UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA
UNAN-MANAGUA
RECINTO UNIVERSITARIO RUBEN DARIO
FACULTAD DE CIENCAS E INGENERIAS
DEPARTAMENTO DE TECNOLOGIA

TRABAJO FINAL DE SEMINARIO DE GRADUACION PARA OPTAR AL TITULO DE INGENIERO ELECTRONICO

EVALUACIÓN DE LAS PRESTACIONES OFRECIDAS POR EL PROTOCOLO PCEP (PATH COMPUTATIÓN ELEMENT PROTOCOL) EN LAS REDES DE TRASPORTE DE DATOS CON TECNOLOGÍA DE TRASMISIÓN GMPLS.

ELABORADO POR

- **Br. Álvaro Uriel Acuña Gaitán**
- **Br. Martha padilla**

Tutor: MsC. Álvaro Segovia

Managua, Nicaragua FEBRERO 2013.

TEMA

ANÁLISIS DE TECNOLOGÍA DE TRANSPORTE DE DATOS.

SUB TEMA

EVALUACIÓN DE LAS PRESTACIONES OFRECIDAS POR EL PROTOCOLO PCEP (PATH COMPUTACIÓN ELEMENT PROTOCOL) EN LAS REDES DE TRASPORTE DE DATOS CON TECNOLOGÍA DE TRASMISIÓN GMPLS.

DEDICATORIA

Dedico este trabajo principalmente a Dios por darnos la vida y permitirnos llegar hasta esta etapa. A nuestros Padres, a mi abuelos Francisco Gaitán Jalinas , a mis tías Ángela María Gaitán Cano, Auxiliadora Gaitán Cano y muy especial a Heriberto Antonio Gaitán Cano por haberme motivado a seguir estudiando que dios lo tenga en su santo reino, por haberme brindado siempre su apoyo, ayuda y comprensión incondicional a lo largo de nuestros estudios. A nuestros Maestros por compartir sus conocimientos y corregirnos siempre para hacerlo mejor a lo largo de nuestra carrera. A mis hermanas y amigos por habernos brindado apoyo y comprensión para poder culminar con este proyecto.

AGRADECIMIENTO

En primer lugar le damos las gracias a nuestro Dios padre misericordioso por darnos el regalo de la vida, darnos fuerza, fortaleza, sabiduría, y dedicación para finalizar este trabajo que es la culminación de estudios de nuestra carrera. A nuestros Padres por su apoyo y comprensión en todas las etapas de nuestros estudios. A todos nuestros Maestros que nos instruyeron a lo largo de nuestra carrera, en especial a nuestro tutor Msc. Álvaro Segovia por habernos brindado su apoyo e instruirnos en el transcurso de la ejecución y redacción de nuestro tema para lograr una buena formación de hábitos necesarios para una preparación profesional. También le agradecemos al Msc. Sergio Sacasa por habernos brindado su colaboración en la fase metodológica de nuestro trabajo.

DEDICATORIA

Dedico este trabajo especialmente al dador de la vida al maestro de maestros a nuestro creador y padre celestial, a mis tías, padres, primas cada uno de los cuales fueron instrumentos para llegar al final.

AGRADECIMIENTO

Quiero agradecer a Dios por la vida y fuerza que me ha otorgado hasta este momento a mi familia por su apoyo y por la confianza que depositaron en mí, a mis amigos por incondicional ayuda y ánimo para continuar por sus palabras de aliento, a la congragación por sus contantes oraciones, a cada uno de nuestros profesores que fueron nuestros guías a lo largo de este caminar

"***el principio de la sabiduría es el temor al señor"***

RESUMEN

En este trabajo se hace un análisis del protocolo PCEP (Path Computación Element Protocol),es un protocolo petición/respuesta que permite la comunicación entre redes multicapa, multidominio, y con diferentes áreas, GMPLS es una evolución del plano de control de MPLS hacia un Plano de Control Común que simplifica el funcionamiento y mantenimiento de una red multicapa con cualquier sistema de transporte (incluso mixto), asegurando la interoperabilidad entre los dispositivos de alto nivel (routers) y los de bajo nivel(OXC, PXC, etc.). GMPLS consiste es un método que contiene una serie de especificaciones usadas para enrutar los paquetes a través de una red por medio de datos adicionales que se encuentran en unas etiquetas añadidas a los paquetes IP. Esto hace que los routers sepan porque camino exactamente deben enviar los datos que le lleguen aumentando la calidad del servicio, el desempeño de las redes y la estabilidad.

El PCEP está basado en un modelo cliente-servidor en el cual un PCC(Path Computation Client) puede enviar un mensaje de petición de cálculo a un PCE(Path Computation Element) y éste responde con otro mensaje que contiene la ruta calculada. PCE calcula la ruta aplicando un algoritmo de computación denominado Dijkstra. Este algoritmo tiene dos fases, en la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una Constrained-TEDase de datos de ingeniería de tráfico)

GMPLS puede verse por tanto, como un integrador de tecnologías, permitiendo la transmisión de información entre los diferentes tipos de redes y unificando el control del tráfico.

Con la evolución de la tecnología se da paso al mejoramiento de las redes de trasporte las cuales son muy relevantes ante la necesidad de sistemas más flexibles y unificados. Por tanto con el análisis de la tecnología GMPLS se estudiara que con la implementación de este medio de transporte en los diferentes tipos de redes la información transmitida sea lo más transparente posible frente al despliegue de nuevas aplicaciones de interés para los usuarios, es decir que sean válidas para cualquier nueva aplicación sin cambios

significativos y retardos que puedan impedir cumplir las expectativas de los usuarios.

GMPLS está basado en enrutamiento IP y modelos de direccionamiento. Esto asume que las direcciones IPv4 y/o IPv6 se usan para identificar interfaces pero también se usan protocolos de enrutamiento IP tradicionales tales como OSPF y el IS IS. El OSPF utiliza el algoritmo Ruta de acceso más corta primero (SPF, Shortest Path First) para calcular rutas en la tabla de enrutamiento. El algoritmo SPF calcula las rutas de acceso más cortas (menos costo) entre el enrutador y todas las redes de la interconexión. Las rutas calculadas mediante SPF nunca presentan bucles, IS-IS y OSPF, son protocolos de estado de enlaces que utilizan el Algoritmo de Dijkstra para encontrar el mejor camino a través de la red. Ambos soportan máscaras de subred de diferente longitud, pueden usar multicast para encontrar routers vecinos mediante paquetes hello y pueden soportar autentificación de actualizaciones de encaminamiento. El protocolo OSPF bien podría ser el más utilizado en redes corporativas grandes, mientras que el protocolo IS-IS es más común en redes de proveedores de servicios. OSPF solamente enruta paquetes IP dentro de un único dominio.

INDICE

Pagina.

CAPITULO 3

PCEP (Path Computation Element Protocol) como posible medio de transmisión basado en la arquitectura petición repuesta como un sistema unificado e integrado en el enrutamiento de paquetes con tecnología GMPLS……**25**

Capitulo 4

Presentar mediante el estudio del protocolo PCEP (Path Computation Element Protocol) el impacto que este presenta en las redes de próxima generación para obtener el cálculo óptimo de rutas en un entorno de red……**34**

INTRODUCCIÓN

PCEP (Path Computación Element Protocol).es un protocolo petición/respuesta que permite la comunicación entre redes multicapa, multidominio, y con diferentes áreas, GMPLS es una evolución del plano de control de MPLS hacia un Plano de Control Común que simplifica el funcionamiento y mantenimiento de una red multicapa con cualquier sistema de transporte (incluso mixto), asegurando la interoperabilidad entre los dispositivos de alto nivel (routers) y los de bajo nivel(OXC, PXC, etc.).. GMPLS consiste es un método que contiene una serie de especificaciones usadas para enrutar los paquetes a través de una red por medio de datos adicionales que se encuentran en unas etiquetas añadidas a los paquetes IP. Esto hace que los routers sepan porque camino exactamente deben enviar los datos que le lleguen aumentando la calidad del servicio, el desempeño de las redes y la estabilidad.

El PCEP está basado en un modelo cliente-servidor en el cual un PCC(Path Computation Client) puede enviar un mensaje de petición de cálculo a un PCE(Path Computation Element) y éste responde con otro mensaje que contiene la ruta calculada. PCE calcula la ruta aplicando un algoritmo de computación. Este algoritmo tiene dos fases, en la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una Constrained-TED(base de datos de ingeniería de trafico) temporal en la cual solo figuran los enlaces que satisfacen las condiciones. En la segunda fase se aplica el algoritmo matemático a esta nueva TED y se calcula la ruta óptima según el criterio de optimización deseado (ruta más corta, enlaces menos cargados, etc.).
La ingeniería de tráfico consiste en trasladar parte del tráfico de los enlaces más congestionados a otros enlaces menos cargados, aunque estén fuera de la ruta con menos saltos.
En el estándar MPLS [RFC 3031] existe una separación entre el plano de datos y el plano de control, esta separación se realiza de manera lógica sobre la misma red MPLS.
En GMPLS esta separación puede ser de manera lógica o física. En una separación lógica los tráficos de datos y de control viajan sobre la misma red. Una separación física significa que el control de la red de datos se realiza a través

de otra red externa, que puede ser diferente a la primera. Para ser capaz de soportar dispositivos con diferentes tipos de conmutación, GMPLS introduce el concepto de “etiqueta generalizada” (generalized label). Este nuevo formato de etiqueta puede representar un paquete, una celda/frame, un *slot* de tiempo, una longitud de onda o una fibra. La longitud de la etiqueta generalizada, así como su formato y contenido dependen del tipo de conmutación del enlace.
En la práctica, un dominio o área contiene múltiples PCE. Para conseguir que los PCC seleccionen de manera efectiva los PCE, se elige un PCE apropiado en base a sus capacidades y repartir eficientemente la carga de peticiones, un PCC debe conocer la localización y características de todos los PCE dentro de su área, o incluso fuera del dominio si se permite. El mecanismo de descubrimiento PCE debe permitir la localización de cada PCE, identificado por una dirección IP en cada área, también identificada por un “Area_ID”.

GMPLS puede verse por tanto, como un integrador de tecnologías, permitiendo la transmisión de información entre los diferentes tipos de redes y unificando el control del tráfico. Con la evolución de la tecnología se da paso al mejoramiento de las redes de trasporte las cuales son muy relevantes ante la necesidad de sistemas más flexibles y unificados. Por tanto con el análisis de la tecnología GMPLS se estudiara que con la implementación de este medio de transporte en los diferentes tipos de redes la información transmitida sea lo más transparente posible frente al despliegue de nuevas aplicaciones de interés para los usuarios, es decir que sean válidas para cualquier nueva aplicación sin cambios significativos y retardos que puedan impedir cumplir las expectativas de los usuarios.

JUSTIFICACION

La transmisión de datos ha sido una de las mayores necesidades que se ha establecido en la actualidad por lo cual los proveedores de redes y de servicios de redes enfrentan retos cada vez mayores, debido a que internet a estado creciendo a una razón exponencial en términos de equipos, dominios y trafico provocando saturación en la estructura de las redes. Las redes troncales están migrando hacia un esquema de redes de nueva generación. Estas redes se utilizan para soportar todo tipo de servicios, por lo que deben ser capaces de soportar múltiples calidades de servicio.

Tradicionalmente las redes troncales se gestionaban de forma centralizada, de manera que los elementos de red eran configurados estáticamente. En estos últimos años se han hecho grandes esfuerzos en la creación de un plano de control común mediante la estandarización de Generalized Multi-Protocol Label Switching (GMPLS), que proporciona configuración dinámica y distribuida de la capa óptica. Sin embargo, el cálculo de caminos en redes ópticas es una tarea compleja en términos de computación al tener en cuenta las restricciones adicionales de los elementos de red ópticos. Cuando dicha tarea deben realizarla los controladores GMPLS, se hace necesario contar con equipos con suficientes recursos computacionales y, por tanto, el coste de los mismos aumenta.

Es por ello que el protocolo PCEP nace como iniciativa del IETF (Internet Engineering Task Force) para tratar el problema del cálculo de rutas usando una serie de variables y restricciones, el cual se evalúa en la actualidad como un elemento capaz de realizar y soportar cualquier tipo de tráfico. Para solucionarlo la IETF ha desarrollado la arquitectura PCEP que permite calcular rutas de una manera simple y eficiente. Esta arquitectura introduce una entidad especial de cálculo (componente, aplicación o nodo de red) que coopera con entidades similares para calcular la mejor ruta posible aplicando restricciones computacionales, así como asegura la coordinación entre ellos ofreciendo de esta manera un plano de control integrado, el cual extiende el conocimiento de la topología y la gestión de ancho de banda a lo largo de todas las capas de red permitiendo de forma efectiva la consolidación de los servicios y el transporte.

El propósito de tener un plano de control es proporcionar elementos de red (enrutadores IP) con la capacidad de solicitar conexiones dinámicas a otro elemento lo que aumenta la flexibilidad. El plano de control es una entidad que realiza llamadas y control de conexiones, las establece, las elimina y las restaura en caso de falla a través de la señalización. En resumen el plano de control es la parte que implementa el enrutamiento, realiza las funciones de señalización y procesamiento de rutas que son asociadas con el plano de datos.

OBJETIVOS

GENERAL

- Analizar el protocolo PCEP (Path computation element protocol) en las redes de transporte de datos con tecnología de trasmisión GMPLS.

ESPECÍFICOS

- Describir los servicios y prestaciones que ofrece el protocolo PCEP (Path Computation Element Protocol) como medio de transporte de datos utilizando la tecnología GMPLS.

- Analizar el protocolo PCEP (Path Computation Element Protocol) como un mecanismo de comunicación que permita mejorar la eficiencia y escalabilidad en la optimización de la redes de transporte de datos utilizando la tecnología GMPLS.

- Determinar el protocolo PCEP (Path Computation Element Protocol) como posible medio de transmisión basado en la arquitectura petición repuesta como un sistema unificado e integrado en el enrutamiento de paquetes con tecnología GMPLS.

- Presentar mediante el estudio del protocolo PCEP (Path Computation Element Protocol) el impacto que este presenta en las redes de próxima generación para obtener el cálculo óptimo de rutas en un entorno de red.

4 DESARROLLO

4.13 GMPLS

Generalized Multi-Protocol Label Switching (GMPLS) son el resultado de grandes esfuerzos en los últimos años en la definición de plano para redes ópticas.

Uno de los objetivos principales de esta arquitectura es extraer la capacidad de cómputo de rutas de los nodos que actualmente hacen esta labor y, de esta forma, éstos pueden ser más simples y baratos.

Simultáneamente, en la red se situarán unos pocos nodos dedicados llamados PCE que serán los encargados del cómputo de rutas para aquellos nodos que lo requieran. Estos elementos PCE pueden ser dotados con capacidades de encaminamiento avanzadas que tengan en cuenta restricciones de ingeniería de tráfico y que satisfarán todas las necesidades de cómputo de los dominos clientes.

