UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Ingeniería

Implementación de Redes Privadas Virtuales con MPLS

TESIS

que para obtener el Título de:

Ingeniero en Telecomunicaciones

Presenta:

Jonathan Mora Cuevas

Asesor: Ing. Rodolfo Arias Villavicencio

Ciudad Universitaria, 2003.

A

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS Y TABLAS

Estructura de la tesis

El objetivo de esta tesis es plantear los fundamentos teóricos para poder entender e implementar MPLS como tecnología subyacente para construir una VPN en la red de un Proveedor de Servicio a fin de brindar conectividad entre sitios de una empresa que necesitan intercambiar información entre sí.

Antes de empezar a leer esta tesis, se deben tener conocimientos acerca del modelo de referencia OSI además de la pila de protocolos TCP/IP y los procedimientos de comunicación que estos establecen. Para ayudar un poco a entender esto, al final de la tesis se anexa un glosario para explicar los términos que aquí se manejan.

Como primera parte, en el Capítulo 1 se trata de llevar al lector a través de la historia de las VPN's y de las tecnologías disponibles para su implementación. Se plantean los requerimientos de conectividad que se han ido presentando a las empresas a medida que se expanden y como se han ido satisfaciendo dichos requerimientos a través de las soluciones planteadas por los Proveedores de Servicio. Como se explica, en base a la tecnología de red con la que se contaba, se planteaba la solución. Así, la meta de los Proveedores de Servicio era mejorar dichas tecnologías para brindar servicios de conectividad, entre ellos las VPN's, persiguiendo metas claras como:

- Disminuir los costos de los servicios
- Facilitar la implementación de los servicios
- Proveer escalabilidad en sus redes
- Tener compatibilidad con las tecnologías existentes

Después de explicar este proceso, dando ventajas y desventajas de construir VPN's con las distintas tecnologías existentes, en el Capítulo 2 se dan bases teóricas de los fundamentos de enrutamiento, es decir, los mecanismos empleados para transportar la información de un nodo a otro de la red.

El Capítulo 3 explica de fondo el estándar MPLS, su arquitectura y su operación. Este Capítulo es importante dado que constituye la base teórica de la nueva tecnología MPLS. Se explican además los beneficios que conlleva implementar esta tecnología en la red de un SP's en comparación con los métodos tradicionales de envío de información además de mencionar los distintos servicios que se pueden implementar si se tiene MPLS habilitado.

En el Capítulo 4 se da un panorama general de las distintas topologías existentes de VPN's y como estas solucionan las necesidades de comunicación de las empresas que se encuentran distribuidas geográficamente y que necesitan intercambiar información entre sí. También, en este capítulo de explica el paradigma MPLS/VPN's dando razón de todos los

conceptos involucrados en este paradigma además de explicar la operación en conjunto con los protocolos de enrutamiento necesarios para transportar la información requerida.

En el Capítulo 5 se explica la forma en que deben de ser configurados los dispositivos de red involucrados a fin de poner en operación una VPN bajo tecnología MPLS. Igualmente para este capítulo se asume que ya se tiene noción en la configuración de los protocolos de enrutamiento. Primeramente se explican los requerimientos básicos necesarios que un cliente necesita para cubrir sus necesidades de conexión. En base a ello se presenta un diseño a fin de implementarse en la red de un proveedor de servicio Internet. Con este planteamiento, se procede a mostrar la forma en que se configuran los equipos dando algunas descripciones del proceso que se sigue.

Al final se incluyen, en el Capítulo de conclusiones, los beneficios de construir VPN's con el estándar MPLS, mostrando que esta es una alternativa que beneficia tanto al cliente como al proveedor de servicios.

Capítulo 1. Introducción

La creación e implementación de estándares de comunicaciones que provean maneras seguras y confiables para comunicar varias entidades se ha vuelto una premisa en el área de comunicaciones.

A medida que las empresas se expandían, se fue necesitando que sus nuevas sedes se comunicaran con el sitio central o entre sí. Ante ello, algunas empresas apostaban por la construcción de sus propias redes privadas para poder comunicar varias de sus entidades o sitios. Obviamente, esto conllevaba costos como la capacitación del personal para operar dicha red, además del mantenimiento de la tecnología empleada para implementar su red. Para una empresa grande la opción de construir una red privada representa una opción viable, no así para pequeñas o medianas empresas.

Como alternativa a ello, algunos proveedores de servicio (SP, *Service Providers*) decidieron brindar un servicio de conectividad, de manera que las empresas pudieran contratar dicho servicio que consiste en emplear la infraestructura de red del SP para interconectar sus sitios. Así las empresas evitarían los gastos de capacitación y administración de su red privada.

De esta manera los SP's plantearon como solución al problema de conectividad las redes privadas virtuales (VPN's, *Virtual Private Networks*). Una red privada virtual es una red de datos que actúa como una extensión de una red privada de una empresa pero que opera sobre una infraestructura compartida, que puede ser la red compartida del proveedor de servicio o la red pública de Internet. Las VPN's habilitan a las empresas compartir información importante con oficinas remotas, usuarios móviles y socios de negocios en forma privada.

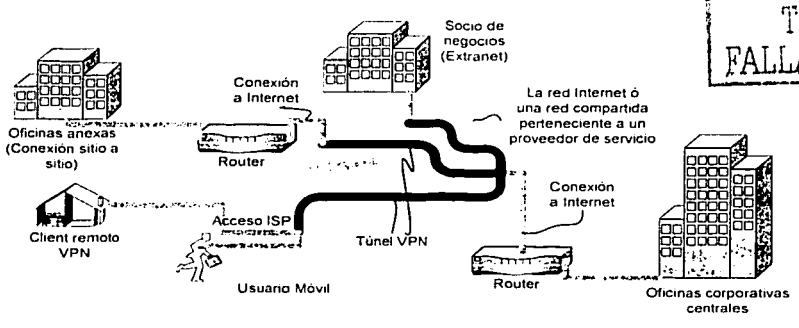


Figura 1.1 Servicios VPN's

PAGINACIÓN DISCONTINUA

Las distintas tecnologías empleadas para brindar servicios VPN's cambian constantemente, siempre con la idea de eliminar las limitaciones de tecnologías anteriores. La creación de tecnologías para la implementación de VPN's ha sido rápido. Primero con la utilización de tecnologías de capa 2, bajo el paradigma orientado a conexión a través de enlaces dedicados y circuitos virtuales FR (*Frame Relay*) o ATM (*Asynchronous Transfer Mode*). Ante sus limitantes, expuestas más adelante, y ante la creciente demanda de los servicios VPN, se planteo la creación de las VPN's bajo el paradigma no orientado a conexión, empleando la tecnología de capa 3 a través de la pila de protocolos TCP/IP, aprovechándose de la gran aceptación y difusión que ha tenido dicha tecnología. Después se pretendió mejorar el servicio para lo cual se ha creado una tecnología que no solo permite brindar un mejor servicio de VPN's sino que ha dado la posibilidad a los proveedores de servicio de mejorar el rendimiento de sus redes, así como facilitar la implementación de estos haciendo que la infraestructura existente sea sumamente escalable. Esto último es muy importante debido a que cada día se van agregando empresas que requieren conectividad y por tanto, se incrementa el uso de los recursos tanto de los SP's como de las redes compartidas como la Internet. De ahí la necesidad de que ambas infraestructuras sean robustas y escalables. Esta última tecnología es el estándar MPLS que implementa las mejores características de la tecnología de capa 2 como lo mejor de la tecnología de capa 3.

Esta variante tecnológica se ilustra con la siguiente figura.

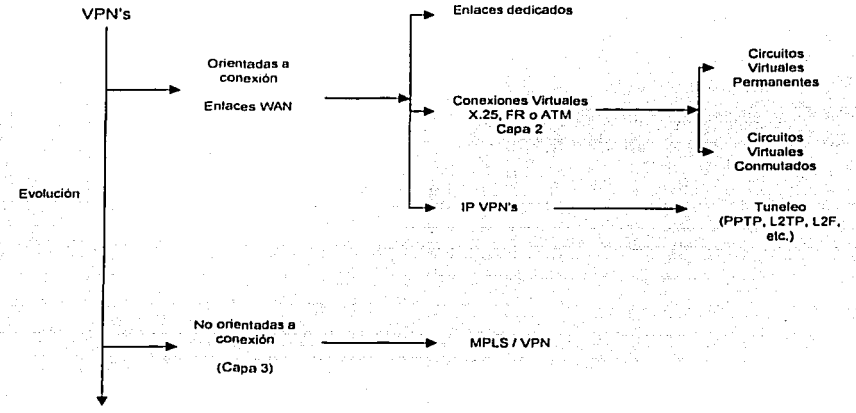


Figura 1.2 Evolución de las VPN's

1.1 Descripción de los paradigmas tecnológicos usados para implementar VPNs

A medida que las empresas se expandían geográficamente, se fueron creando necesidades de conectividad a gran escala. La distribución geográfica de estas hizo que los recursos se fueran dispersando obligando a la empresa a implementar soluciones con respecto

al acceso a estos entre los sitios pertenecientes a la empresa. Además, en ocasiones tenían que comunicarse con alguna otra empresa a fin de compartir información, lo que les llevaba a implementar una solución que les diera conectividad entre empresas.

Ante la expansión de las empresas, fueron surgiendo los usuarios móviles, los cuales debían tener acceso a la información localizada en sitios remotos o sitio centrales de la empresa, por lo que la conectividad remota se convertía en una necesidad.

Hasta no hace mucho tiempo, las VPN's basadas en tecnología de capa 2[1], como FR y ATM, constituían uno de los principales servicios que brindaban los SP's a sus clientes. Dichos SP's poseían infraestructuras de red basadas en tecnologías de conmutación de circuitos. Por ello, los SP's brindaban servicios de transporte basados en tecnologías de capa 2 utilizando enlaces dedicados o circuitos virtuales (VC, *Virtual Circuits*) para la construcción de VPN's.

Estos servicios VPN permiten la conectividad entre diferentes ubicaciones garantizando seguridad y confiabilidad en la comunicación a través de una red FR o ATM constituida por VC's que simulan conexiones punto a punto.

Estas tecnologías de capa 2 funcionan bajo el paradigma orientado a conexión, limitando el acceso no autorizado a la información que pasa por los enlaces dedicados o los VC's. Soporta la transmisión de más de un protocolo de capa de red, como IP, IPX, Decnet, etc., ya que se basa en protocolos de capa 2.

A raíz de la aparición de un nuevo estándar que permite mejorar el envío tradicional de paquetes IP, los SP's han decidido implementarlo en sus redes habilitando que estas sean mucho más rápidas. Gracias a la arquitectura de la tecnología MPLS, se puede trabajar con ambientes mixtos, es decir, con *switches* y enrutadores, además de permitir implementar una gran variedad de topologías en conjunto. El beneficio que proporciona MPLS es de considerarse, ya que además de permitir la implementación de servicios como las VPN's, permite ahorrar costos en la construcción de VPN's.

Como se puede vislumbrar, la tendencia esta en complementar la tecnología subyacente en las redes de los SP's con MPLS para mejorar el rendimiento de las mismas y para permitir brindar los servicios que las empresas demandan a través de algoritmos más sencillos y veloces de enrutamiento de información.

1.2 VPN's basadas en tecnologías de capa 2

Con el advenimiento de FR[2] a principios de los 90's, la demanda de los servicios VPN se incremento. Mas allá de proveer simplemente conectividad al cliente entre sus diferentes entidades, los SP's han sido capaces de proporcionar servicios VPN de capa 2 basados en la tecnología FR a través del uso de circuitos virtuales permanentes (PVC's, *Permanent Virtual Circuits*) y circuitos virtuales conmutados (SVC's, *Switched Virtual Circuits*)

[1] Según el modelo de referencia OSI.

[2] FR se enfilo como el protocolo que reemplazo a X.25.

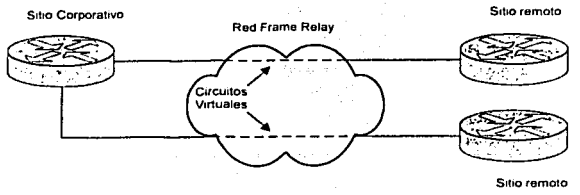


Figura 1.3 Red FR

Cuando las empresas requieren conectividad entre todos y cada uno de los sitios, los PVC's se vuelven una solución muy costosa, ya que estos VC's permanecen en línea todo el tiempo, por lo que esta solución solo es recomendable en redes parcialmente malladas. Mientras que los SVC's sería la mejor solución para redes completamente malladas, ya que estos se "prenden y apagan" de acuerdo a la demanda de tráfico de datos que se requiera.

La implementación de los PVC's se volvió más frecuente en redes FR, tanto en aquellas que funcionan como *carriers*, como aquellas que son privadas y que dan servicios de conectividad.

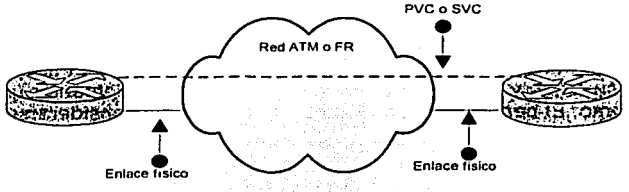


Figura 1.4 Conectividad con Circuitos Virtuales

El uso de FR como tecnología de transporte ha sido beneficioso porque provee las capacidades de las líneas dedicadas[3], pero a un costo mucho menor.

Más recientemente, los SP's comenzaron a ofrecer servicios VPN basados en ATM, que al igual que FR es una tecnología de transporte de capa 2, pero con la ventaja de proveer mayores velocidades y calidad de servicio.

ATM divide los paquetes en celdas para su transmisión por los circuitos virtuales que componen su arquitectura. A través de los circuitos virtuales que se configuran, se estaría simulando un enlace dedicado que conecta un sitio remoto con su sitio corporativo central, habilitando el paso de información seguro y garantizando la calidad de servicio. El uso de PVC's o SVC's en ambientes ATM depende del tipo de aplicación que se este requiriendo.

La naturaleza de estas tecnologías permite garantizar la calidad de servicio ya que poseen mecanismos que aseguran los parámetros que definen la calidad de servicio[4].

Supongamos un modelo de red en el que se tiene una infraestructura de red ATM que conecta enrutadores que pertenecen a una o más corporaciones con sitios conectados a ellos. La

[3] La tecnología de enlaces dedicados fue empleada antes para establecer conexiones punto a punto entre varios sitios pertenecientes a la misma corporación o empresa.
[4] Ancho de banda, retardo, variación de retardo, pérdida de paquetes y disponibilidad.

red esta constituida por *switches* WAN. Los *switches* WAN[5], no pueden ser involucrados en el proceso de enrutamiento ya que son incapaces de mantener información de capa 3 o de seleccionar una ruta para el paquete.

En ambientes WAN[6], los circuitos virtuales se configuran en los *switches* WAN, que simulan enlaces punto a punto. Básicamente conectan un extremo del núcleo WAN con otro. Una vez establecido el VC, los paquetes de capa 3 generados por un dispositivo conectado al núcleo WAN de *switches*, como un enrutador, pueden ser enviados a través del VC hasta el otro extremo a fin de que los reciba otro enrutador. Esto se puede ver en la siguiente figura.

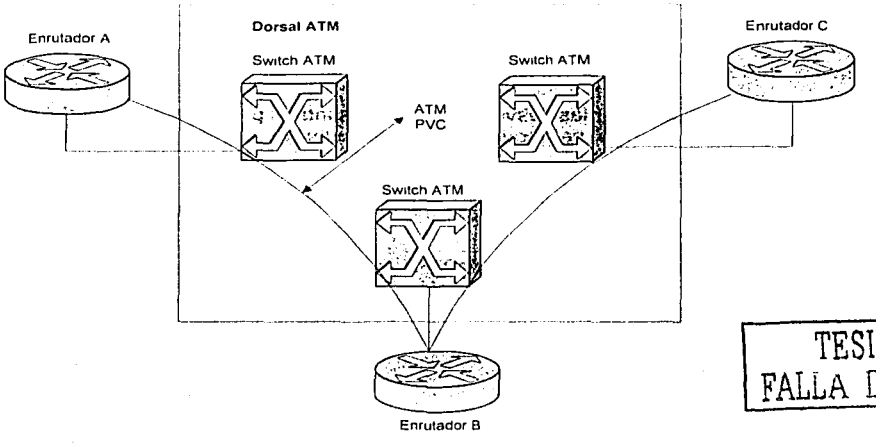


Figura 1.5 Dorsal ATM con un circuito virtual configurado

Los paquetes generados por el enrutador A que deban ser enviados al enrutador C emplearan el enlace ATM para pasar primero por el enrutador B quien lo enviara a C y después ese mismo enlace transportará los paquetes de regreso. Este comportamiento no es deseable ya que se estaría empleando el enrutador B y el *switch* del núcleo ATM cuando es posible emplear otras rutas para llevar dicho tráfico. Estas nuevas rutas se consiguen configurando un VC entre cada enrutador que se encuentre conectado al núcleo ATM.

Entonces si una empresa tiene enrutadores como dispositivos de frontera que le sirven para conectar a sus distintos sitios y desea contratar un servicio de VPN con un SP, el SP necesitará configurar VC's por cada enrutador que necesite conectarse.

Con esta panorámica se nota el problema de flexibilidad al que están expuestos estos modelos de conexión. Cuando se trata de redes pequeñas se puede configurar los VC's ya que no serían muchos pero cuando se trata de redes grandes esto se vuelve tedioso.

[5] Usualmente empleados para implementar redes ATM o FR.
[6] En ambientes LAN, los *switches* son transparentes para los enrutadores, por lo que no se requieren configuraciones adicionales. Usualmente se emplean en redes Ethernet.

Cuando se trata de redes pequeñas se puede configurar los VC's ya que no serían muchos pero cuando se trata de redes grandes esto se vuelve tedioso.

Las desventajas de tener una tecnología basada en los circuitos virtuales son:

- Para cada nuevo enrutador se debe configurar un nuevo VC hacia cada enrutador que ya este conectado a la dorsal.
- Se debe proveer el perfil de tráfico exacto entre enrutadores a fin de poder configurar cada VC.
- Con algunos protocolos de enrutamiento se necesita que los enrutadores establezcan adyacencias con sus vecinos y como son muchos se generarían grandes cantidades de tráfico en la dorsal.

A todo esto tenemos que sumar las desventajas que presenta el pagar por la renta del servicio, además de equipo adicional que se requiera para conectar la red de la empresa con los dispositivos del proveedor de servicio.

Ante estos problemas de escalabilidad se plantea encontrar nuevos métodos para proveer el servicio de VPN.

Ante la creciente demanda del servicio de VPN, y el creciente uso de la Internet además de la gran aceptación como protocolo de comunicación de IP, se pretendió brindar dicho servicio empleando tecnología IP sobre la red pública de Internet. Esto dio origen a la implementación de las VPN's con tecnología de capa 3, que es la capa del modelo de referencia OSI en el cual se desempeña IP.

1.3 VPNs basadas en tecnologías de capa 3

1.3.1 Paradigma MPLS/VPN

1.3.1.1 Envío tradicional de paquetes IP

En un inicio el objetivo de las redes de datos se limitó al paso de información desde un dispositivo origen hasta uno final. Para ello, se tuvieron que elaborar estándares de comunicación a fin de que distintas entidades usaran las mismas reglas para entablar sesiones de comunicación. Estas reglas, o protocolos, se desarrollaron, teniendo mayor aceptación la pila de protocolos TCP/IP, la cual especifica los pasos a seguir antes de que 2 dispositivos de red entablen una sesión para comunicarse.

El envío tradicional de paquetes IP esta basado en la revisión de la dirección IP destino. Cada dispositivo de red capaz de tomar decisiones acerca de la ruta en la red que un paquete debe tomar[7], usualmente enrutadores, realiza una revisión de la dirección IP destino contenida en el encabezado de capa de red del paquete, para tomar una decisión de hacia donde debe ir el paquete para alcanzar su destino final. Estos dispositivos emplean bases de datos, que contienen información de enrutamiento (rutas, métricas, etc.) la cual es recolectada por protocolos de enrutamiento dinámicos y complementada con direcciones estáticas, para decidir el camino de los

[7] Procedimiento conocido como enrutamiento, descrito en el capitulo 2.

paquetes[8].

En este proceso llamado *hop-by-hop destination-based unicast routing*, cada dispositivo toma la decisión de envío independientemente de los demás dispositivos dentro de la red, por lo que no hay un control sobre la ruta completa que un paquete toma al viajar por la red[9].

Además de estos detalles, el proceso tradicional de envió conlleva otras desventajas como lo es la distribución de carga de tráfico no proporcional. Cuando existe más de un posible camino para que viajen los paquetes, puede ocurrir que un enlace se sature y que el otro no. Ante esto, se pueden desarrollar alternativas como lo es el enrutamiento basado en políticas (PBR, *Policy-Based Routing*)[10], sin embargo al implementar PBR en los enrutadores provocaría una disminución en el rendimiento de estos ocasionando disminución en la velocidad de envío de paquetes.

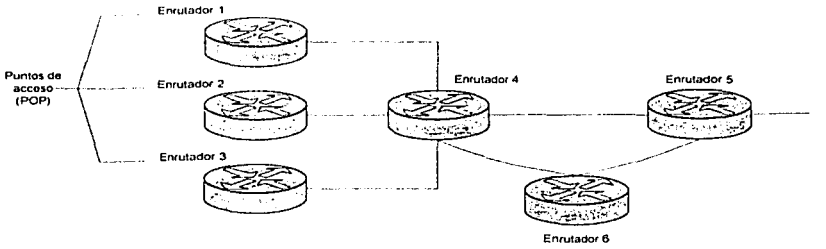


Figura 1.6 Saturación del enlace del enrutador 4 a 5

Para poder obtener mejores resultados en el envío de paquetes, sería recomendable que los enrutadores de ingreso sean los encargados de decidir la ruta completa que un paquete debe tomar a través de la red. Para lograrlo se pensó en utilizar etiquetas para configurar rutas a través de la red desde un extremo a otro. Estas etiquetas servirían para formar la ruta que los paquetes seguirían, los cuales serían previamente etiquetados al ingreso de la red. De esta forma, dependiendo de la etiqueta que se le añada al paquete, será la ruta que éste seguirá desde el ingreso hasta el final de la red.

Estos procedimientos basados en etiquetas son lo que constituyen la nueva tecnología llamada MPLS (*Multiprotocol Label Switching*) que fue diseñado para cubrir y mejorar estas y otras limitaciones del envío tradicional de paquetes IP.

Los mecanismos de la arquitectura de esta tecnología integran las mejores características del *switching* o conmutación de capa 2 con el *routing* o enrutamiento de capa 3. El método de envío esta basado en el *swapping* o cambio de etiquetas que mejoran el rendimiento del enrutamiento de capa de red, además de dar mayor flexibilidad en el provisionamiento de nuevos servicios de enrutamiento ya que no hay necesidad de alterar el método de envío de paquetes. Entre estos nuevos servicios se encuentran las redes privadas virtuales.

[8] Los paquetes que van al mismo destino tomaran la misma ruta a menos que existan dos rutas con el mismo costo, para lo cual los paquetes podrán tomar cualquiera de las dos rutas.
[9] A esto se debe el paradigma de no orientado a conexión asociado con las redes IP.
[10] Lo cual constituye una aplicación de los servicios diferenciados.

1.3.1.2 MPLS y su aplicación en VPN's

La arquitectura de MPLS se divide en dos componentes. Uno de ellos, denominado de control, se encarga de realizar las asociaciones entre las etiquetas y las rutas de capa 3, ayudado por los protocolos de enrutamiento, además de crear y mantener la información referente a las etiquetas que se envían a los demás nodos MPLS[11]. El segundo de ellos se encarga de enviar los paquetes de acuerdo a las etiquetas que llevan en su encabezado MPLS empleando para ello la información de las etiquetas asociadas a las rutas que se construyen en el componente de control. Este componente se denomina de envío o datos.

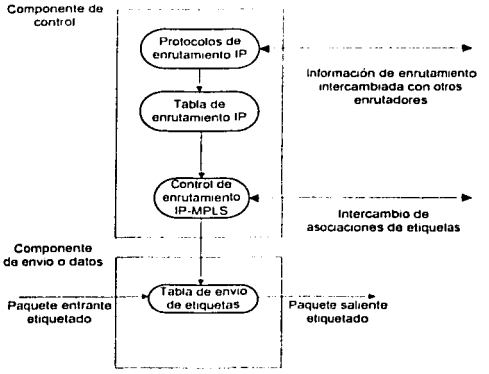


Figura 1.7 Componentes de la arquitectura de MPLS

De esta manera es como MPLS implementa los beneficios tanto de la conmutación de capa 2 con el componente de datos, como el enrutamiento de capa 3 con el componente de control.

En el componente de datos simplemente se usan las asociaciones de las etiquetas hacia las direcciones IP, que indican el siguiente salto, para mandar los paquetes por las rutas previamente configuradas con las etiquetas, realizando un simple cambio de etiqueta en cada nodo MPLS intermedio.

En el componente de control se usan los protocolos de enrutamiento de capa 3 para elaborar las tablas de enrutamiento y para realizar las asociaciones entre las etiquetas y las FEC's[12], tabla elaborada por el componente de control, para después ser distribuidas a los demás nodos MPLS usando un protocolo de distribución de etiquetas.

El estándar MPLS esta diseñado para funcionar bajo infraestructuras de red basadas en conmutación de circuitos, lo que serían las tecnologías FR y ATM, además de funcionar con ambientes de enrutadores. Se puede tener una red híbrida, formada con *switches* y enrutadores y aun así implementar el estándar MPLS.

[11] Los nodos pueden ser tanto *switches* como enrutadores.
[12] Las FEC's (*Forwarding Equivalence Class*), son Clases equivalentes de envío y pueden ser prefijos de direcciones IP, entre otras clases.

Como ya se menciono, además de mejorar el método tradicional de envío, MPLS permite la implementación de varios servicios, entre ellos VPN's. Esto se logra gracias a que su arquitectura, que a diferencia de otras tecnologías de *switching* como FR o ATM, permite transportar más de una etiqueta en el encabezado MPLS que se agrega al paquete IP. Esto es fundamental ya que como vamos a ver, se necesita además de la ó las etiquetas que indican el camino en los dominios MPLS, una etiqueta que indique a que tabla de la red privada virtual pertenecerá el paquete.

La implementación de las redes privadas virtuales con esta tecnología permite implementar las mejores características de algunos modelos empleados hasta antes de la aparición de MPLS. Como se verá más adelante, algunas topologías de red podrán ser combinadas para construir infraestructuras de red que provean servicios VPN's permitiendo a los SP's brindar las mejores características de varios modelos empleados en forma independientemente hasta antes de la aparición de MPLS.

Como se menciono, las tecnologías de capa 2, como FR ó ATM son poco escalables además de que su implementación es un poco laboriosa a través de circuitos virtuales y requiere equipo adicional. Con MPLS es mucho mas sencillo ya que es escalable, el enrutamiento es más sencillo y no requiere infraestructura adicional. El hecho de no requerir infraestructura adicional se ve reflejado directamente en el costo, lo que hace a MPLS una tecnología además de buena, conveniente.

Podemos decir que obtenemos tanto seguridad en las conexiones como el aislamiento de la información que pertenece a cada cliente VPN, además de simplificar el proceso de enrutamiento.

Con MPLS se pueden implementar servicios de ingeniería de tráfico, dando la posibilidad de hacer todo un diseño en cuanto al modo en que la información fluye. Los estándares de la ingeniería de tráfico permitirán entre otras cosas brindar ciento por ciento calidad de servicio así como realizar diseños de red en cuanto al tipo de tráfico y la forma en que será tratado.

Capítulo 2. Fundamentos de enrutamiento

Cuando nos referimos al término *routing*, o enrutamiento, hablamos de la acción de mover la información a través de una red desde un origen hasta un destino.

2.1 Componentes de enrutamiento

El enrutamiento de la información involucra dos procesos que son fundamentales. El primero de ellos es la determinación de la ruta óptima y el segundo de ellos es el transporte de la información, también conocido como *switching* o conmutación de paquetes.

2.1.1 Determinación de la ruta óptima

Los protocolos de enrutamiento emplean métricas para evaluar la mejor ruta que el paquete puede seguir desde el origen hasta el destino. La métrica es un estándar de medida y existen varias métricas empleadas por distintos protocolos de enrutamiento para ayudar a hacer la determinación de la ruta óptima.

Para ayudar al proceso de enrutamiento, los algoritmos de enrutamiento generan tablas de enrutamiento, las cuales contienen una gran variedad de información, por ejemplo las direcciones de las redes que son alcanzables por el enrutador, el siguiente "salto" que deben dar los paquetes para alcanzar un destino en particular, la preferencia por una ruta para determinados paquetes, valores de métricas[13], etc. Los enrutadores comparan las métricas para determinar la ruta óptima. Estas métricas dependen del algoritmo de enrutamiento que se este usando.

Cuando los enrutadores reciben un paquete revisan la dirección destino de éste e intentan asociarlo con una de las direcciones de siguiente salto que tengan registradas.

Los enrutadores mantienen comunicación entre sí a fin de conocer la topología de la red en la cual se encuentran. Para poder mantener actualizadas sus tablas de enrutamiento, estos se comunican empleando mensajes que se envían en periodos establecidos o cuando algún cambio ocurre en la topología de la red. Los mensajes de actualización de enrutamiento son mensajes que generalmente llevan todo o al menos una parte de la tabla de enrutamiento del enrutador que los esta emitiendo. Un enrutador concentra toda la información de los mensajes recibidos a fin de generar una imagen detallada de la topología de la red.

[13] Es una variable asignada a las rutas con el fin de clasificarlas y elegir la ruta óptima.

2.1.2 *Switching* o conmutación

El proceso de *switching* es simple y describe el proceso de transporte de los paquetes que viajan en una red para la mayoría de los protocolos de enrutamiento.

Cuando un *host*[14] requiere mandar información a otro *host* que no se encuentra en su segmento local de red, encapsula los paquetes provenientes de la capa 3 del modelo de referencia OSI, con información de control de la capa 2, usando como dirección física destino la de su *default gateway*, el cual regularmente es un enrutador. El paquete en sí lleva la dirección de red (capa 3) del *host* destino. Posteriormente se hará un cambio en la información de control de capa 2 la cual será definida por el protocolo de capa 2 (WAN o LAN) del próximo salto, permaneciendo intacta la dirección de red. Esto se hará sucesivamente hasta que el paquete llegue al destino final.

Si el *host* se encuentra en el mismo segmento de red, se busca su dirección MAC[15] en la tabla de ARP para poder enviar así el paquete. Si su dirección no se encuentra en la tabla ARP, se envía un paquete *broadcast* solicitando la dirección MAC de la máquina cuya dirección IP corresponde al destino de la información. Esta contestará con su dirección MAC de tal forma que ahora pueda iniciarse la transferencia de información. Si no hay contestación, el paquete se desechará.

2.2 Algoritmos de enrutamiento

2.2.1 Metas de diseño

Los algoritmos de enrutamiento se diferencian dependiendo de los objetivos para los que fueron creados. Sin embargo, las metas principales son las siguientes:

El que sea óptimo. Esta característica se refiere a la capacidad del algoritmo para seleccionar la mejor ruta en base a la métrica que se use y al peso que el algoritmo le asigne. Esto es, si un algoritmo emplea el retardo y el número de saltos que tiene que dar un paquete para llegar a su destino final, y le asigna mayor peso al retardo, entonces el cálculo que se realice para encontrar la mejor ruta estará más determinado por el retardo.

