DEFINICIÓN DE CRITERIOS DE DISEÑO PARA REDES OVPN CON CALIDAD DE SERVICIO (QOS) BAJO EL ESTÁNDAR DIFFSERV SOPORTADO POR EL PROTOCOLO GMPLS

DIANA MARÍA PABÓN MENDOZA
ALEXANDRA SÁNCHEZ DAZA

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO I+D NUEVAS TECNOLGÍAS EN TELECOMUNICACIONES - GNTT
POPAYÁN
2005

DEFINICIÓN DE CRITERIOS DE DISEÑO PARA REDES OVPN CON CALIDAD DE SERVICIO (QOS) BAJO EL ESTÁNDAR DIFFSERV SOPORTADO POR EL PROTOCOLO GMPLS

DIANA MARÍA PABÓN MENDOZA
ALEXANDRA SÁNCHEZ DAZA

Trabajo de Grado presentado como requisito parcial para optar al titulo de Ingeniero en Electrónica y Telecomunicaciones.

Director:
Jose Giovanny López Perafán
Ingeniero en Electrónica y Telecomunicaciones

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO I+D NUEVAS TECNOLGÍAS EN TELECOMUNICACIONES - GNTT
POPAYÁN
2005

Gracias…
A Dios que ilumina mi camino,
A mis Padres por su amor, sabiduría e incesante esfuerzo,
A mis Hermanos por su apoyo incondicional,
A mi Novio por su amor y comprensión,
A mis Familiares y Amigos por su cariño,
Y agradecimiento muy especial a los Ingenieros Giovanny López y Luis Guerrero.

Diana María..

Gracias…
A Dios por haber guiado en este largo camino y por permitirme culminar este sueño.
A mis padres por su amor, comprensión y apoyo incondicional.
A mis hermanas por creer en mis capacidades e incentivarme a seguir adelante a pesar de la adversidad.
A mis amigos y demás familiares por su confianza y aprecio.

Alexandra

AGRADECIMIENTOS

Queremos expresar nuestros agradecimientos al Ing. Giovanny López por su contribución en el desarrollo de este trabajo y al grupo de docentes de la Facultad de Ingeniería Electrónica que contribuyeron en nuestra formación.

CONTENIDO

Página

LISTA DE FIGURAS

Página

LISTA DE TABLAS

Página

INTRODUCCIÓN

El alto crecimiento del tráfico y la necesidad de dar una solución a la provisión de servicios multimedia de alta calidad, han inducido en los organismos de estandarización y en los fabricantes de equipos la creación de nuevas técnicas, tecnologías y protocolos, que, aunque hayan sido creados para solucionar problemas concretos y puntuales de la red, pueden ser estructurados y unidos convenientemente para dar una solución técnica y económica global a la provisión de servicios tanto en el escenario corporativo como residencial, creando de esta manera un nuevo concepto de redes de nueva generación.

Actualmente se deben satisfacer los requerimientos de nuevos servicios anteponiendo siempre la calidad, la eficiencia, economía, seguridad y flexibilidad, bajo esta perspectiva se plantea la prestación del servicio de red privada virtual sobre una red óptica que soporte, el plano de control GMPLS el cual le brinde la capacidad de asignación de recursos más flexible y eficientemente, y que soporte calidad de servicio bajo el modelo de servicios diferenciados (Diffserv) permitiendo que las VPNs mejoren las dificultades para proporcionar suficiente calidad de servicio y adecuada capacidad de transmisión para servicios de gran ancho de banda.

De acuerdo a lo anteriormente descrito, se realiza este documento que desarrolla unos criterios de diseño para una red privada virtual óptica que soporte GMPLS y el estándar Diffserv.

Para este fin se realizó un estudio detallado de la arquitectura del Multiprotocolo de Conmutación de Etiquetas Generalizado que abarca conceptos básicos y sus principales bloques constitutivos para construir un plano de control con múltiples tipos de conmutación y características generales en cuanto a señalización y enrutamiento.

Seguidamente se plantea la definición, requisitos funcionales y arquitectura de las redes privadas virtuales ópticas.

Con toda la información anterior se realiza después la descripción del modelo Diffserv y la arquitectura y procedimiento funcional de una OVPN que soporta GMPLS y que ofrecen calidad de servicio óptica diferenciada.

Finalmente con la investigación y el análisis alcanzado se desarrollan una serie de criterios para el diseño de una OVPN que soporta GMPLS y

calidad de servicio bajo el modelo Diffserv y que se deben tener en cuenta al diseñar una red privada virtual óptica que cumpla con estas características.

Por último se presentan una serie de conclusiones y recomendaciones que son el resultado del análisis y desarrollo del documento y que se espera sirvan de guía para el estudio y aplicación de redes de este tipo.

1. ARQUITECTURA DE GMPLS (GENERALIZED MULTIPROTOCOL LABEL SWITCHING)

El Multiprotocolo de Conmutación de Etiquetas (*Multiprotocol Label Switching*, MPLS) está creciendo en popularidad como un conjunto de protocolos para provisionar y gestionar redes de transporte. MPLS soporta una red de conmutación de paquetes para facilitar ingeniería de tráfico y permitir que se reserven recursos y se predeterminen rutas además provee enlaces virtuales o túneles para conectar nodos que se encuentran en los bordes o extremos de la red y usa etiquetas conmutadas para que los paquetes sigan automáticamente su túnel hacia su salida respectiva.

Actualmente las redes de transporte están evolucionando hacia redes de gran ancho de banda que ya no conmutan sólo paquetes, si no también longitudes de onda o bandas de longitudes de onda *(waveband*), intervalos de tiempo y aún los contenidos de fibras enteras, como por ejemplo las Redes Privadas Virtuales de tipo Óptico (OVPNs).

Con el éxito de MPLS en redes IP, se ha llevado a cabo un proceso de proveedores y normadores para generalizar su modelo de envío de información, sus protocolos de control y aplicabilidad, de tal forma que pueda cubrir también estas redes ópticas, el resultado de todo esto es la elaboración de un conjunto de drafts y normas que definenen El Multiprotocolo de Conmutación de Etiquetas Generalizado (*Generalized Multiprotocol Label Switching,* GMPLS). En este capitulo se describe la arquitectura, los conceptos básicos y principales bloques constitutivos de GMPLS para construir un plano de control en múltiples niveles de conmutación y características generales en cuanto a señalización y enrutamiento.

1.1 TIPOS DE CONMUTACIÓN Y JERARQUIAS DE ENRUTAMIENTO EN GMPLS

GMPLS difiere básicamente de MPLS, en que soporta múltiples tipos de conmutación (TDM, lambda, fibra). Este soporte adicional hacia diferentes tipos de conmutación ha llevado a GMPLS a extender ciertas funciones básicas de MPLS, y en algunos casos añadir nuevas funcionalidades. Todos estos cambios y adiciones impactan las propiedades básicas de los

caminos de Conmutación de Etiquetas (*Labels Switched Paths*, LSPs), la forma en que las etiquetas son pedidas y comunicadas, la naturaleza unidireccional de los LSPs, la forma como se propagan errores, así como la señalización y sincronismo entre los Enrutadores de Conmutación de Etiquetas (*Labels Switched Routers*, LSRs) de ingreso y egreso.

El ancho de banda disponible en una red de conmutación de Paquetes es como una autopista, en donde los paquetes van por ella y al exceder su capacidad se congestiona. Por otro lado el ancho de banda disponible en una red óptica es más parecido al de un sistema de trenes, en el que éstos parten a intervalos regulares, y cualquier información enviada debe reservar una longitud de onda o intervalo de tiempo (IT). Una vez que se hace la reserva, el viaje es completamente confiable y no hay posibilidad de congestión.

La arquitectura de MPLS[1] se ha definido para soportar el envío de Información basado en una etiqueta; en este sentido, se asume que los LSRs tengan un plano de envío que sea capaz de reconocer el inicio y final de las celdas y paquetes para poder procesar sus cabeceras. Con GMPLS se amplía la arquitectura MPLS para incluir los enrutadores LSR cuyos planos de envío reconocen o los extremos de los paquetes o de las celdas y por lo tanto no se puede enviar los datos basados en la información transportada en las cabeceras de dichos paquetes o celdas. Específicamente estos LSRs incluyen dispositivos donde la decisión de envío se basa en ranuras de tiempo, longitudes de onda o puertos físicos.

Los LSRs en las redes ópticas son dispositivos OXC (Cross Conectores Ópticos) que están emergiendo como la opción preferida para conmutar flujos en el orden de los giga, tera y petabits. En general, los enlaces entre estos conmutadores ópticos (OXCs), consisten de fibras ópticas y de variantes de conmutación. Una característica importante es que estos OXCs conmutan grandes flujos de información como una unidad, lo hacen basados en cantidades (lambdas, IT) inherentes al mismo medio, más que examinando cabeceras de cada paquete individual. Todo esto implica entonces que las interfaces de los LSRs tradicionales pueden ser extendidas, y divididas en las siguientes clases [2]:

a) Interfaces Capaces de Conmutar Paquetes (PSC -Packet-Switch Capable): son interfaces que reconocen los límites de celdas y paquetes y pueden enviar datos basados en el contenido de sus cabeceras. Los ejemplos incluyen interfaces de los enrutadores que envían datos basados en el contenido de la cabecera IP o basados en el contenido de la cabecera *"shim"* de MPLS.

b) Interfaces Capaces de Conmutar a Nivel 2 (L2SC): son interfaces que reconocen los límites de la trama/celda y pueden enviar datos basados en el contenido de la cabecera de trama/celda. Los ejemplos incluyen las interfaces de los puentes Ethernet que envían datos basados

en el contenido de la cabecera MAC y las interfaces de los enrutadores LSR de ATM que envían datos basados en los VPI/VCI de ATM.

c) Interfaces Capaces de realizar Multiplexación por División de Tiempo TDM (Time- División Multiplex Capable): son interfaces que envían información basada en intervalos de tiempo (IT) en un ciclo repetitivo. El ancho de banda de una fibra puede ser dividido en IT y la señal óptica es vista como una secuencia de tramas de información, con "N" tramas cada una de tamaño "t" viajando cada segundo "S" (el ancho de banda total de la fibra es NxS), y entonces el ancho de banda se asigna a un flujo particular, simplemente reservando una porción de cada trama. Un ejemplo de este tipo de interfaces son aquellas con las que cuentan los OXCs SDH/SONET.

d) Interfaces Capaces de Conmutar lambdas (LSC-Lambda-Switch Capable): son interfaces que envían información basada en la longitud de onda sobre la que ella es recibida. Dentro de una fibra, el ancho de banda disponible puede ser dividido por frecuencia (longitud de onda o lambda). Un OXC puede operar a niveles de longitudes de onda individuales, y este OXC puede conmutar toda la información que viene en la longitud de onda "A" de la fibra entrante, hacia la longitud de onda "B" de la fibra saliente.

La conmutación de banda de lambdas (Waveband Switching) representa una generalización de esta conmutación de lambdas en el cual se agrupa un conjunto de lambdas y se conmutan como un bloque único, esto tiene grandes beneficios, ya al reducir el número de LSPs requeridos, se ahorra en señalización y en hardware de conmutación. También, el proceso de conmutar una *waveband* puede ayudar a reducir la distorsión óptica que es introducida al separar y conmutar las diferentes lambdas individualmente.

e) Interfaces Capaces de Conmutar Fibras (FSC - Fiber-Switch Capable): son las interfaces que envían datos basados en la posición de los datos en los espacios físicos del mundo real. Un ejemplo de esta interfaz es la de un OXC que puede operar a nivel de una o varias fibras. Aquí toda la información que llega en una fibra (entrante) es conmutada para ser trasmitida hacia otra fibra saliente.

Un circuito se puede establecer únicamente entre interfaces del mismo tipo, dependiendo de la tecnología usada por la interfaz, puede recibir diferentes nombres: circuito SDH, camino óptico, camino de luz, etc. en el contexto de GMPLS, todos estos circuitos representan los LSPs.

En MPLS donde los LSPs están en paralelo, se pueden encaminar juntos hacia un túnel LSP de nivel más alto entre los LSRs de la red. Los paquetes etiquetados que entran al túnel LSP de nivel más alto les dan una etiqueta adicional para verlos a través de la red, y retiene sus

etiquetas de primer nivel para distinguirlas cuando emergen del túnel de nivel más alto. Este proceso de colocar múltiples etiquetas en un paquete se conoce como apilado de etiqueta.

Las pilas de etiquetas permiten una granularidad más fina de la clasificación del tráfico entre los nodos de entrada y salida del túnel que es visible a los LSRs de la red troncal, que encaminan los datos solamente en base a la etiqueta de más arriba de la pila. Esto ayuda a reducir tanto el tamaño de las tablas de encaminamiento 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.

En GMPLS el concepto de LSPs jerárquicos o LSP dentro de otro LSP, ya disponible en MPLS, permite construir una verdadera jerarquía de envío, una jerarquía de LSPs. Esta jerarquía de LSPs puede ocurrir sobre una misma interfaz, o entre diferentes interfaces. Por ejemplo, se puede construir una jerarquía si una interfaz es capaz de multiplexar varios caminos LSP de la misma tecnología (nivel), un camino de bajo orden SDH/SONET LSP (VC-12) anidado en un camino de mayor orden SDH/SONET LSP (VC-4).

El anidado (nested) también puede ocurrir entre interfaces, en la parte superior de esta jerarquía se encuentran las interfaces FSC, seguida por las LSC, las TDM, y luego las PSC. De esta manera como se muestra en la figura 1 un LSP que comienza y termina en una interfaz PSC, puede estar incluido dentro de otro LSP que comienza y finaliza en una interfaz TDM. Este LSP, a su vez, pudiera estar incluido (en conjunto con otros LSPs) dentro de otro LSP que comienza y termina en una interfaz LSC, éste a su vez se puede incluir dentro de otro LSP que comienza y termina en una interfaz FSC.

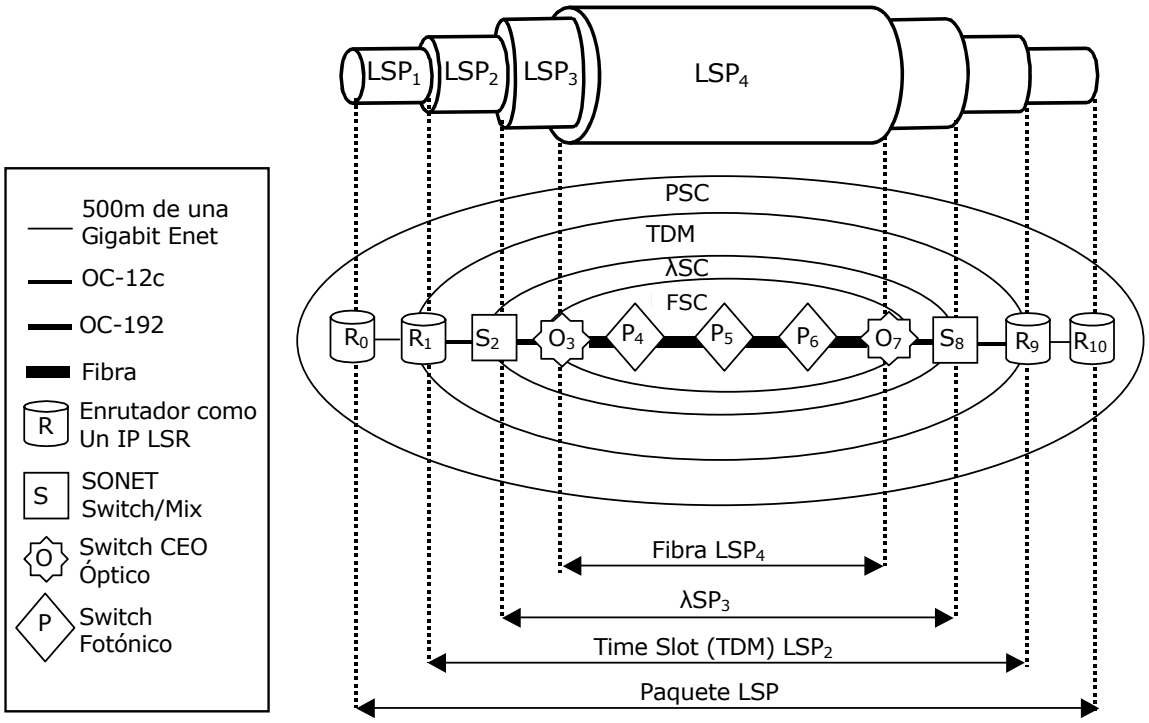


Figura1. Jerarquía de los LSPs

Los LSPs que entran y abandonan el dominio del transporte óptico en el mismo nodo pueden agregarse y ser encapsulados en un único LSP. Esta agregación permite conservar el número de lambdas que se utilizan en el dominio MPLS. La jerarquía de LSPs también ayuda a tratar con la naturaleza discreta del ancho de banda óptico. Cuando se establece un LSP, éste obtiene un ancho de banda discreto (por ejemplo 2.488 Gb/s). Sin embargo, cuando este LSP óptico se trata como un enlace, su ancho de banda no tiene porqué ser discreto. Un LSP de 100 Mb/s que atraviesa el dominio de transporte óptico puede ser encapsulado en un LSP óptico, quedando 2.388 Gb/s para otros LSPs.

1.2 PLANO DE CONTROL GMPLS

El establecimiento de los caminos LSP, cuyo tramo solo tiene interfaces Capaces de Conmutación de Paquetes (PSC) o Capaces de Conmutación de Nivel 2 (L2SC), se define en los planos de control de MPLS y/o MPLS-TE. GMPLS amplía estos planos de control para soportar cada una de las cinco clases de interfaces definidas anteriormente.

El Plano de Control Óptico está diseñado para aprovisionar los recursos ópticos de una manera más simple, rápida y flexible. MPLS se enfoca sobre el plano de información, *data plane*, que es donde se cursa el

tráfico. En cambio, GMPLS se enfoca sobre el plano de control, el cual desempeña la gestión de conexión para este *data plane*, tanto para interfaces PSC, como para las no conmutadas en paquetes (TDM, LSC, FSC). Este plano de control es responsable de mantener actualizada la topología de la red y el estado de sus recursos, así como el establecimiento, mantenimiento y desconexión de los circuitos. Estas funciones son logradas principalmente por los bloques constructivos que se basan en dos familias de protocolos, los de enrutamiento, para descubrimiento de topología y recursos, y los de señalización para provisionamiento de conexión y desconexión.

1.2.1 Protocolos de Señalización

Los protocolos de señalización son responsables de todas las acciones de gestión de conexión, se usan para establecer, remover y modificar LSPs, así como para recuperar información de ellos y son claves para el plano de control. Actualmente existen dos protocolos de señalización ampliamente usados: El Protocolo de Distribución de Etiqueta basado en Enrutamiento por Restricción (*Constraint-based Routing –Label Distribution Protocol,* CR-LDP) y el Protocolo de Reservación de Recursos con Extensión en Ingeniería de Tráfico (*Resource Reservation Protocol-Traffic Engineering Extensión,* RSVP-TE) [3]. Cualquier objeto definido dentro de la especificación GMPLS, puede ser llevado dentro de los mensajes de estos protocolos de señalización y GMPLS no detalla cual de estos dos protocolos de señalización se deben usar dejando a los fabricantes y operadores evaluar en su caso las dos posibles soluciones. (ver Anexo 1)

1.2.2 Protocolos de Enrutamiento

Los protocolos de enrutamiento pueden ser usados para dirigir los aspectos relacionados con capacidades de ruteo para los mensajes de señalización y el descubrimiento de recursos y topología nueva que existe cuando un enlace se establece o falla, o cuando un nodo es activado o desactivado ya que estos eventos cambian la topología de la red, y actúan como disparadores para que el protocolo de enrutamiento actualice los nodos y/o enlaces que se encuentran activos en determinado momento. Sin embargo una de las limitaciones tradicionales de estos protocolos ha sido el no contar con elementos de Ingeniería de Tráfico (TE). Actualmente existen básicamente dos protocolos: El Protocolo de Sistema Intermedio a Sistema Intermedio (*Intermediate System-Intermediate System*, IS-IS) y el Protocolo Primero el Camino más Corto Abierto (*Open Shortest Path First,* OSPF), los cuales han sido ampliamente usados como protocolos de enrutamiento internos (*Interior Gateway Protocol*, IGP) y han sido extendidos a (IS-IS-TE), y a (OSPF-TE) [4] para soportar ingeniería de tráfico TE. (Para ampliar los conceptos de enrutamiento en las redes ópticas ver Anexo 2)

1.2.2.1 Extensiones de TE para enrutamiento IP

Tradicionalmente, un enlace TE es anunciado como agregado a un enlace OSPF o IS-IS "normal". En el anuncio de un enlace se incluyen las propiedades del enlace y las propiedades TE del enlace.

GMPLS cambia esta noción de tres maneras:

-Primero, los enlaces que no son PSC pueden tener propiedades TE; sin embargo no se puede establecer una adyacencia OSPF directamente en dichos enlaces.

-Segundo, un LSP puede ser anunciado como un enlace TE punto a punto, en el protocolo de enrutamiento como una adyacencia de enrutamiento (FA) (ver sección 1.5), así un enlace TE anunciado no tiene que estar entre dos vecinos OSPF directos.

-Tercero, se puede anunciar una cantidad indeterminada de enlaces como un único enlace TE, por lo que de nuevo no hay una relación uno a uno entre una adyacencia regular y un enlace TE.

De esta manera se logra una noción más general de un enlace TE como un enlace lógico con propiedades TE, algunas de las cuales pueden ser configuradas en los LSR anunciantes, otras pueden obtenerse de otros LSRs mediante algún protocolo y otras pueden deducirse del o de los componentes del enlace TE.

Una propiedad importante de un enlace TE está relacionada con el ancho de banda disponible en dicho enlace. GMPLS define diferentes reglas de gestión de disponibilidad para las distintas capas no PSC. Los atributos genéricos del ancho de banda están definidos por las extensiones de enrutamiento TE y por GMPLS, como el ancho de banda no reservado, el máximo ancho de banda reservable, el máximo ancho de banda del LSP.

Un enlace TE entre una pareja de LSRs no implica la existencia de una adyacencia IGP entre dichos LSRs y este enlace TE también debe tener medios para que el LSR anunciante pueda saber de su existencia. Cuando un LSR sabe que un enlace TE está en funcionamiento y es capaz de determinar las propiedades de ingeniería de tráfico del enlace, el LSR puede anunciar dicho enlace a sus vecinos OSPF o IS-IS (ampliados por GMPLS). Las interfaces sobre las que se establecen las adyacencias OSPF o IS-IS ampliadas se llaman "canales de control".

Las extensiones a los protocolos y algoritmos de enrutamiento tradicionales se necesitan para codificar uniformemente y transportar la información de ingeniería de tráfico (TE) del enlace, y de las rutas explícitas que se requieren para la señalización. Además ahora la señalización debe ser capaz de transportar los parámetros requeridos del

LSP tales como el ancho de banda, el tipo de señal, la protección deseada y/o la restauración, la posición en una determinada multiplexación, etc. La mayoría de estas extensiones ya han sido definidas para la ingeniería de tráfico PSC y L2SC para MPLS. Primariamente GMPLS define extensiones adicionales para la ingeniería de tráfico de TDM, LSC y FSC.

1.2.3 Protocolo de gestión de enlace (LMP)

Solamente se requiere un nuevo protocolo especializado para soportar las operaciones de GMPLS, El Protocolo de Gestión del Enlace (*Link Management Protocol*, LMP). Al usar GMPLS en las redes ópticas, evidentemente surgen unos cuantos temas de gestión de redes que deben resolverse. Como ya se ha mencionado, existe un canal de control utilizado para intercambio de protocolos (fuera de banda), aunque también es posible que este intercambio se realice a través de uno o más enlaces de datos (dentro de banda), por lo tanto el trabajo fundamental que el protocolo LMP realiza, es validar el cableado y calidad en general de los enlaces entre nodos adyacentes, validar que cada enlace de datos sea operacional y localizar fallos o gestionar fallas. Por lo tanto el intercambio del protocolo LMP solo se requiere entre nodos adyacentes que están directamente conectados por enlaces de datos.

El modelo tradicional de enrutamiento IP asume el establecimiento de una adyacencia de enrutamiento sobre cada enlace conectando dos nodos adyacentes. Cada nodo necesita mantener cada una de sus adyacencias una por una, y la información de enrutamiento de estado de enlace debe fluir a través de la red, para resolver esto, se introduce el concepto de agrupación del enlace y la configuración manual y el control de estos enlaces al no ser nada práctica ha llevado a la especificación del protocolo LMP para resolver estas cuestiones.

La especificación de LMP de la IETF cubre sus áreas de funcionalidad, algunas de las cuales son opcionales dentro del protocolo y no necesitan estar presentes en una implementación de LMP, entre estás áreas se encuentran la gestión del canal de control o enlaces con ingeniería de tráfico, verificación de la conectividad física de los enlaces de datos, correlación de la información de propiedad del enlace, gestión de falla de enlace (Localización de falla y Notificación de falla) y Autenticación. Una característica única del protocolo LMP es que puede localizar los fallos en las redes opacas (opto electrónicas) y transparentes (all-optical) es decir, independiente del esquema de codificación y de la velocidad usada para los datos. (ver Anexo 1)

1.3 LA SEÑALIZACIÓN GENERALIZADA Y LAS ETIQUETAS

En MPLS, los dos LSRs en cada extremo de un enlace acuerdan como identificarán mutuamente un flujo de tráfico. Para este fin usan una etiqueta (hasta de 32 bits) que es asignada por uno de los LSRs y distribuida al otro LSR usando un protocolo de señalización. Una vez que estos LSRs han acordado este número, ellos también acuerdan que el flujo respectivo de información en cuestión, lleva ese número (etiqueta) en todos los paquetes, y por lo tanto deben ser conmutados de la misma manera.

Con GMPLS este concepto de etiqueta se puede generalizar hacia cualquier cosa que sea suficiente para identificar un flujo de tráfico. Por ejemplo, en una fibra óptica cuyo ancho de banda esté dividido en longitudes de onda, se puede asignar una lambda de éstas completa a un flujo determinado, simplemente los LSRs extremos deben acordar qué frecuencia van a usar y a diferencia de las etiquetas MPLS, en la cual cada paquete está marcado, ahora los paquetes de información, en GMPLS, no presentan ninguna marca de etiqueta, en vez de esto, el valor de la etiqueta se encuentra implícito en el hecho que la información es transportada dentro de una banda de frecuencia acordada.

GMPLS extiende así el concepto de etiqueta, de un número de 32 bits, a un arreglo de bytes de longitud variable e introduce mejoras, como ya se ha mencionado, en los protocolos de enrutamiento OSPF e IS-IS, para que los OXCs puedan intercambiar información sobre la topología de la red, estado de enlaces y cualquier otro dato referente a disponibilidades de recursos ópticos. También se introducen mejoras en los protocolos de señalización RSVP y CR-LDP para así ayudar en los procesos de establecimiento de conexiones.

A continuación se describe como las cantidades de conmutación usadas en las redes ópticas son representadas como etiquetas generalizadas:

a) Etiquetas para fibras *(Whole Fiber Labels*)
Un enlace entre LSRs puede consistir de un conjunto de fibras ópticas. En este caso el valor de la etiqueta es el número de la fibra seleccionada dentro del conjunto. La interpretación del número de fibra/puerto tiene únicamente significado local entre los LSR directamente involucrados.

b) Etiquetas para lambdas *(Wavelength Labels*)
En fibras donde exista WDM, un LSR óptico puede escoger una lambda para cursar un tráfico. En este caso, el valor de la etiqueta es el de la lambda seleccionada.

c) Etiquetas para conjuntos de lambdas *(Waveband Labels*).
Si se agrupan longitudes de onda consecutivas dentro de una banda *(waveband*), de tal forma que todas puedan ser conmutadas de la misma forma, el valor de la etiqueta es un número que identifica a esta banda *(waveband ID*) y existe un par de números (identificadores de canal) que identifican las lambdas extremos de esta banda.

d) Etiquetas para IT *(Timeslot Labels*).
En fibras donde su ancho de banda esté dividido en IT, por TDM, un conmutador óptico puede usar uno o más IT para cursar un tráfico. El valor de etiqueta TDM será suficiente para especificar el IT asignado. Los detalles exactos de la representación de etiqueta TDM depende de la jerarquía TDM en uso, por ejemplo, SONET o SDH. Una etiqueta SDH/SONET está representada por una secuencia de 5 números (S, U, K, L, M), los cuales seleccionan diferentes partes de la jerarquía en cuestión. (Ver Figura 2)

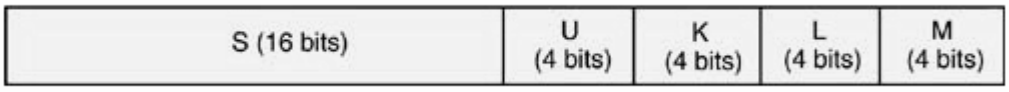


Figura 2. Etiqueta SONET / SDH

Para todos los tipos de etiquetas GMPLS descritas aquí, el valor de la etiqueta implica directamente el ancho de banda disponible para el tráfico en particular. Es decir, si una etiqueta denota un simple VT-6 de SONET, entonces el ancho de banda disponible es el de un intervalo VT-6, el razonamiento es similar para los otros tipos de etiquetas.

1.3.1. Solicitud de etiquetas generalizadas para una conexión

La filosofía utilizada en MPLS para lograr acuerdo de valores de etiquetas, previo al establecimiento de un LSP, básicamente no varía en las redes ópticas. Para entender mejor la solicitud de etiquetas generalizadas para la conexión es importante conocer que, por ejemplo un LSR A a lo largo de un LSP es ascendente de un LSR B si A es más cercano a la fuente que B, entonces, se dice que B es descendente y la solicitud se realiza así:

a- El LSR ascendente *(upstream LSR*) envía una solicitud hacia el LSR descendente *(downstream LSR*), para ello se utiliza un mensaje *Path message* (en RSVP) o *Label Request* (en CR-LDP). Esta solicitud contiene suficiente información sobre el ancho de banda (BW) y calidad de servicio requerido, para que el LSR descendente haga la escogencia de etiqueta.

b- El LSR descendente recibe esta solicitud y asigna un valor de etiqueta que satisfaga los requerimientos especificados en dicha solicitud.

c- El LSR descendente envía una respuesta al LSR ascendente *(Resv*) en RSVP o *(Label Mapping-Mapeo de Etiqueta*) en CR-LDP, el cual comunica el valor de etiqueta seleccionado.

GMPLS generaliza este mensaje de solicitud de conexión para distinguirlo de una solicitud no generalizada y para permitir llevar parámetros adicionales. En RSVP se hace esto a través del *Objeto de Solicitud de Etiqueta Generalizada*, en vez de la solicitud de etiqueta en el mensaje *Path* y en CR-LDP añadiendo un *Generalized Label Request TLV (solicitud de etiqueta generalizada TLV)* al mensaje de solicitud de etiqueta.

Algunas informaciones que necesita el LSR descendente para asignar la etiqueta apropiada, ya se encuentra implícita en el contexto, pero es necesario sin embargo, que el LSR ascendente especifique el "Tipo de Codificación LSP" *(LSP encoding type*), el cual define que la etiqueta a ser usada debe ser un IT, o un lambda, u otra cosa. Este campo soporta los siguientes valores:
ANSI PDH, ETSI PDH, SDH, SONET, DIGITAL WRAPPER, LAMBDA, FIBRA

Ya que algunos enlaces pueden anunciar, su capacidad para soportar más de un tipo de conmutación, el *Objeto de Solicitud de Etiqueta Generalizada / TLV* contiene un campo que indica el modo de Conmutación que se aplica a un LSP particular: fibras, lambdas, etc. En el caso de etiquetas SDH/SONET, puede ser necesario solicitar que el ancho de banda total para un LSP sea dividido en múltiples IT, entonces cuando el Tipo de Codificación LSP es SDH o SONET, la solicitud de etiqueta generalizada lleva campos adicionales que especifican cuántos IT se deben combinar para satisfacer la solicitud como el campo Petición de Número de Componentes *(Requested Number of Components*, RNC) y campos que informen cómo estos IT deberían ser concatenados, incluyendo la información si deberían ser contiguos, como el campo Petición de Tipo de Agrupación *(Requested Grouping Type*, RGT*).*

Una Etiqueta Generalizada solo transporta un solo nivel de etiqueta , es decir, es no jerárquico. Cuando se solicitan múltiples niveles de etiquetas (caminos LSP dentro de caminos LSP), cada camino LSP se debe establecer separadamente.

1.3.2 Restricción en la escogencia de etiquetas

Como ya se ha mencionado, la escogencia de etiqueta para cada enlace la hace el nodo descendente. Para MPLS esto está bien (son simplemente números), pero para GMPLS, en donde las etiquetas están directamente relacionadas con varios recursos de la red, esto puede causar conflictos durante la definición de los enlaces. Por ejemplo, un conmutador óptico basado en micro-espejos puede conmutar entre fibras la lambda recibida, pero no puede cambiar el valor de esa lambda.

La figura 3 muestra dos LSPs ya establecidos en una red óptica, en donde los OXCs o LSRs (se usarán indistintamente estos 2 términos) no pueden ejecutar conversión de longitudes de onda.

Cuando el LSR u OXC C necesita definir un nuevo LSP a través de D y E para llegar a G, él debe elegir una nueva longitud de onda. Si esta escogencia se le dejara al OXC G (el cual sería la forma normal de procesarlo en MPLS), G entonces pudiera escoger la etiqueta representada por la línea continua. Pero esta ya está en uso entre D y E, por lo que no podrá ser usada. Si esta escogencia se le diera al LSR C, el mismo problema ocurriría.

Es por ello que es necesario permitir a los OXCs, a lo largo de los trayectos, que restrinjan y/o influencien la escogencia de etiquetas, para así asegurar que se seleccione la etiqueta apropiada.

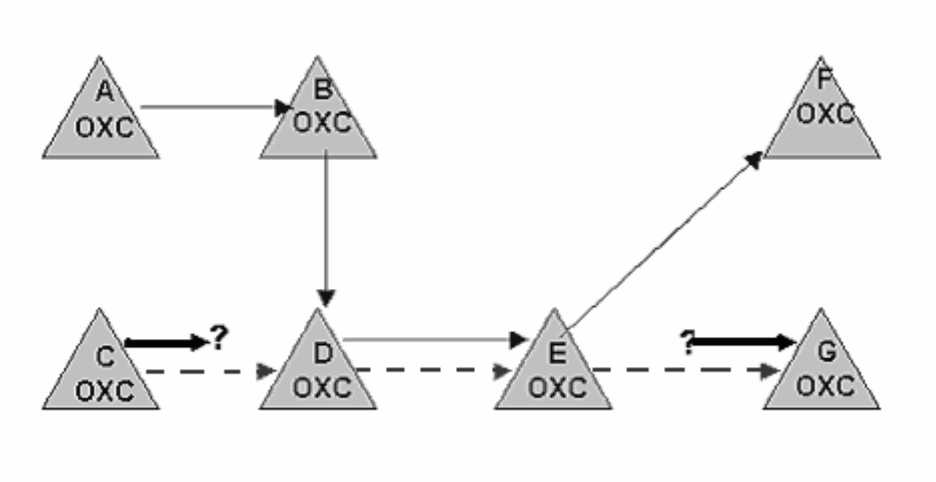


Figura 3. Conflicto de Etiquetas en Conmutadores Ópticos

Para ayudar a esto, GMPLS introduce un nuevo concepto, el Conjunto de Etiquetas *(Label Set,* LS). Un LSR ascendente incluye un LS en su mensaje de señalización (solicitud de LSP) para restringir la escogencia de etiqueta en el LSR descendente (para el enlace local entre ellos). Entonces, el LSR descendente debe seleccionar una etiqueta de lo que le indica el LS recibido, si no puede, no se establece el enlace. Esto es útil en el dominio óptico, cuando un LSR no puede convertir longitudes de onda, o cuando puede recibir y generar un subconjunto de las longitudes de onda que pueden ser conmutadas por los LSRs vecinos o si las tiene limitadas para reducir la distorsión de las señales ópticas.

El LS se construye incluyendo y excluyendo un número arbitrario de bandas y listas de etiquetas. Si no está presente un LS, el LSR descendente no está restringido en su escogencia. A medida que el LS se propaga a través del *Path message*, cada LSR puede generar un nuevo LS

saliente, basado en sus propias capacidades, así como en las propiedades de su LS entrante.