Con el Análisis y Evaluación del Servicio del protocolo PCEP se destacaran las principales características, conceptos, ventajas y su funcionamiento, En una arquitectura basada en el modelo PCEP hay, al menos, un PCE en cada dominio. Sin embargo, un dominio puede contener múltiples PCEs para facilitar el balanceo de carga y evitar puntos únicos de fallo. El PCE recibe solicitudes de cálculo de caminos desde los Path Computation Clients (PCC). Para atenderlas, necesita información actualizada del estado de la red, la cual almacena en la Base de Datos de Ingeniería de Trafico (Traffic Engineering Database - TED)Dicha arquitectura proporciona la funcionalidad necesaria para el cálculo de caminos óptimos con ingeniería de tráfico en redes GMPLS. Además de liberar a los nodos de la red de las tareas de computo, se debe asegurar que el trafico llegue a su destino con seguridad, fiabilidad y optimizando los recursos de la red sobre la que viaja.

GMPLS puede verse, como un integrador de tecnologías, permitiendo la transmisión de información entre los diferentes tipos de redes y unificando el control del tráfico. El principal beneficio que GMPLS ofrece actualmente a los ISPs es una rápida provisión de servicios de cualquier tipo, en cualquier momento, a cualquier destino, con cualquier calidad de servicio, con cualquier grado de disponibilidad y con un coste operativo muy bajo.

PCE calcula la ruta aplicando un algoritmo de computación. Este algoritmo tiene dos fases, en la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una Constrained-TED temporal en la cual solo figuran los enlaces que satisfacen las condiciones. En la segunda fase se aplica el algoritmo matemático a esta nueva TED y se calcula la ruta óptima según el criterio de optimización deseado (ruta más corta, enlaces menos cargados, etc.) de datos (plano de tráfico), ahora puede diversificar para incluir más variedades de tráfico (TDM, Lambda, paquetes, fibra, etc.). Los dispositivos GMPLS son capaces de gestionar cinco tipos de interfaces:

- **Conmutación de paquetes:** Basada en el contenido de la cabecera del paquete (nivel 3).
- **Conmutación de celdas y/o frames:** Basada en el contenido de la cabecera de la celda o frame (nivel 2).
- **Conmutación en tiempo (TDM):** Basada en el slot temporal de un ciclo repetitivo en el que se reciben los datos.
- **Conmutación de longitud de onda (DWDM):** Basada en la longitud de onda en la que se reciben los datos.
- **Conmutación en el espacio:** basada en la fibra o puerto por la que se reciben los datos.

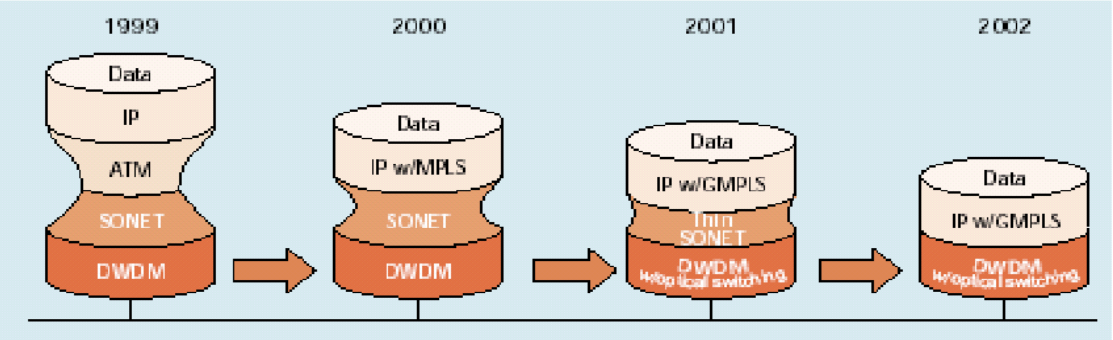

Fig. 1 Evolución de redes

4.14 Arquitectura GMPLS

GMPLS existe una separación entre el plano de datos y el plano de control, en gmpls esta separación puede ser de manera lógica o física En una Separación lógica los tráficos de datos y de control viajan sobre la misma red.

Una separación física significa que el control de la red de datos se realiza a través de otra red externa, que puede ser diferente a la primera. Por ejemplo una red de datos óptica con un plano de control sobre una red IP tradicional. Etiqueta generalizada Para ser capaz de soportar dispositivos con diferentes tipos de conmutación, GMPLS introduce el concepto de "etiqueta generalizada" (generalized label). Este nuevo formato de etiqueta puede representar un paquete, una celda/frame, un slot de tiempo, una longitud de onda o una fibra. La longitud de la etiqueta generalizada, así como su formato y contenido dependen del tipo de conmutación del enlace.

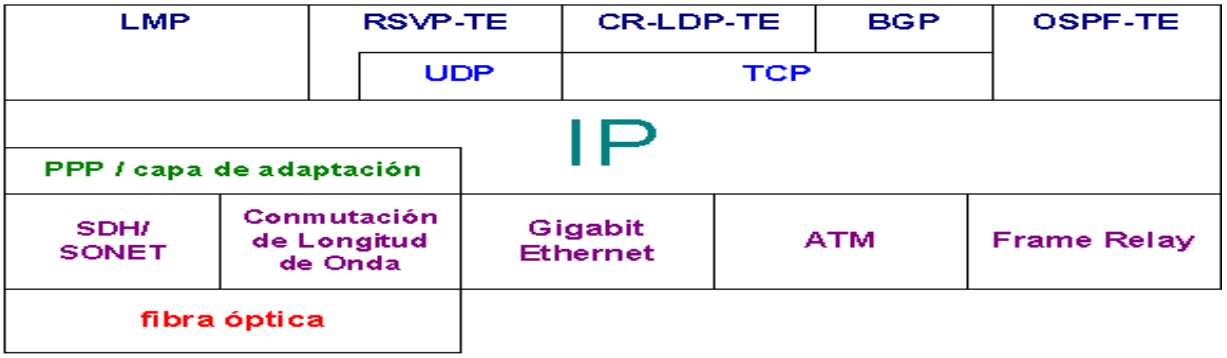

Fig 2. Pilas de protocolo Gmpls

CAPITULO 1

Servicios y prestaciones que ofrece el protocolo PCEP (path computation element protocol) como medio de transporte de datos utilizando GMPLS

Los protocolos de encaminamiento son los encargados de calcular la ruta entre dos puntos de red, con unas determinadas condiciones o restricciones (constraints) para la transmisión de un cierto tráfico. Para realizar este cálculo, es necesario conocer la topología y los recursos de la red.

.

PCEP es un nuevo elemento en las redes GMPLS, se fundamenta en un algoritmo que calcula la ruta más óptima aplicando restricciones en escenarios complejos de grandes redes multicapas, multidominios, con diferentes áreas para optimizar el cálculo de las rutas al ser una entidad centralizada.

El PCEP es un protocolo basado en la arquitectura petición/respuesta que opera sobre el protocolo TCP. Al momento de calcular una ruta aplicando la ingeniería de trafico PCEP toma en cuenta la disponibilidad de recursos (ancho de banda disponible, malla de red, entre otros) restricciones administrativas, entre otros. Una vez definidos todos estos parámetros PCEP calcula una ruta aplicando un algoritmo de computación denominado Dijkstra

Este algoritmo tiene dos fases. En la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una Constrained-TED temporal en la cual solo figuran los enlaces que satisfacen las condiciones. En la segunda fase se aplica el algoritmo matemático a esta nueva TED y se calcula la ruta óptima según el criterio de optimización deseado (ruta más corta, enlaces menos cargados, etc.).

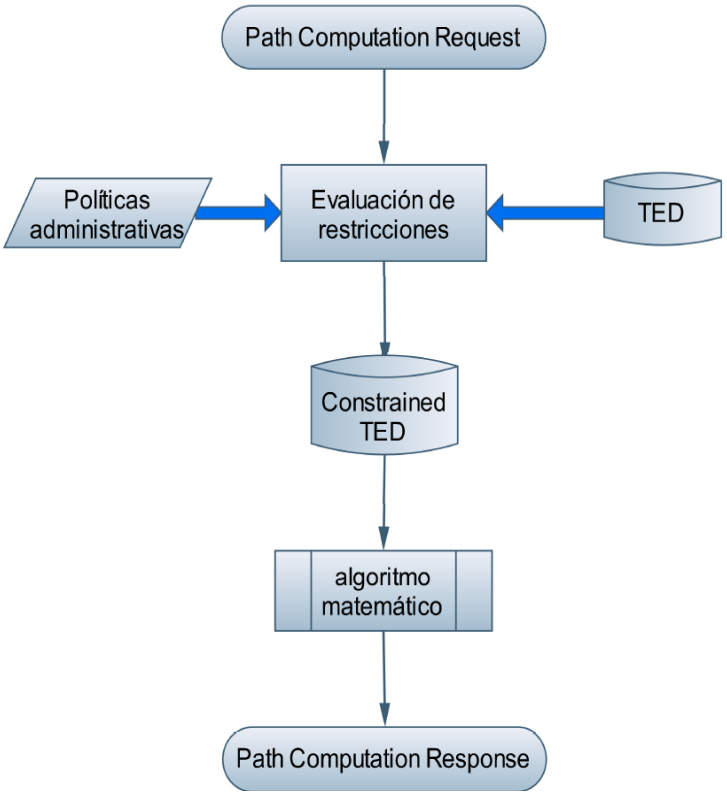

Figura 3. Diagrama de flujo de un PCE

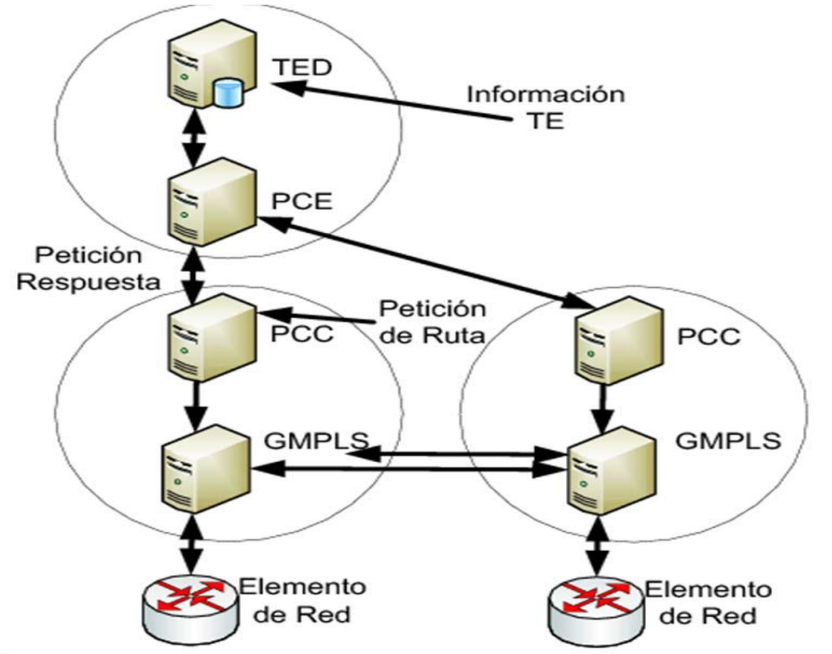

Figura 4. Arquitectura PC

Son diferentes situaciones que sugieren el uso de una arquitectura de red basada en PCE. Estas son algunas de ellas:

4.15 Capacidad de procesado limitada

En ocasiones el cálculo de ruta puede resultar tan complejo que algunos LSRs no dispongan de la capacidad de procesado suficiente para realizar la operación, delegando esta tarea en el PCE, que sí tiene los recursos necesarios.

4.15.1 Visibilidad limitada

En redes con diferentes dominios y/o capas, el conocimiento sobre la red de los LSRs se limita a su propia zona o capa, lo que no siempre puede garantizar la elección de la ruta óptima. La solución puede ser un PCE que tenga acceso a toda la topología de la red, o varios PCEs repartidos en las diferentes regiones y comunicados entre sí.

4.15.2 Ausencia de TED

El mantenimiento de la TED requiere el uso de mucha memoria. Es por ello que en una red con ingeniería de tráfico aplicada puede haber nodos que no soporten las extensiones TE de los protocolos de encaminamiento. En este caso es necesario que la TED sea suministrada externamente por un PCE.

4.15.3 Ausencia de capacidad de enrutado

En las redes ópticas son habituales los dispositivos que no disponen de plano de control o capacidad de routing, como pueden ser los conmutadores fotónicos (transparentes). El PCE es el encargado de enviar a estos nodos los comandos de configuración de hardware correspondientes.

4.15.4 Cálculo de rutas alternativas

Un PCE puede ser usado para calcular rutas alternativas para el rápido restablecimiento de un LSP en caso de que la ruta principal falle.

4.16 Elementos de red

4.16.1 Path Computation Client PCC

Cualquier LSR de la red que requiere a un PCE el cálculo de una ruta de acuerdo al servicio solicitado.

4.16.2 Path Computation Element PCE

Aplicación que realiza el cálculo de ruta de acuerdo a una petición. Al finalizar el cálculo, el PCE envía la información de dicha ruta al PCC.

4.16.3 Traffic Engineering Database TED

Tabla de encaminamiento con ingeniería de tráfico aplicada que utiliza un PCE para realizar el cálculo de rutas.

4.16.4 Path Computation Request

Petición de cálculo de ruta que envía un PCC al PCE.

4.16.5 Path Computation Response

Respuesta que envía el PCE al PCC con la información de la ruta calculada.

4.17 Estructura PCE

La aplicación PCE puede estar implementada en cualquier nodo de la red (composite), o en un servidor dedicado (external). En este segundo caso, el PCE "escucha" de manera pasiva toda la información del protocolo de encaminamiento que intercambian los LSR para mantener actualizada su TED.

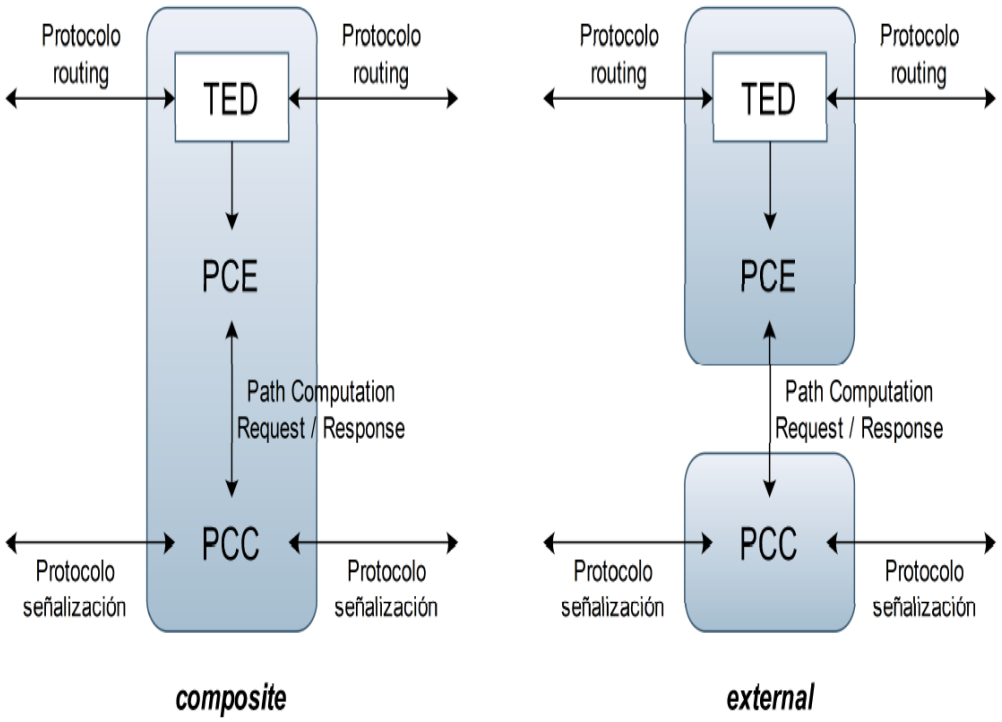

Figura 5. PCE composite y external

Existen dos modos de funcionamiento del PCEP, el intermitente y el permanente. El modo intermitente abre y cierra sistemáticamente una sesión PCEP para cada petición de ruta, esta modalidad es aplicable cuando el envío de una petición es un evento raro.

