ANEXO 1

EL PROTOCOLO DE RESERVACIÓN DE RECURSOS (RSVP) Y EL PROTOCOLO DE GESTIÓN DEL ENLACE (LMP) EN GMPLS

DIANA MARÍA PABÓN MENDOZA
ALEXANDRA SÁNCHEZ DAZA

Director:
Jose Giovanny López Preafán
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

1. EL PROTOCOLO DE RESERVACIÓN DE RECURSOS (RSVP) Y EL PROTOCOLO DE GESTIÓN DEL ENLACE (LMP) EN GMPLS

GMPLS se enfoca en el plano de control óptico que está constituido por dos familias de protocolos los de señalización (RSVP Y CR-LDP) y los de enrutamiento (OSPF e IS-IS) con extensiones de ingeniería de trafico, además de un protocolo especializado para soportar las operaciones GMPLS conocido como LMP. Para entender la señalización basada en GMPLS, es importante mirar uno de estos protocolos de señalización y ya que GMPLS no detalla cual se debe usar y deja a los fabricantes y operadores evaluar para cada caso una posible solución, este documento se enfoca en el protocolo RSVP-TE debido a que es más popular que CR-LDP aunque los dos proporcionan una funcionalidad idéntica.

En este anexo se resumen las extensiones de GMPLS a RSVP-TE pasando primero por detalles básicos de RSVP y RSVP-TE, ya que GMPLS utiliza los mensajes definidos bajo el protocolo RSVP-TE, en cuanto a la petición de las etiquetas y respuestas, pero agrega nuevos elementos de información llamados *objetos* a estos mensajes junto con otras reglas de proceso correspondientes. Además se amplia la funcionalidad del protocolo LMP por su importancia en la gestión de enlaces con Ingeniería de Trafico y su aplicabilidad en GMPLS, teniendo en cuenta que LMP en este contexto, se define independientemente de la especificación de señalización de GMPLS, ya que es un protocolo local que funciona entre nodos adyacentes del plano de datos y se puede usar en otros contextos con protocolos de señalización que no son parte de GMPLS.

1.1 EL PROTOCOLO DE RESERVACIÓN DE RECURSOS (RESOURCE RESERVATION PROTOCOL, RSVP)

Usando RSVP una fuente IP Host (emisora) envía un mensaje para un destino unicast o multicast IP indicando las características del tráfico que este genera y este mensaje es procesado por los enrutadores a través del camino de la fuente a los destinos (receptores). Estos enrutadores toman nota del camino en sentido contrario al emisor y basándose en las características de tráfico recibidas, cada uno de los receptores formula una petición de reservación y transmite al emisor esta petición cruzando el camino en sentido contrario mantenido por los enrutadores de la red.

Cada enrutador reúne los métodos de procesos de la petición de reservación y asignación de recursos locales sobre el enlace que se dirige hacia el receptor, entonces la reservación de recursos unidireccional, desde el emisor a los receptores, es establecida en la red.

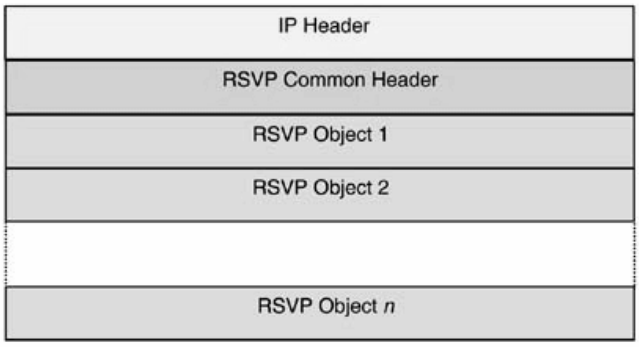
RSVP esta diseñado para soportar tráfico multicast y punto a punto, para propósito de ingeniería de tráfico se ha enfocado solo sobre la aplicación punto a punto. Así en este anexo la discusión se limita al caso solo punto a punto.

1.1.1 Mensajes y objetos rsvp

RSVP define siete mensajes: Path, Resv (reserva), PathErr (Path Error), ResvErr (Error de Reserva), PathTear, ResvTear, ResvConf (reserve Confirm).

Los mensajes Path y Resv son usados para establecimiento de reservaciones para una sesión. Los mensajes PathTear y ResvTear son usados para borrar el estado de sesión y la reservación. PathErr y ResvErr son mensajes de notificación de error. Finalmente, ResvConf es enviado a un receptor para confirmar una reservación.

En la figura 1 se ilustra el formato de los mensajes RSVP y los objetos que llevan estos mensajes, el valor en el campo *Tipo de Mensaje* de la cabecera común RSVP corresponde al número indicado arriba por cada mensaje. Los objetos son codificados en una forma jerárquica; el número de clase identifica una amplia clase de objetos similares y el *Tipo de Clase* identifica un objeto específico dentro de la clase. El campo *Checksum* en la cabecera cubre el mensaje RSVP completo, y el campo *SEND_TTL* contiene el valor tiempo de vida IP con el cual el mensaje será enviado.



Format of RSVP Messages

Version (4-bits)	Flags (4-bits)	Message Type (8-bits)	RSVP Checksum (16-bits)
SEND_TTL (8-bits)		Reserved (8-bits)	RSVP Message Length (16-bits)

Format of RSVP Common Header

Length (16-bits)	Class Number (C-num, 8-bits)	Class Type (C-type, 8-bits)
Object Contents (Variable)		

Format of RSVP Objects

Figura 1. Formato de objetos y mensajes RSVP

1.1.1.1 Sesión

Una sesión es un identificador de un flujo de tráfico y bajo RSVP, las reservaciones son hechas en una sesión base. La identificación (ID) de la sesión consiste en la dirección IP del receptor, la ID protocolar, y el puerto. Esto se lleva como un "*objeto de sesión*" en los mensajes RSVP y el formato de este objeto, para un destino IPv4, se muestra en Figura 2. La identidad del emisor no es parte de la identificación de la sesión.

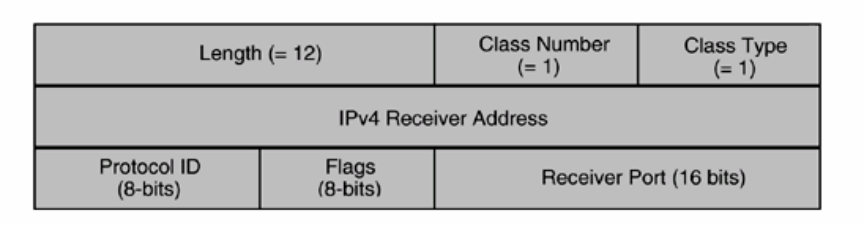


Figura 2. El formato del Objeto De Sesión RSVP

1.1.1.2 Plantilla del emisor

La plantilla del emisor identifica el emisor de un flujo. El formato de este objeto, para un emisor con una dirección IPV4, se muestra en Figura 3. El nombre de "plantilla" se debe a que el mismo formato se usa como un filtro para seleccionar esos paquetes que reciben el tratamiento de calidad de servicio.

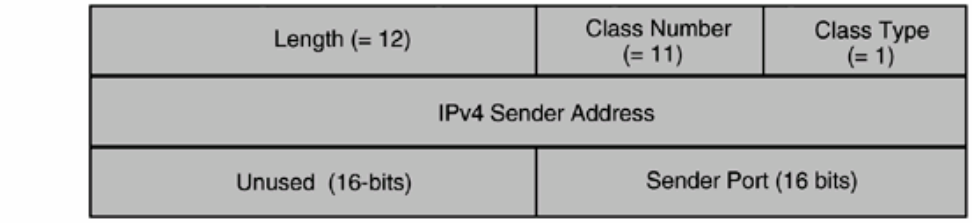


Figure 3. El formato del objeto RSVP Plantilla del Emisor

1.1.1.3 El Tspec del Emisor

El Tspec indica las características del flujo de tráfico generado por un emisor, el propio RSVP no interpreta o usa este objeto, solo lleva este objeto opacamente. La IETF ha definido los parámetros de *Tspec* para las diferentes clases de servicio a ser usadas con RSVP, *el Tspec* se lleva desde el emisor a los enrutadores intermedios, y finalmente al receptor.

1.1.1.4 Flowspec

El Flowspec describe la petición de la reservación. Esto se lleva en los mensajes *Resv,* del receptor hacia el emisor. Los enrutadores intermedios usan *el flowspec* para hacer la reservación y como en el caso del *Tspec*, RSVP no interpreta o usa este objeto, pero lo entrega a varios nodos.

1.1.1.5 Filterspec

El Filterspec describe los paquetes que están recibiendo el tratamiento de calidad de servicio en cada nodo a lo largo del camino del emisor al receptor en una sesión dada. *El Filterspec* se usa para instalar el clasificador del paquete en cada nodo y el formato del *objeto Filterspec* es el mismo que el de la *Plantilla del emisor*.

Además de estos objetos, RSVP define varios "estilos de reservación." Un estilo de reservación indica si la reservación es dedicada a un flujo de un solo emisor al receptor, o es compartida entre los flujos múltiples de los emisores posiblemente diferentes al mismo receptor. La aplicación típica en Ingeniería de tráfico usa la reservación dedicada para los flujos de tráfico de una sola fuente a un destino dado.

1.1.2 Estableciendo una reservación: path y resv

La manera en la cual una reservación se establece para una sesión que usa RSVP se muestra en la figura 4. Donde el mensaje *Path* se origina por el host emisor. Como se muestra en la Figura 5, el mensaje *Path* contiene la identidad del receptor (Sesión), la identidad del emisor (la Plantilla del emisor), y las características de tráfico (Tspec del emisor). Los mensajes RSVP se llevan directamente en los paquetes IP y el paquete IP que lleva el mensaje *Path* se dirige directamente al receptor.

Cada enrutador intermedio que recibe el paquete crea el estado *Path* para la sesión en una base de datos local, antes de remitir el paquete al próximo salto. El Estado del *Path* consiste en *la Plantilla del emisor* recibida, *el Tspec del emisor*, e información de la Sesión, junto con la identidad del salto siguiente/anterior hacia la fuente. Esta información del salto anterior se recibe en el objeto *Hop RSVP*. Este objeto, como se muestra en Figura 6, tiene dos campos: la dirección IP del enrutador anterior que remitió el mensaje *Path,* y la ID de la interfaz saliente (*Manejo de Interfaz Lógica*, LIH) a ese enrutador. Cada enrutador que remite el mensaje *Path* debe reemplazar el *objeto Hop RSVP* recibido con uno nuevo que contiene su propia dirección IP y la identidad de la interfaz sobre el cual el paquete se remite. El mensaje finalmente localiza al receptor que también debe crear el estado *Path* local.

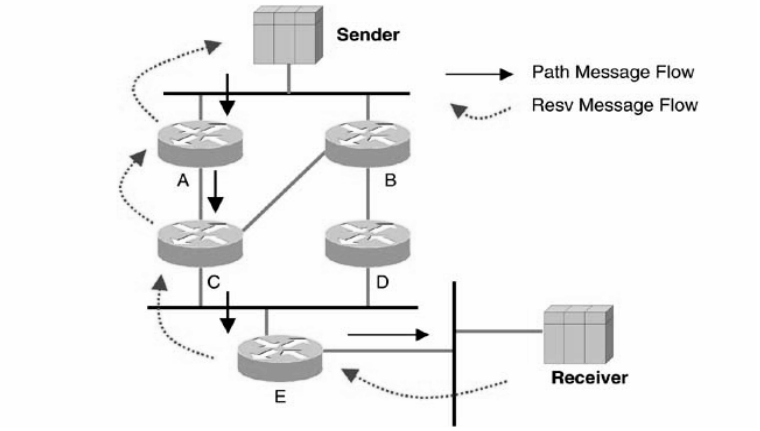


Figure 4. Flujos de Mensaje RSVP para el Establecimiento de la Reservación.

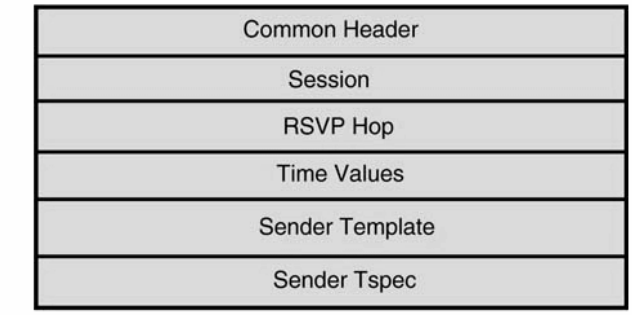


Figure 5. Los Contenidos del Mensaje Path

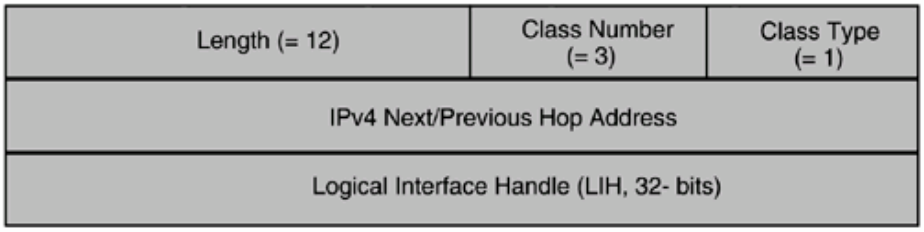


Figure 6. El formato del Objeto Hop RSVP

El receptor utiliza la información del *Tspec* en el mensaje *Path* para formular una petición de reservación. Entonces envía un mensaje *Resv* para el anterior salto en el camino. Las direcciones IP y la información *LIH* recogida del objeto *Hop RSVP* en el mensaje *Path* le permite al receptor determinar qué interfaz local debe usarse para enviar el mensaje *Resv* y a cual próximo nodo debe dirigirse el paquete IP que lleva el mensaje Resv.

