deseadas por el GMPLS.

### 2.11.3 Herramientas

Como en las redes tradicionales, las herramientas estándares tales como el *traceroute* [16] y *ping* [17] se necesitan para la corrección de errores y la monitorización del rendimiento de las redes GMPLS, y principalmente para la topología del plano de control que simulará la topología del plano de datos. Además, estas herramientas proveen información del acceso a la red. Los protocolos de control de GMPLS necesitarán exponer determinadas partes de información con la finalidad de que estas herramientas funcionen adecuadamente y provean información relacionada con el GMPLS. Estas herramientas deben estar disponibles vía el CLI y también deberían estar disponibles para su invocación remota vía la interfase SNMP [18].

### 2.11.4 Correlación de fallo entre múltiples niveles

Debido a la naturaleza del GMPLS y al hecho de que los potenciales niveles puedan estar implicados en el control y transmisión de la información de datos y control de GMPLS, se requiere que un fallo en un nivel se transmita a los niveles adyacentes más altos y más bajos para notificarles del fallo. Sin embargo, debido a la naturaleza de estos

niveles es probable que se necesiten cientos o miles de notificaciones para la transmisión entre niveles.

Esto no es deseable por varias razones:

Primero, estas notificaciones sobrecargan el dispositivo.

Segundo, si el/los dispositivo(s) están programados para emitir notificaciones SNMP (19) entonces el gran número de notificaciones que el dispositivo puede intentar emitir puede sobrecargar la red con una dichas notificaciones.

Además, cuando el dispositivo emita las notificaciones, el NMS que debe procesar estas notificaciones se sobrecargará o procesará información redundante.

Los dispositivos que soportan GMPLS deberían proveer mecanismos para agregar, resumir, activar y desactivar las notificaciones entre niveles. En el contexto de las MIBs de SNMP, todas las MIBs que se usan en el GMPLS deben proveer objetos de activación/desactivación para todos los objetos de notificación y también deben suministrar objetos de resumen de notificaciones o funcionalidad. Los sistemas NMS y las herramientas estándares que procesan notificaciones o hacen el seguimiento a muchos niveles de unos determinados dispositivos deben ser capaces de procesar la gran cantidad de información que potencialmente se puede emitir por los dispositivos de la red; corriendo GMPLS en cualquier punto y en cualquier instante.

## 2.12 UNI Óptico

La interfase entre un nodo frontera y un LSR en el lado de la red del GMPLS se denomina UNI (*User to Network Interface*), mientras que la interfase entre dos LSRs en el lado de la red se llama NNI (*Network to Network Interface*).

El GMPLS no especifica separadamente una UNI y una NNI. Los nodos frontera están conectados a los LSRs en el lado de la red y estos LSRs se conectan sucesivamente entre ellos. Por supuesto, el comportamiento de un nodo frontera no es exactamente igual que el comportamiento de un LSR en el lado de la red; por ejemplo: un nodo frontera puede correr un protocolo de enrutamiento, sin embargo se espera que en la mayoría de los casos no lo haga.

La diferencia entre UNI y NNI tiene sentido si ambas interfases usan protocolos diferentes, o si usan los mismos protocolos pero con algunas diferencias relevantes.

Las extensiones del GMPLS suministran una forma de usar el MPLS para aprovisionar a las redes ópticas. En una red el equipo de interconexión óptica se usa normalmente en el centro de la red; provee una alta capacidad, servicio troncal rápido para los dispositivos de los clientes que usan las tecnologías de red existentes de bajo costo y bajo ancho de banda (como enrutadores IP y conmutadores ATM).

¿Cómo las redes de paquetes o MPLS solicitan servicios de la red de transporte óptico conmutado por ranura de tiempo o lambda? Hay dos posibilidades principales: el modelo puerto y el modelo superpuesto.

### 2.12.1 Modelo puerto

En el modelo puerto [13], el mismo protocolo de señalización (GMPLS) se usa para establecer toda la ruta, tanto los paquetes como los elementos de transporte, con las solicitudes del cliente divididas en las solicitudes necesarias para establecer el túnel interno. Mientras que tiene la ventaja de suministrar un nivel de gestión único al SP, hay algunas consideraciones significativas a tomar en cuenta:

El SP puede desear mantener la información de la topología de la red troncal óptica privada.

Muchos de los equipos disponibles de la red troncal óptica, usan señalización propietaria más que GMPLS.

Los SPs pueden desear mantener las rutas establecidas en la troncal de transporte lo más estable posible, gestionando toda la red en base a los fines de protección y restauración. Denegando así que las solicitudes de servicio de la red de paquetes se efectúen automáticamente.