En el modo permanente, se mantiene establecida la sesión PCEP y su correspondiente conexión TCP por un intervalo de tiempo ilimitado, esta modalidad resulta apropiada cuando las peticiones de ruta se envían de forma

frecuente. Este modo evita abrir y cerrar una conexión TCP para cada nueva petición reduciendo así la carga adicional.

El PCE puede estar en el plano de gestión, siendo parte de un sistema de gestión de red (Network Management System -NMS) tal que dada una petición de servicio, el NMS solicita una ruta al PCE. Para calcular la ruta más adecuada, el PCE requiere la información de estado de la red, la cual esta almacenada en una base de datos de ingeniera de tráfico (TED).
Una vez que el PCE provee una respuesta al NMS, la configuración es enviada a los elementos de red para configurar el servicio.

4.18 Modelo de red

En un modelo centralizado, un único PCE es el que recibe las peticiones de todos los PCCs de un mismo dominio o área. Por seguridad, se puede designar un PCE alternativo (*backup*) que tome el control en caso de fallo del PCE primario. En un modelo distribuido, múltiples PCEs residen en una misma área. Cada PCC puede estar ligado a un particular PCE, o puede ser libre de elegir entre varios. En el caso extremo, cada LSR tiene su propio PCE En la práctica, un dominio o área contiene múltiples PCEs. Para conseguir que los PCCs seleccionen de manera efectiva los PCEs, esto es, elegir un PCE apropiado en base a sus capacidades y repartir eficientemente la carga de peticiones, un PCC debe conocer la localización y características de todos los PCEs dentro de su área, o incluso fuera del dominio si se permite.

El mecanismo de descubrimiento (PCE *discovery mechanism*) [43] debe permitir la localización de cada PCE, identificado por una dirección IP, en cada área, también identificada por un “Area_ID”. También debe informar de las características y capacidades de cada PCE.

Algunas de ellas son:

- Potencia de cálculo (parâmetros estáticos).
- Priorización de las peticiones.

- Capacidad de cálculo sincronizado.
- Tamaño máximo del mensaje de petición.
- Número máximo de solicitudes de ruta en un mensaje de petición.
- Tipos de cálculo de ruta soportados: ruta más corta, ruta por los enlaces menos cargados, etc.
- Restricciones de ruta soportadas: máximo número de saltos, máximo coste, etc.
- Restricciones de enlace soportadas: ancho de banda, latencia, etc.
- Capacidad de cálculo de LSP bidireccionales.
- Tipos de conmutación y capas soportados.

Tanto la localización como las características de los PCEs se pueden configurar manualmente en cada PCC. Pero esta opción puede ser muy laboriosa en grandes redes, y además no permite el descubrimiento de nuevos PCEs, la eliminación de los no-disponibles, o el cambio dinámico de las características de alguno de ellos. En este contexto es de aplicación un mecanismo dinámico de autodescubrimiento. Tanto si un PCE reside en un LSR como si está en un servidor externo, la manera más sencilla y efectiva de darse a conocer es mediante el sistema de inundación (*flooding*). Se añade además un sistema de temporización que permite a un PCC monitorizar la conectividad con el PCE y detectar fallos en la comunicación entre ambos.

Para todo ello, la IETF define una serie de extensiones en los Link State Advertisements (LSA) de los protocolos de encaminamiento OSPF-TE e IS-ISTE RFC 5088] y [RFC [5089].

El PCE puede estar integrado en el mismo equipo que el PCC o puede estar separado del servidor. La solución conjunta en un único servidor es fácil de implementar y no requiere un protocolo estándar de comunicaciones entre el PCC y PCE. En el otro caso, la solución de servidor separado usa el protocolo estándar basado en el esquema petición/respuesta y permite que una única entidad PCE de servicio a múltiples PCCs

La arquitectura del PCE encaja bien para abordar el problema del establecimiento de rutas multidominio. El modelo de interconexión para un escenario multidominio se provee una visión general de los desarrollos en el área de ingeniería de tráfico basado en PCE en redes GMPLS además de un análisis detallado del enfoque de redes PCE en redes multidominio y comparan el rendimiento de las soluciones existentes

Se han definido esquemas del PCE para entornos multicapas. Una red multicapas es una red donde existen varias tecnologías de red. Para este tipo de redes existen, dos modelos de interconexión centralizados y dos modelos distribuidos. Los dos modelos centralizados son los siguientes

4.18.1 PCE único multicapas

Esta arquitectura tiene un PCE único capaz de almacenar la información de todas las capas de la red. Este PCE puede estar en cualquier lugar en un plano de control integrado o en un plano de gestión.

4.18.2 PCE/VNTM (Virtual Network Topology Manager)

El VNTM muestra una topología de red a la capa superior. La capa superior (IP; PCE) puede pedir conexiones extras a la capa inferior. El VNTM puede cambiar las conexiones a la capa superior si sus políticas indican que es la mejor opción. El modo de operación de VNTM podría ser cualquier solución, incluso otro PCE. En cuanto a las soluciones distribuidas se pueden distinguir las siguientes:

4.18.3 Multicooperacion de PCEs de capa única

Esta opción usa un PCE en cada capa y estos pueden intercambiar peticiones cuando estas son requeridas. Debido a este intercambio de peticiones la capa superior puede pedir conexiones a la capa inferior para que puedan modificar la

topología de la capa superior. Además como hay dos PCEs, la solución reduce la complejidad de cálculo en los algoritmos de cada PCE.

4.18.4 Múltiples PCE multicapas

Esta arquitectura tiene múltiples PCEs multicapas de manera que los PCEs disponen información de cada capa de la red. Los PCCs pueden solicitar un cálculo de ruta a cualquiera de los PCEs, pero en general se realiza al más cercano. Una segunda opción es que el PCC envía consultas a un PCE el cual balancea las solicitudes a los otros PCE, lo que reduce el tiempo de cálculo.

Un PCE es capaz de computar LSPs (Label Switched Paths) sobre su propio dominio. Sin embargo, cuando el destino de la ruta solicitada no forma parte de su dominio, se hace necesaria la colaboración entre PCEs de diferentes dominios Dichos PCEs pueden cooperar de igual a igual o de manera jerárquica. Cada uno es el responsable de calcular el segmento del camino perteneciente a su dominio, ya que dispone de la información necesaria para ello.

4.19 Plano de control GMPLS

El propósito de tener un plano de control es proporcionar elementos de red (enrutadores IP) con la capacidad de solicitar conexiones dinámicas a otro elemento lo que aumenta la flexibilidad. El plano de control es una entidad que realiza llamadas y control de conexiones, las establece, las elimina y las restaura en caso de falla a través de la señalización. En resumen el plano de control es la parte que implementa el enrutamiento, realiza las funciones de señalización y procesamiento de rutas que son asociadas con el plano de datos.

4.20 Descripción Funcional PCEP

Para realizar el cálculo de una ruta aplicando la ingeniería de tráfico, el PCEP debe tomar en cuenta un conjunto de restricciones. Por un lado están los recursos disponibles (malla de red, dispositivos, anchos de banda disponibles, etc.) que están reflejados en la TED. Por otro lado los requisitos demandados para el

establecimiento de un LSP (ancho de banda solicitado, número de saltos máximo, retardo permitido, etc.) además de posibles restricciones por políticas administrativas.

Con todos estos parámetros, el PCEP calcula la ruta aplicando un algoritmo de computación. Este algoritmo tiene dos fases. En la primera fase se comparan los requisitos demandados con los recursos disponibles, y se construye una Constrained-TED temporal en la cual solo figuran los enlaces que satisfacen las condiciones. En la segunda fase se aplica el algoritmo matemático a esta nueva TED y se calcula la ruta óptima según el criterio de optimización deseado (ruta más corta, enlaces menos cargados, etc.).

El protocolo consta de 7 posibles mensaje: Open, Keepalive, Request, Responde Notify, Error y Close.

Fase de inicialización: La fase de inicialización consiste en dos pasos sucesivos, primero la creación de una conexión TCP y segundo el establecimiento de una sesión PCEP sobre TCP. Una vez que la conexión TCP ha sido establecida, el PCC y el PCE (conocido como pares PCEP), inician el establecimiento de una sesión PCEP en el que se negocian varios parámetros establecidos en el mensaje Open que incluyen un temporizador Keepalive, un temporizador Dead Timer y potencialmente otras capacidades y políticas detalladas que especifican las condiciones bajo las cuales se envían las solicitudes del cálculo de ruta al PCE.

4.20.1 Arquitectura PCEP

El PCE es una entidad (componente, aplicación, o nodo de red) capaz de calcular una ruta de red aplicando restricciones, por lo que se ha definido una gran cantidad de modos de operación. A continuación se presenta la localización del PCE dentro de las redes de próxima generación, así como su integración en escenarios multicapa y multidominio.

- **Localización:** Para calcular la ruta más adecuada, el PCE requiere la información de estado de la red, la cual esta almacenada en una base de datos de ingeniería de tráfico (TED). Una vez que el PCEP provee una

respuesta al NMS, la configuración es enviada a los elementos de red para configurar y brindar el servicio. Esta situación se muestra en la siguiente figura.

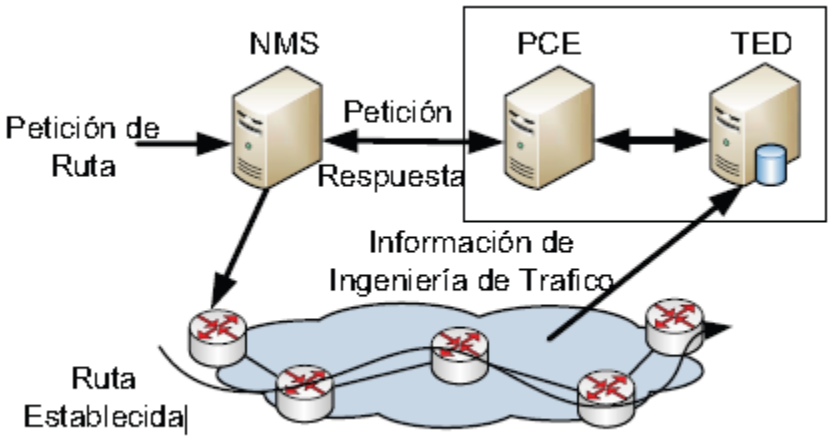

Figura 6 arquitectura PCEP

El equipo que solicita las rutas al PCEP se denomina Path Computation Client (PCC). Usualmente el PCC es un enrutador GMPLS que puede computar una ruta de un camino distribuido usando el algoritmo de encaminamiento estandar GMPLS. Para que el PCEP pueda calcular la ruta debe conocer el estado de la red, para ello se puede utilizar la información de inundación de OSPF y se almacena en una TED. El PCEP puede estar integrado en el mismo equipo que el PCC o puede estar separado del servidor. Ambos casos se muestran en la Fig. La solución conjunta en un único servidor es fácil de implementar y no requiere un protocolo estándar de comunicaciones entre el PCC y PCE. En el otro caso, la solución de servidor separado usa el protocolo estándar basado en el esquema petición/respuesta y permite que una única entidad PCEP.

4.20.2 Protocolos PCEP

Para dar soporte a la nueva tecnología GMPLS y ofrecer la funcionalidad de ingeniería de tráfico, la IETF ha evolucionado dos protocolos del tipo enlace-estado en donde cada router posee información acerca de la totalidad de la

topología y estado de la red. De esta manera, cada uno puede calcular el siguiente salto a cada posible nodo destino de acuerdo a su conocimiento sobre los enlaces (Link State Database LSD). La ruta final será entonces una colección de los mejores saltos posibles entre nodos.

OSPF-TE e IS-IS-TE son muy parecidos en cuanto a funcionamiento. Ambos utilizan el sistema de Link State Advertisements (LSA) para obtener la información sobre la red y construir la LSD. Los LSA son un conjunto de mensajes que envían los LSR por mecanismo de inundación (flooding) de manera periódica, que les permite darse a conocer unos a otros y descubrir nuevos nodos, intercambiar información sobre los enlaces, detectar fallos para tener actualizadas las LSD.

Para evitar problemas de escalado y un excesivo tráfico de routing, las redes se subdividen en áreas o zonas que limitan el flooding, donde cada LSR está identificado de manera única por su dirección IP. A los que no poseen una dirección IP se les denomina “unnumbered”, y se les asocia un identificador ID también único.

El siguiente paso es construir la tabla de encaminamiento o árbol de encaminamiento. Cada LSR calcula la ruta más corta (shortest path) hasta cualquier otro nodo (dentro de la misma área) aplicando el algoritmo de Dijkstra o una variante. Cuándo se produce una variación en la LSD, se re calcula sólo la parte de la tabla/árbol afectada por los cambios. Para implementar la funcionalidad de Ingeniería de Tráfico, la IETF define posteriormente el concepto de “Opaque LSA”. En ellos se incluye información como:

- Ancho de banda máximo, ancho de banda reservable y ancho de banda disponible o no-reservado de un enlace.
- Tipo(s) de conmutación de un nodo.
- Protección Capability: un enlace pueden proporcionar protección a la comunicación teniendo más de una conexión física entre dos puntos.
- Shared Risk Link Groups (SRLG): grupo de enlaces que comparten los mismos recursos físicos, donde un fallo puede afectar a todos.

Con toda esta información añadida, los LSRs pueden construir la Traffic Engineering Database (TED), que no es otra cosa que la tabla de encaminamiento con ingeniería de tráfico aplicada

4.20.3 Tipos de conmutación y jerarquía de transmisión que utiliza PCEP

1. Packet Switch Capable (PSC) interfaces

Interfaces que reconocen el límite de los paquetes y pueden mandar datos basándose en el contenido de sus cabeceras. Se trata de los routers que transmiten datos basados en en contenido de la cabecera IP y las interfaces de los routers que conmutan los datos basados en el contenido de la corrección de la cabecera MPLS.

2. Layer - 2 Switch Capable (L2SC) interfaces

Interfaces reconocen los límites de la trama / celda y pueden conmutar los datos basados en el contenido de las cabeceras de la trama / celda. Son interfaces sobre bridges Ethernet que conmutan datos basados en el contenido de la cabecera MAC e interfaces sobre ATM – LSRs que transmiten datos basados en la VPI / VCI de ATM.