El mensaje *Resv* no puede dirigirse directamente al emisor como el mensaje *Path* se dirigió al receptor porque en las redes IP, la ruta del emisor al receptor no puede ser igual que la ruta del receptor al emisor. Desde que la reservación sea unidireccional del emisor al receptor, es necesario para los mensajes *Resv* progresar a lo largo del mismo camino del mensaje *Path* en dirección contraria. Así, el mensaje *Resv* se envía salto por salto del receptor al emisor que usa la información del salto anterior guardada en cada nodo intermedio.

Los contenidos del mensaje *Resv* se muestran en la Figura 7. Este mensaje tiene *la Sesión*, *el Estilo de la Reservación*, *el Filterspec*, y *los objetos de Flowspec*, adicionalmente, *el objeto Hop RSVP* se usa para indicar el nodo que envió el mensaje. Un enrutador que recibe el mensaje crea el estado local *Resv*, es decir, nombra el flujo recibido e información de *Filterspec*, junto con la información *Hop RSVP* y *el Flowspec* configura el planificador del paquete local que corresponde al enlace saliente apropiado, y el *Filterspec* configura el clasificador del paquete para ejecutar la reservación para la sesión indicada. El enrutador entonces envía el mensaje *Resv* al nodo anterior en el camino del emisor, después de reemplazar el objeto *Hop RSVP*

con su propia información y el mensaje *Resv* finalmente alcanza el emisor, que también debe hacer la reservación del recurso local para el flujo.

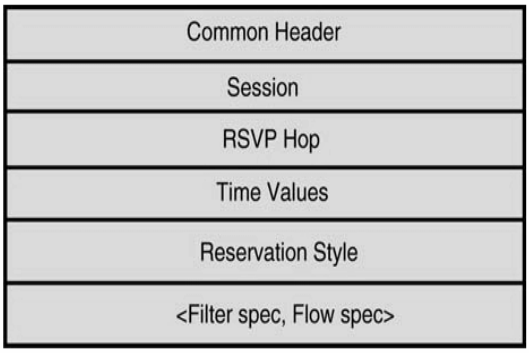


Figura 7 Contenidos del mensaje Resv

Una vez la reservación se ha establecido, los paquetes de los datos pueden fluir del emisor al receptor y si se ha configurado el clasificador del paquete y planificador adecuadamente en el plano de datos, el flujo de tráfico recibe el tratamiento apropiado. El mensaje *Path* y los paquetes de datos que constituyen el flujo de tráfico, se enrutan a lo largo de un camino determinado por el enrutamiento normal de IP basado en el destino, pero el enrutamiento IP es dinámico y una falla en la red puede generar nuevas entradas de tablas de enrutamiento que corresponden a la dirección del receptor, si esto ocurre, los paquetes de datos subsecuentes del emisor serán enrutados sobre un nuevo camino que no tiene los recursos reservados.

1.1.3 El acercamiento al estado suave

En las redes tradicionales orientadas a la conexión, una ruptura en el camino de conexión produciría el restablecimiento de la conexión a lo largo de un nuevo camino antes de que los datos continúen fluyendo. Un ejemplo es la red telefónica. Este acercamiento hace referencia al estado duro aproximado, es decir, al establecimiento y mantenimiento de una conexión explícita. Éste también es el acercamiento seguido en las redes ópticas.

RSVP, sin embargo, sigue el acercamiento al estado suave, bajo este método, no se transmiten mensajes *Resv y Path* fiablemente, es decir, no hay ningún mensaje de reconocimiento cuando un nodo envía un mensaje *Resv o Path* a otro, en cambio, los mensajes *Resv y Path* son regenerados periódicamente por cada nodo con los estados *Resv y Path* "activo", respectivamente. Esto hace referencia a actualizar (refrescar) el estado, y los mensajes regenerados se llaman mensajes de *refresh*. El estado en un nodo es considerado activo si se ha refrescado recientemente y un mensaje Path así generado es idéntico al mensaje Path original, excepto que se remite al destino que usa la información de enrutamiento IP actualmente disponible.

El mensaje de *refresh Resv* es idéntico a uno originalmente generado por el nodo, y se remite al nodo anterior según la información *RSVP Hop* contenida en el estado *Path* correspondiente. Un nodo anula su estado *Path o Resv* si

no recibe un *refresh* de mensaje *Resv o Path*, respectivamente, desde el par RSVP apropiado. Cuando el estado del *Path* se anula, el estado de *Resv* asociado también se anula, y un mensaje *PathTear* se genera. Cuando el estado de *Resv* se anula, el estado *Path* correspondiente no se anula. Un mensaje de *ResvTear*, sin embargo, se genera. Si la ruta cambia, el próximo mensaje *Path* de *refresh* seguiría la nueva ruta y establecerá el nuevo estado del *Path* y el correspondiente estado *Resv*.

El campo *valores de tiempo* en los mensajes *Resv y Path* (Figura 6 y 7) indica el período de tiempo de refresh que se usará por el emisor del mensaje. Esto le permite al receptor del mensaje poner el período de espera para quitar el estado *Resv o Path*. El período de tiempo de refresh se especifica en milisegundos con un número de 32-bit.

1.1.4 Borrar una reservación: pathtear y resvtear

Una reservación a un nodo puede anularse en una de las dos formas siguientes: implícitamente cuando el estado *Path o Resv* se cronometra en tiempo de espera, o explícitamente cuando un mensaje *PathTear* o *ResvTear* se recibe. Un Emisor (o un enrutador intermedio) puede generar un mensaje *PathTear* figura 9 para anular el estado del Path de una sesión. Cuando el estado del *Path* es eliminado en un nodo, el estado de *Resv* también es eliminado y el mensaje de *PathTear*, como el mensaje *Path*, se dirige al receptor del flujo de datos. Un enrutador intermedio que recibe el mensaje de *PathTear* quita el estado *Resv y Path* local (sin embargo, no genera un *ResvTear*). Un mensaje de *PathTear* no se transmite fiablemente y si el mensaje se pierde, el próximo nodo del salto propuesto eventualmente en el tiempo de espera anula sus estados de *Path y Resv*.

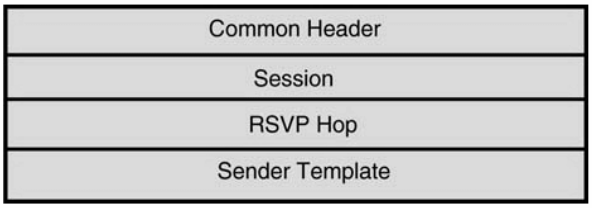


Figura 9. Los Contenidos del Mensaje PathTear

El receptor (o un enrutador intermedio) puede generar un *ResvTear* (Figura 10) para quitar la reservación que corresponde a una sesión. *El ResvTear*, como los mensajes de *Resv*, se transmite salto por salto. La recepción de un *ResvTear* por un nodo produce el levantamiento de sólo el estado *Resv* para la sesión. El estado del *Path* se mantiene y el mensaje de *PathTear, ResvTear* no se transmite fiablemente.

Figure 10. Los Contenidos del Mensaje ResvTear

1.1.5 Errores de resv y path, y confirmación de reservación

Los mensajes *PathErr y ResvErr* se usan para indicar las condiciones del error. El mensaje *PathErr* se envía de un enrutador intermedio al emisor que usa la información del salto anterior, otros nodos en ruta no cambian su estado de *Path* basado en este. El *ResvErr* se envía de un enrutador intermedio al receptor, los nodos en ruta pueden cambiar su estado *Resv* basado en este. Los mensajes *PathErr y ResvErr* contienen los códigos de error que indican el problema.

El mensaje de *ResvConf* se envía del emisor o un enrutador intermedio al receptor para confirmar el establecimiento de la reservación.

Aunque la descripción se ha enfocado hasta ahora en el emisor y el receptor siendo los hosts, es posible que el emisor y receptor sean enrutadores.

1.2 RSVP-TE (PROTOCOLO DE RESERVACIÓN DE RECURSOS CON EXTENSIONES DE INGENIERIA DE TRAFICO

RSVP fue diseñado para ser un protocolo que reserve los recursos a lo largo de un camino preexistente. Con la llegada de la ingeniería de tráfico basada en MPLS, existía el deseo de reusar las aplicaciones de RSVP disponibles para apoyar la creación, mantenimiento, y eliminación de LSPs. El resultado fue RSVP con extensiones de ingeniería de tráfico (RSVP-TE).

Los rasgos importantes de RSVP-TE son:

-El uso de mensajes *Path y Resv* para pedir y asignar las etiquetas para el establecimiento de LSP.

-La habilidad de especificar una ruta explícita al establecer o redireccionar un LSP.

-La habilidad de especificar ancho de banda y otros parámetros al establecer un LSP.

-La habilidad de asociar LSPs relacionados.

-Un nuevo protocolo *Hello* para mantener la adyacencia entre los pares de RSVP.

La especificación de RSVP-TE usa el término "Tunel LSP" para denotar los LSPs punto a punto con o sin los parámetros de calidad de servicio asociados y se introducen varios nuevos objetos en RSVP-TE para apoyar los rasgos anteriores.

1.2.1 Objetos de RSVP-TE

Los objetos de RSVP-TE son los siguientes: petición de etiqueta, etiqueta, ruta explícita, ruta de Registro, identificación en la sesión del túnel LSP, plantilla del emisor, objetos de Filterspec y atributos de sesión.

1.2.1.1 La petición de la etiqueta

El objeto de petición de Etiqueta se lleva en el mensaje *Path*. Se usa por un nodo ascendente para solicitar una etiqueta desde el vecino descendente para el establecimiento del túnel LSP. Bajo RSVP-TE, pueden pedirse tres tipos de etiquetas dentro de un rango específico: la etiqueta MPLS, ATM o una etiqueta Frame Relay. La Figura 11 ilustra el objeto de petición de Etiqueta que corresponde a la etiqueta MPLS. Aquí, el campo L3-PID indica el tipo de unidades de datos de protocolos capa 3 (por ejemplo, IP) eso se llevará por el LSP.

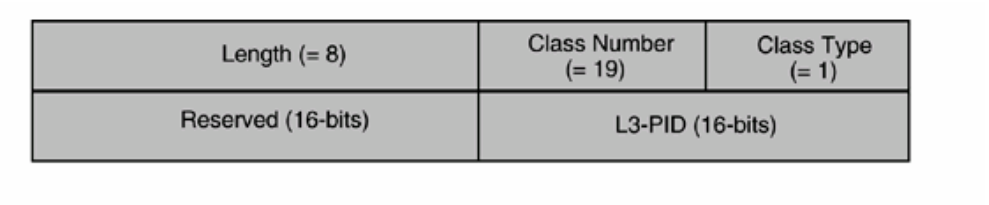


Figure 11. El formato del Objeto de Petición de Etiqueta

1.2.1.2 La etiqueta

El objeto de Etiqueta se lleva en los mensajes *Resv* ascendentes. Este objeto indica la etiqueta que se ha asignado por el vecino descendente en respuesta a una petición de la etiqueta recibida en el mensaje *Path*. El formato del objeto Etiqueta se muestra en Figura 12.

Figure 12. El formato del Objeto de Etiqueta

1.2.1.3 Ruta explícita

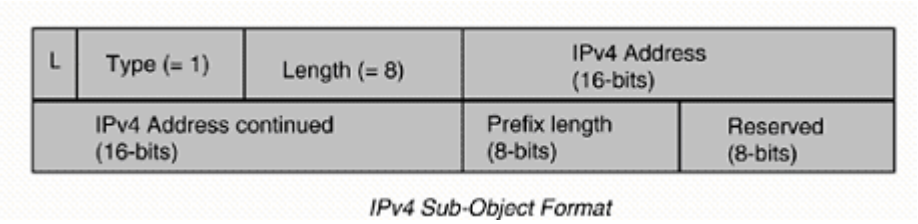
El Objeto de Ruta Explícita (ERO) se lleva en los mensajes del *Path* durante el establecimiento de LSP o redireccionamiento. Hay tres tipos de rutas explícitas básicamente:

a. La ruta explícita estricta: Identifica una serie de nodos adyacentes que describen el camino completo de una fuente a un destino.

b. La ruta explícita suelta: Identifica una serie de nodos no adyacentes a lo largo del camino de una fuente a un destino. Así, una ruta explícita suelta tiene espacios que necesitan ser llenados para conseguir el camino completo.

c. La lista del sistema autónomo (AS): Identifica una serie de sistemas autónomos adyacentes que queda a lo largo del camino de una fuente a un destino. Éste es por consiguiente una forma de ruta explícita suelta.

El formato *ERO* se muestra en Figura 13. Es una sucesión de sub-objetos, cada sub-objeto es un prefijo de IPv4, un prefijo de IPv6, o un número de AS. El bit L indica si un sub-objeto muestra un salto suelto y con este formato, un *ERO* puede ser estrictamente uno de los tres tipos anteriores, o puede ser una mezcla de éstos. Por ejemplo, la parte del ERO puede ser una sucesión estricta de nodos, y una parte puede estar suelta, algunos de ellos son sistemas autónomos. En el formato del *sub-objeto IPv4 ERO*, el campo de direcciones IPv4 puede contener un prefijo de dirección IP de longitud menor de 32 bits. Tal prefijo se fija cuando el salto *ERO* es suelto. El campo de longitud de prefijo indica esto.