En la figura anterior, suponga ahora que el LSR C puede sólo generar longitudes de onda de un cierto rango R, él entonces señaliza un LS que dice: "cualquier cosa en el rango R, menos la longitud de onda representada por la línea punteada". El LSR D modifica esto y re-envía hacia delante: "cualquier cosa en el rango R, menos las líneas punteada y continua", el LSR E recibe este mensaje y lo envía hacia G sin modificarlo. Entonces el LSR G puede seleccionar una longitud de onda que sea aceptable para todos, en este trayecto, si existe.

Pudiera ocurrir, por ejemplo, que este LSR escogiera otra ruta, y mientras estos están en su proceso, otros LSPs B-D-E ya hubieran escogido el mismo trayecto. Esto crea conflicto también, el cual puede ser reducido a través de la implantación del concepto de Etiquetas Sugeridas que se explicara más adelante.

GMPLS también introduce el concepto de Control de Etiquetas Explícitas. Esto mejora el concepto tradicional usado en MPLS, permitiendo ahora que el LSR de ingreso especifique la(s) etiqueta(s) a ser usada(s) sobre uno, algunos o todos los enlaces enrutados explícitamente, para los trayectos en ambos sentidos.

Esto puede ser útil, por ejemplo, cuando el LSR de ingreso insiste que la longitud de onda a ser usada es la misma a través de todo el LSP. Esto puede ser deseable con el fin de evitar la distorsión de la señal óptica. También puede ser útil en Ingeniería de Tráfico (TE), donde el sistema que procesa los trayectos tiene conocimiento de las etiquetas en uso en la red, así como las capacidades de conmutación de los LSRs. En este caso, el trayecto puede ser computado para incluir las etiquetas específicas a ser usadas en cada salto. Las etiquetas explícitas son especificadas por el LSR de ingreso, como parte de la ruta explícita.

1.3.3 Etiqueta sugerida

El tiempo necesario para establecer un LSP óptico puede ser mayor que el correspondiente para un LSP no óptico, debido más que todo a la mecánica del hardware de Conmutación óptico. Esta situación está relacionada con la latencia en el switch (OXC o LSR).

En MPLS, el procedimiento usado ya estipula que el switch tiene que tener la ruta programada cuando se recibe la señal de respuesta, es decir la señal de solicitud de trayecto va progresando por la red, salto a salto, desde el ingreso hasta el nodo de egreso, la señal de respuesta va en sentido contrario, desde el egreso hacia el ingreso, lo que permite que los LSRs se vayan programando. Cuando la respuesta llega al ingreso, ya todo el LSP está programado, y la información ya puede ser enviada. Se

nota que las etiquetas son asignadas por cada nodo descendente dentro de cada salto, facilitando así situaciones de contención. De aquí que, en cada salto, la etiqueta no sea conocida por los LSR superiores, hasta que ellos reciban la señal respectiva de respuesta en el sentido contrario.

Los conmutadores ópticos pueden ser relativamente lentos para programar, aunque el tiempo para seleccionar y ajustar los componentes de conmutación puede ser muy rápido, el tiempo tomado por estos componentes para estabilizarse después de su programación puede ser mucho mayor (medido en milisegundos). Por ejemplo, un micro-espejo puede ser programado rápidamente, pero este espejo puede tomar décimas de milisegundos para estabilizarse y parar de vibrar después de su ajuste, entonces no es nada confiable para un LSR el que envíe una señal de respuesta hacia su vecino LSR superior mientras el espejo esté vibrando, ya que el LSR de ingreso pudiera de inmediato comenzar a enviar información, y ésta pudiera ser conmutada incorrectamente o perdida, de permanecer algo de esta vibración en el espejo.

Es por ello que el tiempo tomado para establecer un LSP que atraviese "n" LSRs ópticos se puede calcular con la siguiente ecuación:

$$T_{LSP} = (2 \times T_S) + (n \times T_P / T_E) \qquad \textbf{(ecuación 1)}$$

T_{LSP} = Tiempo de establecimiento del LSP
T_S = Tiempo de señalización extremo a extremo
T_P = Tiempo de programación
T_E = Tiempo de estabilización en el switch
n = Numero de LSRs ópticos que atraviesa

Para reducir esta latencia en el establecimiento del LSP, GMPLS introduce el concepto de Etiqueta Sugerida. Cada LSR selecciona una etiqueta, la cual él cree que será la más apropiada para usar en el enlace entre él y su LSR descendente. Él señaliza esta etiqueta en su trayecto de envío de señalización, e inmediatamente comienza a programar su propio conmutador, bajo la suposición que esta etiqueta será la elegida.

Cuando se recibe la respuesta, a esta señalización, el mensaje ya lleva una etiqueta. Si esta etiqueta confirma la escogencia sugerida en la solicitud respectiva, no se hace nada más, ya que el switch se encuentra programado. Cuando la programación del switch ya está totalmente estabilizada, la respuesta respectiva de señalización puede ya seguir siendo enviada en sentido ascendente.

Ahora bien, si la etiqueta es diferente de la sugerida, el switch entonces debe ser re-programado, pero en este caso ninguna información se pierde, comparado con el caso cuando ninguna etiqueta era sugerida. En el ejemplo que se muestra en la figura 4, una solicitud de señalización se

recibe en un LSR, y se asume que el protocolo de señalización es RSVP-TE, de tal forma que el mensaje es de tipo "trayecto" *(Path).*

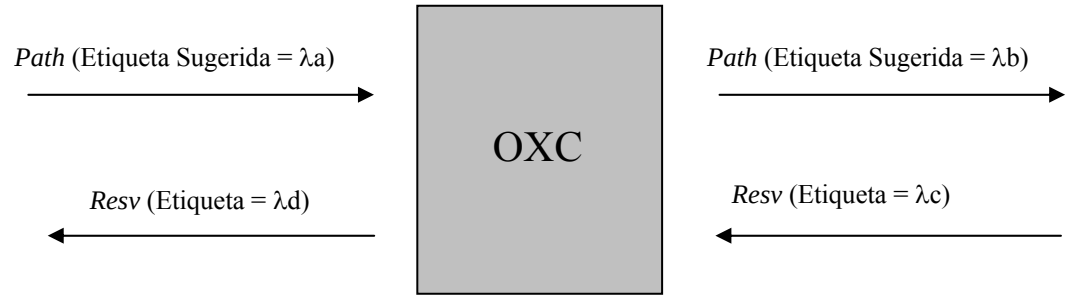


Figura 4. Sugerencia de Etiqueta

Este mensaje *Path* lleva un Objeto de Etiqueta Sugerida, que indica la etiqueta λa, que el LSR superior quisiera que fuera usada sobre el segmento de los LSPs que une estos dos LSRs. El proceso se puede explicar de la siguiente manera:

- Este OXC selecciona una etiqueta para usarla en el enlace ascendente λd = λa si es posible, pero pudiera ser otra etiqueta.

- También él selecciona otra etiqueta en sentido descendente λb (su preferida para este caso). Dependiendo de las propiedades del switch, pudiera ser la misma λ, que se va a utilizar en el sentido ascendente, es decir que, λd = λb, si es que este switch, no es capaz de modificar longitudes de onda.

- El manda también, una instrucción a su matriz de conmutación para que comience a programar la conmutación: λd x λb.

- Entonces él envía un mensaje *Path* en sentido descendente, el cual contiene la etiqueta que le gustaría fuera usada en este enlace, λb.

- En algún momento, él recibe un mensaje *Resv* desde el LSR descendente. Este indica la etiqueta a ser usada en este segmento, suponiendo que se recibe λc pueden suceder 2 cosas:

  1- Que las etiquetas sean diferentes (λc ≠ λb), entonces el switch pudiera tomar un nuevo valor para la etiqueta ascendente λd, (esto es necesario si este switch no puede hacer conversiones en longitud de onda), por ello él escoge la misma etiqueta (λd = λc ≠ λa), envía una instrucción a su matriz de conmutación para programar la nueva cros-conexión (λd x λc) y desprograma la anterior, espera que el switch esté totalmente estable.

2- Que las etiquetas sean iguales ($\lambda c = \lambda b$), en este caso no se requiere ninguna programación adicional, y entonces este OXC o LSR, debe asegurar que la solicitud respectiva se complete satisfactoriamente.

Al final de este proceso, el switch envía su mensaje *Resv* ascendente, indicando así que la etiqueta real a ser usada en ese enlace es la (λd). Si todo ya se ha completado bien, y la conversión de λ no fuera posible, entonces la etiqueta sugerida del mensaje original es usada en todos los mensajes ($\lambda a = \lambda b = \lambda c = \lambda d$).

1.3.4 LSPs bidireccionales

En las especificaciones originales de MPLS, las conexiones bidireccionales requieren el establecimiento de dos LSPs unidireccionales, y esto implica una cierta coordinación entre los dos puntos en cuestión. Se logró, para tal efecto, algunas mejoras, pero aún existía el tema pendiente de que se necesitaban cuatro mensajes de señalización (solicitud y respuesta en cada sentido) para el establecimiento del LSP.

GMPLS extendió y mejoró este concepto, necesitando un sólo mensaje para el establecimiento de este LSP bidireccional. Esto trae obviamente como beneficio el requerir menos señalización y mejor coordinación entre las dos direcciones de flujo.

En este caso, se define al *head end* del LSP como el iniciador o nodo de ingreso, y el *tail end* como el terminador o nodo de egreso. Aquí, GMPLS introduce un nuevo objeto en la solicitud de establecimiento de un LSP, el cual es la Etiqueta Ascendente *(Upstream Label)* que permite que un LSR ascendente le señalice al LSR descendente, cuál debe ser la etiqueta que debe tener el sentido ascendente (es decir, del terminador hacia el iniciador). La figura 5 muestra el intercambio de mensajes de señalización en un LSR. Una vez más se usará en el ejemplo el protocolo RSVP.

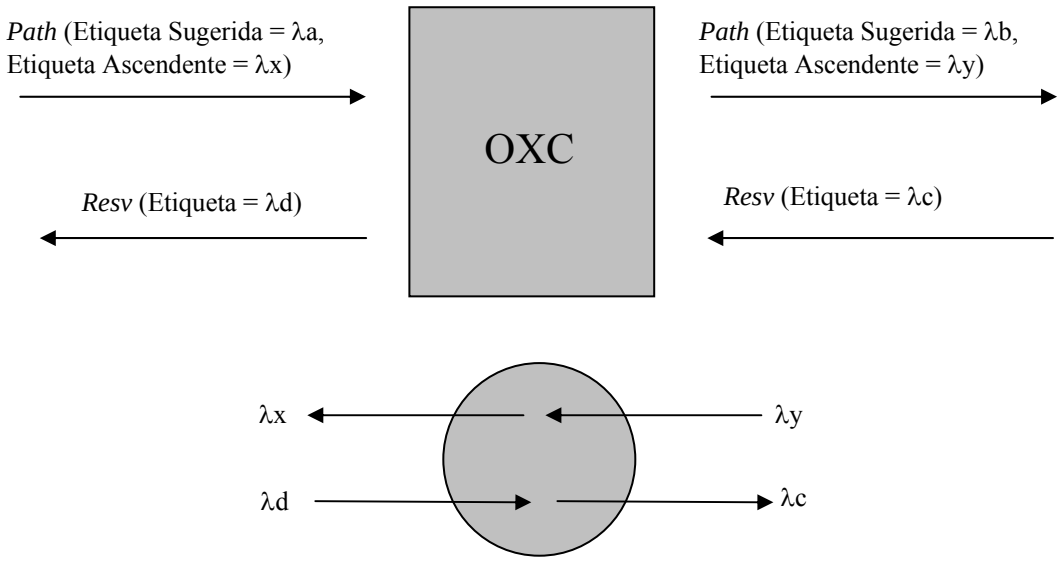


Figura 5. Establecimiento de LSP Bidireccionales

Aquí un mensaje *Path* se recibe en el LSR, este mensaje lleva una Etiqueta Sugerida, la cual es usada para pre-programar este switch en el sentido descendente, y también lleva una Etiqueta Ascendente para ser usada en el sentido contrario. Si la etiqueta indicada (λx) no es la apropiada a ser usada, él entonces debe enviar un mensaje (hacia el LSR ascendente) *Path (PathErr)* indicando tal rechazo. En este caso, dicho mensaje puede incluir una recomendación de cuáles etiquetas pudieran ser usadas del Conjunto de Etiqueta Aceptable (*Acceptable Label Set)*, entonces el LSR ascendente puede repetir el mensaje Path (hacia el LSR descendente) usando una nueva Etiqueta Ascendente escogida del conjunto de posibilidades reseñado por el *Acceptable Label Set*, o de no existir esta posibilidad, él puede entonces re-transmitir "falla en este establecimiento", continuando con la propagación del mensaje *PathErr* hacia nodos superiores.

Si el valor de la Etiqueta Ascendente es aceptable, el LSR selecciona entonces una etiqueta (λy) para ser usada como etiqueta ascendente, pero ahora en su enlace de salida descendente, y lo incluye dentro de este mensaje *Path*. Obviamente si este switch del ejemplo no puede hacer cambios de λ, entonces él mapea internamente la relación (λy = λx).

Cuando el mensaje finalmente alcanza el terminador del LSP y su switch ha sido programado, el paso inverso (sentido ascendente) debe estar completo y puede ser usado inmediatamente. Para terminar de reconfirmar y programar el trayecto descendente, hace falta que se complete el envío del mensaje *Resv* respectivo con las etiquetas definidas (λc y λd) en este caso. Al pasar este mensaje por cada switch, ya quedan cada uno de ellos programados.

Entre dos solicitudes de establecimiento del camino LSP bidireccional viajando en direcciones opuestas, puede haber contención de etiquetas. Esta contención ocurre cuando ambos lados asignan los mismos recursos (puertos) al mismo tiempo. La señalización GMPLS define un procedimiento para resolver esta contención, determinando que el nodo con la ID de nodo más alta gana la contención.

1.3.4.1. Confirmando el Camino de Envío

Con el proceso descrito anteriormente las especificaciones GMPLS establecen que cuando la solicitud de establecimiento del LSP (mensaje Path) llega al terminador, el camino de datos inverso debe ser considerado como establecido y los datos pueden empezar a fluir inmediatamente.

El propósito de sugerencia de etiqueta se frustra cuando se habla del retardo en el nodo terminador porque cada LSR del camino puede considerar que tiene que esperar hasta que su conmutador esté completamente programado antes de enviar la solicitud de establecimiento del LSP hacia el terminador lo que hace muy lento el establecimiento del LSP, ya que cada conmutador puede tomarse una cantidad de tiempo considerable de estabilización.

Alternativamente los LSRs del camino pueden simplemente enviar la solicitud de establecimiento del LSP tan pronto como han comprobado que la programación del conmutador es probablemente satisfactoria, y continuar con la programación de fondo. Esto se confía en varios procedimientos.

Antes de enviar datos, el LSR terminador debe esperar una pequeña cantidad de tiempo para que los otros LSRs se programen satisfactoriamente. Este tiempo puede ser no mayor que el que toma para programar el propio conmutador, pero podría ser mayor en una red compuesta por conmutadores de distintos fabricantes.

La programación de errores en los LSRs de tránsito deben ser inmediatamente informados como fallos de LSP, y el LSR terminador debe estar preparado para manejar estas notificaciones de errores aún si ellas llegan antes que la solicitud original de programación. Esta propuesta permite que el tiempo de establecimiento del LSP converja con el tiempo de establecimiento de un LSP unidireccional descrito anteriormente, pero requiere conocimiento compartido y cooperación entre las implementaciones de conmutador de los LSRs de 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 del mensaje *Resv*. Se solicita por el terminador con una bandera en el mensaje *Resv*. (ver Anexo 1)

El terminador puede usar este mensaje para confirmar que los conmutadores en los nodos de tránsito han sido programados satisfactoriamente. De hecho, el *Resv* no es propagado hacia el iniciador por cualquier LSR hasta que su conmutador esté correctamente programado. Cuando el *Resv* alcanza el 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 (tres más que dos), pero aumenta la estabilidad de la señalización y no requiere más adiciones al protocolo RSVP. En CR-LDP esta opción no está disponible.

1.3.5. Señalización fuera de banda

Existen razones muy importantes del porqué, en estas redes ópticas, es muy conveniente el señalizar fuera de banda, a través del uso de un canal de control, el cual está físicamente separado del canal de información. En MPLS, la distribución de etiquetas para un determinado enlace de datos está señalizado "in band" mediante el envío de mensajes de control sobre el enlace que puede transportar los datos. Por otro lado en las redes ópticas hay fuertes razones para separar completamente los mensajes de control del tráfico de datos, siendo la señalización del tipo fuera de banda, dado que todo el tráfico de datos que pasa a través de un OXC puede ser conmutado sin referencia a los paquetes de datos individuales, no hay necesidad en cuanto al plano de datos de que el OXC entienda de las pilas de protocolos (IP, TCP, UDP etc.) que se necesitan para el manejo de los mensajes de control. En particular, puede que no sea necesario para los OXCs terminar electrónicamente los enlaces individuales.

Entre una pareja de OXCs pueden haber múltiples enlaces de datos. Podría ser antieconómico y confuso, establecer una sesión de señalización separada "in band" dentro de cada enlace. Es más eficiente gestionar los enlaces como un grupo usando una sola sesión de señalización fuera de banda. Por lo tanto normalmente una conmutación óptica separa completamente su plano de control de su plano de datos y las conexiones de control a otros conmutadores van vía una red no óptica y de menores prestaciones.

1.4 MANEJO DE FALLAS EN EL PLANO DE CONTROL

Hay dos tipos principales de fallos que pueden impactar en el plano de control. El primero se relaciona al caso donde la comunicación de control se pierde entre dos nodos vecinos, para el cual, si el canal de control está incluido en el canal de datos, el procedimiento de recuperación del canal de

datos resuelve el problema, pero si el canal de control es independiente del canal de datos, se requieren procedimientos adicionales para la recuperación de este problema. El segundo, se refiere a fallos nodales, se relaciona al caso donde un nodo pierde su estado de control (después de un re-arranque) pero no pierde su estado de envío de datos.

En las redes de transporte, estos tipos de fallos del plano de control no tienen impacto en el servicio de las conexiones existentes. Bajo estas circunstancias, debe existir un mecanismo para detectar el fallo de la comunicación de control y un procedimiento de recuperación debe garantizar la integridad de la conexión en ambos extremos del canal de control.

En cuanto al fallo del canal de control, una vez se restaura la comunicación, los protocolos de enrutamiento también se pueden recuperar pero los protocolos de señalización subyacentes deben indicar que los nodos han mantenido su estado durante el fallo. El protocolo de señalización también debe asegurar que cualquier cambio de estado que se inicie durante el fallo se sincronice entre los nodos.

En un fallo nodal, el plano de control de un nodo re-arranca y pierde la mayor parte de su información de estado. En este caso, ambos nodos ascendente y descendente deben sincronizar su información de estado con el nodo que ha re-arrancado. Con el fin de volver a sincronizar con otros nodos, el re-arranque necesitará preservar alguna información, como los mapeos de las etiquetas de entrada y salida.

1.5 EFICIENCIA EN EL MANEJO DE FALLAS

GMPLS define varias extensiones de señalización que permiten una notificación rápida de fallas y otros eventos a los nodos responsables de la restauración de los LSPs con fallos y a la gestión de errores.

1.5.1 Conjunto de Etiquetas Aceptables para notificación de Error

Estos son los casos que en el MPLS tradicional y en GMPLS se generan como consecuencia de un mensaje de error que contiene la indicación "*Valor de etiqueta inaceptable*". Cuando ocurren estos casos, puede ser útil para el nodo que genera el mensaje de error indicar que etiquetas serían aceptables. Para cubrir este caso, GMPLS introduce la posibilidad de transportar esta información vía el objeto "*Conjunto de Etiquetas Aceptables*". Un Conjunto de Etiquetas Aceptables se transporta en los apropiados mensajes de error específicos de protocolo. El formato de un Conjunto de Etiquetas Aceptable es idéntico al de un Conjunto de Etiquetas.

1.5.2. Notificación rápida

Un requerimiento clave para proporcionar fiabilidad es que la reacción ante los fallos de la red sea rápida y que se puedan tomar decisiones de manera inteligente. Como parte de la notificación de fallos, un nodo con conexiones de tránsito debería poder notificar a los nodos responsables de la restauración de las conexiones, cuándo ocurre un fallo, sin que los nodos intermedios procesen estos mensajes ni modifiquen el estado de las conexiones afectadas. El procesamiento innecesario de los mensajes en los nodos intermedios podría retrasar la notificación e incluso alterar el estado de la conexión en los mismos.

Las extensiones al RSVP-TE permiten la notificación rápida de fallos y otros eventos para determinados nodos. Para CR-LDP normalmente no hay un mecanismo similar. La primera extensión identifica donde han de ser enviadas las notificaciones del evento. La segunda provee un mensaje de Notificación para la notificación general y rápida de eventos, que permiten anunciar a los nodos no adyacentes de los fallos relacionados con el LSP. Estas extensiones se pueden usar para mecanismos de restauración rápida. Se pueden solicitar las notificaciones en ambas direcciones, ascendente y descendente.

El mensaje de Notificación difiere de los mensajes de error normalmente definidos en que pueden ser "dirigidos" a un nodo distinto del vecino inmediato ascendente o descendente y que es un mecanismo de notificación generalizado este mensaje no sustituye los mensajes de error existentes.

El mensaje de Notificación se puede enviar como (a) normalmente, donde los nodos a los que no se dirige envían el mensaje de Notificación al nodo apuntado, similar al *ResvConf* procesado en RSVP o (b) encapsulado en una nueva cabecera IP cuyo destino es igual a la dirección IP apuntada

Una aplicación importante del mensaje de Notificación es la de informar cuándo falla el plano de control pero el plano de datos todavía funciona. En este caso, al enlace se le denomina *enlace degradado*. La importancia de este mecanismo radica en el hecho de que en GMPLS los planos de control y de datos pueden encontrarse físicamente separados y fallar independientemente. En muchos casos es inaceptable eliminar un LSP simplemente porque haya fallado el plano de control. Sin embargo, los fallos en el plano de control limitan las características de gestión proporcionadas por un LSP. Como parte del procedimiento de notificación, en el mensaje de notificación se identifica el LSP afectado y el recurso que ha fallado.

1.6 TÉCNICAS DE PROTECCIÓN Y RESTAURACIÓN EN GMPLS

Un requerimiento clave para el desarrollo de un plano de control común tanto para redes ópticas como electrónicas es la necesidad de mecanismos que permitan una gestión de fallos inteligente 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 debería realizarse en la capa más cercana al fallo. En redes ópticas ésta es la capa física (óptica). Una medida de detección de fallos en la capa física es la detección de pérdida de luz (*loss of light*, LOL). Se están desarrollando otras técnicas basadas en la relación señal a ruido óptica (OSNR), la tasa de error de bit (BER) medida ópticamente, 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 sentido descendente a lo largo de todo el camino de la conexión, permitiendo a todos los nodos descendentes detectar el fallo.

Como se menciono anteriormente el protocolo LMP incluye un procedimiento de localización de fallos diseñado para localizar fallos tanto en redes transparentes y opacas. Este mecanismo se basa en el envío de mensajes *ChannelFail* de 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 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 otra parte, la restauración se basa en el establecimiento dinámico de recursos y puede llevar en tiempo un orden de magnitud mayor que la conmutación de protección. La restauración también conlleva el cálculo dinámico de rutas, que puede ser computacionalmente costoso si los caminos 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 camino y conmutación de línea. En la conmutación de camino el fallo es tratado en los extremos del

camino (nodos inicial y final) mientras que en la conmutación de línea los fallos se tratan en el nodo de tránsito en el que se detecta el fallo. La conmutación de camino se puede subdividir en protección de camino, donde se preasignan caminos secundarios de protección y en restauración de camino, donde las conexiones son reenrutadas, bien dinámicamente o bien utilizando caminos precalculados (pero no preasignados). La conmutación de línea se puede dividir 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).

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 caminos secundarios a través de la red señalizar un switch del camino primario al secundario y viceversa.

1.6.1. Mecanismos de protección

La nomenclatura de los mecanismos de protección es la siguiente:

-**Protección 1+1**: los datos de carga se transmiten simultáneamente sobre dos caminos separados y se utiliza un selector en el nodo de recepción para elegir la mejor señal.

-**Protección M:N:** se comparten M caminos de backup preasignados entre N caminos primarios, sin embargo, los datos no se replican en el camino de backup, sino que son asignados y transmitidos por él, sólo cuando falla el camino primario.

-**Protección 1:N:** se comparte un camino de backup preasignado entre N caminos primarios.

-**Protección 1:1:** se preasigna un camino de backup dedicado para un camino primario.

Las protecciones 1:N y 1:1 son casos especiales de la protección M:N.

1.6.1.1. 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 se ha seleccionado la ruta, se señaliza la conexión utilizando RSVP-TE o CR-LDP, incluyendo un vector de bits de protección que indique qué Tipo de protección de enlace (*Link Protection Type*, LPTs) 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 primario 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 del camino 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 (ver anexo 1). 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 descendente recibe el mensaje *Path* con los nuevos objetos, verifica los parámetros, actualiza el estado de señalización y, o bien responde con un mensajes *Resv* con la nueva etiqueta, o bien genera un mensaje de error.

1.6.1.2. Protección de camino

La protección de camino se realiza en los nodos finales (iniciador y terminador) y requiere la conmutación a un camino alternativo cuando se produce el fallo. Una vez se han calculado los dos caminos, la fuente genera dos conexiones enrutadas explícitamente con los bits «dedicado 1+1» y «no protegido» activos, respectivamente, en el vector de bits de protección del correspondiente mensaje de señalización. El establecimiento indica que estos dos caminos desean reservas compartidas. Para la protección de camino 1+1, la conexión se transmite simultáneamente sobre los dos caminos separados y se utiliza un selector en el nodo terminador para elegir la mejor señal. En cada nodo en el que los dos caminos se ramifican se debe replicar los datos en ambas ramas. En los nodos en los que se unen los caminos se debe elegir los datos de un camino basándose en la integridad de la señal.

En la protección de camino M:N, se preestablecen M caminos distintos para la protección compartida de los N caminos principales. Estos caminos secundarios se utilizan para la conmutación rápida cuando el camino principal falla. Aunque los recursos para estos caminos 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 el camino primario.

1.6.2 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 y por ello le lleva más tiempo conmutar a un camino alternativo 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.

1.6.2.1. Restauración de línea

Para soportar la restauración de línea se selecciona un nuevo camino en un nodo intermedio. Esto conlleva 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 la latencia en la notificación del fallo puede verse considerablemente reducida. En este caso sólo se re-enrutan segmentos de la conexión en lugar del camino entero. 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.

1.6.2.2. Restauración de camino

La restauración de camino conmuta el tráfico a una ruta alternativa alrededor del fallo, donde el nuevo camino se selecciona en el nodo fuente. Se puede optimizar el proceso de restauración, por ejemplo, precalculando rutas alternativas y guardándolas para uso futuro. Un camino restaurado puede reutilizar nodos del camino 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 re-enrutado está en progreso. Si se calculan y preasignan los recursos el re-enrutamiento es más rápido ya que dichos recursos están garantizados a no ser que fallen o que sean reclamados por conexiones de mayor prioridad.

1.7. ADYACENCIAS DE ENVÍO (FA – FORWARDING ADJACENCY)

Para mejorar la escalabilidad puede ser útil agregar varios LSPs en un LSP más grande. Los nodos intermedios sólo verían el LSP externo, no necesitan mantener estados de envío para cada LSP interno, es necesario

intercambiar menos mensajes de señalización y el LSP externo se puede proteger en lugar o además de los LSPs internos lo que aumenta la escalabilidad de la señalización

Para crear un agregado se siguen los siguientes pasos:

a) Un LSR crea un LSP TE.

b) El LSR conforma una adyacencia de envío (FA) fuera de este camino LSP (anunciándolo como un enlace TE en IS-IS/OSPF).

c) Se permite a otros LSRs utilizar las FAs para el cálculo de sus caminos.

d) Se anidan los LSPs originados por otros LSRs en este camino LSP.

Un LSR puede anunciar un LSP como un enlace TE en IS-IS/OSPF. Por lo tanto dicho LSP recibe el nombre de FA-LSP (adyacencia de envío LSP). El enlace anunciado que define la ruta tomada por el LSP es la adyacencia de envío (FA). IS-IS/OSPF difunde la información de los FAs de la misma manera que la información del resto de enlaces. Como consecuencia, en la base de datos de estado de los enlaces de un LSR aparecen enlaces convencionales y FAs.

Cuando un LSR realiza el cálculo del camino utiliza enlaces convencionales y FAs. Cuando se ha completado el cálculo, el LSR utiliza RSVP-TE/CR-LDP para marcar las etiquetas a lo largo del camino. Por definición, se determina una Adyacencia de Envío (FA) como un Enlace de ingeniería de tráfico (TE) entre dos nodos GMPLS, cuyos caminos transitan uno o más nodos GMPLS en la misma instancia del plano de control de GMPLS.

1.8. MEJORAS DE ESCALABILIDAD EN GMPLS

En las capas TDM, LSC y FSC se tienen cientos de enlaces físicos paralelos que conectan dos nodos lo que introduce nuevas restricciones en los modelos de direccionamiento y enrutamiento IP, además los nuevos sistemas DWDM permiten gran cantidad de longitudes de onda por fibra que hace impracticable asociar una dirección IP a cada extremo de cada enlace físico para representar cada enlace como una adyacencia de enrutamiento distinta y para anunciar y mantener estados de enlaces para cada uno de estos enlaces.

GMPLS amplía los modelos de enrutamiento y direccionamiento, para aumentar su escalabilidad con dos mecanismos: los enlaces no numerados y el agrupamiento de enlaces, estos mecanismos se pueden combinar y para implementarlos se necesitan extensiones en los protocolos de señalización y enrutamiento.

1.8.1 Enlaces no numerados

Los enlaces o interfaces no numerados son enlaces que no tienen direcciones IP. Utilizar estos enlaces implica dos necesidades: especificar enlaces no numerados en la señalización para lo cual GMPLS define extensiones simples para indicar un enlace no numerado utilizando dos objetos /TLV: Objeto de ruta Explicita (*Explicit Route Object*, ERO) y El Objeto de Ruta de Registro (*Record Route Object*, RRO) y los sub-objetos Identificación de interfaz no numerada (Unnumbered Interface ID sub-object/sub-TLV) o transportar información TE sobre enlaces no numerados en las extensiones de IGP de ISIS-TE y OSPF-TE.

Dado que los enlaces no numerados no están identificados por una dirección IP, entonces para el propósito de ingeniería de tráfico (TE) , cada extremo necesita algún tipo de identificador local para el LSR al que pertenece el enlace. Los enrutadores LSR en los dos puntos extremos de un enlace no numerado, intercambian entre ellos los identificadores que asignan al enlace. El intercambio de los identificadores se puede conseguir por configuración, por medio de el protocolo LMP, por medio de RSVP/CR-LDP especialmente en el caso donde un enlace es una Adyacencia de Envío o por medio de las extensiones IS-IS o OSPF.

Si se considera un enlace no numerado entre los enrutadores LSR A y LSR B. LSR A elige un identificador para este enlace y LSR B hace lo mismo. Desde la perspectiva de LSR A se refiere al identificador que este asignó al enlace como el "identificador local del enlace" (o solo "identificador local"), y al identificador que LSR B asignó al enlace como el "identificador remoto del enlace" (o solo "identificador remoto"). Igualmente, desde la perspectiva de LSR B el identificador que LSR B asignó al enlace es el identificador local, y el identificador que LSR A asignó al enlace es el identificador remoto. El nuevo sub-objeto de ID de interfaz no numerada /Sub-TLV para el ERO/TLV contiene la identificación IP del enrutador LSR en el extremo ascendente del enlace no numerado y el identificador de la interfaz saliente o el identificador local del enlace con respecto al enrutador LSR ascendente. El nuevo sub-objeto ID de interfaz no numerada para el RRO contiene el identificador de la interfaz saliente con respecto al enrutador LSR que lo añade en el RRO.

La necesidad de transportar información TE sobre los enlaces no numerados en las extensiones IGP TE requiere igualmente definir sub-objetos en ISIS-TE y para OSPF-TE.

1.8.2. Agrupación de enlaces.

El concepto de agrupación de enlaces es fundamental en ciertas redes que emplean el plano de control de GMPLS. Si se considera una red óptica en malla donde los OXCs adyacentes están conectados por cientos de longitudes de onda paralelas, se debería anunciar por separado cada longitud de onda que pueda ser utilizada si se emplean los protocolos de

enrutamiento "link-state", como OSPF o IS-IS, con las adecuadas extensiones para el descubrimiento de recursos.

Cuando se conectan un par de LSPs mediante múltiples enlaces, es posible publicar algunos o todos estos enlaces como un único enlace en OSPF y/o IS-IS. A este proceso se le denomina agrupación de enlaces (Link Bundling) o simplemente agrupación (bundling). Al enlace lógico resultante se le denomina enlace agrupado (bundled link) y sus enlaces físicos son enlaces componentes (component links), identificados por los índices de la interfaz.

Una combinación de los tres identificadores (identificador de enlace agrupado, identificador de enlace componente y etiqueta) es suficiente para identificar el recurso apropiado utilizado por un LSP sin ambigüedad. El propósito de la agrupación de enlaces es mejorar la escalabilidad del enrutamiento al reducir la cantidad de información que tienen que manejar los protocolos OSPF o IS-IS. Esto se consigue mediante la agregación/abstracción de la información, perdiendo con ello algo de la información, por tanto para limitar la cantidad de pérdidas es necesario restringir el tipo de información que puede ser agregada/abstraída.

Para agrupar enlaces se necesitan las siguientes restricciones. Todos los enlaces componentes en una agrupación deben empezar y terminar en el mismo par de LSRs y compartir algunas características comunes o propiedades definidas en OSPF-TE e ISIS-TE. Dentro de estas características comunes se encuentran:

-Tipo de enlace (punto a punto o multi-acceso).
-Métrica TE (un coste administrativo)
-Conjunto de Clases de Recursos en cada extremo de los enlaces.

Un FA también puede ser un enlace componente. De hecho, una agrupación puede consistir en una mezcla de enlaces punto a punto y FAs, pero todos compartiendo algunas propiedades comunes.

Crear un enlace agrupado consiste en agregar los parámetros TE idénticos de cada enlace componente individual para producir parámetros TE agregados. Algunos parámetros pueden ser sumas de características de los componentes, como el ancho de banda no reservado y el máximo ancho de banda reservable. Un nodo GMPLS con enlaces agrupados debe aplicar el control de admisión en base a cada uno de sus enlaces componentes.

2. ARQUITECTURA Y DISEÑO DE LAS REDES PRIVADAS VIRTUALES ÓPTICAS

En las redes de comunicaciones es necesario que el intercambio de información se haga de manera privada, es decir que el mensaje se envíe solo ha determinados receptores. En especial el sector corporativo requiere la implementación de enlaces privados para transportar de forma segura toda su información confidencial. Actualmente Internet se ha convertido en el principal medio mundial de comunicación por tal razón, las corporaciones requieren que las redes de área local trasciendan más allá de este ámbito para incluir personal y centros de información ubicados en la misma ciudad o en otras ciudades, e incluso otros países. Esto se puede lograr a través de las Redes Privadas Virtuales (*Virtual Private Network*, VPN) las cuales demuestran ser una alternativa para las corporaciones, organizaciones y cuerpos nacionales.

El reciente avance y convergencia del Protocolo de Internet (*Internet Protocol*, IP) y el crecimiento explosivo del tráfico de datos que avanza hacia la estandarización de técnicas en las redes ópticas, combinado con la aceptación de las ofertas de IP y servicios VPN basados en el Multiprotocolo de Conmutación de Etiquetas (*Multiprotocol Label Switching*, MPLS) por parte de los proveedores, motivan la consideración de las OVPNs (*Optical Virtual Private Network*) como una de las mejores aplicaciones a futuro de las redes ópticas.

Actualmente, un acercamiento al despliegue de OVPN es a través del plano de control de GMPLS (*Generalized Multiprotocol Label Switching*) visto en el capítulo anterior, este plano inicia el descubrimiento e inventario de elementos y servicios de red, abastecimiento en tiempo real, conectividad extremo a extremo y comunicación unificada. Con estos mecanismos de control de distribución y suministro de ancho de banda dinámico se observara en este capitulo que es posible introducir el concepto de redes privadas virtuales ópticas OVPN que ahorran más eficientemente las fuentes de fibra, y convierten las redes tradicionales de transporte de datos, hacia el servicio de redes inteligentes.