3. Time - Division Multiplex Capable (TDM) interfaces

Interfaces que conmutan los datos basadas en un intervalo de tiempo repitiendo un ciclo. Un ejemplo de este tipo de interfaces es el SONET/SDH *Cross*–Connect (XC), Terminal multiplexer (TM), o Add-Drop Multiplexer (ADM).

4. Lambda Switch Capable (LSC) interfaces

Interfaces que conmutan datos basados en longitudes de onda sobre la que se reciben los datos. Un ejemplo de este tipo de interfaces es el *Photonic Cross* – Connect (PXC) o Optical Cross que pueden operar al nivel de una longitud de onda individual.

5. Fiber - Switch Capable (FSC) interfaces

Interfaces que conmutan datos basados en una posición relativa de un espacio físico. Un ejemplo de esta interfaz es el PXC o OXC que pueden operar al nivel de una o múltiples fibras.

CAPITULO 2

Análisis del protocolo PCEP (Path Computation Element Protocol) como un mecanismo de comunicación que permita mejorar la eficiencia y escalabilidad en la optimización de las redes de transporte de datos utilizando la tecnología GMPLS.

GMPLS está basado en enrutamiento IP y modelos de direccionamiento. Esto asume que las direcciones IPv4 y/o IPv6 se usan para identificar interfaces pero también se usan protocolos de enrutamiento IP tradicionales

GMPLS puede verse, como un integrador de tecnologías, permitiendo la transmisión de información entre los diferentes tipos de redes y unificando el control del tráfico El PCE puede estar en el plano de gestión, siendo parte de un sistema de gestión de red (Network Management System -NMS) tal que dada una petición de servicio, el NMS solicita una ruta al PCE. Para calcular la ruta mías adecuada, el PCE requiere la información de estado de la red, la cual esta almacenada en una base de datos de ingeniería de tráfico (TED). Una vez que el PCE provee una respuesta al NMS, la configuración es enviada a los elementos de red para configurar el servicio.

.

Las redes de próxima generación soportan múltiples servicios sobre una capa común IP con múltiples tecnologías de transporte

En lugar de añadir la funcionalidad del PCE en el plano de gestión, puede estar en el plano de control. El equipo que solicita las rutas al PCE se denomina Path Computation Client (PCC). Usualmente el PCC es un enrutador GMPLS que puede computar una ruta de un camino distribuido usando el algoritmo de encaminamiento estándar GMPLS o puede solicitar una ruta al PCE cuando el algoritmo de encaminamiento no sea estándar. Para que el PCE pueda calcular la ruta debe conocer el estado de la red. Para ello se puede utilizar la información de inundación de OSPF y se almacenan una TED El PCE puede estar integrado en el mismo equipo que el PCC o puede estar separado del servidor. En el otro caso, la solución de servidor separado usa el protocolo estándar basado en el esquema

petición/respuesta y permite que una única entidad PCE de servicio a múltiples PCCs.

Este protocolo de petición/respuesta se conoce como Path Computation Element Protocol (PCEP). En una arquitectura PCE es posible establecer una serie de normas o reglas que afecten de manera directa al funcionamiento del sistema. Pueden aplicarse tanto en el mecanismo de cálculo de rutas (restricciones adicionales, rutas predefinidas), como en las comunicaciones entre PCEs y PCCs.

El administrador de políticas PM (*Policy Manager*), dentro del plano de administración de red, permite a una red llevar a cabo acciones de manera automática en respuesta a eventos o condiciones en base a unas reglas preestablecidas por el administrador.
Ejemplos de estas políticas son:

- Un PCE puede rechazar una petición en base a la identidad del PCC solicitante.

- Un PCE puede aplicar condiciones añadidas en el cálculo de rutas (hora, día, tipo de servicio, cliente que solicita el servicio, etc.) que pueden incrementar o relajar las restricciones del cálculo.

- La existencia de rutas o partes de rutas predefinidas (en forma de ERO) para determinados servicios, pudiendo depender o no de varios factores, como por ejemplo la dirección de origen y/o de destino.

- Un PCE puede restringir y seleccionar la información sobre sus propias características que da a conocer a los demás PCC y PCE.

- La capacidad de un PCC para elegir un PCE u otro en función del servicio solicitado.

- La especificación de la información contenida en un Path Computation Request, es decir, las variables o restricciones (constraints) aplicables al

cálculo de una ruta, así como el criterio de optimización a usar. La administración de políticas es aplicable a todos los elementos de la red (PCCs y PCEs) de manera general o concreta en cada uno de ellos. El protocolo utilizado para la comunicación entre el PM y los PCCs/PCEs no está Cálculo de ruta

El cálculo de una ruta puede realizarse de manera “única” o “múltiple”. En el cálculo único (single path computation) un único PCE es el que calcula una determinada ruta dentro de un área (aunque haya más PCEs). En este caso, el Ingress LSR inicia el establecimiento del LSP con una ruta explícita estricta (*strict*-ERO) proporcionada por el PCE.

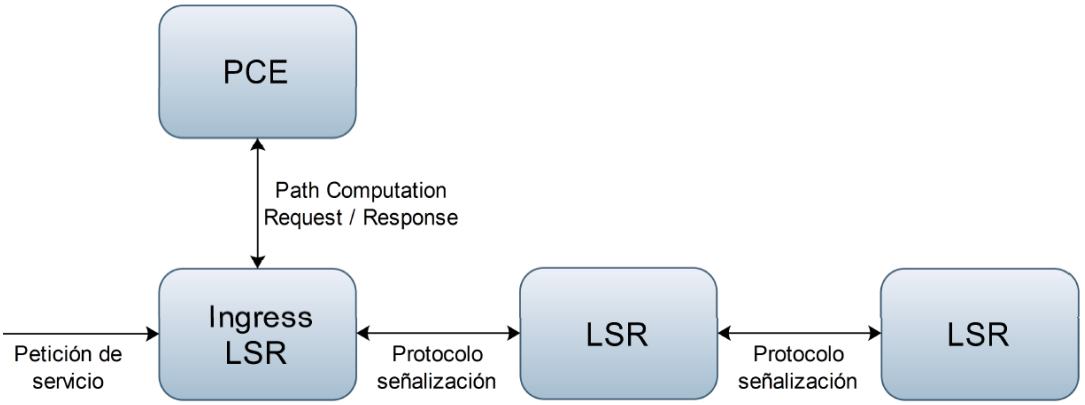

Figura 7. Cálculo de la ruta con comunicación inter –PCE

CAPITULO 3

PCEP (Path Computation Element Protocol) como posible medio de transmisión basado en la arquitectura petición repuesta como un sistema unificado e integrado en el enrutamiento de paquetes con tecnología GMPLS.

PCE surge como iniciativa del IETF para solucionar el problema de calcular una ruta optima aplicando restricciones en escenarios complejos como son redes multicapa, multidominio y con diferentes areas. El concepto de PCE como una entidad de calculo fue validado experimentalmente permite reducir los requisitos computacionales.

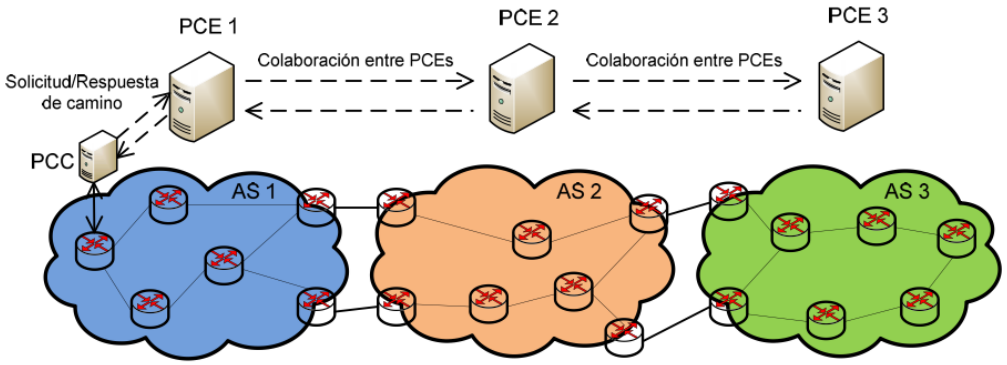

Fig 8. Colaboración entre PCEs en un escenario multidominio

Dentro de la arquitectura PCE existe un nuevo elemento llamado Path Computation Client PCC. El PCC hace solicitudes al PCE, por ello aparece la necesidad del protocolo PCEP que efectua la comunicación entre ambos.

El PCEP es un protocolo basado en la arquitectura petición/respuesta PCEP opera sobre el protocolo de transporte TCP mediante sesiones cliente-servidor. Para ello, utiliza siete tipos de mensajes.

- Open
- Keepalive
- Request
- Responde
- Notify
- Error
- Close.

Un PCC puede mantener sesiones PCEP con múltiples PCEs y, de manera similar, un PCE puede hacerlo con más de un PCC. En cambio, solo se podrá mantener una única sesión a la vez entre los mismos pares de la comunicación (PCC-PCE o PCE-PCE).

Una vez que la conexión TCP ha sido establecida, el PCC y el PCE (conocido como pares PCEP), inician el establecimiento de una sesión PCEP en el que se negocian varios parámetros establecidos en el mensaje Open que incluyen un temporizador Keepalive, un temporizador DeadTimer y potencialmente otras capacidades y políticas detalladas que especifican las condiciones bajo las cuales se envían las solicitudes del cálculo de ruta al PCE.

Si el establecimiento de sesión PCEP falla, porque los pares PCEP no están de acuerdo con los parámetros de sesión o uno de los pares PCEP no responde después de expirar el temporizador de establecimiento, la conexión TCP se cierra inmediatamente. Los mensajes Keepalive se utilizan para asistir los mensajes Open y son enviados una vez que la sesión PCEP ha sido establecida satisfactoriamente.

Cuando se establece una sesión PCEP, es necesario saber que el otro extremo esta aun disponible. Para ese propósito se puede confiar en TCP, pero es posible que la función PCEP remota falle sin perturbar la conexión TCP. Con el fin de manejar esta situación, el PCEP incluye un mecanismo de mantenimiento de conexión basado en un temporizador Keepalive, un temporizador Deadtimer y un mensaje Keepalive. Cada extremo de la sesión PCEP ejecuta el temporizador Keepalive el cual se reinicia cuando se envía un mensaje en la sesión. Si un

extremo de la sesión no recibe ningún mensaje durante el valor del temporizador keepalive, se incrementa el valor del Deadtimer, que cuando expira, la sesión se declara muerta.

Una vez que se ha establecido una sesión PCEP satisfactoriamente entre un PCC y un PCE. El PCC envía una petición de ruta al PCE (mensaje Request) que contienen una variedad de objetos que especifican un conjunto de restricciones y atributos para calcular la ruta. Cada solicitud es única identificada por un ID

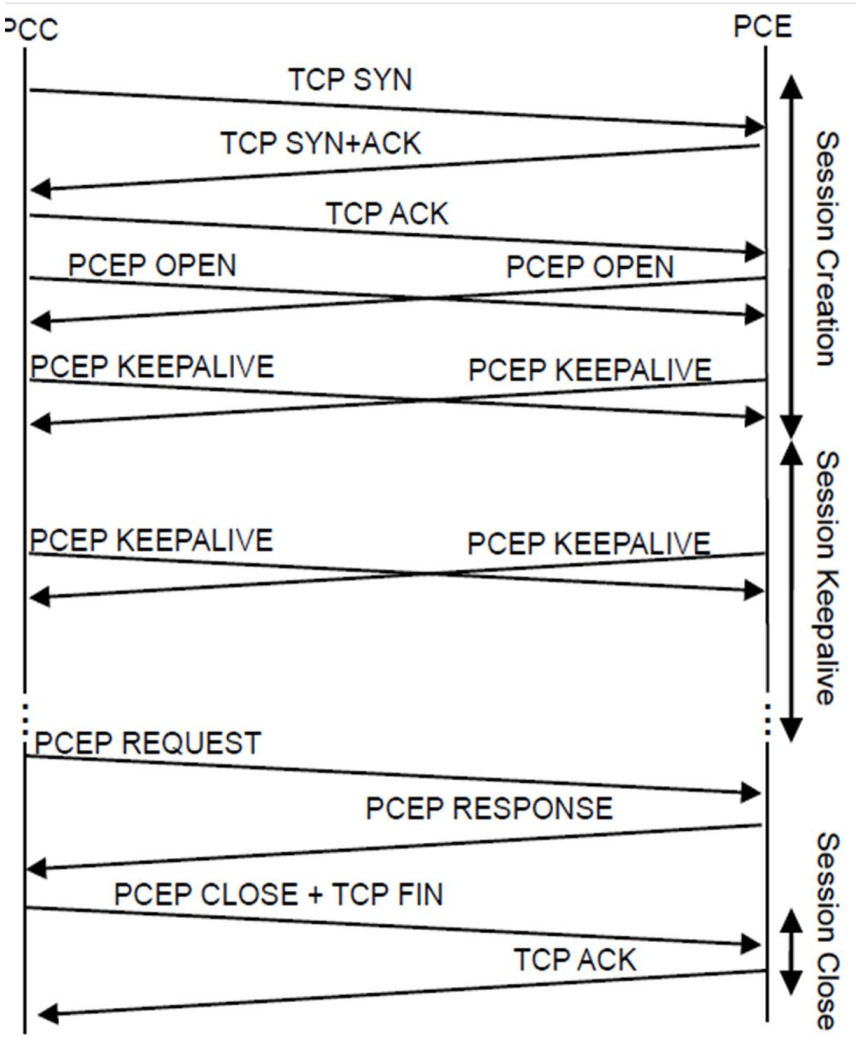

Figura 9. Sesiones PCEP

4.21 Fase de Inicialización

Se distinguen dos pasos dentro de esta fase. El primero es el establecimiento de una conexión TCP entre un PCC y un PCE y el segundo, el establecimiento de

una sesión PCEP sobre la conexión TCP. Una vez establecida una conexión TCP, los dos pares de la comunicación negocian distintos parámetros para establecer una sesión PCEP. Dichos parámetros se envían en mensajes Open e incluyen los temporizadores Keepalive y DeadTimer, además de otra información adicional que determina las condiciones en que un mensaje Request ha de ser enviado a un PCE. Para reconocer los mensajes Open se utilizan los mensajes Keepalive.

4.21.1 Sesión Keepalive

Cuando hay una sesión establecida, tanto el PCC como el PCE tienen la oportunidad de conocer si el otro extremo de la sesión sigue estando disponible. Para ello utilizan un mecanismo basado en mensajes Keepalive y temporizadores Keepalive y DeadTimer. Cada extremo de la conexión utiliza un temporizador Keepalive que se reinicia tras el envió de cualquier mensaje PCEP. Cuando el temporizador expira se envia un mensaje Keepalive. A su vez, los dos extremos también reinician un temporizador DeadTimer cada vez que reciben un mensaje PCEP, de manera que si no reciben ningún mensaje antes de que el DeadTimer expire, entonces declaran muerta la sesión. Los valores de los temporizadores son indicados en los mensajes Open. Un extremo especifica un valor para el temporizador Keepalive y recomienda otro para el DeadTimer del otro extremo. El valor mínimo del temporizador Keepalive es de 1 segundo y se recomienda un valor de 30 segundos. También existe la opción de deshabilitarlo poniéndolo a cero. En cuanto al DeadTimer, su valor recomendado es 4 veces el valor del temporizador Keepalive del otro extremo, lo que evita congestionar la red con mensajes Keepalive.