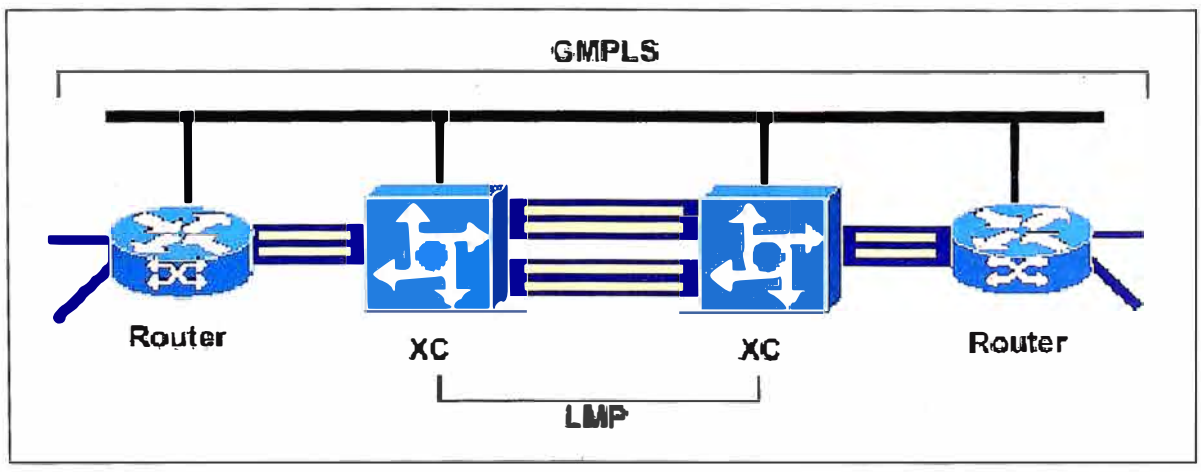


Fig. 2.3: GMPLS Modelo Puerto

### 2.12.2 Modelo superpuesto

En este modelo [13], las redes ópticas y de paquetes son gestionadas independientemente y pueden ser señalizadas por diferentes protocolos. Una solución para la OTN (*Optical Transport Network*) es suministrar una UNI que permita a los dispositivos clientes de la red solicitar conexiones a través de él dinámicamente.