2.1 DEFINICIÓN DE UNA OVPN

Una OVPN surge del concepto de Red Privada Virtual aplicado sobre una red óptica. Una VPN se define libremente como una red en la cual la conectividad del usuario entre varios sitios se desarrolla sobre una

infraestructura compartida (o infraestructura pública) con el mismo acceso o políticas de seguridad como en una red privada. Las VPNs esencialmente proporcionan una red excesivamente privada de enlaces seguros sobre una red pública.

Tradicionalmente Las VPNs pueden ser implementadas como un protocolo de capa de red (capa-3) o protocolo de capa de enlace de datos (capa-2). Como un protocolo de capa 3 los paquetes son encriptados antes de ser enviados vía túneles IP usando un protocolo como IPSec, lo que es técnicamente costoso ya que cada paquete tiene que ser procesado. Otra alternativa es usar protocolos de capa 2, tales como ATM, Circuitos Virtuales (VCs) que pueden ser instalados punto a punto. Aunque esto es menos tedioso que IPSec, aun tiene sus desventajas como por ejemplo, la creación de VCs es dependiente del medio y se convierte en un problema cuando la infraestructura esta hecha de tecnologías de contextos diferentes. También las conexiones segmento a segmento en acoplamiento con VPN incrementan la complejidad y numero de VCs necesitados.

Hasta ahora las VPN's se han desplegado en redes no ópticas. Tales redes tienen un límite de ancho de banda. Además, la disposición de las VPNs es más lenta y complicada debido a las interfaces electrónicas es por esto que surgen las OVPNs. Un sistema que esta basado en una red óptica inteligente y que usa las recientes tecnologías de conmutación ópticas y las integra con funcionalidades WDM, TDM y cross-conectores ópticos. En conjunto con una sofisticada gestión de red, una red óptica abre un rango de opciones para el diseño, gestión, operación e implementación de las redes. Las OVPNs son mas seguras mas flexibles y menos complejas.

Cuando se establece un canal de transmisión por asignación dinámica para el usuario, la OVPN es físicamente separada de la red principal y por consiguiente está libre de accesos no autorizados. Al mismo tiempo, todas las características ofrecidas por una red óptica inteligente están disponibles para usuarios OVPN. Estas incluyen lo siguiente:

- **Redundancia escalable y sofisticada**: la combinación de cross-conectores y WDM permite no solo conmutación de fibra, si no también conmutación basada en canales. Por ejemplo, si una ruptura de línea ocurre, los datos pueden ser enrutados automática e inmediatamente.

- **Transparencia de protocolo**: el gran número de protocolos disponibles hoy pueden causar problemas para los proveedores de servicio y usuarios. Los sistemas transparentes, sin embargo, adaptan fácilmente a todos los protocolos y pueden enfrentarse con cambios en los requerimientos.

- **Un alto grado de flexibilidad**: las redes ópticas inteligentes trabajan sobre el nivel de transporte y pueden transmitir protocolos con velocidades entre 8 Mbits/seg y 2.7 Gbits/seg. Al mismo tiempo, la QoS puede ser garantizada.

- **Soporte para cualquier infraestructura**: Los sistemas ópticos inteligentes soportan topologías punto a punto, punto a multipunto, anillo y malla. Esto significa que es posible agregar sitios y nodos sin costo adicional.

- **La extensión simple de infraestructuras existentes**: las redes ópticas inteligentes pueden ser integradas dentro de alguna estructura de red existente. Esto simplifica los procesos de instalación de OVPNs y reduce los costos.

- **Gestión de red inteligente**: además de la gestión de elemento y gestión de red, cada aplicación individual o longitud de onda que es transmitida dentro de la red puede ser monitoreada y controlada automáticamente.

- **Servicios Dinámicos**: las redes ópticas inteligentes habilitan a los proveedores de servicio para ofrecer servicios automatizados, tales como OVPNs dependientes del tiempo. En este escenario, una VPN podría ejecutar operaciones estándar durante el día, liberando la capacidad en la noche para backups y otras tareas. Alternativamente, dos clientes pueden compartir al tiempo los recursos.

Según los estándares tratados por la IETF. La OVPN es definida como una colección de puertos que conectan los Elementos Ópticos finales de Usuario (CEs) usados por el mismo cliente en la red del proveedor de servicio. Esto permite a los usuarios tener por completo el control de una parte definida de los recursos de red del portador de red. Este servicio protege los recursos de operación del portador permitiendo a los usuarios finales ejecutar muchos circuitos de provisionamiento e iniciar procedimientos.

Los dispositivos finales en una OVPN crean y borran conexiones entre ellos directamente por el software de aplicación de la capa superior. Si se considera la seguridad del servicio, la señalización entre el dispositivo final del cliente y el dispositivo final del proveedor da la aceptación para estar sobre la red privada y se evita la suplantación por entidades externas a esta.

Las infraestructuras de las OVPN son construidas sobre la capa óptica. Así los servicios OVPN proporcionan conexiones ópticas o TDM entre los dispositivos de usuario pertenecientes a la VPN. Una OVPN habilita a los usuarios a tomar ventaja de una red óptica completamente reconfigurable o flexible. También proporciona la habilidad para dividir lógicamente una

red de capa física del proveedor en subredes lógicas, cada una con derechos de acceso de usuario y recursos asignados. Los proveedores que adoptan una OVPN pueden obtener ventajas en cuanto al uso de los recursos ya desarrollados dentro de las redes existentes. (Esto se explica mas adelante, en la sección 2.5.2)

2.2 REQUERIMIENTOS FUNCIONALES DE UNA RED PRIVADA VIRTUAL ÓPTICA

Una buena solución OVPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

a) Seguridad: dentro de este punto se destacan el control de acceso para garantizar la seguridad de las conexiones de la red, el cifrado para proteger la privacidad de los datos y la autenticación para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

b) Control de tráfico: es necesario para que garantice solidez, calidad de servicio y un desempeño veloz. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo, aquí es donde entran a jugar parámetros como la prioridad de los datos y la garantía de ancho de banda.

c) Manejo empresarial: este se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final y la escalabilidad de la tecnología. Por lo tanto, un servicio OVPN debe proporcionar por lo menos lo siguiente:

- **Autentificación del usuario:** el servicio OVPN debe verificar la identidad de sus clientes y restringir el acceso a los usuarios autorizados solamente. Debe también proporcionar auditoria y registros de estadísticas para demostrar quien tuvo acceso a qué información y cuando.

- **Administrador de direcciones:** la solución debe asignar una dirección de cliente OVPN sobre la intranet y debe asegurarse que las direcciones privadas conserven esa intimidad.

- **Cifrado de datos:** los datos que viajan sobre la red pública deben ser ilegibles para los clientes no autorizados por la red.

- **Gestión de llave:** el servicio de OVPN debe generar y restaurar las llaves de cifrado para el cliente y el servidor.

2.3 CONSIDERACIONES DE UNA VPN EN EL AMBIENTE ÓPTICO

En el ambiente óptico, los elementos que constituyen una OVPN son combinación de los recursos de plano de transporte y los recursos de plano de control. El plano de transporte de la OVPN opera como capa óptica incluyendo la fibra física, longitudes de onda o canales TDM. El plano de control de OVPN proporciona algún nivel de control y capacidad de gestión para el usuario.

Los recursos del plano de control son facilidades de control de conexión incluyendo señalización, enrutamiento, software de gestión de recursos. Estos recursos son usados para realizar algoritmos específicos y políticas involucradas en el control de conexión de los recursos del plano de transporte.

Las funciones realizadas por esos recursos del plano de control pueden ser agrupadas en tres extensas categorías [5]:

- Funciones de soporte común, como el canal de comunicaciones físico para señalización.
- Funciones que no requieren conocimiento explicito de los recursos, tales como número de miembros de la OVPN, políticas OVPN, transferencia transparente de información de control de usuario, etc.
- Funciones que requieren conocimiento explicito de los recursos de capa óptica, tales como gestión de recursos de enlace, topología de enrutamiento, etc.

2.4 MODELO DE REFERENCIA DE UNA OVPN

EL modelo de referencia OVPN genérico [6] es mostrado en la figura 6:

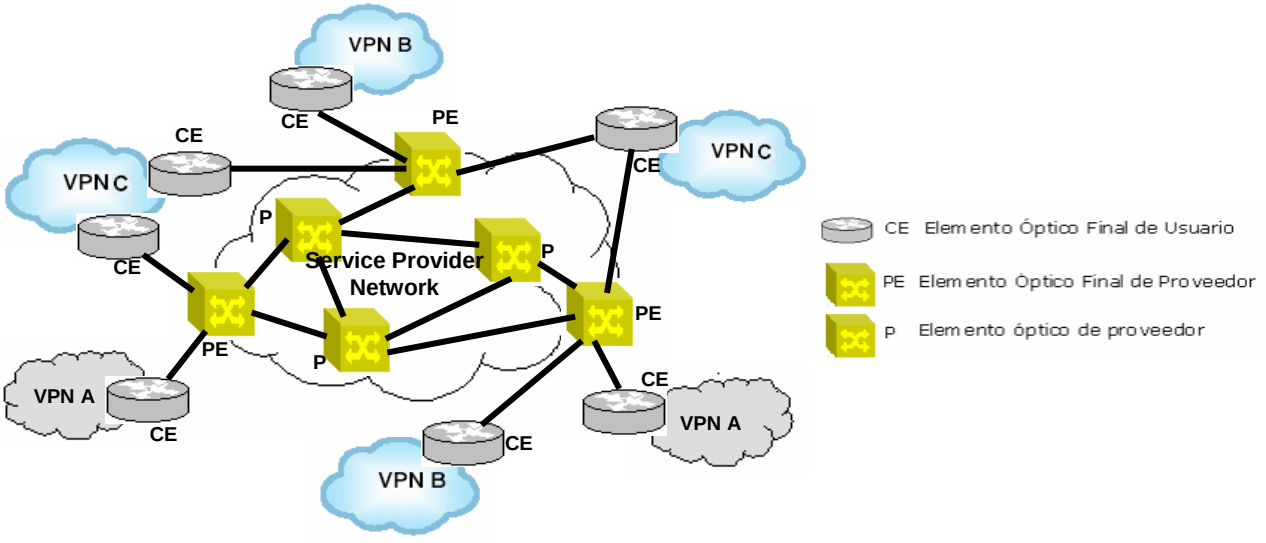


Figura 6. Modelo de referencia OVPN

Una red de proveedor de servicio formada por elementos de red óptica (ONES) tales como Cross Conectores Ópticos-OXCs o cross conectores SONET/SDH, se dividen en P ONES o elementos de redes ópticas de proveedor y en elementos de redes ópticas finales de proveedor o PE ONES.

-Los PE ONES son dispositivos dentro de la red de proveedor que ofrecen el servicio OVPN al usuario.

-Los P ONES son los enrutadores o dispositivos de conmutación dentro de la infraestructura base que interconecta PEs teniendo muy poco conocimiento acerca de la existencia de las OVPNs.

-El CE (elemento óptico final de usuario) proporciona la interfaz al dominio del usuario. Cada CE puede ser el dispositivo de entrada y salida para el usuario OVPN de punto final dentro del domino de usuario. Un ejemplo de un CE podría ser un router o un cross-conector SONET/SDH o un switch Ethernet.

La conectividad entre CEs y PEs puede ser proporcionada de diferentes formas. Por ejemplo dado un CE puede ser conectado a uno o más PEs, y dado un PE puede ser conectado a uno o más CEs que pueden o no pertenecer a la misma OVPN.

El modelo de referencia OVPN proporciona las siguientes características:

- Contrato de usuarios para sistemas de recursos de red específicos tales como puertos de conexión ópticos, longitudes de onda, etc.

- El Concepto de Grupo de usuarios Cerrados (CGU) en una OVPN es soportado de la misma forma que en una VPN.

- La conexión óptica puede ser de tipo PC (conexión permanente), SPC (Conexión lógica permanente suave) o SC (conexión conmutada) dependiendo del método de provisionamiento usado.

- Un sistema OVPN puede pedir reconfiguración dinámica de las conexiones entre sitios dentro del mismo CGU.

- Un usuario puede tener visibilidad y control de recursos de red de acuerdo al contrato de servicios de usuario.

2.4.1 Comunicación entre dos sitios de una OVPN

En el modelo de referencia OVPN, el PE contiene información del dispositivo de cliente, mientras que el P no necesariamente contiene esta información además el PE puede comunicarse con PEs remotos, por eso

un PE puede obtener toda la información de dispositivo de cliente para cada OVPN. El CE contiene la información de dominio de cliente. El PE puede comunicarse con el CE unido a ese PE, para obtener información del dispositivo de cliente de ese CE, y proporcionar información del dispositivo de cliente de la OVPN al cual ese CE corresponde.

Cada puerto sobre un CE que conecta a un PE tiene un identificador que es llamado Identificador de Puerto de Cliente (CPI) y dentro de la red de proveedor de servicio, cada puerto sobre un PE que conecta a un CE tiene un identificador que es llamado Identificador de puerto de proveedor (PPI). Además, cada PE mantiene una Tabla de Información de Puertos (PIT) la cual contiene una lista de pares <CPI,PPI> para cada OVPN, esta tabla representa información del dispositivo de cliente. Una vez un nuevo puerto OVPN es unido a un CE, la información CPI de ese puerto se pasa al PE a través del protocolo BGP (Borde Gateway Protocol) con extensiones multi-protocolo [7], como se explicara mas adelante. Así, un elemento es creado para cada puerto, y La PIT para esta OVPN es actualizada. (Ver figura 7).

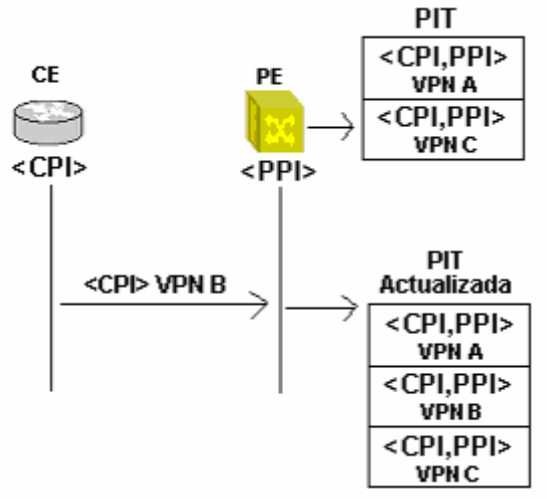


Figura 7. Actualización de la PIT

La asociación de un puerto sobre un CE con una OVPN es hecha por el proveedor de servicio OVPN, como parte del provisionamiento del puerto sobre el PE (asociando el puerto de un PE con la PIT de una OVPN particular, y conectando el puerto de un CE con el puerto de un PE). Luego las PITs son transmitidas a los PEs remotos de la misma OVPN usando BGP. Para restringir el flujo de esta información solamente a las PITs dentro de una OVPN dada, se utiliza la filtración de ruta BGP basada en la "Route Target Extended Community" [8] como se explica a continuación:

Cada PIT en un PE se configura con una o más "Route Target Extended Community", llamadas "export route targets", que se utilizan para etiquetar la información local cuando se exporta en el BGP del proveedor, e "import route Targets", que restringen el conjunto de las rutas que se podrían importar desde el BGP del proveedor dentro de la PIT a únicamente las rutas que tienen por lo menos estas comunidades.

Cuando un proveedor de servicio adiciona un puerto nuevo de OVPN a un PE particular, este puerto es asociado en el tiempo del provisionamiento con una PIT en ese PE, y esta PIT está asociada (otra vez en el tiempo de provisionamiento) con esa OVPN.

Como ya se mencionó, una vez un puerto es configurado en el PE, el CE que esta unido vía este puerto al PE puede pasarle la información del CPI de ese puerto por medio de BGP. Esta información, combinada con la información de PPI disponible para el PE, permite al PE crear la pareja < CPI, PPI > para tal puerto, y después utilizar esta pareja para llenar la PIT de la OVPN asociada a ese puerto.

La distribución de información del dispositivo de cliente se muestra en la figura 8.

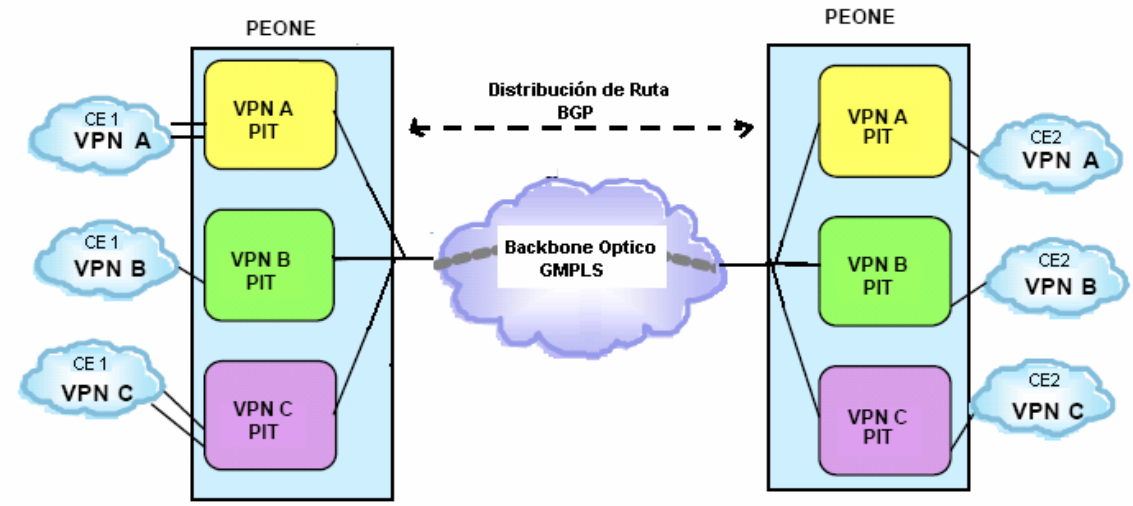


Figura 8. Componentes OVPN

2.4.2 Señalización

Una vez que un CE obtiene la información sobre los CPIs de otros puertos dentro de la misma OVPN ("puertos objetivos"), el CE utiliza la señalización GMPLS para solicitar a la red del proveedor establecer una conexión óptica a un puerto objetivo.

La solicitud originada por el CE contiene el CPI del puerto en el CE que desea utilizar para la conexión óptica, y el CPI del puerto objetivo. Cuando el PE unido al CE que originó la petición recibe esta petición, el PE identifica la PIT apropiada, y después utiliza la información en esa PIT para encontrar el PPI asociado al CPI del puerto objetivo. El PPI debe ser suficiente para que el PE pueda establecer una conexión óptica. La petición alcanza en última instancia el CE asociado al CPI objetivo (la petición todavía lleva el CPI del CE que la originó). Si el CE asociado con el CPI objetivo acepta la solicitud, la conexión óptica es establecida.

La señalización entre un CE y un PE suponiendo el uso del protocolo de señalización RSVP-TE (Ver Anexo 1) se realiza de la siguiente forma:

Si hay un canal de control IP entre el CE y el PE, este puede ser un salto IP, una red privada IP, o aun una VPN IP. Así las direcciones CEs de este canal son nombradas como direcciones de canal de control CE (CE-CC-Addr) y las direcciones PEs de este canal como direcciones de canal de control PE (PE-CC-Addr).

Cuando un CE envía un mensaje Path RSVP al PE, la dirección IP origen en el paquete IP que transporta el mensaje se fija al CE-CC-Addr apropiado, y la dirección IP destino en el paquete se fija al PE-CC-Adrr apropiado. Cuando el PE envía de vuelta al CE el mensaje Resv correspondiente, la dirección IP fuente en el paquete IP que transporta el mensaje se fija al PE-CC-Addr, y la dirección IP destino se fija al CE-CC-Addr. (Ver Figura 9.A)

Así mismo cuando un PE envía un mensaje *Path* RSVP al CE, la dirección IP fuente en el paquete IP que transporta el mensaje se fija al PE-CC-Addr apropiado, y la dirección IP destino en el paquete se fija al CE-CC-Addr apropiado. Cuando el CE envía de vuelta al PE el mensaje *Resv* correspondiente, la dirección IP fuente en el paquete IP que transporta el mensaje se fija al CE-CC-Addr, y la dirección IP destino se fija al PE-CC-Addr. (Ver Figura 9.B)

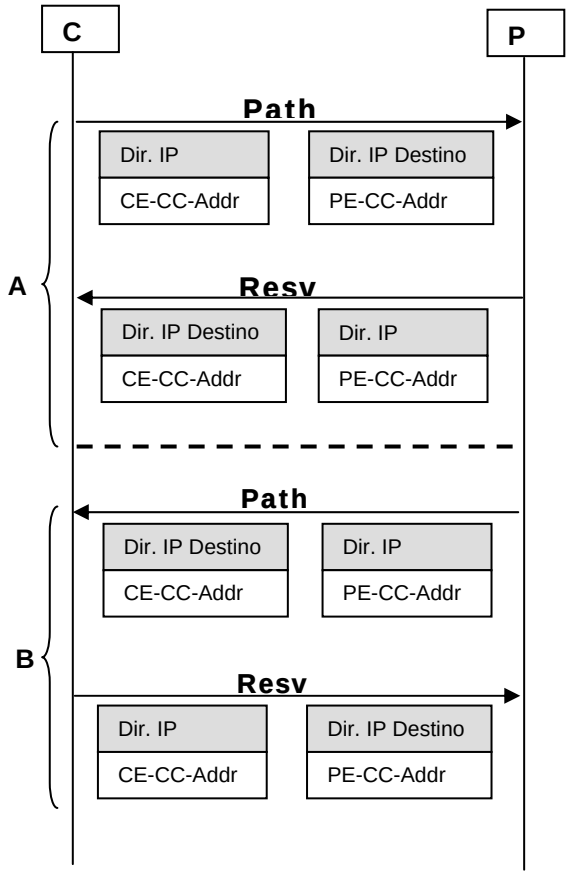


Figura 9. Mensajes Path y Resv entre el CE y PE

Además de ser usado para direcciones IP en el paquete IP que transporta mensajes RSVP entre CE y PE, el CE-CC-Addr y el PE-CC-Addr son también usados en el campo de direcciones de salto Next/Previous del objeto IF_ID RSVP_HOP que es transportado entre CEs y PEs.

En el caso donde un enlace entre CE y PE es un enlace no agrupado numerado, el CPI y el VPN-PPI del enlace son usados para el tipo TLVs 1 o 2 del objeto IF_ID RSVP HOP que es transportado entre el CE y el PE. En el caso donde un enlace entre CE y PE es no agrupado no numerado, el CPI y el VPN-PPI de ese enlace son usados para el campo de direcciones IP del tipo TLV 3. En el caso donde un enlace entre CE y PE es enlace atado, el CPI y el VPN-PPI de ese enlace son usados para el campo de direcciones IP del tipo TLVs 3.

Cuando un CE origina un mensaje *Path* para establecer un LSP desde un puerto particular sobre ese CE a un puerto objetivo particular el CE usa el CPI de su puerto en el O*bjeto Plantilla del Emisor*. Si el CPI del puerto objetivo es una dirección IP, entonces el CE usa este en el objeto Sesión. Y si el CPI del puerto objetivo es una pareja <índice de puerto, dirección IP>, entonces el CE usa la parte de la dirección IP de la pareja en el

Objeto Sesión, y la pareja completa como el subobjeto ID de la interfaz no numerada en el *Objeto de la Ruta Explícita (ERO)*. (Ver Figura 10.A)

Cuando el mensaje *Path* llega al PE de ingreso, el PE selecciona la PIT asociada con la GVPN, y luego usa esta PIT para transformar CPIs transportados en el *Objeto Plantilla del remitente y Sesión* a los PPIs apropiados. Una vez el cambio esta hecho, el PE de ingreso reemplaza los CPIs con estos PPIs. Como resultado, los *objetos Plantilla del Remitente y Sesión* que son transportados en la señalización GMPLS dentro de la red de proveedor de servicio transportan PPIs y no CPIs . (Ver Figura 10.B)

En el PE de salida, el PE realiza el mapeo contrario a los PPIs transportados en el *objeto Plantilla del Remitente y Sesión* dentro de los CPIs apropiados y luego envía el mensaje *Path* al CE que tiene el puerto objetivo. (Ver Figura 10.C)

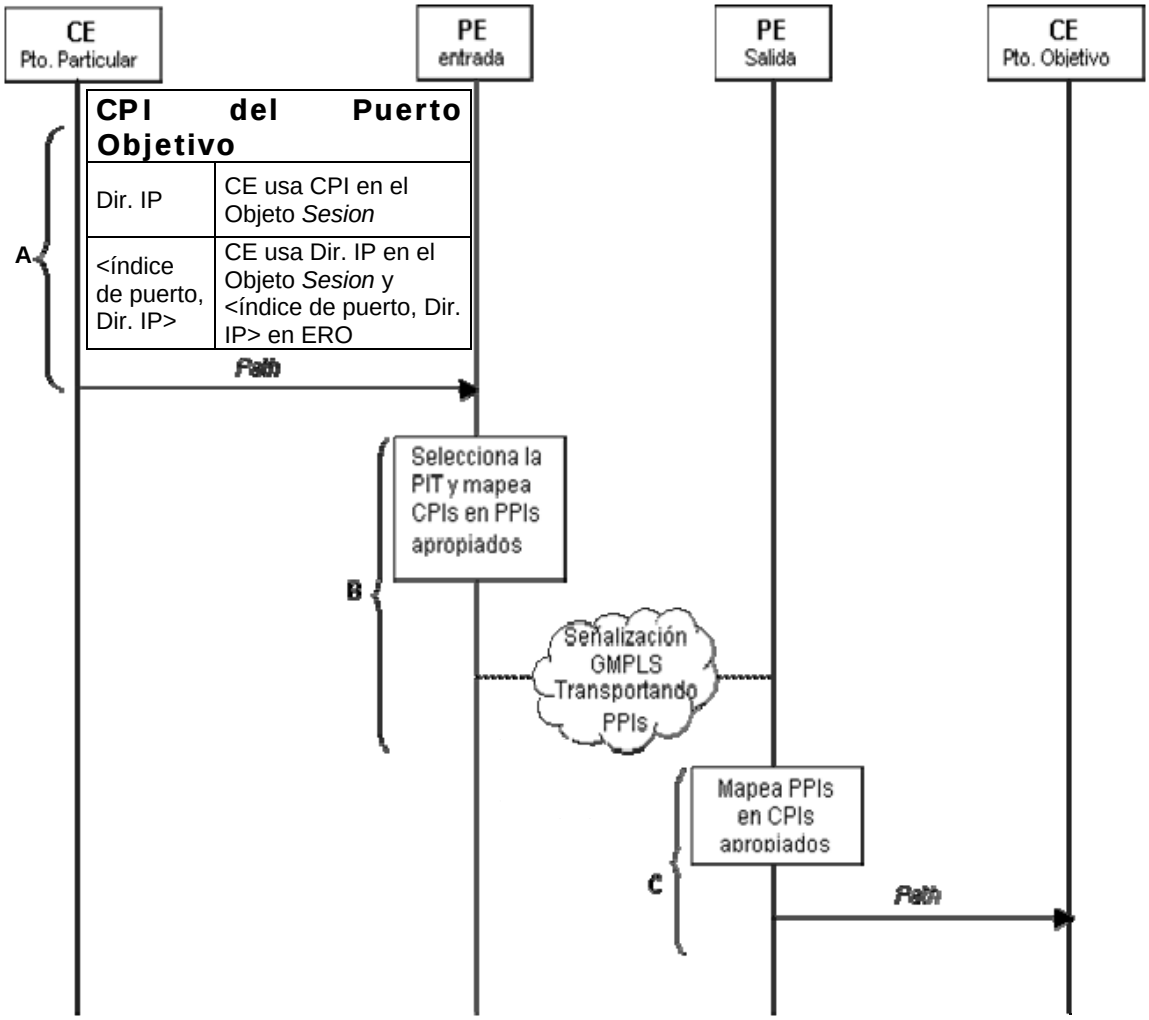


Figura 10. Identificación y mapeo del CPI

Un puerto, además de su CPI y PPI puede también tener otra información asociada a él que describe las características de los canales dentro de ese puerto, tales como: codificación soportada por los canales, ancho de banda de un canal, ancho de banda total sin reservar del puerto, etc., además información sobre ciertas capacidades de la red del proveedor de servicio. Toda esta información es utilizada para asegurarse de que los puertos en cada extremo de una conexión óptica tienen características compatibles, y de que hay suficientes recursos no asignados para establecer una conexión óptica. La distribución de esta información (incluyendo los mecanismos utilizados) es idéntica a la distribución de la información < CPI,PPI>. La Distribución de cambios a esta información debido a establecimiento/terminación de conexiones ópticas es idéntica a la distribución de la información < CPI, PPI >, a menos que los umbrales se deban utilizar para contener el volumen de control de tráfico causado por tal distribución.

Puede ocurrir que para un par de puertos dados dentro de una OVPN, cada uno de los CEs conectado a estos puertos intentaría establecer concurrentemente una conexión óptica al otro CE. Si tener un par de conexiones ópticas entre un par de puertos se ve como indeseable, una manera de resolver esto es tener un CE con el valor más bajo del CPI que se requiere para terminar la conexión óptica originada por el CE. Esta opción se podía controlar por la configuración en los dispositivos del CE.

2.5 VENTAJAS DE LAS OVPN

2.5.1 Ventajas para el cliente

Desde las perspectivas de los clientes hay dos ventajas principales de una OVPN, estas ventajas se aplican sobre y por encima de las ventajas de acceso para una red provista dinámicamente.

- El cliente puede realizar desde afuera la gestión directa de una red óptica permitiendo el control de la gestión de una OVPN a terceros. Esto libera al cliente de la necesidad de configurar y manejar la información de conectividad para los CEs que participan en la OVPN.

- El cliente puede hacer uso de forma reducida de una red óptica. Así, por ejemplo comparte el acceso a la red óptica con muchos otros usuarios; los sitios que corresponden a los clientes se pueden conectar juntos a través de la red óptica sin cargar con el costo completo de desplegar y de manejar la red.

En cierto grado, el cliente puede también gozar de las ventajas del proveedor, es decir, si el proveedor puede sacar más ganancia de las OVPN's y proporcionar mejor diferenciación de servicios, el cliente se beneficiará de servicios de costo más bajo que se adapten mejor a sus necesidades.

2.5.2 Ventajas para el proveedor

Desde la perspectiva de los beneficios del cliente las ventajas del proveedor son por ejemplo que este puede construir servicios dinámicos bajo demanda ofreciendo nuevos servicios de OVPN y enviar datos acerca de los requerimientos de la configuración de los clientes de CE- a -CE.

Una estructura más flexible de OVPN aplicada a la red óptica permite que el proveedor haga un uso más amplio de los recursos de reserva dentro de la red (previamente no usados), puesto que el PE puede ser el responsable de enrutar la conexión a través de la red óptica y esta a su vez puede reclamar control de cómo se utilizan los recursos y ajustar las trayectorias para hacer uso óptimo de todos los recursos disponibles.

Además, Las OVPNs también permiten a proveedores con cobertura de red complementaria ampliar el rango efectivo de sus redes arrendando capacidad excedente a otros.

Un ejemplo es el de un proveedor otorgando servicios de datos a empresas locales. Si este proveedor de servicio requiere ancho de banda adicional para reunir los requerimientos de capacidad de sus usuarios, puede llegar a un proveedor con exceso de capacidad de transmisión para suplir cualquier déficit de ancho de banda. El proveedor de proveedores establece una OVPN para el proveedor subdividiendo su red de capa física en un número de subredes virtuales con apropiado acceso asignado y recursos. Estas subredes aparecen en el sistema administrativo del proveedor como extensiones lógicas de su propia red, mientras el resto de la red del proveedor y la información de alto orden permanece oculta.

En cuanto los dos proveedores han enlazado sus redes con, las operaciones y funciones desplegadas entre los dos son implementadas de una manera segura, definida y autorizada.

El escenario tiene varias implicaciones positivas para el proveedor de servicio, no solamente beneficios de los recursos extra de la red si no también puede ofrecer a sus clientes todos los servicios dinámicos asociados con una red óptica.

2.6 TÉCNICA DE OVPN DINÁMICA

La OVPN puede hacer frente a algunos cambios tales como provisionamiento simplificado, conectividad obligada/restringida, petición de ancho de banda sobre demanda entre un par de puertos dentro de la OVPN y privacidad/ independencia con respecto a direccionamiento y enrutamiento. Para asignar recursos de red óptica más flexible y eficientemente, existe la técnica de OVPN dinámica la cual está aun en investigación. Esta puede ofrecer provisión dinámica de canales ópticos y distribución de recursos en tiempo real. Para esto se extienden las OVPNs con dos nuevas funciones: gestión de conexión dinámica y rápida protección/restauración.

2.6.1 Gestión de conexión dinámica

Con está función, la OVPN puede ser establecida, modificada o eliminada dinámicamente de acuerdo al servicio de tiempo real. Los enlaces relacionados son propuestos para acondicionar diferentes servicios. Para soportar el tráfico en tiempo real, los enlaces en tiempo real son usados para voz y video. Con los enlaces diferenciados las redes pueden soportar más clases de servicios en la capa de enlace a diferencia de los servicios que se soportan solamente en la capa IP. Esto es muy atractivo para las redes de acceso y redes metropolitanas donde cada vez se hace necesario soportar más servicios.

Entre dos nodos adyacentes en una OVPN se usa un Grupo de Enlace Privado Virtual (VPLG)[1], el cual puede proporcionar grupos de enlaces para diferentes OVPNs. Además una OVPN no puede usar enlaces externos excepto sus propios VPLGs, los grupos de enlaces pueden ser cambiados dinámicamente de acuerdo a las políticas.

Como ilustra la figura 11, para soportar diferentes OVPNs los enlaces son divididos en varios VPLGs tales como VPLG 1 y VPLG 2. Los enlaces en VGPL 1 son usados únicamente por la OVPN 1, y no pueden ser usados por otras OVPNs. Si son necesarios más enlaces, la OVPN 1 puede solicitar más enlaces adicionales al VPLG 1; y si los enlaces son más de los que se necesitan, entonces los enlaces libres pueden ser borrados desde el VPLG 1. Con esta flexibilidad los enlaces pueden ser usados eficientemente.

[1] VPLG es definido en "Link management extensión in generalized MPLS", proceedings of SPIE, pp.139-146, 2002, y no es un método estandarizado al igual que la técnica de OVPN dinámica.

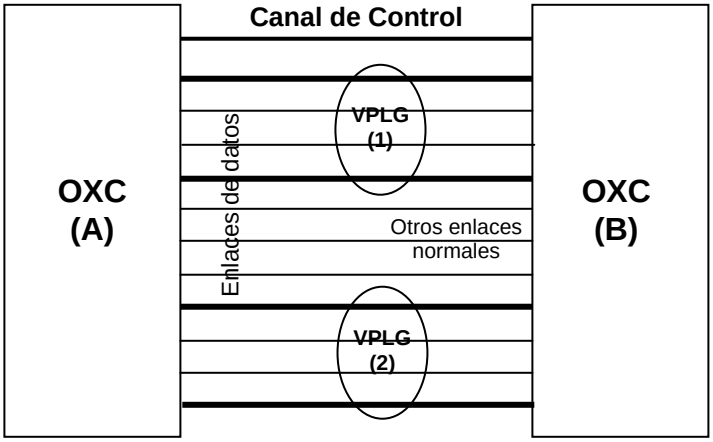


Figura 11. Enlaces entre OXCs Con funciones OVPN

En la figura 11 son usadas dos tipos de líneas para diferenciar las dos clases de enlaces de datos. Las líneas gruesas son para los enlaces de datos de alto nivel (enlaces en tiempo real), los cuales tienen la mas alta prioridad. Esto significa que los enlaces deben ser protegidos de ante mano y cuando alguna falla ocurra deben ser los primeros que se restauren. Las líneas delgadas son los enlaces normales. Cada OVPN puede contener gran cantidad de enlaces de estos dos tipos. Cuando los enlaces son requeridos por la Interfaz de usuario o la Interfaz de proveedor, los parámetros de propiedad de los enlaces deberían ser negociados.

El parámetro de propiedad de enlace puede indicar si la petición es una petición OVPN o no, cuantos enlaces en tiempo real necesita el tráfico, y cuantos enlaces normales. Si el recurso libre de la red óptica puede satisfacer la petición, el plano de control deberá aceptar la petición y establecer las conexiones. Cuando el tráfico ha finalizando los enlaces utilizados (incluyendo los enlaces usados por las OVPN) deben ser liberados.

Para el VPLG 1 en la figura 11, dos enlaces de tiempo real y dos enlaces normales están en uso. Los otros enlaces normales son usados por aplicaciones no OVPN o para protección de la OVPN si es necesario.