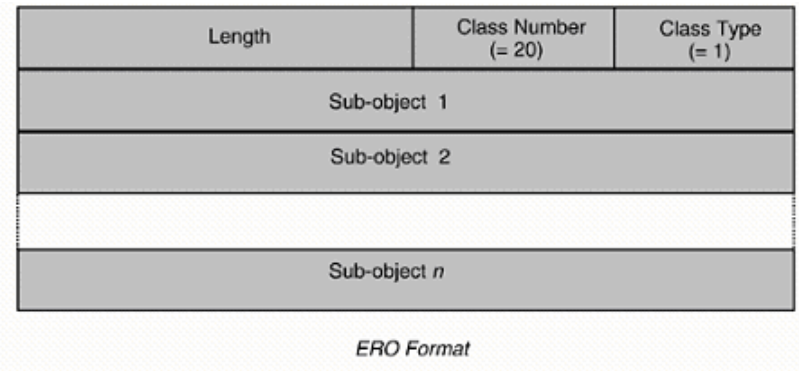


Figure 13. Los Detalles del formato ERO

Con el *ERO* que está presente en los mensajes *Path*, el envío de estos mensajes se manejan ahora diferente que bajo RSVP. Se supone un nodo que recibe un mensaje *Path* con un *ERO* en el que el nodo lista en el primer sub-objeto un salto estricto a este nodo desde el nodo anterior y determina el próximo nodo para remitir el mensaje así:

1. El segundo sub-objeto en el ERO indica a un vecino directamente alcanzable: El nodo elimina el off del primer sub-objeto y envía el mensaje *Path* al vecino.

2. El segundo sub-objeto no indica directamente un nodo remoto conectado: El nodo elimina el off del primer sub-objeto y cualquiera remite el mensaje *Path* al próximo salto hacia el nodo remoto como determinado desde su tabla de enrutamiento IP, o calcula unas rutas explicitas estrictas o sueltas para el nodo remoto y los prefijos *ERO* existentes con la ruta explícita calculada, y luego envía el mensaje *Path* al próximo nodo en la ruta calculada.

3. el segundo sub-objeto indica un AS: El nodo elimina el off del primer sub-objeto y determina el nodo fronterizo en su AS o en un vecino AS (si el propio nodo es un nodo fronterizo en su AS) para enviar el mensaje *Path*. Una vez el próximo nodo es determinado, las opciones para enviar son iguales que en (2).

1.2.1.4 La ruta de registro

El Objeto de Ruta de Registro (RRO) se lleva en los mensajes de *Path*. Se usa para registrar la sucesión real de nodos (o interfaces) atravesadas por un LSP que se ha establecido. La asignación de la etiqueta en varios saltos también puede registrarse. Este objeto proporciona una manera de supervisar los caminos de LSPs, así como para descubrir los *loops* cuando la asignación de ruta explícita suelta se usa para establecer LSPs.

1.2.1.5 Identificación del Tunel LSP

Este objeto se trata separadamente por direccionamiento IPv4 e IPv6. A continuación, se considera sólo el caso de IPv4.

El túnel de LSP se identifica como un nuevo sub-objeto bajo el objeto *sesión*. El formato de este objeto (denotado como objeto Sesión IPv4 del Túnel LSP) se muestra en Figura 14, donde la dirección de punto final del túnel Ipv4 indica la dirección del nodo de salida (el destino) en el cual el túnel LSP termina. El ID del túnel es un número de 16bits asignado por la fuente. El ID extendido del túnel es un campo de 32 bits adicional que puede usarse para extender el campo de ID del túnel opcionalmente. El uso típico es poner la dirección IP de la fuente aquí.

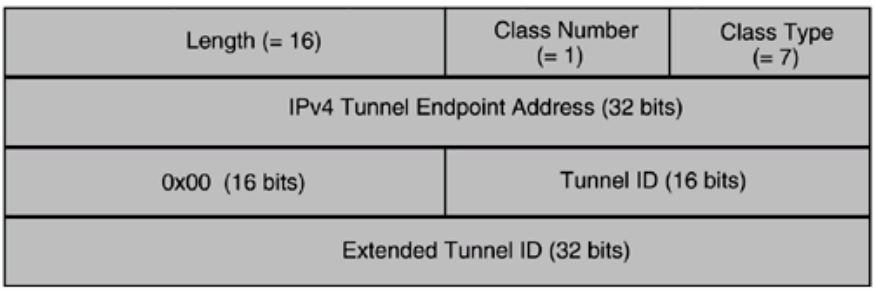


Figure 14. El Objeto de Sesión de Túnel LSP IPv4

Este objeto puede ser común a través de múltiples LSPs relacionados, mientras proporciona a los LSRs en la red un medio para asociar estos LSPs. Esta asociación es útil en ciertas aplicaciones tales como modificación no-disociadora del ancho de banda de LSP.

El identificador de LSP se lleva en *el objeto de Plantilla de emisor* como un sub-objeto. Este nuevo sub-objeto se llama *el objeto de plantilla de emisor del Túnel de LSP IPv4* y su formato se muestra en Figura 15. El identificador de LSP es una combinación de la dirección IPV4 de la fuente y un sufijo de 16- bits (denotado como ID LSP) asignado por esta fuente. El mismo formato se usa para definir el Túnel de LSP IPv4 Filterspec que se envía en los mensajes *Resv* para identificar el LSP específico a la función de clasificación del paquete. Dos LSPs entre la misma fuente y destino puede tener los mismos valores para el objeto de Sesión de Túnel de LSP IPv4 (llamada ID) mientras tienen distintos valores para los identificadores de LSP .

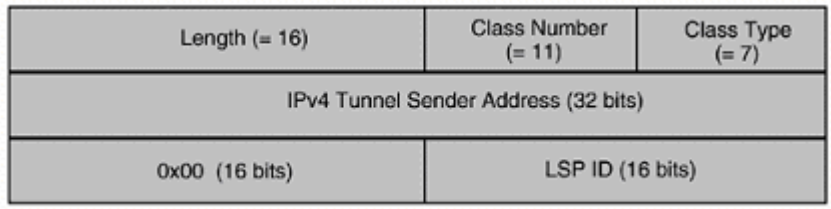


Figure 15. Objeto Plantilla Emisor del Túnel LSP IPv4

1.2.1.6 Atributos de sesión

El objeto *atributos de sesión* se lleva en los mensajes del *Path*. Este describe parámetros extensos relacionados a la sesión además de los parámetros de QoS descritos en *el Tspec*. Hay dos formatos definidos para los atributos de la sesión, uno de ellos es un super-conjunto del otro. Éste es el formato ilustrado en la Figura 16. Aquí, los campos tienen el siguiente significado:

- Exclude Any: este es un campo de banderas de 32-bits, cada bit indica un enlace específico “color”. El parámetro de color para los grupos de enlaces es según algún criterio administrativo (por ejemplo, todos los enlaces de baja-velocidad se les asigna el color 1). El LSP no puede ser enrutado sobre cualquier enlace que se le ha asignado un color que corresponde a un bit fijado a 1 en cualquier campo excluido.

- Include Any: este es un campo de banderas de 32-bits, cada uno indica un color de enlace específico. El LSP sólo debe enrutarse sobre enlaces que tienen por lo menos asignado uno de los colores indicados.

- Include all: este es un campo de banderas de 32-bits, cada uno indica un color de enlace específico. El LSP sólo debe enrutarse sobre los enlaces que tienen todos los colores indicados asignados.

- Setup Priority: este campo de 8 bits define la prioridad del LSP con respecto a otros LSPs cuando se obtienen los recursos Se definen ocho niveles de prioridad, de 0 a 7, (con 0 siendo la prioridad más alta). Al establecer un LSP

con prioridad de instalación *s*, otro LSP que sostiene la prioridad mayor que *s* puede ser apropiado para disponer el espacio para el anterior.

- Holding Priority: este campo de 8 bits define la prioridad del LSP con respecto a otros LSPs en retención de los recursos. Se definen ocho niveles prioridad, de 0 a 7, (con 0 siendo la prioridad más alta). Un LSP establecido con una prioridad de sostenimiento *h* puede apropiarse por otro LSP con la prioridad de instalación menor que *h*. La prioridad de sostenimiento de un LSP siempre debe ser más alta que su prioridad de Instalación, es decir, el valor de prioridad de sostenimiento h debe ser menor del valor de prioridad de instalación s).

- Flags: este es un vector de 8-bits de banderas. Se definen tres banderas y la bandera de "Diseño de protección local" se activa fijando un bit a 1 (de orden bajo). Esta bandera indica que un LSR intermedio puede reenrutar un LSP en una falla sin tener en cuenta la ruta especificada en el *ERO* original.

- Name Lenght: este es un campo de 8-bits que indica la longitud (en bytes) del campo de Nombre de Sesión.

- Session Name: carácter string que indica el nombre de la sesión.

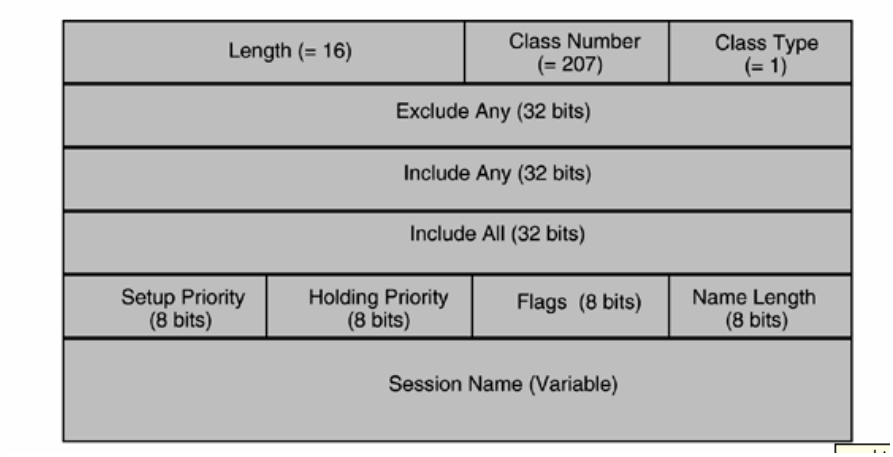


Figure 16. El Objeto de atributos de sesión

1.2.2 Estableciendo un tunel LSP

Un túnel LSP se crea típicamente entre un LSR de ingreso y un LSR de egreso dentro de una red (recordando que la aplicación de RSVP-TE es para ingeniería de tráfico). El establecimiento de este túnel se activa típicamente por la acción administrativa, por ejemplo, un comando desde el sistema de gestión de red al LSR de ingreso. Basado en la información de la asignación de enrutamiento, la QoS requerida y los atributos de sesión, un *ERO* se calcula primero. Este cálculo puede hacerse en el sistema de gestión o por el LSR de ingreso el cual construye un mensaje *Path* dirigido al destino IP apropiado. Este mensaje contiene *el ERO*, un *objeto de Petición de Etiqueta*, *la identificación del túnel*, los atributos de sesión y opcionalmente *el RRO*.

El progreso del mensaje *Path* descendente es similar a como pasa bajo RSVP. Un LSR que recibe el mensaje *Path* crea el estado del *Path* local y este estado del *Path* incluye *el ERO* recibido, los atributos de sesión, y así sucesivamente. El LSR determina las asignaciones de recurso locales para el LSP y determina los próximos LSRs para remitir el mensaje *Path* examinando y extendiendo quizás *el ERO* que fija la información *RSVP Hop* (y RRO, si es requerido) apropiadamente y entonces envía el mensaje *Path* a los próximos LSRs. El mensaje *Path* finalmente alcanza el LSR de salida.

El mensaje *Resv* se envía por el LSR de salida en respuesta al mensaje *Path* recibido. La progresión de este mensaje es similar al caso de RSVP, sólo que cada LSR también envía la etiqueta asignada para el LSP en el mensaje *Resv*. Un LSR que recibe el mensaje *Resv* usa la etiqueta asignada por el LSR descendente y la etiqueta se ha asignado ascendentemente para fijar su tabla de envío MPLS apropiadamente. Además, en esta fase, un LSR compromete los recursos locales requeridos realmente al LSP. Finalmente, el mensaje *Resv* alcanza el LSR de ingreso y el LSP se establece.

La figura 17 muestra un ejemplo de establecimiento de túnel LSP en una red pequeña de cinco LSRs MPLS. El LSP se establece de LSR R1 a LSR R4, con un ancho de banda de 500 Kbps, prioridad de instalación 3 y prioridad de sostenimiento 2. La figura 18 muestra algunos de los detalles del proceso. Aquí, R1-R4 indican las direcciones IP de los LSRs respectivos. Además, se asume que los LSRs son conectados por enlaces punto a punto no numerados cuyos identificadores de interfaz están marcados. El LSR R1 calcula *el ERO*, dado por <R1, R2, R3, R4>, y se asume que cada LSR escoge la interfaz local para localizar los próximos LSR en el camino. Los mensajes muestran los contenidos de los campos significantes.