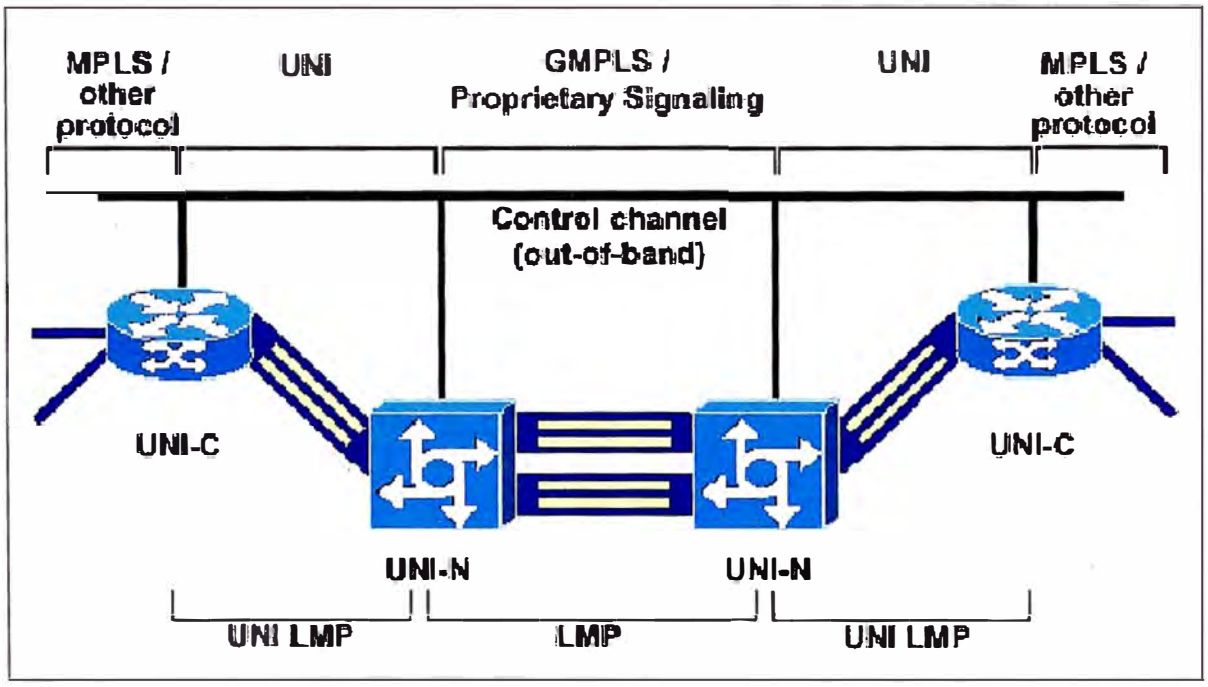


Fig. 2.4: Modelo Superpuesto

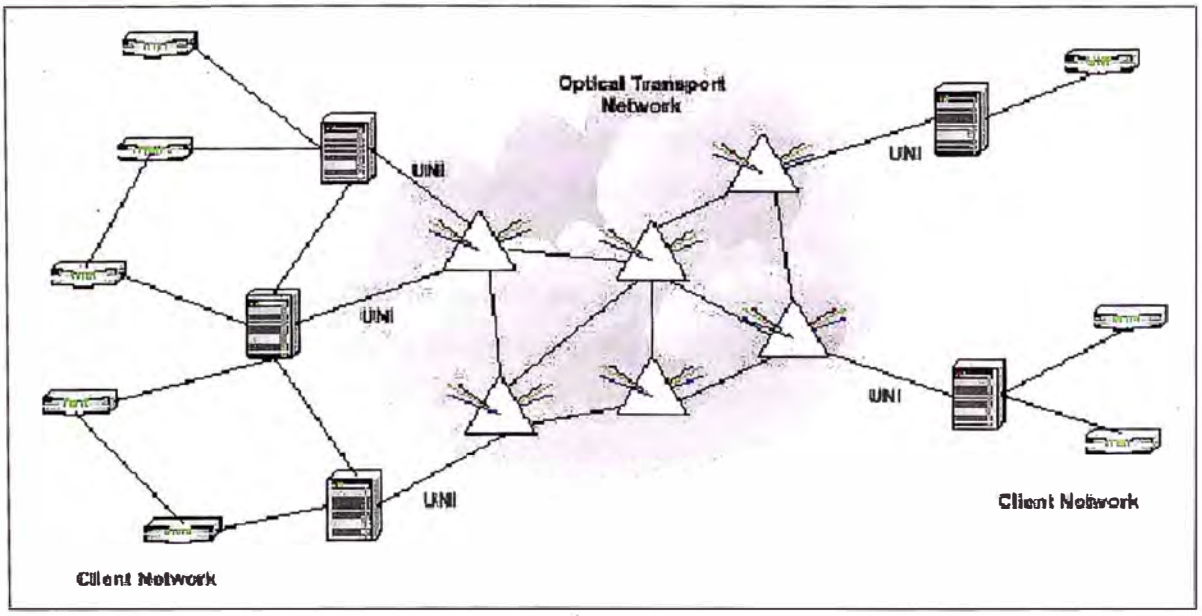


Fig. 2.5: La OTN y el Acceso UNI

Entonces, se necesita definir un protocolo de señalización como puente a la UNI. Como resultado se establece un túnel interno entre los nodos extremos de la UNI-N usando el GMPLS o algún otro mecanismo de señalización propietario. Este túnel se puede aprovisionar con tiempo o bajo demanda en respuesta a la solicitud del cliente. La ruta de datos entre los nodos cliente se establecen al superponerlos a este túnel interno.

### 2.12.3 Servicios UNI

Los nodos frontera del cliente y la OTN que soportan la UNI no son puertos de señalización tradicionales, en que el SP OTN acuerda un contrato con el cliente para suministrar un determinado nivel de servicio a través de la red. Un mensaje UNI desde el cliente a la OTN es mejor visto como una solicitud de servicio.

Es importante que haya un método definido para identificar y autenticar clientes a través de la UNI. Esto permite a la OTN verificar que la cuenta de un cliente esté autorizada antes de conceder la solicitud de conexión. Con fines de facturación y auditoria; la OTN puede realizar un seguimiento de la conexión, asignando un identificador de la conexión que es válido más allá del tiempo de vida de la conexión y devolviendo esto al cliente. Con el fin de establecer una conexión un cliente necesita descubrir que servicios están disponibles de la OTN, después de esto debe señalar sus requerimientos a través de la UNI. Los tipos de parámetros de servicio señalizados a través de la UNI son:

Ancho de banda solicitado por la conexión.
Clase de servicio (por ejemplo el servicio de protección/restauración requeridos por la red).
Diversidad.
Características específicas del plano de datos (por ejemplo: para SONET/SDH; puerto, transparencia e información de concatenación).

Un requerimiento fundamental de la UNI es que a los clientes no se les permite el acceso a las direcciones internas y a la información de la topología de la OTN. Esto significa que las solicitudes de conexión de la UNI no están permitidas a unas determinadas rutas explícitas. El parámetro diversidad permite a un cliente UNI solicitar que una nueva conexión siga una ruta diferente a un conjunto de conexiones previas sin requerir el conocimiento interno de la OTN. Esto es necesario para permitir al cliente solicitar una reserva distinta a la ruta primaria.

### 2.12.4 Direccionamiento y encaminamiento

Un cliente que solicita una conexión a través de una OTN, necesita identificar los extremos de la conexión, el propio origen y el destino usando algún esquema de direccionamiento.

La solución es usar un nuevo espacio de direcciones distinto para los clientes UNI. En este caso, la OTN asigna una sola dirección a cada extremo cliente; denominada dirección asignada a la red de transporte o dirección TNA (*Transport Network Address*). El uso de un esquema de direccionamiento que esté separado de las direcciones internas de la OTN y del protocolo cliente tiene los siguientes beneficios:

Las direcciones internas OTN no son reveladas a través de las fronteras administrativas (revelando las direcciones internas de la OTN fuera de las fronteras de la OTN se ve como un riesgo de seguridad significativo). En cambio la asignación de cada dirección cliente usando direcciones TNA y mapeando entre las direcciones asignadas y las direcciones internas del conmutador es un tema dentro de las fronteras de la OTN.

La OTN puede organizar las direcciones TNA maximizando la eficiencia de encaminamiento y cálculos de accesibilidad para sus clientes.

Separando las TNAs de las direcciones cliente, la UNI puede suministrar una ruta intacta para clientes usando diferentes protocolos para la interconexión.

Al mismo tiempo, el uso de las TNAs impone determinadas responsabilidades a los clientes y a la OTN:

Los clientes se deben registrar con la OTN recibiendo luego una TNA.