2.6.2 Rápida protección y restauración

Esta función puede proporcionar dos tipos de esquemas de protección y restauración: dentro de los VPLGs y fuera de los VPLGs. El primero es para reservar una ruta de protección o calcular una ruta de restauración dentro de los VPLGs, la política y el procedimiento son decididos por el cliente de la OVPN. Una vez ocurre falla en un enlace, la ruta afectada será automáticamente restaurada dentro de todos los VPLGs que pertenecen a la OVPN. Este avance será operado de acuerdo a la

distribución de tráfico de la OVPN. El recurso de red óptica fuera de los VPLGs funciona de la misma manera.

Cuando el recurso en los VPLGs no es muy adecuado para mantener una ruta de protección/restauración, se implementa el recurso fuera de los VPLGs para proteger y restaurar el enlace fallido. En este caso el proveedor asegura: QoS para el cliente de la OVPN, rutas equilibradas y asigna ancho de banda para maximizar la utilización completa de la red. Usualmente varias OVPNs serán afectadas por fallas de enlace, esto será favorable para la restauración del tráfico afectado en toda la red simultáneamente.

Estos esquemas harán la asignación de recurso de red óptico más eficientemente, la restauración finalizada más rápidamente, y la base de datos de estado de enlace (LSBD) actualizada más excepcionalmente. La ruta de protección reservada puede ser modificada o eliminada dinámicamente si la petición del servicio cambia.

2.6.3 OVPN dinámica en una red de cinco nodos

A modo de ejemplo se aplica la técnica de OVPN dinámica para cinco nodos que usan GMPLS como mecanismo de señalización.

La figura 12 muestra el proceso de establecimiento dinámico de conexiones OVPN, la primera función de gestión dinámica de la conexión. Se asume una OVPN A cruzando la red del proveedor entre el cliente A1 y el cliente A2. Primero uno de los CEs en la OVPN envía un requerimiento por la ruta de operación al PE que esta conectado. Luego el protocolo OSPF calcula la ruta óptima, y la red del proveedor establece LSPs de acuerdo a los requerimientos del cliente, tales como ancho de banda, y requerimientos QoS. Finalmente el LMP actualiza las LSDB para asegurar que el recurso de enlace designado para la OVPN A es exclusivo. Al mismo tiempo, los VPLGs son asignados a la OVPN de acuerdo a la demanda del cliente.

Como se ilustra en la figura 12, la OVPN A realmente establece dos caminos unidireccionales, uno desde el cliente A1 al A2 a través del OADM (Optical Add-drop Multiplexer), el OXC3 y el OXC2, y el otro desde el cliente A2 al A1 a través del OXC2, OXC4, OXC1 y el OADM. De la misma manera la OVPN B construye realmente una ruta bidireccional entre el cliente B1 y B2 a través OXC1, OXC4, OXC2. Las rutas OVPN pueden ser cambiadas dinámicamente de acuerdo al servicio de tiempo real.

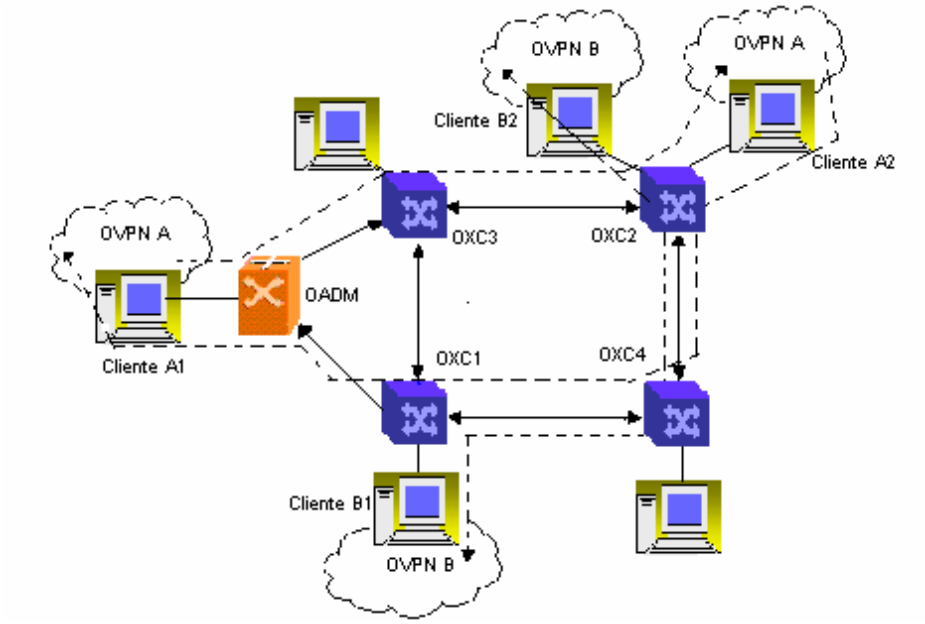


Figura 12. Gestión de la Conexión OVPN dinámica

La restauración rápida es ilustrada en la figura 12. Cuando los enlaces físicos entre OXC2 y OXC3 son interrumpidos, el mecanismo de restauración rápida, basado en el algoritmo genético, puede calcular una ruta de restauración que va desde el cliente A1 al A2 a través del OADM, OXC3, OXC1,OXC4 y el OXC2 y reemplazar el camino que falló tan pronto como sea posible. Como ya se mencionó dos tipos de esquemas de protección y restauración están disponibles: dentro de los VPLGs y fuera de los VPLGs, las cuales son elegidos de acuerdo al estado de la red o la demanda de clientes. En la figura 13, el segundo esquema (fuera de las VPLGs) es adoptado.

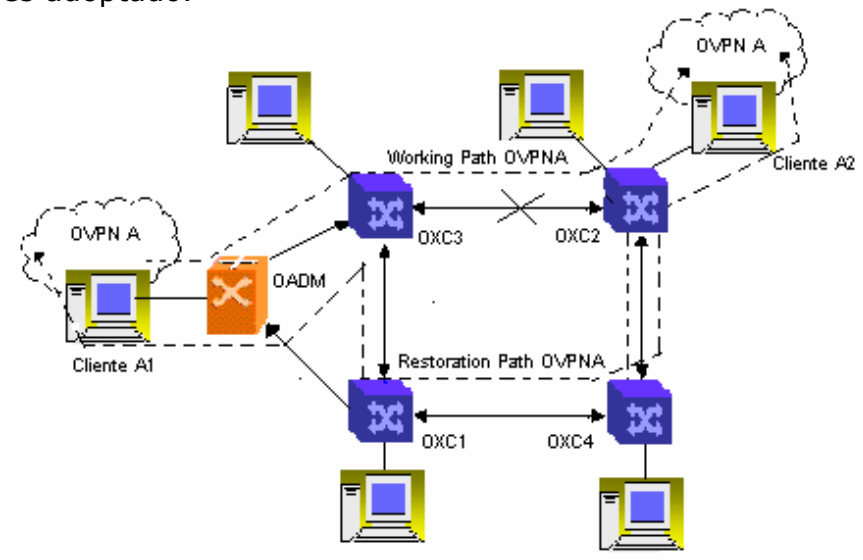


Figura13. Mecanismo de Restauración OVPN dinámica

3. CALIDAD DE SERVICIO BAJO DIFFSERV PARA OVPNs QUE SOPORTAN GMPLS.

En ciertos tipos de datos que circulan actualmente por las redes, por ejemplo tráficos con requerimientos de tiempo real (voz o video), es deseable que no ocurra pérdida de información, que exista un gran ancho de banda disponible, y que los retrasos en los envíos de estos paquetes de datos sean mínimos. Es por ello que surge la necesidad de aplicar Calidad de Servicio (QoS) y métodos de diferenciación de tráfico particulares con el fin de otorgar preferencia a estos datos sensibles.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas, por lo tanto implementar QoS, hace el rendimiento de la red más predecible y la utilización de ancho de banda más eficiente.

La falta de suficiente QoS y provisión de adecuada capacidad de transmisión para servicios de gran ancho de banda son desventajas que presentan actualmente las VPNs. Para resolver estos problemas, han sido sugeridas las OVPNs sobre IP/GMPLS sobre DWDM como una solución donde la tecnología de red óptica DWDM es usada como el backbone de la red y GMPLS como protocolo de control para transferencia de datos sobre IP.

Así, una OVPN sobre IP/GMPLS sobre DWDM es considerada como la tendencia para VPNs de nueva generación soportando varios servicios multimedia en tiempo real. Dentro de esta arquitectura, proporcionar servicios garantizando QoS a través de diferenciación de servicio (Diffserv) y la recuperación de calidad de servicio son los puntos claves.

En este capitulo inicialmente se describe de manera general el modelo DiffServ, luego se presenta la arquitectura y procedimiento funcional de una OVPN sobre IP/GMPLS sobre DWDM ofreciendo Calidad de Servicio Óptica Diferenciada (DOQoS) y el establecimiento de un LSP Optico basado en clases DOQoS y finalmente se muestra un esquema de mantenimiento de QoS basado en análisis y recuperación de fallas.

3.1 DEFINICIÓN DE CALIDAD DE SERVICIO (QoS)

La "Calidad de Servicio" es la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también, como el cumplimiento de un conjunto de requisitos estipulados en un Acuerdo de Nivel de Servicios (*Service Level Agreement*, SLA) entre un Proveedor de servicio de Internet (*Internet Service Provider*, ISP) y sus clientes.

QoS (Quality of Service) consiste también en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio: se debe tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (Frame Relay, X.25, SDH, ATM, etc) de manera que la gestión de calidad de servicio implica la interacción con estas tecnologías y con los equipos de conmutación, que son los que finalmente determinarán el nivel de calidad de servicio alcanzado.

Algunas redes operan de acuerdo al modelo de entrega del mejor esfuerzo (Best Effort), donde todo el tráfico tiene igual prioridad de ser entregado a tiempo. Cuando ocurre la congestión, todo este tráfico tiene la misma probabilidad de ser descartado.

Además del modelo anterior existen otros dos tipos de calidad de servicio:

Modelo Intserv: se fundamenta en la reserva y asignación de recursos basándose en flujos de tráfico y utiliza algún protocolo de reservación de recursos a lo largo de los enrutadores implicados en la comunicación, como por ejemplo RSVP. El principal problema de este modelo es la necesidad de mantener información sobre cada flujo en todos los enrutadores de la red, lo cual lleva a problemas de escalabilidad.

Modelo Diffserv: se caracteriza por la priorización de determinado tipo de tráfico y la agrupación de los flujos de datos individuales en grandes agregados de tráfico de acuerdo a la "clase de servicio" a la que pertenezcan, dependiendo de esta clase de servicio recibirán un trato distinto en los diferentes elementos de la red. Además este modelo utiliza diferente información de la cabecera de los paquetes para distinguirlos y clasificarlos y conocer el tratamiento que debe recibir el tráfico en los nodos de la red Diffserv.

3.2 CALIDAD DE SERVICIO BAJO EL ESTANDAR DIFFSERV

Los servicios diferenciados (Diffserv) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio.

Este modelo sobresale respecto al modelo Intserv porque en este último la información de estado para cada reservación necesita ser mantenida por cada enrutador a lo largo del trayecto y la escalabilidad para cientos de miles de flujos (propio de una red óptica) se convierte en un problema, mientras que con Diffserv se obtienen varias ventajas, entre ellas que los enrutadores operen más rápido, ya que se limita la complejidad de la clasificación y el encolado, además de minimizar el tráfico de señalización y almacenamiento.

En Diffserv los paquetes que pertenecen a una determinada clase se marcan con un código específico: el DSCP (*DiffServ Code Point*,). Este código es todo lo que se necesita para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, lo que se conoce como Comportamiento por Salto (*Per Hop Behavior*, PHB).

A través de Diffserv se plantea asignar prioridades a los diferentes paquetes que son enviados por la red. Los nodos intermedios (enrutadores) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que Diffserv como se mencionó anteriormente ofrece mejores características de escalabilidad que Intserv.

Dentro del grupo de trabajo de Diffserv de la IETF se define el campo servicios diferenciados (*Differentiated Services*, DS) donde se especifican las prioridades de los paquetes y en el subcampo Punto de Código de servicios diferenciados (*Differentiated Service Code Point*, DSCP) donde se especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como para IPv6.

Una vez que existe la capacidad de marcar los paquetes utilizando DSCP, es necesario proporcionar el tratamiento apropiado a cada una de las clases de tráfico. La colección de paquetes con el mismo valor DSCP circulando hacia una dirección determinada, es llamada Agregado de Tráfico (Behavior Agrégate, BA). Es así como múltiples aplicaciones/fuentes, pueden pertenecer al mismo BA. El PHB se refiere a la programación, encolamiento, limitación y modelación del comportamiento de un nodo, basado en el BA perteneciente al paquete.

3.2.1 Arquitectura de Diffserv

En la arquitectura definida por Diffserv aparece nodos de frontera DS de egreso e ingreso, así como nodos DS internos (Ver figura 14). Este conjunto de nodos definen el dominio Diffserv el cual presenta un tipo de políticas y grupos de PHB que determinarán el tratamiento de los paquetes en la red.

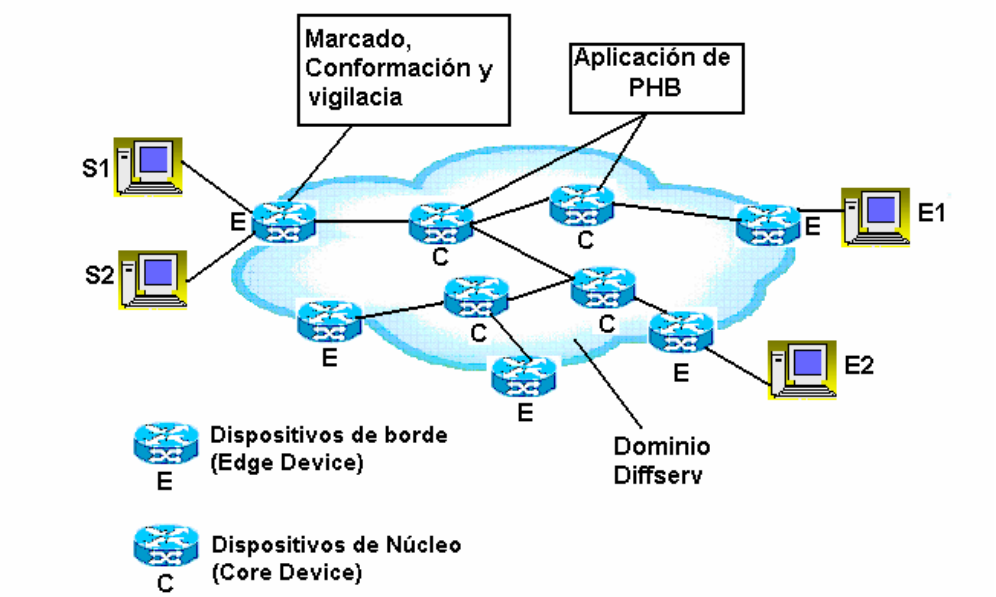


Figura 14. Arquitectura Diffserv

Se debe tener en cuenta que un dominio Diffserv puede estar formado por más de una red, de manera que el administrador será responsable de repartir adecuadamente los recursos conforme al acuerdo de nivel de servicio (*Service Level Agreement*, SLA) entre el cliente y el proveedor del servicio.

A continuación se describen las diferentes funciones que deben realizar los nodos DS:

-**Nodos de frontera DS**: son los dispositivos de borde (Edge Device) necesarios para realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera deben clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de la dirección IP, puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como clasificador multi-campo (*Multi-Field Classifier*, MF). Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos.

Los nodos DS de ingreso serán responsables de asegurar que el tráfico de entrada cumpla con los requisitos de algún Acuerdo de condicionamiento de Tráfico (*Traffic Conditioning Agreement*, TCA), que es un derivado del SLA, entre los dominios interconectados. Por otro lado los nodos DS de egreso deberán realizar funciones de acondicionamiento de tráfico o conformación de tráfico (*Traffic Conformation*, TC) sobre el tráfico transferido al otro dominio DS conectado.

-Nodos internos DS: son los dispositivos de núcleo (Core Devices) que realizan limitadas funciones de TC, tales como remarcado de DSCP. Los nodos DS internos solo se conectan a nodos internos o a nodos externos de su propio dominio.

A diferencia de los nodos externos para la selección del PHB solo se tiene en cuenta el campo DSCP y es el BA quien clasifica paquetes basado en el código DS solamente.

3.2.2 El Campo Servicios Diferenciados (DS)

Cada paquete IP lleva un byte llamado octeto de Tipo de Servicio (TOS) que es una característica poco utilizada de IP. En IP versión 6 de 128 bits, hay un byte equivalente llamado octeto de Clase de Servicio (CoS).

El campo de 6 bits es conocido como el campo de los Servicios Diferenciados y es marcado con un patrón específico de bits llamado código DS (ver figura 15), usado para indicar cómo cada enrutador debe tratar al paquete.

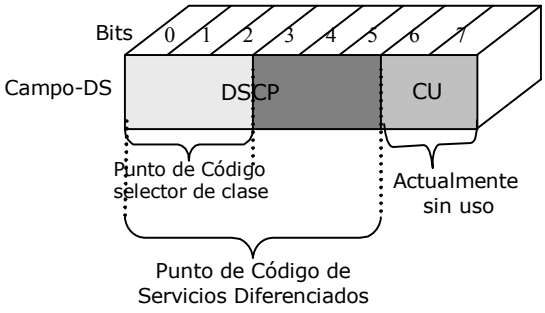


Figura 15. Octeto TOS.

El campo de 6 bits contiene hasta 64 diferentes valores binarios. Los códigos restantes dejan espacio para innovación y optimización de operacionales locales. El marcado de un paquete con el DSCP puede ocurrir en dos lugares:

• la fuente original de tráfico, que puede ser un servidor web que marque el tráfico. Esto tiene la ventaja de que el clasificador puede tener conocimiento explícito de la aplicación en uso y puede por consecuencia marcar paquetes de una manera dependiente de la aplicación.

• un enrutador, como el primer enrutador que el tráfico encuentra el cual clasifica y marca el tráfico. Esto tiene la ventaja de que no se necesita ningún cambio a servidores, pero requiere de alguna "inteligencia" extra en los enrutadores.

Cuando un paquete entra en un enrutador, la lógica de enrutamiento selecciona su puerto de salida y el valor DSCP es usado para conducir el paquete a una cola específica o tratamiento específico en ése puerto. El PHB particular es configurado por un mecanismo administrador de red, fijando la tabla de comportamiento de QoS dentro del enrutador.

3.2.3 Clasificación de los PHB.

3.2.3.1 Default Behavior

El valor de DSCP es cero y el servicio esperado es exactamente el servicio por defecto de la Internet de hoy (por ejemplo, la congestión y pérdida son completamente descontroladas).

3.2.3.2 Expedited Forwarding behavior (EF)

El valor recomendado es 101110. EF intenta permitir la creación de servicios en tiempo real con una tasa de throughput[2] configurable. Con EF se minimiza el retardo, el jitter y se asegura baja pérdida de paquetes y/o ancho de banda asegurado proporcionando el mayor nivel de QoS. También recibe por ello el nombre de "Servicio Premium". Este servicio aparece en los puntos finales como una conexión punto a punto o una "línea virtual alquilada".

Las Pérdidas, latencia y jitter[3] se deben a lo que experimentan las colas de tráfico mientras transitan por la red. Por lo tanto, el proporcionar bajas pérdidas, latencia y jitter para algunos agregados de tráfico, significa asegurar que el agregado vea muy pocas colas o ninguna. Las colas se incrementan cuando la tasa de tráfico entrante excede la tasa de salida en algún nodo.

La creación de este servicio se divide en dos partes:

[2] **Throughput**: Flujo de datos máximo permitido a través de un canal, sin que se produzcan errores en la transmisión.

[3] **Jitter:** es el periodo del desplazamiento de la frecuencia de su lugar ideal

1. La Configuración de los nodos de manera que el agregado tenga una tasa de tráfico mínima de salida bien definida[4].

2. Acondicionar el agregado tal que su tasa de tráfico entrante en cualquier nodo sea siempre menor que la tasa de salida mínima configurada para ése nodo.

3.2.3.3 Assured Forwarding behavior (AF)

El PHB Assured Forwarding (AF) está basado en el servicio seguro (*assured service*, AS), en el cual:

• Se "asegura" que el tráfico conforme al perfil contratado para un flujo será entregado sin pérdidas con probabilidad muy alta, aún en caso de congestión.

• Se permite exceder el perfil, pero con el previo conocimiento de que el tráfico en exceso no será entregado con una probabilidad tan alta.

• Se garantiza la secuencialidad dentro de cada flujo, independientemente de que los paquetes estén o no dentro del perfil.

El PHB AF permite ofrecer distintos niveles de "garantía de entrega" o de calidad relativa para paquetes IP. Para esto se definen N clases AF tal que a cada clase AF se le reservan ciertos recursos (buffer y ancho de banda) en cada uno de los nodos DS, de forma que los retardos y/o pérdidas de una clase sean siempre inferiores a los de una clase de menor prioridad.

Dentro de cada clase, los paquetes se pueden clasificar a su vez en M categorías de preferencia de descarte (dependiendo del marcado en la frontera). En caso de congestión la preferencia de descarte determina la importancia relativa del paquete dentro de la clase. Actualmente N=4 y M=3 son definidos para uso general. Un paquete que pertenezca a una clase AF *i* y tenga una preferencia de descarte *j* es marcado con el código Af*ij.*

En un nodo DS el nivel de "garantía de entrega" de un paquete IP depende de los recursos asignados a su clase AF, la carga actual de la clase AF y en caso de congestión en la clase AF, la precedencia de descarte del paquete.

Una clase AF también puede ser configurada para recibir más recursos que los mínimos previstos cuando hay exceso de recursos en otras clases AF o de otros grupos PHB.

[4] "**Bien definida**" significa independiente del estado dinámico del nodo, en particular de la intensidad de otro tráfico en el nodo.

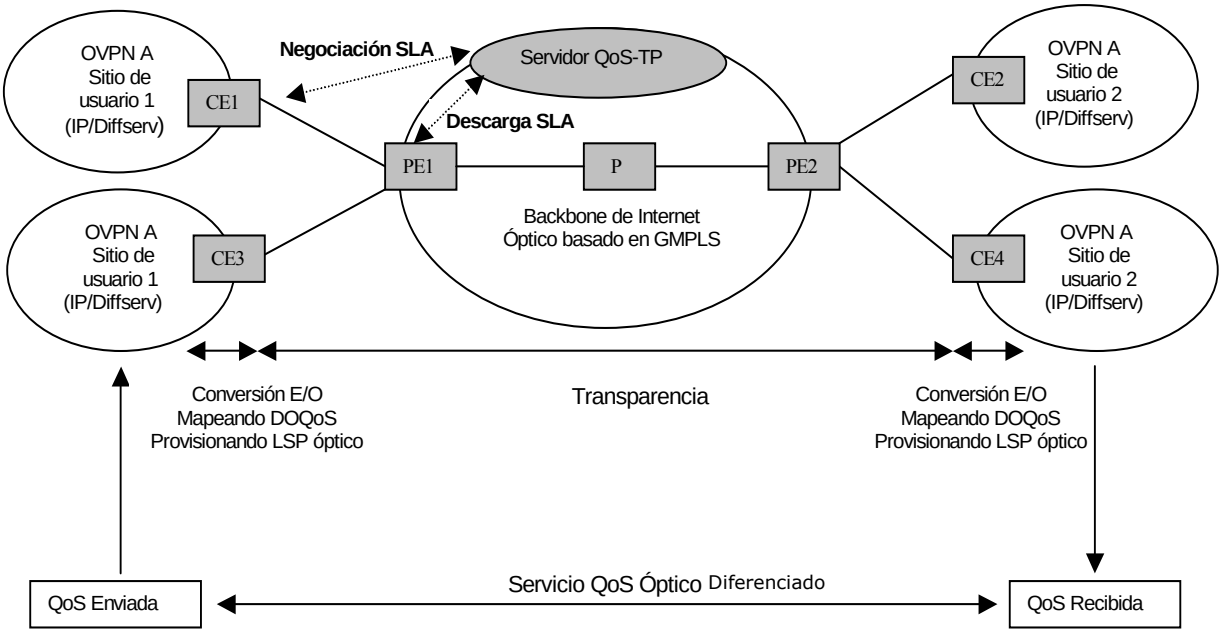
3.3 DIFFSERV EN OVPNs SOBRE IP/GMPLS SOBRE DWDM

Una Red Privada Virtual (VPN) sobre Internet tiene el beneficio de ser flexible y efectiva en costo. Sin embargo esta tiene dificultades para proporcionar suficiente QoS y adecuada capacidad de transmisión para servicios de alto ancho de banda.

Debido al incremento de la demanda de gran ancho de banda para Internet y la necesidad de asegurar QoS en una VPN sobre Internet, IP/GMPLS basado en un plano de control combinado con gran ancho de banda, y la red óptica DWDM que incrementa la capacidad de transporte en una fibra óptica, son vistos como un acercamiento favorable para realizar la futura arquitectura "OVPN sobre IP/GMPLS sobre DWDM" en la cual se efectúa el establecimiento de LSP ópticos (O-LSP) y un esquema de mantenimiento de QoS basado en clases de servicio diferenciadas.

3.3.1 Arquitectura y procedimiento funcional de OVPNs con DiffServ.

La estructura OVPN sugerida esta compuesta de sitios de usuario en el dominio de control eléctrico y la red backbone basada en DWDM en el dominio de control óptico, respectivamente (Ver figura 16).



CE: Dispositivo de Cliente de Borde
PE: Dispositivo de Proveedor de Borde
P: Dispositivo de Proveedor

Figura 16. Modelo OVPN para proporcionar Servicio QoS Óptico Diferenciado (DOQoS).

El escenario externo del usuario es una red IP basada en Diffserv. Este agrega paquetes IP los cuales tienen el mismo nivel de QoS en los nodos de borde de Cliente (CE) para reducir la complejidad de la red.

El backbone de la red OVPN es una red DWDM basada en GMPLS que consiste de nodos de borde de proveedor (PE) y nodos de proveedor (P) y envía tráfico de datos desde los sitios de usuario sin conversiones electrónicas-ópticas-electrónicas (E-O-E).

El backbone cuenta con un servidor de política de tráfico QoS (QoS-TP server) para soportar Calidad de Servicio Óptica Diferenciada (DOQoS) entre sitios de usuario. Este negocia parámetros SLA describiendo el nivel de servicio entre el sitio de usuario y el backbone de la red OVPN y establece un trayecto óptico de acuerdo a los parámetros negociados. De esta manera, el servidor puede administrar completamente la red para soportar los servicios que satisfacen el SLA a través del trayecto óptico entre usuarios finales.

El procedimiento completo de establecimiento de un O-LSP y mantenimiento de QoS para proporcionar DOQoS se muestra en la figura 17.

Las fases A y B muestran la formación del trayecto óptico diferenciado para proporcionar DOQoS entre sitios de usuario, y la fase C es un mecanismo de mantenimiento de QoS por medio de un procedimiento de recuperación de fallas en el backbone de la red OVPN.

La Fase A representa el procedimiento de negociación SLA entre el sitio de usuario y el servidor QoS-TP. Un nodo CE en el sitio del usuario envía una petición SLA que especifica las direcciones IP fuente y destino, el CPI y el PPI, la información de flujo IP agregado, el ancho de banda y parámetros QoS.

Cuando el servidor QoS-TP recibe esta petición verifica el acuerdo del contrato de tráfico que fue negociado con la OVPN. Si este cumple el contrato existente, entonces el servidor QoS-TP descarga los parámetros SLA sobre el agente de política en el PE de ingreso apropiado para solicitar una decisión de asignación SLA.

El nodo PE calcula el trayecto con garantías de QoS, y si satisface al ancho de banda demandado y los parámetros específicos de las clases DOQoS en todos los nodos del trayecto, entonces el SLA es aceptado. Si el servidor QoS-TP recibe un mensaje de que los parámetros SLA han sido aceptados por el nodo PE, se informa al nodo CE de ingreso para que se negocie el SLA entre los dominios de control óptico y electrónico.

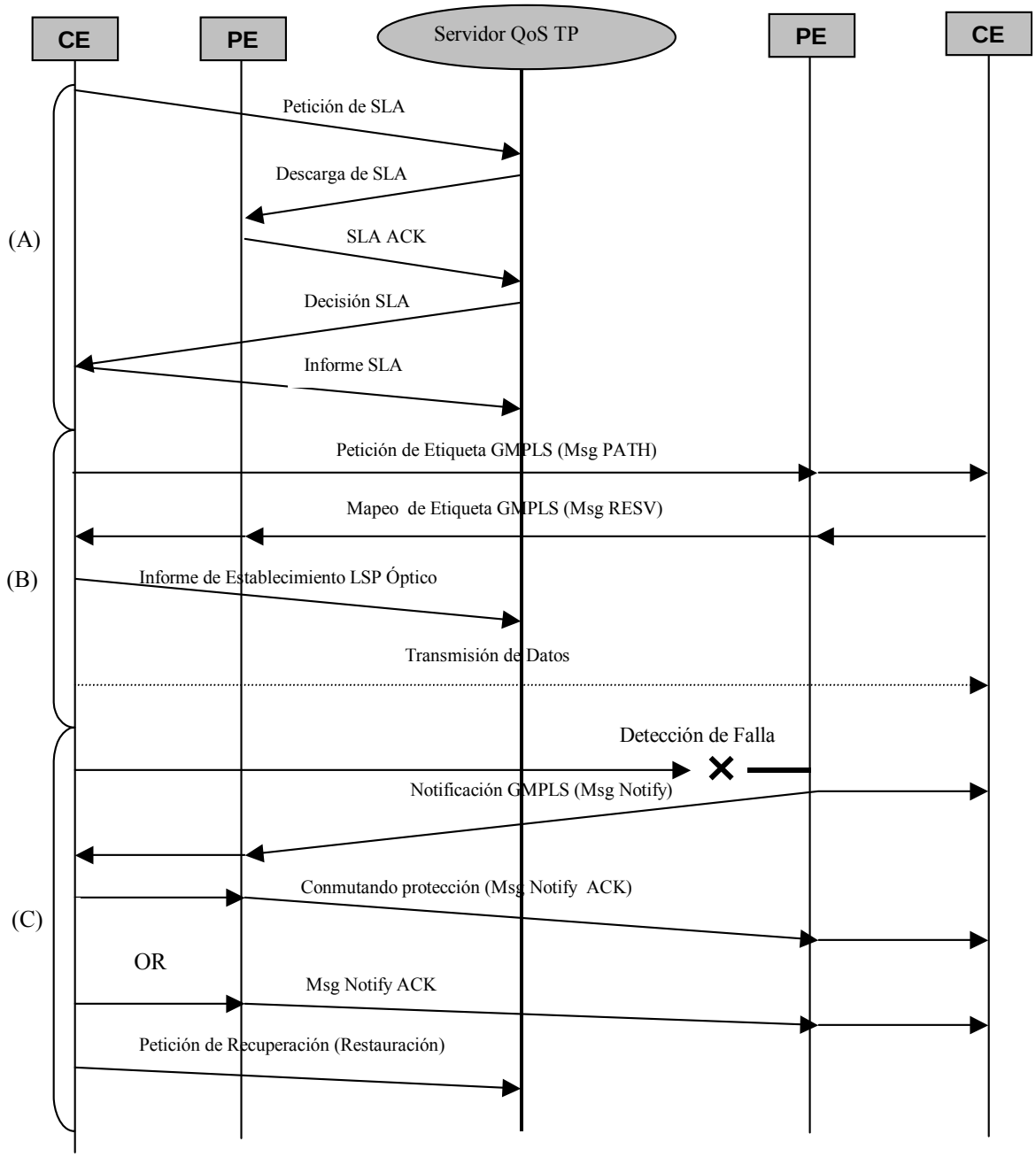


Figura 17. Mecanismo de Operación de la OVPN para proporcionar DOQoS.

La fase B es el procedimiento de distribución de etiqueta de GMPLS para establecer un O-LSP en la OVPN. Generalmente, un protocolo de señalización GMPLS (RSVP-TE o CR-LDP) es usado. Como se mencionó en el primer capítulo, RSVP-TE es el protocolo seleccionado para la asignación de etiquetas.

El mensaje PATH asigna una longitud de onda o puerto por medio de sus objetos GMPLS tales como Petición de Etiquetas Generalizadas, Etiqueta Sugerida, Conjunto de etiquetas, Etiqueta ascendente, etc. (Ver Anexo 1). Si un nodo CE de ingreso recibe el mensaje RESV, la distribución de etiqueta es operada sobre todos los nodos del trayecto óptico entre los usuarios finales.

La fase C es el procedimiento de recuperación de QoS para fallas de red o ataques en el backbone de la OVPN. Las fallas en la red OVPN son detectadas por inter-operación del modulo de monitoreo de potencia (PMM) y el agente gestor de recurso óptico (ORMA). La localización es determinada por la función de gestión de fallas del protocolo LMP.

La ocurrencia de una falla es notificada al nodo CE de la OVPN, y el procedimiento de recuperación se establece de acuerdo al nivel de la clase DOQoS.

Para transmitir transparentemente los datos de usuario a través del backbone de la red OVPN, la estructura de la capa protocolar se muestra en la figura 18.

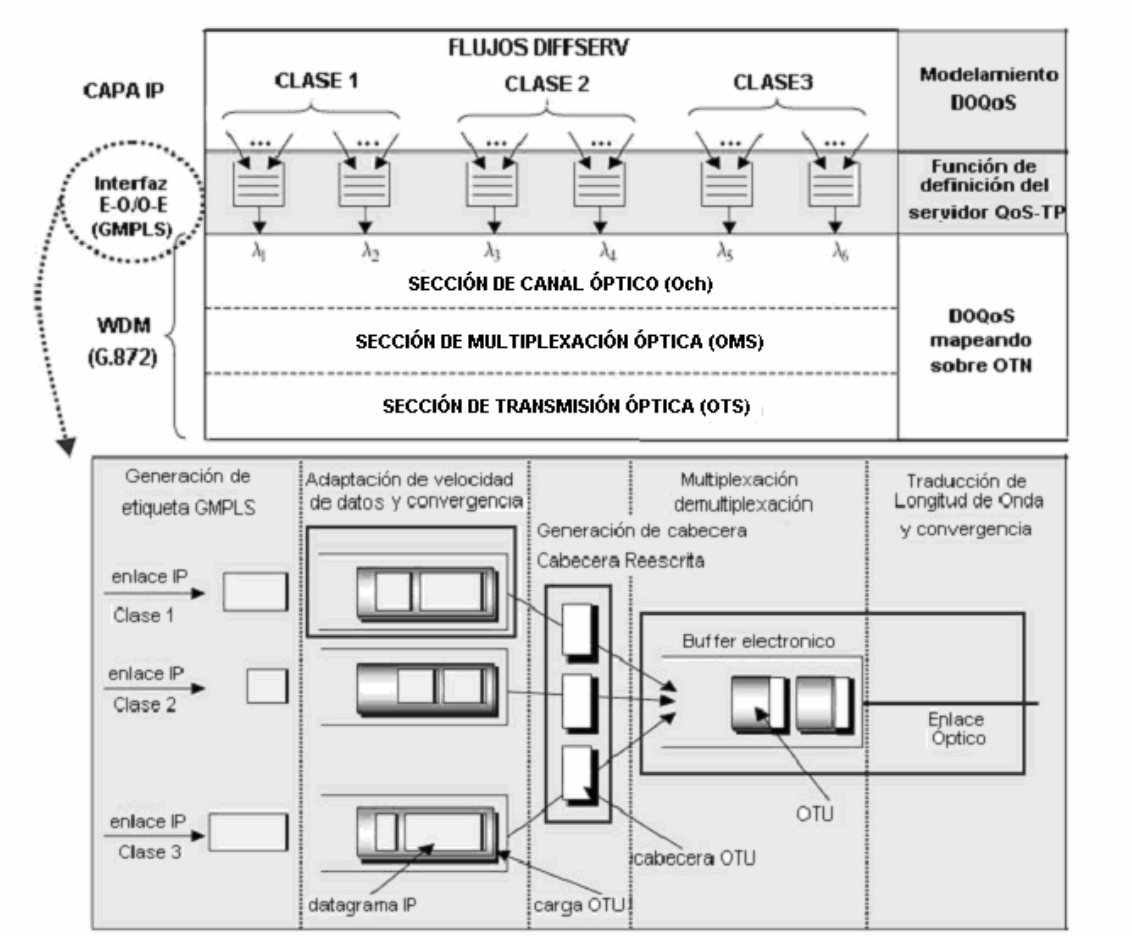


Figura 18. Mapeando DOQoS de servicios IP diferenciados en CE

La OVPN basada en Diffserv reduce la complejidad de la red, primero agrupando flujos de tráfico IP que tienen los mismos requerimientos de QoS y segundo mapeando directamente la clase de servicio sugerida a los canales ópticos en el nodo CE para suministrar DOQoS.