4.21.2 Path Computation Request

Cuando se ha establecido una sesión y un PCC ha seleccionado un PCE entre los de su dominio, dicho PCC puede solicitar rutas al PCE utilizando mensajes Request.

Un mensaje Request contiene varios objetos que especifican las restricciones y atributos para el cálculo del camino y está identificado unívocamente por un identificador de petición. Entre la información que contiene el mensaje Request se encuentran, por ejemplo, las direcciones IP del origen y el destino o, si la ruta

solicitada es multi-dominio, puede indicarse el procedimiento a seguir. Un PCC puede solicitar un conjunto de rutas en el mismo mensaje Request, asi como un PCE puede proporcionar varias respuestas para un mismo camino.

4.21.3 Path Computation Reply

Después de haber recibido una solicitud de ruta, el PCE realiza el cálculo correspondiente, cuyo resultado puede ser positivo o negativo. En el caso de se haya podido obtener un camino que satisfaga el conjunto de restricciones solicitadas, el PCE envía el camino o el conjunto de caminos al PCC en un mensaje Reply. En cambio, si no se ha podido encontrar ningún camino, el PCE se lo comunica al PCC indicando, si lo considera necesario, las restricciones que no se han podido satisfacer.

4.21.4 Finalización de la sesión PCEP

Cuando uno de los dos extremos desea terminar la sesión PCEP, debe mandar un mensaje Close al otro extremo y después cerrar la conexión TCP. Si es el PCE el que finaliza la sesión, el PCC deberá borrar todos los estados relacionados con las peticiones pendientes de ser atendidas. De forma similar, si el PCC es el que cierra la sesión, el PCE borrara todas las peticiones de ese PCC pendientes de ser calculadas. El mensaje Close solo pude ser enviado para finalizar la sesión PCEP si la sesión ha sido previamente establecida Debe tenerse en cuenta que como PCEP opera sobre TCP, si la conexión TCP falla, la sesión PCEP se cerrara inmediatamente. La sesión PCEP también puede finalizar si un PCE/PCC recibe un mensaje desconocido a una frecuencia elevada. Cuando se finaliza una sesión, el PCE/PCC debe cerrar la conexión TCP y no enviar ningún mensaje más en la sesión PCEP.

4.21.5 Notificaciones

Es posible que el PCE necesite notificar algún evento a un PCC (o viceversa) mediante un mensaje.
Notification. Por ejemplo, el PCE puede informar acerca de la sobrecarga de mensajes que sufre, así como un PCC puede cancelar peticiones si lo considera necesario.

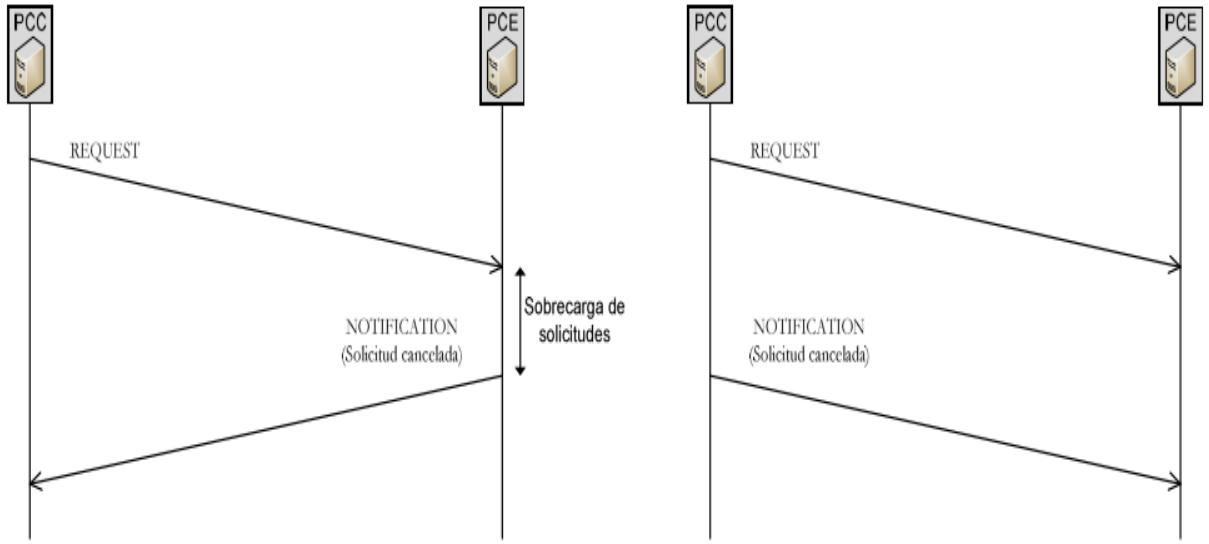

Figura 10. Notificaciones del PCE (izq) y PCC (der)

4.21.6 Recepción de un mensaje desconocido

Una implementación PCEP que recibe un mensaje PCEP desconocido debe enviar un mensaje de error con el flag Error-value igual 2 (capacidad no soportada). Si un PCC/PCE recibe un mensaje desconocido a una tasa igual o mayor que el máximo de mensajes desconocidos, el PCC/PCE debe enviar un mensaje PCEP close con el valor Reason igual a 5 (Recepción de un numero inaceptable de mensajes desconocidos). El valor recomendado para mensajes desconocidos es de 5. Si esto ocurre PCC/PCE debe cerrar la conexión TCP y no debe enviar ningún mensaje PCEP sobre la sesión PCEP.

4.21.7 Solicitud de cálculo de ruta enviada del PCC al PCE

Una vez que se ha establecido una sesión PCEP satisfactoriamente entre un PCC y un PCE. El PCC envía una petición de ruta al PCE (mensaje Request) que contienen una variedad de objetos que especifican un conjunto de restricciones y

atributos para calcular la ruta. Cada solicitud es única identificada por un ID. Este proceso se muestra en el esquema de la Figura.

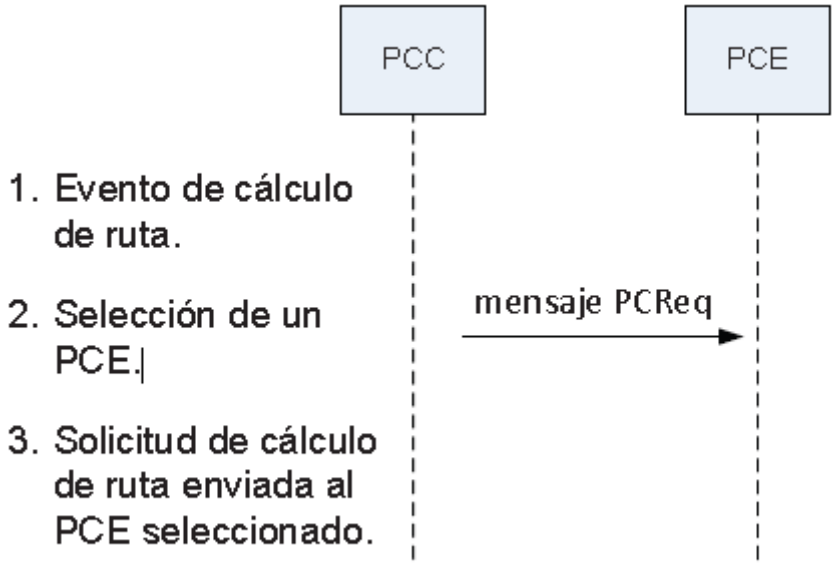

Figura11. Solicitud de cálculo de ruta

4.21.8 Respuesta del cálculo de ruta enviada del PCE al PCC

El PCE al recibir la solicitud acciona un cálculo de ruta que al resolverse retorna un mensaje Response. El resultado del cálculo de la ruta puede ser:

- Positivo (Fig. calculo positivo): Si el PCE resuelve satisfactoriamente el cálculo de ruta que satisface el conjunto de restricciones requeridas, retorna un conjunto de rutas calculadas al PCC solicitante. Hay que remarcar que el PCE soporta la capacidad de recibir en una solicitud simple el cálculo de más de una ruta.
- Negativo (Fig. calculo negativo): Si el PCE no resuelve el cálculo de la ruta que satisface el conjunto de restricciones, envía un mensaje reply al PCC con una respuesta negativa. El PCC al recibir la una respuesta negativa puede decidir volver a enviar la solicitud modificando la o tomar cualquier otra acción apropiada.

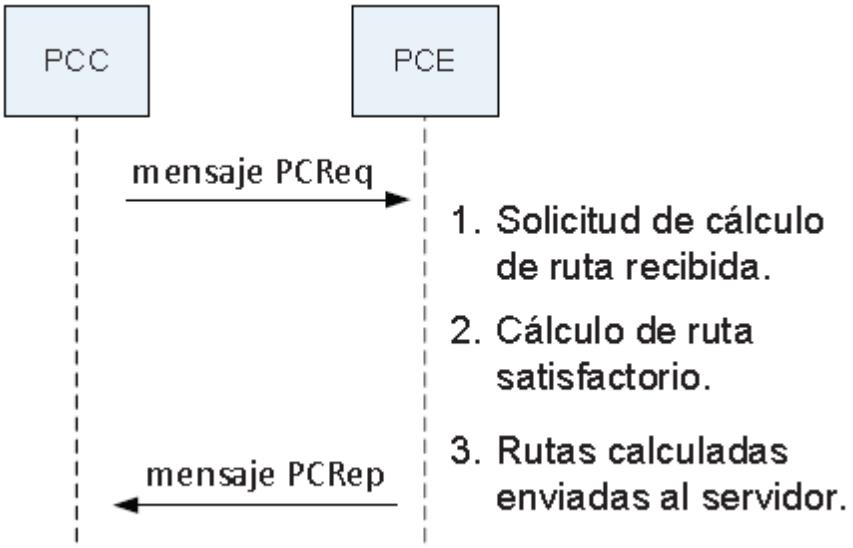

Figura 12. Calculo positivo

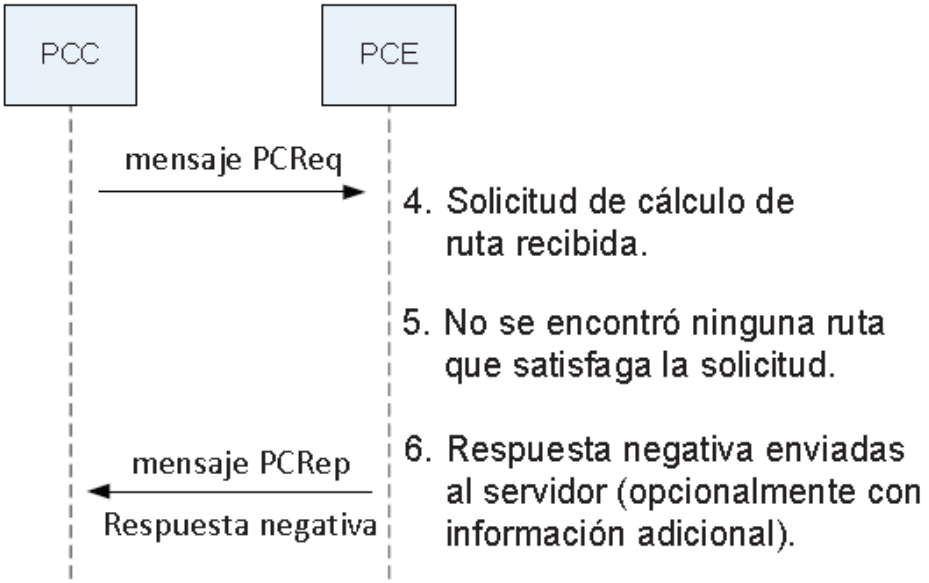

Fig13. Calculo negativo

4.21.9 Mensajes de Error PCEP

Los mensajes de error PCEP se envían en diversas situaciones. Por ejemplo cuando una condición de error de protocolo se cumple o cuando la petición no es compatible con la especificación del PCEP (recepción de un mensaje con un objeto obligatorio perdido, referencia de solicitud desconocida, violación de

políticas, mensaje inesperado). La siguiente Fig. Muestra el ejemplo de un mensaje de error enviado del PCE al PCC.

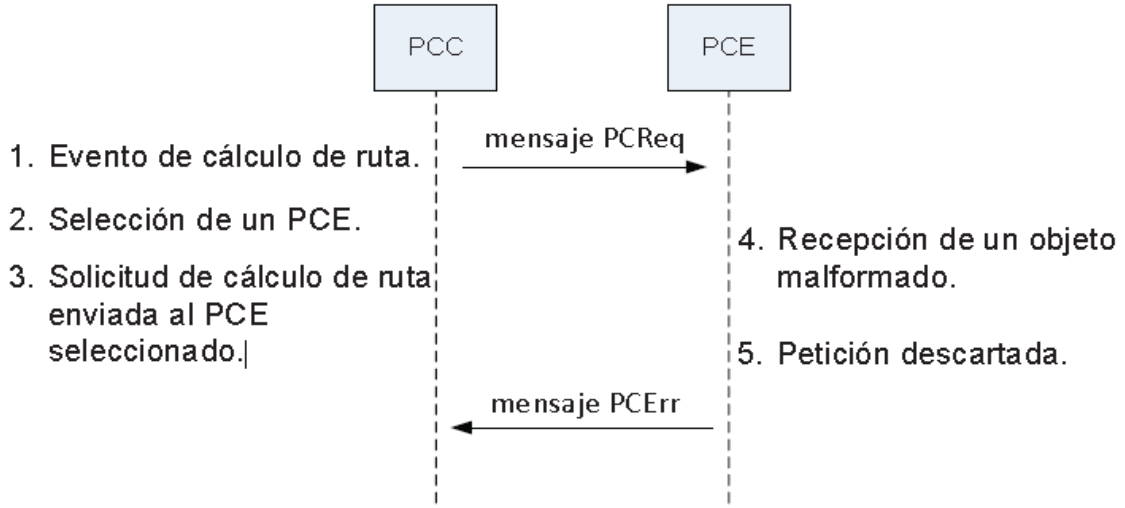

Fig14. Mensaje de error PCEP

4.21.10 Mensajes Close PCEP

Cuando uno de las pares PCEP desea terminar la sesión, este primero envía un mensaje PCEP Close y luego cierra la conexión TCP. Si el PCE finaliza la sesión, el PCC borra todos los estados relacionados con las peticiones pendientes previamente enviadas al PCE. Similarmente, si el PCC finaliza la sesión, el PCE borra todas las peticiones de ruta enviadas por el PCC. El mensaje Close solo pude ser enviado para finalizar la sesión PCEP si la sesión ha sido previamente establecida. La sesión PCEP también puede finalizar si un PCE/PCC recibe un mensaje desconocido a una frecuencia elevada. Cuando se finaliza una sesión, el PCE/PCC debe cerrar la conexión TCP y no enviar ningún mensaje más en la sesión PCEP.