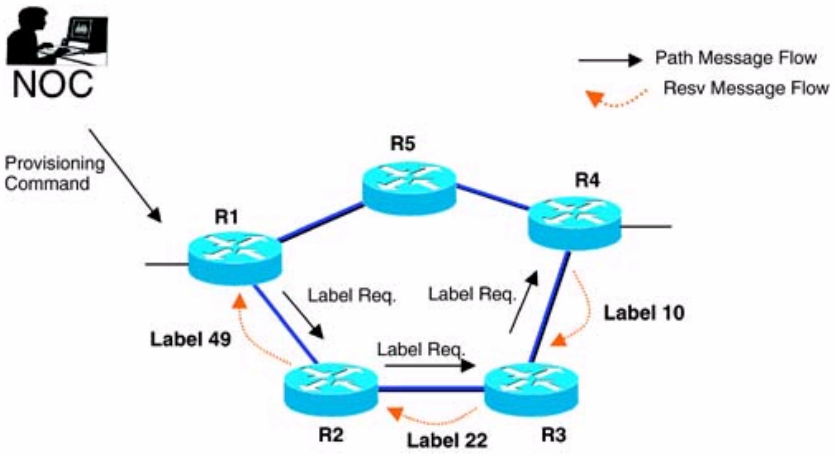


Figure 17. Ejemplo del Establecimiento del Túnel LSP

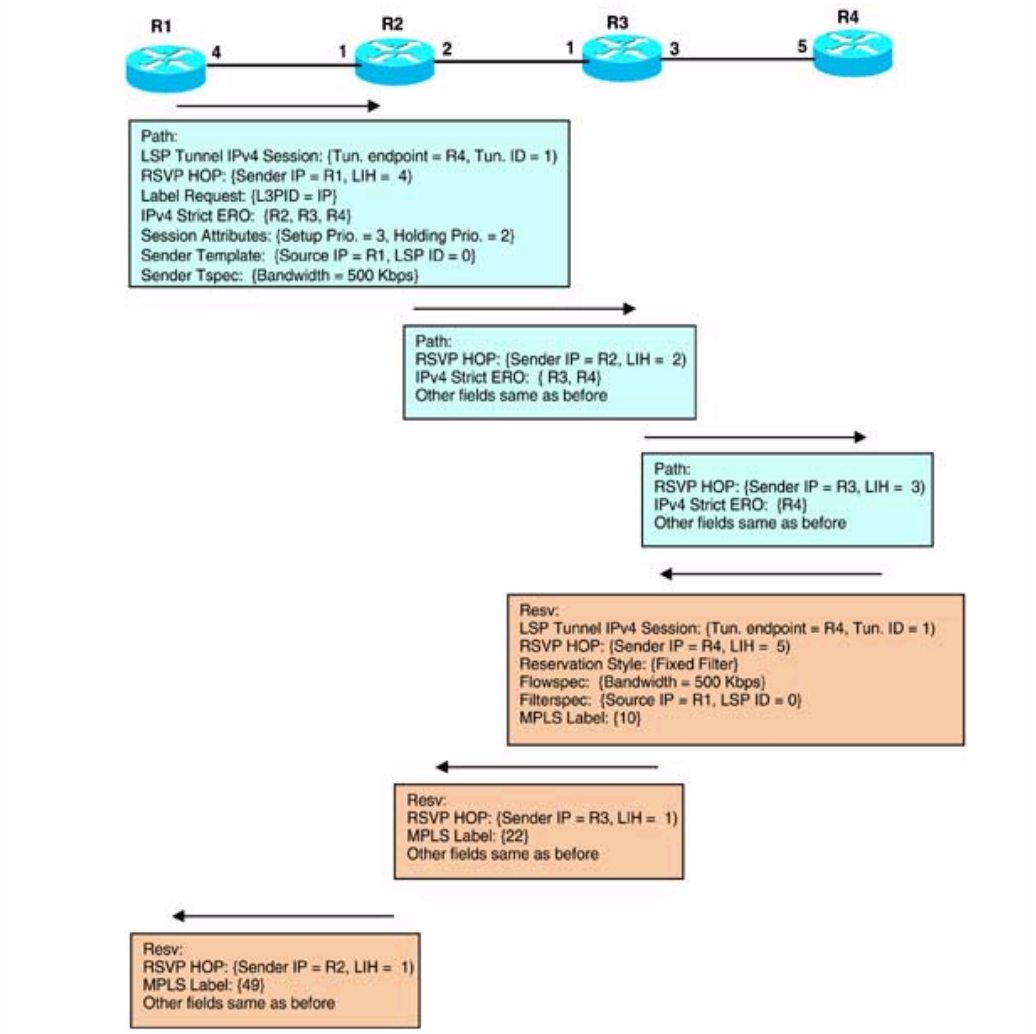


Figure 18. Detalles de Ejemplo de Establecimiento del túnel LSP

1.2.3 Estado suave de RSVP-TE

RSVP-TE confía en el mecanismo del estado suave básico proporcionado por RSVP. El estado de *Path y Resv* debe refrescarse periódicamente, pero, el establecimiento del LSP se controla por una ruta explícita. En el caso de RSVP, el mensaje *refresh* se adapta para dirigir los cambios, es decir, un mensaje *Path refresh* se envía al próximo salto hacia el destino. Bajo RSVP-TE, por ejemplo un LSR A que tiene que enviar un mensaje *Path refresh* a un LSR B descendente dado por el ERO tiene varios escenarios posibles:

1. El LSR B es el próximo salto estricto LSR en el ERO, y el LSR A ha determinado que B es inalcanzable: hay dos posibilidades aquí:

a. El Re-enrutamiento Local: el LSR A determina una ruta alrededor de la falla (teniendo en cuenta la QoS LSP y parámetros de la sesión) para LSR B. Este entonces envía el mensaje *Path refresh* a lo largo de esta ruta prefijando la ruta al *ERO* original, pero este tipo de re-direccionamiento local no puede usarse si son fallas propias del LSR B.

*b. El Restablecimiento***:** el LSR A envía un mensaje *PathErr o ResvTear* hacia el LSR de ingreso que indica la incapacidad para establecer el LSP. El ingreso reestablecerá el LSP con un nuevo *ERO* que evita el segmento del problema. Los LSRs en el *ERO* antiguo (y no en el nuevo ERO) esperan sus estados *Path y Resv*.

2. El LSR B es un próximo salto suelto en el ERO: En este caso, *el Path refresh* es exactamente igual que en el caso de RSVP cuando los cambios de ruta ocurren. El LSR A simplemente envía el mensaje *Path refresh* a lo largo de la ruta actual al próximo salto LSR (remoto) en el ERO.

3. El LSR A para de recibir los mensajes *Path refresh*: según RSVP en el procedimiento de estado suave, el LSR A quita los estados de *Path* local y *Resv* después de enviar un mensaje *PathTear* hacia LSR B. No hay ninguna consecuencia si LSR B no es alcanzable.

4. El LSR de ingreso determina un cambio en ruta que afecta el *ERO*: Este caso es similar al caso del restablecimiento en (1).

1.2.4 El protocolo hello RSVP-TE

RSVP-TE introduce un nuevo mensaje de RSVP llamado "*Hello*." Cada LSR envía un *Hello* a cada uno de sus pares RSVP-TE frecuentemente (el valor por defecto es una vez cada 3 segundos). Este mensaje sirve como un mecanismo para detectar las fallas del nodo rápidamente. Un LSR considera a su par como fallido si no recibe un mensaje *Hello* desde el par dentro de un cierto período de tiempo (el valor por defecto es 12 segundos).

1.2.5 Eliminación de un túnel LSP

Un túnel LSP es removido debido al estado suave de pausa o por la acción explícita por uno de los LSRs en *el Path*. El proceso de remover ordenadamente consiste en un LSR de ingreso que envía un mensaje de *PathTear* hacia la salida. El formato de este mensaje es similar al RSVP *PathTear* pero con el objeto de la sesión reforzado (con la identificación del túnel). *El PathTear* se envia basado en el estado del *Path* disponible a cada LSR. Un LSR que recibe el *PathTear* quita los estados *Path y Resv*, después de remitir el *PathTear* al próximo LSR.

Un *ResvTear* puede enviarse por el LSR de salida o cualquier LSR intermedio. Esto produce sólo la remoción del estado *Resv* en los LSRs intermedios.

1.2.6 la reducción de RSVP refresh

Un problema con el acercamiento de estado suave es la necesidad de refrescar el estado *Path y Resv* correspondiente a cada LSP independientemente. Desde que no se transmitan los mensajes de RSVP fiablemente, *el refresh* tiene que ser realizado con bastante frecuencia a los dos mensajes para asegurar que los LSPs se establezcan rápidamente y para mejorar la respuesta de falla. Esta frecuente actividad de *refresh,* multiplicada por el número de LSPs, podría generar un problema para los

LSRs. Una solución para aliviar este problema es la reducción del *refresh* RSVP introduciendo las siguientes capacidades:

-Una manera de unir mensajes que pertenecen a LSPs múltiples en un solo mensaje.

-Un mecanismo de mensajería fiable entre pares RSVP.

-Una manera de abreviar la información de *refresh* usando un identificador corto

La primera capacidad se realiza introduciendo un nuevo mensaje agrupado que puede llevar los mensajes múltiples (Path, Resv, etc.) de un LSR a otro. Los mensajes constitutivos en un mensaje agrupado pueden pertenecer a LSPs diferentes.

La segunda capacidad elimina la característica de transmisión de mensajes RSVP no confiable esencialmente entre dos nodos. Esto permite que sea reducida la frecuencia de *refresh.*

La tercera capacidad elimina la necesidad de enviar mensajes enteros *Path y Resv* cuando se refresca. Todas estas capacidades son opcionales es decir un nodo RSVP no necesita soportar estas capacidades para interactuar con aquellos que las tienen. De hecho, dos nodos RSVP sólo invocan estas capacidades si dos de ellos las soportan.

1.3 GMPLS EXTENSIONES PARA RSVP-TE

Las extensiones de RSVP-TE a GMPLS consisten en unos nuevos objetos, un nuevo mensaje, y los procedimientos asociados GMPLS traen cambios significantes al uso de RSVP-TE y estos son:

-Aplicación de la separación entre el plano de datos y el plano de control. En particular, en el modelo RSVP los mensajes de control se unen a las interfaces específicas del plano de datos, en GMPLS se eliminan (Ver sección 2.1)

-Dilución del modelo de estado suave, como se describió en las secciones 1.3 y 2.3, las fallas o faltas de comunicación en el plano de control llevan a acciones en el plano de datos bajo RSVP y RSVP-TE. Las extensiones de GMPLS apuntan a garantizar que los eventos de fallas en el plano de control no afecten el destino de conexiones cuyo plano de datos es perfectamente operacional. Esto se hace instituyendo los procedimientos de recuperación de plano de control.

-Se hace énfasis sobre los procedimientos de recuperación del plano de control ya que las extensiones de GMPLS permiten que dos pares RSVP-TE coordinen la recuperación de información de estado después de un evento de falla del plano de control, durante este proceso de recuperación, las conexiones existentes del plano de datos quedan intactas.

-Soporta conexiones bidireccionales mientras RSVP-TE soporta LSPs unidireccionales, por tanto las extensiones de GMPLS permiten la bidireccionalidad.

-La Introducción de un mecanismo de notificación remoto. La mensajería de RSVP-TE sigue el camino de conexión, por otra parte GMPLS introduce una extensión de la notificación que permite la mensajería entre los nodos remotos a lo largo de rutas que no están atadas al camino de conexión.

Ahora se entrará a examinar las extensiones de GMPLS usando el término GMPLS RSVP-TE. Además se usa el término conexión o LSPs y el término elemento de la red (NE) o LSRs indistintamente.

1.3.1 objetos GMPLS RSVP-TE

1.3.1.1 Petición de Etiqueta Generalizada

Este objeto se lleva en el mensaje Path, y reemplaza el objeto de petición de etiqueta de RSVP-TE (sección 2.1.1). Este objeto lleva los siguientes parámetros de conexión, y su formato se ilustra en la Figura 19:

1. El tipo de codificación LSP (LSP Type encoding): indica el tipo de conexión, por ejemplo, SONET /SDH, PDH, etc.

2. El tipo de conmutación (Switching Type): esta información indica el tipo de conmutación (Paquete, TDM, fibra, etc.) esto necesita ser efectuado para cada interfaz a medida que la conexión es conmutada.

3. Protocolo generalizado ID (G-PID): el tipo de carga útil que se lleva en la conexión (por ejemplo, paquete sobre SONET).

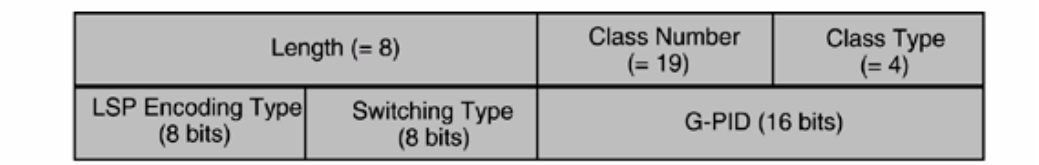


Figura 19. El formato del Objeto de petición de Etiqueta Generalizado

La información adicional de campos que pertenecen a la conexión se lleva en los objetos de RSVP-TE existentes. Éstos son:

4. Identificación de punto final fuente y destino: estas son para direcciones IPv4 o IPv6.

5. Ancho de banda: este es el ancho de banda requerido por la conexión. Un conjunto de valores discretos, cubriendo el rango de DS-0 a OC-768/STM-256, se ha definido usando el formato del punto flotante de de 32-bits de la IEEE.

La información de dirección de fuente se lleva en el objeto *Plantilla del emisor*, la dirección de destino se lleva en *el objeto Sesión*, y el ancho de banda se lleva en *el objeto Tspec*. Además, cuando una conexión de SONET/SDH se establece, los parámetros de tráfico relacionados se codifican. Los parámetros de tráfico se llevan en el nuevo *Tspec* del emisor de SONET/SDH y *objetos Flowspec* SONET/SDH.