En la interfaz E-O/O-E, los paquetes IP de la capa más alta son clasificados en las clases 1, 2 y 3 (ver figura 18) de acuerdo a parámetros específicos como se describe más adelante.

Las etiquetas GMPLS apropiadas se asignan de acuerdo al nivel de las clases DOQoS y la velocidad de transmisión es controlada por la carga de la unidad de transporte óptica (OTU) que contiene el datagrama IP y la etiqueta GMPLS. Después de crear la cabecera OTU, los flujos OTU son adaptados a la capa WDM para transformar la señal eléctrica a la longitud de onda óptica de acuerdo a la QoS apropiada.

La capa E-O/O-E mantiene la calidad de las señales ópticas con la tasa de error de bit (BER), la relación señal a ruido eléctrico (el.SNR) y SNR óptico (OSNR) para garantizar QoS punto a punto en los niveles de las

diversas clases DOQoS. Las funciones en esta interfaz son ejecutadas por el servidor QoS-TP y el ORMA. Además esta capa también garantiza QoS punto a punto en el nivel de la longitud de onda en el Canal Óptico (Och) para transmitir paquetes IP transparentemente a través de los canales ópticos.

3.3.2 Clases DOQoS

La Clasificación genérica de los tipos de aplicaciones soportadas por el Internet Óptico de Próxima Generación (NGOI) y las OVPNs, puede ser dividida en:

Clase 1 o Servicio Premium: aplicaciones que requieren absolutas garantías de QoS, que tienen requerimientos rígidos en tiempo real, baja pérdida de garantías, retardo, jitter y máximo ancho de banda.

Clase 2 o Servicio Seguro: requiere ciertas garantías de QoS mínimas; ofrecen un nivel esperado de ancho de banda con límite de retraso estadístico como un servicio que presenta un alto grado de tiempo-sensibilidad.

Clase 3 o Servicio de mejor esfuerzo: aquellos que no requieren en todo garantías de QoS explicitas tales como: servicios actuales de Internet por ejemplo transferencia de archivo, navegador web, y e-mail que son soportados por TCP y UDP.

Dentro de los tres servicios descritos anteriormente, la clase DOQoS es clasificada de acuerdo a los parámetros (retardo, jitter, ancho de banda, etc.) de la especificación de nivel de servicio (SLS) VPN negociado en el establecimiento de llamada con respecto a requerimientos BER/el.SNR/OSNR, el esquema de asignación de recurso óptico y supervivencia requerida frente a fallas de red o ataques se muestra en la figura 19. Esta clasificación será aplicada al modelo OVPN sugerido para proporcionar DOQoS.

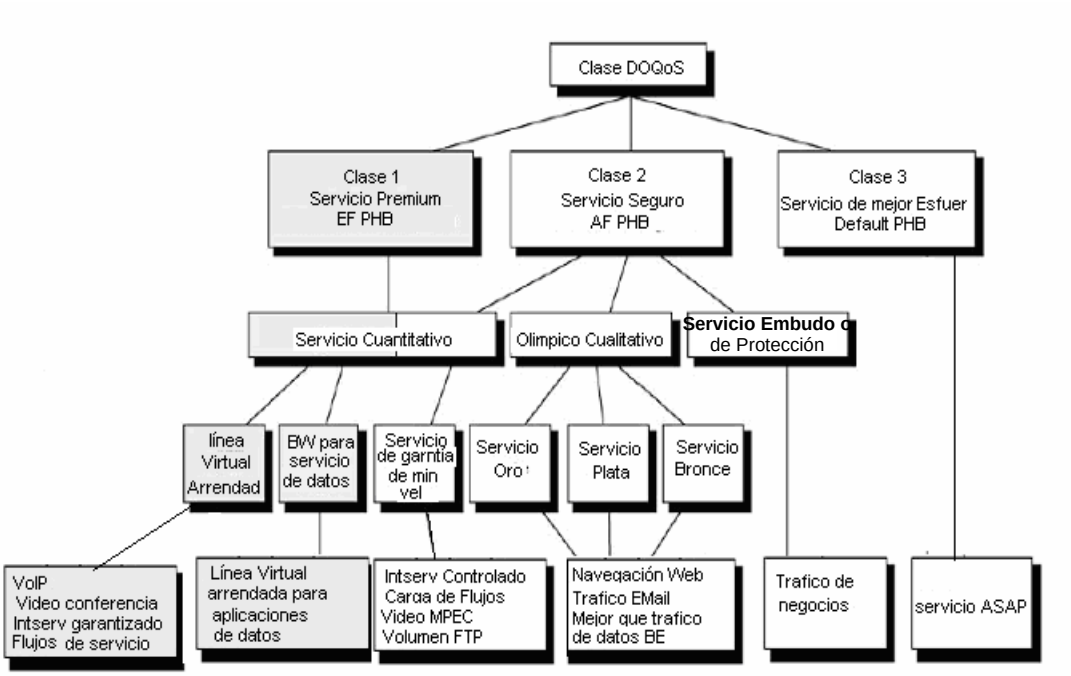


Figura 19. Especificación DOQoS

El contenido de la especificación de nivel de servicio VPN (SLS VPN) contiene los parámetros esenciales de QoS relacionados, incluyendo alcance e identificación de flujo, parámetros conforme al tráfico, y garantías de servicio. Mas específicamente, el SLS VPN tiene los siguientes campos: *alcance* (scope) que muestra el rango de la topología en el cual la política será aplicada; *identificador de flujo* (flujo Id), representa el flujo que comparte por lo menos una característica común, *el identificador de tráfico* que describe las características de tráfico del flujo de paquete IP correspondiente al Flujo Id; *el tratamiento de exceso* indica el parámetro que describe como procesar tráfico excesivo mas allá del perfil convenido; y *parámetros de desempeño*, consistentes de retraso, jitter, perdida de paquete y throughput.

En la cabecera GMPLS, hay un campo *Exp* que es reservado para uso experimental. Este campo se puede usar para clases de servicio (CoS) permitiendo la implementación de servicio de Internet óptico diferenciado, además se pueden procesar paquetes de acuerdo a la prioridad indicada por el valor Exp de los paquetes especificando el servicio de aplicación. El mapeo de acuerdo a las características de servicio se muestra en la tabla 1.

Tabla 1. Valor del Campo Exp GMPLS de acuerdo a los tipos de servicio

Tipo de Servicio	Campo Exp de GMPLS
Servicio Cuantitativo	
Servicio de línea arrendada virtual	111
Ancho de Banda para servicio de datos	110
Velocidad mínima de Servicio Garantizado	101
Servicio Funnel	100
Servicio Olímpico Cuantitativo	
Oro	011
Plata	010
Bronce	001
Servicio de Mejor Esfuerzo	000

3.3.2.1 Parámetros de Desempeño Óptico

En una red DWDM, una fuente-destino tiene varios trayectos ópticos. Para determinar la calidad del servicio óptico en cada camino, es necesario definir características tales como BER, retardo, jitter y el esquema de protección que caracteriza cada trayecto óptico.

Mientras la señal óptica viaja a través de los componentes del trayecto óptico tales como OXC, segmentos de fibra y EDFAs (Erbium Doped Fiber Amplifiers), puede variar por diversas causas tales como jitter, wander[5], crosstalk[6] y amplificadores de emisión espontánea (ASE).

Cuando las señales se propagan hacia el nodo de egreso, la señal de transmisión tiende a ser modificada y su calidad puede rápidamente degradarse. La mayoría de estas modificaciones pueden ser determinadas calculando BER en el nodo receptor, este es uno de los parámetros más importantes para la medida de desempeño del trayecto óptico. Sin embargo, es difícil medir BER en el nivel óptico, ya que el dato en un O-LSP de una OVPN es enviado transparentemente dentro de la conversión O-E.

Para medir el desempeño de la transmisión óptica, el BER se obtiene por el factor Q [9]. El factor Q es un nuevo parámetro que evalúa la calidad de señal, el cual mide la relación señal a ruido (SNR) basado en estadísticas de ruido Gaussiano en el diagrama de ojo.

La relación entre BER, el.SNR, OSNR, y factor Q puede ser expresada por las ecuaciones 2 ,3 y 4 [10]. Además, una clase DOQoS es clasificada

[5] **Wander**: Fluctuación lenta de fase digital
[6] **Crosstalk:** Diafonía- Acoplamiento no deseado de las señales eléctricas presentes en un medio de transmisión con las de otro próximo.

para definir los límites de BER, el.SNR, y OSNR como requerimientos de QoS. Estos factores son usados para detectar fallas de red y por ataques.

$$BER(Q) \cong \left(\frac{1}{\sqrt{2\pi}}\right) * \left(\frac{\exp(-Q^2/2}{Q}\right) \qquad \textbf{(ecuación 2)}$$

$$el.SNR = 10\log Q^2 \qquad \textbf{(ecuación 3)}$$

$$OSNR_{0.1nm} = \frac{(1+r)*(1+\sqrt{r})^2}{(1-r)^2} * \frac{Be}{Bd} * Q^2 \qquad \textbf{(ecuación 4)}$$

r = 0.15 (relación de extinción de la señal óptica transmitida)
Be = 0.75 x f_o (ancho de banda de ruido eléctrico debido a la frecuencia f_o)
Bd = 12.6GHz o 0.1 nm (ancho de banda óptico para medida OSNR)

Ya que en general las señales ópticas tienen una alta capacidad de porcentaje de datos, una falla podría resultar en pérdidas considerables de estos. Por lo tanto los mecanismos de protección y restauración son muy importantes para asegurar que los caminos ópticos sean transparentes ante problemas tales como una línea óptica interrumpida y una longitud de onda dañada.

El servicio premium que transmite datos en tiempo real (como el sonido), requiere muy alta fiabilidad. Este servicio es protegido por un mecanismo de protección local QoS sobre el nivel del canal óptico o un procedimiento backup GMPLS dentro de un tiempo de recuperación de 50ms o menos.

La QoS fiable del *servicio seguro* requiere que se genere un trayecto backup en cualquier suceso de incidentes usando un esquema de restauración O-LSP de GMPLS. El esquema de restauración O-LSP tiene que encontrar dinámicamente un O-LSP de recuperación para reemplazar el camino óptico dañado entre los PEs de ingreso y egreso, esto requiere un tiempo de recuperación mas largo que en el *servicio premium* (diez a cientos de ms). Este esquema utiliza mejor los recursos pero puede tener sucesos de recuperación bajos.

El *servicio de mejor esfuerzo* recomienda un esquema de restauración O-LSP en el nivel IP, donde la interrupción del servicio debido a cualquier falla es compensada por retransmisión de TCP dentro de un rango de tiempo de servicio de 100ms a varios segundos.

3.3.3 Esquema de establecimiento O-LSP basado en clases DOQoS

La interfaz E-O/O-E para mapear el actual flujo de servicio IP diferenciado, el servidor QoS-TP, y la función ORMA son definidos en el plano de control del nodo OVPN para implementar un mecanismo de

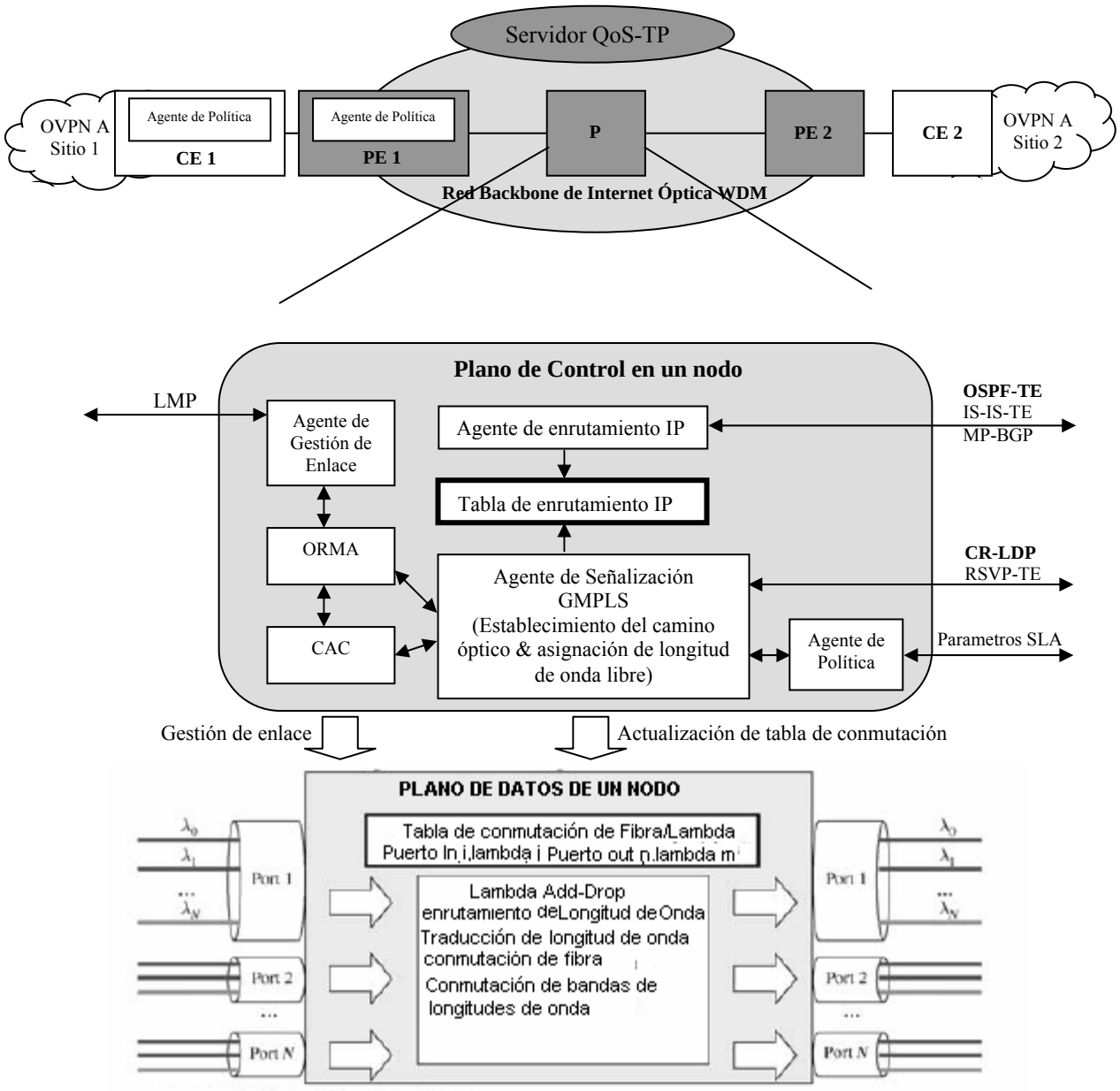
asignación de longitud de onda efectivo. Además, es sugerido el procedimiento de establecimiento de un O-LSP para proporcionar DOQoS.

El servidor QoS-TP maneja la gestión dinámica del SLA entre el sitio de usuario y el proveedor de servicio OVPN y proporciona la gestión de balanceo de carga necesario para mejorar la utilización de la red. Este también maneja operaciones de recuperación de fallas QoS debido a daños en la red o ataques. Además, administra la red completa para proporcionar servicios que se encuentran en el SLA a través del trayecto óptico entre los usuario finales.

Cuando en el backbone de la red OVPN empiezan a darse un nuevo conjunto de características de servicio o funciones, es importante que los cambios en el sitio del usuario sean mínimos. Los enrutadores del lado del usuario deben seguirse usando como antes, así ocurran varios cambios en el backbone de la red OVPN. Esto permite asumir un acercamiento centralizado en el cual un servidor central de política proporciona una interfaz de usuario, la cual puede intercambiar parámetros dinámicos de negociación SLA con un canal de comunicación seguro y realizar un cálculo de camino QoS centralizado y controlar los nodos ópticos dentro del backbone de la red OVPN.

Sin embargo, este acercamiento conduce a problemas de cuello de botella cuando el tamaño de la red empieza a crecer. Por consiguiente, la solución es un acercamiento descentralizado en el cual el servidor de política central solo realiza gestión SLA, mientras que el cálculo de camino QoS y la reservación de recurso son realizados en los PEs de una manera distribuida.

El Gestor de Red de Recurso Óptico (ORMA), clasifica y reserva recursos ópticos en tiempo real interactuando con el LMP y también configura longitudes de onda, enlaces, nodos y amplificadores ópticos disponibles para establecer dinámicamente caminos ópticos. Además, este recibe datos acerca del factor Q monitoreado para calcular el valor BER y tomar la decisión de si es necesario el uso de un mecanismo de recuperación para verificar las limitaciones de la clase de servicio correspondiente. Este también decide como la aceptación/rechazo de la llamada de acuerdo al desempeño de los recursos ópticos disponibles, interactúa con el control de admisión de llamada (CAC). Finalmente, reúne la información del estado de la red y de recursos ópticos de reserva para interactuar con el agente de señalización. (Ver Figura 20).



ORMA: Agente Gestor de Recurso Óptico
CAC: Agente de Control de Admisión de llamada
OSPF-TE: Extensiones OSPF para soporte de GMPLS
IS-IS-TE: Extensiones IS-IS para soporto de GMPLS
MP-BGP: Extensiones multiprotocolo para BGP-4
CR-LDP-TE: Extensiones CR-LDP para soporte de GMPLS
RSVP-TE: Extensiones RSVP-TE para soporte de GMPLS

Figura 20. Procedimiento de negociación SLA y bloques funcionales en un nodo OVPN

3.3.3.1 Procedimiento de negociación SLA

Para soportar servicios ópticos diferenciados a través del backbone de la red OVPN, es necesario implementar un procedimiento de negociación SLA entre el lado del usuario y el servidor QoS-TP como se mostró en la figura 17 (fase A). La figura 20 describe el procedimiento de negociación SLA y los bloques funcionales en el nodo OVPN.

Primero, un agente de política del CE envía una petición SLA que especifica las direcciones IP fuente y destino, el CPI/PPI, la información de flujo IP agregado, ancho de banda y parámetros QoS. Cuando el servidor QoS-TP recibe esta petición, verifica el contrato de tráfico prenegociado con el proveedor de servicio OVPN. Si se satisface el contrato de tráfico, entonces el servidor QoS-TP descarga los parámetros SLA sobre el agente de política en el PE de ingreso apropiado (PE1 en la figura 20) para solicitar una decisión de asignación SLA, el cual a su vez establece un O-LSP usando señalización RSVP-TE.

El agente de política transmite los parámetros al agente de señalización GMPLS de manera que este puede establecer el O-LSP GMPLS desde el PE de ingreso al PE de egreso y puede reservar recursos a lo largo del camino.

Cuando el agente de señalización GMPLS recibe una activación para el establecimiento de un O-LSP, este pregunta al agente de enrutamiento cuales extensiones OSPF o IS-IS debe usar para el soporte de GMPLS (OSPF-TE, IS-IS-TE respectivamente) y encontrar el mejor camino de QoS garantizado para ese enrutador PE de egreso. La dirección de este PE de egreso se resuelve usando las extensiones Multiprotocolo BGP (MP-BGP) que se usan para intercambiar información de enrutamiento entre el lado del usuario en la misma OVPN como se explico en el capitulo 2.

En cada nodo de transito donde el trayecto de QoS garantizado es calculado en el agente de enrutamiento, el ancho de banda solicitado y los parámetros específicos de la clase DOQoS en el mensaje son examinados por el CAC y el ORMA para mirar si es o no posible establecer el O-LSP. Luego este agente de enrutamiento envía el resultado al servidor QoS-TP. En cuanto el servidor obtiene el resultado, informa al agente de política del CE para negociar el SLA entre el dominio electrónico y el óptico.

La figura 21 muestra un organigrama del procedimiento de negociación SLA considerando clases DOQoS entre el CE y el servidor QoS-TP. La negociación SLA es aplicada de acuerdo a los niveles de clase de servicio.

Para el *servicio premium*, como se definió en la sección 3.3.2, la negociación SLA es resuelta para seleccionar un camino activo y un

camino auxiliar satisfaciendo los requerimientos de QoS en la fracción de la longitud de onda preasignada.

Para el *servicio seguro* y el de *mejor esfuerzo*, los cuales tienen menor prioridad comparada con la del *servicio premium*, el SLA es resuelto para seleccionar un camino activo que satisface los requerimientos de QoS en la fracción de longitud de onda pre-asignada.

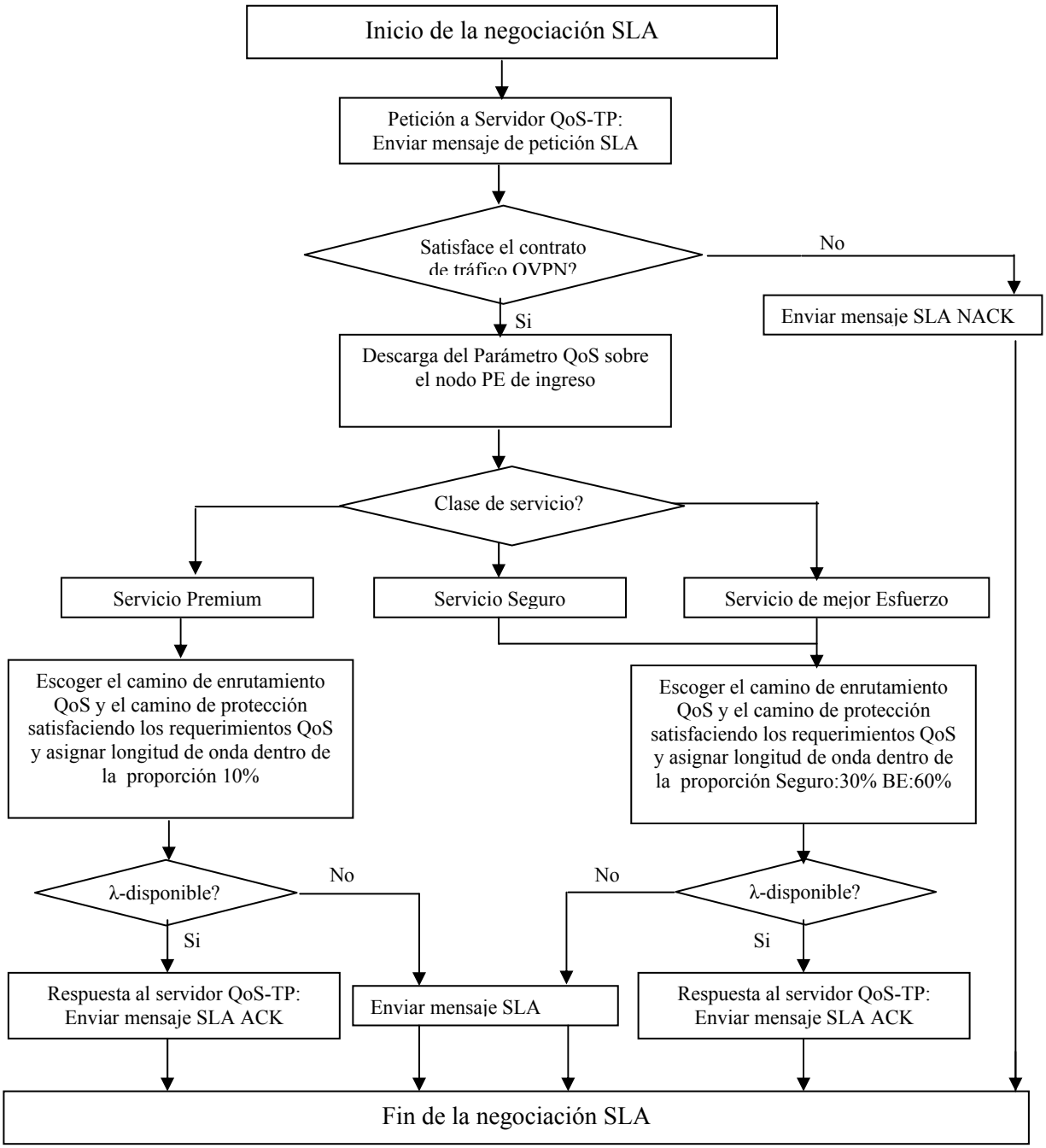


Figura 21. Procedimiento de negociación SLA

3.3.3.2 Señalización para establecer un O-LSP

Después de la negociación SLA entre el lado del usuario y el backbone de la red OVPN, el procedimiento de señalización GMPLS es manejado para el establecimiento del O-LSP. El protocolo de señalización RSVP-TE es usado para la distribución de etiquetas como se ilustra en la figura 22 con los mensajes para reservar recursos PATH y RESV.

Para establecer un O-LSP diferenciado basado en clases DOQoS, el campo Exp en la cabecera GMPLS es usado como función CoS para asignar diferentes valores para cada clase de servicio. El tráfico de cada clase DOQoS y los parámetros QoS son definidos con el descriptor de tráfico (*Tspec*), La especificación de servicio *(Rspec)* y el objeto *Adspec* en RSVP-TE. Como los recursos son reservados con estos parámetros, la QoS diferenciada puede ser garantizada.

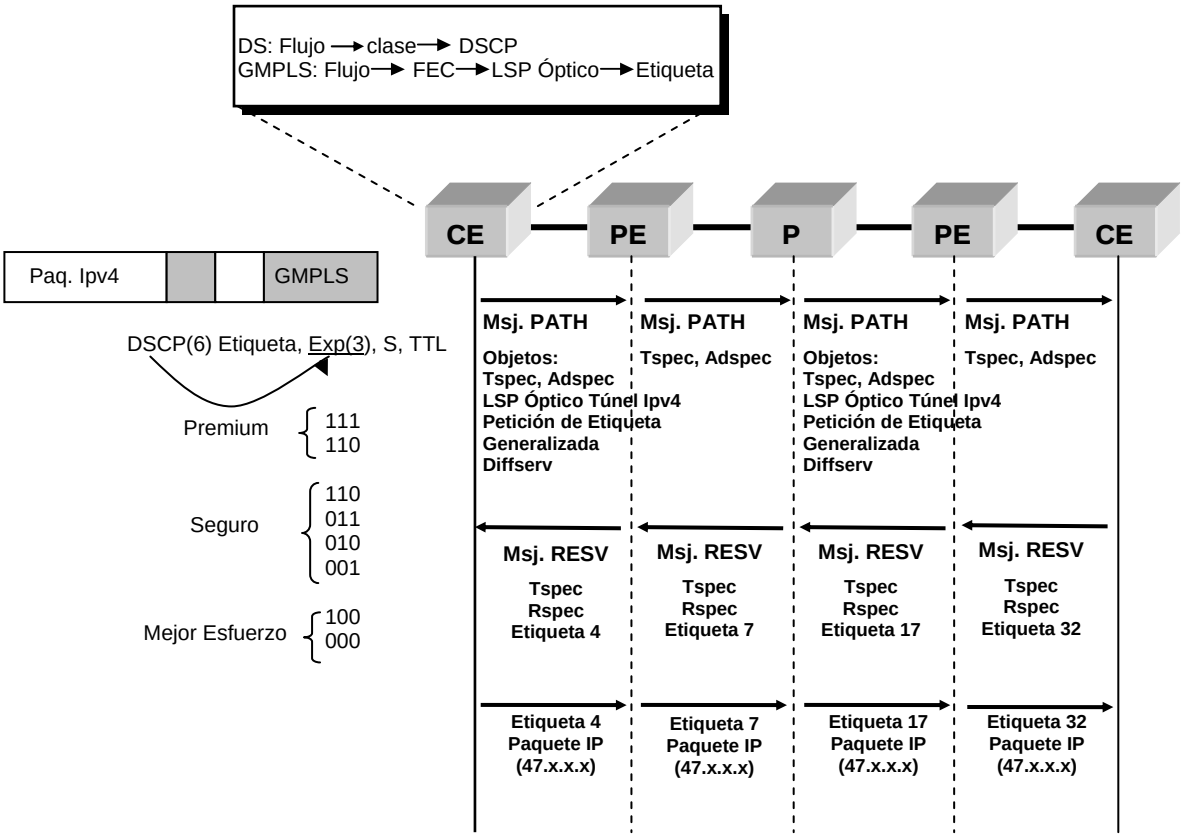


Figura 22. Mecanismos de operación RSVP-TE para asegurar QoS

Tabla 2. Objetos Tspec, Rspec y Adspec

Tspec	p	La máxima velocidad a la cual los paquetes son transmitidos
	r	(bytes/s)
	b	La velocidad a la cual la señal llega al bucket (bytes/s)
	m	El tamaño del bucket de señal (bytes)
	M	El máximo tamaño del paquete que puede ser aceptado (bytes)
		Cualquier paquete con un tamaño mas pequeño que m sera contado como m bytes (bytes)
Rspec	R	La velocidad del servicio o requerimiento de ancho de banda (bytes/s).
	S	La cantidad extra de retardo que un nodo puede adicionar que aun reune el requerimiento de retardo punto a punto. (ms)
Adspec	Bpath	La cantidad de ancho de banda disponible a lo largo del camino seguido por un flujo de datos.
	Qmindel	El mínimo retraso del paquete de un salto o un camino
	Path MTU	La máxima unidad de transmisión (MTU) a lo largo de un camino.
	C_{tot}	La suma de C sobre un camino (C: Termino de error dependiente de la velocidad, medido en byte)
	D_{tot}	La suma de D sobre un camino (D: Termino de error independiente de la velocidad, medido en unidades de 1 micro-segundo)
	C_{sum}	La suma parcial de C entre puntos formados
	D_{sum}	La suma parcial de D entre puntos formados

La tabla 2 muestra los parámetros pertenecientes a los objetos *Tspec*, *Rspec* y *Adspec* necesarios para soportar aplicaciones deseando servicio garantizado.

El *servicio premium* requiere un estricto limite de retraso punto a punto así como ninguna perdida de paquetes, pero solo para el flujo de paquetes que estén de acuerdo con la especificación de tráfico dado. Además, para satisfacer los requerimientos de QoS estrictos, el flujo deberá garantizar un ancho de banda constante. Para esto, un CE de salida busca información para r, b, p y m desde el *Tspec* y para Qmindel, contenidos de error (Ctot, Dtot), PathMTU y Bpath desde el Adspec. El retraso de encolamiento punto a punto (Qdelreq) en el peor caso puede ser obtenido restando Qmindel del tiempo de retraso máximo requerido por el CE de egreso. R puede ser obtenido aplicando Qdelreq, Ctot, Dtot, M, r, b y p en las ecuaciones (4) a (6).

$$Qdelreq = \frac{(b-M)(p-R)}{R(p-r)} + \frac{M+C_{tot}}{R} + D_{tot}\,(p > R \geq r) \qquad (\textbf{ecuación 5})$$

$$Qdelreq = \frac{M+C_{tot}}{R} + D_{tot}\,(R \geq p \geq r) \qquad (\textbf{ecuación 6})$$

$$Qdelreq = \frac{b}{R} + \frac{C_{tot}}{R} + D_{tot}\,(R \leq r) \qquad (\textbf{ecuación 7})$$

Para una exitosa solicitud de reservación de recurso, R deberá ser reducido si es mas grande que el valor de Bpath. El CE de egreso fija el

Rspec con R calculado y el mensaje RESV conteniendo Rspec es enviado al CE de ingreso a través del camino de esta manera la QoS requerida puede ser garantizada.

El servicio seguro no requiere valores específicos para tiempo de retrazo y pérdida de paquetes, pues este permite un cierto rango de paquetes. Los parámetros de tráfico son definidos por *Tspec y Rspec*. Diferente al *servicio premium*, el valor p en *Tspec* no es especificado ya que *el servicio seguro* permite una cierta cantidad de perdida de paquetes dependiendo de la situación de la red.

Como el servicio de *mejor esfuerzo* no necesita reservar recursos específicos, el nodo CE de ingreso puede establecer un túnel O-LSP sin reservación de recurso enviando un mensaje PATH que contiene el *Tspec* puesto en cero y si este recibe un mensaje RESV conteniendo los parámetros *Tspec* y *Rspec* puestos en cero, un túnel O-LSP de recurso no reservado es establecido entre los CEs punto a punto.

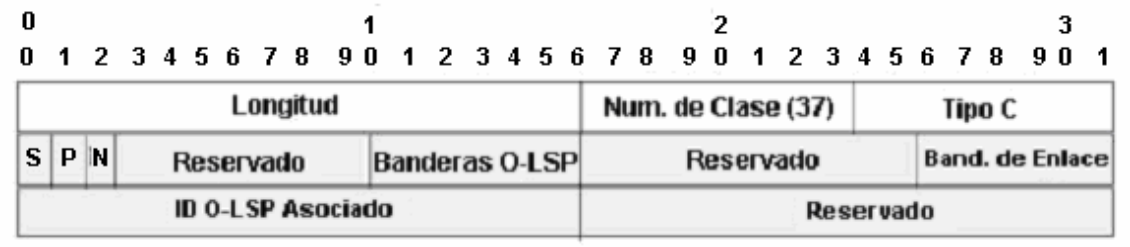
Para *el servicio seguro* o el de *mejor esfuerzo*, que usan el esquema de restauración de GMPLS o nivel IP como mecanismo de recuperación, solo se establece el camino activo.

Pero para *el servicio premiun* que usa el esquema de protección GMPLS, se necesita un camino de protección adicional. Para esto, es necesario fijar a uno el bit P usando el objeto de protección del mensaje PATH como se muestra en la figura 23, que indica que el O-LSP solicitado es un O-LSP protegido.

El objeto *protection* representa el tipo de recuperación O-LSP punto a punto (1:1, 1+1, malla compartida, extra-tráfico, etc.) y el descriptor del camino activo respaldado por el camino de protección (campo asociado O-LSP Id en la figura 23). Tal camino de protección como el camino activo reserva recursos con los objetos *Tspec, Rspec y Adspec*.

Cuando una falla ocurre en el camino activo, el tráfico en este camino es conmutado sobre el camino de protección, esto es hecho usando el mensaje *Notify*[7] con un nuevo código de error que indica "Falla en el LSP activo (Solicitud *Switchover*)*".*

[7] **Mensaje Notiyfy**: Mensaje de RSVP-TE para informar la localización de fallas entre nodos.



S: Cuando se establece a 1, este bit indica que el O-LSP solicitado es un O-LSP secundario. Cuando se fija a 0 (por defecto), este indica que el O-LSP solicitado es un O-LSP primario.
P: Cuando esta en 1, este bit indica que el O-LSP solicitado es un O-LSP protegido.
N: Cuando esta en 1, este bit indica que el mensaje *Exchange* del plano de control es usado solamente para notificación durante la conmutación de protección. Cuando se fija a 0 (por defecto), este indica que el mensaje *Exchange* del plano de control es usado para propósitos de conmutación de protección.
Banderas O-LSP: Indican el tipo de recuperación O-LSP punto a punto deseado. (No especificado / Tráfico Extra / Desprotegido / Malla compartida / Dedicado 1:1 (con tráfico extra) / Dedicado 1+1 Unidireccional / Dedicado 1+1 Bidireccional).
Bandera de Enlace: Indica el tipo de protección de enlace deseado.
ID O-LSP Asociado: Identifica el O-LSP protegido por este O-LSP o el O-LSP protegiendo este O-LSP

Figura 23. El formato del objeto *protection*

3.3.4. Mecanismo de Mantenimiento QoS

El backbone de la red OVPN es una red de transporte todo-óptica DWDM compuesta de OXCs transparentes. La figura 24 representa el sistema DWDM compuesto de los elementos ópticos básicos. En este modelo, un lightpath consiste de un número de OXCs intermedios entre los nodos fuente y destino, interconectados por segmentos de fibra, amplificadores y taps (opcionales).

Los componentes ópticos que constituyen un nodo DWDM en general incluyen un conmutador cross-conector (con o sin función de conversión de longitud de onda), un demultiplexor que consta de divisor de señales (opcional) y filtros ópticos, y un multiplexor compuesto de combinadores de señal.