Simplicidad y con bajo *overhead*. Los algoritmos se elaboran lo más simple que se pueda, sin perder la eficiencia. Esto es de vital importancia cuando el algoritmo tiene que ser implementado sobre un sistema con pocos recursos físicos.

Robustez. Significa que el algoritmo debe realizar correctamente lo que deba hacer aún en situaciones no comunes y adversas, por ejemplo fallas en el *hardware*, alta carga e incluso malas implementaciones. Es importante que los algoritmos de enrutamiento funcionen adecuadamente, ya que estos se ejecutan en los enrutadores que generalmente son puntos de conexión y cuyas fallas pueden derivar en problemas mayores.

Convergencia. Esta es una característica muy importante y se refiere al proceso de acuerdo en la selección de la mejor ruta entre varios enrutadores. Cuando hay bajas o altas en las rutas, los mensajes de actualización de rutas viajan a través de la red para que sean recalculadas

[14] Termino que se refiere a una PC.

[15] Las direcciones MAC se buscan en la tabla de ARP (*Address Resolution Protocol*) que es una tabla que guarda relaciones entre las direcciones IP con sus direcciones MAC.

las mejores rutas en base a las métricas que emplee cada algoritmo de enrutamiento. Cuando algún algoritmo converge en forma lenta, puede llegar a ocasionar *loops*[16] en la red.

Flexibilidad. La flexibilidad esta determinada por la habilidad de un algoritmo de enrutamiento para hacer el cálculo de otra mejor ruta una vez detectada una alta o baja de alguna ruta. Los algoritmos de enrutamiento pueden ser configurados para que se adapten a los cambios como pueden ser referentes al ancho de banda de una ruta, el tamaño de una cola, el retardo de la red, entre otras opciones.

2.2.2 Clasificación de los algoritmos de enrutamiento

Los algoritmos de enrutamiento se clasifican en:

- Multirutas y monorutas
- *Link-state* y *distance vector*

2.2.2.1 Multirutas y monorutas

Los algoritmos multirutas son aquellos que soportan el manejo de múltiples rutas hacia un mismo destino, es decir, que el tráfico puede ser dividido sobre varias rutas disponibles para llegar al destino final. Contrario a lo que son los algoritmos que no lo soportan, los cuales solo pueden manejar una sola ruta.

Una de las ventajas de los multirutas es que proveen lo que se llama el balanceo de carga.

2.2.2.2 *Link-state* y *distance vector*

Los algoritmos de enrutamiento de estado de enlace (*link-state*) mandan información a todos los nodos de la red. Cada enrutador envía solo una parte de su tabla de enrutamiento que describe el estado de sus enlaces. Con esto los enrutadores construyen una imagen de la topología completa de la red que almacenan en sus tablas de enrutamiento. Sus mensajes son pequeños y realizan actualizaciones solo cuando han ocurrido cambios en la red.

Los algoritmos de estado de enlace requieren mayor capacidad de procesamiento en los CPU's además de mayor memoria. Son los que convergen más rápidamente evitando que se formen *loops*.

Los algoritmos vector-distancia (*distance vector*), llaman a los demás enrutadores para que envíen la información completa de sus tablas de enrutamiento, con la característica de que solo llaman a sus vecinos por lo que su conocimiento topológico de la red se limita a sus vecinos. Estas actualizaciones de tablas de enrutamiento son más pesadas que las que hacen los de estado de enlace y se realizan periódicamente. Sus implementaciones son más sencillas y requieren menos procesamiento y memoria que los de estado de enlace.

[16] Ruta donde los paquetes nunca alcanzan su destino, es decir, circulan cíclicamente a través de la misma serie de nodos de red. Contribuyen al congestionamiento en la red.

2.2.3 Clasificación de los esquemas de enrutamiento

Se pueden clasificar como sigue:

- Estáticos y dinámicos
- Planos y jerárquicos
- *Host-intelligent* y *router-intelligent*
- Intradomain y Interdomain

2.2.3.1 Estáticos y dinámicos

El esquema de enrutamiento estático emplea tablas de mapeo que se establecen antes de que se inicie el proceso de enrutamiento. Estas tablas no se alteran a menos que alguien manualmente lo haga. Este tipo de implementación de rutas estáticas funciona adecuadamente donde el tráfico es predecible y donde el diseño de la red es simple y la necesidad de escalar no es imprescindible.

Como este esquema no puede reaccionar ante los cambios que suceden en las grandes y cambiantes redes que existen ahora, no se considera apropiado. Por ello la mayoría de las redes usan esquemas de enrutamiento dinámicos, los cuales se ajustan a las circunstancias cambiantes de las redes, actualizando las tablas de enrutamiento por medio de los mensajes de actualización de enrutamiento. Cuando un cambio ha ocurrido, los mensajes obligan a que los enrutadores recalculen las rutas y envíen nuevos mensajes de actualización de rutas.

Lo que se acostumbra es que los esquemas de enrutamiento dinámico se complementen con algunas rutas estáticas cuando así sea conveniente.

2.2.3.2 Planos y jerárquicos

Algunos esquemas de enrutamiento trabajan en *espacios planos* y otros lo hacen en *espacios de niveles* o *jerárquicos.* Cuando hablamos de sistemas de enrutamiento planos, los enrutadores se dice que son pares o *peers* de todos los demás enrutadores. Cuando estamos en un sistema de enrutamiento jerárquico, hay enrutadores que por un lado forman una dorsal de enrutamiento y por otro, existen áreas formadas por una serie de entradores conectados en algún punto a la dorsal. El proceso es simple, cuando los paquetes salen de algún *host* y viajan hacia los enrutadores que no pertenecen a su área, estos envían los paquetes a los enrutadores de la dorsal, donde se redireccionan hacia el área destino. Ya en ese punto, los paquetes de nuevo van hacia los enrutadores que no forman parte de la dorsal y son enviados finalmente hacia el *host* final.

Los sistemas de enrutamiento forman grupos de enrutamiento lógicos, llamados dominios o sistemas autónomos. Los enrutadores se pueden comunicar con otros enrutadores que se encuentren en el mismo dominio o con enrutadores que se encuentren en distintos dominios. Los esquemas de enrutamiento son los que determinan que enrutadores pueden comunicarse entre sí.

Este esquema de enrutamiento es muy útil ya que permite configurar y asociar dominios a lo que serían grupos comunes de trabajo, o empresas, ya que estas están estructuradas en dominios que comparten las mismas políticas de comunicación. Con esto se reducen las cargas de tráfico de los mensajes de actualización de rutas, ya que los mensajes solo fluyen en el dominio que deben estar.

2.2.3.3 *Host-intelligent* y *router-intelligent*

Al referirnos al término *host-intelligent* hablamos de que algunos esquemas de enrutamiento asumen que el nodo final de la fuente determinará la ruta completa, esto se conoce como *source routing*. En este caso los enrutadores se limitan a almacenar y enviar los paquetes, evitando cualquier tipo de operación o cálculo.

Otros esquemas, asumen que los *host* no conocen ninguna ruta, por lo que los enrutadores son los que asumen la ruta que debe seguir el paquete a través de la red.

2.2.3.4 Intradominio y Interdominio

Algunos esquemas de enrutamiento solo trabajan dentro de un dominio o *intradominio*, lo que quiere decir los enrutadores solo pueden comunicarse con otros enrutadores que se encuentran ubicados en un mismo dominio.

El esquema complementario trabaja entre dominios o *interdominios*, lo que permite que enrutadores configurados con protocolos que empleen este esquema, se puedan comunicar con enrutadores que se encuentran en dominios distintos.

2.2.4 Métricas de enrutamiento

Los algoritmos de enrutamiento necesitan información para poder realizar sus cálculos y determinar la mejor ruta. Esta información es tomada de las tablas de enrutamiento. El como los algoritmos de enrutamiento determinan la mejor ruta esta basada en el uso de distintas métricas. Algunos son tan buenos que pueden combinar el uso de varias métricas para poder determinar la mejor ruta. Las métricas más comunes son las siguientes:

- Retardo
- Ancho de banda
- Confiabilidad
- Tamaño de la ruta
- Carga
- Costo del uso del enlace

El retardo en el enrutamiento es una métrica común que se emplea frecuentemente refiriéndose al tiempo que se emplean en mover los paquetes del origen al destino final. Depende de muchos factores como puede ser el ancho de banda del enlace, las colas de información que se forman en los nodos por los que debe pasar, además de la congestión que se presente en la red.

En ancho de banda se refiere a la capacidad del enlace para transportar paquetes. El uso de esta métrica no es definitivo ya que muchas veces el hecho de que un enlace posea mayor capacidad para transmitir los paquetes no quiere decir que sea la mejor ruta hacia el destino final.

Cuando hablamos de transmisión de información una de las cosas más importantes es que no existan errores en la transmisión. Un parámetro empleado para medir esto es la tasa de errores de bits. Entre menor tasa de errores de bit se tenga, podemos decir que existe mayor confiabilidad.

El tamaño de la ruta es posiblemente la métrica mas empleada. En algunos casos esta es determinada por los administradores de red. Cuando es así, esta métrica es la suma de los valores o costos asignados por los administradores sobre cada ruta. Esta métrica también se refiere al número de saltos que tiene que dar un paquete para llegar a su destino final.

La carga se refiere al grado de recursos que ocupan a un dispositivo. Por ejemplo el número de paquetes que se procesan o el grado de ocupación de un procesador, generalmente aplicado a los enrutadores o incluso el grado de uso de un enlace.

Por último el costo del enlace. Esta métrica es importante ya que en algunos casos cuando la información no es vital que sea transmitida en tiempo real, las empresas preferirían que se envíe por los enlaces que no tengan costos significativos, en vez de enviarse por enlaces que ocasionen costos adicionales.

2.3 Clasificación de los protocolos de enrutamiento

Los protocolos de enrutamiento tienen varias clasificaciones. De acuerdo al tipo de algoritmo y de acuerdo al tipo de esquema de enrutamiento usado.

En cuanto al esquema de enrutamiento, que involucra la jerarquía en la que se estén empleando se clasifican en:

- IGP's (*Interior Gateway Protocol*)
- EGP's (*Exterior Gateway Protocol*)

Atendiendo al tipo de algoritmo se clasifican como:

- *Distance vector*
- *Link-state*

Los protocolos *distance vector* son:

- ✓ RIP (Sus dos versiones)
- ✓ IGRP

Como *link-state* tenemos:

- ✓ OSPF
- ✓ IS-IS

Como *Path Vector* esta:

- ✓ BGP

Y como híbridos esta:

- ✓ EIGRP

Atendiendo a la clasificación de IGP's:

- ✓ RIP
- ✓ IGRP
- ✓ OSPF
- ✓ IS-IS

Como EGP's tenemos:

- ✓ EGP
- ✓ BGP

Ahora en cuanto a la información que algunos protocolos de enrutamiento manejan en sus actualizaciones, podemos incluir otra clasificación.

- *Classfull*
  - IGRP
  - RIPv1
- *Classless*
  - RIPV2
  - OSPF
  - BGP
  - EIGRP

Los protocolos que entran en la categoría de *classless* mandan la información de su máscara de red en sus actualizaciones. Esto habilita la posibilidad de manejar VLSM[17], para hacer un mejor uso del espacio de direcciones. Los protocolos *classfull* no mandan información de la máscara de subred de las rutas que anuncian, por lo que no pueden manejar VLSM.

Las redes también entran en esta clasificación. Las subredes que no pertenezcan a clases puras, es decir que no sean de la clase A, B, C o D, se clasifican como *classless*. Por ejemplo la subred 150.185.128.5 con máscara de 255.255.192.0. El término *classfull* define las redes o subredes que pertenecen a una clase pura, es decir, la definida como clase A, B, C o D. Un ejemplo de ella es la 192.168.27.0 con máscara de 255.255.255.0.

A continuación se describirá brevemente el funcionamiento y características de cada protocolo de enrutamiento mencionado.

[17] *Variable-Length Subnet Mask* (VLSM), especifica la habilidad para manejar, para el mismo número de red, una máscara de red diferente con diferentes subredes.

2.4 RIP (*Routing Information Protocol*)

2.4.1 Introducción

Es un protocolo de enrutamiento que esta basado en el bloque de protocolos que emplean los algoritmos *distance vector* desarrollados para comparar en forma matemática las distintas rutas disponibles para obtener la mejor hacia el destino final.

Este protocolo específicamente tiene dos versiones: RIP versión 1 y RIP versión 2. La diferencia más importante es que la versión dos tiene una extensión que soporta el envió de información de la máscara de subred en sus mensajes de actualización.

También habilitó el envió de más información en sus mensajes de actualización, por ejemplo a través de esta información permite el uso de un método simple de autentificación con el fin de poder construir tablas de actualización con información confiable, teniendo de esta manera tablas seguras.

RIP es uno de los protocolos que aun se emplean, sin embargo el problema de este protocolo, cuyo algoritmo surgió de algunas investigaciones académicas, es que no es escalable cuando tiene que trabajar en redes grandes, debido a limitantes de alcance.

2.4.2 Características de RIP

RIP cuenta con los siguientes procesos y características.

- Actualizaciones de enrutamiento
- Relojes de enrutamiento
- Estabilidad de enrutamiento
- Métricas de RIP

2.4.2.1 Proceso de actualización de ruta

Los mensajes de actualización de RIP actualizan toda la tabla de enrutamiento de los enrutadores. Estas actualizaciones se realizan con transmisiones de *broadcast* o por difusión ocurriendo en dos tiempos: en intervalos establecidos previamente y cuando un cambio de la topología de la red ha ocurrido.

Cuando un mensaje de actualización de enrutamiento se envía a un enrutador, y el mensaje contiene una diferencia con respecto a alguno de los registros de la tabla de enrutamiento donde llegó el mensaje, el enrutador realiza el cambio pertinente incrementando el valor de la métrica en 1 y registrando como su próximo salto al enrutador que envió el mensaje de actualización. Una característica de RIP es que mantiene exclusivamente la mejor ruta, esto es aquella que tiene la menor métrica hacia el destino final.

Una vez que el enrutador ha actualizado su tabla de enrutamiento, este envía mensajes de actualización a los demás enrutadores, aunque aún no sea el momento que tiene programado para enviar mensajes de actualización de ruta.

2.4.2.2 Relojes de enrutamiento

RIP emplea 3 relojes para manejar el envió información de enrutamiento hacia los otros enrutadores.

- Reloj de actualización de enrutamiento
- Reloj de expiración de enrutamiento
- Reloj de vaciado de ruta

El reloj de actualización de enrutamiento establece el intervalo de tiempo en el cual se van a realizar las actualizaciones de las rutas periódicamente. Esta establecido a 30 segundos generalmente y cuenta con un tiempo de más generado aleatoriamente para prevenir posibles congestiones en la red que podrían ser ocasionadas por el intento de todos los enrutadores de enviar al mismo tiempo sus actualizaciones.

Ahora, las rutas pueden ser marcadas como inválidas debido al término del tiempo que marca el reloj de expiración del mensaje de actualización, establecido a 180 seg, debido a la falta de un anuncio que indique la presencia de las rutas en cuestión sobre la red. Estas siguen siendo almacenadas por un periodo en la tabla de enrutamiento del enrutador. Este último periodo esta marcado por el reloj de vaciado de ruta que después de 240 seg. borra el registro.

2.4.2.3 Estabilidad de enrutamiento

RIP cuenta con mecanismo para tener cierta estabilidad. Por ejemplo para evitar los *loops*, o que un paquete quede atrapado en la red viajando por "siempre", se limita el número de saltos que puede dar un paquete para llegar a su destino final. Conociendo que cuando un paquete pasa por un enrutador su métrica de salto es incrementada en 1, el destino se marca como inalcanzable cuando esta métrica alcanza el valor de 16, es decir, que el máximo número de saltos permitidos para un paquete antes de llegar al destino final es de 15.

2.4.2.4 Métrica de enrutamiento de RIP

La métrica que emplea RIP está clasificada como tamaño de ruta y se refiere al número de saltos que tiene que dar el paquete para llegar de un origen a su destino. Es así como conoce la distancia entre los orígenes y destinos, siendo cada sistema intermedio un punto de incremento en la métrica.

2.4.3 Formato de paquete

2.4.3.1 RIP v1

Contiene un encabezado de 24 bytes y esta formado por 9 campos de información del protocolo.

Comando	Número de versión	Cero	Identificador de la familia de dirección	Cero	Dirección IP	Cero	Cero	Métrica

Figura 2.1 Formato de paquete RIPv1

Los campos son los siguientes:

Comando: Indica si se trata de un paquete que transporta una petición o una respuesta.
Número de versión: Indica la versión RIP que se esta usando.
Cero: Fue agregado para hacerlo compatible con las muchas versiones de RIP.
Identificador de la familia de dirección: Dependiendo del protocolo que se este manejando, es el identificador que se le tiene asignado, por ejemplo para el caso de IP es 2. Esto se debe a que RIP fue diseñado para trabajar con distintos protocolos de red.
Dirección: Especifica la dirección de la entrada que será actualizada.
Métrica: Indica cuantos saltos han sido dados durante el viaje hasta el destino.

2.4.3.2 RIP v2

La versión 2 de RIP, contiene mayor información útil en sus paquetes. Igual que RIP v1, el encabezado de RIP v2 ocupa 24 bytes con 9 campos.

Comando	Número de versión	Cero	Identificador de la familia de dirección	*Route tag*	Dirección IP	Máscara de red	Próximo salto	Métrica

Figura 2.2 Formato de paquete RIP v2

Los campos son:

Comando: Este campo indica si se trata de una respuesta o de una petición que lleva información de la tabla de enrutamiento. Cuando se trata de una respuesta puede tratarse de una respuesta a una petición o una actualización de enrutamiento que no se solicito. Como petición pedirá parte o toda la información de la tabla de enrutamiento del enrutador solicitado.
Versión: Indica la versión empleada de RIP. Para RIP 2 tiene el valor 2.
Cero: Campo sin emplear.
Identificador de familia de dirección: Como RIP esta diseñado para manejar información de enrutamiento de varios protocolos, el valor de este campo ayuda a definir el tipo de dirección de acuerdo al protocolo que se esta manejando. Para IP es de 2.
Route tag: Ayuda a distinguir que método se empleó para aprender rutas internas o rutas externas.
Dirección IP: Contiene la dirección lógica del paquete que esta entrando.
Máscara de subred: Contiene información de la máscara de subred en conjunto con la dirección IP.
Próximo salto: Contiene la dirección del próximo salto que debe dar el paquete.
Métrica: Contiene el número de saltos que ha dado el paquete en la red, incrementándose este valor al pasar por cada uno de los enrutadores por los que tiene que pasar.

2.5 OSPF (*Open Shortest Path First*)

2.5.1 Introducción

OSPF es un protocolo de enrutamiento desarrollado a mediados de los años 80's para suplir las carencias de otro protocolo de enrutamiento llamado RIP, ante la limitante que tenía este último para trabajar en redes grandes y que no eran homogéneas. Fue desarrollado por el grupo IGP (*Interior Gateway Protocol*) de la IETF (*Internet Engineering Task Force*).

Este protocolo fue desarrollado para trabajar sobre redes IP para usarse en la Internet con el algoritmo SPF (*Shortest Path First*) y fue el resultado de numerosos trabajos previos a este sentido, desarrollados para la ARPANET.

2.5.2 Características de OSPF

OSPF es un protocolo estándar de enrutamiento de estado de enlace y entra dentro de la clasificación de los protocolos IGP. Los protocolos de estado de enlace envían mensajes de estado de enlace, LSA's (*link-state advertisement*), a los demás enrutadores, los cuales son avisos que contienen información acerca de las métricas empleadas, la información referente a las interfaces de los enrutadores, además de algunas otras variables de importancia.

Con esta información el algoritmo SPF (*Shortest Path First*), bajo el cual esta construido el protocolo OSPF, calcula lo que sería la ruta más corta a un determinado nodo, además de servir para llenar lo que serían bases de datos de la topología de la red.

Se trata de un algoritmo de enrutamiento multiruta, lo que implica que soporta el conocimiento de más de una ruta hacia un mismo destino. Permite el balanceo de carga sobre enlaces que tienen igual costo y la métrica que emplea esta asociada a un costo.

Soporta el enrutamiento basado en peticiones TOS (*type-of-service*) de capas superiores. Esto es muy útil ya que permite que las aplicaciones puedan especificar una mayor prioridad a sus paquetes avisando a los enrutadores que los manejen como urgentes, por ejemplo. Lógicamente, después de determinar la urgencia de estos paquetes, el algoritmo SPF haría el cálculo de la mejor ruta en base a este campo TOS especificado en paquetes IP.

Soporta VLMS (*Variable Lenght Subnet Mask*). Esto se debe a que en los avisos LSA's, se incluye información referente a la máscara de subred IP. Con VLMS se habilita a los administradores de red poder segmentar aún más una subred previamente establecida, permitiendo hacer mucho más flexible el diseño y por tanto la utilización del espacio de IP's que se pueden asignar.

También se caracteriza por ser un protocolo intra-AS o intra-dominio, con la capacidad de poder enviar avisos a enrutadores que se encuentren en otros sistemas autónomos. OSPF puede trabajar bajo una estructura jerárquica de enrutamiento.

2.5.3 Jerarquía de enrutamiento

Cuando hablamos de una jerarquía de enrutamiento, la entidad más grande se denomina como un sistema autónomo (SA). Un sistema autónomo es un conjunto de redes bajo una administración común que comporten las mismas políticas de enrutamiento.

Los sistemas autónomos, también conocidos como dominios, pueden dividirse en lo que se denomina como áreas. Las áreas son redes contiguas en conjunto con los *hosts* que se encuentran junto a ellas.

Una de las ventajas al tener dividido en áreas un sistema autónomo es que se disminuye la información de enrutamiento que los enrutadores de cada área tienen que almacenar, siendo esta tan sólo la referente a su propia área, y el como llegar al área que interconecta a todas, es decir, la dorsal principal. Todos los enrutadores que tienen varias interfaces pueden ser miembros de varias áreas y se denominan ABR's (*Area Border Routers*), que son los que forman la dorsal principal (área 0). En si, los enrutadores de la dorsal principal forman un área OSPF. Cada uno de estos mantiene en forma separada una base de datos de la topología de la red de cada área donde se encuentra adjuntado. La topología de cada área es conocida solo por los enrutadores involucrados en dicha área, estando oculta para los enrutadores de otras áreas.

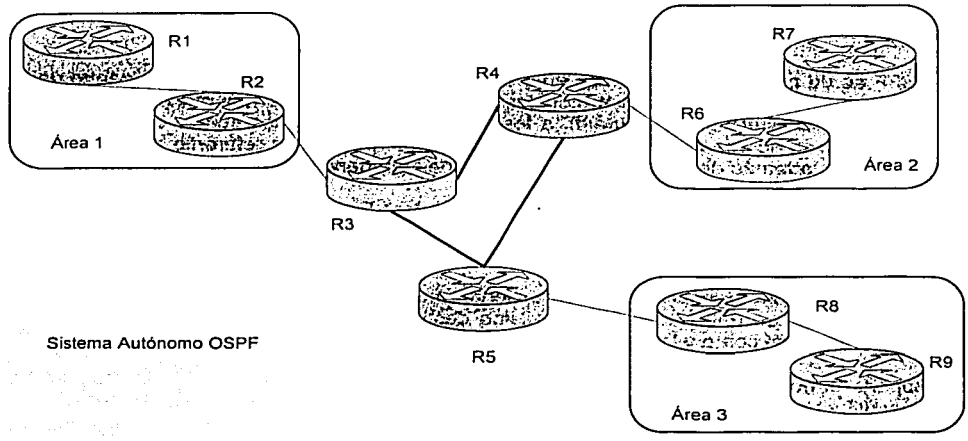


Figura 2.3 Sistema Autónomo OSPF

Las bases de datos de la topología de la red son básicamente una imagen completa de las ligas que mantienen las redes en relación a los enrutadores, y se forman con base a los LSA's (*link-state advertisements*) que envían de forma incremental a los enrutadores (es decir, sólo cuando existe un cambio en la red). Ahora como estos avisos son enviados a todos los enrutadores que se encuentran dentro de la misma área, estos enrutadores tendrán la misma base de datos de la topología de la red.

Con base a está jerarquía, se establecen básicamente dos formas de comunicarse entre los enrutadores. La primera se establece si los enrutadores involucrados se encuentran en la misma área jerárquica, conociéndose como enrutamiento intraárea. La segunda se forma cuando los enrutadores están en áreas distintas, conociéndose como interárea.

El conjunto de todos los ABR's es lo que conforman la dorsal principal, y estos enrutadores son los encargados de la distribución de las bases de datos de la topología de las distintas áreas.

2.5.4 Algoritmo SPF

Cuando un enrutador configurado para correr OSPF inicia operaciones, lo primero que realiza es iniciar una estructura de datos del protocolo de enrutamiento, para poder almacenar la información de recibirá del estado de los enlaces de los cuales estará al pendiente. Después esperará información de los protocolos de capas inferiores, como la de enlace, que le dirán si las interfaces funcionan adecuadamente y si están listas para trabajar. Una vez establecido que funcionan, SPF empleará el protocolo HELLO de OSPF que servirá para conocer cuales enrutadores están en su periferia, es decir sus vecinos. El enrutador recién prendido, enviará estos paquetes y sus vecinos le enviarán una respuesta con los mismos paquetes HELLO logrando conocer quienes son sus vecinos. Otro de los objetivos de estos mensajes HELLO es conocer si un enrutador vecino se encuentra disponible o no.

Otra de las tareas del protocolo HELLO es determinar el rol de los enrutadores cuando estos se localizan en redes que soportan o que están funcionando con más de dos enrutadores (por ejemplo en redes tipo ethernet o Frame Relay). Este tipo de redes se denominan como redes multiacceso y existen dos roles que pueden ser asignados a enrutadores en este tipo de redes. El primero es el enrutador designado, aludiendo a que esta designado para generar los LSA's de la red multiacceso y de hacer réplicas de los LSA's internos hacia el exterior. El segundo rol es el enrutador designado de respaldo.

Al tener un enrutador encargado para la generación de los LSA's, esto reducirá cargas de tráfico de información de enrutamiento, ya que no tiene caso que varios enrutadores con la misma información repliquen sus datos.

2.5.5 Formato de paquete

Los paquetes OSPF están constituidos por 9 campos comenzando con un encabezado de 24 bytes y terminando con el campo de datos, de tamaño variable.

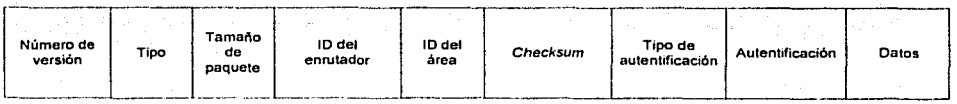


Figura 2.4 Formato de paquete OSPF

Los campos son los siguientes:

Numero de versión: Contiene la versión del protocolo OSPF que se esta empleando.
Tipo: Contienen el tipo de paquete OSPF actual.
Tamaño de paquete: Contiene el tamaño en bytes, incluyendo el encabezado.
ID del Enrutador: Contiene el identificador del enrutador origen.
ID del Área: Contiene el identificador del área al que pertenece el paquete.
Checksum: Contiene información que ayuda a saber su el paquete sufrió alguna modificación durante su tránsito del origen al destino.
Tipo de autentificación: Parámetro configurable en cada enrutador de área.
Autenticación: Contiene la información de la autenticación.
Datos: Contiene los datos.

La autenticación se realiza a través del algoritmo *Hash* MD5.

2.6 IGRP (*Interior Gateway Routing Protocol*)

2.6.1 Introducción

Es un protocolo propietario de CISCO desarrollado a mediados de los años 80's y su principal objetivo fue proveer un protocolo de enrutamiento robusto que trabajara dentro de los sistemas autónomos. En un inicio se diseño para que trabajara en redes IP, aunque después se implementó para trabajar sobre cualquier ambiente de red lográndose que CISCO lo migrara para que se ejecutase en redes CLNP (*Connectionless-Network Protocol*).

A mediados de los 80's el protocolo IGP más común era RIP, aunque sus mismas limitaciones de alcance fueron creando la necesidad de crear un protocolo de enrutamiento más robusto que satisficiera las necesidades de las redes crecientes en cuantò a tamaño y tecnología y métodos de enrutamiento.

2.6.2 Características de IGRP

IGRP es un protocolo IGP cuyo algoritmo de enrutamiento esta clasificado como *distance vector*.

Los enrutadores que ejecutan el algoritmo *distance vector*, realizan una comparación matemática de una medida de distancia como primer parámetro para determinar la mejor ruta. Esta medida de distancia se denomina como vector distancia. Los enrutadores también deben de enviar información referente a su tabla de enrutamiento, ya sea una parte o toda su tabla en sus mensajes de actualización de enrutamiento hacia sus vecinos, exclusivamente.

Soporta enrutamiento multiruta, es intradominio y es dinámico, además de tener una métrica compuesta.

La métrica compuesta se calcula en base a valores matemáticos que son tomados como factores de peso para la carga, el ancho de banda, la confiabilidad y el retardo de la red. Cada una de estas métricas pueden tomar los valores que se muestran en la siguiente tabla.

	Mínimo	Máximo
Retardo	1	2^{24}
Ancho de banda	1.2kbps	10Gbps
Confiabilidad	1	255
Carga	1	255

Tabla 2.1 Métricas de IGRP[18]

Estas métricas son complementadas por constantes que pueden ser definidas en forma manual. Estas constantes se mapean contra cada una de las métricas produciendo lo que sería una métrica compuesta.

Los valores de las métricas y el de las constantes pueden ser establecidos por el administrador, dándole la capacidad de poder influir en la determinación de la ruta escogida. Esto hace que IGRP sea un protocolo de enrutamiento muy flexible.

[18] FUENTE: *Internetworking Technologies Handbook*, CISCO.

Las actualizaciones se realizan por *broadcast* o difusión y se hace una actualización periódica completa de la tabla de enrutamiento. Se caracteriza por ser un protocolo *classfull.*

2.6.3 Características de estabilidad

Actualizaciones:

- *Holddowns*
- *Split horizon*
- *Poison-reverse*

2.6.3.1 *Holddown*

Es el tiempo durante el cual los enrutadores mantienen un cambio en alguna ruta al menos hasta que todos los enrutadores hayan sido actualizados. El tiempo es un poco mayor al que tomaría a la red completa haber actualizado sus tablas de enrutamiento.

Cuando una ruta se viene abajo en la red, un vecino se entera porque ya no le llegan mensajes de actualización de enrutamiento, entonces, este recalcula las nuevas rutas hacia los destinos que pasaban por la ruta caída y envía sus mensajes de actualización. Como estos mensajes de actualización ocurren en forma repentina (*triggered updates*), puede que no lleguen inmediatamente a todos los nodos de la red. En consecuencia, puede pasar que un enrutador que tiene que ser avisado de la caída de alguna ruta, mande sus avisos de actualización de ruta a algún dispositivo que ya había sido avisado de la falla de dicha ruta, por lo que estarían incoherentes en cuanto a la información de enrutamiento. Por esto es necesario que los enrutadores mantengan cierto tiempo algunas actualizaciones de rutas hasta que la información de enrutamiento sea coherente en toda la red.

2.6.3.2 *Split horizon*

Es un mecanismo que esta basado en la premisa de no enviar ninguna actualización de una ruta por la interfase por donde fue aprendida. Esto con el fin de prever *loops* que pudieran afectar el desempeño de la red.