1.3.1.2 Etiqueta Generalizada

El objeto de Etiqueta Generalizada reemplaza *el objeto de la Etiqueta* en el mensaje *Resv* de RSVP-TE (sección 2.1). El formato de este objeto se muestra en Figura 20. El campo de la Etiqueta puede contener varios tipos de la etiqueta, incluso la etiqueta MPLS y las etiquetas SONET/SDH.

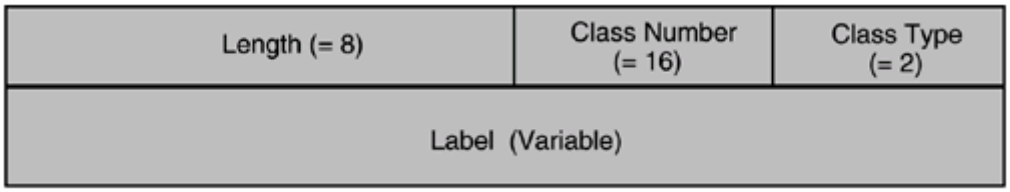


Figure 20. El formato del Objeto de Etiqueta

1.3.1.3 Etiqueta Sugerida

La Etiqueta sugerida se lleva en el mensaje *Path*. Como se observa en el ejemplo de la Figura 21, el LSR descendente asigna la etiqueta para la dirección de fuente-a-destino de la conexión. La característica de la *Etiqueta Sugerida* le permite a un LSR "sugerir" a su vecino descendente inmediato la etiqueta generalizada a ser retornada durante la fase de respuesta.

Una etiqueta sugerida tiene el mismo formato de la etiqueta generalizada. Además, un LSR descendente puede no aceptar una etiqueta sugerida, es decir, puede devolver una etiqueta diferente en la fase de respuesta. En este caso, el LSR ascendente puede reestablecer el cross-conector. Finalmente, dado que el provisionamiento de la conexión no tiene las exigencias urgentes de tiempo como conmutación de protección, el valor de etiqueta sugerida durante el aprovisionamiento es bastante impreciso.

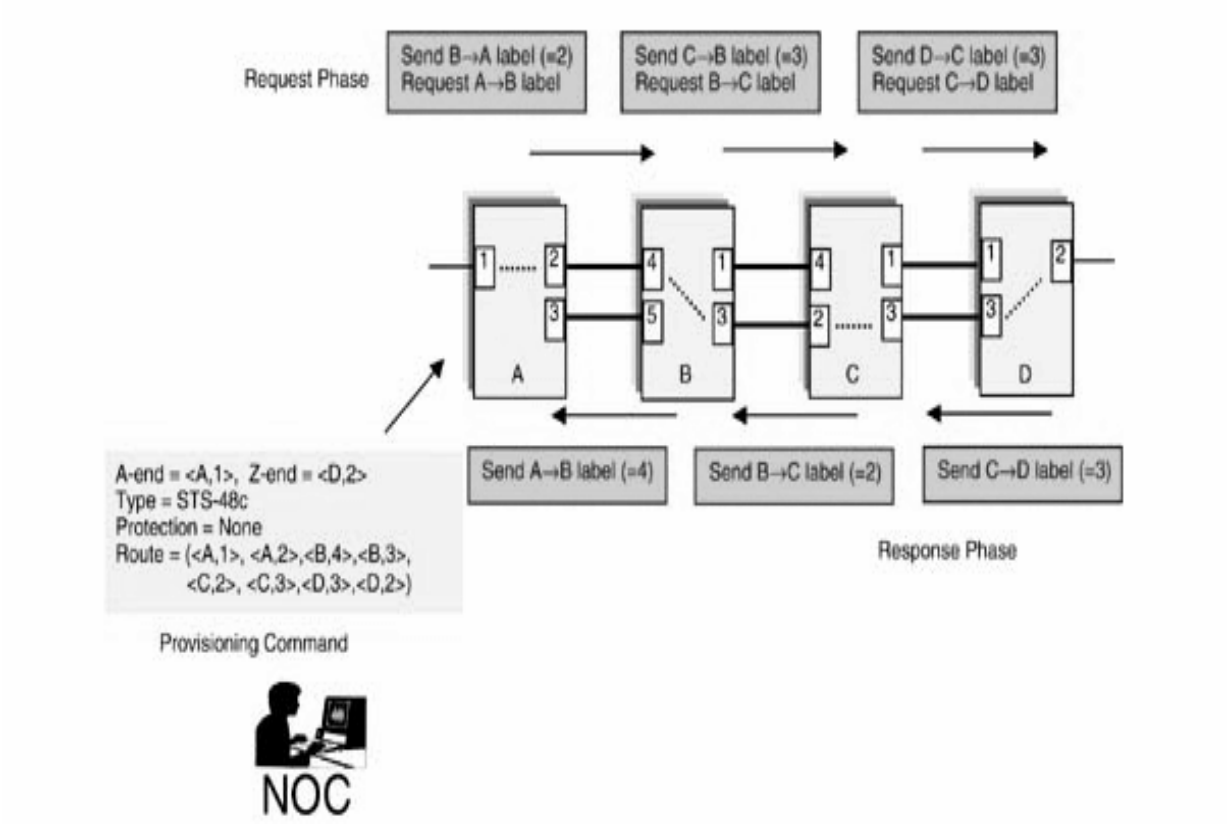


Figura 21. La Petición de la etiqueta y las fases de Respuesta en el aprovisionamiento de la conexión

1.3.1.4 Etiqueta Ascendente

La Etiqueta ascendente se lleva en el mensaje *Path*. Esta etiqueta está presente si un al establecerse un LSP bidireccional. Como se describió antes, el LSR descendente asigna la etiqueta para el envío (de la fuente al destino) en la dirección del LSP durante la fase de respuesta de aprovisionamiento (Figura 21). Esto se lleva como una etiqueta generalizada en el mensaje *Resv*. Una etiqueta ascendente, por otro lado, indica la etiqueta ascendente seleccionada para la dirección contraria del LSP (del destino a la fuente). La etiqueta ascendente tiene el mismo formato de la etiqueta generalizada. Claramente, el tipo específico de etiqueta debe coincidir para las dos direcciones del LSP. Además, los parámetros tienen que ser los mismos para ambas direcciones del LSP.

1.3.1.5 Conjunto de Etiquetas

El Conjunto de etiquetas se lleva en el mensaje *Path*. Se usa por un LSR ascendente para controlar la selección de etiquetas por LSRs descendentes. Es decir, un LSR indica el conjunto de etiquetas que son aceptables por este en el mensaje de petición. Un LSR descendente debe seleccionar una etiqueta de este conjunto. Por ejemplo, considere el caso de aprovisionar un LSP de longitud de onda a través de una red toda óptica dónde los switches no pueden realizar la conversión de la longitud de onda. Aquí, el LSR fuente indicaría un conjunto de longitudes de onda que tiene disponible para la conexión en *el Objeto Conjunto de Etiqueta*. Cuando los mensajes de petición

se dirigen hacia el destino, cada LSR intermedio mira el conjunto de etiqueta recibido, considera las longitudes de onda localmente disponibles y potencialmente disminuye el conjunto de etiquetas disponibles modificando el objeto de conjunto de Etiqueta y enviando el objeto a su vecino descendente. Cuando la petición alcanza el LSR destino, puede escoger una de las etiquetas permitidas (las longitudes de onda) para el LSP e indicar esto en el mensaje de respuesta. La misma etiqueta se propaga luego al LSR fuente.

El formato del *objeto conjunto de etiqueta* se muestra en la Figura 22, aquí, el campo *"Actión"* indica lo siguiente:

Actión = 0 (la lista Inclusiva): indica cada etiqueta incluida en el conjunto. Un LSR puede escoger sólo una etiqueta que se lista.

Actión = 1 (la lista Exclusiva): indica cada etiqueta excluida. Un LSR puede escoger cualquier etiqueta excepto aquéllas listadas.

Actión = 2 (el rango Inclusivo): Indica un rango de etiquetas incluido en el conjunto. Un LSR puede escoger sólo una etiqueta incluida en el rango. El *objeto conjunto de etiquetas* contiene dos etiquetas, cada una para el inicio y el fin del rango.

Actión = 3 (el rango Exclusivo): Indica un rango de etiquetas excluido en el conjunto. Un LSR no puede escoger una etiqueta incluida en el rango. *El objeto conjunto de etiquetas* contiene dos etiquetas, una para el inicio y otra para el fin del rango.

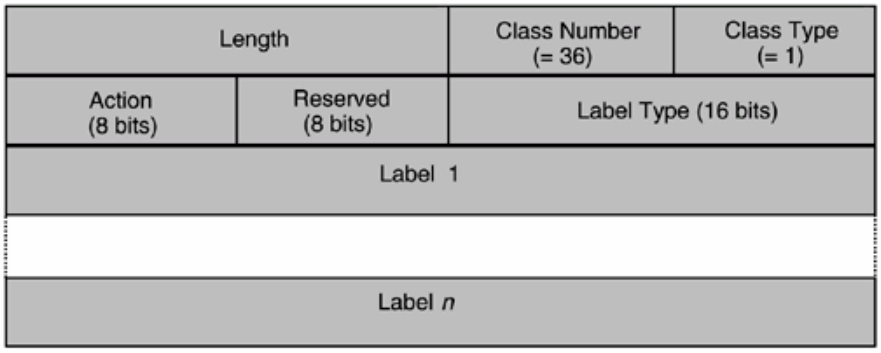


Figure 22. El formato de Objeto conjunto de Etiquetas

El campo " Label Type o Tipo de Etiqueta" indica el tipo de etiqueta.

1.3.1.6 Conjunto de Etiquetas Aceptables

El Conjunto de Etiquetas aceptables se lleva en mensajes seguros *PathErr, ResvErr,* y *Notificación*. Cuando un LSR no puede aceptar una etiqueta dada, puede generar un mensaje de error con el conjunto de etiquetas aceptables. *El objeto Conjunto de Etiquetas Aceptables* tiene el mismo formato que el objeto conjunto de etiquetas.

1.3.1.7 La Información de Protección

La Información de protección se lleva en el mensaje Path. Este objeto indica la protección deseada para el LSP en cada enlace en el camino de conexión. Este objeto puede estar presente al aprovisionar los caminos de funcionamiento y de protecciones de la conexión camino-protegido extremo a extremo. El formato del objeto de Información de Protección se ilustra en la figura 23. Los siguientes campos están presentes:

- **El bit Secundario (S):** Este campo de un bit indica si la conexión que está siendo provisionada es primaria (de funcionamiento, S = 0) o secundaria (de protección, S = 1). La petición del modo de protección que sigue sólo es aplicable a las conexiones primarias.

- **Banderas de Enlace:** Este campo de 6 bits es un vector de banderas. El bit que se fija indica que el modo de una protección específica se solicita. Se puede fijar mas de un bit si más de un modo de protección es aceptable. La selección del modo de protección específica es entonces una decisión local en cada LSR**.**

-Bit 5 (orden alto) Protección reforzada: Indica que la protección buena 1+1 se desea. Típicamente, este bit se podría fijar para pedir un tipo de protección de cuatro fibras BLSR/MS-SPRING.
-Bit 4 1+1: Indica que se desea la protección 1 + 1.
-Bit 3 1:1: Indica que se desea la protección 1:1.
-Bit 2 Compartido: Indica que se desea la protección 1:N o M:N.
-Bit 1 No protegido: Indica que la conexión no debe protegerse en cada enlace.
-Bit 0, Tráfico extra: Indica que la conexión puede ser enrutada como tráfico extra en cada enlace, esto puede ser apropiado para proteger otras conexiones.

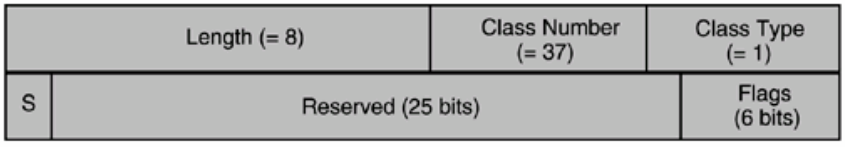


Figure 23. El formato del Objeto de Información de Protección

Claramente, sólo el modo no protegido puede solicitarse para las conexiones secundarias (cuando S = 1). Es decir, el resto de los modos de las protecciones no es aplicable a una conexión secundaria (de protección) que proporciona protección de camino extremo a extremo a una conexión primaria (de funcionamiento).

1.3.1.8 Estado Administrativo

El objeto de *estado administrativo* se usa en los mensajes de señalización para indicar que un LSP está siendo administrativamente borrado, o esta siendo puesto en un modo de prueba. La señalización de GMPLS proporciona una manera de señalar estas acciones administrativas. Esto asegura que los

LSRs en el camino de conexión no se equivoquen en las acciones administrativas para los eventos de fallas y dispararen las acciones de protecciones. El formato del objeto de *estado administrativo* se ilustra en Figura 24. Los siguientes campos están presentes:

-Reflect (R): Este bit indica que el objeto de estado administrativo recibido debe reflejarse por el nodo receptor en un mensaje apropiado. El uso de este bit se aclara cuando se observa la eliminación de un LSP.

-Testing (T): Este bit indica que la conexión está siendo fijada en el modo de la comprobación. Las acciones a ser tomadas a cada nodo que recibe el objeto de estado administrativo con el bit T fijo no se especifica.

-Administratively Down (A): Este bit indica que la conexión está establecida como baja administrativamente.

-Deletión in Progress (Eliminación en marcha) (D): Este bit indica que la conexión está siendo borrada. El uso del bit D durante la eliminación de conexión se describe más adelante.