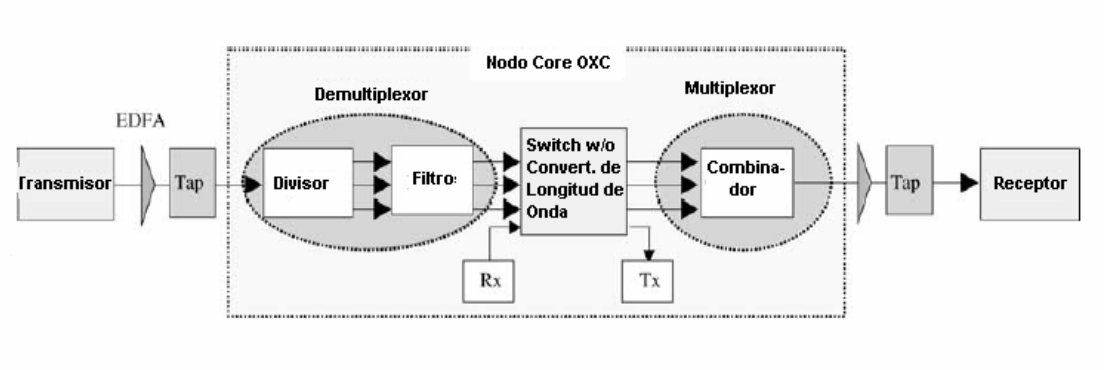


Figura 24. Modelo del backbone de la red OVPN

3.3.4.1 Análisis de fallas QoS

Las fallas QoS en las OVPNs pueden ser considerada de tres tipos. Primero, una falla causada por la violación del contrato inicial de tráfico negociado con el proveedor de servicio OVPN. Segundo, una ruptura de servicio causada por el mal funcionamiento del sistema como resultado de una falla repentina o ataque intencional de elementos activos en la red óptica. Finalmente, una degradación del servicio causada por la atenuación gradual de la calidad de la señal. La tabla 4 resume una clasificación de fallas QoS y su correspondiente mecanismo de detección.

Primero que todo, puede ocurrir una falla causada por violación del contrato de tráfico entre el usuario y el servidor QoS-TP en la petición de establecimiento de un O-LSP CE a CE. El servidor de tráfico QoS- TP informa la falla de la negociación SLA al usuario, y solicita el contrato de tráfico para reajustarlo.
Segundo, la interrupción del servicio causada por una falla o ataque intencional debido al daño de la fibra o transmisor causando mal funcionamiento del láser, puede ser clasificada en tres niveles tales como nivel de enlace, canal y nodo como se muestra en la tabla 3. Ya que la interrupción del servicio incurre en perdida de señales ópticas, es posible obtener la alarma de perdida de luz (LOL) del PMM ubicado en cada nodo. (Ver Figura 25).

Tabla 3. Mecanismos de detección y clasificación de fallas QoS

Categoría		Causa	Característica	Detección
Violación del Contrato de Tráfico		Por violación del contrato de tráfico pre-negociado	Rechazo SLA	Función de gestión SLA del servidor QoS-TP
Interrupción del Servicio	Nivel de Enlace	Daño del enlace físico de la fibra	Perdida de luz (LOL)	Alarma LOL desde el modulo de monitoreo de potencia
	Nivel de Cana	Bloqueo de Canal de Long. De Onda		
	Nivel de Nodo	Daño del nodo		
Degradación del Servicio	Por Ruido	Ruido de intensidad relativa de emisión espontánea amplificado.	Calidad de atenuación de señal gradual	BER/el.SNR/OSNR Estimación por el factor Q.
	Por Distorsión	Dispersión cromática No lineal (SPM,XPM,FWM...)		
	Por crosstalk	Crosstalk interferometico		

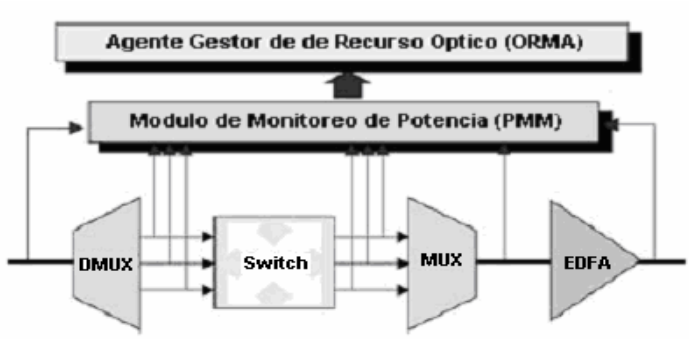


Figura 25. Modelo de detección de fallas QoS

Finalmente, la degradación del servicio es causada por el ruido de fluctuación aleatoria, distorsión de pulso o crosstalk. Sobre todo, la fluctuación aleatoria puede ser distribuida con el proceso Gaussiano tal como ASE o ruido de intensidad relativa (RIN). Generalmente, estas degradaciones de calidad de señal pueden ser detectadas analizando la sobre carga de datos en el nivel eléctrico después de la conversión óptica a eléctrica (por ejemplo, en el caso de usar los bytes B1, B2 en el sistema SDH). Sin embargo, un O-LSP de la OVPN, que no convierte señales ópticas a eléctricas, requiere monitoreo en el nivel óptico. El factor Q es el método para medir la calidad de la señal sin conversión Óptica a eléctrica.

3.3.4.2 Recuperación QoS

La recuperación QoS se realiza en el siguiente orden secuencial: detección de fallas, localización de falla, notificación de falla, y recuperación QoS (protección/restauración).

- **Detección de Fallas**: la violación del contrato de tráfico, puede ser detectada durante el procedimiento de la negociación SLA. De lo contrario, la interrupción del servicio o degradación ocurre durante el proceso de transmisión de datos a través del O-LSP. Asi que hay un mecanismo de detección requerido.

Un modelo de detección de falla QoS se muestra en la figura 25. El PMM de cada nodo detecta las fallas del sistema en el multiplexor/demultiplexor, conmutador o amplificador. Este mas adelante detecta la LOL monitoreando la potencia de entrada y envía la información BER monitoreada con el factor Q al ORMA (Ver figura 26).

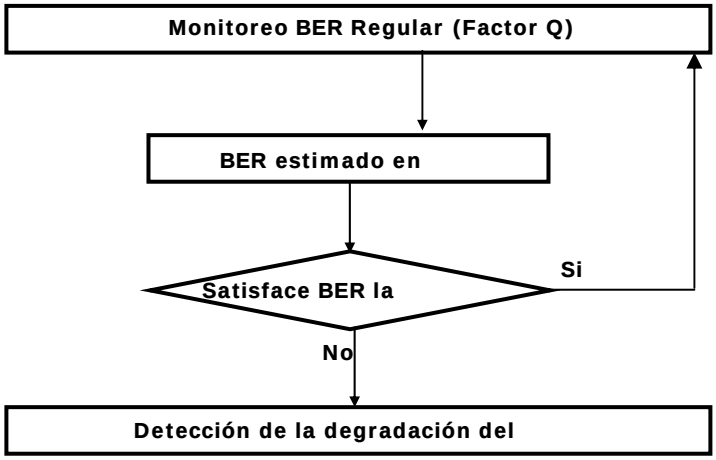


Figura 26. Mecanismo de detección de degradación del servicio

El ORMA detecta la interrupción del servicio con la alarma LOL del PMM. La degradación del servicio es obtenida comparando el valor BER monitoreado regularmente con los límites especificados en la clase de servicio.

- **Localización de Falla:** La localización de falla es el paso de localización que informa el lugar de origen de la falla separando los elementos en mal funcionamiento del tráfico existente, y usa la función de gestión de falla de LMP, el LMP de GMPLS se muestra en la figura 27.

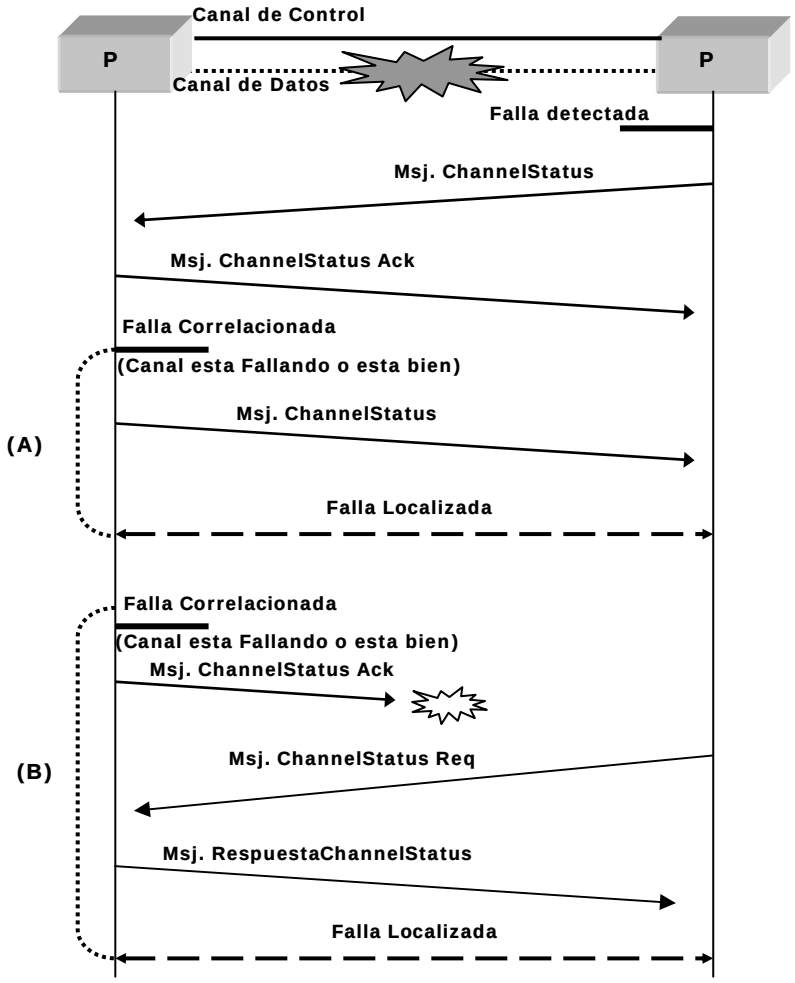
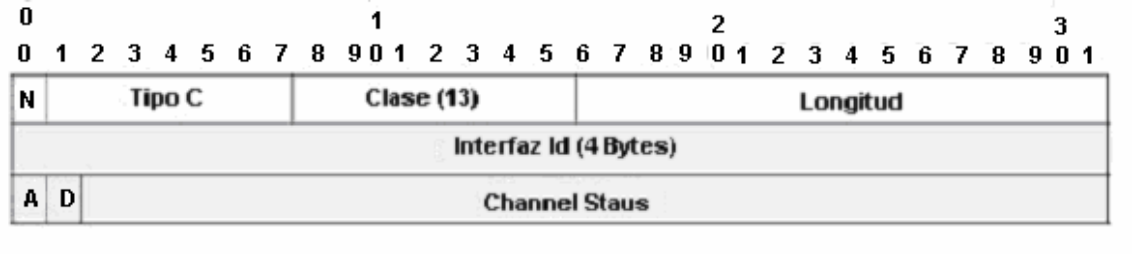


Figura 27. Localización de Fallas usando LMP

Si las fallas definidas en la tabla 4 son detectadas en el ORMA (como se muestra en la figura 25), el LMP informa al nodo ascendente adyacente acerca de la falla usando el mensaje *Channel Status* que contiene un objeto *Channel Status* como se define en la Figura 27.

El objeto *Channel Status* representa el descriptor del enlace de datos (Campo Interface_Id en la figura 28), el estado del enlace de datos (señal correcta, señal degradada, señal fallida), y la dirección del canal de datos.



Interfaz Id: El identificador de enlace de datos
A: (Bit Activo) Indica que el canal esta asignado para tráfico de usuario y el enlace de datos debería ser activamente monitoreado.
D: (Bit Dirección) Indica la dirección (Transmitida /Recibida) del canal de datos

Figura 28. Formato del objeto Status Channel

Cuando el nodo ascendente recibe el mensaje *Channel Status*, este envía un mensaje de regreso *Ack Channel Status* al nodo ascendente y chequea si el O-LSP tiene otras fallas. Después, este localiza la falla entre dos nodos notificándola al nodo descendente por medio de un mensaje *Status Channel* como se muestra en la figura 27 (A). Si no hay mensaje *Channel Status* después del reconocimiento de una falla, este podría ser localizado enviando un mensaje *Channel Status Request* como se muestra en la figura 27 (B).

- **Notificación de Falla**: La notificación de fallas para informar la localización de estas a los nodos intermedios en el O-LSP y el nodo que tiene la responsabilidad del esquema de recuperación usan un mensaje *Notify* RSVP-TE.

En el caso de *servicio premium*, un mensaje *Notify*, que representa una "Falla de trayecto activo; Petición Swichover", es transmitido al CE de ingreso como se muestra en la figura 29 (A). El mensaje *Notify* informa acerca del descriptor de enlace activo y la información de falla así como la degradación de señal, la falla de señal y así sucesivamente. Cuando el CE de ingreso recibe estos mensaje *Notify*, este conmuta a un camino de protección que se muestra en la figura 29 (B), y este informa al CE de egreso usando un mensaje *Notify Ack* como se muestra en la figura 29 (C).

En el caso de *servicio seguro*, el camino de restauración podría ser obtenido dinámicamente reemplazando el camino óptico dañado entre los nodos. Además, el mensaje *Notify* es enviado al CE de ingreso para anunciar que una falla ha estado ocurriendo (igual que en la figura 29(A)). Entonces el CE responde con un mensaje *Notify Ack* (igual que en la figura 29 (C)) y pregunta por el calculo de un nuevo camino satisfaciendo los requerimientos para el servidor QoS-TP (igual que en la figura 29(F)).

En el caso del servicio de *mejor esfuerzo*, este usa un esquema de restauración en el nivel IP. En cuanto el CE de ingreso recibe un mensaje *Notify* de la falla este contesta con el mensaje *Notify Ack* (igual que en la figura 29 (A) y (C) y compensa a través de retransmisión TCP.

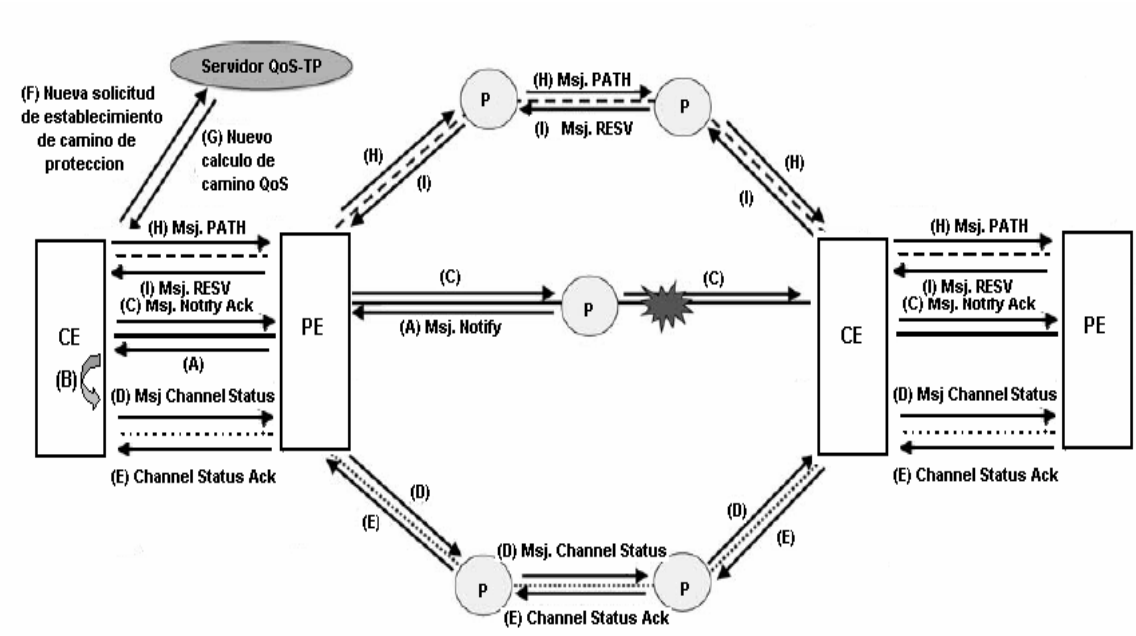


Figura 29. Procedimiento de recuperación de servicio Premium

- **Recuperación QoS (Protección/Restauración):** el *servicio premium* usando el esquema de protección GMPLS conmuta tráfico con un camino de protección preparado para recuperar tráfico después de recibir un mensaje *Notify* en el CE de ingreso. A la vez cada nodo informa acerca de la asignación del tráfico de usuario y solicita monitoreo constante usando el bit A en el mensaje *Channel Status* del LMP para activar el canal de control como se muestra en la figura 29 (D). El nodo descendente recibe este mensaje de vuelta con un mensaje *Channel Status Ack*, y actualiza el estado óptico del ORMA que gestiona los recursos ópticos como se muestra en la figura 29 (E). Luego, para el establecimiento de un nuevo camino de protección, el CE de ingreso pregunta al servidor QoS-TP para hacer el calculo de un nuevo camino de protección que satisfaga los requerimientos QoS como se muestra en la figura 29(F). Si el servidor QoS-TP calcula el nuevo camino de protección, entonces los recursos son reservados por el mecanismo explicado en la sección 3.3.3 y mostrados en la figura 29 (G-I).

En el *servicio seguro*, el cual busca el camino de restauración que satisface los requerimientos QoS como se muestra en la figura 29 (F). Si el servidor QoS-TP tiene calculado un camino de restauración, entonces

los recursos son reservados por el mecanismo explicado en la sección 3.3.3 y se muestran en la figura 22.

Finalmente en el servicio de *mejor esfuerzo*, que no requiere garantías explicitas de QoS, una falla es compensada por retransmisión TCP ya que usa el esquema de restauración del nivel IP.

4. DESARROLLO DE CRITERIOS PARA EL DISEÑO DE UNA OVPN QUE SOPORTA GMPLS Y DIFFSERV

Después de haber realizado un estudio detallado del Multiprotocolo de Conmutación de etiquetas Generalizado (GMPLS), las Redes Privadas Virtuales Ópticas (OVPNs) y el estándar DiffServ, en este capitulo se formulan los criterios de diseño para una red que integra estos tres conceptos.

Inicialmente se plantean los criterios de dimensionamiento donde se consideran los aportes que GMPLS brinda a los proveedores y que permiten determinar las razones por las cuales se debe instaurar en una red óptica, además, los requerimientos que se deben tener en cuenta para implementar una OVPN, la planeación de capacidad y la migración de la red.

En cuanto a la arquitectura física de la red se definen las topologías que ésta soporta y luego se plantean unos criterios de funcionamiento donde se determina la configuración lógica de la red, los diferentes modelos de control que pueden implementarse, los modelos de enrutamiento, señalización y gestión del enlace, el esquema de QoS y los aspectos generales de seguridad.

Finalmente, se establecen los criterios de dispositivos físicos y medio de transmisión necesarios para la implementación final del diseño de la red.

4.1 CRITERIOS DE DIMENSIONAMIENTO

4.1.1 Aportes de GMPLS al proveedor

Algunos de los principales beneficios que ofrece GMPLS de los cuales los proveedores de servicio esperan el más positivo impacto se pueden clasificar en las siguientes áreas:

- Protección y restauración Integrada
- Rápido provisionamiento de servicio
- Incremento de ingresos por usuarios

4.1.1.1 Protección y restauración integrada

Los proveedores de servicio requieren un alto nivel de disponibilidad de red para soportar los requerimientos de fiabilidad, aplicaciones de usuario

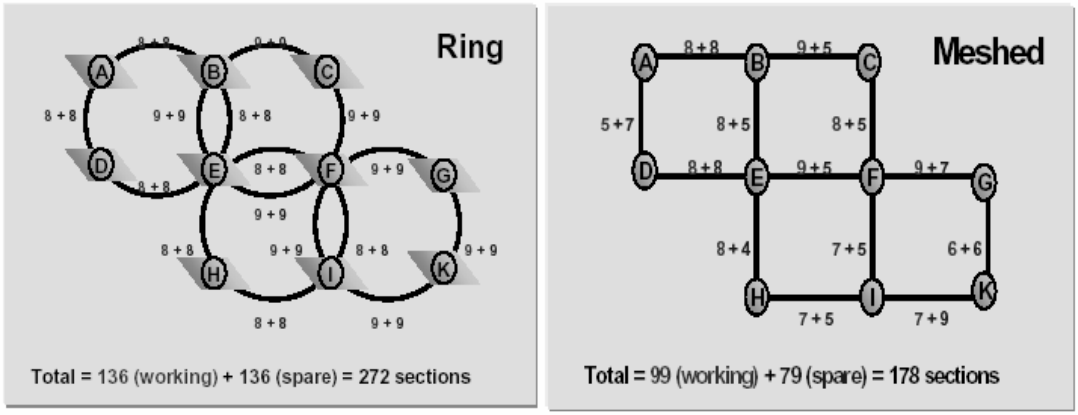
final y Acuerdos de Nivel de Servicio (SLAs). Para lograr altos niveles de disponibilidad, las redes deben implementar técnicas de recuperación en las capas de datos y transporte. Estos esquemas de restauración son diseñados para proteger la red de todo tipo de fallas incluyendo cables cortados, fallas de tarjeta enrutadora, interrupciones de potencia, etc.

GMPLS habilita una técnica de recuperación dinámica multi-capa. Además de la recuperación de fallas ópticas, la capa óptica también ayuda con recuperación de fallas de enrutador. La red óptica reconfigura e incluso re-optimiza la topología IP lógica durante una falla de enrutador.

Como resultado de la restauración de red y capacidades de protección de GMPLS. Algunas de las áreas donde el proveedor de servicios puede lograr ahorros con capacidades de restauración y protección de GMPLS son las siguientes:

- **Plan de restauración y diseño de gestión:** algunos proveedores de servicio han migrado de anillos SDH protegidos a redes en malla para reducir significativamente costos. Una topología de anillo requiere dimensionamiento de toda la sección para el tráfico máximo punto a punto en el anillo y capacidad de protección igual a la capacidad de operación.

En contraste, una red de enlaces mallados SONET/SDH punto a punto puede optimizar el ancho de banda activo y disponible de cada sección, por consiguiente reduce significativamente el costo total de equipos. Esto se ilustra en la figura 30.a y 30.b



(a) **(b)**

Figura 30. Topología de anillo (a) y topología en malla (b)

Para tomar ventaja de una topología en malla, GMPLS trabaja con el establecimiento de inteligencia y automatización en los dispositivos ópticos. La mayor parte del tiempo, la red óptica en malla opera como

una red basada en enrutadores en la forma como esta transporta y restaura el tráfico. Cuando se restauran fallas ópticas, la inteligencia inherente de redes en malla, da a la red más opciones de restauración. Las operaciones de restauración pueden lograr una mayor flexibilidad y configuración dinámica con redes en malla acopladas con GMPLS.

Esta red óptica más inteligente simplifica los procesos de planificación de restauración y ahorra tiempo en manejar los diseños de restauración.

- **Tiempo de restauración y Mano de Obra:** si las fallas en la red de datos pueden ser restauradas en la capa óptica, la restauración puede ocurrir más rápidamente por varias razones. La capa óptica típicamente opera en una alta velocidad y la restauración ocurre en un nivel muy ordinario (es decir, puede conmutar en un momento dado, una cantidad muy grande de tráfico). Esto también minimiza o elimina rupturas en la red de datos. En el caso de una red basada en enrutadores, si la red óptica puede ocultar la falla del enlace, el enrutador no necesita actualizar tablas de enrutamiento y redirigirse.

- **Capacidad disponible**: Los proveedores de servicio tienen que reservar capacidad para protección en las capas de datos y transporte. Usando GMPLS, no necesitan tener gran cantidad de capacidad disponible en la capa IP para recuperar fallas de enrutador IP (o cambios en el modelo de tráfico), la red óptica reconfigura la topología IP lógica durante tales condiciones de falla. Sin embargo, la capacidad disponible aun tiene que ser prevista para distribuir fallas de capa muy baja tales como cables rotos o fallas de cross-conectores ópticos. Es también necesaria mucha capacidad en la capa óptica para soportar la reconfiguración de la topología IP lógica y el tráfico enrutado en la topología.

- **Puertos de Enrutadores**: el ahorro de capacidad puede resultar en ahorro de puertos de enrutadores, además de ahorro del puerto de enrutador en ingeniería de tráfico multi-capa. Los proveedores de servicio pueden aliviar el costo asociado con los puertos de enrutadores soportando el ancho de banda disponible. Los grandes proveedores de servicios pueden esperar ahorrar en costos de capital asociados con puertos enrutadores y capacidad disponible como resultado de usar GMPLS en su red.

Para los proveedores de servicio la restauración y protección está empezando a ser un factor obligatorio para la red, debido a que las empresas utilizan cada vez más la red IP pública para sus funciones de negocios y experimentan el impacto del tiempo fuera de servicio.

Algunas compañías tienen rígidos requerimientos de restauración incluyendo planes desastrosos de continuidad de recuperación de negocios. GMPLS está diseñado para ayudar a proveedores de servicio a

direccionar los requerimientos de disponibilidad de las empresas, minimizando la susceptibilidad a fallas.

4.1.1.2 Rápido provisionamiento de servicio

La intervención humana y el mapeo manual de circuitos son requeridos actualmente para crear nuevos circuitos en las redes particularmente en las ópticas. Este es un proceso muy complejo y a menudo resulta en errores que el proveedor de servicio corrige para provisionar satisfactoriamente el circuito.

GMPLS puede solucionar algunos de esos problemas en el provisionamiento haciendo este proceso mucho mas rápido y uniforme. GMPLS permite provisionamiento en tiempo real y está diseñado para operar en ambientes multi-vendedor, multi-capa y multi-proveedor. Asi, los proveedores de servicio pueden establecer el servicio en minutos u horas usando un proceso automatizado con pequeña o ninguna intervención humana.

Las siguientes son algunas áreas donde las capacidades de provisionamiento de GMPLS permiten reducciones significativas en gastos operacionales:

- **Provisionamiento de tiempo y mano de obra:** muchos de los beneficios de provisionamiento de GMPLS representan ahorros de costos en tiempo de provisionamiento y requerimientos de mano de obra. Los proveedores de servicio describen diferentes maneras por las cuales GMPLS puede ayudarlos a lograr ahorros en costos como son: Descubrimiento de red automatizada, Provisionamiento automatizado extremo a extremo y auto–provisionamiento de usuario

- **Sistemas y Herramientas de provisionamiento**: los proveedores de servicio también pueden ahorrar costos de capital. Ya que no necesitan invertir en sistemas de provisionamiento múltiple. El descubrimiento completo de la red y la inteligencia de la red óptica permiten eliminar o minimizar la necesidad de algunas herramientas de diseño de red y ahorrar en costos de gestión y mantenimiento de sistemas con la solución GMPLS integrada.

- **Tiempo de entrenamiento y costo:** la modernización de los procesos y la integración de funciones requerirán entrenamiento y algo de tiempo para que los usuarios acepten y se sientan cómodos con la tecnología a pesar de la inversión inicial de tiempo de entrenamiento y costo en GMPLS, los beneficios pesan mas que los tiempos de entrenamiento y costos requeridos para operar y soportar sistemas de provisionamiento múltiple y bases de datos múltiples y procesos manuales. La solución de tener sistemas disímiles para plataformas o

capas diferentes empieza a incrementarse así como la red se vuelve más compleja.

Por el contrario en la solución GMPLS, el nivel de esfuerzo permanece relativamente constante aun así el proveedor de servicio adicione más elementos de red y capas

4.1.1.3 Incremento de ingresos por usuario

GMPLS puede mejorar los ingresos en las siguientes formas:

- **Incremento de los ingresos usando SLAs estrictos:** Los servicios pueden ser adaptados a los requerimientos reales del cliente en aspectos como: ancho de banda, tiempos de restauración, conectividad dinámica, tratamiento de tráfico, y tiempos de provisionamiento. Las tarifas premium pueden ser aplicadas a servicios con SLAs "firmes".

- **Más ingresos en menor tiempo**: el auto-provisionamiento y las capacidades de provisionamiento automático pueden reducir el periodo entre el tiempo de peticiones del cliente de un servicio y el tiempo en el que el servicio empieza a ser prestado. Ahora se permite al proveedor de servicio cargar a su cuenta el servicio más rápidamente

- **Mejora de velocidad de innovación de servicio:** Los aumentos en ingresos pueden ser alcanzados desde el lanzamiento de mejoras para servicios existentes y/o el lanzamiento de servicios nuevos y diferenciados. La inteligencia inherente de la red da a los proveedores de servicio la flexibilidad para soportar servicios nuevos y futuros sin hacer incrementos significativos de inversiones. El proveedor de servicio se puede enfocar sobre la definición, provisionamiento, soporte, y gestión a nivel del servicio y relegar otras funciones a la red inteligente.

4.1.2 Requerimientos que se deben tener en cuenta para implementar una OVPN

Las VPN ópticas son un servicio soportado por GMPLS lo cual facilita su implementación permitiendo un servicio de conectividad segmento a segmento sobre una red óptica entre múltiples sitios, reconfiguración transparente de las conexiones locales e incremento o decremento de ancho de banda, así como el uso de la red y/o los cambios de política de red.

Los clientes pueden lograr un mayor nivel de control sobre el comportamiento y configuración de la red usando características de auto-provisionamiento. Controlando su propio ancho de banda, conjunto de priorizaciones, o cambios de distribución de ancho de banda.

Los proveedores de servicio tienen solo que demarcar la superficie de los servicios posibles y pueden ofrecerlos dadas las capacidades disponibles en las plataformas ópticas y de datos.

Es necesario tener en cuenta al momento de implementar una OVPN los siguientes requerimientos en cuanto al servicio en general, al proveedor y al usuario que son una abstracción del proceso de interconexión entre dos sitios de una OVPN descrito en la sección 2.4.1:

4.1.2.1 Requerimientos generales del servicio

1-El servicio OVPN debe soportar tratamiento de puertos y enlaces tal como construcciones lógicas que son utilizadas para representar el agrupamiento de recursos físicos por una OVPN. El servicio OVPN se puede construir usando el mecanismo de enlace agrupado que se describió en la sección 1.8.2.
2-El servicio OVPN debe proporcionar soporte para un amplio espectro de topologías OVPN, tales como: hub-and-spoke , malla completa ,híbrida, etc., las cuales se tratarán mas adelante.

3-El servicio OVPN debe soportar control directo donde existe un canal de control en banda con los enlaces y canales de conexión de datos entre el CE y el PE ONE, o el control indirecto donde existe un canal de control fuera de banda para los enlaces de datos y canales entre el CE y PE ONE. Además, un servicio OVPN debe permitir múltiples enlaces de datos con un canal o enlace de control asociado.

4-El direccionamiento, la señalización y enrutamiento que interactúan entre el proveedor de la red y las redes cliente, están basados actualmente en los modelos de interconexión (modelo overlay, peer, aumentado) del plano de control estándar GMPLS.

5-Para el control y el provisionamiento del servicio OVPN, se deben soportar mecanismos de control distribuidos y centralizados para adaptarse a las plataformas de control y gestión de servicio usadas por diversos proveedores.

4.1.2.2. Requerimientos de la red del proveedor de servicio

1-El servicio OVPN debe permitir que los enlaces de las diferentes OVPNs sean conectados con un PE ONE dado ya que es este quien tiene almacenada la información del dispositivo de cliente.

2-El servicio OVPN debe proporcionar mecanismos para que los puertos en un PE ONE sean divididos en conjuntos (desarticulados), cada conjunto para una OVPN dada. Esto es lo que permite que cada PE pueda tener conectados a el varios CEs.

3-El servicio OVPN no requiere que todos los puertos en un PE ONE dado tengan las mismas características.

4-Para simplificar las operaciones, mejorar la escalabilidad y presentar estabilidad, el servicio OVPN debe proporcionar mecanismos para que un PE ONE dado que tiene por lo menos un puerto asociado con una OVPN dada pueda conocer el resto de los puertos de esa OVPN, incluso si estos puertos están sobre otros PE ONES y aun si esos otros PE ONES pertenecen a otros proveedores de servicio.

5-El servicio de OVPN puede asumir que cada puerto PE ONE tiene un identificador (Identificador de Puerto de Cliente, PPI) que es inequívoco en la red de proveedor de servicio a la que este puerto pertenece. Y en el caso donde el servicio OVPN se extienda a múltiples proveedores de servicio (interconectados), se asume que este identificador es inequívoco a través de todos los puertos PE ONE de esos proveedores de servicio.

6- El servicio OVPN debe permitir que los puertos PE ONE sean identificados en los dispositivos del cliente por las direcciones de la capa de red (por ejemplo direcciones IPv4), o por una combinación del identificador del PE ONE y un índice de puerto/interfaz (por ejemplo interfaces no numeradas IP).

7-Para propósitos de escalabilidad, es recomendable reducir al mínimo la cantidad de cambios de configuración cuando se elimina o adiciona un puerto a o desde una OVPN dada. Igualmente, es deseable que los cambios de configuración/aprovisionamiento solamente se den sobre el dispositivo que este conectado a este puerto.

8- Una red de servicio debe soportar una OVPN que se extienda (interconecte) a múltiples proveedores de servicio o múltiples redes dentro de un solo proveedor de servicio.

4.1.2.3 Requerimientos del cliente

1- El servicio OVPN debe permitir enlaces desde diferentes OVPNs para ser conectados a un PE ONE dado. Asimismo, debe permitir que enlaces desde diferentes OVPNs sean conectados con un CE dado.

2- El servicio OVPN no requiere que todos los puertos en un CE dado tengan las mismas características.

3-El servicio OVPN debe soportar el establecimiento de la conectividad entre un par de puertos que pertenecen a una OVPN dada para estar bajo control del cliente de esa OVPN. El servicio debe proporcionar mecanismos para restringir tal conectividad solamente a los puertos que pertenecen a esa OVPN particular.

4- El servicio OVPN puede asumir que todos los puertos CE que pertenecen a una VPN dada tienen identificadores (Identificador de Puerto de Cliente, CPI) que son únicos dentro de esa OVPN pero no fuera de ella. (como consecuencia, los identificadores de los puertos CE conectados con un PE ONE dado pueden ser ambiguos).

5- El servicio de OVPN debe permitir que los puertos CE sean identificados por cualquiera de las direcciones de la capa de red (direcciones IPv4, IPv6,), o por una combinación del identificador CE y el índice de puerto/interface (Por ejemplo, interfaces IP no numeradas).

6-La arquitectura del servicio OVPN debe soportar los escenarios VPN jerárquicos en los cuales un proveedor de servicio, ofrece servicio OVPN a otro proveedor de servicio quien entonces revende ese servicio de OVPN a sus clientes.

4.1.3 Planeación de Capacidad

El ancho de banda es un factor muy importante y decisivo en la ejecución de servicios sobre una nueva red, pues asegura la adecuada prestación de ellos con alta calidad, posibilitando además la implementación de nuevas soluciones en el futuro.

Al realizar la planeación de una red óptica, cualquiera que sea el propósito de ésta, se debe definir si los requerimientos y necesidades que se presentan en la red son lo suficientemente fuertes para tomar la decisión de implementar GMPLS. Este análisis se debe realizar en base a aspectos como las aplicaciones que soporta, los servicios que se van a prestar, la calidad de estos, y sobre todo la velocidad de transmisión y el ancho de banda necesario para satisfacer las necesidades planteadas.

También debe tenerse en cuenta que cualquier tecnología futura debe tener como característica fundamental la escalabilidad. De esta manera, se hace necesario indicar la forma en que el diseñador de la red podría reemplazar o actualizar los equipos ópticos de conmutación por OXCs, o alternativamente, como se integraría el funcionamiento de un conmutador electrónico con un componente óptico para transformarlo en un OXC. Esto con el fin de reducir el costo del diseño, implementación y futura migración de la red

4.1.4 Migración de Redes

Es importante tener en cuenta este aspecto al momento de diseñar una red ya que permite considerar el estado actual de la red y su adaptación a las exigencias que traen consigo las tecnologías de nueva generación como lo es en este caso GMPLS y el servicio OVPN.

En la actualidad las redes ópticas presentan un gran número de capas. Cada una de estas capas está preparada para manejar un determinado tipo de tráfico y proporcionar unos servicios específicos. Con el tiempo han surgido incluso equipos independientes que están especializados en una capa y en un tipo de tráfico como por ejemplo: enrutadores IP, conmutadores ATM, dispositivos SONET/SDH o conmutadores DWDM. Si bien este planteamiento permite simplificar el diseño de los dispositivos, conduce a redes complejas y difíciles de gestionar. Por ello, últimamente se está tendiendo a reducir el número de dispositivos distintos que se pueden encontrar en la red, consolidando determinadas capas y mejorando sus funcionalidades, a la vez que se eliminan otras redundantes.

La figura 31 se muestra la evolución que está experimentando el modelo de capas de las redes ópticas.