Por ejemplo teniendo dos enrutadores, el A y el B, siendo que el A tiene la red A mas cerca que B. El enrutador A envía en sus mensajes de actualización a B que puede alcanzar la red A a través de él mismo. El enrutador B no tiene porque enviar en sus actualizaciones hacia A ninguna ruta que involucre la red A, ya que el enrutador A esta más cerca que el B por lo que sería innecesario. La situación es esta: si el enlace hacia la red A falla, y si no se tuviera la regla *split horizon*, el enrutador B le diría en sus mensajes al enrutador A que puede alcanzar la red A a través del mismo enrutador A, lo que sería un error. Si se tiene habilitada la regla, el enrutador B no avisaría de las rutas que el mismo enrutador A conoce y no se producirían *loops* en la comunicación.

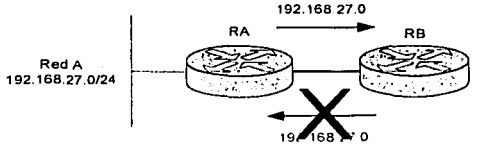


Figura 2.5 Regla *Split Horizon*

2.6.3.3 *Poison-reverse update*

Este tipo de actualizaciones son llevadas a cabo para prevenir *loops* en redes grandes, un poco para complementar las reglas de *split horizon* que están para prevenir los *loops* entre enrutadores adyacentes.

Cuando una ruta de red es aprendida por un enrutador a través de otro enrutador que no esta directamente conectado a dicha red, el primero colocara una métrica infinita hacia el enrutador que no esta directamente conectado a la red. El siguiente ejemplo, lo muestra gráficamente.

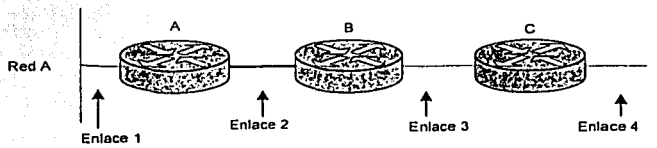


Figura 2.6 Regla *Poison-reverse update*

1. El enrutador C sabe que alcanza a la red A.
2. En caso de que el enlace 2 se caiga, sin *Poison Reverse Update*, B recibiría una actualización de C indicándole que puede alcanzar la red A por medio de C, acción no posible porque el enlace 2 no esta levantado.
3. Para evitar este *loop*, B le pone una métrica infinita a C, para que no piense en C como una posible ruta para llegar a la red A.

2.6.4 *Timers*

IGRP mantiene una serie de variables y temporizadores que le ayudan a controlar sus procedimientos como las actualizaciones periódicas que realiza, entre otras cosas.

El primer temporizador se llama de **actualización**, y especifica el periodo en el que debe de enviarse un mensaje de actualización de enrutamiento a los enrutadores vecinos. Por omisión tiene un valor de 90 segundos. El siguiente temporizador se denomina de **ruta inválida** y determina el tiempo que debe de esperar un enrutador por algún mensaje de actualización de una ruta antes de declararla inválida. El valor para esta variable es por defecto de tres veces el tiempo de la variable de actualización, o sea 270 segundos.

Existe una tercera variable que determina el tiempo de *holddown*, por defecto es de tres veces el periodo de actualización mas 10 segundos, se llama ***hold-time***. Por último el temporizador de **flujo**, que determina cuanto tiempo debe pasar para eliminar una ruta de la tabla de

enrutamiento, vale 630 seg.

2.6.5 Tipos de rutas IGRP

IGRP anuncia tres tipos de rutas: internas, externas y de sistema.

Las rutas internas son rutas de las subredes que están en la red adjunta a la interfase del enrutador. Las rutas externas son aquellas que no pertenecen al sistema autónomo al que pertenece el enrutador. Las rutas de sistema son rutas que están dentro del sistema autónomo. Las rutas de sistema no incluyen información de las subredes. En la siguiente figura se ilustran estas rutas.

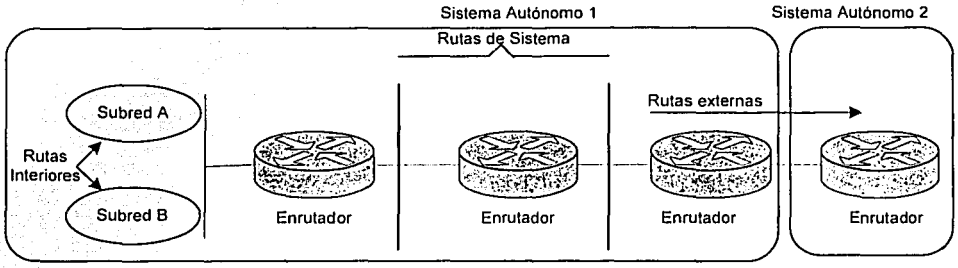


Figura 2.7 Tipos de rutas IGRP

2.6.6 Formato de paquete

El paquete de IGRP consta de 8 campos. Un mismo paquete puede contener múltiples entradas, máximo hasta 104. Las entradas siguen inmediatamente de este encabezado de paquete IGRP.

Código OP	Edición	Número de Sistema Autónomo	Número de rutas interiores	Número de rutas de sistema	Número de rutas exteriores	Checksum

Figura 2.8 Formato de paquete IGRP

Los campos son:

Versión: Actualmente con valor 1.

Código OP: Cuando son paquetes de petición IGRP vale 1 y cuando son de actualización IGRP es 2.

Edición: Este campo evita aceptar una actualización anterior a la más reciente. Su valor siempre se incrementa cuando ocurre un cambio en la información de enrutamiento.

Número de Sistema Autónomo: Se refiere al ID (identificador) del proceso IGRP. Permite que múltiples procesos IGRP intercambien información empleando un mismo enlace de datos común.

Número de Rutas Interiores: Número de entradas en la actualización que son subredes de una red conectada directamente.

Número de Rutas del Sistema: Número de rutas de redes que no están conectadas directamente. Por ejemplo rutas que han sido sumarizadas por un enrutador de frontera.

Número de Rutas Exteriores: Número de rutas de redes que han sido identificadas como redes por *default.*

Checksum: Se calcula sobre el encabezado IGRP y todas las entradas empleando complemento a uno de 16 bits de la suma.

2.7 EIGRP (*Enhanced Interior Gateway Routing Protocol*)

2.7.1 Introducción

EIGRP fue el resultado del constante cambio en cuanto a la diversidad y el tamaño de las redes actuales. Su arquitectura esta basada en módulos y soporta por si mismo múltiples protocolos de capa de red existentes. Sus capacidades y eficiencia se ve mejorada al implementar los beneficios de los algoritmos *link-state* junto con los *distance vector*, clasificándose como híbrido.

EIGRP es la versión actualizada de IGRP, agrega mas funcionalidades que lo hacen un protocolo de enrutamiento sumamente robusto y estable, y tiene una excelente compatibilidad con su antecesor IGRP. Las rutas son fácilmente importables y exportables de IGRP a EIGRP y viceversa. Las métricas pueden emplearse indistintamente para ambos protocolos ya que son fácilmente trasladables, si es que son empleadas por enrutadores dentro de un mismo sistema autónomo.

EIGRP posee un conjunto de protocolos adicionales que le hacen ser un protocolo de enrutamiento más eficiente en comparación con los basados en algoritmos vector-distance.

2.7.2 Características de EIGRP

Las principales capacidades que provee EIGRP que sobresalen en comparación con los otros protocolos de enrutamiento son:

- Rápida convergencia
- Soporte de VLMS
- Actualizaciones parciales
- Soporte para múltiples protocolos de capa de red

Para ciertos tipos de paquetes que maneja EIGRP, se manejan lo que son transmisiones *multicast* en lugar de *unicast*. Esto permite que varias entidades puedan recibir en una única transmisión información referente al estado de los vecinos, lo que ocasiona un tiempo de convergencia menor que otros protocolos de enrutamiento.

El soporte de VLMS permite que las rutas puedan ser sumarizadas, lo que provoca que las tablas de rutas sean de menor tamaño y que cierta información de enrutamiento sea menos densa.

Los enrutadores que corren EIGRP almacenan las tablas completas de enrutamiento de sus vecinos, lo que les permite fácilmente encontrar rutas alternas y si no las encuentran lanzan peticiones a sus vecinos solicitando información sobre rutas alternas. Las actualizaciones de información de enrutamiento son parciales y ocurren solo cuando la métrica de una ruta ha cambiado. Las actualizaciones son parciales para no enviar información que puede estar ya contenida en los demás enrutadores, lo que ahorra consumo en ancho de banda, y se limita sólo a aquellos enrutadores que necesitan ser actualizados.

La capacidad de EIGRP para trabajar con múltiples protocolos de red le hacen sumamente escalable, además de que puede adaptarse para trabajar con nuevos protocolos de capa de red desarrollados por distintas entidades de acuerdo a sus necesidades.

Las tecnologías que permiten que EIGRP soporte múltiples protocolos de red, además de mejorar los tiempos de convergencia y de soportar solo actualizaciones periódicas son descritas en seguida.

2.7.3 Tecnologías fundamentales de EIGRP

Las cuatro tecnologías que permiten un mejor desempeño de EIGRP sobre los demás protocolos de enrutamiento son:

- *Neighbor discovery/recovery*
- RTP (*Reliable Transport Protocol*)
- *DUAL finite-state machine*
- *Protocol-dependent modules.*

2.7.3.1 *Neighbor discovery/recovery*

Este mecanismo se basa en el envió de pequeños mensajes *hello.* Estos son enviados periódicamente a los vecinos. Una vez recibidos, el enrutador lo interpreta como una señal que indica que están listos para intercambiar información. Este mecanismo habilita a los enrutadores para conocer si un vecino es alcanzable y esta funcionando, permitiéndoles aprender dinámicamente acerca de otros enrutadores que se encuentran directamente conectados a su red.

2.7.3.2 RTP (*Reliable Transport Protocol*)

Este mecanismo es el encargado de garantizar que los paquetes EIGRP sean entregados a todos los vecinos. Este protocolo será el responsable de que los tiempos de convergencia sean bajos.

Cuando estamos en un medio donde hay soporte *multicast*, como es el caso de la tecnología *Ethernet*, RTP aprovecha esta capacidad para enviar solo un paquete *multicast* del tipo *hello* en lugar de transmitir paquetes *unicast* hacia los enrutadores vecinos en forma individual. Este tipo de paquetes son los que no se requiere que sean entregados en forma confiable, por cuestiones de eficiencia. En cambio algunos otros paquetes EIGRP necesitan ser enviados en forma confiable como es el caso de los paquetes de actualización.

Cuando se envían paquetes EIGRP en forma no confiable, el paquete contiene un indicador que le informa al receptor que no es necesario hacer un reconocimiento de dicho paquete. En cambio, cuando se envía un paquete en forma confiable, este indicador le dice al receptor que debe existir un reconocimiento de dicho paquete.

2.7.3.3 *DUAL finite-state machine*

Este algoritmo involucra el proceso de cálculo relacionado con todas las rutas advertidas por todos los enrutadores vecinos. Emplea información de distancia para seleccionar rutas libres de *loops* y para elegir aquellas rutas que han de ser agregadas a las tablas de enrutamiento a través de los *feasible successors.*

Los *feasible successors* son enrutadores que se encargan del envío de paquetes a través de las rutas con el menor costo hacia un destino, garantizando que la ruta elegida no forma parte

de un camino con *loops*. Estos son empleados para evitar hacer recálculos de las rutas cuyas métricas han cambiado. Esto es, cuando la métrica de una ruta cambia, el algoritmo de actualización por difusión (DUAL) revisa si existe un enrutador *feasible sucesor*, si sí, no se realiza el recálculo para encontrar la mejor ruta. Si no existe un *feasible sucesor*, el recálculo es obligatorio para determinar el nuevo *feasible sucesor*. Este recálculo se llama cálculo por difusión y comienza con el envió de un paquete de petición de un enrutador hacia todos sus vecinos. Cada uno de estos vecinos puede enviar dos tipos de respuestas: la primera para indicar que tiene un *feasible successor* disponible para la ruta y la segunda que indicaría que esta participando en el recálculo. Después de recibir respuesta de cada uno de los vecinos, el enrutador puede alterar la información del destino en la tabla de enrutamiento y elegir un nuevo *feasible successor*.

2.7.3.4 *Protocol-dependent modules*

Estos módulos son los encargados de cumplir los requisitos específicos de cada protocolo de capa de red. Los protocolos más comunes para los cuales provee soporte son IPv4, AppleTalk e IPX.

2.7.4 Componentes de enrutamiento para EIGRP

Para poder desempeñarse como protocolo de enrutamiento, EIGRP se basa en cuatro conceptos fundamentales.

2.7.4.1 Tablas de vecinos

Cuando un nuevo vecino es encontrado, la información referente a su interfase y su dirección es almacenada en la tabla. También se almacena información que emplea el RTP. Esta información son números de secuencia que sirven para llevar un control de los reconocimientos y los paquetes. Para poder detectar cuando los paquetes están en desorden, se almacena el último número de secuencia enviado por un enrutador.

Por cada modulo de dependencia de protocolo de red existe una tabla de vecino. Cuando un paquete *hello* se envía, lleva asociado un tiempo que determinará el tiempo que un vecino considerará alcanzable y funcional al enrutador emisor. Si durante este tiempo no es recibido algún otro paquete *hello*, entonces el emisor se determina inalcanzable y automáticamente este cambio en la topología de la red es informado al algoritmo de actualización por difusión.

2.7.4.2 Tablas de la topología

Estas tablas contienen todos los destinos anunciados por los enrutadores vecinos además de una lista de los vecinos que han anunciado dichos destinos y las métricas por cada vecino.

En cuanto a la métrica, se anunciará la menor resultante de sumar la ruta advertida de todos los vecinos más el costo de la interfase por donde se aprendió dicha ruta.

2.7.4.3 Estados de ruta

Indican el estado en que se encuentra una ruta hacia un destino. Cuando un enrutador no realiza un recálculo referente a un destino se dice que la ruta esta en estado pasivo. Cuando se

realiza el recálculo, se dice que esta en estado activo. Evidentemente cuando existe un *feasible successor*, las rutas estarán en estado pasivo.

2.7.4.4 Etiquetado de ruta

EIGRP soporta rutas internas y rutas externas. Las rutas internas serán aquellas asociadas a dispositivos que se encuentren conectados directamente a los dispositivos de red que estén configurados para ejecutar EIGRP dentro del sistema autónomo EIGRP. Las rutas externas serán las aprendidas por otros protocolos de enrutamiento o aquellas rutas estáticas que residan en las tablas de enrutamiento.

Las rutas externas son etiquetadas con la siguiente información:

- ID del enrutador EIGRP que distribuyo la ruta
- Número del sistema autónomo del destino
- Etiqueta de administrador configurable
- Identificador del protocolo externo
- Métrica del protocolo externo
- Bit como bandera para enrutamiento por defecto.

El etiquetado de las rutas permite a los administradores personalizar y tener control sobre las políticas de enrutamiento.

2.7.5 Tipos de paquetes EIGRP

Los tipos de paquetes que emplea EIGRP son:

- *Hello*
- *Acknowledge*
- *Update*
- *Query* y *reply*

Los paquetes *hello* son empleados por el mecanismo de *neighbor discovery/recovery* y no requieren de un reconocimiento. Son enviados en transmisiones *multicast*.

Los paquetes Acknowledge es un paquete *hello* pero sin datos. Siempre son enviados en transmisiones *unicast*.

Los paquetes *update* se emplean para indicar el grado de alcance de un destino. Siempre son enviados en forma confiable y cuando se ha descubierto un vecino nuevo, son enviados en transmisiones *unicast* para que puedan construir sus tablas de topología.

Los paquetes *query* son enviados en forma confiable y siempre son *multicast*.

Los paquetes *reply* son enviados en forma confiable y se envían para indicar al enrutador que origino un query que no recalcule una ruta si es que existe un *feasible successor*. Son paquetes *unicast* dirigidos al enrutador que realizó el *query*.

2.7.6 Formato de paquete

Consta de un encabezado de 7 campos con un tamaño de 20 bytes más un campo TLV de tamaño variable.

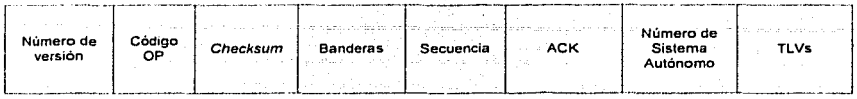


Figura 2.9 Formato de paquete EIGRP

Los campos significan:

Versión: Vale 1.
Código OP: Indica el tipo de paquete.

1. *Update*
2. *Query*
3. *Reply*
4. *Hello*
5. IPX SAP

Checksum: Se calcula sobre la porción completa de EIGRP del datagrama IP.
Banderas: El bit *INIT*, cuando vale 1, significa que la ruta contenida en ese paquete es la primera de una nueva relación de vecinos. El bit *Condicional Receive*, cuando vale 2, es empleado por el algoritmo de *Multicast Reliable* de CISCO.
Secuencia: Un número de secuencia de 32 bits que usa RTP.
ACK: La última secuencia de 32 bits que fue escuchada de un vecino. Por ejemplo, un paquete *hello* con un valor distinto de cero es un ACK.
Número de Sistema Autónomo: El número de SA del dominio EIGRP.
TLV (*Type/Length/Value*): Existen varios tipos de TLV's, pero todos comienzan por un campo de 2 bytes denominado Tipo seguido de un campo de 2 bytes que indica tamaño. Los campos que siguen dependen del valor del campo Tipo, clasificándose como sigue:

TLV's generales:
Tipo
0x0001: Parámetros EIGRP generales.
0x0003: Secuencia (Usado por *Reliable Multicast* de CISCO)
0x0004: Versión del *software* EIGRP.
0x0005: Próxima secuencia *multicast* (Usado por *Reliable Multicast* de CISCO)

TLV's IP:
Tipo
0x0102: Rutas internas IP
0x0103: Rutas externas IP

TLV's Apple Talk
Tipo
0x0202: Rutas internas *Apple Talk*
0x0203: Rutas externas *Apple Talk*
0x0204: Configuración de cable *Apple Talk*

TLV's IPX
Tipo
0x0302: Rutas internas IPX
0x0303: Rutas externas IPX

2.8 Protocolos de enrutamiento OSI

2.8.1 Introducción

La ISO (*International Organization for Standarization*) desarrolló un conjunto de protocolos para emplearse con el bloque de protocolos de OSI (*Open System Interconnection*). Éstos protocolos son: IS-IS (*Intermediate System to Intermediate System*), ES-IS (*End System to Intermediate System*) y IDRP (*Intermediate Routing Domain*).

IS-IS fue originalmente creado para trabajar en redes ISO CLNP (*Conectionless Network Protocol*) aunque después se mejoró para que pudiera soportar lo que son las redes IP.

2.8.2 Terminología de red OSI

Cuando hablamos de redes que trabajan con el estándar OSI, necesitamos definir ciertos conceptos que serían análogos a los que se emplean en la terminología de las redes IP.

En cuanto a los dispositivos "centrales" que intervienen podemos mencionar a los sistemas finales y los sistemas intermedios.

Los Sistemas Finales (ES) se refieren a los dispositivos o nodos de una red que no tienen la capacidad de enrutar la información, como los *hosts*. Los Sistemas Intermedios (IS) se refieren a aquellos nodos de red o dispositivos que tienen la capacidad de enrutar la información, como los enrutadores.

Considerando el ambiente en el que se desenvuelven estos dispositivos, se emplean términos como dominio, área, enrutamiento de nivel 1 y enrutamiento de nivel 2.

El término dominio hace referencia a un grupo de redes (o colección de áreas) que comparten una administración común además de tener un grupo de políticas de enrutamiento comunes. Un dominio de enrutamiento provee conectividad a todos los sistemas finales. Un concepto que en ocasiones se toma como análogo es el de sistema autónomo.

Cuando nos referimos a un área, hablamos de un conjunto de redes y *host* ligados que se especifican con un grupo denominado área.

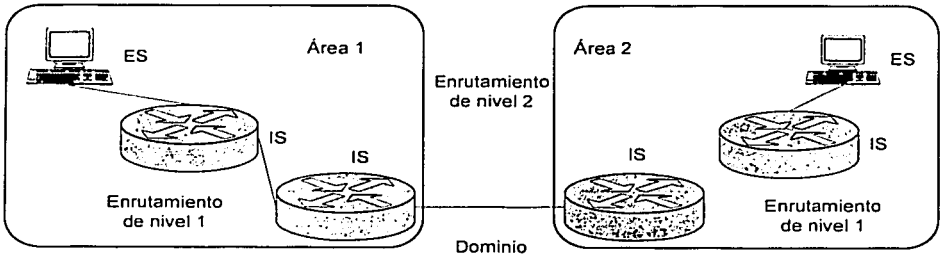


Figura 2.10 Dominio OSI

Cuando hablamos de enrutamiento de nivel 1, se hace referencia al enrutamiento que realizan los enrutadores de nivel 1 que están dentro de un área específica. El enrutamiento de nivel 2 se refiere al enrutamiento que se realiza entre las áreas de enrutamiento 1.

2.8.3 ES-IS (*End System to Intermediate System*)

ES-IS es un protocolo que especifica como los dispositivos finales aprenden de la existencia de los sistemas intermedios y viceversa.

Básicamente ES-IS es un protocolo de descubrimiento que proporciona capacidad para aprender sobre sistemas que se encuentren dentro de la misma subred. Este protocolo soporta o reconoce tres tipos de conexiones.

- Subredes punto a punto
- Subredes de *broadcast*
- Subredes de topología general

Las subredes de punto a punto proveen un enlace punto a punto entre dos sistemas como los enlaces seriales WAN.

Las subredes de *broadcast*, como la tecnología *Ethernet* y el estándar 802.3 de IEEE emplean una dirección *multicast* especial para llegar a todos los nodos de la subred.

Las subredes de topología general, como X.25 soportan un número determinado de sistemas.

El proceso que emplean para conocerse entre ES y IS se conoce como configuración.

2.8.3.1 Configuración de ES-IS

Este proceso es indispensable para que exista el enrutamiento entre los dispositivos finales. El protocolo ES -IS emplea información que manda periódicamente a los sistemas finales y a los sistemas intermedios.

Existen dos tipos de mensajes que emplea para este propósito. Los mensajes *hello* que generan los ES's y que envían a los IS's se denominan como mensajes ESH's. Los otros son mensajes *hello* que generan los IS's y que envían a los ES's, se llaman mensajes ISH's.

Estos mensajes *hello* se envían a todos los sistemas finales e intermedios que se encuentren en la subred y su propósito es enviar información acerca de la dirección de la capa de red y subred del sistema que los generó.

2.8.3.2 Información de direccionamiento ES-IS

Cuando estamos en el mundo de redes de OSI, hablamos de un direccionamiento distinto al de las redes IP. En el proceso de configuración descrito anteriormente, el protocolo ES-IS transporta la información de las direcciones de red y subred de OSI. Estas direcciones denominadas como direcciones de capa de red OSI ayudan a identificar el NSAP (*Network Service Access Point*) o la NET (*Network Entity Title*).

El NSAP es la interfase entre la capa 4 y la capa 3 de OSI, y la NET es una entidad de capa de red dentro de un sistema OSI IS. NSAP son las direcciones que emplea CLNS.

Los puntos en los cuales un ES o un IS se conectan físicamente a la subred, se denominan direcciones de subred de punto de enlace, SNPA's (*subnetwork point-of-attachment addresses*) o direcciones de subred OSI. Las SNPA's sirven para identificar a cada sistema dentro de la subred y son únicos.

2.8.4 IS-IS (*Intermediate System to Intermediate System*)

Se trata de un protocolo de enrutamiento OSI *link-state* que utiliza el algoritmo SPF, es jerárquico, dinámico y esta diseñado para trabajar dentro de un dominio de enrutamiento, o sea intradominio. Especificado por la ISO, fue diseñado para operar en OSI CLNS (*Connectionless Network Service*).

Para poder soportar dominios de enrutamiento, emplea lo que es una jerarquía de segundo nivel. Cuando se trata de dominios grandes, estos son divididos en áreas para una mejor administración, además de simplificar el diseño y la operación. Entonces el enrutamiento que se da dentro de un área se denomina como enrutamiento de nivel 1. Cuando se da el enrutamiento entre áreas se denomina como enrutamiento de nivel 2.

El hecho de que sea un protocolo jerárquico simplifica las cuestiones del diseño de la dorsal, ya que los enrutadores que están configurados como IS's de nivel 1, solo necesitan conocer como llegar la enrutador IS de nivel 2 más cercano, sin importar el área de destino al cual vaya dirigido el paquete.

De manera que si ocurre un cambio en cuanto al protocolo de enrutamiento interárea, esto no tendrá el mayor impacto en la implementación del protocolo de enrutamiento intraárea.

Los paquetes IS-IS tienen su propio formato por lo que no son encapsulados en CLNS o en IP, sino que se encapsulan directamente en la capa de enlace de datos.

En las redes OSI CLNS no existen protocolos tales como ARP, ICMP, o IDRP, sino que en vez de eso el mismo protocolo ES-IS provee el mismo tipo de reportes para los IS's y los ES's.

2.8.4.1 Métrica IS-IS

IS-IS emplea sólo una métrica la cual es definida arbitrariamente y se refiere al valor máximo de una ruta. Su valor puede tener un valor máximo de 1024. Cualquier enlace puede tener un valor máximo de 64. Para poder calcular el valor de la ruta, se suman todos los valores de los enlaces individualmente.

IS-IS define tres métricas opcionales o costos: retardo, costo y error. Sus nombres son evidentes y nos indican a que se refieren. El retardo indica la cantidad de retardo que presenta un enlace particular. El costo se refiere a lo que cuesta el uso de determinado enlace y el error indica la tasa de errores que se presenta en la transferencia de datos sobre un enlace.

Una característica de IS-IS es que emplea éstas métricas, las cuales están asociadas a lo que es la calidad de servicio (QoS)[19], para calcular las rutas a través de la red.

[19] La calidad de servicio es una opción que se habilita en el encabezado del paquete CLNP.

2.8.4.2 Operación de enrutamiento en redes OSI

Como se dijo anteriormente, en ambientes OSI, tenemos sistemas finales y sistemas intermedios dentro de un dominio de enrutamiento jerárquico.

Cuando se inician los sistemas, el sistema final (o *host*) comienza la búsqueda de IS, descubriéndolo escuchando los mensajes ISH. Cuando este *host* quiere enviar información a otro *host* lo primero que realiza es enviar la información a uno de los IS que se encuentren directamente conectados a el. El IS revisará la dirección destino y enviará la información por la mejor ruta. Como los IS's están escuchando los mensajes ESH's, sabrán si el ES destino se encuentra en la misma subred que el ES origen. Si es así entonces el IS se encargará de finalizar la conexión.

Cuando no se encuentra en la misma subred ni en la misma área, el IS enviará la información al IS de nivel 2 que continuará con el proceso a fin de alcanzar el ES final.

Todos los IS's generan mensajes de actualización *link-state* a fin de generar una imagen de la topología de la red. Estos mensajes contienen información referente a los ES's y los IS's a los que esta conectado, además de las métricas asociadas. Estos mensajes se envían a todos los enrutadores IS vecinos, los cuales inundan la red a fin de formar imágenes completas de la topología de la red.

2.8.4.3 Operaciones de enrutamiento IS-IS

Los enrutadores que corren IS-IS mandan mensajes *hello* sobre todas sus interfaces que estén configuradas con IS-IS a fin de encontrar vecinos y formar adyacencias. Para poder formar adyacencias, es necesario primeramente que estén directamente conectados además de conocer los criterios necesarios para ello. Los principales criterios son que se emplee el mismo tipo de autentificación, el tipo de IS además del tamaño de MTU[20].

Los enrutadores generan paquetes *link-state* (LSP) con información de sus interfaces además de información aprendida por otros enrutadores adyacentes. Una vez generados inundan la red sobre todos los vecinos excepto a aquel del cual recibió el mismo LSP.

A partir de los LSP's, los enrutadores construyen las bases de datos de los estados de los enlaces y es cuando el árbol de la ruta más corta (SPT[21]) se calcula para cada IS, considerándose cada IS como la raíz.

2.8.4.4 Direcciones NSAP

Las direcciones empleadas en los paquetes CLNS se denominan NSAP (*Network Service Access* Point). NSAP especifica un servicio particular en la capa de red de un nodo.

Este tipo de direccionamiento emplea el concepto de direccionamiento de dominio jerárquico, en el cual la entidad más global es un dominio que es dividido en subdominios. Estos subdominios tienen asociado un plan único de direccionamiento para construcción de direcciones NSAP que es proporcionado por una autoridad de direccionamiento.

Las direcciones NSAP consisten de 3 partes: dirección de área, el identificador de sistema y el selector NSAP.

[20] (*Maximum Transfer Unit*) Unidad de transferencia máxima de un paquete.

[21] A partir del SPT se construye la tabla de enrutamiento.

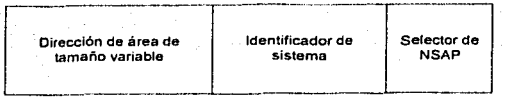


Figura 2.11 Dirección NSAP

La sección de área de una dirección NSAP[22] contiene dos partes principales. La primera se emplea para el enrutamiento de nivel 2 y se denomina parte de dominio inicial (IDP[23]) y la segunda es usada para el enrutamiento de nivel 1 y se llama parte específica de dominio (DSP[24]).

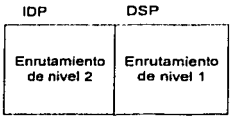


Figura 2.12 Dirección de área

El IDP se divide en dos partes, ambas son identificadores. La primera consiste en un identificador de autoridad y formato (AFI[25]) de un byte y un identificador de dominio inicial (IDI[26]) de tamaño variable.

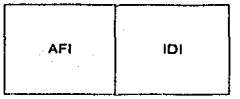


Figura 2.13 IDP

El DSP consiste de una cadena de dígitos que especifica una implementación de tecnología de transporte de una autoridad AFI.

Conjuntando lo que es la parte IDP y la que es la DSP se forma la primera parte de una dirección NSAP, que es la dirección de área la cual es de tamaño variable.

En cuanto al identificador de sistema suele emplearse un tamaño fijo de 6 bytes.

El selector de NSAP (NSEL) se emplea para identificar la capa de transporte, similar a lo que sería el número de puerto en redes IP. Cuando este se especifica con un valor de cero, las direcciones NSAP se denominan Título de Entidad de Red (NET[27]). Como los enrutadores IS tienen este campo en cero, se dice que tienen direcciones NET's las cuales van desde 8 hasta 20 bytes de tamaño.

Las condiciones de direccionamiento son las siguientes:

[22] El formato y la codificación se especifican en el documento ISO 8348/Ad2.
[23] *Inicial Domain Part*
[24] *Domain Specific Part*
[25] *Authority and Format Identifier*
[26] *Inicial Domain Identifier*
[27] *Network Entity Title*

1. Los IS's y ES's dentro de un dominio de enrutamiento deben tener identificadores de sistema únicos y del mismo tamaño.
2. Todos los enrutadores en una misma área deben tener la misma dirección de área.
3. Los enrutadores de nivel 2 poseen identificadores de sistema únicos en el dominio.
4. Los enrutadores de nivel 1 tienen identificadores de sistema únicos en el área.

En este tipo de direccionamiento, los enrutadores poseen solo una dirección NSAP por enrutador, a diferencia de los IP que poseen una dirección IP por interfaz que posea el enrutador.

2.8.4.5 Formato de paquetes IS-IS

El formato de paquetes IS-IS esta definido dependiendo del tipo de paquete que se este manejando.

2.8.4.5.1 Tipos de paquetes

Existen 4 tipos de formato de paquetes. Estos son:

Los paquetes *hello* IS-IS, que se emplean para descubrir enrutadores vecinos y para formar adyacencias. Además de estos, existen los paquetes *hello* que generan los ES's hacia los IS's denominados como ESH's, y los que generan los IS's hacia los ES's que se llaman ISH's.