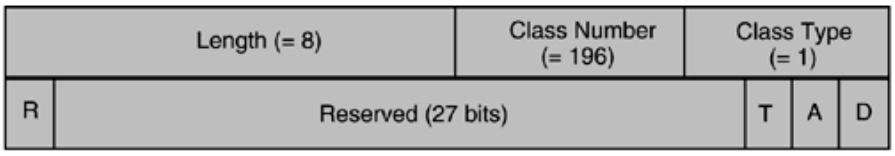


Figure 24. El formato del Objeto de Estado Administrativo

1.3.1.9 Identificación de la Interfaz

Bajo MPLS-TE, se envían los mensajes de señalización sobre los mismos enlaces de los flujos de datos. Así, las etiquetas que se asignan son específicas para las interfaces sobre las cuales se reciben los mensajes de la señalización.

Bajo GMPLS, los canales de control sobre los cuales se envían los mensajes de la señalización pueden ser distintos de los enlaces de los datos. Por ejemplo podría haber un enlace de control fuera de banda, (por ejemplo, Ethernet) conectando dos switches ópticos. Los mensajes de señalización que pertenecen al LSP provisionado sobre todos los enlaces de datos pueden enviarse sobre este enlace fuera-de-banda. Así, debe ser posible en los mensajes de la señalización identificar explícitamente los enlaces de datos sobre los cuales las etiquetas han sido asignadas. *El objeto de identificación de interfaz* hace esto.

Generalmente, bajo GMPLS, las interfaces pueden tener diferentes tipos de direccionamiento, como se muestra en la figura 25. En esta figura se dibujan dos LSRs adyacentes con sus direcciones IP (escogidas arbitrariamente para este ejemplo) aunque no todos estos modos de direccionamiento se pueden usar en la práctica. Se muestran Cuatro tipos de enlaces:

-Un enlace numerado agrupado (Numbered Link Bundle) (también llamado un "enlace TE"): Este enlace de agrupación consiste de múltiples componentes de enlaces. El enlace agrupado tiene una dirección IP para cada fin, mostrado en la figura. Los componentes de enlaces son reconocidos por distintos identificadores para cada fin.

-Un enlace agrupado no numerado (Unnumbered Link Bundle): Es lo mismo descrito anteriormente, sólo que el enlace agrupado no tiene una dirección IP asignada para algún fin y en cambio, un identificador localmente distinto se usa para algún fin para identificar el agrupamiento.

-Un enlace numerado individual (Numbered Individual Link): Éste es un enlace punto a punto con una dirección IP asignada a cada fin.

-Un enlace no numerado individual (Unnumber Individual Link): Éste es un enlace punto a punto con un identificador localmente distinto para cada fin.

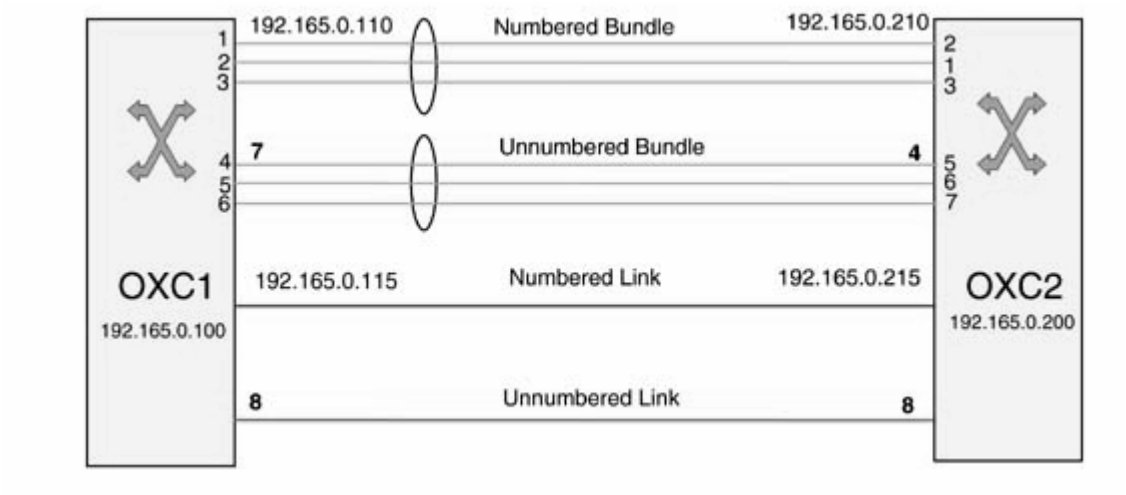


Figura 25. Diferente esquema de direccionamiento de interfaz

El concepto de bundling (agrupamiento) se usa para reducir el enrutamiento en el encabezado. Durante la señalización, sin embargo, el enlace preciso para la asignación de la etiqueta debe identificarse aun cuando es parte de un enlace agrupado. *El objeto de identificación de interfaz* (llamados los objetos IPv4 IF_ID_RSVP_HOP) sirve para este propósito. Este objeto se usa en GMPLS RSVP-TE en lugar del *objeto RSVP Hop*. El formato de este objeto se muestra en Figura 26. Para entender cómo este objeto se usa, note que en la Figura 25, cada interfaz que termina un enlace (sea individual o enlace de componente) tiene un identificador distinto para cada LSR. Éste es el identificador señalizado que usa el objeto de identificación de interfaz.

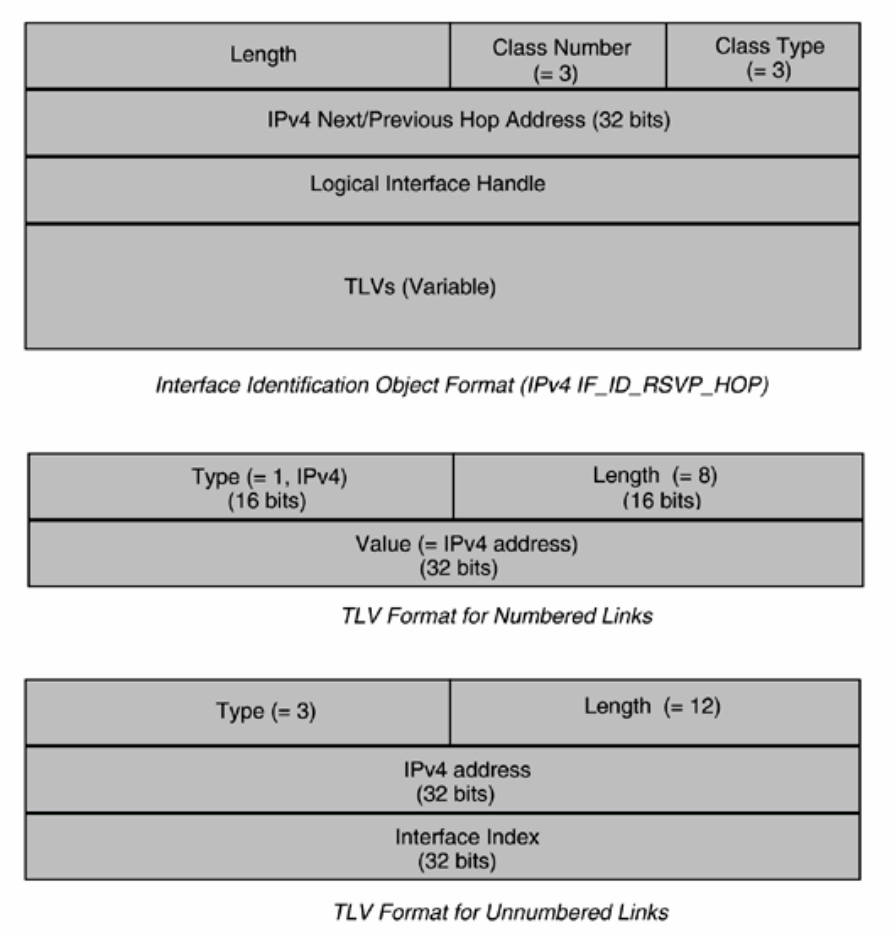


Figure 26. La Identificación de la interfaz

Con este objeto, se capturan tanto la dirección del plano de control desde la cual el mensaje GMPLS RSVP-TE se envía, y el identificador de enlace de componente del plano de datos. El primero se captura en el IPv4 anterior o en la dirección del próximo salto y los campos LIH (Manejo de Interfaz Lógica) como en el caso de RSVP-TE regular y el último se captura como sigue. Si el enlace de datos es numerado, la dirección IPv4 del enlace se usa como se mostró en el primer TLV y si el enlace de datos es no numerado, entonces la dirección IPv4 del LSR y los distintos identificadores de interfaz se capturan como se mostró en el segundo TLV. Este uso se describe más adelante con mayor detalle.

1.3.1.10 Petición de Notificación

El objeto de Petición de Notificación puede estar presente en los mensajes *Path*. Este objeto indica la dirección IP a las cuales las notificaciones relacionadas con las fallas deben enviarse. Cada LSR que procesa el mensaje *Path* puede anotar esta información para propósitos de la notificación.

1.3.2 El mensaje de notificación

El mensaje de notificación es un nuevo mensaje introducido bajo GMPLS RSVP-TE como se mostró en el capitulo anterior. Este proporciona un mecanismo para un LSR para informar a un LSR remoto (normalmente al

ingreso o a la salida) sobre un evento relacionado con el LSP (normalmente un evento de falla). Un LSR genera un mensaje de notificación si ha recibido un objeto de petición de notificación en el mensaje *Path*. El mensaje de notificación es diferente de *PathErr* y *ResvErr* y puede enrutarse independientemente del camino de conexión. El mensaje de notificación no reemplaza éstos mensajes de error. Este mensaje contiene un código del error y un objeto de ID de Mensaje.

La recepción del mensaje de Notificación se reconoce por el receptor con un mensaje *Ack* que es un mensaje de notificación con un *objeto Ack* de ID del Mensaje.

1.3.3 Establecimiento de un LSP bajo GMPLS RSVP-TE

Explicado ya, el procedimiento de establecimiento de túnel LSP bajo RSVP-TE no debe ser difícil suponer acerca de cómo el provisionamiento de LSP trabajará bajo GMPLS RSVP-TE. En esencia, se usan los mensajes *Path y Resv* para la fase de petición y respuesta de provisionamiento (ilustrado en la figura 21). hay algunas diferencias, entre la manera como RSVP-TE se usa para el establecimiento de LSP en las redes MPLS y como GMPLS RSVP-TE se usa para aprovisionar las conexiones en las redes ópticas.

-Primero se debe considerar que la señalización de RSVP-TE ocurre sobre los mismos enlaces en que el LSP correspondiente se establece; entre los pares GMPLS RSVP-TE se requiere un enlace de control de señalización separado. Este enlace de control es considerado parte de la Red de Comunicación de Datos (*Data Comunication Network*, DCN) y la DCN podría ser implementada en banda, por ejemplo, usando los bytes del encabezado SONET/SDH , o podría ser una red de fuera de banda por ejemplo, una red IP.

-Al usar GMPLS RSVP-TE, el mecanismo de la mensajería fiable descrito en la sección 1.2.6 RSVP-TE se usa típicamente.

-El plano de Control reinicia los procedimientos como se describe en la sección 1.3.5 que se llevan a cabo al usar GMPLS RSVP-TE.

El procedimiento de establecimiento de conexión se describe mejor con la ayuda de un ejemplo. Las figuras 27a y 27b extienden el ejemplo de provisionamiento de la figura 21 con los detalles de los mensajes *Resv y Path,* respectivamente. Considerando la figura 27a primero, se muestra una red de cuatro LSRs. Cada LSR tiene una dirección IP y hay otra en los enlaces entre los LSRs A y B, pero todos los otros enlaces son no numerados. Además todos los enlaces son asumidos como enlaces OC-48 y para los enlaces de datos, el enlace de control entre los LSRs se muestra con las líneas punteadas. Además, cada interfaz de enlace de control se identifica por la dirección IP del LSR correspondiente y una ID de interfaz (LIH) mostrada cerca a este.