La OTN debe suministrar un servicio de resolución de direcciones, que traduzca entre la dirección remota del protocolo del cliente y la dirección remota TNA.

La OTN debe ser capaz de distribuir los mapeos de la dirección TNA del cliente y la información de accesibilidad a todos los nodos frontera que suministran la UNI (intra-dominio).

Diferentes OTNs deben ser capaces de distribuir la información de direccionamiento entre ellos (inter-dominio).

### 2.12.5 Realización de la UNI en los protocolos GMPLS

Aunque la UNI no es una relación estándar puerto a puerto de GMPLS, la función de señalización requerida por la UNI es muy parecida a la conseguida por los existentes protocolos RSVP y CRLDP de señalización de GMPLS. Con algunas extensiones para soportar las características especiales de la UNI tales como el direccionamiento TNA, la diversidad y la identificación de la conexión, estos protocolos se pueden usar para la señalización de la UNI.

Similarmente las distintas funciones de gestión del enlace y de identificación del servicio que realizan el cliente y los vecinos de la UNI en la OTN se pueden conseguir con extensiones del LMP. El mapeo entre las especificaciones estándares y de los protocolos UNI no es trivial, así un nodo frontera para una OTN provista de GMPLS necesita ser capaz de correr UNI a través de algunas interfases y de señalización óptica estándar a través de otras.

Mayor información acerca de las especificaciones que describen de como los protocolos existentes se pueden extender para proveer la funcionalidad UNI se encuentran en el documento producido por el OIF (*Optical Internetworking Forum*) [21].

# CAPITULO III
# IMPLEMENTACION DEL GMPLS

Antes de describir el proceso de implementación del GMPLS, abordaremos las extensiones que incorpora este sobre el MPLS-TE.

## 3.1 Mejoras del GMPLS sobre el MPLS-TE

Algunas extensiones importantes del GMPLS sobre el MPLS-TE se detallan a continuación:

En el MPLS-TE, los enlaces atravesados por un LSP pueden incluir una mezcla de enlaces con codificaciones heterogéneas de etiquetas. El GMPLS amplía esto incluyendo enlaces donde la etiqueta se codifica como una ranura de tiempo, una longitud de onda o una posición en el espacio físico.

En el MPLS-TE, un LSP que transporta el protocolo IP tiene que empezar y terminar en un enrutador. El GMPLS amplía esto requiriendo que un LSP empiece y acabe en un tipo similar de LSR.

Los tipos de datos que pueden ser transportados en GMPLS por un LSP se amplía para permitir datos como SONET/SDH, G.709, 1Gb ó 10Gb Ethernet, etc.

El uso de FAs provee un mecanismo que puede mejorar la utilización del ancho de banda, cuando la asignación de ancho de banda se puede realizar solamente en unidades discretas; así como un mecanismo para agregar el estado de envío, permitiendo así que el número de etiquetas requeridas sea reducido.

El GMPLS permite que una etiqueta sea sugerida por un nodo ascendente con la finalidad de reducir el retardo inicial. Esta sugerencia se puede superponer por el de un nodo descendente, pero en algunos casos a costa de un tiempo inicial más alto del LSP.

El GMPLS se amplía con la finalidad de restringir el rango de etiquetas que se pueden seleccionar por un nodo descendente. En GMPLS, un nodo ascendente puede restringir las etiquetas a lo largo de un LSP ya sea de un solo salto o a lo largo de todo el LSP. Esta característica es útil en las redes ópticas cuando la conversión de la longitud de onda no está disponible.

Mientras que los LSPs tradicionales basados en TE (y aún basados en LDP) son unidireccionales, el GMPLS soporta el establecimiento de LSPs bidireccionales.

El GMPLS soporta la finalización de un LSP en un determinado puerto de salida.

El GMPLS con RSVP-TE soporta un determinado mecanismo RSVP para una notificación rápida de fallo.

Para las interfases TDM, LSC y FSC, la asignación de ancho de banda para un LSP se puede realizar solamente en unidades discretas.

Se espera tener menos etiquetas en enlaces TDM, LSC o FSC que enlaces PSC o L2SC; porque los anteriores son etiquetas físicas en vez de etiquetas lógicas.

### 3.2 Implementación del GMPLS

La implementación del GMPLS en una determinada arquitectura de red no es un proceso inmediato; es necesario analizar primero y decidir en que parte de la red se requiere este cambio y cual será el orden de la implementación. Para empezar, GMPLS y PSS (*Photonic Service Switching*) puede desarrollarse solamente en una capa del modelo tradicional de red "overlay", para posteriormente extenderse en sucesivas fases según se requiera y mejorar de este modo la eficiencia de la red. El proceso de implementación de GMPLS y PSS se puede resumir en las siguientes fases:

**Primera Fase:** Supongamos que esta es la fase inicial en la que se encuentran la mayoría de las redes actuales basadas en un modelo "*overlay*". La red de servicios IP ejecuta protocolos IP/MPLS. Por otro lado, la red de transporte (SONET/SDH óptico) utiliza protocolos propietarios o de gestión de red para facilitar la configuración y el establecimiento de las conexiones entre los elementos de la red. Las peticiones de establecimiento o de terminación de conexiones se realizan por vía telefónica o a través de una interfase *web*.