También tenemos el formato de paquetes que corresponde a los LSP's o paquetes de estado de enlace, de los cuales existen cuatro tipos:

- Pseudonodo de nivel 1
- No pseudonodo de nivel 1
- Pseudonodo de nivel 2
- No pseudonodo de nivel 2

El tercer tipo de formato es el de los paquetes de numero de secuencia (SNP's), los cuales ayudan a mantener la misma información en los enrutadores sincronizando las bases de datos generadas por los LSP's.

Por último los SNP's parciales son usados para hacer peticiones de LSP's y recibir reconocimiento de los mismos LSP's.

Estos cuatro tipos de paquetes contienen formatos distintos con tres partes lógicas que los identifican. La primera consiste en un encabezado fijo de 8 bytes que comparten todos los paquetes IS-IS. La segunda parte consiste de un formato fijo que especifica el tipo de paquete y la tercera parte es una parte que identifica el formato de paquete siendo de tamaño variable.

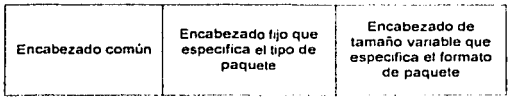


Figura 2.14 Encabezado de un paquete IS-IS

El encabezado común de los 3 tipos de paquetes es de 8 bytes y está conformado por 8 campos.

Identificador de protocolo	Tamaño del encabezado	Versión	Tamaño del identificador	Tipo de paquete	Versión	Reservado	Máximo número de direcciones de área

Figura 2.15 Encabezado común

Los campos son:

Identificador de Protocolo: Identifica el protocolo IS-IS y es constante con valor de 131.
Tamaño del encabezado: Es fijo y es de 8 bytes para que no difiera de los paquetes CLNP's.
Versión: Contiene el valor 1 de la actual especificación IS-IS.
Tamaño del identificador: Especifica el tamaño de la porción ID de la dirección NSAP.
Tipo de paquete: Especifica el tipo de paquete IS-IS.
Reservado: Es igual a cero.
Máximo número de direcciones de área: Especifica el número de direcciones que se permiten en el área actual.

2.8.5 IS-IS Integrado

Este protocolo fue desarrollado para poder soportar más protocolos de capa de red, adicionalmente al CLNP. Contiene un mayor número de campos en el formato de sus paquetes que sirven para informar a los enrutadores configurados con IS-IS que pueden alcanzar otros enrutadores con información de enrutamiento de otros protocolos.

También recibe el nombre de *Dual IS-IS* y fue diseñado para soportar redes CLNP e IP. Con esto, se puede implementar un único protocolo para soportar ambientes IP, OSI o híbridos.

Se dice que cuando se emplean dos protocolos de enrutamiento independientes uno del otro, estos operan como "*Ships in the night*" ya que ninguno de los dos tiene conocimiento de la existencia del otro. Para cada colección de protocolos OSI e IP se emplea un bloque de protocolos de enrutamiento que operan como "*Ships in the night*".

2.8.6 IDRP (*Interdomain Routing Protocol*)

2.8.6.1 Introducción

IDRP es un protocolo OSI empleado por enrutadores para enrutar información de dominios distintos. Diseñado para trabajar con los protocolos IS-IS, ES-IS y CLNP, incluye las siguientes características:

- Soporte para calidad de servicio CLNP.
- Eliminación de *loops* a través de marcas en las rutas de los dominios de enrutamiento atravesados.
- Reducción en la información de enrutamiento además del procesamiento a través de entidades denominadas confederaciones.
- Empleo de RTP, que es un protocolo de transporte confiable.
- Uso de encriptación.

IDRP es un protocolo cuyo funcionamiento esta basado en BGP y maneja su propia terminología.

2.8.6.2 Topología de IDRP

IDRP emplea los sistemas intermedios de frontera BIS[28] para realizar el enrutamiento interdominio. Estos se encuentran ubicados como salidas en los dominios de enrutamiento. Al igual que otros protocolos interdominio, IDRP esta organizado jerárquicamente y para administrar mejor las redes, esta organizado con dominios de enrutamiento o RD, que IDRP identifica con lo que son los identificadores de dominios de enrutamiento o RDI[29]. IDRP emplea una base de datos de enrutamiento o RIB[30] que contiene rutas que eligen los BIS para enviar la información y se generan con la información que reciben de los enrutadores dentro de un RD o de otros BIS's.

El término confederación se emplea para describir a un conjunto de dominios de enrutamiento, la cual es vista como un único dominio de enrutamiento para los dominios de enrutamiento que se encuentran fuera de la confederación.

2.8.6.3 Enrutamiento IDRP

Cuando pasa un paquete por distintos dominios de enrutamiento, este es marcado con un identificador. Con esto se forman las rutas IDRP que son una secuencia de identificadores de dominios de enrutamiento.

Los BIS están configurados para aprender de los dominios de enrutamiento, de las confederaciones así como de sus propios vecinos, considerando que ya saben a que dominio pertenecen.

Ahora las rutas que se decide que pasen o que sean enviadas como información a otros BIS, deben cumplir con las políticas locales de cada BIS. Los cambios en el cálculo de las rutas obedecen a tres tipos de eventos: cuando un BIS se cae, cuando se levanta y cuando nuevos avisos de actualizaciones ocurren.

Uno de los métodos que se emplean para evitar *loops* es marcar las actualizaciones con un identificador. Con esto se sabrá cuando los nuevos mensajes de actualizaciones contienen rutas nuevas o recalculadas.

[28] *Border Intermediate System*
[29] *Routing Domain Identifier*
[30] *Routing Information Base*

2.9 BGP (*Border Gateway Protocol*)

2.9.1 Introducción

BGP (*Border Gateway Protocol*) es un protocolo de enrutamiento robusto y escalable que se emplea para intercambiar información entre sistemas autónomos.

Tiene dos denominaciones comunes. Una es EBGP y se le llama con este nombre cuando funciona como protocolo de enrutamiento entre sistemas autónomos y la otra es IBGP y se le denomina así cuando un proveedor de servicio intercambia información de rutas dentro de un sistema autónomo.

BGP es escalable, emplea parámetros de ruta que le permiten mantener cierta estabilidad en cuanto al mantenimiento de todas las rutas que maneja y también le ayuda a definir políticas de enrutamiento. A estos parámetros se les denomina como atributos.

Otro factor que hace de BGP un protocolo estable para poder manejar grandes cantidades de información de enrutamiento, es el manejo del CIDR (*Classless Interdomain Routing*). El CIDR permite reducir considerablemente el tamaño de las tablas de enrutamiento, ya que en lugar de que un enrutador anuncie un bloque de 256 direcciones clase C, con el uso del CIDR solo anunciara una dirección de clase B para representar todo este bloque.

Los enrutadores configurados con BGP intercambian de manera completa información de sus tablas de enrutamiento. Esto sucede inmediatamente que una conexión del tipo TCP se establece entre vecinos BGP. Cuando se detecta que una ruta ha cambiado en una tabla de enrutamiento, esta actualización es enviada por el enrutador a sus vecinos, siendo la ruta que cambio la única que se envía. Cabe señalar que BGP no manda mensajes de enrutamiento periódicamente y que cuando manda información solo manda las rutas consideradas óptimas hacia la red destino.

2.9.2 Atributos de BGP

Una característica de las rutas que son registradas por BGP, es que éstas tienen asociados parámetros, llamados atributos, que ayudan a determinar la mejor ruta entre un origen y un destino cuando existen múltiples rutas. Los atributos se explican a continuación.

2.9.2.1 Peso

Se trata de un atributo propietario de CISCO, es local en cada enrutador, y se asigna para cada ruta que se registra. Este atributo no se publica a enrutadores vecinos. Cuando existen más de dos rutas hacia un mismo destino, la ruta elegida será aquella cuyo peso sea mayor. Ahora, estas dos rutas estarán registradas en la tabla de enrutamiento BGP, pero la ruta que tenga el mayor peso será la que pase a formar parte de la tabla de enrutamiento IP.

2.9.2.2 Preferencia Local

Este atributo determina un punto de salida preferido de un sistema autónomo cuando existen varios puntos de salida. Este atributo se propaga en la información que manda un enrutador BGP hacia sus vecinos, pero dentro del sistema autónomo local.

Cuando un enrutador recibe un aviso de una red, se le asigna a esta ruta un valor de preferencia local. Si otro enrutador recibe otro aviso hacia la misma red, se le asigna otro valor de preferencia local. Estos valores si son intercambiados en los mensajes de actualización de rutas y aquel que tenga el mayor valor en cuanto a preferencia, será elegido como el punto de salida hacia la red anunciada, generalmente de otro sistema autónomo.

El punto de salida siempre llevará hacia otro sistema autónomo que haya anunciado una de sus rutas a dos enrutadores de otro sistema autónomo.

2.9.2.3 Discriminador multisalida (MED)

Es un atributo que se propaga dentro de un sistema autónomo local. Se emplea como "sugerencia" hacia un SA externo para que tome en consideración determinada ruta si es que cualquier enrutador del SA externo esta tomando en cuenta algún otro atributo BGP para la selección de la mejor ruta.

2.9.2.4 Origen

Este atributo determina la forma en que una ruta es aprendida por BGP. Este parámetro puede tener tres de los siguientes valores:

IGP. Si la ruta fue aprendida del interior del sistema autónomo.
EGP. Si la ruta fue aprendida de un aviso entre sistemas autónomos.
Incompleta. Ocurre cuando el origen no se conoce o cuando se hace una redistribución de rutas a BGP.

La redistribución de rutas se realiza cuando en un sistema se están corriendo varios protocolos de enrutamiento y se requiere que uno de ellos sepa las rutas aprendidas por el otro protocolo y viceversa.

2.9.2.5 Ruta de SA

Cuando un aviso de ruta hacia un destino pasa por varios sistemas autónomos, cada uno de los sistemas autónomos le agrega su número de SA a una lista de números de SA's. Ésta es la manera en que BGP puede detectar *loops*. Supongamos el caso en que un enrutador en el SA 1 envía avisos de ruta a otro enrutador en un sistema autónomo 2 y a un enrutador más en el SA 3. El aviso sería {1}. En caso de que los SA's 2 y 3 regresen la ruta al enrutador del sistema autónomo 1, el atributo de ruta tendrá {2,1} y {3,1} respectivamente. Si en el aviso de ruta, el enrutador del sistema autónomo 1 detecta su número de sistema autónomo, este rechazara el aviso de ruta.

Los enrutadores que se encuentran el los SA's 2 y 3 anunciarán el uno al otro, como se muestra en la siguiente figura, que pueden alcanzar dicha ruta introduciendo en el atributo de ruta AS su propio número de SA. Supongamos el caso en el que el enrutador C recibe un anuncio de la ruta 192.168.27.0 proveniente del enrutador B. Dicha ruta no será introducida en la tabla de enrutamiento del enrutador C ya que el atributo de ruta AS {2,1} contiene registrados más números de SA's que el anunció de ruta que le hizo el enrutador A, con el atributo de ruta AS {1}, siendo la

ruta aprendida del enrutador A la que será registrada en la tabla de enrutamiento IP del enrutador C.

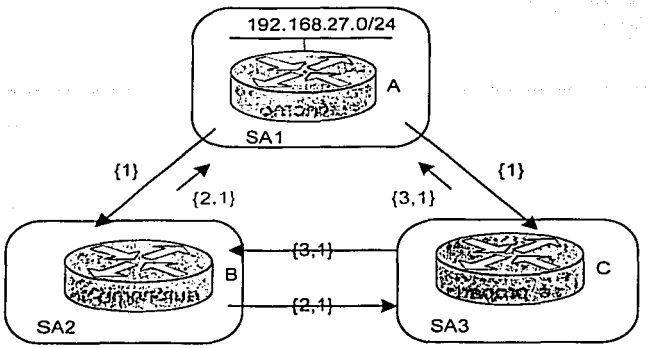


Figura 2.16 Ruta de SA

2.9.2.6 Próximo salto

Este atributo se refiere a la dirección IP del enrutador que esta anunciando la ruta. Cuando se emplea EBGP esta dirección se refiere al *peer* con el que se entabla una conexión TCP. Cuando hablamos de IBGP, la dirección del próximo salto se acarrea dentro del AS. Para que el aviso de ruta sea válido y no sea descartado dentro del AS, es necesario que este funcionando un IGP que sea el encargado de transportar información referente al próximo salto, además de cumplir con el requisito de que el próximo salto sea alcanzable.

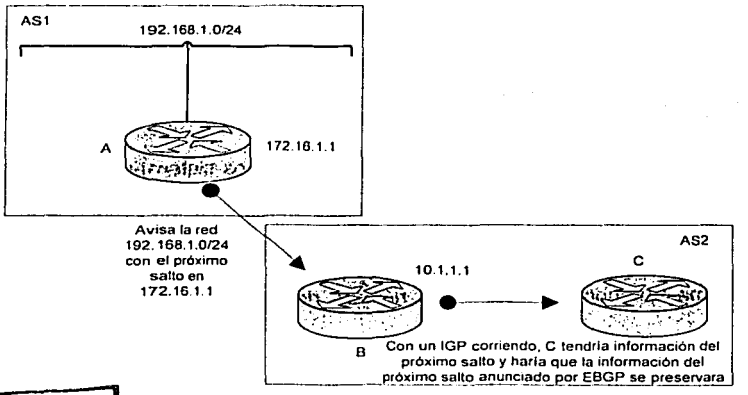


Figura 2.17 Próximo salto

2.9.2.7 Comunidad

Los atributos de comunidad ayudan al administrador a formar grupos de destinos a los cuales se les puede aplicar políticas de enrutamiento, como la preferencia, o la redistribución de rutas.

Básicamente determinan a que enrutadores se les anuncian determinadas rutas. Los atributos de rutas están predefinidos y son los siguientes:

No-export: Implica que una vez avisada una ruta hacia el destino entre sistemas autónomos, el sistema autónomo que recibió el aviso no propagará este mensaje hacia algún otro sistema externo.

No-advertise: Implica que dentro de un sistema autónomo, no habrá avisos de una determinada ruta que contenga el atributo de comunidad puesto en no-advertise entre *peers*.

Internet: Implica que las rutas con este atributo serán avisadas a toda la comunidad de Internet.

2.9.3 Algoritmo de selección de ruta BGP

Una vez definidos los parámetros de ruta que emplea BGP, se establece el orden de prioridad que determinará la elección de la mejor ruta de entre muchas que posiblemente puede recibir un enrutador BGP de múltiples orígenes. BGP seleccionará solo una ruta como la mejor ruta.

1. Si el próximo salto es alcanzable, la ruta es válida. Si no, se desecha la ruta.
2. El peso asignado a una ruta.
3. El valor asignado a la preferencia local.
4. Se dará preferencia a la ruta originada en el enrutador actual.
5. La ruta que contenga el atributo de ruta AS más corto.
6. Después se analizará la ruta que contenga el origen más cercano. Esto es primero una ruta aprendida por IGP, después por EGP y al último una incompleta.
7. En seguida la ruta con el MED más corto.
8. Después se preferirán las rutas internas sobre las externas.
9. La penúltima regla aplica a la ruta que este más cerca de un IGP.
10. Por último la ruta que contenga el identificador del enrutador BGP más pequeña.

Capítulo 3. MPLS

La conmutación de etiquetas es una tecnología que ha sido implementada a través de varios esquemas dependiendo de las necesidades de quien lo necesita. La IETF ha propuesto un estándar que maneja dicha tecnología y elimina el hecho de que cada entidad trabaje con tecnologías de conmutación de paquetes que no son compatibles las unas con las otras. El estándar propuesto es MPLS (*Multiprotocol Label Switching*).

3.1 Introducción

Desarrollado a finales de los 90's por la IETF, MPLS es un protocolo para administrar una red que integra características de capa 2 referentes a los enlaces de red hacia elementos de capa 3 dentro de un esquema particular.

Con las redes tradicionales IP no se podía tener control para monitorizar, categorizar o etiquetar los paquetes. MPLS provee mecanismos para habilitar estas herramientas de administración, empleando como elemento las *etiquetas*. Al ser un protocolo *overlay*[31] le permite trabajar en la capa más alta de IP y así, MPLS puede trabajar en la misma red IP sin interferir en su operación. De hecho, MPLS no pretende sustituir a IP, sino proveer las capacidades para implementar reglas al tráfico IP para que éste pueda ser clasificado, marcado y que sea sujeto a ciertas políticas, como manejo de ancho de banda, retardo, etc.

Los componentes básicos que forman una red MPLS son los enrutadores que se ubican en la parte de acceso de la red, o que se encuentran en la frontera de la red MPLS. Estos enrutadores tienen como funciones básicas examinar los paquetes IP que entran y colocarles el encabezado MPLS, donde se ubica la etiqueta, así como eliminar las etiquetas del paquete una vez que estos abandonan la dorsal.

Dentro de la dorsal MPLS se ubican otros enrutadores que se encargan de intercambiar las etiquetas de un paquete a fin de determinar la ruta que debe seguir desde el punto de entrada al de salida de la dorsal MPLS.

Las rutas están determinadas completamente desde un enrutador de frontera hasta otro por las etiquetas. De tal manera que la ruta completa de un paquete que entra a la dorsal MPLS ya esta determinada de acuerdo a la etiqueta que le coloque el enrutador de frontera a la entrada de la dorsal. Esta característica simula conexiones dedicadas durante el periodo de uso contraponiéndose al paradigma de las redes IP, las cuales funcionan bajo el paradigma no orientado a conexión.

[31] Se explica más adelante, en el capítulo 4 de VPN's.

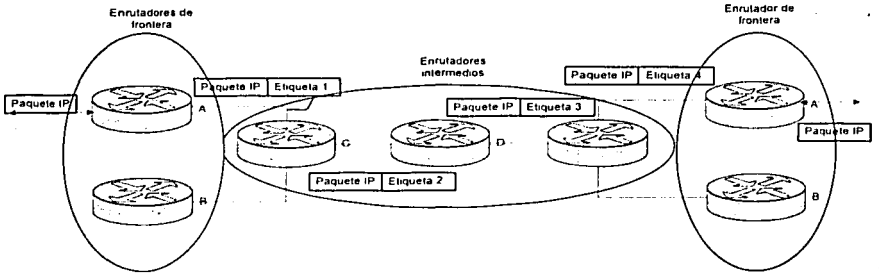


Figura 3.1 Red MPLS

Una de las mayores ventajas de MPLS es que provee herramientas para el control del tráfico de datos. Por ejemplo puede manejar y garantizar la calidad de servicio (QoS, *Quality of Service*) que ofrecen las tecnologías de capa de transporte como ATM o FR (*Frame Relay*) sin la necesidad de poseer líneas dedicadas.

La facilidad para crear redes privadas virtuales con MPLS esta ocasionando que esta tecnología se expanda apresuradamente y que los clientes las implementen ya que en cuestión de costos representa una gran ventaja.

3.2 Antecedentes

En el pasado, no existía control sobre el tipo de tráfico que se manejaba en las redes, ya que no se tenían los métodos para hacer un manejo adecuado de los recursos disponibles en ellas. La información era entregada basándose en el concepto de *mejor esfuerzo*, es decir, si existía suficiente ancho de banda se entregaban los paquetes y si no pues se desechaba la información aleatoriamente, afectando a todos los servicios por igual. De esta problemática surge la necesidad de crear métodos que pudieran ofrecer manejo de tráfico y calidad de servicio (QoS, *Quality of Service*).

Los elementos en los cuales se basa el parámetro QoS son ancho de banda, retardo, *jitter*[32], y pérdida de tráfico para sistemas OSI. En cuanto al retardo y el *jitter*, la conmutación de etiquetas puede hacer mucho, mejorando el *jitter* y reduciendo el retardo. Con el ancho de banda no puede hacer demasiado, ya que eso es inherente de la capacidad del enlace.

La primera tecnología en emplear el concepto de *switching* (conmutación) fue el estándar X.25, que surgió debido a la necesidad que tuvieron las empresas para comunicarse entre sí. X.25 empleaba un valor que identificaba el tráfico de un usuario dentro de un enlace físico que era compartido por varios usuarios, quienes pensaban disponer del ancho de banda total del enlace, creándose el concepto de *circuito virtual*. El identificador de cada circuito se denominó número de canal lógico o LCN (*Logical Channel Number*).

Las tecnologías actuales como ATM y FR siguen empleando estos conceptos, como circuitos virtuales e identificadores de tráfico o "etiquetas". Para FR los identificadores de los

[32] Variación en el retardo.

circuitos virtuales se denominan DLCI's (*Data Link Connection ID's*) y para ATM son VPI's/VCI's (*Virtual Path ID's / Virtual Circuit ID's*).

MPLS, que emplea etiquetas para identificar el tráfico, no tiene problemas al trabajar con redes FR y ATM, por lo que la evolución hacia esta nueva tecnología mejorada no involucra mayores problemas.

MPLS esta enfocado a trabajar con IPv4 e IPv6, sin embargo puede soportar otros protocolos de red. También no restringe ninguna tecnología de transporte para ser empleada como ATM y FR, ya que la intención es que pueda trabajar directamente sobre la capa 2.

3.3 Arquitectura de MPLS

La mayoría de las mejoras de MPLS con referencia a los métodos de envió que emplea IP, están basadas en extensiones de los protocolos ya existentes. Además, algunas tecnologías como el manejo del QoS y lo que es ingeniería de tráfico son muy parecidas a las que emplean las tecnologías ATM y FR.

Una de las grandes ventajas de MPLS en relación a otros protocolos es su modularidad. Las actualizaciones al protocolo y la adición de nuevas funciones pueden hacerse fácilmente sin afectar el modo en que opera este protocolo. Esto gracias a que la arquitectura de MPLS se divide en dos componentes básicos. El primero llamado de control y el segundo denominado de datos que a continuación se describen.

3.3.1 Componente de control

El componente de control en un nodo MPLS puede identificar clases de tráfico, conocidas como FEC's (*Forwarding Equivalente Classes*). Estas clases de tráfico conforman una tabla la cual es intercambiada entre los nodos MPLS y sirve para hacer las asociaciones entre etiquetas y FEC's que también son intercambiadas entre los nodos usando un protocolo de distribución de etiquetas. Los enrutadores de frontera emplean esta tabla así como las asociaciones para etiquetar los paquetes entrantes y enviarlos a la red MPLS.

Con esta información intercambiada se construye en cada nodo una tabla LFIB (*Label Forwarding Information Base*), que emplea el componente de datos para enviar los paquetes etiquetados a través de la red MPLS.

Con la ayuda de los protocolos de enrutamiento de capa 3, este componente se encarga de construir las rutas que seguirán los paquetes usando como elemento de control las etiquetas y las FEC's. A estas rutas se les conoce como LSP (*Label Switched Path*) o rutas conmutadas de etiquetas, ya que están construidas en base a etiquetas que son como indicadores en cada nodo MPLS diciendo el camino que debe seguir un paquete al pasar por dicho nodo desde su origen hasta su destino.

Es así como este componente se ayuda de los protocolos de enrutamiento de capa 3 para elaborar las rutas.

3.3.2 Componente de datos

Este componente emplea la base de datos que crea el componente de control para propagar los paquetes etiquetados a través de la red. La estructura de este componente es similar a la empleada por tecnologías de capa 2, ya que solo realiza un *swicheo* de etiquetas para enviar los paquetes al siguiente nodo, evitando realizar el *lookup* (revisión) sobre cada paquete en cada nodo para revisar dirección destino contenida en el encabezado de cada paquete, logrando mejorar el rendimiento de este proceso. Es así como MPLS implementa lo mejor de la tecnología de capa 2.

Si se trata de un enrutador de frontera, en el componente de datos se le agregaría un elemento más para poder enviar los paquetes sin etiquetas, como se ilustra en la siguiente figura.

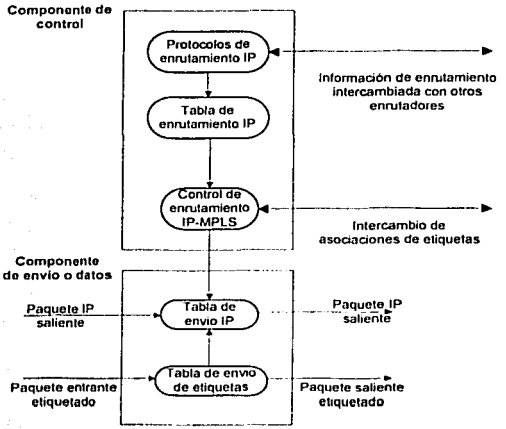


Figura 3.2 Arquitectura de MPLS

Entonces, mientras el componente de datos o envío se encarga de hacer la entrega de la información de un origen a un destino, el componente de control se encarga de construir las tablas de enrutamiento, además de mantenerlas y distribuir la información de enrutamiento junto con la correspondiente información de etiquetas.

3.3.3 Tipos de nodos MPLS

En un dominio MPLS existen distintos roles que deben cumplir los nodos configurados para ejecutar MPLS.

Los enrutadores que se encuentran en la orilla del dominio MPLS se denominan LER's (*Label Edge Routers*) o también llamados de ingreso o egreso. Y los nodos que se encuentran en la parte intermedia de la red MPLS se denominan como nodos de conmutación de etiquetas, de tránsito o simplemente LSR's (*Label Switching Routers*).

Los nodos de frontera o LER's son los encargados de hacer el asignamiento de etiquetas, son los que realizan el mayor trabajo revisando los encabezados de los paquetes que van entrando y realizan el procesamiento para manejar las etiquetas además de controlar e indicar la manera en

que el trafico que esta sujeto a calidad de servicio atravesará la red MPLS, dejando la tarea de solo conmutar lo paquetes a lo que seria el núcleo de la red, eliminando la tarea de procesamiento a esta parte esencial de la red, por lo que el rendimiento y la rapidez aumentan considerablemente.

Los nodos intermedios o LSR's, realizan las operaciones de transmisión de los paquetes basándose exclusivamente en las etiquetas que llevan los paquetes[33].

Las operaciones que realizan estos nodos con las etiquetas son extracción y colocación de estas. Las operaciones de extracción de etiquetas pueden ser realizadas una sola vez por cada nodo MPLS que atraviesa el paquete etiquetado e igualmente solo puede colocarle una etiqueta a la vez.

Las operaciones de extracción de etiquetas generalmente dependen de la capacidad del nodo para manejar estas operaciones. Es fundamental que el nodo sepa cuando eliminar la última etiqueta ya que si el siguiente salto no posee capacidad para manejar etiquetas (es decir, que no forma parte del dominio MPLS) tendrá conflictos con el paquete.

Al igual que los enrutadores, los *switches* de capa 2, como los *switches* ATM son capaces de realizar las operaciones sobre las etiquetas, pero necesitan de una actualización en su *software* para desenvolverse como *switches* ATM-LSR. Por ejemplo, un *switch* ATM realiza las operaciones de envío basándose en su tradicional mecanismo de conmutación de celdas ATM, procedimiento que es llevado a cabo por el componente de datos. Ahora el *switch* ATM necesita ser actualizado en el componente de control para que pueda comportarse como nodo MPLS.

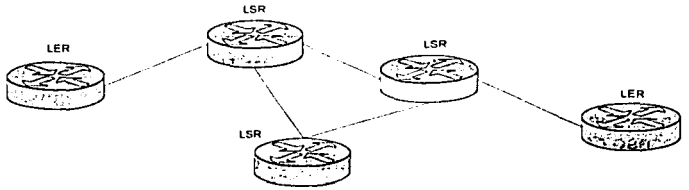


Figura 3.3 Nodos LER y LSR

Aquí se describen las funciones de los tipos de nodos MPLS.

Tipo de nodo MPLS	Funciones del nodo MPLS
LSR	Envío de paquetes etiquetados
LER	Análisis del encabezado de capa 3, colocar etiqueta y enviar el paquete al dominio MPLS. Recibir un paquete etiquetado y extraer la etiqueta para enviar el paquete IP puro.
ATM-LSR	Ejecuta los protocolos MPLS en el plano de control para configurar los circuitos virtuales. Envía los paquetes etiquetados como celdas ATM.
ATM-LER	Puede recibir un paquete etiquetado o no, segmentarlo en celdas ATM y enviarlas hacia el siguiente nodo ATM-LSR. También puede recibir una celda ATM, reagruparla para formar el paquete original y enviarlo como paquete etiquetado o no etiquetado.

Tabla 3.1 Nodos MPLS

[33] Los LSR's solo se fijan en las etiquetas que están en el nivel más alto, o la etiqueta que esta hasta arriba en la pila de etiquetas del paquete sin fijarse en la información de capa 3 u otra.

3.4 Conceptos MPLS

3.4.1 Etiqueta

Una etiqueta es, de forma condensada, como un encabezado de un paquete IP que posee la información suficiente para enviar el paquete del origen a su destino. Esta etiqueta no es una dirección IP, sino que es un valor numérico que es acordado entre dos nodos MPLS para indicar una conexión a lo largo de una la red MPLS.

La etiqueta, cuyo significado es generalmente local a la red o a los nodos en cuestión, es pequeña, de tamaño fijo y sirve para identificar y codificar clases de tráfico.

MPLS tiene compatibilidad con otras tecnologías de transporte como ATM y FR ya que estas tienen sus propias etiquetas. Así, MPLS emplea estas etiquetas para realizar las decisiones de envío.

Cuando hablamos de tecnologías *Ethernet* o conexiones punto a punto, se emplea un encabezado especial denominado *shim* de 32 bits de tamaño.

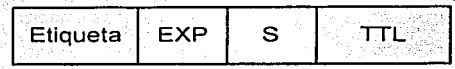


Figura 3.4 Formato de etiqueta *Shim*

El campo de etiqueta, usualmente de significado local, representa una clase particular de tráfico durante el proceso de envío, y es de 20 bits.

El campo EXP, considerado como experimental, es considerado para implementaciones de QoS.

El campo S indica si existe apilado de etiquetas o no en el paquete.

El campo TTL (*Time-to-live*), tiempo de vida, indica el número de nodos MPLS que un paquete ha atravesado para llegar a su destino.

3.4.1.1 Encabezado y encapsulado MPLS

La colocación del encabezado MPLS varia dependiendo del tipo de medio que se este usando. Cuando el medio es *Ethernet* se emplea la etiqueta *shim* como encabezado pero cuando se usan tecnologías de capa 2 como ATM y FR el encabezado podría decirse que va incrustado en los campos DLCI's y VPI's/VCI's de dichas tecnologías ya que ahí es donde iría el valor de la etiqueta para enviar el paquete a su destino a través de la red MPLS.

Entonces, el encabezado MPLS tiene un tamaño de 32 bits y esta formado por cuatro campos fundamentales. Éste se coloca siempre antes del encabezado de capa 2 y después del encabezado de capa 3[34].

Otro concepto importante es el denominado *Label Switching Tunneling* que consiste en el encapsulado de un paquete con un encabezado llevando la etiqueta asignada. Este nuevo paquete pasara la red de conmutación exclusivamente empleando dicho encabezado y cuando llegue a la

[34] A menos que la etiqueta este incluida en lo que son los campos VCIDs de ATM o FR.

otra orilla de la red, este encabezado se removerá para poder ser enviado usando la información de paquete original.

La etiqueta puede residir en 1 o 2 encabezados dentro del paquete. Puede estar en el encabezado ATM o FR y en el encabezado especial denominado *shim*.