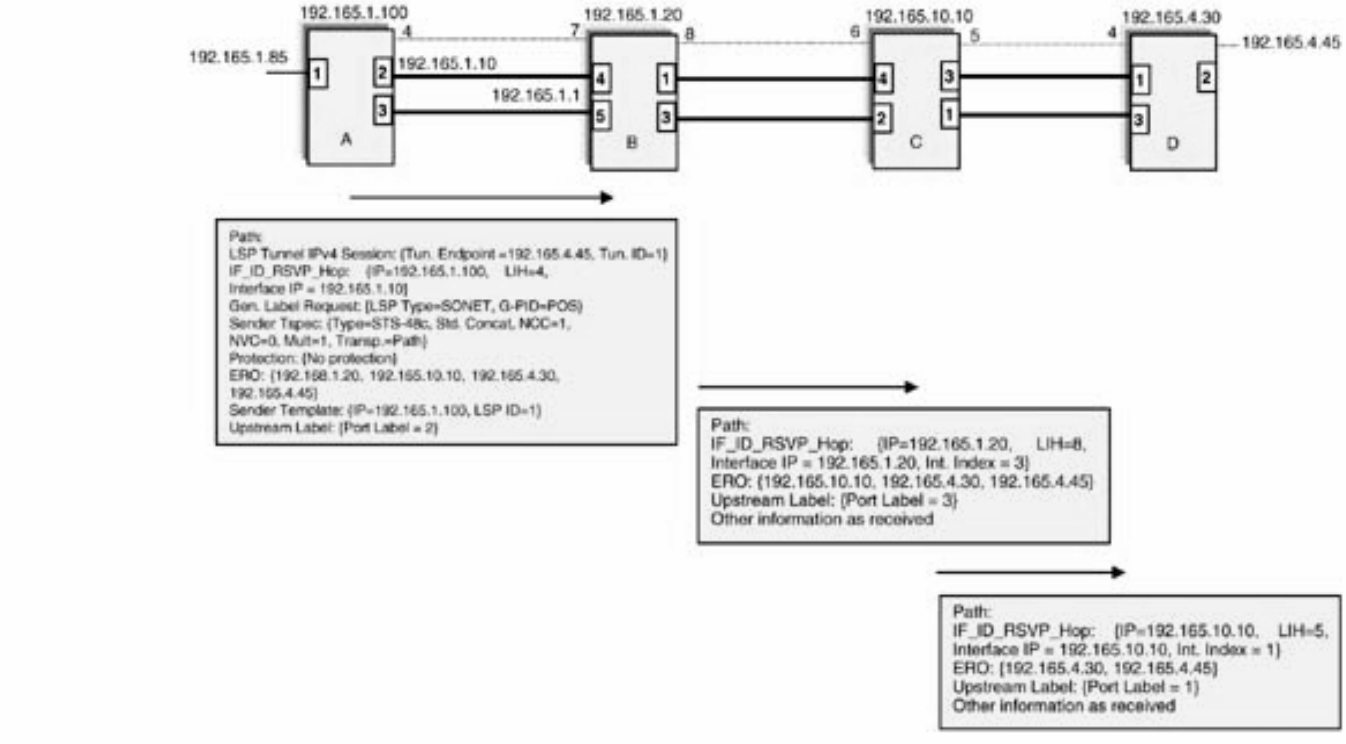


Figure 27a. El Flujo de Mensaje Path bajo GMPLS RSVP-TE

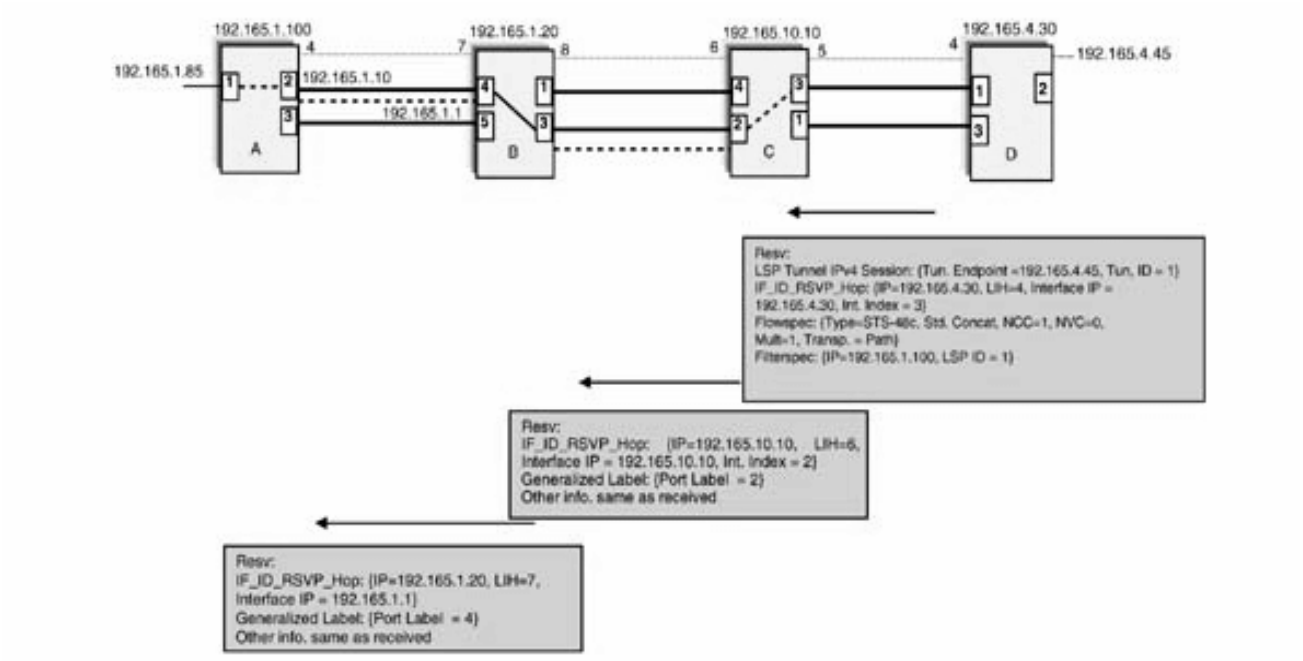


Figure 27b. El Flujo de Mensaje Resv bajo GMPLS RSVP-TE

El LSR A recibe una activación de provisionamiento para establecer un LSP de STS-48c bidireccional entre su interfaz 1 (con dirección IP 192.165.1.85) y el LSR D (con dirección IP= 192.165.4.30), una interfaz 2 (dirección IP = 192.165.4.45). Basándose en la información de enrutamiento disponible, el LSR A calcula una ruta explícita que atraviesa los LSRs B, C, y D. En este

caso, cada LSR es responsable de seleccionar el enlace actual para el próximo LSR cuando el LSP se aprovisiona.

Se muestra el mensaje *Path* generado por el LSR A y este mensaje tiene el *objeto de Sesión de Túnel LSP IPv4* fijado para indicar el destino remoto y la *ID del túnel* localmente asignada. *El ERO* lista las direcciones IP de LSRs en el camino y *El objeto de identificación de Interfaz* (IF_ID_RSVP_HOP) indica ambos los IDs del canal de control (dirección IP y LIH) y la ID del enlace de datos (dirección IP para numerar, y direcciones IP más el índice de la interfaz para los enlaces no numerados), las listas de objeto de Etiquetas Generalizadas, el tipo de LSP como SONET y el G-PID como el Paquete sobre SONET (POS). Los parámetros de trafico SONET se dan en el *Tspec del Emisor*. Las listas de *Plantilla del Emisor,* la dirección IP del LSR A y la ID LSP localmente asignada. Finalmente, el objeto de la Etiqueta ascendente indica la etiqueta seleccionada para la dirección D a A de la conexión. Si los enlaces son OC-48, ellos pueden acomodar cada uno una conexión de STS-48c y dentro del tipo de etiqueta se indica la etiqueta del puerto en lugar de la etiqueta de SONET.

Cuando el mensaje *Path* progresa, cada LSR intermedio crea su estado del *Path*, y propaga el mensaje *Path* al próximo LSR después de modificar el *ERO,* la información de la etiqueta ascendente y la información de identificación de interfaz. El mensaje localiza el LSR D finalmente el cual avisa que el destino es local y así termina el mensaje.

El correspondiente flujo de mensaje *Resv* se muestra en Figura 27b. El mensaje *Resv* generado por D contiene la etiqueta para el segmento de conexión del C a D. La información de *Flowspec* refleja los parámetros de tráfico recibidos en *el Tspec* esencialmente. La progresión del mensaje *Resv* se muestra en la figura. Como cada LSR procesa el mensaje *Resv*, este pone el apropiado cross-conector para establecer las dos direcciones de la conexión. El provisionamiento de conexión se completa cuando A recibe el mensaje *Resv* y fija el apropiado cross-conector. La conexión extremo a extremo que usa las líneas punteadas se muestra en la figura.

En la figura 27 no se muestra la entrega fiable de mensajes *Path y Resv* pero se realiza de acuerdo a lo descrito anteriormente y su uso es típico en la red óptica. El uso de esta opción significa que el refresco de estado suave puede ser poco frecuente. El mecanismo de estado suave no se elimina completamente (es parte de la definición de RSVP), pero el período de tiempo entre refreshes es típicamente puesto a un valor alto. Las rupturas en el camino de conexión son típicamente determinadas por los mecanismos de SONET/SDH incorporados, y así un alto valor de tiempo de refresh no afecta la sensibilidad de GMPLS RSVP-TE para reaccionar a los fracasos de conexión.

1.3.4 Eliminación de la conexión bajo GMPLS RSVP-TE

Bajo RSVP-TE, una fuente anula un túnel LSP enviando un *PathTear*. Como los progresos de *PathTear*, los LSRs intermedios quitan sus estados *Resv* y *Path* simplemente. El mismo procedimiento no puede usarse en una red óptica. En cuanto un LSR ascendente anula su estado (y remueva el cross

conector), los LSRs descendentes pueden descubrir una falla de conexión y puede acudir a la acción de protección o puede mandar fuera las alarmas innecesarias. Así, GMPLS RSVP-TE introduce las fases extras en la eliminación de conexión tal que los LSRs a lo largo del camino de conexión están alerta de una eliminación en progreso antes de que la eliminación real ocurra. Los objetos de Estados Administrativos (Figura 24) se usan en este procedimiento.

Considerando el LSP que era configurado en el ejemplo ilustrado en la Figura 27. La secuencia del mensaje para la eliminación de esta conexión cuando se inicia por la fuente (LSR A) se muestra en la figura 27a. Aquí, el LSR A primero envía un mensaje *Path* para comenzar la eliminación. Este mensaje es similar a los mensajes *Path* periódicos enviados para la conexión sólo que tienen el objeto de Estado Administrativo con los bits R y D fijados a 1. Como este mensaje progresa a lo largo del camino de conexión, cada LSR intermedio nota que la conexión está en el proceso de eliminarse así, ellos no inician las acciones de protección si observan fallas a lo largo del camino de conexión. Cuando el destino (LSR D) recibe el mensaje *Path*, genera un *Resv* en respuesta. Desde que el bit R sea fijado en *el Objeto de Estado Administrativo* recibido el LSR D refleja el objeto en el mensaje *Resv* con el bit R puesto a 0 y el bit D puesto a 1. Cuando un LSR A recibe el mensaje de *Resv* con el objeto de Estado Administrativo, envía un mensaje *PathTear* usual. Cuando este mensaje progresa a lo largo del camino de conexión, los LSRs en la ruta remueven el estado del *Path* y *Resv* asociados con la conexión.

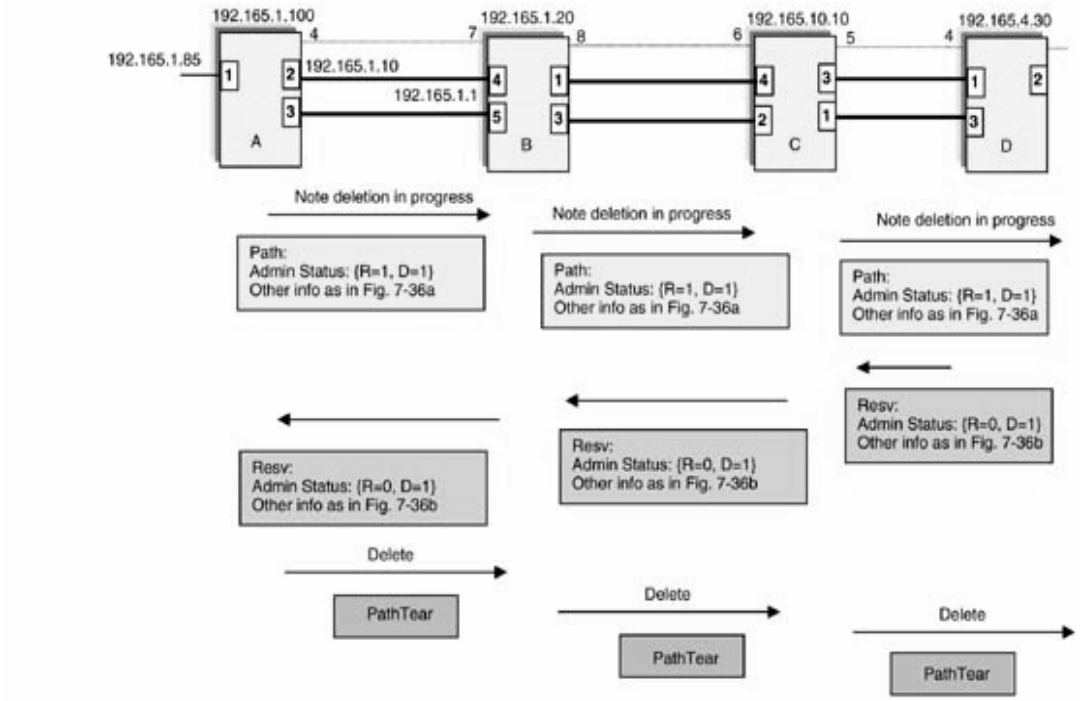


Figura 28a. Eliminación iniciada por la Fuente

La secuencia del mensaje cuando la eliminación se invoca por el destino (LSR D) se muestra en Figura 28b. Aquí, el LSR D primero envía un mensaje *Resv* con el objeto de Estado Administrativo. Los bits R y D en este objeto se ponen en 1. Este mensaje se propaga hacia la fuente (LSR A), y cada LSR

intermedio nota que la conexión esta próxima a ser eliminada. Cuando un LSR A recibe el mensaje, genera un *PathTear* como antes.