**Segunda Fase:** Se diseña para aumentar la velocidad y la precisión de las peticiones de conexión; incrementando de este modo la eficiencia y flexibilidad de la red. Se automatizan las peticiones de la red de servicio a la red de transporte para el establecimiento y terminación de las conexiones. Para ello se utiliza una interfase de señalización basada predominantemente en GMPLS.

**Tercera Fase:** Consiste en la estandarización de los protocolos a través de las capas, acercando la red hacia un control integrado de las capas de servicio y transporte. En esta fase, los protocolos GMPLS sustituyen a los protocolos propietarios y de gestión de red en la red de transporte para facilitar el establecimiento de las conexiones entre nodos.

**Cuarta Fase:** Esta es la fase final de la integración. Una vez que los operadores pueden aprovechar la eficiencia de una arquitectura de red con integración vertical, la integración del plano de control continúa. GMPLS es entonces el estándar para los protocolos de señalización y enrutamiento de todos los tipos de tráfico (longitudes de onda, TDM y paquetes) a través de la red de conmutadores PSS. Todos los elementos de red tienen ahora conocimiento del resto de elementos de red que transportan cualquier tipo de tráfico. Finalmente, la eficiencia de los conmutadores se maximiza convenientemente mediante la instalación de una combinación óptima de tarjetas de línea para los diferentes tipos de servicios en función de la carga de tráfico.

# CAPITULO IV
# BENEFICIOS AL IMPLEMENTAR GMPLS

Entre los principales beneficios que obtenemos al implementar GMPLS tenemos:

## 4.1 Técnicas de protección y restauración

Un requerimiento clave para el desarrollo de un plano de control común tanto para redes ópticas como electrónicas es la necesitad de mecanismos que permitan una gestión de fallos en los protocolos de señalización, enrutamiento y gestión de enlaces. A nivel de conexión la gestión de fallos consiste en cuatro pasos primarios:

Detección
Localización
Notificación
Mitigación

La detección de fallos debe realizarse en la capa más cercana al fallo. En las redes ópticas ésta es la capa física. Una medida de detección de fallos en la capa física es la detección de pérdida de luz (LOL: *Loss Of Light*). Se están desarrollando otras técnicas basadas en la relación señal a ruido óptico (OSNR), en la tasa de error de bit (BER) medida ópticamente, en dispersión, diafonía y atenuación.

La localización de fallos requiere la comunicación entre los nodos para determinar dónde ha ocurrido el fallo. Una consecuencia interesante de utilizar LOL para la detección de fallos es que dicha LOL se propaga en el sentido de bajada a lo largo de todo la ruta de la conexión, permitiendo a todos los nodos de bajada detectar el fallo.

El LMP incluye un procedimiento de localización de fallos diseñado para localizar fallos tanto en redes transparentes (*all-optical*) y opacas (opto-electrónicas). Este mecanismo se basa en el envío de mensajes *ChannelFail* del LMP entre nodos adyacentes sobre el canal de control, separado de los canales de datos. Esta separación del plano de control y de datos permite que se utilice un único conjunto de mensajes para la localización de fallos, independientemente del esquema de codificación del plano de datos.

Una vez que se ha detectado y localizado el fallo se utiliza la protección y restauración para mitigarlo. La diferencia entre protección y restauración se centra en las distintas escalas temporales en las que operan cada una. La protección requiere recursos preasignados y está diseñada para reaccionar rápidamente ante fallos (menos de un par de centenas de milisegundos). Por ejemplo, la conmutación de protección automática de SONET (APS) está diseñada para conmutar el tráfico de una ruta primaria a una secundaria en menos de 50 ms. Esto requiere la transmisión simultánea a lo largo de ambas rutas (llamada protección 1+1) con un selector en el nodo de recepción decidiendo que ruta utilizar. Por otra parte, la restauración se basa en el establecimiento dinámico de recursos y puede tardar más que la conmutación de protección. La restauración también conlleva al cálculo dinámico de rutas, que puede ser computacionalmente caro, si las rutas de backup no están precalculados o si los recursos precalculados ya no están disponibles.

La protección y la restauración se han abordado tradicionalmente utilizando dos técnicas:

Conmutación de ruta; en esta el fallo es tratado en los extremos de la ruta (nodos inicial y final). La conmutación de ruta se puede subdividir en protección de la ruta, donde se preasignan rutas secundarias de protección y en restauración de la ruta, donde las conexiones son reenrutadas dinámicamente o utilizando rutas precalculadas (pero no preasignadas).

En la conmutación de línea el fallo se trata en el nodo de tránsito en el que se detecta el fallo. La conmutación de línea se puede subdividir en protección *span*, donde se conmuta el tráfico a un canal paralelo alternativo y restauración de línea, donde el tráfico se conmuta a una ruta alternativa entre los dos nodos (esto implica atravesar nodos intermedios adicionales).

### 4.1.1 Mecanismos de protección

Para utilizar la protección deben existir mecanismos que permitan:

Distribuir las propiedades relevantes del enlace, como el ancho de banda de protección y las capacidades de protección.

Establecer rutas secundarias a través de la red.

Señalizar un conmutador de la ruta primaria a la secundaria y viceversa.