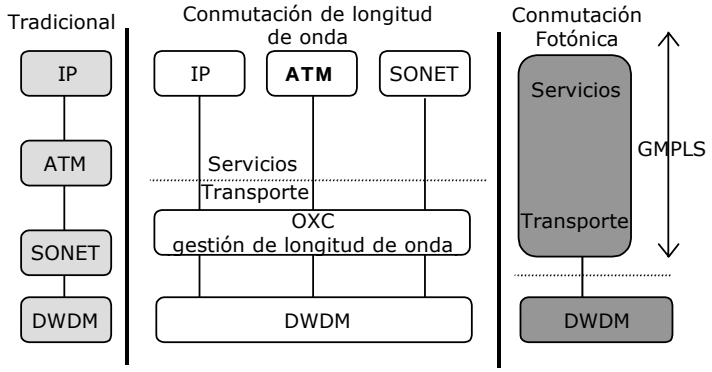


Fig. 31. Evolución del modelo de capas.

GMPLS representa el planteamiento más prometedor para la consolidación de las redes ópticas ya que ofrece un plano de control integrado, el cual extiende el conocimiento de la topología y la gestión de ancho banda a lo largo de todas las capas de red, permitiendo de forma efectiva la consolidación de los servicios y el transporte.

El establecimiento de GMPLS en una determinada arquitectura de red no es necesario que se realice totalmente. No es una cuestión de todo o nada, sino de dónde primero y en qué orden. Para empezar, GMPLS puede desplegarse 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.

A continuación se explican cuatro fases del proceso de implementación de GMPLS en una red:

- Fase 0: 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 red. Las peticiones de establecimiento o de terminación de conexiones se realizan por vía telefónica o a través de un interfaz Web.

- Fase 1: 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 conexiones. Para ello se utiliza un interfaz de señalización basada predominantemente en GMPLS.

- Fase 2: 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 conexiones entre nodos.

- Fase 3: 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. Todos los elementos de red tienen ahora conocimiento del resto de elementos de red que transporten cualquier tipo de tráfico.

Además de las fases descritas anteriormente para la implantación de GMPLS, una solución de red consolidada debe resolver los siguientes aspectos:

– La migración de la red consolidada debe efectuarse sin interrupciones y de forma transparente para los clientes existentes (y nuevos) del servicio de red. Si la nueva red consolidada sirve a clientes en nuevas ubicaciones, dichos nodos deben conectarse sin obstáculos con los nodos anteriores.

– La red consolidada debe mejorar las tasas de retorno internas de los operadores reduciendo las inversiones de capital en el crecimiento de la red y los costes operativos de su mantenimiento.

– La red consolidada debe estar preparada para las aplicaciones de red, nuevas y emergentes. La interconexión entre los antiguos y los nuevos servicios es un requisito clave antes de reducir el número de redes paralelas. El interfuncionamiento (interworking) implica una gran cantidad

de consideraciones operativas, especialmente entre sistemas de soporte para redes diferentes.

4.2 TOPOLOGÍAS FÍSICAS DE LA RED

La selección de una topología para una OVPN es un cambio administrativo que sirve para examinar mecanismos de protocolo que pueden ser usados para automatizar la construcción de la topología deseada y así reducir la cantidad de configuraciones necesitadas. Por lo tanto es útil para un dispositivo de borde OVPN anunciar información de la topología a otros dispositivos de borde OVPN.

Naturalmente, para la topología, todos los sitios OVPN son alcanzables desde los otros; la topología simplemente restringe la manera en que el tráfico es enrutado a través de los sitios.

La topología para una OVPN consiste de un conjunto de nodos interconectados por O-LSPs y puede ser en malla completa, hub and spoke o una topología arbitraria.

4.2.1 Topologia Hub and Spoke

Diferentes topologías OVPN están disponibles. La mas común es la topología hub and spoke , en la cual un número de sitios remotos están conectados a un sitio central, por ejemplo una oficina central y un número de oficinas de área local auxiliares. Los sitios remotos no tienen conectividad directa con otros, solamente al hub y desde el hub. Es posible también tener dos sitios hub o tener conexiones dobles, para carga compartida o propósitos de backup. (Ver figura32)

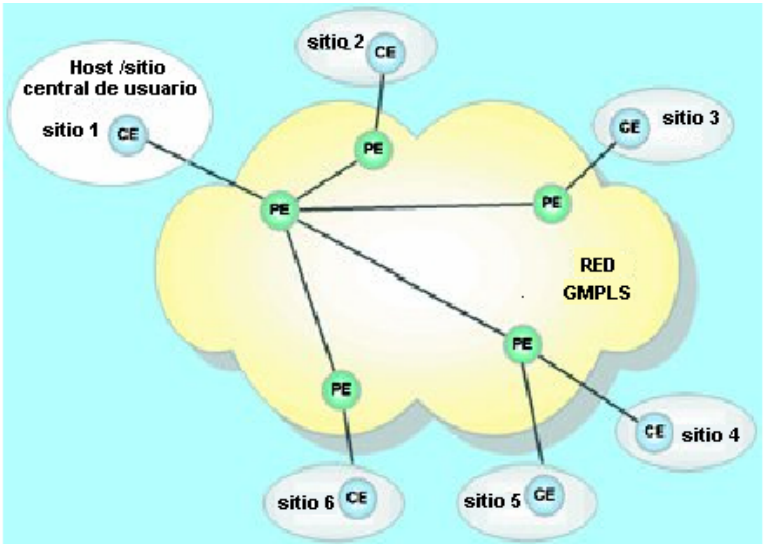


Figura 32. Topología Hub and spoke

4.2.2 Topología Malla Completa

En malla completa u OVPNs de usuario hay completa conectividad entre todos los sitios en la OVPN. Hay también variaciones en las OVPNs de malla completa en las cuales se impide a ciertos sitios tener rutas directas a los otros; estas son conocidas como mallas parciales u OVPNs híbridas. (Ver figura 33)

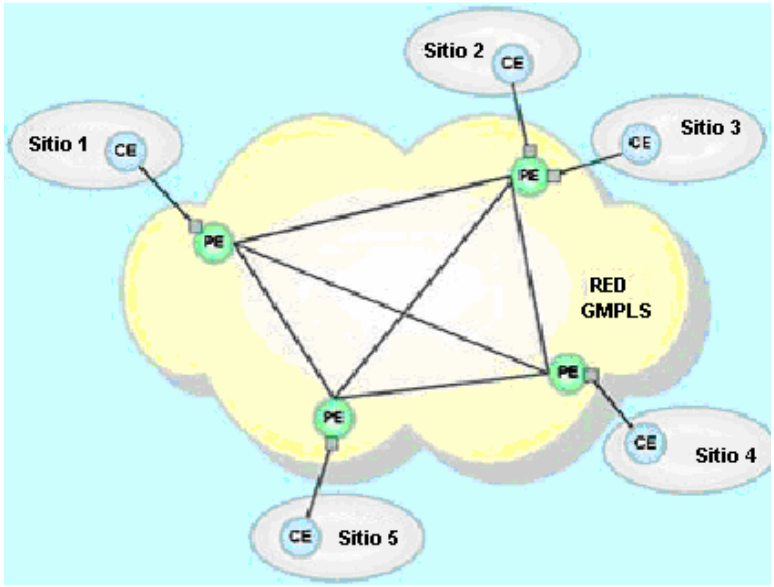


Figura 33. Topología de malla completa

En el pasado, las topologías hub and spoke tendían a ser usada más frecuentemente debido al alto costo o complejidad de proporcionar capacidades de enrutamiento completas entre cada nodo. Con OVPN GMPLS eso no es un gran problema.

4.3 CRITERIOS DE FUNCIONAMIENTO

Para el diseño de una red óptica que presta servicio OVPN es esencial considerar la funcionalidad requerida de esta, al igual que las capacidades y limitaciones de aquellos componentes que la conforman, con el fin de utilizar de la mejor manera posible los recursos.

4.3.1 Topología lógica de red

Una topología lógica consiste de canales ópticos entre nodos llamados lightpaths que se establecen en términos de sus nodos fuente y destino. Estos transportan tráfico punto a punto sin conmutación electrónica, creando una capa óptica de la topología. Esta topología es diseñada en

base a un modelo de tráfico y a una topología física. El conjunto de lightpaths y enrutadores definen una topología lógica, superpuesta a la topología física hecha de fibras ópticas y OXCs.

Es muy importante en el diseño de toda red hacer una configuración lógica, pues permite optimizar algunas medidas por ejemplo minimizar la congestión de la red o el promedio de retraso de los paquetes. Además proporciona adaptabilidad (cuando el modelo de tráfico cambia), capacidad de auto recuperación (cuando la topología física cambia debido a fallas de componentes de red) y actualización (cuando la topología física cambia debido a la adición o modernización de componentes de red).

Para el diseño de una topología lógica es necesario tener en cuenta los siguientes aspectos:

1. Determinación de una buena topología lógica, es decir cual nodo puede ser conectado óptimamente a otro nodo.
2. Enrutamiento de lightpaths sobre la topología física.
3. La asignación optima de longitudes de onda a los lightpaths.
4. El enrutamiento de tráfico sobre la topología lógica.

Los aspectos 2 y 3 definen el problema de asignación y enrutamiento de longitud de onda (RWA) en redes ópticas.

Los aspectos 1 y 4 determinan los pares de nodos que deben ser conectados por lightpaths directos y el enrutamiento del tráfico el cual forma una parte importante en el diseño de la red.

Teniendo en cuenta todo lo mencionado anteriormente se puede definir la configuración lógica de la red soportada por el plano de control GMPLS y su servicio de OVPNs mediante el siguiente proceso:

- Definir las subredes ópticas que conforman la red: esto permite segmentar la red en grupos de nodos caracterizados por patrones similares, tales como fabricante de equipos, distancia entre equipos, cantidad de conexiones, entre otros.

- Ubicar los puntos de frontera de cada una de las subredes ópticas y de la red óptica GMPLS como un todo: luego de definir las subredes que conformarán la red, se debe definir los puntos a través de los cuales estas se interconectarán a las demás subredes, formando así una gran red óptica. Además se debe definir los puntos a través de los cuales la red conformada se interconectará con otras redes semejantes.

- Ubicar los puntos de acceso de clientes OVPN a la red óptica GMPLS: con esto se definen los nodos extremos a través de los cuales los dispositivos de las OVPNs se interconectarán a la red GMPLS.

- Asignar las interfaces de red a cada uno de los puntos de frontera definidos: luego de definir los puntos de frontera, se procede a asignarle a cada uno de estos la interfaz lógica conveniente.

4.3.2 Determinación del Modelo de Control

Para establecer una conexión entre dos dispositivos cliente por una red multi-capa, los planos de control de las dos redes necesitan interactuar entre sí. Por consiguiente, varios modelos de interconexión de planos de control han sido definidos y son soportados por GMPLS: el modelo overlay o tradicional, el modelo aumentado, y el modelo peer. Ellos difieren en el grado de integración entre los planos de control respectivos y es importante comprender que cada uno de estos modelos tiene su propio ámbito de aplicabilidad. El modelo de interconexión óptimo depende del modelo comercial escogido.

GMPLS puede utilizarse con el modelo overlay en el que cada tipo de tráfico se gestiona por medio de su propio plano de control. Sin embargo, el gran potencial de GMPLS hace posible la evolución hacia un modelo peer en el cual cada elemento de red posee información completa sobre el resto de elementos y sus capacidades de enlace.

Los modelos overlay y peer se aplican tanto en el enrutamiento como en la señalización. La arquitectura overlay mantiene capas de red separadas para cada tipo de tráfico y dominios administrativos diferentes. En cambio, las redes basadas en una arquitectura peer se construyen con dispositivos que tienen información completa sobre los otros dispositivos en todas las capas de red. Por tanto, el modelo overlay es adecuado para realizar funciones de red entre operadores, ya que permite que la información de enrutamiento de cada operador de red se mantenga dentro de su propio dominio administrativo. Por otro lado, el modelo peer resulta mucho más adecuado para las funciones de red dentro del dominio de un proveedor de servicios o entre proveedores de servicios con protocolos compatibles, dado que permite mayor flexibilidad en la optimización de las labores de enrutamiento.

4.3.2.1 El modelo Overlay

En el modelo overlay, el enrutamiento, la señalización, la ingeniería de tráfico y la gestión de los recursos internos a los dominios de enrutamiento de las redes ópticas se tratan independientemente de los procesos equivalentes a las redes clientes. La red de transporte óptica ofrece un servicio de conexión entre puntos de acceso a la red de proveedor; sus procesos internos son opacos a las redes clientes y establece en respuesta a una solicitud de conexión un camino entre enrutadores de borde. Este circuito aparece para la red IP como un enlace

clásico, de acuerdo al protocolo de transporte en la red cliente. (Ver figura 34)

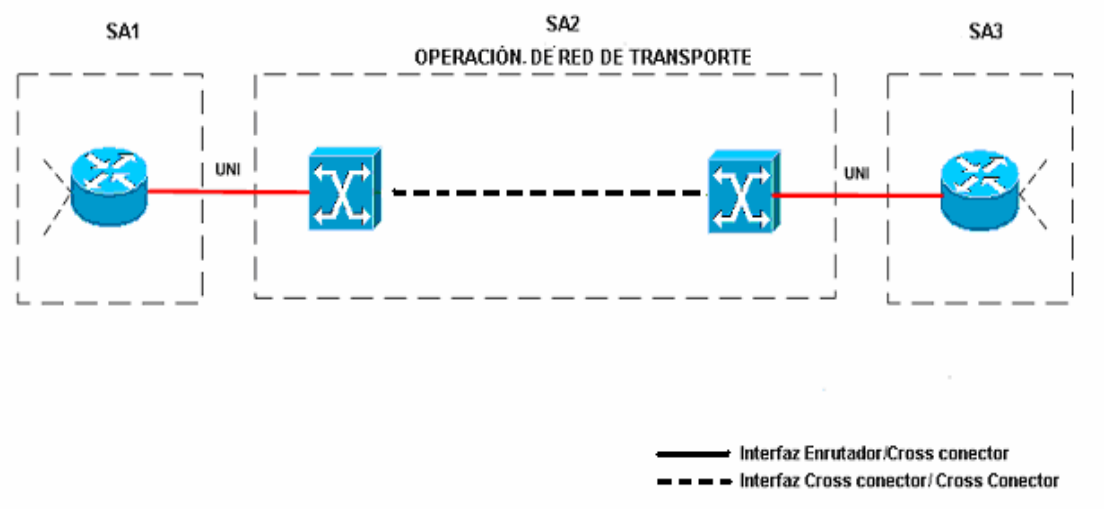


Figura 34. Modelo Overlay

La información intercambiada a través de la UNI permite a la red de transporte óptica prestar un servicio de tránsito interconectando enrutadores de diferentes SA (sistemas autónomos). Este servicio requiere el suministro de información de accesibilidad de los enrutadores distantes bajo control de normas de gestión establecidas por las entidades en cuestión.

Si las redes de transporte y sus redes clientes comparten una misma técnica de plan de solicitud, el modelo de servicio se dice "unificado". Las redes IP llevan los mensajes asociados a los protocolos de enrutamiento IP y de señalización GMPLS.

Si las redes de transporte y las redes clientes tienen planes de solicitud diferentes, el modelo de servicio se dice "diversificado". La interfaz entre enrutadores y cross conectores establece una relación de tipo "usuario-servidor". Este modelo tiene la ventaja de no obligar a la adopción de una misma técnica de solicitud para todas las redes.

Las dos principales razones para desplegar un modelo overlay son:

1. Este modelo de interconexión es el más fácil de llevar a cabo para los proveedores con una base instalada de equipos TDM y para quienes se enfrentan a un crecimiento significativo de tráfico IP y servicios relacionados.

2. Para aquellos proveedores que ofrecen servicios de transporte puede no ser deseable divulgar información interna de sus redes ópticas (por

ejemplo, la capacidad de protección de recursos, la topología física, etc.) a los Proveedores de Servicio de Internet (ISPs) quienes arriendan su capacidad.

En el contexto del modelo overlay, los planos de control actúan entre si a través de las Interfaces Usuario- red (UNI).

4.3.2.2 Modelo Aumentado

Este modelo contempla una operación integrada de las redes IP y de las redes de transporte ópticas a través de un plan de solicitud común. Se aplica en particular cuando se considera un servicio de interconexión extremo a extremo que implica primero un ISP local, un operador de red óptico de larga distancia y un segundo ISP distante. (Ver figura 35)

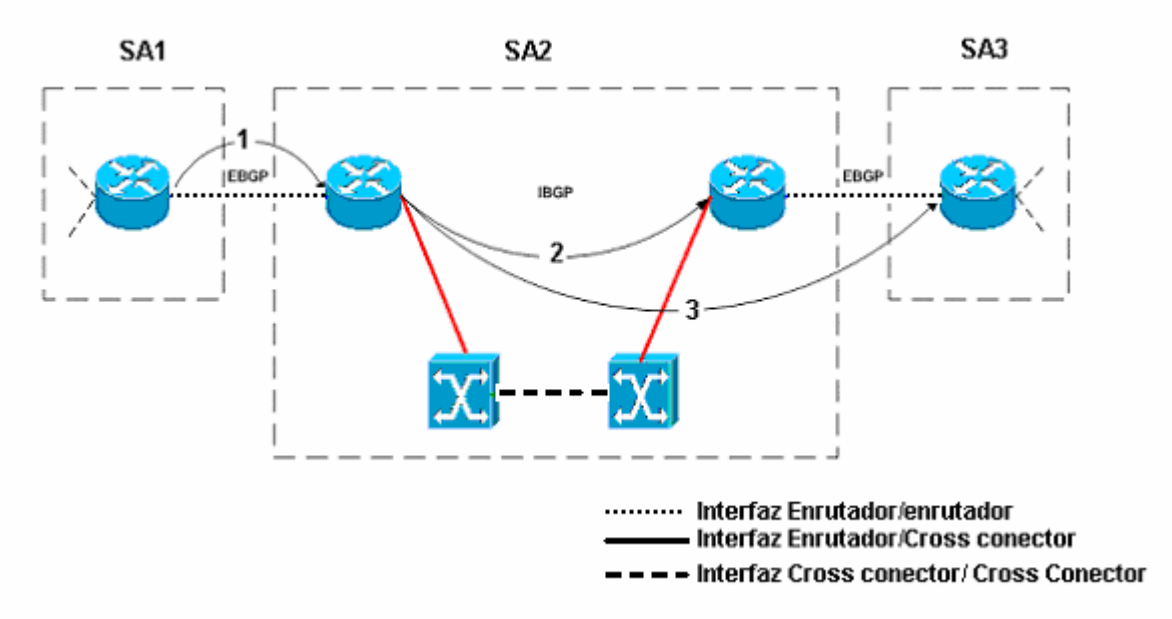


Figura 35. Modelo Aumentado

Se consideran varios dominios de enrutamiento, integrando o los enrutadores de redes (SA1 y SA3), o los cross conectores, o los dos (SA2). Este modelo consiste en adaptar el protocolo de enrutamiento Inter-dominio BGP.

1- La información de accesibilidad del SA1 es transmitida por los enrutadores de borde hacia los cross conectores del SA2 gracias al protocolo EBGP.

2-El protocolo IBGP distribuye esta información a los elementos de la red

3- Se transmiten a continuación hacia el SA distante por los cross conectores o por los enrutadores de borde del SA intermedio. Estos flujos

de información son llevados por las redes de solicitud de los sistemas implicados, de modo que la distribución de la información de accesibilidad de las redes IP distantes a través de una red de transporte óptica no plantee nuevos problemas. Pero, la puesta efectiva del servicio de transporte en el plan de transferencia introduce nuevas especificaciones:

-Un proceso de señalización GMPLS es necesario para el establecimiento del circuito, a partir de un protocolo de señalización común a los distintos AS implicados. La decisión de emitir una petición o de borrar un circuito se relaciona con la ingeniería de tráfico de las redes clientes y de la actualización establecida entre la red de transporte y las redes clientes. Este nivel de decisión implica una gestión dinámica de las conexiones por las redes de transporte.

-Un mismo circuito óptico debe poder llevar varios caminos GMPLS a nivel paquete. El enrutador que inicia el circuito solo conoce, en principio, al cross conector vecino; la elección del camino seguido en la red de transporte óptica es esencial para la ingeniería de transporte del operador. Para que la petición de un circuito MPLS entre enrutadores de borde de AS distantes no se traduzca en la creación de un nuevo circuito óptico, es necesario añadir a la información de accesibilidad de las redes IP distantes, la dirección del cross conector dando la accesibilidad. Las redes IP clientes identifican entonces los circuitos ópticos activos por sus cross conectores de extremo.

- Este modelo no exalta la técnica de establecimiento de los circuitos GMPLS a partir de la información de accesibilidad Inter.-dominio. La identificación de los cross conectores de borde corre el riesgo sin embargo de ser un requisito previo a la petición de establecimiento de circuito. La utilización de BGP en el contexto GMPLS pide que el SA intermedio precise los puntos de entrada y salida del sistema.

El modelo aumentado es apropiado solo para proveedores con múltiples Sistemas Autónomos (AS) o para las grandes corporaciones.

4.3.2.3 Modelo Peer

En este modelo, aplicable a un solo sistema autónomo, una única instancia del protocolo de transporte IGP es responsable de la distribución y el mantenimiento de la información de estado de enlaces (que interconectan dos enrutadores, dos cross conectores o un enrutador y un cross conector):

-Las bases de estado de enlaces administrados por los enrutadores de redes o los cross conectores son idénticas.

-Los enrutadores de redes integran las características específicas de los enlaces ópticos en el cálculo de sus caminos.

-Un mismo protocolo de señalización GMPLS permite el establecimiento de circuitos que implican a enrutadores de redes y a cross conectores.

El cálculo del camino para el establecimiento de un circuito entre un enrutador del dominio IGP y un enrutador distante, tiene en cuenta la topología del sistema. El establecimiento del camino bidireccional GMPLS es iniciado por un mensaje descendente que integra explícitamente en conjunto los enrutadores y cross conectores hasta el enrutador distante. (Ver figura 36)

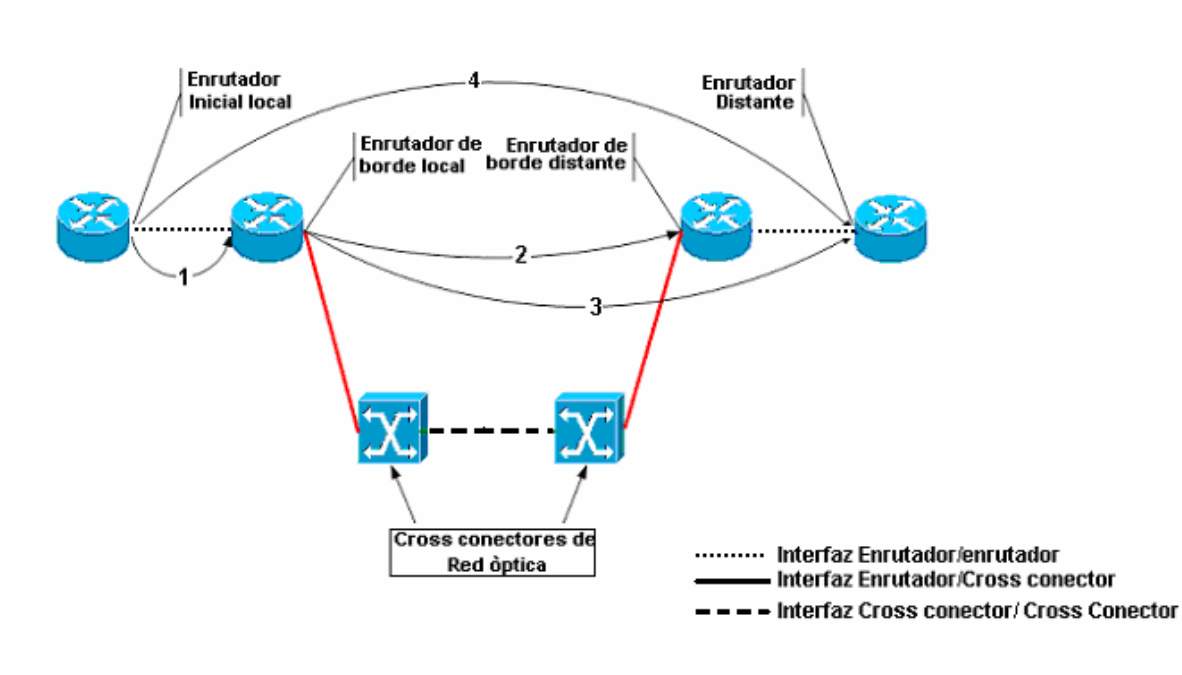


Figura 36. Modelo Peer

1 -El enrutador local inicia una solicitud de establecimiento de un camino hacia el enrutador distante.

2 -El primer enrutador de borde sobre este camino reconoce la existencia de la interfaz enrutador de redes cross conector e inicia el establecimiento de un circuito GMPLS que interconecta el enrutador de borde local y el enrutador de borde distante.

3- Los procesos se continúan hasta el enrutador final distante utilizando el circuito óptico secundario como un enlace virtual entre enrutadores de redes de borde.

4- Finalmente la validación o nueva atribución de etiqueta por el mensaje que proviene del enrutador distante.

El modelo peer, es esencial para operadores que controlan los enrutadores IP y la infraestructura de transporte óptica ya que les permite perfeccionar su diseño de red y funcionamiento extremo a extremo.

4.3.3 Modelo de enrutamiento y direccionamiento

GMPLS se basa en los modelos de enrutamiento y direccionamiento IP. Esto implica que las direcciones IPv4 e IPv6 se utilizan para identificar las interfaces y que los protocolos de enrutamiento distribuidos tradicionales también se utilizan. El descubrimiento de la topología y el estado de los recursos de todos los enlaces en un dominio de enrutamiento se consigue a través de estos protocolos.

Dado que el plano de control y el de datos están desacoplados en GMPLS, un vecino del plano de control no tiene porqué serlo del plano de datos, por ello se requieren protocolos como LMP para asociar los enlaces TE con los nodos vecinos.

Las direcciones IP no se utilizan únicamente para identificar interfaces en hosts IP y enrutadores. De manera general, identifican cualquier interfaz PSC y no PSC. De igual forma, los protocolos de enrutamiento IP se utilizan para encontrar rutas para los datagramas IP con un algoritmo SPF (Shortest-Path-First) y también para encontrar rutas para circuitos no PSC utilizando un algoritmo CSPF (Constrained Shortest-Path-First).

En un modelo superpuesto, cada capa no PSC particular se puede ver como un conjunto de sistema autónomos (AS) interconectados de manera arbitraria. Análogamente en el enrutamiento tradicional IP, cada AS es gestionado por un única autoridad administrativa. El intercambio de la información de enrutamiento entre ASs puede realizarse a través de un protocolo de enrutamiento entre dominios como por ejemplo BGP. Cada AS puede estar subdividido en distintos dominios de enrutamiento y cada uno puede ejecutar un protocolo de enrutamiento intra-dominio.

Cada dominio de enrutamiento (routing Domain, RD) puede estar dividido en áreas. Un RD se compone de nodos habilitados para GMPLS. Estos nodos pueden ser nodos de frontera o LSRs internos.

GMPLS define extensiones a los protocolos de enrutamiento intra-dominio OSPF e IS-IS. Estas extensiones son necesarias para diseminar características estáticas y dinámicas relacionadas con los nodos y los enlaces.

4.3.3.1. Direccionamiento de capas PSC y no PSC

Al utilizar direcciones IPv4 y/o IPv6 no se tienen que situar en el mismo espacio de direccionamiento que las direcciones públicas utilizadas en

Internet. Se pueden utilizar las direcciones IP privadas si no tienen que ser intercambiadas con ningún otro operador. En caso contrario se requieren direcciones IP públicas. Si se utiliza un modelo integrado, dos capas pueden utilizar el mismo espacio de direccionamiento.

Los espacios de direccionamiento de IPv4/IPv6 son más que suficientes para acomodar cualquier capa no PSC. Se puede esperar, de manera razonable, tener muchos menos dispositivos no PSC que hosts y enrutadores actualmente

Nuevas restricciones en los modelos de direccionamiento y enrutamiento IP surgen por los cientos de enlace físicos paralelos que se pueden tener conectando dos nodos y por sistemas como DWDM que permiten cientos de longitudes de onda por fibra que dificultan asociar una dirección IP a cada extremo de cada enlace físico para representar cada enlace como una adyacencia de enrutamiento distinta y para anunciar y mantener estados de enlaces para cada uno de estos enlaces. Con este propósito GMPLS como se menciono en el primer capitulo amplía los modelos de enrutamiento y direccionamiento, para aumentar su escalabilidad con enlaces no numerados y agrupamiento de enlaces. Estos mecanismos se pueden combinar e implementar haciendo uso de las extensiones GMPLS en los protocolos de señalización (RSVP-TE o CR-LDP) y enrutamiento (OSPF-TE o IS-IS-TE).

4.3.4 Modelo de señalización Generalizada.

La señalización GMPLS extiende ciertas funciones básicas de los protocolos de señalización RSVP-TE o CR-LDP y en algunos casos añade funcionalidades. Estos cambios afectan las propiedades básicas de los LSPs, cómo se solicitan y comunican las etiquetas, a la naturaleza unidireccional de los LSPs, cómo se propagan los errores y la información proporcionada para sincronizar el ingreso y la salida.

La especificación de la señalización GMPLS se compone de tres partes:
- Una descripción de la funcionalidad de la señalización.
- Extensiones RSVP-TE.
- Extensiones CR_LDP.

Además define los siguientes bloques constructivos:

1. Un nuevo formato de solicitud de etiqueta genérico.
2. Etiquetas para las interfaces TDM, LSC y FSC llamada Etiqueta Generalizada.
3. Soporte para la conmutación de una banda de longitudes de onda.
4. Sugerencia de etiqueta por el canal ascendente con propósitos de optimización.
5. Restricción de etiquetas por el canal ascendente para soportar restricciones ópticas.

6. Establecimiento de LSPs bidireccionales con resolución de contiendas.
7. Extensiones para la notificación de fallos rápida.
8. Información de protección centrándose actualmente en la protección del enlace más indicación de LSP primario y secundario.
9. Enrutamiento explícito con control explícito de etiquetas para un grado de control fino.
10. Parámetros específicos de tráfico por tecnología.
11. Manejo del estado administrativo del enlace.

GMPLS es una arquitectura genérica con muchas opciones. Sólo los bloques constructivos 1, 2 y 10 son obligatorios y sólo dentro del formato específico requerido. Los bloques 6 y 9 normalmente deberán ser implementados. Los bloque constructivos 3, 4, 5, 7, 8 y 11 son opcionales.

Una red de conmutación de longitud de onda típica debe implementar los bloques constructivos 1, 2 (el formato genérico), 4, 5, 6, 9 10 y 11. El bloque 3 sólo será necesario en la conmutación por bandas de longitudes de onda (waveband switching).

4.3.5. Modelo de gestión de enlace

Cuando se usa GMPLS para señalizar los LSPs a través de las redes ópticas, aparecen muchos aspectos de gestión que se resuelven con el desarrollo del protocolo LMP como son:

• La forma en que se puede precisar la localización de un fallo donde la mayoría de los conmutadores de una red óptica son fotónicos y no pueden detectar automáticamente el "Loss of Light"

• La forma en que se puede proteger el protocolo de enrutamiento para no tener que anunciar un gran número de enlaces, cuando el enlace entre dos conmutadores consta de una agrupación numerosa de fibras ópticas.

•De que manera los dispositivos vecinos con un gran número de fibras, pueden acordar como direccionar estos enlaces sin configurar manualmente cada nodo con el esquema de numeración de enlace del otro dispositivo.

•Dado que se requiere algún protocolo de sesión de canal para direccionar estas cuestiones, el protocolo necesita características adicionales como autenticar los puertos de sesión y detectar sesiones interrumpidas.

Entre dos nodos de una red óptica, puede haber múltiples enlaces paralelos ópticos de datos que pueden transportar 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.

• Transparente, por ejemplo si un 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).

El trabajo fundamental que el LMP realiza, es validar el cableado de los enlaces entre nodos adyacentes, validar que cada enlace de datos está operacional y localizar fallos. Por lo tanto el intercambio de protocolo LMP solo se requiere entre nodos adyacentes que están directamente conectados por enlaces de datos. La especificación de LMP de la IETF cubre las siguientes áreas de funcionalidad de este protocolo: Gestión del Canal de Control, Verificación del Enlace, Correlación de Propiedad del Enlace, Gestión del Fallo, Autenticación. Las dos primeras son procedimientos obligatorios y los demás son opcionales.

En la tabla 4 se resumen las principales funcionalidades de los protocolos que corresponden a los tres modelos descritos anteriormente que soporta GMPLS:

Tabla 4. Descripción de los protocolos de GMPLS

PROTOCOLOS		DESCRIPCIÓN
Enrutamiento	OSPF-TE IS-IS-TE	Protocolos de enrutamiento para el auto-descubrimiento de topología de red, anuncio de disponibilidad de recurso (es decir, ancho de banda o tipo de protección). Las mayores mejoras son las siguientes: Anuncio de tipo de protección del enlace (1+1, 1:1, no protegida, tráfico extra). Implementación de enlaces derivados (Adyacencia de envío) para mejorar la escalabilidad. Aceptación y anuncio de enlaces sin direcciones IP –ID del enlace. ID de Interfaz de entrada y de salida. Descubrimiento de ruta para back-up que es diferente que el camino primario (Riesgo-compartido enlace de grupo).
Señalización	RSVP-TE CR-LDP	Protocolos de señalización para el establecimiento de LSPs con ingeniería de tráfico. Las mayores mejoras son las siguientes: Intercambio de etiquetas para incluir redes no basadas en paquetes (etiquetas generalizadas). Establecimiento de LSPs bidireccionales. Señalización para establecimiento de caminos back-up (Información de protección). Rápida asignación de etiqueta vía etiqueta sugerida.

		Soporte de conmutación de bandas de longitudes de onda –conjunto de longitudes de onda contiguas conmutadas al mismo tiempo.
Gestión de enlace	LMP	**Gestión del canal de control**: Establecimiento por negociación de parámetros de enlace (es decir, la frecuencia de envío en mantenimiento –en actividad de mensajes) y garantizar la actividad de un enlace (Protocolo Hello). **Verificación de conectividad del enlace:** Garantiza la conectividad física del enlace entre los nodos adyacentes usando un mensaje de prueba como PING. **Correlación de propiedad del enlace**: Identificación de las propiedades del enlace de los nodos adyacentes (es decir mecanismos de protección). **Aislamiento de fallas**: Aislamiento de una o múltiples fallas en el dominio óptico. **Autenticación**: Suministra confirmación criptográfica de la identidad del nodo vecino.

4.3.6. Interconexión

El éxito de GMPLS parcialmente depende de su habilidad para comunicarse con las muchas infraestructuras de red existentes ATM o Frame Relay. La interconexión con redes ATM y Frame Relay permite transporte de información del plano de control y de datos intercambiada entre dos redes similares. (es decir, redes ATM) a través de una red disímil (es decir, GMPLS)

La implementación de funciones de interconexión entre estas redes enfrentan estos problemas:

1. La interconexión en el plano de control es muy complicada porque diferentes conjuntos de protocolos son usados en cada red (es decir: enrutamiento, interfaz red a red privada en ATM versus OSPF-TE en redes GMPLS).

2. El mantenimiento de la calidad de servicio extremo a extremo como el tratamiento de datos que viajan a través de diferentes tipos de red es esencial.

3. La conmutación GMPLS puede ser basada en paquetes, TDM, longitudes de onda, bandas de longitudes de onda, o en fibra. Esto crea varias combinaciones en el contexto de interconexión del plano de datos entre las redes GMPLS y redes ATM o Frame Relay (FR), las cuales llevan datos en celdas o tramas respectivamente.

4.3.7 Esquema de Calidad de Servicio

Actualmente es muy importante para el diseño de una red tener en cuenta la Calidad de Servicio (QoS) ya que este factor es el que permite a un elemento de red tener la capacidad para asegurar que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos. Para esto se debe tener en cuenta lo siguiente:

- Una red debe garantizar el ofrecimiento de un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros de QoS como son: el retardo, la variación del retardo (jitter) y la pérdida de paquetes.

- La implementación de Políticas de Calidad de Servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

  · Asignar ancho de banda en forma diferenciada
  · Evitar y/o administrar la congestión en la red
  · Manejar prioridades de acuerdo al tipo de tráfico
  · Modelar el tráfico de la red

- En muchos casos no se tiene capacidad suficiente para asegurar QoS al tráfico total. Sin embargo, existen diferentes tipos de tráfico con diferentes requerimientos por lo cual si se divide la capacidad de los enlaces separando el tráfico de distintas clases se puede lograr cumplir con los requerimientos de QoS de cada clase.