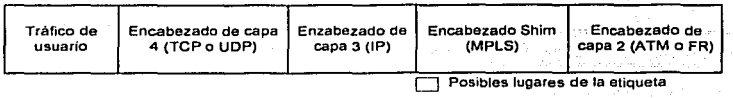


Figura 3.5 Colocación de etiqueta

3.4.2 FEC

Las clases equivalentes de envio o FEC's (*Forwarding Equivalente Classes*) describen la asociación de un bloque de paquetes pertenecientes a la misma clase de tráfico. Las clases de tráfico generalmente se elaboran con información referente a la aplicación que genera el tráfico, enfocándose a lo que sería el número de puerto (información de capa 4). También se elaboran usando las direcciones IP, IPX o AppleTalk destino (información de capa 3), direcciones MAC y VCID's destino (información de capa 2).

El objetivo de las FEC's es identificar grupos de paquetes para darles el mismo trato en cuanto a operaciones de envió a través de la red MPLS. La asignación de prioridad sobre las FEC's facilita el manejo de tráfico de los paquetes así como la capacidad para proveer QoS, fundamental para MPLS.

La FEC a la cual se asigna un paquete o un grupo de estos se codifica como un valor de tamaño fijo llamado "etiqueta".

En MPLS el asignamiento de un paquete en particular a una FEC se hace solo una vez, cuando entra el paquete al dominio MPLS. De esta forma, solo se revisa una sola vez la dirección IP y no en cada nodo como en el enrutamiento tradicional, ayudando a mejorar el retardo y el *jitter*.

Cada LSR construye una tabla para especificar como un paquete debe ser enviado. Esta tabla, llamada LIB (*Label Information Base*), esta constituida por asociaciones de FEC's a etiquetas.

3.4.3 LSP

La ruta conmutada de etiquetas o LSP (*Label Switched Path*) es una ruta predeterminada que un bloque de paquetes, ligado a una FEC, atraviesan una red MPLS para alcanzar el destino. Las LSP's son unidireccionales y para poder enviar el tráfico de regreso debe de emplearse una LSP adicional.

A través de este concepto es como se establece que MPLS esta orientado a conexión, ya que las etiquetas determinan, previo a que un bloque de paquetes inicie su recorrido, la ruta que estos deberán cruzar pasando por los nodos MPLS.

3.4.4 *Label Stack*

El apilado de etiquetas o *label stack* es un grupo de etiquetas que un paquete puede llevar en el encabezado MPLS. Una vez que un enrutador de frontera o LER determina que un paquete esta sujeto a reglas de conmutación de etiquetas, este tiene la capacidad para transportar más de una etiqueta en el encabezado MPLS.

Esta característica permite que exista una jerarquía en el enrutamiento, ya que habilita a los paquetes viajar dentro de un dominio o entre dominios diferentes.

El procesamiento de varias etiquetas en un paquete se realiza en base a la técnica LIFO (Last In First Out), es decir, que la última etiqueta en entrar será la que sea procesada mientras el paquete este cruzando la red, hasta que algún nodo MPLS la extraiga.

3.4.4.1 Jerarquía de conmutación

Cuando los paquetes viajan en la red Internet, estos atraviesan múltiples nodos que se encuentran agrupados en grupos lógicos llamados dominios. En teoría si estos dominios son administrados y configurados con políticas distintas cada uno, no sería posible que la información pasara de un punto a otro. Con MPLS esto es posible ya que independientemente de las políticas de enrutamiento, si se habilitan ciertos nodos con MPLS, los paquetes pueden atravesar dichos dominios empleando solo el parámetro que usa MPLS para enviar los paquetes al destino final.

El punto importante en esto radica en que el procesamiento de las etiquetas se hace con la etiqueta que fue colocada al final, sin importar el nivel o el número de etiquetas que han sido colocadas previamente o las que falte por colocar en el paquete. Esto es, que no importan cuantos dominios haya pasado anteriormente y las políticas empleadas para el asignamiento de las etiquetas o cuantos falten para alcanzar el destino, el procesamiento de los paquetes en un dominio intermedio no variará lo que da la ventaja de ser sumamente escalable.

Si se trata de un dominio intermedio que lleva paquetes con una pila de etiquetas de un nivel 2, el penúltimo nodo MPLS puede dejar que el último nodo MPLS, o LSR de egreso de este dominio, realice una extracción de etiqueta, permitiendo que en el siguiente dominio el paquete pueda seguir siendo direccionado empleando la etiqueta de nivel 1.

Cuando ya no sigue otro dominio MPLS, el penúltimo nodo debe hacer la extracción de la etiqueta, ya que una vez que se ha alcanzado el ultimo nodo, no tiene caso que se siga llevando ésta, ya que el objetivo se ha cumplido, que es de llegar al ultimo nodo. Además evitaría que el último nodo realizara dos revisiones en el encabezado del paquete, ya que tendría tomar la decisión de a donde enviar el paquete revisando la información de capa 3, después de haber realizado la última extracción. La ventana de que el penúltimo nodo realiza una extracción de etiqueta, habilita a que el último nodo solo realice una revisión de la información necesaria para realizar la decisión de envío del paquete a nivel IP.

Si el siguiente dominio no es MPLS, entonces se debe asegurar que al llegar al nodo LSR de egreso, el paquete salga con el apilado de etiquetas vacío, para que el nodo que no es MPLS pueda hacer la decisión de envío empleando la información de capa 3.

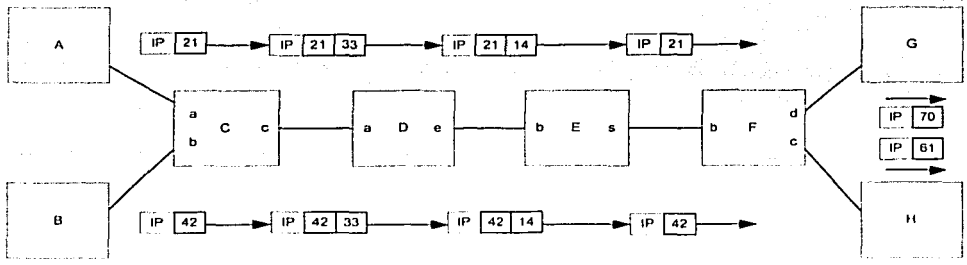


Tabla de C	
Entrada	Salida
a.21 b.42	c.Push 33 c.Push 33

Tabla de D	
Entrada	Salida
a.33	e.14

Tabla de E	
Entrada	Salida
b.14	s.Pop

Tabla de F	
Entrada	Salida
b.21 b.42	d.70 c.61

Figura 3.6 Apilado de etiquetas

3.4.5 *Label swapping*

Las operaciones de envió en una red de conmutación de etiquetas consisten en el chequeo del valor de una etiqueta entrante para poder determinar el valor de la etiqueta saliente además de la interfaz saliente y otra información como el puerto, la encapsulación de capa 2, etc. Estas operaciones se realizan en cada nodo MPLS.

MPLS es una tecnología de *forwarding* y *swapping* o *mapping* de etiquetas que mejora el rendimiento en el enrutamiento de capa de red, permitiendo hacer más flexible la entrega de servicios de enrutamiento.

El proceso de *label swapping* consiste en el cambio de etiqueta del paquete en cada nodo MPLS, específicamente en los LSR's, ya que los LER's se encargan ya sea de colocarlas o extraerlas. Dichas etiquetas serán las que determinen el camino a los paquetes a través de las LSP's.

Para este proceso son fundamentales los protocolos de distribución de etiquetas, ya que para que un nodo pueda cambiar la etiqueta de un paquete, debe saber la etiqueta que esta esperando el nodo que va a recibir el paquete. Los protocolos para la distribución de las etiquetas pueden ser varios como LDP (*Label Distribución Protocol*), RSVP (*Resource Reservation Protocol*), BGP y otros. Algunos se les han agregado extensiones para soportar la distribución de las etiquetas y otros para que puedan soportar calidad de servicio (QoS).

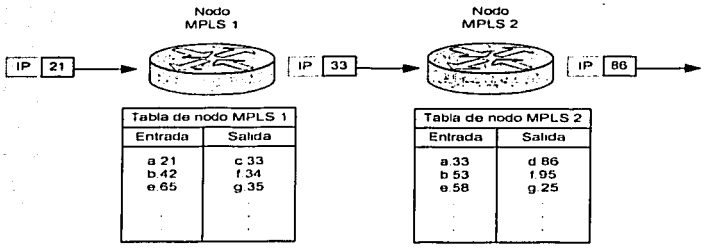


Figura 3.7 Cambio de etiqueta (*Label swapping*)

En este ejemplo el nodo MPLS 1 ya sabe que el nodo MPLS 2 esta esperando un paquete con la etiqueta 33 por la interfase *a* para reenviarlo con una nueva etiqueta por la interfase *d*.

3.4.6 *Binding*

El proceso en el cual las etiquetas son asignadas a las FEC's se denomina *binding* o asociación y es una operación que realizan los enrutadores LER's y LSR's. La asociación se realiza entre 2 nodos empleando un protocolo de distribución de etiquetas.

La asignación de etiquetas tiene dos ámbitos en los cuales puede darse:

Espacio de direcciones por interfase: Las etiquetas son asociadas con cada una de las interfaces del LSR o LER habilitando la reutilización de las etiquetas en cada una de las interfaces, asemejándose al modo en que las tecnologías ATM y FR hacen uso de las etiquetas.

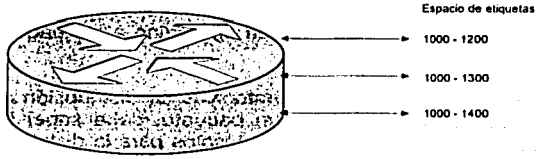


Figura 3.8 Espacio de direcciones por interfase

Espacio de direcciones por plataforma: Las etiquetas no se pueden repetir en las interfaces que pertenecen al mismo enrutador ya que este espacio de etiquetas lo comparten todas las interfaces de dicha plataforma.

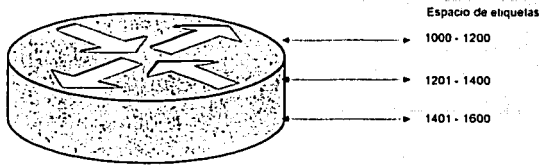


Figura 3.9 Espacio de etiquetas por plataforma

3.4.7 Agregación

Cuando agrupamos un bloque de FEC's con sus correspondientes etiquetas, en realidad producimos otra FEC a la cual le podemos asignar una única etiqueta que podemos emplear para transportar todo el trafico correspondiente a todas las FEC's. A este proceso se le llama agregación y es útil, ya que permite disminuir la cantidad de tráfico de control que se tiene que transportar.

Los dispositivos capaces de realizar este proceso son los LER's y los LSR's.

3.4.8 *Label Merging*

En este proceso a múltiples paquetes que llegan con distintas etiquetas, se les asigna una sola etiqueta la cual producirá que estos paquetes tengan una sola interfase de salida, común para todos los paquetes.

La capacidad de un LSR de realizar este proceso queda demostrado si es capaz de recibir 2 o más paquetes con diferentes etiquetas por distintas interfaces y enviarlos al siguiente salto por la misma interfaz de salida empleando una única etiqueta, con la condición de que tengan el mismo destino.

Esta capacidad de fusionar varias etiquetas con una sola etiqueta, permite que los LSR empleen menos cantidad de etiquetas de salida. Equivaldría a decir que se necesita una sola etiqueta por todas las FEC's que ingresen, a diferencia de no tener esta capacidad, donde se requeriría tantas etiquetas por cada FEC que ingrese.

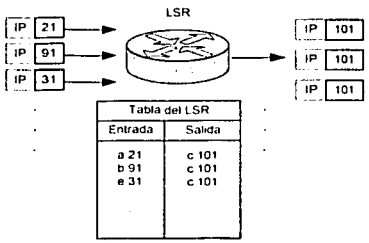


Figura 3.10 *Label merging*

El LSR cambia las etiquetas de los paquetes, que tienen el mismo destino, y les coloca una etiqueta común lo que provoca que tengan una sola interfaz de salida.

3.4.9 Tablas en MPLS

Para que MPLS pueda soportar el manejo de etiquetas relacionando las que entran a un nodo MPLS con las etiquetas salientes y las interfaces salientes, es necesario contar con tablas que nos den información referente a esto.

Estas tablas son las siguientes:

NHLFE (*Next Hop Label Forwarding Entry*). Contiene información que permite a los paquetes etiquetados ser reenviados al siguiente salto. Dicha información es el próximo salto que debe dar el paquete además de las operaciones que debe realizar el LSR con las etiquetas que se tengan en el apilado de ellas, entre otras cosas. Algunas de las operaciones son las siguientes:

- Reemplazar la etiqueta en la parte más alta del apilado de etiquetas con la etiqueta nueva especificada.
- Extraer la etiqueta del apilado.
- Reemplazar la etiqueta en la parte más alta del apilado de etiquetas con la etiqueta nueva especificada y en su caso colocar más etiquetas sobre el apilado de etiquetas.

ILM (*Incoming Label Map*). En esta tabla se mapean las etiquetas que van entrando a un bloque de entradas NHLFE.

En este caso las etiquetas funcionan como índices que acceder a esta tabla. Cuando una etiqueta es mapeada a un bloque de NHLFE que contiene más de una salida, se debe de elegir una de estas antes de ser enviado. Esto habilita que se pueda hacer balanceo de carga, ya que se puede especificar que determinados paquetes con ciertas etiquetas sean acarreados por más de una salida. Esta tabla es empleada por paquetes que ya han sido etiquetados.

FEC-to-NHLFE Map (FTH). Cuando los paquetes no han sido etiquetados se emplea esta tabla, en la cual se mapea cada FEC a entradas NHLFE. Igualmente debe de elegirse solo una salida de entre varias de estas que estén contenidas en la NHLFE cuando una FEC sea mapeada a un bloque de NHLFE.

3.4.10 Selección de la ruta LSP

Existen dos métodos para elegir lo que sería la ruta LSP para un determinado FEC.

- Enrutamiento explícito
  - Estricto
  - Amplio
- Enrutamiento salto por salto

El método salto por salto es el que tradicionalmente se emplea, permitiendo a cada nodo elegir independientemente el próximo salto que deban dar un bloque de paquetes asociados a un determinado FEC.

Con el método de enrutamiento explícito, no se permite que los nodos decidan independientemente el siguiente salto para cada FEC. En vez de esto y con ayuda de información de estado de enlace, se puede elegir los LSR's que deban formar parte de una ruta LSP. Generalmente esta tarea la tienen asignada los nodos MPLS de ingreso y egreso o los LER's. Si un LER decide la ruta completa, es decir, todos los LSR's por los que deba pasar una FEC, entonces se habla de enrutamiento explicito estricto. Cuando solo elige unos cuantos se dice que es enrutamiento explícito amplio.

La forma de elegir las LSPs es diversa, por ejemplo para hacerlo dinámicamente pueden hacer uso de información de estado de enlace. O también puede hacerse a través de configuración.

Las ventajas que presenta el enrutamiento explicito son varias. Por ejemplo, permite en redes MPLS manejar la ingeniería de tráfico además de poder especificar políticas en el enrutamiento. También evita estar especificando la ruta explícita sobre cada paquete IP.

Ahora puede existir un problema cuando no se tenga una etiqueta saliente que indique el camino que deba seguir un paquete etiquetado entrante. Si la ILM no tiene una etiqueta saliente, podría emplearse otra información, como la información de capa 3, para tomar la decisión de envió del paquete, pudiendo no ser lo mas conveniente. Esto nos llevaría incluso a formar *loops*.

Para el control de *loops* se emplea lo que es el campo TTL, ya que este limita el tiempo que un paquete esta transitando la red. El problema viene cuando en algunos segmentos de la red este no se maneja, entonces ya no se puede tener un adecuado control de *loops* utilizando este campo.

3.5 Protocolos para la Distribución de Etiquetas

3.5.1 Introducción

Para que un LSR pueda cambiar la etiqueta de un paquete entrante y reenviarlo a su LSR de bajada, debe tener un método que le permita aprender que valor de etiqueta esta esperando el LSR de bajada.

Ante esta necesidad existen distintos protocolos que permiten la distribución de etiquetas, algunos limitados exclusivamente a estas funciones. A través de estos protocolos se puede preparar el camino para el soporte de calidad de servicio, sin embargo esto se logra por medio de extensiones a estos protocolos para cumplir con tales requerimientos. Existen algunos otros protocolos que están hechos para reservar recursos en la red, característica fundamental para soportar QoS, pero no están diseñados para la distribución de etiquetas y que igualmente han sido extendidos para soportar la distribución.

La IETF desarrollo un protocolo para complementar la arquitectura de MPLS. Este es LDP (*Label Distribution Protocol*) y fue diseñado sólo para la distribución de etiquetas, sin capacidad para proveer QoS. Sin embargo al igual que BGP, puede ser extendido para soportar reservación de recursos.

Para LDP, existe una extensión para habilitar el manejo de recursos y es el protocolo CR-LDP (*Contraint-Based* LDP) que permite configurar rutas LSP. CR-LDP[35] tiene la capacidad de emular circuitos conmutados en la red, además de ser usado con tráfico que es sensible a retardos.

3.5.2 LDP (*Label Distribution Protocol*)

Los LSR's llevan a cabo un proceso en el cual establecen el valor de las etiquetas que deben emplear para poder transportar el tráfico que fluye entre dichos nodos. LDP permite soportar este requerimiento. LDP se usa para establecer y mantener las asociaciones de las etiquetas entre los nodos MPLS.

Los LSR's que emplean LDP para intercambiar información, se llaman LDP *peers* o pares LDP y cuando intercambian información lo hacen estableciendo sesiones entre ellos.

3.5.2.1 Transporte de LDP

Para poder enviar la información referente a las etiquetas, es necesario contar con un "transporte" confiable. MPLS necesita que los mensajes LDP, en los cuales va dicha información, sean entregados en secuencia además de soportar que varios mensajes LDP sean transportados en un único paquete.

Para soportar estos requerimientos, se emplea el protocolo TCP como transporte.

[35] CR-LDP opera independientemente del IGP.

3.5.2.2 Reglas para mapear paquetes a LSP's

Como se mencionó, los paquetes se agrupan en clases equivalentes de envío o FEC's, las cuales determinan rutas LSP's únicas.

LDP es más restrictivo en cuanto al número de parámetros para la determinación de FEC's. Define FEC's para:

- Prefijos de direcciones IP
- Direcciones de *host.*

Las siguientes reglas se aplican en orden antes de que un paquete pueda ser asignado a una ruta, o sea a una clase determinada y por ende a una ruta LSP. Considérese lo siguiente:

> Una dirección "iguala" un prefijo de dirección si y solo si esa dirección comienza con dicho prefijo.
> Un paquete "iguala" una LSP si y solo si esa LSP tiene un Prefijo de dirección como elemento FEC que es igual a la dirección destino del paquete.

- ✓ Si hay exactamente una LSP que tiene una Dirección de *Host* como elemento FEC y ésta es idéntica a la dirección destino del paquete, entonces el paquete es mapeado a esa LSP.
- ✓ Si hay múltiples LSPs, y cada una tiene una Dirección de *Host* como elemento FEC que es idéntica a la dirección destino del paquete, entonces el paquete es mapeado a una de estas LSPs. El procedimiento de elegir una de las múltiples LSPs no esta definido para LDP.
- ✓ Si el paquete iguala exactamente una LSP, el paquete es mapeado a esa LSP
- ✓ Si un paquete iguala múltiples LSPs, este es mapeado a la LSP cuyo Prefijo de dirección sea lo más parecido a la dirección destino del paquete. Si no hay una LSP cuyo prefijo de dirección iguale lo más posible la dirección destino del paquete, el paquete se mapea a una de las múltiples LSPs cuyo Prefijo de dirección iguale a la dirección destino más que los otros.
- ✓ Si se sabe que un paquete debe pasar por un enrutador de egreso en particular y existe una LSP que tiene un Prefijo de dirección como elemento FEC el cual es la dirección de dicho enrutador, entonces el paquete es mapeado a ese LSP.

3.5.2.3 Sesiones LDP

El establecimiento de sesiones es fundamental para el intercambio de etiquetas entre LSR's. Éstos emplean mecanismos para el descubrimiento de vecinos empleando mensajes *hola* que son enviados periódicamente. Si dos LSR's no están conectados directamente porque forman parte de dominios diferentes es posible que puedan establecer una LSP. Para lograrlo se hace uso de la pila de etiquetas que puede transportar un paquete IP. Solo es necesario agregar a la tabla de etiquetas de un LSR la etiqueta con la que se podría "identificar" el tráfico que va dirigido a un LSR que no esta conectado directamente o que no es adyacente.

3.5.2.4 Reglas para la asignación y distribución de etiquetas

El proceso de asignación de etiquetas lo realiza un nodo MPLS, generalmente aquel que se encuentra en el ingreso de la red MPLS. Este proceso de asignación de etiquetas lo describe el proceso de *binding* o asociación, el cual asocia una etiqueta a un determinado FEC. Para lograrlo se emplea el método *downstream binding*.

3.5.2.4.1 *Downstream binding*

Existen dos variaciones de este método:

- **Asignación sin solicitud:**

En este método un nodo MPLS asigna una etiqueta a una FEC y le avisa o distribuye a su nodo adyacente de dicha asignación.

Cuando la asignación la hace un enrutador a otro en la dirección del flujo de los datos, se dice que es un *downstream* LSR o enrutador de bajada (Rd) y el enrutador que recibe dicha asignación se denomina *upstream* LSR (Ru).

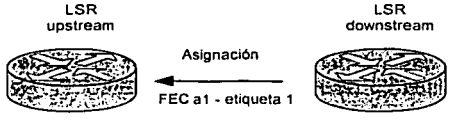


Figura 3.11 Asignación y distribución sin solicitud

- **Asignación por demanda:**

En este tipo de asignación, un nodo MPLS solicita una determinada etiqueta para un determinado FEC.

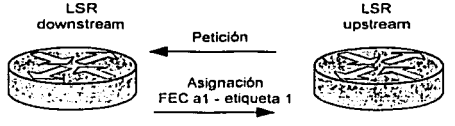


Figura 3.12 Asignación y distribución por demanda

Generalmente los nodos adyacentes son los encargados de acordar las asociaciones de etiquetas a FEC's.

3.5.2.4.2 Control de etiquetas para su distribución

Existen dos tipos de formas en que los nodos MPLS acuerdan y distribuyen una determinada etiqueta para un determinado FEC.

- **Control independiente**
- **Control ordenado**

La forma independiente es cuando un nodo, que recibe un aviso de una ruta por medio de un IGP, hace la asignación de etiquetas en forma independiente y la distribuye a los enrutadores que están a su alrededor. En esta opción es indispensable configurar el nodo que recibió el aviso y los enrutadores que recibirán la asignación, ya que todos los nodos deben realizar la misma asignación de etiqueta al mismo FEC. De lo contrario, los paquetes que no tengan asignado el mismo FEC, y por lo tanto no tengan identificado una ruta LSP, serán descartados.

Figura 3.13 Control independiente

La forma ordenada, es más segura aunque es un método más lento. El asignamiento y distribución empieza por una orilla de la red MPLS, cuando recibe un aviso de una ruta, el LER hace la asignación y avisa de esta asignación al nodo inmediato que tenga, siguiendo este orden hasta llegar al otro lado de la red.

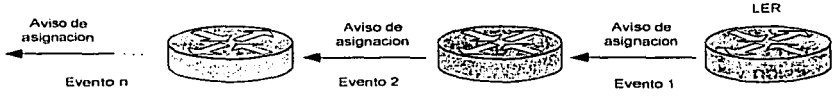


Figura 3.14 Control ordenado

3.5.2.5 Mensajes LDP

Existen cuatro clasificaciones de mensajes LDP y son las siguientes:

- Mensajes de descubrimiento de vecinos
- Mensajes de sesiones
- Mensajes de avisos
- Mensajes de notificaciones

Los mensajes de descubrimiento se emplean para conocer cuando un LSR tiene vecinos a los cuales se tenga que anunciar, además sirven para anunciar si están activos. Esta clase de mensajes emplean direcciones *multicast* y se transmiten, empleando el puerto UDP, como mensajes *hello* que son mandados periódicamente.

Los mensajes de sesión ayudan a establecer, mantener y eliminar una sesión establecida entre LSR's. Ayuda a preparar el enlace para que los pares puedan enviar mensajes sobre TCP.

Los mensajes de avisos se encargan de distribuir los mapeos de las etiquetas para cada FEC. Ayudan a crear, modificar y borrar las etiquetas empleadas.

Por ultimo los mensajes de notificación ayudan a monitorear el estado de la sesión, brindando información de errores y diagnostico.

El formato de los mensajes LDP es como se muestra en la siguiente figura, también llamado PDU (*Protocol Data Unit*), el cual tiene un encabezado LDP seguido de 1 o más mensajes que pueden ser acarreados en el mismo PDU.

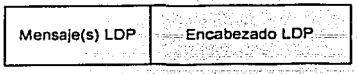


Figura 3.15 Formato del PDU LDP

3.5.2.5.1 Formato de encabezado LPD

Para disminuir el procesamiento en los enrutadores, LDP puede enviar varios mensajes con un único encabezado en un paquete.

El formato del encabezado es el siguiente.

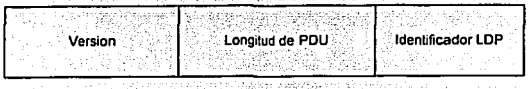


Figura 3.16 Formato de encabezado LDP

El campo versión indica la versión del protocolo LDP, que actualmente es la número 1.

El campo longitud de PDU indica el tamaño en bytes de los mensajes LDP quitando los campos de versión y de longitud.

El campo identificador de LDP es de 6 bytes y se divide en dos partes. La primera indica el identificador del enrutador, o su dirección IP, la cual consta de 4 bytes y la segunda parte, los últimos 2 bytes indican el espacio de etiquetas que maneja dicho LSR. Cuando las etiquetas están en un espacio de plataforma, estos 2 bytes tienen valores de cero.

3.5.2.5.2 Formato de mensaje LPD

Todos los mensajes LDP tienen el mismo formato.

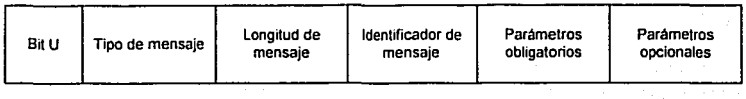


Figura 3.17 Formato de mensaje LDP

El bit U indica el desconocimiento de un tipo de mensaje. Cuando contiene el valor de 1, el mensaje se descarta.

El campo tipo de mensaje identifica una de las clasificaciones de mensajes que se transporta.

El campo longitud de mensaje incluye los campos identificador de mensaje, parámetros obligatorios y los opcionales en su valor.

El identificador de mensaje es de valor único y esta asociado a cada tipo de mensaje.

3.5.2.5.3 Tipos de mensajes LPD

LDP emplea 11 mensajes en total para realizar sus funciones de distribución de etiquetas.

Estos son:

- Notificación
- Hola
- Inicialización
- Con vida
- Dirección
- Dirección de retiro
- Mapeo de etiqueta
- Petición de etiqueta
- Petición de suspensión de uso de etiqueta
- Etiqueta de retiro
- Liberación de etiqueta

El mensaje de notificación ayuda para que un par LDP indique a su par acerca de mensajes de errores o algunas otras notificaciones. Por ejemplo, mensajes no conocidos, la expiración en un mensaje, errores en la inicialización para una sesión, etc. En caso de que un mensaje de notificación indique un error, el par LDP terminará la sesión eliminando las asociaciones de etiquetas con las FEC's que se habían establecido en dicha sesión.

El mensaje hola es enviado periódicamente por un par LDP para indicar que se encuentra funcionando, además de incluir parámetros de este mismo mensaje como son cuantos mensajes hola se pueden enviar y recibir y que tan a menudo. Los LSR's mantienen registros de mensajes hola de sus posibles pares. Manejan un tiempo que negocian entre ellos para saber cuanto tiempo mantienen los registros antes de recibir otro mensaje hola de su posible par. Algunos otros parámetros opcionales indican un número de secuencia que ayuda a detectar posibles cambios en la configuración de envíos de mensajes.

Los mensajes de inicialización son importantes ya que definen parámetros que permiten definir métodos de intercambio de etiquetas. También ayuda a definir los métodos para negociar etiquetas si se emplean etiquetas de ATM o FR. Tiene parámetros que indican el tipo de asignación de etiquetas como puede ser sin solicitar o por demanda.

Los mensajes con vida se emplean para monitorear y saber si la conexión TCP que soporta las sesiones LDP esta activa.

Los mensajes de dirección son empleados por un par LDP para enviar a su otro par sus direcciones de interfaz, ayudando a mantener una base de datos para mapear estas direcciones con los próximos saltos.

Los mensajes de direcciones de retiro eliminan de las bases de datos las direcciones advertidas por los mensajes de dirección.

Los mensajes de mapeo de etiquetas son muy importantes y se encargan de llevar información para avisar a un par LDP de la asociación de una etiqueta a una FEC. Cuando un LSR realiza una asociación de etiqueta a FEC y la tiene que distribuir a múltiples pares, el propio LSR decide si asigna una sola etiqueta a un FEC por cada par al que tenga que avisar o si asigna una etiqueta por FEC para todos los pares que tenga que avisar.

Los mensajes de petición de etiquetas los usan los LSR's para pedir a un par LDP que realice una asociación de una etiqueta con una FEC.

Los mensajes de petición de suspensión de uso de etiqueta sirven para quitar las asociaciones de las etiquetas a determinadas FEC's. Esto se realiza por configuración o en caso de que un LSR no reconozca una FEC a la cual asocio con una etiqueta previamente.

Para complementar este mensaje existe el mensaje de etiqueta de retiro que lo produce el LSR que recibió el mensaje previo.

El mensaje de petición de suspensión de uso de etiqueta elimina el mensaje de petición de etiqueta.

3.5.2.6 Procedimientos para el uso y distribución de etiquetas

En el ambiente MPLS contamos con distintos nodos, los cuales efectúan diferentes procedimientos. Tenemos los *downstream* LSR y los *upstream* LSR.

Los procedimientos que realiza un *downstream* LSR con respecto a las etiquetas son:

- Distribución
- Retiro

Los procedimientos que realiza un *upstream* LSR son:

- De petición
- De no disponibilidad
- De liberación
- De uso de etiqueta

3.5.2.6.1 Procedimientos del *downstream* LSR

Distribución

Un LSR de bajada (Rd) emplea este procedimiento para determinar cuando es necesario realizar la distribución de las asociaciones de una etiqueta con un determinado FEC, que clasifica en este caso prefijos de red. Existen cuatro procedimientos distintos de distribución llevados a cabo por el LSR de bajada y son:

- *PushUnconditional*
- *PushConditional*
- *PulledUnconditional*
- *PulledConditional*

Para los cuatro procedimientos deben suponerse las siguientes condiciones:

Se supone que en la tabla de enrutamiento del enrutador *downstream* existe un prefijo de dirección que se denominará como X.
Para el prefijo X, el enrutador *upstream* es par del enrutador *downstream*, es decir, que este último debe distribuir etiqueta con respecto al prefijo X.

PushUnconditional

Primero el Rd debe hacer la asociación de la etiqueta con el prefijo de dirección. Segundo debe distribuir a su par LDP de dicha asociación y mantener registradas todas las asociaciones que distribuye. Con este método se distribuirán etiquetas asociadas a todos los prefijos existentes en la tabla de enrutamiento del Rd, sin condición.

Los LSRs configurados para ejecutar asignación sin solicitud y control de etiquetas independiente, serán los que usen este método.

PushConditional

A diferencia del anterior, en éste solo se distribuyen asociaciones de etiquetas de aquellos prefijos de direcciones que han sido previamente recibidos de otro LSR, con la condición de que deben residir dichos prefijos en la tabla de enrutamiento del Rd. Ese otro LSR tendría que ser el próximo salto para dicho prefijo.