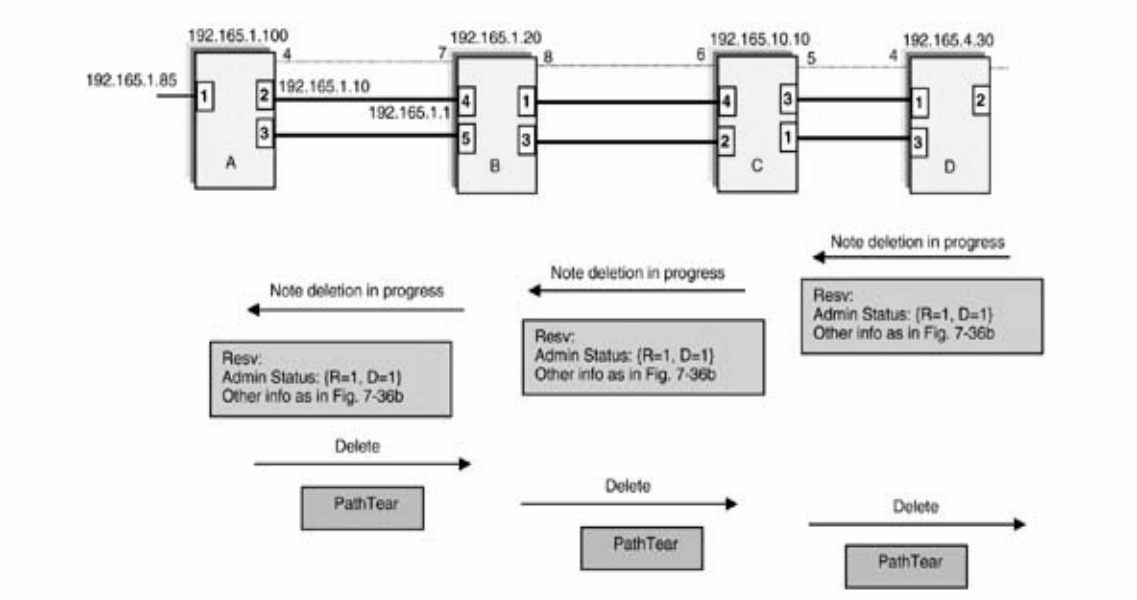


Figure 28b. Eliminación iniciada por el Destino

1.3.5 Los procedimientos de reactivación GMPLS RSVP-TE

Un resultado de la separación del plano de control y de datos es que las fallas en el plano de control no implican fallas en el plano de datos. Considerando la figura 27 de nuevo. El enlace de control entre LSRs se muestra como una línea punteada y como se menciono antes, este enlace podría ser un enlace separado fuera-de banda o un canal de control en banda. En cualquier caso, una falla en el enlace de control o una falla del proceso de software de señalización no implica que cualquiera de las conexiones del plano de datos previamente establecidas hayan sido afectadas. Así, bajo GMPLS RSVP-TE, las conexiones de datos no son removidas cuando la comunicación de control se rompe (considerando que bajo RSVP-TE, los no recibimientos de los mensajes *Path* de *refresh* llevan a remover el estado *Path* y *Resv* a un LSR). En cambio, GMPLS RSVP-TE introduce los procedimientos de reactivación del plano de control, es decir, un nodo que pierde el enlace de control con otro intentará sincronizar su estado *Path* y *Resv* cuando el enlace de control se reestablece. Entretanto, las conexiones o las fallas pueden ser eliminadas manualmente. El proceso de la sincronización asegura que los pares RSVP-TE tengan una vista consistente de las conexiones cuando ellos recuperan fallas desde el plano de control.

Así, se nota que la eliminación de conexiones en redes ópticas que usan GMPLS RSVP-TE es típicamente el resultado de una acción administrativa o de fallas del plano de datos. Las rupturas temporales en la comunicación del plano de control no llevan a tal eliminación. El plano de control reactiva los procedimientos.

1.4 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 el intercambio de protocolo 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 esté 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 del LMP, entre estás áreas se encuentran la Gestión del Canal de Control, Verificación del Enlace, Correlación de Propiedad del Enlace, Gestión de Falla y Autenticación que se describen con detalle a continuación.

1.4.1 Gestión del canal de control

Está área de funcionalidad cubre el establecimiento, configuración y mantenimiento de un canal de control IP entre un par de nodos vecinos LMP. La Gestión del Canal de Control hace referencia a la negociación y al mantenimiento de la propia sesión del LMP. Los mensajes Hello del LMP se usan para confirmar que la sesión está aún funcionando. Es necesaria la negociación de los parámetros con el fin de acordar los valores de los parámetros por sesión tales como los períodos de temporización del Hello, nivel soportado del protocolo y soporte para características opcionales del protocolo.

• **La Selección del Canal de Control**
No está actualmente dentro del objetivo del LMP, pero no obstante es un requerimiento importante para el trabajo del LMP. Los puertos LMP deben conocer como usar el(los) mismo(s) canal(es) de control cuando intercambian mensajes LMP.

•**La Negociación de los Parámetros**

Permite que un par de nodos LMP converjan en un conjunto aceptable mutuo de parámetros de configuración. El intercambio del protocolo implica tres mensajes (Config, ConfigAck, ConfigNack) cada uno de los cuales puede contener un número variable de subobjetos describiendo determinados parámetros (tales como valores de temporización y soporte de elementos opcionales del protocolo). Los resultados del proceso de negociación de los parámetros se acuerdan por intervalos de tiempo para el mantenimiento del canal de control y el acuerdo del conjunto soportado de capacidades del LMP.

• **El Mantenimiento del Canal de Control**
Implica un continuo intercambio de mensajes Hello entre un par de nodos LMP, con el fin de confirmar que el canal de control está aún operacional. Durante el traspaso de operaciones LMP a un canal de control de reserva, se puede producir un fallo del canal de control. Si ningún canal de control LMP está activo, es imposible estar seguro del estado de los enlaces de datos y el LMP no puede recoger ninguna información adicional.

Los enlaces de datos están marcados como degradados y los componentes de señalización pueden ser avisados de que pueden haber problemas y no ser apropiadamente rectificados. Los componentes de señalización podrían tomar una acción para solucionarlo como el reenrutamiento de los LSPs.

1.4.2 Enlaces TE

Entre un par de conmutadores ópticos puede haber un gran número de fibras ópticas. Dado que es normal el caso de que varias de estas fibras tengan las mismas propiedades en cuanto a los protocolos de enrutamiento corresponden (es decir los mismos puntos extremos, la calidad de servicio, etc.) no tiene sentido inundar la base de datos de enrutamiento con información duplicada de cada fibra individual. Por lo tanto en cuanto a los fines del enrutamiento, las fibras con las mismas propiedades están agrupadas en un enlace TE y solo el enlace TE se anuncia vía enrutamiento.

Sin embargo, si las fibras individuales no son conocidas a través de la información de enrutamiento, los LSRs de GMPLS necesitan una forma de identificar las fibras individuales dentro de un enlace TE, de forma que una señal conmutada en una fibra por el LSR ascendente pueda ser recogida por uno descendente. El LMP cubre esta necesidad suministrando mecanismos para mapear la ID usada en un extremo de una fibra óptica con la ID usada en su otro extremo lo que se conoce como verificación del enlace y agrupando conjuntos de IDs en cualquier extremo de la correspondiente ID del enlace TE lo que se conoce como resumen del enlace.

1.4.3 Verificación del enlace

La Verificación del Enlace tiene dos finalidades una de ellas es la verificación de la conectividad de los datos en determinados enlaces de datos y la otra es la determinación automática del mapeo entre las IDs de las interfaces local y remota tanto para los enlaces de datos como los enlaces TE.

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

El proceso de verificación del enlace implica varios pasos:

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

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

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

• El intercambio de EndVerify / EndVerifyAck.

Los resultados del proceso de verificación del enlace, ilustrados en la figura 9, son la determinación de que enlaces de datos han sido comprobados satisfactoriamente, los mapeos entre las IDs de las interfaces local y remota de los enlaces de datos y los mapeos entre las IDs de las interfaces local y remota de los enlaces TE.

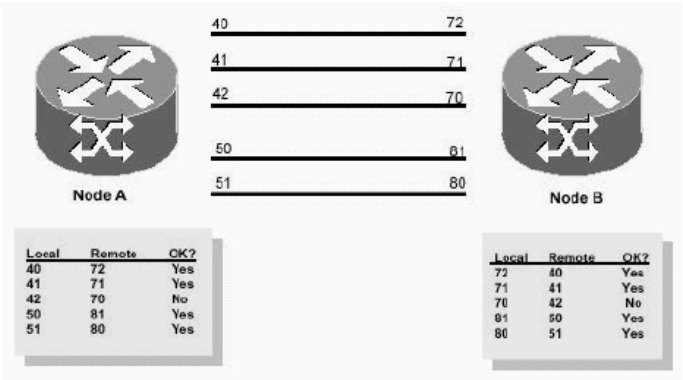


Figura 27. Tabla de verificación de enlace

1.4.4 Resumen de la propiedad del enlace

El principal propósito de esta función es descubrir y acordar entre dos nodos LMP adyacentes los mapeos de las IDs de interfaz y las propiedades de los enlaces de datos. Esto se consigue con el intercambio de los mensajes

LinkSummary / LinkSummaryAck / LinkSummaryNack, cada uno de los cuales contiene múltiples subobjetos.

Los subobjetos de enlace TE indican los mapeos entre las IDs de los enlaces TE local y remoto, junto con otra información sobre los enlaces TE (tales como la protección y la capacidad de multiplexación). Cada Enlace TE agrega múltiples enlaces de datos, indicados por los subsiguientes subobjetos del enlace de datos.

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

Los resultados del proceso de correlación de la propiedad del enlace son entonces la confirmación de que los mapeos entre las IDs de las interfaces local y remota son consistentes entre nodos LMP (que es particularmente importante donde los mapeos han sido pre-configurados mas que determinados dinámicamente vía la verificación del enlace); la confirmación de que la agregación de los enlaces de datos en los Enlaces TE es consistente entre nodos LMP adyacentes y el acuerdo sobre las propiedades y capacidades de los canales de datos.

La agregación de los enlaces de datos en Enlaces TE se ilustra en la figura 28.

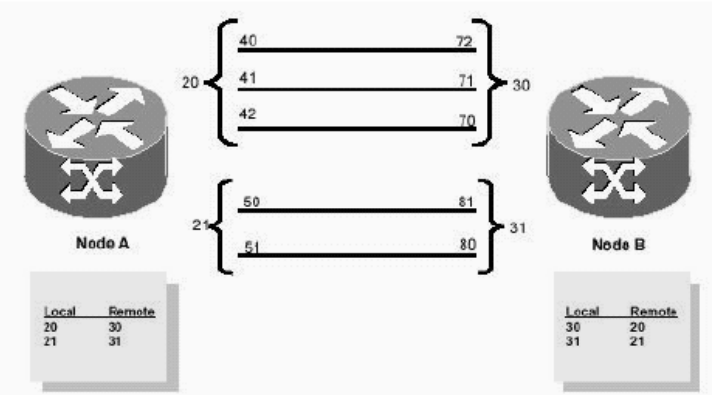


Figura 28. Mapeos del enlace TE

1.4.5 Detección de falla

Los caminos de luz normalmente atraviesan múltiples enlaces de datos que van de la entrada a la salida. Cuando este camino de luz falla, el LMP suministra una manera de localizar que enlace de datos ha fallado.

Muchos conmutadores ópticos fotónicos son transparentes, en el sentido de que propagan la señal de la luz sin ninguna interferencia. Pueden conmutar datos por fibra, longitud de onda o ranura de tiempo sin necesidad de examinar en absoluto la señal actual. Consecuentemente, si la señal desaparece debido a un fallo de algún sitio ascendente, el conmutador puede simplemente no enterarse.

En el peor caso típico, la ausencia de la señal solo es detectada cuando se necesita volverla a convertir en forma electrónica para enviarla sobre una red conmutada de paquetes. Entonces la única información es que hay un fallo en uno de los enlaces ópticos en algún sitio del LSP a través de cual se esperaba la llegada de paquetes.

La detección del fallo LMP se usa en este escenario para localizar el enlace en que ocurrió el fallo y se procede de la siguiente forma:

El proceso se inicia en el nodo descendente que nota primero el fallo en el enlace de datos por tanto este nodo envía un mensaje Channel Failure a su vecino ascendente de este enlace y el nodo ascendente determina que enlace(s) de datos entrante/ascendente se conecta al enlace de datos fallado saliente/descendente, por tanto, si el correspondiente enlace de datos entrante también ha fallado, el nodo ascendente responde con un ChannelFailureAck y propaga el proceso de detección del fallo enviando un nuevo mensaje ChannelFailure al nodo siguiente ascendente. Alternativamente, este nodo puede haber notado el LOL (Loss of Light) por si mismo y así ya ha propagado el ChannelFailure ascendentemente.

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

Los resultados del proceso son la indicación de que ha fallado un determinado enlace de datos y la indicación de si el fallo ha sido localizado en este nodo precisamente, en el enlace descendente a este nodo.

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

1.4.6 Autenticación

La autenticación suministra confirmación criptográfica de la identidad del nodo vecino. Dado que el canal de control entre un par de nodos LMP puede pasar a través de una nube arbitraria IP, incluso Internet, es importante poder autenticar los mensajes que son recibidos por este canal. Para explicar porque esto es necesario, se puede considerar la denegación de servicio que se podría causar enviando un mensaje falso BeginVerify de LMP al conmutador óptico troncal, para instruirlo para empezar la verificación de todos sus enlaces de datos.

Si la verificación de enlace procede, el envío normal de datos estaría suspendido durante la fase de comprobación. Por lo tanto opcionalmente, las sesiones LMP pueden negociar el uso del algoritmo hash MD5 (algoritmo diseñado para comprobar la integridad de los datos en transmisiones de cualquier tipo) que sirve para autenticar los mensajes de control.

Cuando se acuerda la autenticación, cada mensaje de control se firma añadiéndole una firma de 16 octetos calculada de una clave secreta

compartida y un hash MD5 (una huella digital del mensaje donde no existe información alguna de la cadena original) de los contenidos del mensaje