La nomenclatura de los mecanismos de protección es la siguiente:

Protección 1+1: Los datos de carga se transmiten simultáneamente sobre dos rutas separadas y se utiliza un selector en el nodo de recepción para elegir la mejor señal.

Protección M:N: Se comparten M rutas de backup preasignadas entre N rutas primarias; sin embargo, los datos no se replican en la ruta de backup, sino que son asignados y transmitidos por estas, sólo cuando falla la ruta primaria.

Protección 1:N: Se comparte una ruta de backup preasignada entre N rutas primarias.

Protección 1:1: Se preasigna una ruta de backup dedicada para una ruta primaria.

Entre los principales mecanismos de protección tenemos:

**a) Protección Span**

La protección span se lleva a cabo entre dos nodos adyacentes y se basa en la conmutación a un canal o enlace de backup cuando ocurre un fallo. Como parte de las extensiones de enrutamiento GMPLS, el tipo de protección del enlace se anuncia para que se pueda utilizar la protección span en el cálculo de la ruta. Una vez que se ha seleccionado la ruta, se señaliza la conexión utilizando RSVP-TE o CR-LDP, incluyendo un vector de bits de protección que indique que LPTs (*Link Protection Type*) son aceptables para dicha conexión.

Cada nodo que proporciona una protección *span* dedicada 1+1 debe replicar los datos en dos canales separados. Esto requiere utilizar el doble de ancho de banda de la conexión entre el par de nodos y la capacidad de replicar los datos en ambos canales. Cuando se detecta un fallo en el nodo de recepción, éste debe conmutar del canal de trabajo al canal de protección.

En la protección *span* compartida M:N se tienen que detectar los fallos antes de realizar la conmutación ya que los datos no se encuentran replicados en los canales primarios y de backup. Cuando se localiza un fallo, el nodo de subida puede iniciar una protección *span* local enviando un mensaje de refresco RSVP *Path*. Los mensajes de refresco de la ruta son elementos de RSVP que permiten a los nodos intermedios actualizar el estado de un LSP. Esto permite realizar la conmutación del canal primario al de reserva. El intercambio previo de la configuración de protección compartida utilizando LMP minimiza la posibilidad de un conflicto en el canal de backup cuando se realiza la conmutación de protección. Cuando el nodo de bajada recibe el mensaje *Path* con los nuevos objetos, verifica los parámetros, actualiza el estado de señalización y responde con un mensaje Resv con la nueva etiqueta o genera un mensaje de error.

**b) Protección de la ruta**

La protección de la ruta se realiza en los nodos finales (iniciador y terminador) y requiere la conmutación a una ruta alternativa cuando se produce el fallo.

Una vez que se han calculado las dos rutas, la fuente genera dos conexiones enrutadas explícitamente con los bits activos: "dedicado 1+1" y "no protegido" respectivamente, en el vector de bits de protección del correspondiente mensaje de señalización. El establecimiento indica que estas dos rutas desean reservas compartidas. Para la protección de la ruta 1+1, la conexión se transmite simultáneamente sobre las dos rutas separadas y se utiliza un selector en el nodo terminador para elegir la mejor señal. En cada nodo, donde las dos rutas se ramifican se debe replicar los datos en ambas ramas. En los nodos en los que se unen las rutas se debe elegir los datos de una ruta basándose en la integridad de la señal.

En la protección de la ruta M:N, se pre-establecen M rutas distintas para la protección compartida de las N rutas principales. Estas rutas secundarias se utilizan para la conmutación rápida cuando la ruta principal falla. Aunque los recursos para estas rutas de backup están preasignados, el tráfico de baja prioridad puede utilizar estos recursos teniendo en cuenta que dicho tráfico será bloqueado si se produce un fallo en la ruta primaria.

### 4.1.2 Mecanismos de restauración

La restauración se ha diseñado para reaccionar rápidamente ante fallos, utilizando el ancho de banda eficientemente. Pero, normalmente requiere el establecimiento de recursos y el cálculo de rutas dinámicamente; por ello le lleva más tiempo conmutar a una ruta alternativa que las técnicas de protección. La restauración se puede implementar en la fuente o en un nodo intermedio una vez que el nodo responsable haya sido notificado mediante los mecanismos de notificación mencionados anteriormente o utilizando mensajes de error estándar.

Los mecanismos de restauración son los siguientes:

**a) Restauración de la línea**

Para soportar la restauración de línea se selecciona una nueva ruta en un nodo intermedio. Esto conlleva a que el tráfico atraviese nodos adicionales de tránsito. La restauración de línea puede ser beneficiosa para las conexiones que atraviesan múltiples

saltos y/o largas distancias ya que el retardo en la notificación del fallo puede verse considerablemente reducido. En este caso sólo se reenrutan segmentos de la conexión en lugar de toda la ruta. La restauración de línea puede romper los requerimientos TE si hay definida una ruta explícita para la conexión. Las restricciones utilizadas para enrutar la conexión pueden ser enviadas para que un nodo intermedio, que realice la restauración de línea pueda calcular una ruta alternativa apropiada. Este problema es similar al problema de establecimiento/mantenimiento de requerimientos TE que atraviesan múltiples áreas.