Los LSRs configurados para ejecutar asignación sin solicitud y control de etiquetas ordenado, serán los que usen este método.

PulledUnConditional

Siendo X un prefijo de dirección que reside en la tabla de enrutamiento de un Rd y Ru pide explícitamente una asociación de etiqueta al mismo prefijo X a Rd, éste debe hacer la asociación y distribuirla inmediatamente a Ru.

En el caso que dicho prefijo de dirección no este en la tabla de enrutamiento de Rd o que Rd no es el par para la distribución de etiquetas con respecto a dicho prefijo, entonces Rd debe informar a Ru que no puede distribuirle una asociación en ese momento.

En el caso de que Rd haya distribuido ya una etiqueta hacia Ru, es posible que Rd asocie y distribuya una segunda etiqueta para el mismo prefijo.

Los LSR configurados para ejecutar distribución de etiquetas sobre demanda y control de etiquetas independiente, serán los que usen este método.

PulledConditional

Si se tiene un LSR que ya ha anunciado una asociación a un Rd y un Ru le pide explícitamente a Rd una asociación, se procede a realizar la asociación y posteriormente la distribución a Ru.

Si el prefijo de dirección, para el cual Ru esta pidiendo una asociación, no reside en la tabla de enrutamiento de Rd, o si Rd no es el distribuidor de etiquetas para Ru, entonces Rd informa a Ru que no puede proveer una asociación al momento.

Rd no podrá contestar con una asociación a Ru para determinado prefijo de dirección, hasta que reciba de un LSR una asociación para dicho prefijo de dirección, que en este caso el LSR debería de ser el próximo salto para dicho prefijo.

Los LSR configurados para ejecutar distribución de etiquetas sobre demanda y control de etiquetas controlado, serán los que usen este método.

Retiro

Consiste en eliminar una asociación de etiqueta con un prefijo de dirección. Debe enviarse un mensaje de desasociación a todos los nodos que hayan recibido dicha asociación.

3.5.2.6.2 Procedimientos del *upstream* LSR

- *RequestNever*

En este procedimiento se libera al *upstream* LSR de la tarea de realizar una petición de asociación de etiqueta a un Rd.

- *RequestWhenNeeded*

Se realiza una petición de asociación y distribución cuando una dirección de ruta o prefijo es reconocido.

- *RequestOnRequest*

Un LSR realizara este procedimiento para emitir una petición cuando reciba otra. Por ejemplo si un LSR no puede ser un LER, entonces emitirá otra petición que enviará a otro LSR.

- *NotAvailable Procedure*

Cuando un Rd no sea capaz de proveer una asociación a un Ru, este procedimiento indicará la manera en que un Ru debe proceder. Las opciones son con los dos siguientes procedimientos:

RequestRetry
RequestNoTry

El procedimiento *RequestRetry* indicará que el Ru debe volver a ejecutar la petición de asociación en un momento posterior.

El procedimiento *RequestNoTry* indica que nunca realizará una petición de asociación, asumiendo que el Rd distribuirá una asociación cuando la tenga disponible.

- *Release Procedure*

Se refiere a la eliminación de la asociación de una etiqueta con un determinado FEC. Las opciones para que se de éste procedimiento son que un Rd deje de ser el próximo salto para un determinado prefijo de dirección, lo que provocaría que para el Ru deje de tener sentido seguir almacenando dicha asociación.

Existen dos procedimientos que indican el comportamiento de un Ru cuando esto se da.

ReleaseOnChange
NoReleaseOnChange

El primer procedimiento lo realiza el Ru para liberar la etiqueta e informar al Rd que lo ha hecho.

El segundo procedimiento lo realiza para mantener la asociación, en el caso de un eventual cambio referente a que el Rd se vuelva a convertir en el próximo salto de dicho prefijo de dirección.

- *Label Use Procedure*

El uso de la etiqueta estará determinado si el Rd es el próximo salto de Ru para el prefijo de dirección al cual esta asociado la etiqueta. Cuando Rd deje de serlo, no se hará uso de dicha etiqueta. Dos procedimientos ayudan a que este procedimiento se ejecute.

UseImmediate
UseIfLoopNotDetected

El primer procedimiento se ejecuta cuando no hay procedimiento de detección de *loops*. Cuando esto se da, Ru procede a hacer uso inmediato de la etiqueta.

El segundo procedimiento se emplea cuando un *loop* se ha detectado en la LSP. Cuando esto sucede, el Ru para inmediatamente el uso de la etiqueta hasta que deje de detectarse un *loop* en la LSP.

3.6 Otros protocolos

3.6.1 RSVP, *Resource Reservation Protocol*

Desarrollado a principios de los 90's, RSVP fue diseñado para garantizar una entrega fiable de datos en las redes de área local, ya que cada vez se manejaban mayores cantidades de información y era complicada manejarlas con los enrutadores convencionales.

El protocolo RSVP esta diseñado para reservar recursos para una sesión. Brindando una característica adicional al método tradicional de envió de paquetes, RSVP atiende los requerimientos de la aplicación del usuario final.

Ante la carencia de establecer caminos o rutas para los paquetes en las redes IP, orientadas a no conexión, RSVP esta diseñado para configurar estas rutas además de garantizar el ancho de banda necesario para que las aplicaciones que lo requieran tengan un rendimiento óptimo sobre dichas rutas.

Con RSVP se establecen enlaces punto a punto con la capacidad para satisfacer los requerimientos de QoS, necesario para poder ejecutar MPLS. Con RSVP, todos los nodos que forman la ruta a cruzar, están avisados de los requerimientos de ancho de banda que deben reservar para un determinado enlace.

El mecanismo de transporte que emplea RSVP es IP, ya sea versión 4 o 6. Opera con *multicast* o *unicast*.

RSVP se comunica empleando dos tipos básicos de mensajes:

- PATH
- RESV

El mensaje PATH lo emite un servidor o un enviador de tráfico y lo manda a uno o múltiples receptores. A este mensaje le contesta un mensaje RESV el cual debe de viajar por el mismo camino que viajo el mensaje PATH. En las redes MPLS, la etiqueta viaja en este último mensaje.

RSVP requiere que el receptor del tráfico realice una petición de QoS para un determinado tráfico. Una vez elaborada la petición, el receptor envía un perfil de QoS que es analizada por el protocolo RSVP. Como resultado del análisis, RSVP envía a todos los posibles nodos participantes en la ruta los requerimientos de QoS necesarios a reservar.

Los mensajes PATH son empleados para configurar la ruta que será ocupada por una sesión. Estos dos mensajes contienen la suficiente información para satisfacer las necesidades de ancho de banda.

Una característica de RSVP es que puede ser empleado para distribuir etiquetas, empleadas en las redes MPLS.

Se puede usar BGP para poder descubrir el LER de egreso para poder enrutar el tráfico a otro sistema autónomo. El LER de ingreso inicia con un mensaje PATH hacia el LER de egreso a través de cada LSR a lo largo de una ruta. Cada nodo recibe un mensaje PATH para recordar el paso del flujo y para saber que una sesión se esta creando. El LER de egreso usa el mensaje RESV para reservar recursos con parámetros de tráfico y QoS en cada LSR a lo largo de la ruta que formara parte de la sesión. Una vez llegado este mensaje al LER de ingreso, un mensaje RESVConf es regresado al LER de egreso para confirmar la sesión sobre la LSP. Después de

haber establecido la ruta, algunos mensajes de actualización son enviados para mantener la ruta así como mantener los recursos reservados. Esto queda descrito en la siguiente figura.

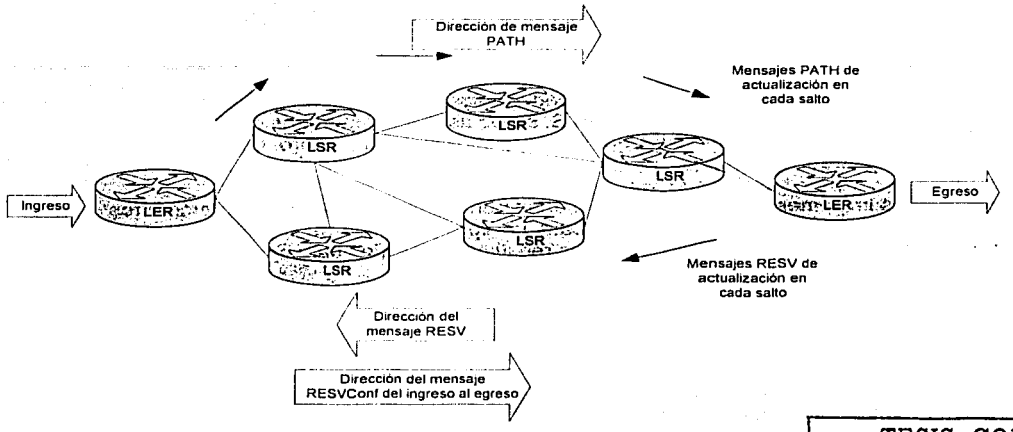


Figura 3.18 Flujo de mensajes RSVP

3.6.2 BGP

La conveniencia de identificar FEC's con rutas o prefijos de red es mucha. A través de uso de un protocolo que distribuya rutas o prefijos de red, se puede hacer que la misma distribución de etiquetas se realice al mismo tiempo que cuando se distribuyen dichas rutas.

El hecho de emplear un protocolo que distribuya rutas permite prescindir del uso de un protocolo adicional como LDP para la distribución de las etiquetas.

En el caso de BGP, éste tiene la capacidad para distribuir etiquetas. Cuando distribuye una ruta, puede estar distribuyendo al mismo tiempo una etiqueta que esta asociada a una ruta. La etiqueta es transportada en los mensajes de actualización que BGP emplea para anunciar rutas. Para ello es necesario tener las extensiones multiprotocolo de BGP versión 4.

Se puede emplear el enrutador reflector para la distribución de etiquetas, aprovechando que el enrutador reflector se emplea para el intercambio de rutas entre enrutadores BGP lográndose buena escalabilidad.

3.7 Ingeniería de tráfico

3.7.1 Introducción

Existen dos tecnologías que nos permiten aplicar métodos de ingeniería de tráfico (TE, *Traffic Engineering*) en redes MPLS. Los procedimientos de la TE permiten que los paquetes que han sido etiquetados al ingreso de la red MPLS, se les asignen parámetros de TE para que puedan ser programados a fin de garantizarles niveles de ancho de banda, control de congestión así como variación en el retardo.

Ambas implementaciones permiten manejar una determinada ruta con parámetros de QoS y CoS[36], lo que asegura una óptima ruta para un tipo específico de tráfico, entendiéndose por óptima ruta una ruta capaz de proporcionar los recursos necesarios para soportar dicho tráfico.

Los protocolos para la distribución de etiquetas fueron mejorados para que pudieran soportar la reservación de rutas explícitas LSP, a fin de poder brindar calidad de servicio y para poder implementar procedimientos de ingeniería de tráfico. Tal es el caso de LDP el cual fue extendido a CR-LDP (*Constraint-Based Routed LDP*). El otro caso fue RSVP, aunque en este caso, RSVP fue desarrollado en un inicio para garantizar la entrega de información, reservando recursos de la red física y fue mejorado para proveer funciones de distribución de etiquetas y para proveer operaciones de ingeniería de tráfico. La extensión fue TE-RSVP (*Traffic Engineering RSVP*).

Estos protocolos funcionan como protocolos de señalización en las redes MPLS para poder soportar los requerimientos básicos de este tipo de redes, y teniendo como objetivo principal el establecimiento de LSP's punto a punto en base a un QoS determinado para MPLS.

Esta última característica es muy útil cuando se intenta diseñar enlaces sobre redes públicas o cuando se configuran redes privadas virtuales.

3.7.2 Protocolos de Ingeniería de Tráfico

3.7.2.1 TE-RSVP

Las extensiones al protocolo RSVP propuestas para implementar operaciones de ingeniería de tráfico en redes MPLS, son lo que constituyen TE-RSVP.

Cuando se implementa TE-RSVP no es necesario que RSVP sea implementado completamente en la red. Solo es necesario que los LER´s o los LSR's soporten las extensiones de enrutamiento explícito para MPLS[37].

TE-RSVP es un protocolo de estado suave[38] que emplea UDP sobre datagramas IP como mecanismos de transporte entre pares.

---

[36] QoS define parámetros que garantizan ancho de banda, retardo, *jitter* y pérdida de datos mientras que CoS indica como deben de ser tratados los paquetes cuando un protocolo de capa superior los manda a un protocolo de capa inferior dentro del modelo de referencia OSI.

[37] TE-RSVP y CR-LDP soportan enrutamiento explicito con sus dos variantes: amplio y estricto.

Los servicios de ingeniería de tráfico que están disponibles para MPLS son:

- Parámetros de tráfico y QoS

  Ofrecen la capacidad para definir reglas terminales y comportamientos por salto basados en velocidad de datos, ancho de banda de enlaces y el peso dado a estos parámetros.

- Notificación de fallas

  Cuando ocurren las fallas al momento de establecer una LSP, se enviaran mensajes de notificación de las mismas, de acuerdo a los *timers* de mensajes de refresco.

- Restauración de fallas

  A través de políticas de mapeo, se recuperan automáticamente fallas en cada dispositivo que este siendo usado para soportar una LSP.

- Detección de *loops*

  Esto es requerido solo para LSPs construidas con enrutamiento no estricto.

- Soporte multiprotocolo

  Soporte para cualquier tipo de protocolo.

- Administración

  Con el uso de los identificadores de las LSP's se identifican estas de tal manera que puedan ser fácilmente identificables y administrables.

- Registro de objetos de ruta

  Provee la habilidad de describir el actual arreglo de rutas a las partes interesadas.

- Prioridad de ruta

  Parámetro que da la habilidad para descontinuar una ruta existente para que un túnel de mayor prioridad pueda ser establecido.

Este protocolo requiere que mensajes de actualización sean enviados a cada *peer* periódicamente para indicar que la sesión establecida aun se requiere. Si este mensaje no se envía, entonces se detectará la ausencia de estos y se procederá a borrar la información de las sesiones, liberando etiquetas empleadas y los recursos para que otras sesiones puedan disponer de dichos recursos.

[38] Los protocolos de estado suave están mandando constantemente mensajes de actualización que ayudan a mantener abiertas las sesiones establecidas, contrario a los de estado duro, que solo emplean mensajes para iniciar y terminar las sesiones establecidas.

Precisamente por ser un protocolo de estado suave y al generar *overhead*, no es escalable[39]. De acuerdo al estándar que define TE-RSVP, un enrutador requerirá recursos físicos proporcionales al número de sesiones que sean habilitadas en dicho enrutador. Si se habilitan muchas sesiones pequeñas en enlaces de alta capacidad, se puede sobrecargar el enrutador hasta provocar que sea inadmisible.

Como posibles soluciones, se hizo posible que en un mismo datagrama pudieran viajar varios mensajes RSVP con el fin de disminuir el *overhead*, proceso conocido como *bundling*. Con la agregación de varios mensajes en un mismo paquete, se disminuyo el tiempo para generarlos así como el tiempo para analizarlos aunque aun se trabaja para mejorar dicho detalle.

Por otra parte RSVP permite reservar ancho de banda para solo una dirección IP. Se emplea el concepto *microflow* para indicar que el destino contiene solo una dirección IP. Actualmente se trabaja para que pueda soportar servicios diferenciados.

3.7.2.2 CD-LDP

Como se sabe, LDP fue creado para llevar a cabo las funciones de distribución de etiquetas necesarias para que MPLS funcione.

Surgió después de RSVP y con CR-LDP no es necesario implementar un nuevo protocolo ya que con su estructura actual de mensajes y algunas extensiones es suficiente para proveer ingeniería de tráfico.

Al igual que TE-RSVP, soporta la construcción de LSP's con enrutamiento explícito estricto y amplio. CR-LDP emplea UDP y TCP. UDP lo emplea para descubrir pares LDP y TCP lo emplea para funciones de mapeo, control, administración y peticiones de etiquetas.

La forma de implementar QoS es muy similar a la tecnología de ATM. Tiene la capacidad para alojar ancho de banda basado en la prioridad de las LSP's.

CR-LDP es un protocolo de estado duro, permite la creación de LSPs enrutadas explícitamente estrictas y no estrictas, teniéndolas habilitadas hasta que un sistema de administración decida eliminar dichas LSP. Provee mecanismos de descubrimiento de vecinos por medio de mensajes *multicast* empleando paquetes UDP, enviándolos a todos los vecinos dentro de la misma subred.

Las extensiones de CR-LDP para proporcionar ingeniería de tráfico en redes MPLS son:

- Parámetros de QoS y tráfico

Ofrecen la capacidad para definir reglas terminales y comportamientos por salto basados en velocidad de datos, ancho de banda de enlaces y el peso dado a estos parámetros.

- Prioridad de ruta

Habilita para establecer prioridad para permitir o no permitir la priorización de otra LSP.

[39] Las actualizaciones periódicas van consumiendo cada vez más ancho de banda conforme el número de sesiones aumenta, lo que puede ser muy inconveniente al usar enlaces de baja capacidad. Por otra parte cada enrutador debe mantener en memoria cada sesión abierta, lo que la va consumiendo hasta agotarla. Otro punto es que la administración de las sesiones se vuelve extremadamente difícil conforme el número de sesiones aumenta.

- Reoptimización de ruta

Ofrece la habilidad de re-enrutar LSP's enrutadas no estrictamente con base en cambios de patrones de tráfico e incluye la opción de usar el fijado de ruta.

- Notificación de fallas

Cuando ocurren las fallas al momento de establecer una LSP, envía mensajes de notificación de las mismas a través del soporte que brinda TCP.

- Restauración de fallas

A través de políticas de mapeo, se recuperan automáticamente fallas en cada dispositivo que este siendo usado para soportar una LSP.

- Detección de *loops*

Esto es requerido solo para LSP's construidas con enrutamiento amplio.

- Suporte multiprotocolo

Provee soporte para cualquier tipo de tráfico.

- Administración

A través del identificador de la LSP, se permite el fácil manejo de las LSP.

CR-LDP solo requiere que al inicio de la configuración de la sesión sea intercambiada información, manteniéndose la LSP hasta que un programa de administración decida que ya no es necesaria la LSP y tire la conexión. Mientras la sesión este abierta y en uso, se empleara TCP/IP para establecer y mantener la LSP con los mensajes apropiados.

Si un enlace TCP falla, todas las sesiones asociadas a una LSP se destruyen. Esto último impacta en forma importante a la red. Respecto a esto, RSVP tiene ventaja ya que sus túneles son locales por lo que si uno falla no afecta a los demás.

Como sabemos, con LDP al establecer las rutas conmutadas, el ingreso de un paquete a la red, que pertenece a una FEC, es mapeado a una LSP. Con CR-LDP, además de proveer esta característica, introduce el concepto de servicios diferenciados. Este concepto indica que cuando un paquete ingresa a la red, además de mapearlo a una LSP, se le asignan parámetros que serán empleados en el transcurso del paquete por la red. Combinando estos conceptos se permite la agregación de tráfico para poder ser acarreado en la dorsal de una red.

Característica	CR-LDP	TE-RSVP	Comentario
Configuración inicial	Mensaje de petición de etiqueta	Mensaje PATH conteniendo un objeto de petición de etiqueta.	
Configuración cumplida	Mensaje de mapeo de etiqueta	Mensaje RESV, que contiene la etiqueta.	
Servicios diferenciados definidos	DIFF-SERV_PSC TLV	Objeto DIFFSERV_PSC	Ambos contienen el código DiffServ y son incluidos en el mensaje de petición

			de configuración.
Soporte para LSP punto a multipunto	no	no	Pendiente
Capacidad para ruta fuente	Es acarreada en la lista TLV	Es acarreada en el objeto EXPLICIT_ROUTE	Especifica la ruta usada para formar la ruta conmutada.
Fase de desarrollo	Nueva	Vieja con extensiones	Objetos RSVP son modificados para ser usados en redes MPLS.
Transporte de señalización	UDP para el descubrimiento y TCP para sesiones	Datagramas IP en crudo o encapsulación UDP para el intercambio de mensajes	Detección de fallas no determinístico con RSVP; Una falla TCP puede tener un catastrófico impacto con las LSP's con CR-LDP.
Estado de conexión	Estado duro	Estado suave	El estado suave es no escalable; RSVP soporta agregación de mensajes de refresco.
Confiabilidad	Las fallas producen señalización proactiva	Depende del tiempo en estado suave para detectar al falla	Detección de falla no determinístico con RSVP.
Administrabilidad	LSR, LDP, TE MIBS	MIBS LSR y RSVP modificadas	
Extensibilidad	Especificas del fabricante	Objetos experimentales	
Escalabilidad	Conexiones en estado duro reducen la señalización de las sesiones.	Requiere la reducción de los mensajes de refresco, agregación para minimizar el overhead de estado suave	
Interoperatividad	Soporte para la mayoría de las tecnologías de transporte: FR, ATM, Ethernet	Tuneleo a través de redes ATM deben ser configuradas manualmente.	

Tabla 3.2 Comparación entre TE-RSVP y CR-LD

Capítulo 4. Redes Privadas Virtuales

4.1 Introducción

La utilización de Redes Privadas[40] para proveer conectividad entre la empresa corporativa y las oficinas anexas o usuarios móviles presenta grandes limitantes respecto a los costos generados, flexibilidad y tiempos de implementación.

Las VPN[41]s han surgido como alternativa para proveer la conectividad necesaria cubriendo los requerimientos que las tecnologías anteriores no hacían. Así, la implementación de estas puede llevarse a cabo empleando redes públicas como FR[42] o la Internet o empleando una red privada compartida como la de un Proveedor de Servicio.

La tradición de construir las VPNs sobre enlaces FR o ATM[43] ha venido a menos por la creciente aceptación de la tecnología IP. Como sabemos, la tecnología que emplea la Internet esta basada en lo que es el protocolo IP y muchos Proveedores de Servicio cuentan con redes bajo tecnología IP, por ello, la provisión del servicio VPN ha ido cambiando de tecnología subyacente, convirtiéndose en una necesidad desarrollar nuevos mecanismos compatibles con el protocolo IP que cumplan con los requerimientos que las tecnologías anteriores no cubrían.

Con las redes privadas construidas con tecnologías anteriores a FR y ATM, el tráfico de un solo cliente era transportado sobre un solo enlace dedicado. El paradigma usado por estas tecnologías fue trasladado a la Internet, con la idea de que el tráfico de más de un cliente pase por el mismo enlace físico. Para poder permitir que la información fuera transmitida como si se tuviese un solo canal, se desarrollaron inicialmente varios protocolos para poder construir los así después llamados túneles. El *tuneleo* consiste en la capacidad de encapsular la información en paquetes IP para poder ser enviados a través de la red pública ocultando la infraestructura de la red pública que se esta empleando.

Los protocolos para construir túneles en redes IP juegan un papel muy importante para la construcción de las así después llamadas *IP VPNs*, las cuales han venido a complementar las carencias de las Redes Privadas y VPNs tradicionales construidas sobre circuitos virtuales.

El hecho de construir IP VPNs empleando la infraestructura pública tiene ciertas ventajas. Cuando se construían VPNs de circuitos virtuales, forzaban al cliente a invertir en equipo adicional para que

[40] Redes LAN interconectadas por una red WAN con enlaces dedicados
[41] Red Privada Virtual (*Virtual Private Network*)
[42] *Frame Relay*
[43] *Asychronous Transfer Mode*

soportara dicha tecnología, lo que incurría en costos adicionales. Cuando se construyen redes privadas sobre la Internet, no se requiere equipo adicional para poder proveer y acceder a estos servicios. Además se puede proveer un esquema en el que las tareas de administración sean trabajo del Proveedor de Servicio (*Service Provider*, SP) y no del cliente.

También, el hecho de construir las VPNs sobre tecnología IP conlleva lidiar con las limitaciones del protocolo IP, que en sus inicios carecía de mecanismos que son inherentes a la construcción de las VPNs. Estas limitaciones son seguridad además de rendimiento, entre otras características necesarias para desarrollar VPNs. También, estas IP VPNs están más orientadas a conectar un usuario remoto a la red privada perteneciente a una empresa, es decir una conexión usuario-LAN, siendo que los negocios están requiriendo, además de este tipo de conexiones, mayor intercambio de información entre empresas o redes privadas, o sea, conexiones LAN-LAN.

De esta forma, extensiones hacia el protocolo IP fueron necesarias para proveer estas y otras características que se demandan. A pesar de la creación de estas extensiones hacia el protocolo IP para la creación de VPNs, no fueron del todo suficientes ya que en la actualidad las aplicaciones requeridas demandan mayores anchos de banda además de un mejor rendimiento, velocidad y sobre todo seguridad ante la creciente expansión de los elementos activos de una empresa que necesita estar comunicada. Para suplir la anterior necesidad, surgieron varias técnicas sobre redes IP, las cuales se han ido mejorando y diversificado.

Con la aparición de MPLS como estándar para mejorar el envío tradicional de información en la red, se pudo brindar el servicio de VPN para conexiones sitio-sitio, entre otros.

El nuevo paradigma creado para brindar servicios VPNs es MPLS/VPNs. Como se estudiará, MPLS permite implementar desde las topologías más comunes de VPNs hasta las que permiten obtener mayores beneficios. La arquitectura de este estándar y su interacción con otros protocolos permite desarrollar VPNs robustas al grado de proveer seguridad, alto rendimiento, escalabilidad, calidad de servicio, confiabilidad, bajos costos y la ventaja de que poder emplear la infraestructura existente de una red IP.

Además, este paradigma esta más orientado a la formación de VPNs entre sitios, es decir, que permite de una manera más fácil conectar LANs, distribuidas geográficamente a través de una red pública IP.

4.2 Redes Privadas Virtudes

Una Red Privada Virtual (VPN, *Virtual Private Network*) es una extensión de una red privada que permite enlazar ya sea *hosts* o redes empleando la infraestructura pública y compartida a fin de acceder a los recursos de la red privada.

Los componentes de red que componen una solución de VPN dependen de sus alcances. Así, una solución completa de VPN tiene los siguientes elementos:

- Proveedor de servicio: Es la organización que es dueña de la infraestructura (equipos y medios de transmisión) que provee las líneas dedicadas a los clientes. El proveedor de servicio ofrece al cliente el servicio de VPN.
- El cliente: Es quien requiere el servicio y se conecta a la red del SP a través del Equipo en Sitio del Cliente (*Customer Premises Equipment*, CPE). El CPE es usualmente un dispositivo que ensambla y desensambla paquetes (PAD, *Packet Assembly and*

- *disassembly*) que provee conectividad plana de terminal, un puente, o un enrutador. El dispositivo CPE es usualmente llamado dispositivo CE (*Customer Edge*).

- Equipo CE: Dispositivo que se conecta a través de un medio de transmisión (usualmente líneas dedicadas aunque también pueden ser conexiones de marcado telefónico) a un equipo del SP, el cual puede ser un conmutador X.25, FR o ATM o un enrutador IP. Este último equipo usualmente es llamado PE (*Provider Edge*).

- Equipo PE: Dispositivo de frontera perteneciente al proveedor de servicio y al cual se conectan los dispositivos del cliente.

- Equipo *P-network*: Son los dispositivos que el proveedor de servicio posee en el núcleo de su red. Nos referiremos a ellos como *switches* P o enrutadores P.

- Sitio: Se refiere a la parte contigua a la red del cliente. Un sitio puede conectarse a una red formada por dispositivos P a través de una o varias líneas de transmisión, usando uno o varios dispositivos CEs y PEs, dependiendo de los requerimientos de redundancia.

- Las líneas dedicadas: Estas son proporcionadas al cliente por el SP para comunicar a los equipos CE con los equipos PE. En un modelo VPN *Overlay*, las líneas dedicadas sirven para transportar una o varias conexiones lógicas frecuentemente llamadas circuitos virtuales (*Virtual Circuit*, VC). Los VCs pueden ser dedicados (*Permanent Virtual Circuit*, PVC) o establecidos por demanda (*Switched Virtual Circuit*, SVC). Algunas tecnologías emplean términos especiales para los VCs, como lo son los DLCIs (*Data Link Connection Identifier*, DLCI) para *Frame Relay*.

- Tasa de transmisión: El SP puede brindar una tasa plana para el servicio de VPN, la cual normalmente depende del ancho de banda disponible para el cliente, o una tasa basada en el uso, la cual puede depender del volumen de información o la duración en que ésta es intercambiada.

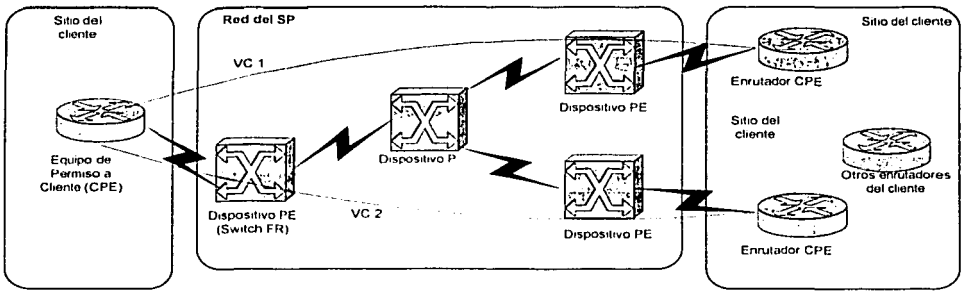


Figura 4.1 VPN típica sobre una red FR

4.3 Clasificación de VPNs

En un inicio el servicio de redes privadas virtuales era ofrecido con:

- Líneas dedicadas (LD) para conectividad permanente

- Líneas de marcado telefónico para conectividad temporal

Como el ancho de banda en las LD solo se ocupaba por periodos a lo largo del día, se decidió proveer esquemas de comunicación equivalente a las LD, dando origen a las primeras redes privadas virtuales empleando tecnología X.25 y *Frame Relay* y después con ATM.

Estas emulaciones de líneas dedicadas se conocen como circuitos virtuales y pueden ser permanentes (PVC, *Permanent Virtual Circuit*) o establecidos por demanda (SVC, *Switched Virtual Circuit*).

Al ser introducidas nuevas tecnologías para la implementación de VPN's, surgieron una diversidad de tipos de VPN's, de acuerdo a los siguientes criterios:

- El uso de tecnología de capa 2 ó 3 (X.25, FR, ATM o IP)
- La topología de la red (*hub-and-spoke, fully meshed, partial meshed*)
- Capa OSI en la cual se intercambia información topológica de la red (Modelos *Overlay* y *Peer-to-Peer*).
- Necesidades de negocios (*intranets, extranets*, VPDN)

4.3.1 VPNs como solución a necesidades de negocios

4.3.1.1 Redes Privadas Virtuales por Marcado Telefónico (VPDN)

Este tipo de VPNs solucionan el problema de conectividad de aquellos usuarios móviles o aquellos empleados que se encuentran ubicados lejos de la compañía y necesitan conectividad a la LAN de la empresa.

Esta tecnología emplea un Servidor de Acceso a Red (NAS, *Network Access Server*) y una puerta de enlace (*Home Gateway*). El NAS recibe la llamada y la envía a la puerta de enlace. También se encarga de intercambiar *frames* PPP entre el cliente y la organización. La puerta de enlace termina la autenticación así como la sesión PPP además de negociar con el cliente algunos parámetros PPP, como la IP.

Uno de los requisitos para intercambiar *frames* PPP a través de un túnel entre el NAS y el *Home Gateway* es que exista cualquier infraestructura IP entre ellos.