- El modelo de Servicios Diferenciados en una OVPN sobre GMPLS se puede lograr a través de la aplicación conjunta de los siguientes mecanismos:

  1. Después de tener establecida una completa arquitectura de red es decir las OVPNs sobre el backbone de red GMPLS con sus respectivos CE en el lado del usuario, PE y P en el lado del proveedor se debe implementar un servidor de política de tráfico QoS el cual soporta la DOQoS (Calidad de servicio diferenciada) y es el que negocia los parámetros del SLA y establece el trayecto óptico.

  2. Luego de tener establecida la red, lo primero que hace Diffserv es dividir el volumen total del tráfico en clases con requerimientos diferentes de QoS de acuerdo a parámetros específicos (BER, retardo, jitter). Las tres clases en que se puede lograr la distribución de flujo son: Servicio Premium, Servicio seguro y Servicio de mejor esfuerzo que se explicaron en la sección 3.3.2.

2. Una vez dividido el flujo en clases, se realiza el procedimiento de distribución de etiquetas de GMPLS para establecer un O-LSP en la OVPN de acuerdo al nivel de las clases DOQoS.

3. Cuando se presentan fallas en la red o ataques al backbone la recuperación de QoS se realiza de la siguiente manera: detección, localización, notificación y protección/restauración. Igual que el paso anterior la recuperación se establece de acuerdo al nivel de las clases DOQoS.

Además de los parámetros técnicos que permiten aplicar QoS en una red, existen otros muy importantes que deben tenerse en cuenta que son los Acuerdos de Nivel de Servicio (SLAs), los cuales permiten definir los siguientes aspectos:

- Las responsabilidades del proveedor en términos del nivel de funcionamiento de la red (rendimiento, tasa de pérdidas, retrasos, variaciones) y
- La disponibilidad temporal
- El método de medida,
- Las consecuencias cuando los niveles de servicio no se consiguen o si los niveles de tráfico definidos son superados por el cliente.

Pudiendo determinar los puntos en común entre los objetivos de la organización y las expectativas del cliente, se puede identificar claramente los puntos críticos a tener en cuenta en el servicio que presta y, por ende, establecer la base de los proyectos para mejorar la calidad.

4.3.7.1 Beneficios al aplicar QoS

Al aplicar QoS se obtienen beneficios para las aplicaciones, las empresas y para los proveedores de servicio, estos son:

Ventajas para las aplicaciones: es cada vez más importante que los administradores de las redes aseguren que éstas entreguen unos niveles apropiados de calidad. Es aquí donde las tecnologías de QoS cobran especial importancia, proporcionando a los administradores las utilidades para la entrega de datos críticos del negocio en los periodos y con unas garantías determinadas.

Ventajas para las empresas: las tecnologías de QoS permiten a los administradores de red:

- Manejar las aplicaciones sensibles al jitter, como las de audio y vídeo.
- Manejar el tráfico sensible al retardo, como la voz en tiempo real.
- El control de pérdidas en los momentos en los que la congestión sea inevitable.

Ventajas para los Proveedores de Servicio: las tecnologías de QoS permiten a los proveedores de servicio ofrecer muchas más prestaciones, como el soporte del tráfico en tiempo real, o como la asignación específica de ancho de banda, que se suele especificar en los Acuerdos de Nivel de Servicio [11]

4.3.8 Aspectos generales de Seguridad

GMPLS define una nueva arquitectura del plano de control para múltiples tipos de elementos de red y dado que los caminos LSP establecidos usando GMPLS transportan altos volúmenes de datos y consumen significativos recursos de red, se requieren mecanismos de seguridad para salvaguardar la red fundamental contra ataques en el plano de control y/o el uso no autorizado de recursos de transporte de datos, por lo tanto los requerimientos de seguridad dependen del nivel de confianza entre nodos que intercambian los mensajes de control GMPLS así como de la exposición del canal de control a terceros.

En general a un nodo de red se le pueden aplicar más relajadamente los requerimientos de seguridad cuando intercambia mensajes de control GMPLS con nodos bajo el mismo dominio administrativo que cuando habla con nodos de otro dominio. A este respecto, las interfaces de red de usuario (UNI) y red a red deben tener unos mayores requerimientos de seguridad que las interfaces nodo a nodo.

Los mecanismos de seguridad pueden proporcionar dos propiedades principales: autenticación y confidencialidad. La autenticación puede proveer verificación del origen, integridad del mensaje y protección de la respuesta, mientras que la confidencialidad asegura que una tercera persona no puede descifrar el contenido de un mensaje. En situaciones donde el despliegue de GMPLS requiere primariamente autenticación, se pueden usar los respectivos mecanismos de autenticación de los protocolos de componente GMPLS. Adicionalmente, el conjunto de protocolos IPSEC se puede usar para proveer autenticación, confidencialidad o ambas, para el canal de control GMPLS; esta opción ofrece el beneficio de protección combinada de todos los protocolos de componente GMPLS.

Sin embargo el propio GMPLS no introduce nuevas consideraciones de seguridad a la señalización actual MPLS-TE (RSVP-TE, CR-LDP), protocolos de enrutamiento (OSPF-TE, IS- IS-TE) o protocolos de gestión de red.

4.4 CRITERIOS DE DISPOSITIVOS FISICOS Y MEDIO DE TRANSMISIÓN.

Es importante tener en cuenta al momento de implementar el diseño de la red algunos factores que afectan su optimo desempeño así como los diferentes dispositivos que pueden utilizarse.

4.4.1 La fibra óptica

Actualmente existen dos categorías generales de fibra óptica, la multi-modo y la mono-modo.

La multi-modo, tiene un núcleo mas grande que la mono-modo y obtiene su nombre del hecho de que modos numerosos, o rayos de luz, pueden ser simultáneamente transportados por ella.

El segundo tipo general de fibra, es la mono-modo la cual tiene un núcleo que permite un solo modo de luz a la vez. Como resultado, la fidelidad de la señal se mantiene en distancias grandes. Esta característica proporciona mas capacidad de ancho de banda que la que se logra usando fibras multi-modo. Debido a su gran capacidad para transportar información y bajas perdidas intrínsecas, las fibras mono-modo son preferidas para distancias grandes y aplicaciones de gran ancho de banda incluyendo DWDM.

La transmisión de luz en la fibra óptica presenta cambios que se resumen en las siguientes tres categorías:

4.4.1.1 Atenuación

La Atenuación en la fibra óptica es causada por factores intrínsecos, como la dispersión y absorción, y por factores extrínsecos, que incluyen inconvenientes desde el proceso de fabricación, el ambiente, y doblamiento físico. La dispersión más común, *la dispersión de Rayleig,* es causada por pequeñas variaciones en la densidad del vidrio que son más pequeñas que las longitudes de onda usadas y por consiguiente actúan como objetos de dispersión. La dispersión afecta longitudes de onda cortas y limita el uso de longitudes de onda por debajo de 800nm.

La atenuación debido a la absorción es causada por una combinación de factores, incluyendo las propiedades intrínsecas del propio material, las impurezas en el vidrio, y algunos defectos atómicos en el vidrio. Estas impurezas absorben la energía óptica, causando que la luz se empiece a disminuir. La absorción intrínseca es un problema clave en las longitudes de onda largas y se incrementa dramáticamente por encima de 1700nm.

Los factores principales que afectan la atenuación en fibras ópticas son la longitud de la fibra y la longitud de onda de la luz. La atenuación en la fibra es compensada principalmente por medio del uso de amplificadores ópticos.

4.4.1.2 Dispersión

La Dispersión es la propagación de pulsos de luz cuando viajan a través de la fibra óptica. La dispersión resulta en distorsión de la señal, la cual limita el ancho de banda de la fibra. Dos tipos generales de dispersión afectan los sistemas. Uno de estos efectos, la dispersión cromática que es lineal, mientras la dispersión de modo de polarización (PMD), es no lineal.

La dispersión cromática ocurre debido a que diferentes longitudes de onda se propagan con una velocidad diferente. Aunque la dispersión cromática no es generalmente un problema en velocidades inferiores a 2.5 Gbps, esta se incrementa con altas velocidades de bits.

4.4.1.3 Efectos No lineales

Además de PMD, hay otros efectos no lineales. Ya que los efectos no lineales tienden a manifestarse cuando la potencia óptica es muy alta, ellos se vuelven importantes.

Los efectos lineales tales como atenuación y dispersión pueden ser compensados, pero los efectos no lineales son acumulados. Ellos son el mecanismo de limitación fundamental en la cantidad de datos que pueden ser transmitidos en la fibra óptica.

Los mas importantes tipos de efectos no lineales son *dispersión Brillouin estimulada, dispersión Raman estimulada, modulación auto-fase, y mezcla de cuatro ondas.*

4.4.2 Características de las señales ópticas y desempeño

La medida básica de desempeño de transmisión de señales digitales es una cantidad cuantitativa probabilística conocida como BER. dada una muestra grande de bits recibidos, el BER da el porcentaje de bits de error.

Los siguientes fenómenos básicos afectan el BER de una señal:

-Ruido y en particular ruido por bit.

-Interferencia inter-símbolo: es la señal interfiriendo con ella misma.

-Interferencia Inter-canal: otras características interfiriendo con la señal.

-Efectos no lineales.

4.4.3 Transmisores y receptores ópticos

Los emisores y detectores de luz son dispositivos activos en extremos opuestos de un sistema de transmisión óptica. Los emisores de luz, son dispositivos de transmisión de borde que convierten señales eléctricas a pulsos de luz. Esta conversión es lograda modulando externamente una onda continua de luz basada en la señal de entrada, o usando un dispositivo que puede generar directamente luz modulada. Los detectores de luz realizan la función opuesta de emisores de luz. Ellos son dispositivos receptores de borde opto electrónicos que convierten pulsos de luz en señales eléctricas.

-Los dispositivos emisores de luz usados en la transmisión óptica son: LEDs y diodos láser o lásers semiconductores. Los LEDs son dispositivos relativamente lentos, apropiados para usos en velocidades de menos de 1 Gbps; ellos muestran un ancho espectro amplio, y transmiten luz en un cono relativamente extenso. Estos dispositivos son menos usados en comunicaciones de fibra multi-modo. Los láser semiconductores, por otro lado, tiene mejores características de funcionamiento para aplicaciones de fibra mono-modo.

Los requerimientos para lásers incluyen longitud de onda precisa, ancho espectro reducido, suficiente potencia y control de chirp[8].

-Sobre el extremo receptor, es necesario recuperar la señal transmitida en diferentes longitudes de onda sobre la fibra. Esto se hace usando un dispositivo llamado *el foto detector*. Dos tipos de foto detector son ampliamente desplegados, el fotodiodo PIN (Positivo-intrínseco-Negativo) y el fotodiodo de avalancha (APD).

El fotodiodo PIN trabaja sobre principios similares pero contrario a los LEDs. Es decir, la luz es absorbida mas que emitida, y los fotones son convertidos a electrones en una relación 1:1.

Los APDs son dispositivos similares a los fotodiodos PIN, pero proporcionan ganancia a través de un proceso de amplificación: un fotón actúa en el dispositivo descargando muchos electrones.

El fotodiodo PIN tiene muchas ventajas, incluyendo bajo costo y fiabilidad, pero los APDs tienen alta sensibilidad de recepción, exactitud, son más costosos y muy sensibles a la temperatura.

[8] **Chirp:** el cambio en frecuencia de una señal sobre el tiempo.

4.4.4 Regeneradores, repetidores y amplificadores ópticos

Las señales ópticas sufren degradación cuando atraviesan enlaces ópticos debido a dispersión, perdidas, cross talk, y no linealidad asociada con la fibra y los componentes ópticos. Los regeneradores son dispositivos que consisten de componentes ópticos y electrónicos para proporcionar las 3R, regeneración-reamplificación, remodelación y retemporización. La retemporización y remodelación detectan la señal digital que es distorsionada y ruidosa y vuelven a crearla como una señal limpia.

En la práctica, las señales pueden viajar más de 120 km entre amplificadores. En distancias más grandes de 600 a 1000 km, la señal debe ser regenerada. Esto ocurre debido a que un amplificador óptico amplifica solamente las señales y no realiza las otras funciones (remodelación y retemporización).

Los recientes avances tecnológicos en transmisión han incrementado la distancia que puede ser atravesada sin amplificadores y regeneración 3R. Debe notarse que los amplificadores son únicamente dispositivos ópticos mientras que los regeneradores requieren conversión (O/E) y conversión (E/O).

Los amplificadores ópticos (OA) posibilitan la amplificación de todas las longitudes de onda a la vez y sin conversión (OEO). Además al usarse en los enlaces ópticos, pueden también ser utilizados para aumentar la potencia de la señal después de multiplexar o antes de demultiplexar. El amplificador de fibra dopado con erbio (EDFA) es el amplificador comúnmente utilizado.

Los parámetros claves de los amplificadores ópticos son la ganancia, la igualdad de ganancia, el nivel de ruido y la potencia de salida. Sin embargo los parámetros claves cuando se selecciona un EDFA son el bajo ruido y la igualdad de ganancia.

4.4.5 Conmutadores Ópticos

Los sistemas de transmisión no son suficientes para construir una red óptica. Las señales ópticas necesitan ser multiplexadas y demultiplexadas en los puntos finales. Estas también necesitan ser clasificadas y conmutadas en los nodos intermedios.

Basados en la tecnología de fabricación del conmutador, los conmutadores ópticos pueden ser clasificados ampliamente dentro de dos categorías: opacos (OEO) y transparentes (OOO).

Los conmutadores ópticos opacos, también llamados cross-conectores u OXCs, convierten las señales ópticas recibidas en la entrada a señales

eléctricas, conmutan las señales eléctricas usando un tejido de conmutación electrónico, y finalmente convierten la señal eléctrica nuevamente en señal óptica a la salida. El nombre OEO toma la operación principal del conmutador en esencia que es convertir la señal óptica entrante en señal eléctrica y luego convertirla de nuevo en una señal óptica.

Los conmutadores transparentes, también llamados cross-conectores fotónicos o PXCs, por otra parte, no hacen la traducción óptica a eléctrica; ellos conmutan la señal óptica entrante desde el puerto de entrada al puerto de salida en forma óptica (es decir OOO). Los conmutadores transparentes operan óptimamente sobre un rango de longitudes de onda llamado pasa banda. Para cualquier estado constante, la transparencia óptica permite al dispositivo funcionar independiente del tipo (es decir análogo, digital), formato (es decir, SCM, SONET,GbE), o velocidad (es decir, 155Mbps, 10Gbps,10Ghz) de la información sobre la señal óptica que es transportada.

Uno de los problemas con los conmutadores OEO es que ellos necesitan ejecutar múltiples traducciones opto-eléctricas que pueden ser complejas y costosas. Entre los aspectos positivos la señal óptica sufre regeneración y traducción de longitud de onda como resultado de la traducción opto-eléctrica,

Los conmutadores OOO por otra parte no ejecutan traducción opto-eléctrica. Como resultado, ellos tienen el potencial de ser más económicos. Los conmutadores OOO, sin embargo son incapaces de regenerar la señal y traducir longitudes de onda. Algunos de ellos también carecen de la ejecución de monitoreo y capacidades de gestión de fallas que los conmutadores OEO ofrecen.

4.4.6 Multiplexores Add/Drop y Cross Conectores Digitales

Los cross conectores digitales, aunque no son elementos puramente ópticos juegan un importante papel en las redes ópticas de hoy. Ellos pueden operar sobre señales ópticas o señales eléctricas. Su tejido de conmutación sin embargo es puramente óptico.

Dependiendo de la granularidad[9] de conmutación, ellos pueden ser categorizados en: cross conectores banda ancha, banda extensa o ultra banda. Los cross conectores banda ancha conmutan señales en la granularidad de 1.5 Mbps (DS1) mientras los cross conectores banda extendida operan a granularidad 50 Mbps (STS-1). Ultra banda es la ultima adición para la familia de los cross conectores digitales, este tipo de cross conectores ópticos operan sobre las señales ópticas y usan un tejido de conmutación eléctrico de 2.5 Gbps (STS-48).

[9] **Granularidad:** Capacidad del Canal

Las redes ópticas de hoy también usan multiplexores add-drop (ADM). Los ADMs son típicamente adaptados en una topología de anillo conectando múltiples PoPs (puntos de presencia) de proveedores de servicio. Como el nombre sugiere, ellos son usados para tráfico add/drop para un PoP a o desde el anillo.

Los anillos ADM operan a diferentes velocidades y el tráfico puede ser added/drooped para diferentes granularidades. Actualmente existen estándares que especifican las características exactas y estructura de varias señales sobre las que los cross conectores digitales y ADMs operan. En contraste para el caso OOO donde pocos estándares aun existen.

En el anexo 3 se encuentra la validación de los criterios de diseño propuestos en este capitulo.

5. CONCLUSIONES Y RECOMENDACIONES

- En los últimos años el enrutamiento IP ha evolucionado para incluir nuevas funcionalidades desarrolladas en la arquitectura MPLS. Recientemente se ha extendido MPLS con GMPLS como un plano de control que puede utilizarse con nuevos dispositivos como los OXCs. Esta generalización proporciona el plano de control común estandarizado necesario en la evolución de redes ópticas abiertas e interoperables y simplifica las operaciones y la gestión, lo que reduce el coste de las operaciones y proporciona un amplio rango de escenarios de desarrollo.

- La Arquitectura GMPLS extiende MPLS, al incluir nuevos tipos de conmutación: división en el tiempo, longitud de onda y espacial. El principal foco de GMPLS es el plano de control de estas diversas capas de conmutación ya que cada una de ellas pueden utilizar físicamente distintos planos de datos o de envío. El desarrollo de GMPLS requiere además modificaciones de los actuales protocolos de señalización como RSVP y CRL-DP y de encaminamiento como OSPF e IS-IS con mejoras de ingeniería de tráfico. También ha disparado el desarrollo de nuevos protocolos tales como LMP para gestión de los enlaces.

- La funcionalidad proporcionada por GMPLS, su asociada noción generalizada de una jerarquía de LSPs y la agrupación crean suficiente flexibilidad para el soporte de la separación o la unificación de casi cualquier paradigma operacional deseado por un operador. Con la racionalización del soporte de la multiplexación y la conmutación en una forma jerárquica y la inteligencia flexible de la ingeniería de tráfico, el valor de la conmutación óptica GMPLS será esencial en cualquier solución que lleve a gestionar grandes volúmenes de tráfico de una forma eficiente.

- GMPLS ofrece la posibilidad de migrar las redes desde la actual arquitectura compleja y costosa a un modelo más eficiente y simple. Los proveedores de servicio quienes implementan GMPLS no solo verán ahorros significantes a través de la eficiencia de red mejorada, sino también estarán habilitados para ofrecer servicios avanzados de grandes ingresos como las OVPNs para usuarios ya existentes y nuevos.

- Un acercamiento al despliegue de las OVPNs es a través del plano de control GMPLS que gracias a sus mecanismos de control de distribución y

suministro de ancho de banda dinámico permiten la introducción del concepto de redes privadas virtuales ópticas que ahorran más eficientemente fuentes de fibra y convierten las redes tradicionales de transporte de datos hacia el servicio de redes inteligentes permitiendo que el proveedor de servicio comparta recursos, amplíe su alcance y mejore la eficiencia operacional.

- Las capacidades de restauración y protección de GMPLS permiten abordar eficientemente el funcionamiento de la red, a la vez que hace posible la introducción de nuevos servicios.

- Una red GMPLS permite gestionar tráfico a través de todas las capas de la red, asignando recursos eficientemente a la capa mas apropiada, por consiguiente se crean servicios diferenciados y se suplen necesidades, mientras se reducen costos a través del uso optimo de recursos. GMPLS además habilita a proveedores de servicio para acumular grandes beneficios a través de acuerdos de nivel de servicio más flexibles y extensos ofrecidos a los usuarios. Con asignación de recursos ya no restringidos para una capa de red especifica, los proveedores de servicio tienen gran flexibilidad en designar y reforzar SLAs, los cuales pueden ser usados para generar nuevos ingresos.

- Aplicar calidad de servicio en una red cuantifica el tratamiento que el tráfico debe esperar a medida que circula por ella, cumpliendo además con requerimientos de ciertos parámetros relevantes para el usuario final estipulados en los acuerdos de nivel de servicios asegurando una entrega de la información necesaria o crítica, permitiendo que el rendimiento de la red sea más predecible y la utilización de ancho de banda más eficiente.

- La diferenciación de servicios permite la priorización de determinado tipo de tráfico y la agrupación de flujos de datos en grandes agregados de tráfico de acuerdo a la clase de servicio a la que pertenezcan, lo que representa para la red que los enrutadores operen más rápido al reducir la carga de estos dispositivos ya que se limita la complejidad de la clasificación y el encolado, además se minimiza el tráfico de señalización y el almacenamiento.

- La falta de suficiente QoS y provisión de adecuada capacidad de transmisión para servicios de gran ancho de banda en tiempo real son desventajas actuales de las VPNs que llevan a pensar en las OVPNs que soportan GMPLS como una solución para soportar servicios multimedia en tiempo real con garantía de QoS, y en la diferenciación de servicios como un esquema para desplegar dicha calidad de servicio.

- Las clases de diferenciación de calidad de servicio óptica (DOQoS) son consideradas para soportar servicios en tiempo real que son sensibles al retraso y requirieren gran ancho de banda en una OVPN que soporta GMPLS. La implementación de una longitud de onda efectiva para esta

red usa mecanismos en la interfaz E-O/O-E y el servidor de política de tráfico QoS junto con el Agente Gestor de Recurso Óptico (ORMA) de la OVPN para establecer un O-LSP que permita soportar DOQoS y analizar fallas de calidad de servicio o de red causadas por ataques y un esquema de mantenimiento QoS se puede sugerir para cada clase DOQoS.

En cuanto a recomendaciones se pueden sugerir las siguientes:

- Es recomendable el estudio de ASON (Red óptica de Conmutación Automática) que es una arquitectura que define los componentes en un plano de control óptico y las interacciones entre estos. Por ser ASON un concepto complementario de GMPLS se puede analizar cómo sería la integración de estos dos conceptos dentro de las redes de próxima generación.

- También se recomienda para estudios posteriores la Ingeniería de Tráfico (TE) como otra forma de implementar calidad de servicio en una red óptica que soporta GMPLS ya que por ser un tema tan importante y amplio se puede sugerir para el desarrollo de otro trabajo de grado.

GLOSARIO

ADM	Add Drop Multiplexer, Multiplexor de inserción de extracción
AF	Assured Forwarding, Envío Seguro
APD	Avalanche Photodiode, Fotodiodo de avalancha
AS	Assured Service, Servicio Seguro
ASE	Amplified Spontaneous Emisión, Amplificador de Emisión Espontánea
ASON	Automatic Switched Optical Network, Red Óptica Conmutada Automática
ATM	Asynchronous Transport Network, Red de Transporte Asíncrona
BA	Behavior Agregate, Agregado de tráfico
BER	Bit Error Rate, Tasa de Error de Bit
BGP	Border Gateway Protocol, Protocolo de Borde de Pasarela
BLSR	Bidirectional Line Switched Ring, Anillo Conmutado de línea Bidireccional
CAC	Control de admisión de llamada, Call Admisión Control
CE	Edge Client, Cliente de borde
CGU	Closed User Group, Grupo de Usuarios Cerrados
CoS	Class of Service, Clase de Servicio
CPI	Customer Port Identifier, identificador de Puerto Cliente,
CR-LDP	Constraint-based Routing-Label Distribution Protocol, Protocolo de Distribución de Etiquetas basado en Enrutamiento por Restricción
CSPF	Constraint-based Shortest Path First, Primero el camino más corto basado en restricciones
Diffserv	Differenciated Services, Servicios diferenciados
DOQoS	Differentiated Optical Quality of Service, Calidad de Servicio Óptica Diferenciada
DS	Differetiated Services, Servicios Diferenciados
DSCP	Differentiated Service Code Point, Punto de código de servicios Diferenciados
DWDM	Dense Wavelength Division Multiplexing, Multiplexación por División de Longitud de Onda Densa
EBGP	External Border Gateway Protocol, Protocolo de Borde de Pasarela Externo
EDFAs	Erbium Doped Fiber Amplifiers, Amplificadores de Fibra Dopados con Erbio
EF	Expedited Forwarding, Envío Apresurado
el.SNR	Electrical signal-to-Noise, Relación señal a ruido eléctrico
E-O-E	Electronic-Optic-Electronic, Electrónico-Óptico-Electrónico
ERO	Explicit Route Object, Objeto de ruta Explicita
FA	Forwarding Adjacency, Adyacencia de Envío
FEC	Forwarding Equivalency Class, Clase de Equivalencia de Envió
FSC	Fiber-Switch Capable, Capacidad de Conmutar Fibra

GMPLS	Generalized Multi-Protocol Label Switching, Multiprotocolo de Conmutación de Etiquetas Generalizado
IBGP	Internal Border Gateway Protocol, Protocolo de Borde de Pasarela Interno
IETF	Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet
IGP	Inter-Gateway Protocol, protocolo Interno de Pasarela
IP	Internet Protocol, Protocolo de Internet
IPSec	Internet Protocolo Security, Protocolo de Seguridad IP
IS-IS	Intermediate System to Intermediate System, Sistema Intermedio a Sistema Intermedio
IS-IS-TE	Intermediate System to Intermediate System- Traffic Engineering Extensión, Sistema Intermedio a Sistema Intermedio-Extensiones de Ingeniería de Tráfico
ISP	Internet Service Provider, Proveedor de Servicio de Internet
LMP	Link Management Protocol, Protocolo de Gestión de Enlace
LOL	Loss of light, pérdida de luz
LPT	Link Protection Type, Tipo de protección de enlace
L2SC	Layer2 Switching Capable, Capacidad de Conmutación de Capa 2
LS	Label Set, Conjunto de Etiquetas
LSBD	Link status database, Base de Datos de estado de enlace
LSC	Lambda Switch Capable, Capacidad de Conmutación De Longitud de Onda
LSP	Label Switched Path, Camino de Conmutación de Etiqueta
LSR	Label Switching Router, Enrutador de Conmutación de Etiquetas
MAC	Control de Acceso al Medio, Medium Access Control
MF	Multi-Field, Multi-Campo
MP-BGP	Multiprotocol Extensions –BGP, Extensiones Multiprotocolo-BGP
MPLS	Multi-Protocol Label Switching, Multiprotocolo de Conmutación de Etiquetas
NGOI	Next generation Optical Internet, Internet Óptico de Nueva Generación
OA	Amplificadores ópticos
OADM	Optical Add-Drop Multiplexer, Multiplexor Add/Drop Óptico
OCh	Optical Channel, Canal Óptico
O-E-O	Optic-Electronic-Optic, Óptico- Eléctrónico-Óptico
O-LSP	Óptical Label Switched Path, Camino de Conmutación de etiquetas Óptico
ONEs	Óptical Network Elements, Elementos de red Óptica
OVPN	Optical Virual Private Network, Red Privada Virtual Óptica
ORMA	Optical Resource management Agent, Agente Gestor de Recurso Óptico.
OSNR	Óptical Signal to noise, Relación señal a ruido óptica
OSPF	Open Shortest Path First, Primero el camino más corto abierto.
OSPF-TE	Open Shortest Path First-Traffic Engineering Extension, Primero el camino más corto abierto-Extensión de Ingeniería de tráfico.
OXC	Optical Cross-Connect, Cross conector Óptico
OTU	Optical Transport Unit, Unidad de transporte Óptica

PC	Permanent connection, Conexión Permanente
PE	Provider Edge, Proveedor de Borde
PE ONEs	Provider Edge- Optical Network Elements, Elementos de red Óptica de proveedor de borde.
PHB	Per Hop Behavior, Comportamiento por Salto
PIN	Positive-Intrinsic-Negative, Positivo Intrínsico Negativo
PIT	Port Information Table, Tabla de Información de Puertos
PMD	Polarization Mode Dispersión, Dispersión de modo de polarización
PMM	Power Monitoring Module , Modulo de Monitoreo de Potencia
P ONEs	Provider - Optical Network Elements , Elementos de red óptica de Proveedor.
PoP	Points of presence, Puntos de Presencia
PPI	Provider Port Identifier, identificador de puerto de proveedor
PSC	Packet Switching Capable, Capacidad de Conmutación de Paquetes
PXCs	Photonic Cross Connect, Cross conector fotónico
QoS	Quality of Service, Calidad de Servicio
QoS-TP	Quality of Service-traffic Policy, Calidad de Servicio-Política de Tráfico
RD	Routing Domain, Dominio de Enrutamiento
RIN	Ruido de Intensidad Relativa, Relative Intensity Noise
RGT	Requested Grouping Type, Petición de Tipo de Agrupación
RNC	Requested Number of Components, Petición de número de componentes
RRO	Record Route Object, El Objeto de Ruta de Registro
RSVP	Resource Reservation Protocol, Protocolo de reserva de recursos
RSVP-TE	Resource Reservation Protocol-Traffic Engineering Extension, Protocolo de reserva de recursos-Extensiones de ingeniería de tráfico
RWA	Routing and Wavelength Assignment, Asignación y Enrutamiento de longitud de Onda
SA	Autonomous System, Sistema autónomo
SC	Switched Connection, Conexión Conmutada
SDH	Synchronous Digital Hierarchy, Jerarquía Digital Síncrona
SLA	Service Level Agreement, Acuerdo de nivel de servicio
SLS	Service Level Specification, Especificación de Nivel de Servicio
SONET	Synchronous Optical Network, Red Óptica Sincronica
SPC	Soft permanent logical connection, Conexión lógica permanente suave
SPF	Shortest Path First, Primero el camino más Corto
STM	Synchronous Transport Module, Modulo de Transporte Sincrono
STS	Synchronous Transport Signal, Señal de Transporte Sincrono
TC	Traffic Conformation, Conformación de Tráfico
TCA	Traffic Conditioning Agreement, Acuerdo de Condicionamiento de Tráfico
TCP	Transmission Control Protocol, Protocolo de Control de Transmisión
TDM	Time Division Multiplexing, Multiplexación por División de Tiempo
TE	Traffic Engineering, Ingeniería de Tráfico
TLV	Type-Length-Value, Tipo-Longitud-Valor

ToS	Type of Service, Tipo de Servicio
UNI	User Network Interface, Interfaz de red de usuario
UDP	User Datagram Protocol, Protocolo de Datagrama de Usuario
UPSR	Unidirectional Path Switched Ring, Anillo Conmutado de Camino Unidireccional
VC	Virtual Container, Contenedores Virtuales
VCI	Virtual Channel Identifier, Identificador de canal virtual
VPI	Virtual Path Identifier, Identificador de trayecto virtual
VPLG	Virtual Private Link Group, Grupo de Enlace Privado Virtual
VPN	Virtual Private Network, Red privada Virtual
WDM	Wavelength Division Multiplexing, Multiplexación por división de longitud de Onda.

REFERENCIAS ESPECÍFICAS

[1] IETF Draft recommendation,"GMPLS–Generalized Multiprotocol Label Switching Arquitecture",febrero de 2003.

[2] IETF RFC 3031 recommendation,"MPLS–Multiprotocol Label Switching Arquitecture",enero de 2001.

[3] IETF RFC 3073 recommendation," Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions",enero de 2003.

[4] IETF Draft recommendation, "OSPF Extensions in Support of Generalized Multi-protocol Label Switching".

[5] ITU-T draft recommendation, "L1VPN network and service architectures". Julio, 2003.

[6] H. Ould-Brahim et al., "Service Requirements for Optical Virtual Private Networks", Internet Draft, Diciembre 2002.

[7] RFC2858, "Multiprotocol Extensions for BGP-4."

[8] "BGP Extended Communities Attribute", Internet draft, draft-ietf-idr-bgp-ext-communities-08.txt, Feb. 2005.

[9] Rec. G.976, Test methods aplicable to optical fiber submarine cable systems, COM 15R68 (TSB, 7 Nov. 1996), Sect. 7.6.1.1: Measurement of Q-factor. pp. 172-174 and Annex A.4: "Q-factor" p.17.

[10] G. Bendelli, et al., Optical performance monitoring techniques, ECOC 2000 (Munich, Germany, Sept. 2000), paper 11.4.1, pp. 113-1168.

[11] Pérez, Jairo Daniel. Calidad de Servicio en Redes (QoS). EAFIT 2003

BIBLIOGRAFÍA GENERAL

ÁLVAREZ, Sebastián Andrés; GONZÁLEZ, Agustín José. estudio y configuración de calidad de servicio para protocolos ipv4 e ipv6 en una red de fibra óptica wdm. Universidad Técnica Federico Santa María. España.

BANERJEE, Ayan; DRAKE, John; LANG, Jonathan P; TURNER, Brad. Generalizad Multiprotocolo Label Switching: Una Visión de las Mejoras de encaminamiento y Gestión.2001

BART, Rousseau; DIMITRI, Papadimitriou. Demystifying GMPLS, A technical perspective. White Paper, Alcatel.

BART, Rousseau; DIMITRI, Papadimitriou. Generalized Multi-Protocol Label Switching The telecommunications holy grail or a pragmatic means of raising carrier profitability? . White Paper, Alcatel.

BATTITI, Roberto; SALVADORI, Elio. Quality of Service in IP over WDM: considering both service differentiation and transmission quality. Universit`a di Trento, Dipartimento di Informatica e Telecomunicación

CALLE, Eusebi; MARZO, Jose L; VILÀ, Pere. QoS protection: Formulation and experimental analysis of the MPLS case. Universidad de Girona, España

CALLE, Eusebi. Enhanced fault recovery methods for protected traffic services in GMPLS networks. February 2004.

CHAE, C.J.; TUCKER R.S; Implementation of Multiple Optical Viertual Private Networks over WDM passive Optical Network.

Draft-ietf-idr-bgp-ext-communities-09.txt. BGP Extended Communities Attribute.

Draft-oulbraim-ovpn-requirementa-01.txt, Service Requirements for Optical Virtual Private Networks.

Draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-06.txt. GVPN Services: Generalized VPN Services using BGP and GMPLS Toolkit. Febrero 2005

Dynamic Switched Optical Services-An introduction.White Paper.Nortel Networks

FUENMAYOR T, Carlos J. Conmutación por etiquetas Multiprotocolo generalizada en redes optica. 2002

Generalized MultiProtocol Label Switching (GMPLS). Web ProForum Tutorials. IEC

GAO, Donghui; ZHOU, Zhiyu. An efficient Adaptation of RSVP-TE in GMPLS.

GOLMIE, Nada; NDOUSSE, Thomas D; SU, David H. A Differentiated Optical Services Model for WDM Networks. National Institute of Standards and Technology.

GU, Wanyi; GUI, Xuan; SONG, Hongsheng; XU, Yunbin; ZHANG, Jie. Análisis and design of optical virtual private networks (OVPN) over ASON. Optical Communication Center of Beijing University of Posts and Telecommunications.

JIAO, Yueguang; LI, Yanhe; REN, Jian; XU, Zhengchum; ZHANG Hanyi; ZHENG Xiaoping; ZHU Jia. GMPLS- based dynamic OVPN technique in ASON. Department of Electronic Engineering, Tsinghua University, Beijing, China.

JUE, Jason P; LU, Kejie; ZHANG, Tao. Differentiated Contention Resolution for QoS in Photonic Packet-Switched Networks. Journal of lightwave technology, VOL. 22, NO. 11, NOVEMBER 2004.

LIN, Jintong; WU, Jean. Performance evaluation of dynamic OVPN in OBS Architecture from prospective view of ASON.

MOUNGLA, Hassine; KRIEF, Francine. Service Differentiation over GMPLS. LIPN Laboratory. Paris

OULD-BRAHIM, Hamid. Optical VPNs. Nortel Networks

RFC 3471. Network Working group.

RFC 2858. Multiprotocol Extensions for BGP-4 **.** Network Working group

YUN, Ana. GMPLS MλPLS. Temas Avanzados de Redes de Ordenadores. Notas de clase. 2001

Enlaces Web:

www.juniper.net
www.dataconnection.com
www.lucent.com
www.nortel.com
www.cisco.com
www.alcatel.com
www.iec.org
www.ietf.org
www.nwfusion.com/news/tech/2003/0428techupdate.html
www.convergedigest.com/tutorials/mpls6/page1
www.qoptics.com/index.php?fuseaction=products.overview&page_id=17
www.lightmaze.com/HTML/en/e_services3.htm
www.javvin.com/protocolMBGP.html