Capitulo 4

Presentar mediante el estudio del protocolo PCEP (Path Computation Element Protocol) el impacto que este presenta en las redes de próxima generación para obtener el cálculo óptimo de rutas en un entorno de red.

Las redes troncales estaban gestionadas de forma estática y centralizada. Este sistema de gestión se encargaba de configurar cada equipo de la red por donde se encaminaba la conexión. Dos hechos cambiaron este paradigma de gestión centralizada en redes Troncales. Por un lado, los elementos de red ópticos, como Óptica Cross-Connects (OXC) Reconfigurable Optical Add Drop Multiplexers (ROADM), avanzaron tecnológicamente para poder reconfigurarse de forma dinámica. Por otro lado, la introducción del paradigma Automatically Switched Optical Network (ASON) y Generalized Multi-Protocol Label Switching (GMPLS) creó un plano de control unificado que permite crear y destruir Label Switched Paths (LSP) de una forma automática. Al ser un plano de control unificado, se puede controlar múltiples dispositivos desde equipamiento ethernet, IP/MPLS a equipamiento óptico.

Este cambio en la arquitectura crea una red de nueva generación con tres planos: plano de datos, de control y de gestión. El plano de datos se encarga del transporte de la información de los usuarios. La ITU define el plano de gestión como la entidad que gestiona las funciones del plano de transporte, el plano de control y el sistema en su completo y asegura la coordinación entre ellos. Se usa para las operaciones centralizadas de la red como son la facturación, la gestión de fallos o la monitorización de la calidad de servicio, entre otros. La ITU define el plano de control como la entidad que se encarga de las conexiones, su establecimiento, liberación y restauración.

4.22 Requisitos para el protocolo PCEP

Un PCC que solicita el cálculo de un camino, debe ser capaz de indicar en el mensaje Request: El tiempo que los recursos deberán estar reservados (ancho de banda, ranuras de tiempo, longitud de onda, etc.) o la granularidad de los recursos, que se refiere a la posibilidad de reservar no solo los recursos, sino también los enlaces o nodos involucrados. Si los recursos deben ser reservados para posteriores peticiones. El PCE debería ser capaz de:

- Calcular el o los caminos solicitados y, de acuerdo a las indicaciones del PCC, reservar los recursos elegidos por un periodo de tiempo.

- El tiempo determinado por el PCE nunca debe ser menor que el solicitado por el PCC (puede ocurrir que el PCE solo pueda reservar recursos para unos tiempos en concreto, múltiplos de un valor). Alternativamente, podría enviar un mensaje de Error al PCC si el camino no puede ser calculado o pre-reservado.

- También debería ser capaz de aplicar una granularidad diferente a la indicada en la solicitud. En tal caso, debe comunicárselo al PCC.
  Además, el PCE debería poder responder en el mensaje Reply lo siguiente:

- Si los recursos han sido pre-reservados correctamente y el periodo de tiempo utilizado, que podría ser diferente del solicitado.

- La granularidad de los recursos reservados, que podría ser diferente a la indicada por el PCC.

- Proporcionar, por ejemplo, un identificador de pre-reserva para que el PCC pueda cancelarla.

En base a estos requisitos, se proponen una serie de extensiones al protocolo PCEP para su correcto funcionamiento. Un PCC que solicita un camino al PCE, debe incluir en su mensaje Request dos objetos: PCC_ID_REQ y RESERVATION. El primero de ellos, se usa para indicar la dirección IP del PCC. El objeto RESERVATION indica la intención del PCC de pre-reservar los recursos asignados a su petición. En él puede indicarse el tipo de recurso solicitado y el tiempo que se quiere que dicho recurso sea reservado. El PCE, en respuesta a la petición del PCC y opcionalmente, puede incluir un objeto RESERVATION_CONF [35] en el mensaje Reply indicando el tiempo que el recurso ha sido reservado finalmente y el identificador de la reserva.

También se propone la posibilidad de que un PCC pueda cancelar una reserva indicándolo en un mensaje Notification. Para ello debería incluir el identificador de la reserva en un objeto RESERVATION_ID TLV

4.23 Calculo de ruta

4.23.1 Descripción funcional

4.23.2 Secuencia típica en el proceso de cálculo de un TE LSP:

1. Una solicitud de un nuevo camino llega a un dominio MPLS/GMPLS, por lo que el Label Edge Router (LER) de entrada debe empezar el establecimiento de un camino con diferentes restricciones hacia el destino.

2. El LER actúa como un PCC y solicita al PCE el cálculo del mejor camino posible dentro de su dominio. En la comunicación utilizan PCEP.

3. El PCE puede calcular el camino de manera individual o colaborando con otros PCEs del mismo dominio. Para ello comprueba si las restricciones solicitadas pueden ser satisfechas basándose en la información obtenida de la TED y en sus políticas locales.

4. El PCE calcula el camino mediante un algoritmo de cómputo.

5. Cuando el camino es calculado, el PCE se lo proporciona al PCC y éste establece dicho camino mediante el protocolo de señalización utilizado.

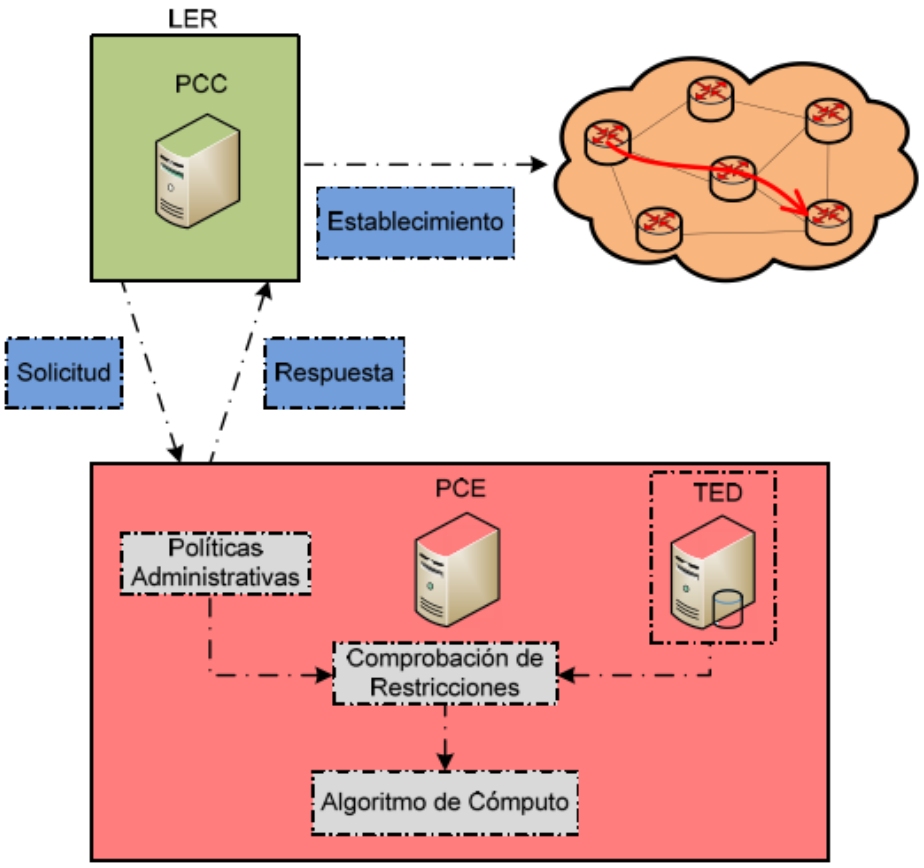

Fig15. Descripción Arquitectura basada en PCEP

4.24 Evaluación de sistemas GMPLS-PCE

Para hacer una evaluación de la eficiencia de un sistema GMPLS-PCE en términos de Ingeniería de Tráfico, se definen cuatro criterios:

- **Optimización:** la habilidad de maximizar la cantidad de tráfico que puede transitar por una red con unas garantías QoS. Se pueden considerar diferentes criterios de optimización, como por ejemplo, minimizar la carga total de la red, maximizar el ancho de banda residual de los enlaces más saturados, o, en caso de congestión, minimizar el número de peticiones rechazadas.

- **Escalabilidad:** la habilidad de escalar bien al incrementar el número de cualesquiera de sus elementos: enlaces, LSRs, PCEs, etc.

- **Estabilidad:** la habilidad de evitar re-enrutados y reconfiguraciones y minimizar cualquier perturbación en la red como consecuencia del establecimiento de nuevos LSPs.

- **Reactividad:** la habilidad de reaccionar y adaptarse rápidamente a una redistribución del tráfico como consecuencia de un cambio en la topología de la red (nuevos enlaces o fallos en los existentes).

4.24.1 Escalabilidad

El continuo crecimiento de Internet es debido a que cada vez son más los sistemas autónomos que se conectan entre si a través de routers externos. Además de tener en cuenta la posibilidad de acceder al exterior del sistema autónomo a través de un determinado router externo u otro se debe tener en cuenta que se tiene varios proveedores de servicios y es más versátil elegir en cada momento el router exterior y servicio requerido que establecer una ruta y servicio por defecto cuando se trata de routing externo como se tenía hasta ahora. OSPF soluciona este problema permitiendo tener en la base de datos del mapa local los denominados “gateway link state records”. Estos registros nos permiten almacenar el valor de las métricas calculadas y hacen más fácil el cálculo de la ruta óptima para el exterior. Por cada entrada externa existirá una nueva entrada de tipo “gateway link state records” en la base de datos, es decir, la base de datos crecerá linealmente con el número de entradas externas tal como ocurre con los protocolos de vector distancia, pero el coste del cálculo de las rutas crecerá en función de N*log*N para OSPF y no en función de N^2 como ocurre en los protocolos de vector distancia.

4.24.2 Comunicación cliente-servidor

4.24.2.1 Comunicación entornos inter-dominios

Una vez que el PCE ha descubierto otros elementos PCE en los dominios adyacentes, contará con una base de datos de candidatos a colaborar a la hora de recibir una petición de cómputo de LSP interdominio. En dicho momento, deberá llevar a cabo un proceso de selección del PCE adecuado. Para ello, el PCE inicial deberá contar con información relativa a cada uno de los PCE candidatos, información que es proporcionada habitualmente por los mecanismos de descubrimiento interdominio junto con el anuncio del PCE.

Cuando el proceso finaliza, el PCE inicial se comunicará con el PCE seleccionado utilizando el protocolo PCEP. El resto de la operación se lleva a cabo de forma similar al trabajo intradominio excepto por el hecho de que el PCE inicial debe confiar en que el PCE colaborador computará el segmento de LSP que le corresponde cumpliendo las mismas restricciones (no tendrá visibilidad de los dominios adyacentes). Este proceso se repetirá hacia delante, dominio por dominio, hasta que se alcance el dominio final o destino del LSP.

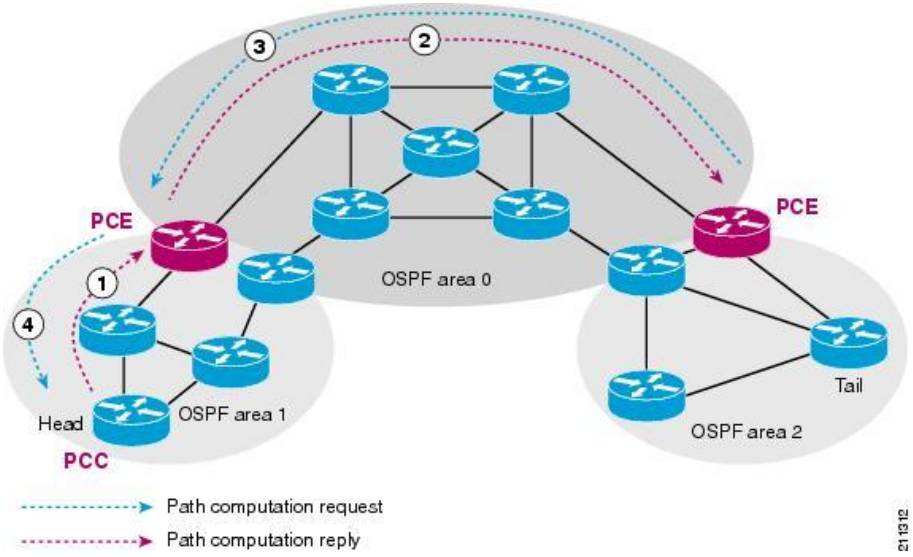

Figura16. Comunicación entornos inter-dominios

El PCE debería ser capaz de:

- Calcular el o los caminos solicitados y, de acuerdo a las indicaciones del PCC reservar los recursos elegidos por un periodo de tiempo.

- El tiempo determinado por el PCE nunca debe ser menor que el solicitado por el PCC (puede ocurrir que el PCE sólo pueda reservar recursos para unos tiempos en concreto, múltiplos de un valor). Alternativamente, podría enviar un mensaje de Error al PCC si el camino no puede ser calculado o pre-reservado.

  También debería ser capaz de aplicar una granularidad diferente a la indicada en la solicitud. En tal caso, debe comunicárselo al PCC.

  Además, el PCE debería poder responder en el mensaje Reply lo siguiente:

  - Si los recursos han sido pre-reservados correctamente y el periodo de tiempo utilizado, que podría ser diferente del solicitado.

  - La granularidad de los recursos reservados, que podría ser diferente a la indicada por el PCC.

  - Proporcionar, por ejemplo, un identificador de pre-reserva para que el PCC pueda cancelarla.

  En base a estos requisitos, se proponen en una serie de extensiones al protocolo PCEP para su correcto funcionamiento. Un PCC que solicita un camino al PCE, debe incluir en su mensaje Request dos objetos: PCC_ID_REQ y RESERVATION. El primero de ellos,se usa para indicar la dirección IP del PCC.

  El objeto RESERVATION indica la intención del PCC de pre-reservar los recursos asignados a su petición. En él puede indicarse el tipo de recurso solicitado y el tiempo que se quiere que dicho recurso sea reservado. El PCE, en respuesta a la petición del PCC y opcionalmente, puede incluir un objeto RESERVATION_CONF en el mensaje Reply indicando el tiempo que el recurso ha sido reservado finalmente y el identificador de la reserva.

  También se propone la posibilidad de que un PCC pueda cancelar una reserva indicándolo en un mensaje Notification. Para ello debería incluir el identificador de la reserva en un objeto RESERVATION_ID TLV.

4.24.3 Fiabilidad de la comunicación

PCEP debe soportar el intercambio seguro de paquetes. Esta condición puede ser inherente del propio protocolo o puede ser adquirida por la elección de un protocolo de transporte adecuado.

Concretamente, la detección y recuperación de mensajes perdidos debe ser lo suficientemente rápida para no afectar la operación del PCEP.
En algunos casos, como puede ser después de la caída de un enlace, un PCE puede saturarse debido a la recepción simultánea de un alto número de peticiones. Ante esta situación, el PCE debe informar de su estado y puede limitar la tasa de recepción de mensajes de petición.