Los protocolos empleados para este tipo de VPN's son L2TP y L2F.

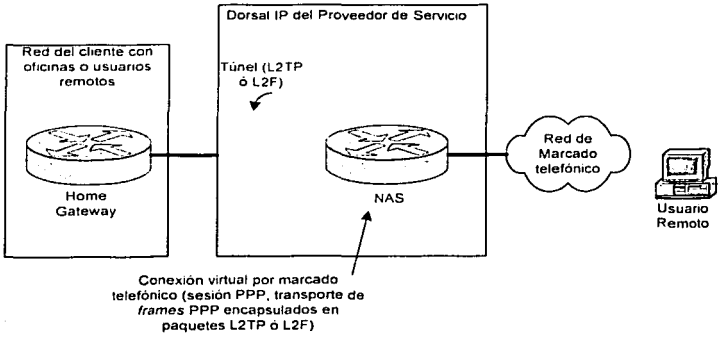


Figura 4.2 Red Privada Virtual por marcado telefónico

4.3.1.2 VPNs para *Intranets* y *Extranets*

Este tipo de soluciones se implementaban con tecnología de capa 2, como X.25, FR o ATM ya que para poder construirlas sobre la Internet se necesitaban implementar mecanismos de seguridad, calidad de servicio y aislamiento que no era posible implementar sobre la Internet.

Por dichas razones muchas empresas no emplean la Internet, ya que no pueden igualar las características que les ofrece una infraestructura privada como su *Intranet*.

En el caso de las *Extranets*, son soluciones que se implementan usualmente sobre la Internet debido a que los requerimientos de calidad de servicio son menores que las *Intranets*. Generalmente se lleva a cabo entre los sitios centrales de las empresas.

Debido al fenómeno de la globalización, la expansión de las empresas se va haciendo más frecuente además de la necesidad de intercambiar información con otras empresas.

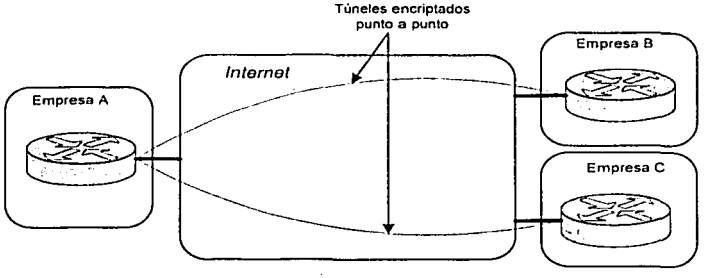


Figura 4.3 *Extranet* típica

4.3.2 Capa OSI en la cual se intercambia información topológica de la red

Existen dos modelos para esta clasificación de VPN.

4.3.2.1 Modelo *Overlay*

Las características principales de este modelo son:

- El proveedor de servicio provee líneas rentadas emuladas al cliente, osea circuitos virtuales permanentes o establecidos por demanda.
- El cliente intercambia su propia información de enrutamiento entre sus CE's (Enrutador extremo del cliente) sin que el proveedor se servicio sepa de ello, y de la estructura interna del cliente.

La calidad de servicio (QoS) esta en términos del ancho de banda (CIR, *Commited Information Rate*) y de un ancho de banda máximo disponible para el circuito virtual (PIR, *Peak Information Rate*).

Para poder garantizar el QoS es necesario que previamente se identifique el tipo de tráfico o que se disponga de un circuito virtual por tipo de tráfico, lo que resultaría muy caro. Las redes VPN con este modelo pueden implementarse con tecnología de capa 2 (X.25, FR, ATM, SMDS) aunque también se puede con tuneleo de IP sobre IP empleando los métodos de tuneleo con GRE y con IPSec.

Las desventajas de este modelo son varias:

- Se necesita conocer el perfil de tráfico del sitio para implementar al máximo las capacidades de los circuitos virtuales.
- Cuando son redes con más conexiones entre sus sitios, aumenta la complejidad de la configuración.
- Cuando se implementa con tecnología de capa 2 se incrementan los costos ya que la mayoría de las redes están basadas en IP.

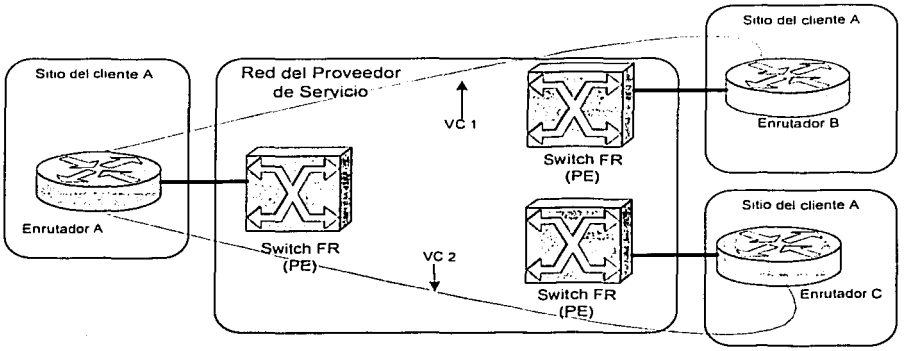


Figura 4.4 Modelo Overlay

4.3.2.2 Modelo Peer-to-Peer

En este modelo de VPN la característica principal es que el proveedor de servicio intercambia información de enrutamiento de capa 3 con el cliente permitiendo que la información viaje de sitio a sitio por la ruta óptima ya que el proveedor conoce la infraestructura interna del cliente.

Las ventajas sobre el modelo *overlay* son:

- Se puede agregar un nuevo sitio simplemente configurando el PE al que esta conectado, sin necesidad de crear un circuito virtual para conectarlo a cada sitio existente.
- La administración del ancho de banda es simple ya que solo se necesita que el cliente proporcione el ancho de banda entrante y saliente para su sitio y no el perfil de tráfico.
- El enrutamiento entre los enrutadores del cliente (CEs) es óptimo ya que el SP conoce la topología de la red del cliente y por tanto puede brindar un esquema óptimo de enrutamiento entre sitios.
- El enrutador del cliente sólo intercambia información de enrutamiento con un solo PE a diferencia del modelo *Overlay* donde se pueden tener múltiples vecinos y por tanto la información intercambiada crece proporcionalmente.

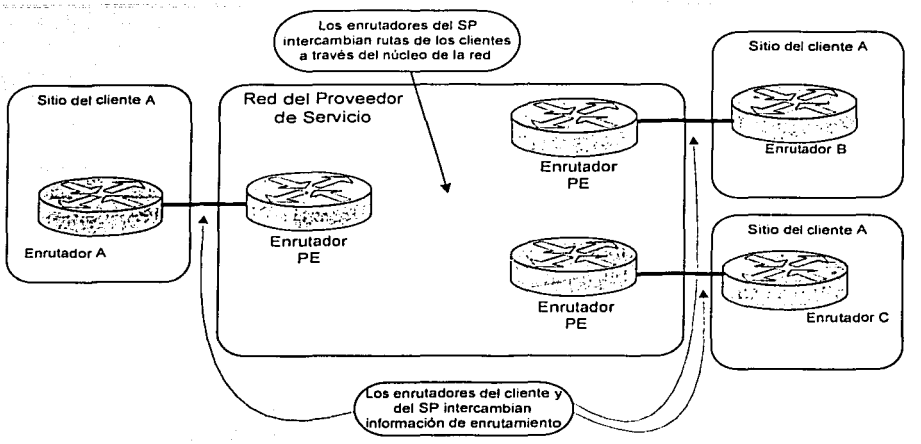


Figura 4.5 Modelo Peer-to-Peer

Existen dos implementaciones del modelo *Peer-to-Peer*:

- Enrutador compartido
- Enrutador dedicado

En el modelo compartido el enrutador PE contiene las rutas VPN de los clientes conectados a dicho enrutador. Se debe configurar listas de acceso para poder mantener aisladas y privadas las rutas de cada cliente.

En el modelo dedicado existe exclusivamente un enlace hacia un PE, siendo éste PE exclusivo del cliente.

En el modelo *Peer-to-Peer* todos los protocolos de enrutamiento empleados generan tablas de enrutamiento por cada VPN en los enrutadores PE. Los enrutadores PE contienen rutas VPN solo de aquellos clientes conectados a ellos.

Ambos modelos tienen desventajas. Cuando hablamos del modelo compartido es muy difícil mantenerlo y configurarlo ya que se deben desarrollar listas de acceso en cada interfaz de cada enrutador. Con respecto al modelo dedicado, su configuración y administración puede ser muy simple sin embargo, puede resultar muy caro si hablamos de que el SP debe dar conectividad a muchos clientes con muchos sitios muy dispersados.

Las desventajas que comparten ambos modelos son:

- Los clientes comparte el mismo espacio de direcciones IP, lo que no permite a los clientes desarrollar su propio direccionamiento privado. Si desean direccionamiento privado este debe ser dado por el SP o en lugar de ello deben emplear direcciones públicas IP.

- El cliente no puede insertar una ruta por *default* en la VPN que pertenece. Esto limita al cliente a obtener acceso a Internet a través de otro SP.

La manera en que se realiza el enrutamiento es como sigue.

Se ejecuta cualquier IGP entre el PE y el CE. Dentro de la red del proveedor de servicio se ejecutará BGP. El enrutador PE distribuirá las rutas a BGP aprendidas del CE hacia los enrutadores P del proveedor. Siendo los enrutadores P los únicos que tendrán las rutas de todos los clientes VPN. Para no confundirlas se propagan con el atributo de BGP que las identifica (es el ID del cliente).

Los PE recibirán solo aquellas rutas originadas en los CE's que pertenecen a las VPN que tienen configuradas.

4.3.3 Topologías típicas VPN's

4.3.3.1 Hub-and-Spoke

Esta topología la describe el modelo de empresa que tiene oficinas remotas que se conectan al sitio central. Generalmente emplea tecnología de capa 2 como FR o ATM.

Como esta topología esta basada en el modelo *overlay*, es necesario establecer circuitos virtuales. Existe un servicio en el cual se puede disponer de 2 circuitos virtuales por el precio de uno pero solo se puede enviar tráfico sobre uno. Se llama *shadow* PVC.

Pueden existir escenarios más complicados para esta topología como por ejemplo aumentar la redundancia colocando una conexión ISDN que respalde un enlace rentado FR.

Esta topología se recomienda cuando la mayor cantidad de información pasa de las oficinas remotas al sitio central y no cuando la mayor cantidad de información fluye entre los mismos sitios. Además de adaptarse a empresas que tienen una estructura jerárquica.

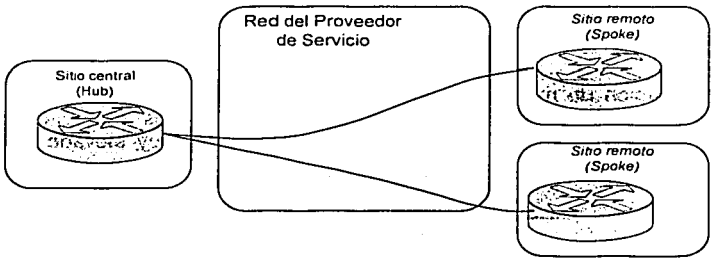


Figura 4.6 Topología típica *Hub & Spoke*

En esta topología generalmente no se aplican reglas de seguridad al tráfico que fluye entre las oficinas por ser pequeñas cantidades. Lo que impide que las empresas empleen otro tipo de topologías, que pudieran beneficiar más al cliente, son los costos como la complejidad para implementar otro tipo de topología.

4.3.3.2 Mallas parciales y completas (*Partial* y *Full-Mesh*)

La topología anterior no se recomienda cuando:

- La mayor cantidad de información debe fluir entre los sitios y no entre un sitio remoto y el sitio central.
- Las aplicaciones necesitan de una conexión punto a punto.
- Las empresas multinacionales necesitan establecer enlaces internacionales, debido a los costos que implica

Para cubrir este tipo de requerimientos se recomiendan las topologías de mallas parciales (*partial-mesh*) y las de mallas completas (*full-mesh*). Estás topologías proveen VCs para conectar los sitios.

En la configuración de malla parcial no todos los sitios se comunican entre sí y en la configuración de malla completa sí.

La configuración de malla parcial es más flexible ya que permite habilitar solo conexiones entre los sitios que intercambian mayores cantidades de tráfico.

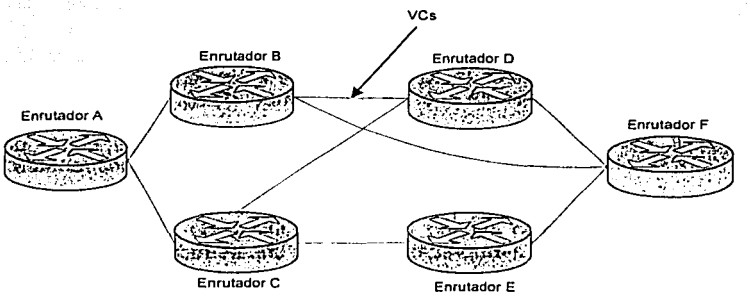


Figura 4.7 Topología de Malla parcial

En la configuración de malla completa solo es necesario establecer el ancho de banda necesario entre los sitios de la VPN y después se configuran los circuitos virtuales. Esta implementación no es muy recomendable ya que el costo resulta muy elevado además que la administración de los VCs se vuelve tediosa.

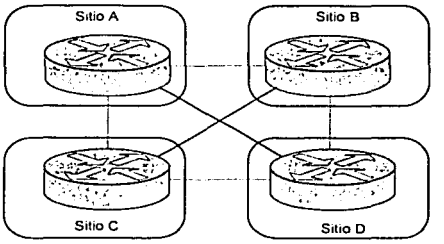


Figura 4.8 Topología de Malla completa

4.3.3.3 Híbrida

Combina las topologías *hub-and-spoke* y mallas parciales permitiendo un diseño modular de la red, es decir, se configuran las partes de acceso, distribución y núcleo de la red.

Para poder configurar una *extranet*, se puede realizar con las topologías de *overlay* y *hub-and-spoke*. Solo se prefiere por razones de QoS ya que si se utilizará la Internet sería más difícil proporcionarlo.

Para servicios centralizados de *extranet* es altamente recomendado el modelo *overlay* ya que los circuitos virtuales son establecidos desde los sitios a la organización central.

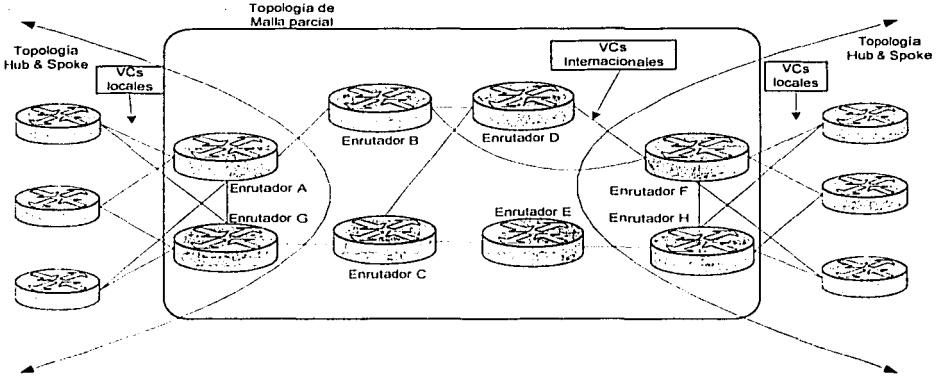


Figura 4.9 Topología híbrida (Malla parcial y *Hub & Spoke*)

Extranet

Este tipo de topologías puede ser implementado con los modelos *Overlay* o *Peer-to-Peer* enfocándose más en la parte de seguridad. En esta topología cada sitio es el encargado de proporcionar los mecanismos de seguridad.

La única razón válida, hasta antes de la aparición de MPLS, por la cual es mejor usar una *Extranet* en vez de la red pública de Internet es el provisionamiento de QoS además de la protección a la información que se intercambia.

Bajo el modelo *Peer-to-Peer*, cada sitio debe especificar la cantidad de trafico que va a transmitir y la que va a recibir, facilitando al SP su implementación. De manera que el cliente paga solo por los VCs que emplea. Por ello para este tipo de topologías es más recomendable dicho modelo.

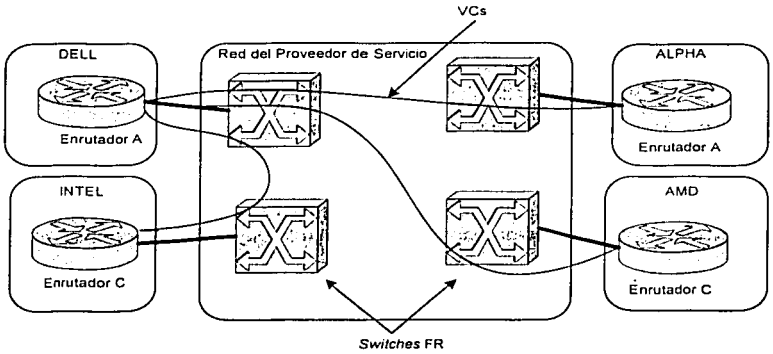


Figura 4.10 *Extranet* con el modelo *Overlay*

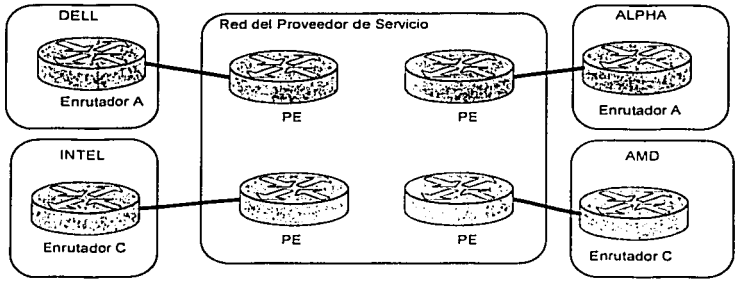


Figura 4.11 *Extranet* con el modelo *Peer-to-Peer*

4.4 Arquitectura MPLS/VPN

4.4.1 Introducción

Hemos visto los modelos principales para construir VPNs con las tecnologías disponibles: *Overlay* y *Peer-to-Peer.*

Como se puede intuir, el modelo *Overlay* presenta problemas de escalabilidad cuando se manejan cientos de sitios que requieren conexión además de que el cliente puede experimentar problemas en el manejo de su información de enrutamiento, ya que el SP solo le da las conexiones para que los CEs del cliente puedan intercambiar su información.

El modelo *Peer-to-Peer* presenta el problema de que no tiene un aislamiento total en cuanto a las rutas de un cliente, ya que en el núcleo de su red, propiamente los enrutadores P, manejan todas las rutas obtenidas por un PE, además de que se deben de coordinar el espacio de direcciones que manejan distintos clientes.

MPLS/VPN provee una solución para la construcción de VPN's con las mejores características de los modelos *Overlay* y *Peer-to-Peer.*

Provee las ventajas del *switcheo* de capa 2 con el enrutamiento de capa 3. Soluciona los problemas de escalabilidad del modelo *Overlay* que tiene que proveer muchos circuitos virtuales entre los CE's y soluciona las carencias del modelo *Peer-to-Peer* como son: la falta de aislamiento entre clientes y la coordinación del espacio de direcciones entre clientes.

Tiene los beneficios del enrutamiento simple que implementa el modelo *Peer-to-Peer* además de facilitar la implementación de casi cualquier topología VPN[44].

También da una aproximación al modelo orientado a conexión, paradigma IP, por medio de las rutas conmutadas de etiquetas (LSP's, *Label Switched Path*) que son creadas en base a la topología en vez del tráfico. Permite que una infraestructura de red IP entregue servicios privados sobre una infraestructura pública.

4.4.2 Componentes de la arquitectura de MPLS/VPN

4.4.2.1 Tablas de envío y enrutamiento VPN

Cuando se tienen dos clientes que solicitan el servicio de VPN, ambos clientes podrían estar usando el mismo espacio de direcciones, si es que es privado. Si el SP quiere brindar el servicio con el modelo *Peer-to-Peer*, nos encontramos con que no sería fácil porque las direcciones de los sitios que se conectarían estarían traslapados (*overlapping*).

Como solución al problema del uso del mismo espacio de direcciones al implementar el modelo *Peer-to-Peer*, la arquitectura de MPLS/VPN lo soluciona de la siguiente forma: emplea una tabla de enrutamiento y envío (VRF, *VPN Routing and Forwarding*) por cada VPN configurada en cada enrutador, en el caso mas simple. Así, los clientes o sitios pertenecientes a dicha VPN tienen acceso a todas las rutas pertenecientes a dicha tabla.

[44] MPLS/VPN soporta sólo IP como protocolo de capa 3. Otros protocolos como IPX o AppleTalk deben aun ser *tuneleados* en la red IP.

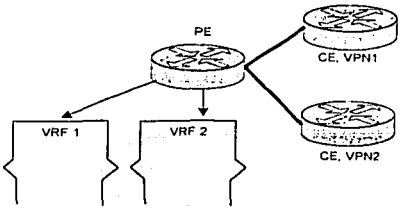


Figura 4.12 Solución al *Overlapping* con el modelo *Peer-to-Peer*

El único requisito es que el espacio de direcciones sea único dentro de la VPN, pudiendo ser público o privado. Mientras dos clientes VPN no se quieran comunicar, pueden emplear el mismo espacio de direcciones.

4.4.2.2 Enrutadores virtuales

Para poder sostener la idea de que por cada VPN manejar una tabla de envío y enrutamiento con direcciones públicas o privadas se introduce el concepto de enrutadores virtuales, de los cuales se crean tantos como VPN's estén configuradas en un PE.

En estos enrutadores virtuales existen también interfases asociadas a las tablas de envío, reglas para importar y exportar rutas dentro de las tablas VPN, protocolos de enrutamiento que recolectan información para llenar las tablas VPN, etc.

El componente, dentro de la arquitectura MPLS/VPN, que almacenará las rutas VPN se conoce como una instancia de envío y enrutamiento VPN, llamada VRF y se compone de una tabla de enrutamiento y una tabla de envío IP VPN.

En general, se tienen además de las VRF's una tabla global para enviar tráfico que no es VPN o para enrutar las rutas externas a la VPN.

Cuando no hay conectividad entre clientes VPN, se tiene asociada a una VPN solo una tabla VRF, pero en casos donde si hay conectividad, existe más de una VRF por VPN. Para poder manejar un nivel de conectividad mayor es necesario definir un nuevo concepto, conocido como sitio.

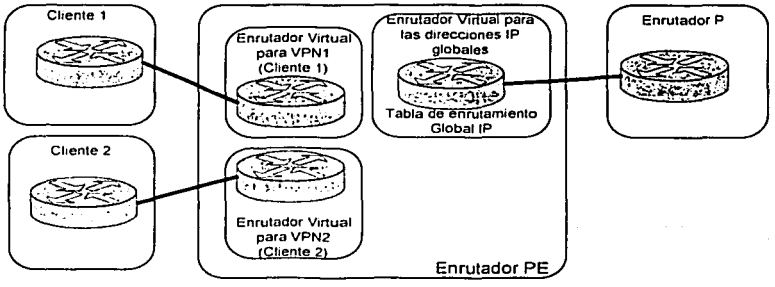


Figura 4.13 Enrutador Virtual

4.4.2.3 Traslape de VPNs

En la arquitectura MPLS/VPN se introduce el concepto de sitio, para denominar parte de una organización y en base a esto se define una red privada virtual. Una VPN es el conjunto de sitios que comparten información de enrutamiento que es común a ellos. Con este panorama puede ser más compleja la arquitectura, ya que un sitio puede pertenecer a una o más redes VPN.

Con esta panorámica ya no es una VRF por VPN sino una VRF por cada sitio ya que en las VRF's deben existir las rutas disponibles para dicho sitio y no para otros sitios que pertenezcan a la misma VPN. Esto lleva a establecer que en una VRF puedan existir rutas de diferentes VPN's. Entonces, dentro de la arquitectura de MPLS/VPN, una tabla VRF contiene una colección de rutas que deben estar disponibles para un sitio en particular conectadas a un enrutador PE, siendo que estas rutas puedan pertenecer a más de una VPN.

La regla que permite definir el uso de las VRF's es:

Todos los sitios que compartan la misma información de enrutamiento (o sea que pertenecen al mismo bloque de VPN's) y que esta permitido que se comuniquen directamente entre ellos, y que están conectados al mismo PE, pueden ser colocados en la misma VRF[45].

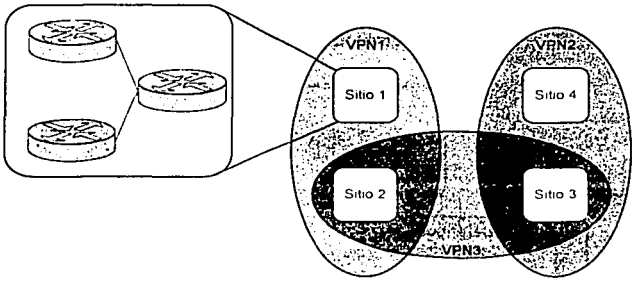


Figura 4.14 Traslape de VPNs y Sitios

Los sitios 2 y 3 en un inicio forman parte de las VPN's 1 y 2 respectivamente pero al entablar comunicación se tiene que formar lógicamente otra VPN para que pueda crearse una tabla VRF que sea la que contenga la información de enrutamiento de esta nueva VPN, la cual solo le corresponde a ambos sitios y no a los sitios 1 y 4.

4.4.2.4 Route Target

Con estas condiciones, una tabla VRF puede contener rutas de múltiples VPN's siendo necesario identificarlas. Para poder identificarlas al momento de exportarlas o importarlas se utiliza el *route target* (RT).

El RT se agrega a las rutas VPN cuando estas son exportadas, para ser importadas, por una VRF. Funciona como un identificador de VPN o VRF y sirve para poder marcar las rutas VPN

[45] Conviene mantener el número de VRFs al mínimo. Se recomienda una VRF para el sitio central y otra VRF para todos los sitios remotos conectados al mismo PE.

con el fin de saber en que tabla VRF debe de ser insertada la ruta VPN. Si no se tiene este identificador, cuando una ruta de una determinada VPN sea recibida por un enrutador PE, éste no sabrá cual tabla VRF, si es que tiene configuradas varias, contiene las rutas de dicha VPN.

Ahora, se puede asociar un bloque de RT's a una determinada VRF. Si una ruta contiene al menos uno de estos RT, entonces dicha ruta será introducida a dicha VRF.

Este identificador es de 64 bits de tamaño.

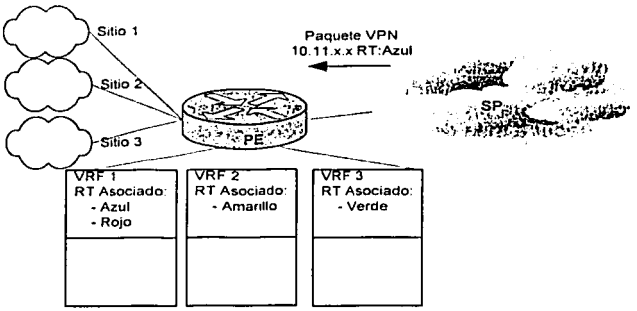
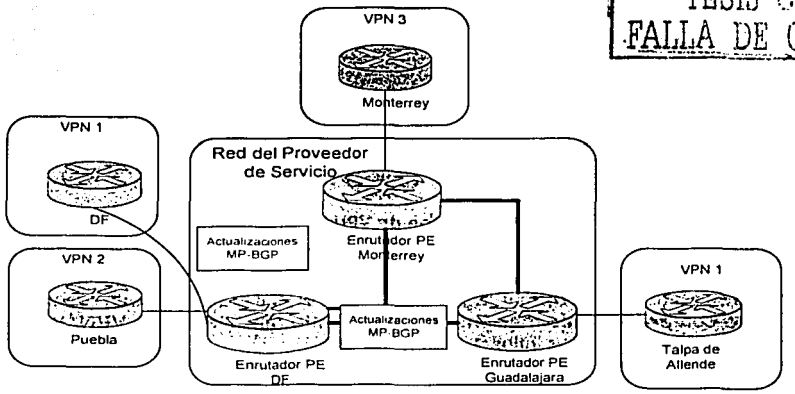


Figura 4.15 Empleo del *Route Target*



Enrutador PE del DF:

Genera actualizaciones MP-BGP
De: VPN 1 DF
RT: 100:26

De: VPN 2 Puebla
RT: 100:27

Enrutador PE de Guadalajara:

Configurado para importar rutas con:
RT: 100:26
De: VPN 1 DF

RT: 100:27
De: VPN 2 Puebla

Enrutador PE de Monterrey:

Configurado para importar rutas con:
RT: 100:27
De: VPN 2 Puebla

Figura 4.16 Uso del RT

En la figura anterior podemos ver que el sitio de Talpa de Allende, perteneciente a la VPN 1, puede comunicarse con el sitio del DF perteneciente a su misma VPN, además del sitio de

Puebla perteneciente a la VPN 2, por medio de la importación de las rutas de dichos sitios, a través del RT, a su tabla VRF.

El sitio de Monterrey perteneciente a otra VPN, la 3, puede conectarse solo al sitio de Puebla perteneciente a la VPN 2 y no al sitio del DF perteneciente a la VPN 1. Lo logra importando solo las rutas que tienen el RT que identifica las rutas de la VPN 2 y omite aquellas que tienen como RT el que identifica a las rutas de la VPN 1.

4.4.2.5 Route Distinguisher

Para poder mantener la información de las VPNs como única dentro de un mismo equipo es necesario anexar a las direcciones IP un identificador único a fin de que los clientes VPN puedan emplear el mismo espacio de direcciones sin que se traslapen las direcciones en la dorsal MPLS/VPN. A dicho identificador se le denomina *Route Distinguisher* (RD) y se acostumbra usar uno para cada cliente VPN.

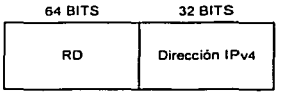


Figura 4.17 *Address Family* VPN-IPv4 o VPNv4

El RD tiene un tamaño de 64 bits y se agrega a la dirección IP tradicional para formar lo que sería direcciones de 96 bits conocidas como direcciones VPNIPv4 o VPNv4. El propósito de emplear este RD es diferenciar las direcciones que tengan un prefijo idéntico pero que pertenezcan a distintos clientes VPN. Esto es de vital importancia, porque como se explicará, se empleará BGP para realizar el transporte de las rutas y este protocolo solo transporta la mejor ruta y si se encuentra dos rutas con el mismo prefijo, aunque pertenecientes a distintos clientes VPN, BGP eliminará la propagación de una de ellas dejando incomunicado uno de los sitios.

Se emplea BGP para transportar la información VPN debido a su facilidad para manejar muchas rutas además de poder transportar información adicional que le corresponde a las rutas. Como BGP en su estado normal solo maneja direcciones IPv4, es necesario habilitar a BGP para que transporte las direcciones VPNIPv4, es decir, las direcciones IPv4 con el RD adjuntado, a fin de mantener únicas las direcciones IP a través de la dorsal MPLS/VPN.

También se emplean las extensiones de BGP para poder acarrear el RT como un atributo de la ruta y así poder distinguir a que VRF pertenece una ruta VPN. MP-BGP es el protocolo que se maneja para poder hacer uso de las extensiones de BGP además de poder manejar información de más de un protocolo de enrutamiento, ya que el SP puede comunicarse con varios clientes VPN que manejen distintos protocolos de enrutamiento. Por ello es necesario habilitar sesiones MP-BGP a través de la dorsal MPLS/VPN.

En general, el RD se emplea para establecer diferencias entre las direcciones IP. Habilita el uso de los mismos prefijos de dirección IP para distintas VPNs.