**b) Restauración de la ruta**

La restauración de una ruta conmuta el tráfico a una ruta alternativa alrededor del fallo, donde la nueva ruta se selecciona en el nodo fuente. Se puede optimizar el proceso de restauración, precalculando rutas alternativas y guardándolas para uso futuro. Una ruta restaurada puede reutilizar nodos de la ruta original y/o incluir nodos intermedios adicionales. Los recursos de los nodos de bajada son reutilizados (compartidos) siempre que sea posible y los recursos de los nodos intermedios que ya no se necesitan son liberados. Esta compartición de recursos aumenta las probabilidades de la conexión para conseguir los recursos requeridos cuando el reenrutamiento está en progreso. Si se calculan y preasignan los recursos, el reenrutamiento es más rápido ya que dichos recursos están garantizados; a no ser que fallen o que sean reclamados por conexiones de mayor prioridad.

## 4.2 El plano de control de GMPLS

GMPLS extiende los planos de control originales de MPLS y/o MPLS-TE para soportar cada una de las cinco interfases definidas en la sección 2.3. El plano de control de GMPLS se compone de protocolos de señalización y enrutamiento que han sido modificados para soportar GMPLS. Estos protocolos utilizan direcciones IPv4 y/o IPv6. Sólo se necesita un protocolo especializado para soportar las operaciones de GMPLS como es el LMP.

LMP proporciona mecanismos para mantener la conectividad del canal de control, verificar la conectividad física de los enlaces de datos, correlacionar la información de propiedad del enlace y gestionar los fallos en los enlaces. LMP está definido en el contexto de GMPLS, pero está especificado independientemente de la señalización GMPLS, por lo que puede utilizarse en otros contextos y con otros protocolos de señalización.

LMP puede establecer, mantener y gestionar los canales de control. Los canales de control pueden transportarse en banda o fuera de banda.

La mayoría de tecnologías que se pueden utilizar por debajo del nivel PSC requieren cierto nivel de TE. El establecimiento de LSPs a estos niveles tiene que tener en cuenta ciertas restricciones que no permiten utilizar el algoritmo SPF; en su lugar se utiliza enrutamiento SPF basado en restricciones. Los nodos que establecen los LSPs necesitan más información sobre los enlaces que la proporcionada por los protocolos estándar intra-dominio. Estos atributos TE son distribuidos utilizando los mecanismos ya existentes en los protocolos IGP.

GMPLS extiende dos protocolos *link-state* intra-dominio tradicionales OSPF-TE e IS-IS-TE. Esto es necesario para codificar y transportar uniformemente la información de un enlace TE. Un enlace TE es una representación: en los anuncios de estados de los enlaces de los protocolos OSPF e IS-IS y en la base de datos de estados de los enlaces de ciertos recursos físicos y sus propiedades entre dos nodos GMPLS.

La nueva señalización deberá soportar la creación de rutas específicas (*source routing*), transportar los parámetros requeridos del LSP (ancho de banda, tipo de señal, protección y/o restauración deseada, posición en un determinado multiplexor, etc.) para los nuevos tipos de interfases.

## CONCLUSIONES

1. La implementación de MPLS se esta realizando con mayor frecuencia en las redes actuales; debido a que optimiza los recursos y abarata los costos de operación y mantenimiento. Además las restricciones que presenta ya están siendo analizadas y resueltas por el GMPLS.

2. El GMPLS aparece como una extensión del MPLS para cubrir principalmente las tecnologías de conmutación óptica tales como DWDM, TDM y SONET/SDH; permitiendo estándares en el plano de control que permitan la construcción de redes ópticas automatizadas con dispositivos de múltiples proveedores; especificando para ello un mínimo de requerimientos de estos.

3. Con el plano de control de GMPLS en las redes ópticas, basados en la flexibilidad, el aprovisionamiento y el control se lograría la automatización de la Internet, la capacidad de Ingeniería de Tráfico de IP se realizaría con el establecimiento del LSP de MPLS.

4. El objetivo de GMPLS es integrar en un mismo plano de control; la red IP y los conmutadores ópticos, de manera que el operador vea el enrutamiento óptico como una funcionalidad más de los enrutadores IP; es decir soporta no solo dispositivos que conmutan paquetes sino también los que conmutan en el dominio del tiempo, la longitud de onda, o el espacio. Además GMPLS ofrece las ventajas propias de las estrategias de integración, como son:

   Al realizar bajo un mismo proceso la adición eléctrica con la multiplexación óptica se optimiza el uso del ancho de banda.

   El monitoreo y la protección se realiza a un nivel eléctrico, eliminado la necesidad de introducir mecanismos adicionales a nivel óptico, en consecuencia se elimina la necesidad de una gestión de la capa óptica.

5. La inclusión del LMP en el GMPLS es un gran paso para los suministradores de redes ópticas porque soluciona los problemas de interoperabilidad causados por el uso de protocolos de control y gestión no estandarizados.

6. El GMPLS será una parte integral del despliegue de la siguiente generación de las redes de datos. Suministra los puentes necesarios entre los niveles IP y fotónico que permiten el crecimiento interoperable y escalable en paralelo en las dimensiones IP y fotónicas. Con el GMPLS que rellena dinámicamente el espacio entre la infraestructura de transporte tradicional y los niveles IP, se está preparando el terreno para un rápido despliegue de servicios y eficiencias operacionales. Las provisiones necesarias han sido realizadas para soportar una suave transición desde un transporte segregado tradicional y un modelo superpuesto de servicio a un modelo de puerto más unificado.