PCEP o su protocolo de transporte deben ofrecer las siguientes funcionalidades:

- Detección y notificación de mensajes perdidos o corruptos.
- Retransmisión automática de mensajes perdidos.
- Control de mensajes duplicados.
- Control de congestión.
- Detección de fallo de comunicación PCEP.
- Distinción entre fallo de canal y fallo del otro dispositivo (PCE/PCC), después de la recuperación de la comunicación PCEP.

4.24.4 Seguridad de la comunicación

PCECP debe garantizar la seguridad de la comunicación entre entidades. Esta seguridad se traduce en mecanismos que protejan contra:

- La suplantación de identidad (*spoofing*) mediante un sistema de identificación y autenticación.

- La vulneración de confidencialidad (*snooping)* mediante técnicas de encriptación.

- Ataques de denegación de servicio (*DoS*). Ej. filtrado de paquetes, limitación de tráfico.

Una política administrativa puede impedir que un PCE proporcione rutas explícitas. Si un PCC solicita una ruta explícita cuando no está permitido, el PCE envía un mensaje de error y descarta la petición.

CONCLUSIONES

En este proyecto se hizo un análisis del protocolo de transporte de datos PCEP (Path computation element protocol) como posible medios de transmisión usando tecnología (GMPLS) Generalized Multi-Protocol Label Switching, de una visión global y genérica de las arquitecturas GMPLS desarrolladas por la IETF, además del sistema de enrutamiento que proporciona a la evolución tecnológica y las necesidades que motivaron el desarrollo de estos estándares. En concreto, la creación de un plano de control común e inteligente que permite a los diferentes operadores la configuración, utilización y mantenimiento de sus redes de un modo seguro, fácil, más eficiente y sobre cualquier tecnología de transporte y transmisión de datos. En definitiva, los sistemas GMPLS-PCEP son un peldaño más en la constante evolución del mundo de las telecomunicaciones, proporcionando una adaptación inteligente de las redes al crecimiento exponencial del tráfico, integrando las diferentes tecnologías existentes, y ofreciendo el soporte para los nuevos servicios y aplicaciones que los usuarios demandan.

BIBLIOGRAFIAS

http://www.eps.uam.es/esp/...fin.../Annamuro Machicao Jose Luis

http://www.eps.uam.es/esp/alumnos/trabajos fin máster/Annamuro Machicao José Luis

http://www.vlopezalvarez.com/Profesional/Publications/Conferences/2011 Jitel.pdf

http://tools.ietf.org/html/rfc5440Fhttp://www.ietf.org/rfc/rfc4802.txt

http://www.ietf.org/rfc/rfc3032.txt

http://translate.google.com.ni/translate?hl=es-419&sl=en&u=

ANEXO

Protocolos de Enrutamiento

Los protocolos de enrutamiento son los encargados de calcular la ruta entre dos puntos de red, con unas determinadas condiciones o restricciones (*constraints*) para la transmisión de un cierto tráfico. Para realizar este cálculo, es necesario conocer la topología y los recursos de la red.

Estos protocolos especifican cómo se comunican los enrutadores (routers) en una red computacional y diseminan información que les permite a los enrutadores elegir rutas entre dos nodos en la red a través de algoritmos de enrutamiento. Cada enrutador tiene inicialmente un conocimiento mínimo de la red, limitado a las redes directamente conectadas a éste. Un protocolo de enrutamiento comparte esta información con vecinos inmediatos y así eventualmente los enrutadores obtienen un mayor conocimiento general de la red. El concepto básico detrás de los protocolos por Estado de Enlace es que todos los nodos de la red (los enrutadores) construyen un mapa de conectividad de la red en forma de grafico que muestra qué tiene conexión con cuál otro. Todos los enrutadores, entonces pasan a calcular el mejor camino desde ellos mismos hasta cualquier otro posible nodo de la red. El conjunto de mejores caminos conforma la tabla de enrutamiento del nodo. Una manera sencilla de caracterizar estos algoritmos es que los nodos solo hablan de sus vecinos. Entre los protocolos de enrutamiento por Estado Enlace existen los protocolos IS-IS y OSPF.

Protocolo OSPF

- **Open Shortest Path First – Traffic Engineering OSPF**

El protocolo OSPF (de sus siglas en inglés, Open Shortest Path First) es un protocolo de red adaptativo, diseñado específicamente para correr sobre el

protocolo IP. La versión 2 del mismo está definida específicamente para IPv4, mientras que para la compatibilidad con IPv6 fue necesario hacerle actualizaciones al mismo, las cuales están definidas en su versión 3. OSPF también fue diseñado para ser compatible con VLSM (Variable Length Subnet Masking). Está diseñado para intercambiar información de enrutamiento dentro de una interconexión de redes extensa o muy extensa. La mayor ventaja de OSPF es que es eficaz; requiere un uso escaso de la red, incluso en el caso de interconexiones de redes de gran tamaño. La mayor desventaja de OSPF es su complejidad, requiere una organización adecuada y resulta más difícil de configurar y administrar. OSPF utiliza el algoritmo Ruta de acceso más corta primero (SPF, Shortest Path First) para calcular rutas en la tabla de enrutamiento. El algoritmo SPF calcula las rutas de acceso más cortas (menos costo) entre el enrutador y todas las redes de la interconexión. Las rutas calculadas mediante SPF nunca presentan bucles.

En vez de intercambiar entradas de la tabla de enrutamiento como los enrutadores RIP, los enrutadores OSPF mantienen un mapa de la interconexión de redes que se actualiza tras cualquier cambio en la topología de la red. Este mapa, denominado base de datos de estado de vínculos, se sincroniza entre todos los enrutadores OSPF y se utiliza para calcular las rutas de la tabla de enrutamiento. Los enrutadores OSPF vecinos forman una adyacencia, que es una relación lógica entre enrutadores para sincronizar la base de datos de estado de vínculos. Los cambios de la topología de la interconexión de redes se abordan de manera eficaz en toda la interconexión de redes, a fin de garantizar que la base de datos de estado de vínculos de cada enrutador esté sincronizada y sea precisa en todo momento. Tras recibir los cambios de la base de datos de estado de vínculos, vuelve a calcularse la tabla de enrutamiento. A medida que aumenta el tamaño de la base de datos de estado de vínculos, aumentarán también los requisitos de memoria y el tiempo de cálculo de las rutas. Para resolver este problema, OSPF divide la interconexión de redes en áreas (grupos de redes contiguas) que están conectadas entre sí a través de un área troncal. Cada enrutador sólo mantiene una base de datos de estado de vínculos para aquellas áreas que estén

conectadas al enrutador. Los enrutadores de borde de área (ABR, Area Border Routers) conectan el área troncal con las demás áreas.

Para reducir más la cantidad de información de enrutamiento suministrada a las áreas, OSPF permite utilizar áreas de rutas internas. Un área de rutas internas puede contener puntos de entrada y salida únicos (ABR único), o varios ABR, si cualquiera de ellos se puede utilizar para conectar con destinos de rutas externas.

Cuando se diseñó se quiso que cumpliera los siguientes requisitos:

- ser abierto en el sentido de que no fuera propiedad de una compañía.
- que permitiera reconocer varias métricas, entre ellas, la distancia física y el retardo.
- ser dinámico, es decir, que se adaptará rápida y automáticamente a los cambio de la topología.
- ser capaz de realizar en encaminamiento dependiendo del tipo de servicio.
- que pudiera equilibrar las cargas dividiendo la misma entre varias líneas.
- que reconociera sistemas jerárquicos pues un único ordenador no puede conocer la estructura completa de Internet.
- que implementara un mínimo de seguridad.

El protocolo OSPF reconoce tres tipos de conexiones y redes:

- líneas punto a punto entre dos dispositivos de encaminamiento.
- redes multiacceso con difusión (por ejemplo, la mayoría de redes LAN).
- redes multiacceso sin difusión (por ejemplo, la mayoría de redes WAN de conmutación de paquetes).

La función del OSPF es encontrar la trayectoria más corta de un dispositivo de encaminamiento a todos los demás. Cada dispositivo de encaminamiento

tiene almacenada en una base de datos la topología de la red de la que forma parte. Al arrancar un dispositivo de almacenamiento, este protocolo envía paquetes hello por todas sus líneas punto a punto y los retransmite a todos los demás dispositivos de encaminamiento. Gracias a las respuestas que recibe sabe cuáles son sus dispositivos de encaminamiento vecinos. El OSPF se basa en el intercambio de información entre los dispositivos de encaminamiento adyacentes, que no es lo mismo que vecinos. Para que no todos los dispositivos tengan que hablar con los demás, se designa uno como adyacente a todos los demás y es este el que intercambia información con los restantes. Por motivos de seguridad se determinada un dispositivo de encaminamiento como secundario por si el primario cae. Normalmente, el dispositivo de encaminamiento inunda de mensajes de actualización de estado del enlace a todos sus dispositivos de encaminamiento adyacentes. Estos mensajes tienen un número de secuencia y además para hacerlos confiables son reconocidos por el mensaje reconocimiento de estado del enlace. Además existen otros dos mensajes: descripción de la base de datos que es utilizado para anunciar las actualizaciones que tiene el transmisor, y solicitud de estado de enlace que es utilizado para solicitar información a un compañero. Todos los mensajes utilizados en el OSPF se envían como paquetes IP en bruto.

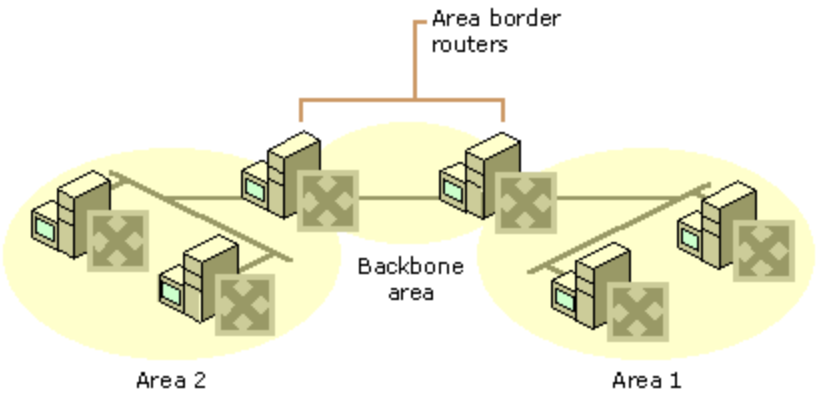

Figura17. Diagrama de una interconexión de redes OSPF.

Estado OSPF

- **Desactivado (DOWN):** En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización).

- **Inicialización (INIT):** Los routers (enrutadores) OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los Routers vecinos. Cuando una interfaz recibe su primer paquete Hello, el router entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa. Los dos tipos de relaciones son Bidireccional y Adyacencia. Un router debe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.

- **Bidireccional (TWO-WAY) (encaminador = enrutador):** Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino. El estado Bidireccional es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros enrutadores y eventualmente construir una tabla de enrutamiento, cada enrutador OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre enrutadores OSPF que involucra una serie de estados progresivos basados no solo en los paquetes Hello, sino también en el intercambio de otros 4 tipos de paquetes OSPF. Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea

completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

- **Inicio de Intercambio (EXSTART):** Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos. Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

- **Intercambio (EXCHANGE):** En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.
- **Cargando (LOADING):** Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace

(LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

- **Adyacencia completa (FULL):** Cuando el estado de carga ha sido completada, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

Principales Ventajas y Características del Protocolo OSPF

❖ **Ventajas**

- Las rutas calculadas mediante OSPF nunca presentan bucles.
- OSPF puede escalar a interconexiones de redes mayores o mucho mayores.
- La reconfiguración correspondiente a los cambios de topología de la red es más rápida.

❖ **Características de OSFP**

- Protocolo de Estado de Enlace (Algoritmo de Djikstra)
- Protocolo de diseño jerárquico.
- Soporte de VLSM y subneting discontinuo
- Su métrica es el costo y es calculada en base al ancho de banda.
- Utiliza el puerto 89 de TCP
- Localiza, mantiene y redescubre vecinos mediante mensajes de “Hello”
- Transmisión confiable de sus mensajes

- Mensajes de actualización enviados a una dirección Multicast.
- Garantiza una topología libre de lazos.
- Filtros de ruta para controlar la interacción con otros protocolos de enrutamiento.
- Reconfiguración dinámica de toda la configuración de OSPF.
- Coexistencia con RIP.
- Suma y eliminación dinámica de interfaces.

Protocolo IS-IS

- **Intermediate System to Intermediate System – Traffic Engineering IS-IS-**

El protocolo IS-IS es un protocolo de estado de enlace, o SPF (shortest path first), por lo cual, básicamente maneja una especie de mapa con el que se fabrica a medida que converge la red. Es un protocolo de enrutamiento interior, su desarrollo estuvo motivado por la necesidad de un sistema no propietario que pudiera soportar un gran esquema de direccionamiento y un diseño jerárquico. Este protocolo permite a sistemas intermedios (IS's) dentro de un mismo dominio cambiar su configuración e información de ruteo para facilitar la información de encaminamiento y funciones de transmisión de la capa de red. El protocolo de encaminamiento IS-IS está pensado para soportar encaminamiento en grandes dominios consistentes en combinaciones de muchos tipos de subredes. Esto incluye enlaces punto a punto, enlaces multipunto, subredes X.25 y subredes broadcast tales como las ISO 8802 LANs. Para poder soportar dominios grandes, la previsión está hecha para que el ruteo intradominio sea organizado jerárquicamente.

IS-IS define dos tipos de red: subredes broadcast y redes punto-a-punto.

- **Adyacencias en Enlaces Punto-a-Punto:** Un enlace punto-a-punto conecta dos routers. Después de que cada uno de los routers reciba un paquete Hello, cada uno declara el otro extremo como alcanzable y cada

extremo envía un CSNP, que contiene una lista de todos los enlaces almacenados en la BBDD de estado-enlace, lo que conlleva una sincronización de las BBDD de estado-enlace de cada máquina. Los Hellos periódicos mantienen la adyacencia. Si un router no recibe un Hello dentro del tiempo de espera (holdtime) el vecino es declarado caído y la BBDD purgada de cualquier entrada asociada a ese router. El intevalo de Hellos por defecto es cada 10 seg. El holdtime es de 30 seg.

- **Adyacencias en enlaces Broadcast:** En estos enlaces cada router sólo recibe paquetes enviados por el DIS (designated Intermediate System) – esto se hace para controlar la cantidad de tráfico que necesita ser generada y manterner las adyacencias y las BBDD. El DIS tiene la responsabilidad de inundar con LSPs a todos los sistemas IS-IS conectados, más exactamente, el DIS inyecta los LSPs para el pseudonodo. El pseudonodo representa la LAN, con cada router simulando una interfaz en un router imaginario. Este router imaginario es el llamado pseudonodo. Como si fuera un router real, el psedonodoinyecta un LSP cuando existe un cambio en el status de sus conexiones. Las adyacencias con los otros routers son mantenidas por el DIS. Si hay un problema con éste o un router con prioridad más alta aparece en la red, es identificado rápidamente y un nuevo router es elegido en lugar del viejo DIS. La elección está basada en la prioridad y declarada en la interfaz. En el caso de que todas estén configuradas por defecto a 64, el mayor número SNPA (dirección de enlace de datos) determina el DIS.