7. La funcionalidad proporcionada por el GMPLS, su asociada noción generalizada de una jerarquía de LSPs y la agrupación crea suficiente flexibilidad para el soporte de la segregación o la unificación de cualquier requerimiento operacional deseado por un operador. Con la racionalización del soporte de la multiplexación y la conmutación en una forma jerárquica y combinando con la Ingeniería de Tráfico de MPLS, el valor de la conmutación óptica de GMPLS será esencial en cualquier solución que requiera gestionar grandes volúmenes de tráfico de una forma muy eficiente en cuanto a costos para los proveedores de servicios.

| | |
|---|---|
| MIB | Managment Information Base |
| MPLS | Multi-Protocol Label Switching |
| NHLFE | Next Hop Label Forwarding Entry |
| NMS | Network Management System |
| NNI | Network to Network Interfase |
| O-UNI | Optical User to Network Interfase |
| OEO | Optical-Electronic-Optical |
| OIF | Optical Internetworking Forum |
| OLS | Optical Line Systems |
| OSNR | Optical Signal to Noise Ratio |
| OSPF | Open Shortest Path First |
| OTN | Optical Transport Network |
| OXC | Optical Cross-Connect |
| PSC | Packet Switched Capable |
| PSS | Photonic Service Switched |
| PXC | Photonic Cross-Connect |
| RRO | Record Route Object |
| RSVP | ReSource reserVation Protocol |
| RSVP-TE | ReSerVation Protocol Traffic Engineering |
| SDH | Synchronous Digital Hierarchy |
| SNMP | Simple Network Management protocol |
| SONET | Synchronous Optical Network |
| SP | Service Provider |
| SPF | Shortest Path First |
| SVC | Switched Virtual Circuit |
| SVP | Switched Virtual Path |
| TCP | Transport Control Protocol |
| TDM | Time-Division Multiplexing |
| TE | Traffic Engineering |
| TLV | Threshold Limit Value |
| TM | Terminal Multiplex |
| TNA | Transport Network Address |
| TTL | Time To Live |
| UNI | User to Network Interfase |
| VC | Virtual Circuit |
| VCI | Virtual Circuit Identifier |

| | |
|---|---|
| VP | Virtual Path |
| VPI | Virtual Path Identifier |
| VPN | Virtual Private Network |

## BIBLIOGRAFIA


[1] RFC 3031, "Multiprotocol Label Switching Architecture" www.ietf.org

[2] E. Rosen, A. Viswanathan y R. Callon , "Multiprotocol Label Switching Architecture", Draft de Internet, 1999.

[3] Rekhter, Rosen, "Carrying Label Information in BGP-4".

[4] Awduche, Berger, Gan, Li, "Extensions to RSVP for LSP Tunnels".

[5] Andersson, Doolan, Feldman, Fredette, Thomas, "LDP Specification", RFC 3036, Enero del 2001.

[6] Wijnen, B., Presuhn, R., y K. McCloghrie, "View- based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", IETF RFC 2575,Abril de 1999.

[7] Davie, Lawrence, McCloghrie, Rekhter, Rosen, "MPLS using LDP and ATM VC Switching", RFC 3035, Enero del 2001.

[8] Conta, Doolan y Malis, "Use of Label Switching on Frame Relay Network Specification", RFC 3034, Enero del 2001.

[9] D. Awduche, "Extensions to RSVP for LSP Tunnels", Draft de Internet, 1999.

[10] CCAMP Working Group, "Generalized Multi-Protocol Label Switching" Draft de Internet, Agosto del 2002.

[11] B.Jamoussi, "Constraint-Based LSP Setup Using LDP", Draft de Internet, Enero de 1999.

[12] Angela Belda, "Generalized Multi-Protocol Label Switching", Setiembre del 2002, www.opencontent.org/openpub/

[13] Ayan Banerjee, John Drake, Jonathan Lang y Brad Turner, "GMPLS: Una Visión de las Mejoras de Enrutamiento y Gestión", Enero del 2001.

[14] K. Kompella, "IS-.IS Extensions in Support of GMPLS", "OSPF Extensions in Support of GMPLS", Drafts de Internet, Julio del 2002.

[15] Lang, "Link Management Protocol", Draft de Internet, Agosto del 2000.

[16] G. Malking, "Traceroute Using IP Option", RFC 1393, Enero del 1993, www.ietf.org

[17] RFC 1739, " A Primer on Internet and TCP/IP Tools", Diciembre de 1994, www.ietf.org

[18] K. White, "Definitions of Managed Objects for remote ping, traceroute, and lookup operations", RFC 2925, Setiembre del 2000, www.ietf.org

[19] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to community-based SNMPv2, RFC 1901, Enero de 1996, www.ietf.org

[20] Rosen, Rekhter, Tappan, Fedorkow, Farinacci, A. Conta, "MPLS Label Stack Encoding", RFC 3032, Enero del 2001.

[21] http://www.oiforum.com/public/impagreements.html, "UNI-NNI", Enero del 2005.