- **Adyacencias en enlaces NBMA:** Un enlace NBMA no es ni un medio de Broadcast ni un enlace punto-a-punto. Usando PVCs, las redes NBMA (FR, ATM, X.25) proporcionan múltiples conexiones con una sóla interfaz, lo que puede ser visto como una forma de LAN. La confusión surge cuando IS-IS ve que el enlace es multiacceso, como no tiene conocimiento de nubes WAN multiacceso, cree que el medio es alguna forma de LAN con

capacidad de Broadcast. Cisco recomienda que los enlaces sean configurados como una serie de enlaces punto-a-punto.

Características de IS-IS

- Enrutamiento jerárquico
- Comportamiento sin asignación de clases.
- Rápida inundación de nueva información.
- Rápida convergencia.
- Muy Escalable.
- Ajuste flexible del temporizador.

Estructura Jerárquica IS-IS

Se definen dos tipos de routers: Un router de Nivel 1 negocia el primer nivel de enrutamiento, encontrando el destino final dentro del área. Un router de Nivel 2 encuentra el área dentro de la que se encuentra el destino final. Ambos tipos de routers se combinan con los routers de Nivel 1-2 que corren ambos procesos de Nivel 1 y 2 y puden ser considerados como un tercer tipo de router.

- **Router de Nivel 1:** O router Intra-area. Es similar a un Stub Router en OSPF. Su conocimiento de la red es limitado al área y emplea una ruta por defecto al router de Nivel 2 más cercano para enrutar tráfico externo al área donde se encuentra. Los router de Nivel 1 tienen una base de datos de estado-enlace idéntica entre ellos.
- **Router de Nivel 2:** Router Inter-area. Son necesarios para el enrutamiento entra áreas distintas tal como los routers de backbone en OSPF. Los routers de Nivel 2 se comunican via Hellos que sólo son comprendidos entre ellos. Su base de datos de estado-enlace es también idéntica.
- **Router de Nivel 1-2:** Son routers tanto Intra como Inter-area, una característica similar a los routers fronterizos de área en OSPF, que pueden tener vecinos en diferentes áreas porque envían Hellos tanto de Nivel 1

como de Nivel 2 y por tanto pueden comunicarse con ambos tipos de routers. Almacenan una base de datos de estado-enlace de Nivel 1 y otra para el Nivel 2 con la información necesaria para el enrutamiento Inter-area.

Estos routers informan a los routers de Nivel 1 de que son routers de Nivel 2 y que pueden enviar tráfico a otras áreas. Pueden informar también a otros routers de Nivel 2 de las áreas a las que está conectado.

Enrutamiento IS-IS

Las áreas en IS-IS están definidas en el enlace, lo que significa que el router entero está en un área, al contrario que en OSPF, donde las áreas se definen el nivel de interfaz. Para que las actualizaciones de enrutamiento de Nivel 2 puedan ser intercambiadas, todos los routers de Nivel 2 deben ser contiguos. Los routers con una capa de enlace de datos común se convierten en vecinos IS-IS si los paquetes Hello que ambos intercambian cumplen ciertos criterios. El proceso difiere ligeramente dependiendo del medio, pero la información que viaja en los paquetes Hello es esencialmente la misma. Cada paquete declara el origen y las capacidades de la interfaz. Una vez formada la adyacencia de produce el intercambio de información de enrutamiento en forma LSPs, de esta manera, cada router recaba la información de las redes conectadas de cada router para crear una tabla de topología detallada e idéntica.

Para crear o mantener una adyacencia, ambas interfaces deben concordar en lo siguiente:

- El tamaño máximo del paquete (MTU) debe ser el mismo.
- Cada uno de los routers debe estar configurado en el mismo Nivel de Enrutamiento (Niveles 1 ó 2) de manera que puedan decodificar los Hellos envíados por el otro router.
- Si ambos routers son de Nivel 1 deben estar configurados en el mismo área.

- Para que un router de Nivel 1 pueda comunicarse con un router de Nivel 2, uno de ellos debe estar configurado como un router de Nivel 1-2.
- El System ID debe ser único para cada router.
- Si la autenticación está configurada, debe ser idéntica en ambos routers.

Tipos de paquetes IS-IS

- Los intervalos de envio de Hellos (incluído el Holddown timer) deben coincidir, de otra manera resultaría en un enlace que flapea o cálculos DPF interminables.

  Existen 3 tipos de paquetes:

- Hello. Crean y mantienen relaciones entre vecinos y adyacencias. Pueden ser:
  - LAN Nivel 1. Generados por routers de Nivel 1 ó 1-2.
  - LAN Nivel 2. Generados por routers de Nivel 2 ó 1-2.
  - Punto-a-Punto. Generados por routers de Nivel 1, 2 y 1-2.

- LSP Llevan información sobre los vecinos conectados al router. Pueden ser de dos tipos:
  - Nivel 1. Generados por routers de Nivel 1 ó 1-2.
  - Nivel 2. Generados por routers de Nivel 2 ó 1-2.

- Paquete de Número de Secuencia (SNP). Describen los LSPs en la BBDD de estado-enlace del router que transmite. La información es condensada y nunca inundada, sino que sólo es vista entre vecinos. Los SNP aseguran la sincronización de la BBDD de estado-enlace mediante grupos de distribución de LSPs en LAN y sin ACKs explicitos individuales, ACKs de LSPs individuales y, por último, la petición de LSPs al iniciarse. Existen dos tipo de SNP para cada Nivel de enrutamiento:

- SNP Completo (CSNP), que incluye cada LSP en la BBDD: Nivel 1 y Nivel 2.
- SNP Parcial (PSNP), Incluye un subconjunto de LSPs, empleado para solicitar LSPs individuales y agradecer la recepción de estos LSPs: Nivel 1 y Nivel 2.

Comparación de los protocolos OSPF e IS-IS

IS-IS y OSPF, son protocolos de estado de enlaces que utilizan el Algoritmo de Dijkstra para encontrar el mejor camino a través de la red. Ambos soportan máscaras de subred de diferente longitud, pueden usar multicast para encontrar routers vecinos mediante paquetes hello y pueden soportar autentificación de actualizaciones de encaminamiento. El protocolo OSPF bien podría ser el más utilizado en redes corporativas grandes, mientras que el protocolo IS-IS es más común en redes de proveedores de servicios. OSPF solamente enruta paquetes IP dentro de un único dominio. Este protocolo obtiene información sobre la receptor parte de los otros nodos y construye el mapa de la topología, la cual determina a su vez la tabla de enrutamiento que se le presenta a la capa de red. OSPF es rápido en detectar cambios en la topología (enlaces dañados, por ejemplo) y toma simples segundos en converger a una nueva estructura de enrutamiento. La información de estado de enlace es guardada en cada enrutador como una base de datos de la topología. Estas copias son todas puestas al día periódicamente difundiendo paquetes DBD (del inglés, Database Description) a través de toda la red. Una red corriendo el protocolo OSPF puede ser subdividida en áreas para simplificar la administración y optimizar el tráfico y el uso de recursos. Las políticas de enrutamiento son gobernadas por métricas externas asociadas a cada interface. Estas métricas incluyen la distancia entre enrutadores (tiempo del viaje ida y vuelta), congestionamiento del enlace (o en su defecto, la velocidad a la cual se pueden transmitir los datos), la disponibilidad y confiabilidad

de los enlaces. Todos estos factores influyen y ayudan a mantener un balance dinámico de la carga entre rutas de igual métrica.

Existen diferencias importantes en el modo de operar de IS-IS y OSPF, por ejemplo, en el modo en que la dirección de área es asignada. En IS-IS, la dirección de área y de host son asignados al router entero, mientras que en OSPF el direccionamiento es asignado al nivel de interfaz. Por lo tanto un router IS-IS unicamente estará en un área (Todos los routers de Nivel 1 necesitan un router de Nivel 1-2 para conectarles a otra área). El router de Nivel 1-2 puede ver el resto del SA y se ofrece como ruta por defecto al área de Nivel 1. Es importante también la diferencia entre estos protocolos de manejar los paquetes hello. Este es el único método por el cual los routers pueden saber si un router vecino sigue estando disponible en la red. A diferencia de OSPF, los routers IS-IS son capaces de enviar dos tipos diferentes de saludos (paquetes hello). Los routers IS-IS pueden ser de Nivel 1, Nivel2 o Nivel 1-2, los routers CISCO son routers L1-L2, por lo que cada interfaz IS-IS estará habilitada para enviar tanto mensajes hello L1 como L

Diferencias

- Mientras que IS-IS opera en la parte superior de la capa 2, OSPF opera en la capa 3.
- IS-IS es un protocolo de capa 3 con su propio paquete de capa 3, mientras que OSPF utiliza paquete IP.
- la fragmentación es responsabilidad de IS-IS, sin embargo en OSPF la fragmentación es responsabilidad de IP.
- IS-IS tiene compatibilidad con IPv6 o que admite VLSM.

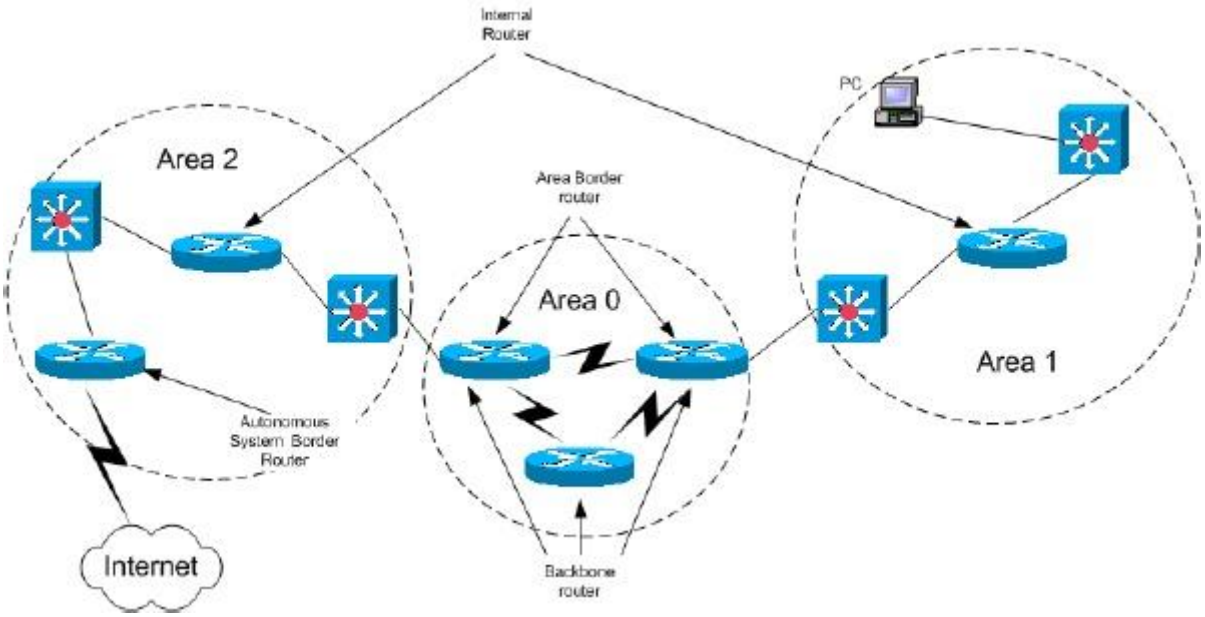

Figura 18 Muestra la jerarquía de enrutamiento en diferentes áreas

Algoritmo de encaminamiento Dijkstra

El algoritmo puede ser descrito como:

N= conjunto de nodos en la red.
S = nodo origen.
M = conjunto de nodos incorporados en un instante t por el algoritmo.
D ij = el coste del enlace del nodo i al nodo j. Teniendo en cuenta que:
Dii = 0;
Dij = infinito si los dos nodos no están conectados directamente.
Dn = coste del camino de coste mínimo desde un nodo s hacia un nodo n que es conocido por el algoritmo.

El algoritmo tiene tres pasos; los pasos 2 y 3 son repetidos hasta que M = N, es decir, se han calculado todos los caminos posibles con todos los nodos de la red.

1.- Inicializar:
M = {s}
Dn = dsn para n<>s
2.- Encontrar el nodo vecino que no está en M tal que
Dw = min DjDw = min Dj
Y j no pertenece a M.
Añadir w a M.

3.- Actualizar el camino de coste mínimo :
Dn = min [Dn, Dw + dwn] para todo n no perteneciente a M.

Si el último termino es el mínimo, el camino desde s hasta n es ahora el camino desde s hasta w concatenado con el enlace desde w hasta n.

Tipos de enrutamiento

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados. OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de enrutamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database) de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser parcelado en su área.

- **Enrutamiento Estático:** El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

  - Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
  - Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.

- Existe una sóla conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

- **Enrutamiento Predeterminado:** Es una ruta estática que se refiere a una conexión de salida o Gateway de último recurso. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0.

- **Enrutamiento Dinámico:** Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

Tráfico de enrutamiento

OSPF mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- **Paquetes Hello (tipo 1):** Cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.

- **Paquetes de descripción de base de datos estado-enlace (DataBase Description, DBD) (tipo 2):** Se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.

- **Paquetes de estado-enlace o Link State Advertisements (LSA):** Los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estatus del router y el tipo de información transmitido en el LSA, se distinguen varios formatos (entre paréntesis, las versiones de OSPF en que se utilizan):

  - (OSPFv2 y v3) Router-LSA o LSA de encaminador.
  - (OSPFv2 y v3) Network-LSA o LSA de red.
  - (OSPFv2 y v3) Summary-LSA o LSA de resumen. En OSPFv2 se distinguen dos tipos: tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna. En OSPFv3, los Summary-LSA tipo 3 son renombrados como Inter-Area-Prefix-LSA, y los tipo 4 pasan a denominarse Intra-Area-Prefix-LSA.
  - (OSPFv2 y v3) AS-External-LSA o LSA de rutas externas a la red.
  - (OSPFv3) Link-LSA o LSA de enlace, que no se retransmite más allá del link del origen.

GLOSARIO

GMPLS Generalized Multi-Protocol Label Switching

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IP Internet Protocol

IS-IS Intermediate System-Intermediate System

LER Label Edge Router

LSA Link State Advertisement

LSP Label Switched Path

LSR Label Switch Router

MPLS Multi-Protocol Label Switching

NGTN Next Generation Transport Network

NMS Network Management System

NNI Network to Network Interface

OSPF Open Shortest Path First

PCC Path Computation Client

PCE Path Computation Element

PCEP Path Computation Element Communication Protocol

QoS Quality of Service

RSVP Resource reservation Protocol

TCP Transmission Control Protocol

TE Traffic Engineering

TED Traffic Engineering Database

WDM Wavelength-Division Multiplexing

Conmutación de paquetes: Esta basada en el contenido de la cabecera del paquete

Conmutación de celdas y/o frames: Se basa en el contenido de la cabecera de la celda o frame

Conmutación en tiempo (TDM): Basada en el slot temporal de un ciclo repetitivo en el que se reciben los datos.

Conmutación de longitud de onda (DWDM): Basada en la longitud de onda en la que se reciben los datos.

Conmutación en el espacio: basada en la fibra o puerto por la que se reciben los datos.