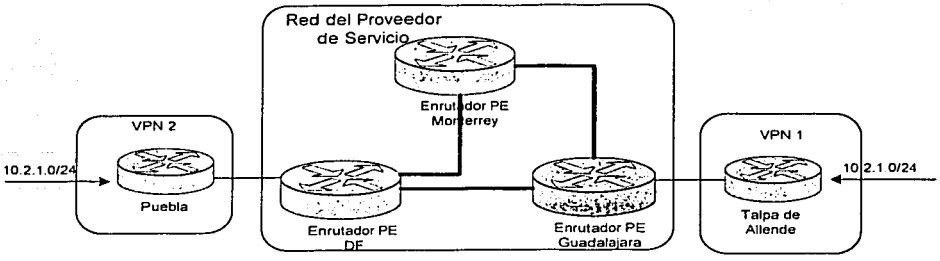


Figura 4.18 Selección de la mejor ruta sin el *Route Distinguisher*

En la figura anterior se ilustra como sin el RD, se puede dejar incomunicado a un sitio, ya que BGP selecciona solo la mejor ruta y las demás las desecha. Así, si elige la actualización proveniente del sitio de Puebla, el sitio de Talpa de Allende se quedará incomunicado y viceversa.

El RD soluciona esto, formando las direcciones VPNv4, logrando hacer únicas las direcciones en la red MPLS/VPN, aun si tienen el mismo prefijo de dirección. El panorama sería el siguiente.

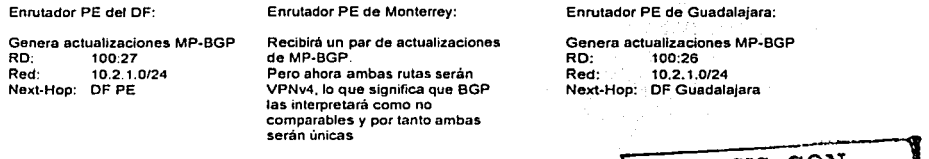


Figura 4.19 Uso del RD

4.4.3 Modelo de conexión MPLS/VPN

Para configurar la dorsal de un SP a fin de que pueda brindar servicios de VPN a través de tecnología MPLS, primeramente se deben de visualizar los elementos técnicos que componen dicho servicio.

- Los enrutadores P, que serían los LSRs, forman el núcleo de la dorsal.
- Los enrutadores PE, que serían los LERs, se comunican con los enrutadores P a través de MPLS y con los enrutadores del cliente emplean IP.
- Los enrutadores P y PE deben compartir un protocolo de enrutamiento IGP, además de un protocolo de distribución de etiquetas, que puede ser LDP o incluso BGP.
- Los enrutadores PE manejan una topología de malla completa a través de sesiones MP-iBGP a fin de intercambiar información de enrutamiento de distintos protocolos.

- Los enrutadores CE, conectados directamente a la red del SP por medio de los PE, ejecutarían un protocolo de enrutamiento a fin de dar la información necesaria a los PE.

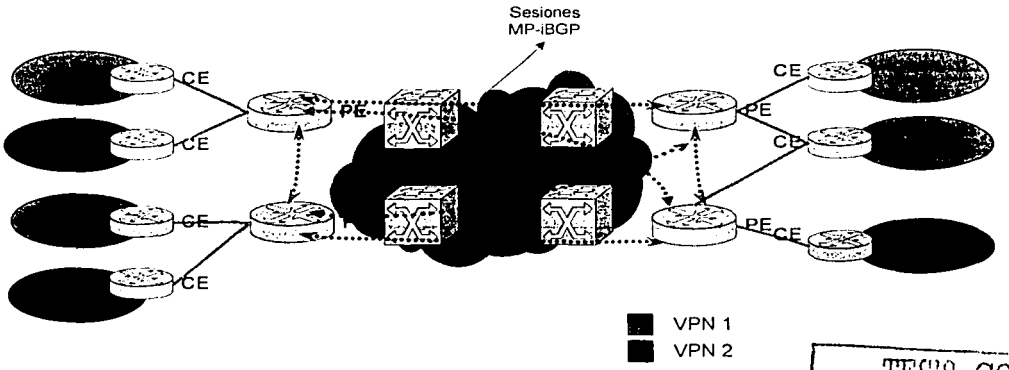


Figura 4.20 Modelo de conexión MPLS/VPN

4.4.3.1 Propagación de la información de enrutamiento VPN

El proceso de transportar las rutas VPN puede ser analizado en dos partes:

- La información que tiene que ser intercambiada entre PE's.
- La información originada en el cliente VPN que tiene que ser enviada al PE.

Intercambio de información de enrutamiento entre PEs

Para el intercambio de información de enrutamiento entre PE's existen dos casos:

- Que se ejecute un protocolo de enrutamiento por cada VPN. Esta alternativa acarrea problemas de escalabilidad cuando existe un gran número de VPN's.
- Que se ejecute un solo protocolo de enrutamiento que sea capaz de transportar todas las rutas VPN.

La tecnología MPLS/VPN emplea esta segunda opción. El protocolo de enrutamiento que se concibió para que realizara esta tarea fue *MultiProtocol* BGP, que es una extensión de BGP.

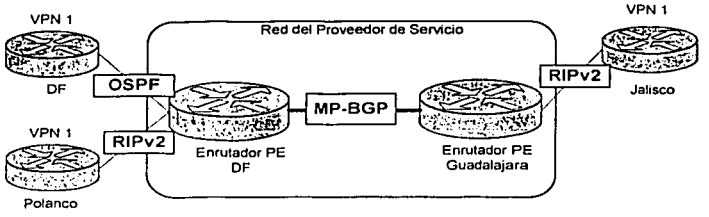
Este protocolo transporta las direcciones VPNv4 de un PE a otro. Algunas de las ventajas de este protocolo sobre otros, como IGRP o IS-IS, son las siguientes:

- Es capaz de soportar millones de rutas en sus tablas de enrutamiento.
- Está diseñado para ser multiprotocolo, es decir, soportar el transporte de familias de direcciones (*address-family*) diferentes.
- Puede intercambiar información entre PE's que no están directamente conectados entre sí.

- Puede transportar información adicional correspondiente a las rutas VPN y mantener dicha información incluso fuera de la dorsal (fuera de los enrutadores P) empleando los atributos de BGP[46].

La información adicional que puede transportar BGP le hace sumamente útil al emplearlo en la arquitectura de MPLS/VPN. Esta es una de las ventajas importantísimas del uso de MP-BGP para transportar las rutas VPN ya que permite transportar el RT como un atributo más.

La información que transporta MP-BGP no incumbe mucho a los enrutadores P, ya que con la arquitectura de MPLS/VPN, la información se transporta atendiendo al *switcheo* de etiquetas que son colocadas antes del paquete IP VPN.



Enrutador PE DF

La información de enrutamiento se recolecta de los sitios VPN a través de los protocolos de enrutamiento que se ejecutan por cada VRF configurada (contexto de enrutamiento)

Sesiones MP-BGP

La información de enrutamiento de las VRFs es distribuida en MP-BGP y enviada a través del núcleo de la red.

Enrutador PE Guadalajara

La información de enrutamiento se recibe por medio de MP-BGP. Dependiendo de las reglas de importación y exportación, las rutas se insertan en las VRFs y opcionalmente son enviadas a los CEs.

Figura 4.21 MP-BGP como protocolo de transporte de múltiples protocolos de enrutamiento

Intercambio de información de enrutamiento entre los CE's y los PE's

Los PE's recolectan información de los sitios de los clientes por medio de los protocolos de enrutamiento que están ejecutándose en las interfaces conectadas a los clientes. Así, el enrutador PE puede recolectar información de OSPF, RIP o también algunas rutas estáticas del cliente. Es aquí donde interviene MP-BGP para transportar esta información recolectada.

Todas las rutas recolectadas serán distribuidas a MP-BGP, independientemente del protocolo de enrutamiento del cual fueron aprendidas. Antes de ser redistribuidas se les agrega a las rutas el RD así como el RT originado en la correspondiente tabla VRF.

Al llegar al otro PE, se insertarán las rutas en las tablas VRF de acuerdo al RT adjuntado y el RD se desechará, quedando la dirección IP tradicional de 32 bits. MP-BGP redistribuirá las rutas a los procesos (protocolos de enrutamiento) que se estén ejecutando en las interfaces del PE. Cuando uno de estos procesos es BGP la redistribución es automática, en caso de que no sea BGP se tiene que configurar manualmente.

Ahora el contexto de enrutamiento es muy importante ya que limita a cada protocolo de enrutamiento para llenar de información solo una tabla VRF. Para lograr esto, el PE se configura para que la información obtenida de una interfase sea asociada a una tabla VRF en particular. Esto

[46] *Las Comunidades Extendidas de BGP*

evita el traslape de direcciones en el caso de que dos VPN's empleen las mismas direcciones y que en cada una de ellas se este ejecutando el mismo protocolo de enrutamiento.

Envió de paquetes VPN (En los enrutadores Ps)

El transporte de paquetes VPN en la red de enrutadores del proveedor de servicio, enrutadores P, se realiza empleando netamente la tecnología MPLS.

Los enrutadores PE almacenan[47] dos tipos de etiquetas:

- Las etiquetas asociadas a los enrutadores de la dorsal, o a las rutas asociadas a las rutas IGP, y que son transportadas por LDP.

Las rutas IGP, así como las etiquetas asociadas a estas rutas son almacenadas en las tablas globales.

- Las etiquetas asociadas a las rutas VPNs y que son transportadas por MP-BGP.

Las rutas VPN así como las etiquetas asociadas a estas rutas son almacenadas en las tablas VRFs.

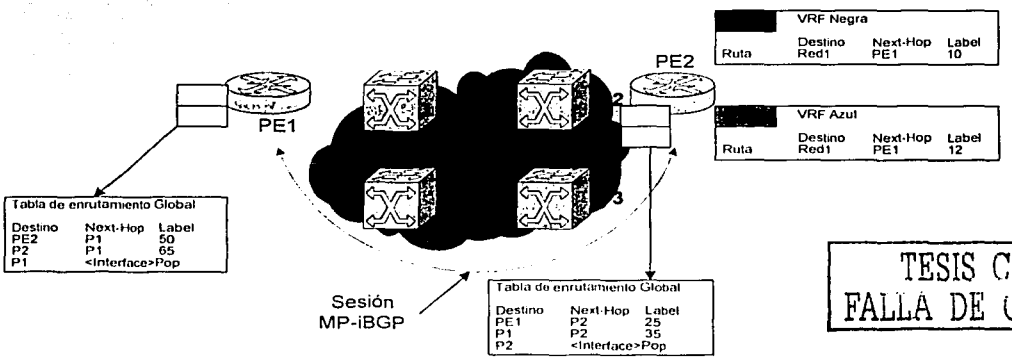


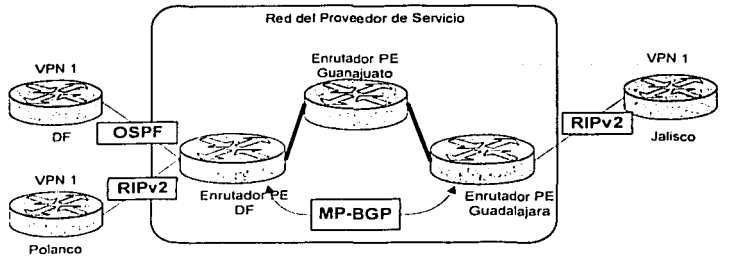
Figura 4.22 Comunicación entre PEs

Se utilizan 2 niveles de etiquetas, empleando el apilado de etiquetas (*label stack*) de MPLS. En el PE de ingreso (LER de ingreso) todos los paquetes VPN son identificados con una etiqueta que identifica al enrutador PE de egreso (LER de egreso, *Label Edge Router*) con el fin de enviar todos los paquetes a ese destino.

Para que el LER de ingreso pueda asignar etiquetas hacia el enrutador de egreso, es necesario utilizar una característica que se pueda asociar a una etiqueta. En principio el LER de egreso envía su propio identificador que es su dirección de *host* (usualmente la dirección de *loopback*) hacia la red, por medio de un IGP. El enrutador P inmediato asocia una etiqueta a esta dirección y la transmite hasta el LER de ingreso. Para la distribución de estas etiquetas se emplean los procesos de distribución de MPLS, como puede ser LDP y BGP. De esta manera el LER de

[47] Se almacenan en las tablas LFIB

ingreso, al igual que los enrutadores P, sabe que etiqueta asignar a los paquetes VPN que recibe para que puedan ser enviados hasta el LER de egreso.



Enrutador PE DF (Egreso)

Cada PE usa un identificador único, como la dirección de host (usualmente la dirección IP de *loopback*), la cual es anunciada por un IGP.

Todas las rutas anunciadas por dicho PE, tendrán como valor del atributo Next-Hop de BGP la dirección IP de *loopback* del PE de egreso

Enrutadores P

Cada enrutador P asigna una etiqueta a la dirección de *loopback* del enrutador PE de egreso y la propaga a sus vecinos.

Las etiquetas son distribuidas a través de LDP. Las rutas son distribuidas a través del IGP.

Enrutador PE Guadalajara (Ingreso)

El enrutador de ingreso (y todos los demás PEs) reciben la etiqueta asociada con la dirección de *loopback* del enrutador PE de egreso.

Con esto, la dorsal esta habilitada para transportar los paquetes VPN con MPLS.

Figura 4.23 Etiqueta de nivel 1

La segunda etiqueta que se emplea le dice al LER de egreso hacia que VPN tiene que dirigir los paquetes VPN que recibe. Esta etiqueta es asignada a cada ruta dentro de las tablas VRF's en cada PE y son propagadas empleando MP-BGP, siendo únicas a cada ruta. Ahora todos los PE's receptores las insertarán en sus tablas VRF, las rutas con sus respectivas etiquetas.

Una vez definido el objetivo de ambas etiquetas, la operación es simple. Cuando un paquete VPN llega al PE de ingreso, este revisa sus tablas VRF y asigna la etiqueta correspondiente a la dirección destino del PE de egreso. Después de la tabla global de envió se toma una segunda etiqueta que es la que apunta hacia el PE de egreso. Los *switches* PE transportaran el paquete empleando como única información la etiqueta más alta en el apilado, la última, para llegar al PE de egreso sin revisar la información que exista debajo de ella.

Al llegar al PE de egreso, este desechará la última etiqueta y realizará solo una revisión sobre la segunda etiqueta, la cual le dará información sobre la tabla VRF en la cual debe insertar la ruta e incluso la interfase de salida. Con esto, el PE revisara la tabla VRF y decidirá hacia que enrutador CE debe ir dirigido el paquete.

Este último proceso se puede optimizar, eliminando la tarea de quitar la última etiqueta al último PE. Se puede hacer que el penúltimo PE elimine la última etiqueta, permitiendo que el último PE sólo realice una revisión sobre la primera etiqueta.

4.5 Operación de la arquitectura de MPLS/VPN

Una vez explicados los conceptos de la arquitectura de MPLS/VPN se procede a realizar una implementación, para ejemplificar, suponiendo una topología VPN *Intranet* integrada por sitios que pertenecen a la misma organización. La estructura provee una conectividad total entre los sitios que conforman la *Intranet*. En este modelo, se integraran dos clientes con sitios geográficamente separados.

Para ejemplificar la operación de la arquitectura de MPLS/VPN emplearemos el siguiente modelo de red.

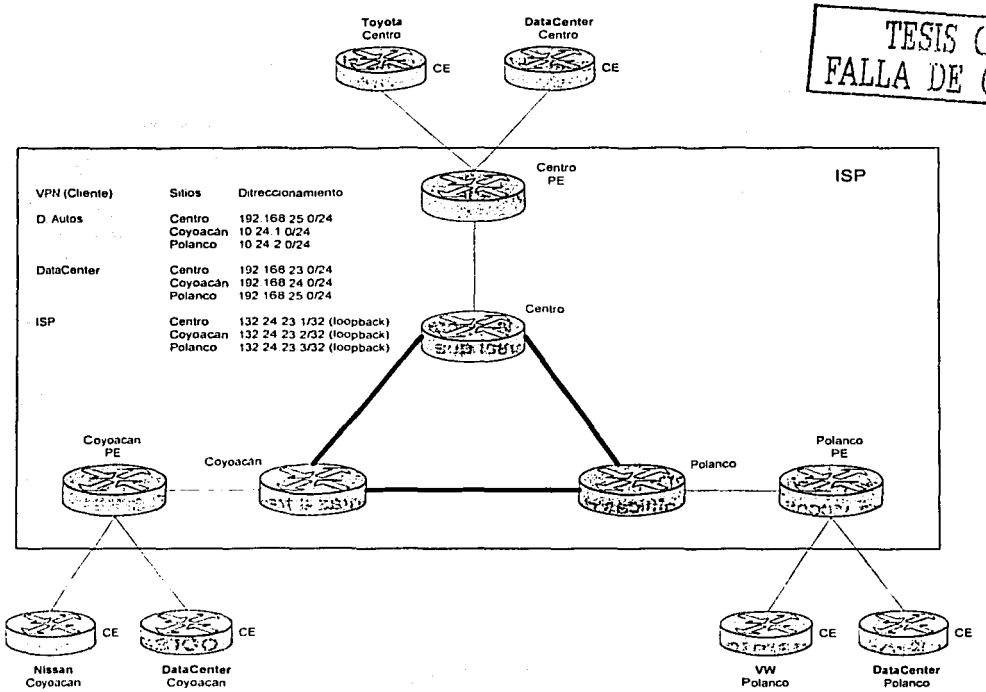


Figura 4.24 Modelo de red para proveer el servicio de VPN en una dorsal MPLS/VPN

4.5.1 Descripción

El modelo esta constituido por un ISP, cuya infraestructura consta de una serie de enrutadores que ejecutan MPLS. Esto habilita al SP brindar una serie de servicios, entre los cuales se encuentran las VPNs.

En este caso, brindará servicio a un par de empresas que requieren constituir, en forma independiente, una *Intranet* entre sus sitios que se encuentran geográficamente distribuidos y necesitan conectividad entre cualquiera de sus sitios, es decir una malla completa. Empleará el modelo *Peer-to-Peer* ya que la información de enrutamiento del cliente la conocerá el SP.

El SP consta de tres POPs ubicados en la zona Centro, Polanco y Coyoacán de la Ciudad de México. Esta parte constituye la parte de distribución. Además, el núcleo de la red o la dorsal, esta constituida por enrutadores que interconectan los POPs y permiten que la información pueda viajar de un lado a otro en la dorsal. El SP se comunicará con los clientes VPN a través de algunos protocolos de enrutamiento. Nos enfocaremos en IPv4 para los clientes conectados al PE Coyoacán y enrutamiento estático con los demás clientes.

El primer cliente VPN lo constituye una empresa que vende Autos y tiene 3 sitios que se conectan entre sí en una malla completa a través de la red compartida del proveedor de servicio. Tiene sitios en la zona Centro, Polanco y Coyoacán. Dichos sitios cuentan con un enrutador CE que se conecta a la red del SP, directamente al PE. En cuanto al direccionamiento de la empresa es privado.

El segundo cliente VPN es la empresa DataCenter que respalda información importante de distintas empresas e igualmente tiene 3 sitios que se comunican entre sí. Están ubicados en las zonas Centro, Polanco y Coyoacán. Se conectan a los PEs del SP a través de los enrutadores CEs ubicados en cada sitio. Su direccionamiento es privado.

Se nota que dos de los sitios, pertenecientes a distintos clientes, emplean el mismo direccionamiento. Como se menciono, a través del RD, se evita el problema de enlapamiento, por lo que los clientes podrán operar sin tener que modificar su direccionamiento.

Con este modelo de red, se mostrará la operación de los conceptos de la arquitectura MPLS/VPN a fin de dar servicios VPN en una dorsal que ya ejecuta MPLS.

Los pasos a seguir para dar el servicio de VPN en una dorsal con MPLS, descritos enseguida son:

- Definir y configurar las VRFs.
- Definir y configurar los RD
- Definir y configurar las políticas de importar y exportar rutas a través del RT.
- Configurar los enlaces PE-CE
- Asociar las interfaces de los CE a las VRF previamente definidas
- Configurar el dominio MP-BGP.

4.5.2 Provisionamiento del servicio de VPNs sobre una dorsal habilitada con MPLS

4.5.2.1 Definición y configuración de las VRF's

El primer paso para proveer un servicio de una VPN sobre una infraestructura de MPLS es configurar las instancias de enrutamiento y envió virtuales o las VRF's.

Como todos los sitios tienen presencia en los tres POPs del SP, todos los enrutadores PE deben tener configuradas las VRFs. El comando que se emplea para configurar una VRF en un PE es:

```
Coyoacán(config)# ip vrf Autos
```

Al introducir el comando IP VRF entramos al submodo de configuración de la VRF y se crean las tablas de enrutamiento CEF y la VRF[48].

Después de ello se procede a configurar la VRF que básicamente serían algunos parámetros como son el *Route Distinguisher* (RD), para hacer única la información de la VPN en el dominio MPLS/VPN y las políticas de exportación e importación de rutas a través del RT.

4.5.2.2 Definición y configuración del RD

La importancia del RD es mucha. Sabemos que en la arquitectura MPLS/VPN no se restringe el uso del espacio de direcciones privadas o públicas y que estas deben ser únicas en la dorsal para que MP-BGP pueda interpretarlas como no comparables[49]. Esto último se debe a que MP-iBGP selecciona la mejor ruta hacia un destino. Si dos clientes están empleando el mismo espacio de direcciones y se anuncian como 2 actualizaciones hacia un PE que esta configurado con MP-iBGP, este eliminará una de las rutas, dejando sin comunicación el sitio que anunció una ruta duplicada. Por la naturaleza del proceso de decisión de BGP es necesario proveer un mecanismo externo, ajeno a MP-iBGP, que permita distinguir dos rutas pertenecientes a diferentes clientes VPN con el mismo prefijo de dirección.

Por ello la existencia del RD. El RD se adjunta enfrente de la dirección IPv4 y es único por cada VPN o un bloque de sitios dentro de una VPN. De esta manera direcciones IP con el mismo prefijo que pertenezcan a diferentes clientes VPN serán consideradas por MP-BGP como no comparables.

Este mecanismo no soluciona el problema que implica que varios clientes dentro de una VPN compartan el espacio de direcciones, es decir que dos clientes VPN se quieran comunicar. Para ello se tendría que desarrollar NAT u otra tecnología.

Se recomienda emplear un RD por VPN cuando los sitios que pertenecen a dicha VPN solo pertenecen a una VPN. Si un sitio llega a formar parte de otra VPN, será difícil determinar el RD a emplear para dicho sitio. Para evitar este tipo de problemas, en ocasiones se utiliza un RD por VRF.

El RD tiene 2 formatos. En uno se emplea el número de sistema autónomo más un número asignado por el ISP.

Figura 4.25 Formato de RD

En el segundo formato se emplea la dirección IP más un número asignado por el ISP.

[48] Es necesario habilitar la CEF, ya que es un requisito de MPLS.
[49] En el proceso de selección de BGP, las rutas con distinto prefijo no se someten al mismo proceso de selección. Para MP-BGP, las rutas con igual prefijo, pero con distinto RD, no se someten al proceso de selección.

Figura 4.26 Formato de RD

Se recomienda la primera ya que los números de sistema autónomo son asignados por la IANA[50] y son únicos. Cuando se emplea un número de SA[51] privado se suele emplear el segundo formato.

Se utiliza el número de sistema autónomo como los dos primeros bytes del RD ya que si un sitio quiere formar parte de otra infraestructura MPLS/VPN con otro proveedor de servicios, el RD se mantendría único. La otra parte la asigna el SP. Este parámetro es asignado en el submodo de configuración de la VRF.

```
Coyoacán(config-vrf)# rd 100:26
```

4.5.2.3 Definición y configuración de las políticas de importación y exportación de rutas a través del RT

Ahora es necesario establecer un mecanismo que permita determinar en que tablas deben ser colocadas las rutas que se propagan por la dorsal de MPLS/VPN a través de MP-BGP. Este mecanismo se basa en un parámetro que se adjunta a la ruta y que indica al PE en que VRF se debe importar una ruta VPN.

El *Route Target* (RT) es el parámetro que nos permitirá desarrollar políticas de importación y exportación de rutas VPN en las VRF's. Como el RT es un parámetro que debe ir adjuntado a la ruta, se definieron dos nuevas comunidades para BGP, llamadas comunidades extendidas[52]. Una de estas comunidades nos permite transportar este parámetro como información adicional a la ruta a lo largo de las sesiones MP-BGP entre los PE's. La forma en que el RT es adjuntado a la ruta es igual que con los atributos estándar que BGP transporta.

Así, las políticas de importación y exportación se definen acorde al valor de esta comunidad permitiendo a una VRF contener rutas de las VPN's que se especifique[53].

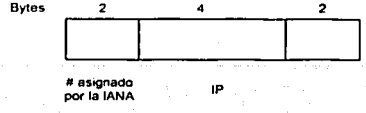
---

[50] *Internet Assigned Numers Authority.*

[51] Sistema Autónomo. Bloque de enrutadores que comparten políticas de enrutamiento.

[52] **Formato del atributo comunidad extendida de BGP**
Cada comunidad extendida tiene un valor hexadecimal que la identifica y es de 8 bytes. Los primeros 2 bytes indican el tipo de atributo y los 6 restantes el valor del atributo.

La comunidad extendida RT se identifica con el tipo 0x0002 o 0x0102 y el SOO es del tipo 0x0003 o 0x0103. La estructura del campo valor depende del bit más significativo del campo tipo. Así si el campo tipo empieza con el valor 0x01, la estructura del campo valor sería:



Formato de una comunidad extendida de BGP

[53] Un sitio puede contener rutas que otro sitio de la misma VPN no tiene, a través del uso del RT.

Generalmente se configura en un enrutador PE ambas políticas, importación y exportación del mismo RT para poder publicar las rutas del sitio y al mismo tiempo para poder recibir las rutas de otro sitio que pertenece a la misma VPN.

Así, para el ejemplo tratado definimos los siguientes RD.

Cliente VPN	Número de Sistema Autónomo	Valor único	RD
Autos	100	26	100:26
DataCenter	100	27	100:27

Tabla 4.1 Asignación de RD

En el caso del cliente Autos la configuración del RT sería:

```
Coyoacán(config-vrf)# route-target export 100:26
Coyoacán(config-vrf)# route-target import 100:26
ó
Coyoacán(config-vrf)# route-target both 100:26
```

Ambos comandos son introducidos en el submodo de configuración de la vrf.

La otra comunidad extendida definida es el Sitio de Origen (SOO, *Site of Origin*) que permite prevenir *loops* y solo aplica cuando un sitio es *multihomed*[54] hacia la dorsal MPLS/VPN. Si la dorsal recibe una actualización del sitio, se identifica de donde se aprendió para que no sea readvertida la misma actualización al sitio que la generó. Esta comunidad se configura a través de la sentencia *route-map*.

4.5.2.4 Configuración de los enlaces PE's a CE's

Antes de describir el proceso de configuración conviene describir algunos conceptos asociados al proceso de recolección de información por parte de los PEs, información que será aprendida de los CEs para ser almacenada en las tablas VRF, ó tablas globales, de los enrutadores virtuales.

Un requisito en la arquitectura MPLS/VPN es el aislamiento de la información VPN. Para ello se definen los contextos de enrutamiento. Se mantienen logrando que las rutas aprendidas por una interfaz se asocien a una VRF. Cada VRF tiene asociado un contexto de enrutamiento o proceso de algún protocolo de enrutamiento, el cual es asociado a una interfaz en específico y dicha interfaz está asociada a la VRF. Cualquier ruta aprendida a través de dicha interfaz será colocada en la VRF. Cualquier otra ruta aprendida por la misma interfaz que no sea parte del mismo contexto de enrutamiento (o proceso del protocolo de enrutamiento), será colocada en una tabla de enrutamiento global. Esto permite la separación de la información de enrutamiento en diferentes contextos, aun si la información es aprendida del mismo proceso del protocolo de enrutamiento o de una instancia de un protocolo de enrutamiento. Por ejemplo, la dorsal puede tener sesiones BGP habilitadas para transportar rutas IPv4 y también puede tener sesiones BGP habilitadas para transportar rutas VPNv4. Así, estaríamos definiendo dos contextos distintos.

[54] Son sitios que tienen más de un punto de acceso a la dorsal del SP.

4.5.2.4.1 Enrutamiento estático

Dicho lo anterior, analizaremos el caso del los clientes que no ejecutan ningún protocolo de enrutamiento para comunicarse con el SP. Emplean el enrutamiento estático, que es el proceso más simple para establecer un enlace entre un PE y un CE. Se recomienda para sitios *stub*[55]. Simplemente se configura la dirección del CE en la VRF en forma estática, bajo ningún proceso y también se deben colocar las rutas de las redes que se encuentran detrás de los CE's en las VRF's si es que otros miembros de las VPN's desean alcanzarlas.

La información de enrutamiento estática será redistribuida posteriormente a BGP para que pueda ser propagada en las sesiones MP-BGP.

En el modelo de red expuesto, los sitios conectados al PE Polanco emplean enrutamiento estático. Para configurar las rutas estáticas en las VRF's correspondientes se emplea el siguiente comando:

```
Polanco(config)# ip route vrf <nombre de la VRF> <IP> <máscara de red> <interface>
Polanco(config)# ip route vrf Autos 10.24.2.0 255.255.255.0 serial0
Polanco(config)# ip route vrf DataCenter 192.168.25.0 255.255.255.0 serial0
```

Después, como se menciono, se procede a publicar estas rutas empleado las sesiones MP-BGP. Para lograrlo se redistribuyen las rutas en el proceso BGP a través del comando *redistribute* dentro del *address-family* correspondiente.

El *address-family* define un contexto de tipos de rutas. Así, las rutas almacenadas en la VRF Autos deben ser distribuidas al proceso de BGP para su posterior publicación en las sesiones MP-BGP. Por cada VRF configurada en el PE, se debe especificar un *address-family* que indique la redistribución de rutas a BGP. Esto se define dentro del proceso BGP a fin de que sean las sesiones MP-BGP las encargadas de transportar dichas rutas.

```
Polanco(config)# router bgp 100

Polanco(config-router)# address-family ipv4 vrf Autos
Polanco(config-router)# redistribute static
Polanco(config-router)# exit address-family
```

El comando ***redistribute static*** indica que las rutas estáticas serán advertidas a los otros PEs mediante las sesiones BGP que, posteriormente, serán activadas entre los PEs. Este comando se ejecuta solo para las rutas asociadas a la VRF Autos configuradas estáticamente y se coloca dentro del proceso estándar de BGP.

Lo que faltaría sería, bajo el contexto del *address-family* de las rutas VPNv4 dentro del proceso estándar de BGP, habilitar las sesiones MP-BGP entre los PEs.

4.5.2.4.2 RIPv2

Cuando se tiene habilitado RIPv2 como proceso corriendo en un enlace PE-CE igualmente se tiene que asociar cada proceso a cada VRF por una determinada interfase para mantener el contexto de enrutamiento.

[55] Sitios que solo poseen un punto de entrada hacia la dorsal de SP.

Cuando se ejecuta RIP es necesario indicarle que rutas advertir y sobre que interfaces, es decir, indicar las interfaces que están habilitadas para ejecutar RIP. Mediante el comando ***network***, dentro de la configuración del proceso RIP, se definen todas las rutas[56] que serán advertidas empleando todas las interfaces habilitadas con RIP.

Como ya se mencionó, un requisito de la arquitectura MPLS/VPN es mantener los contextos de enrutamiento. Por ello, el comando ***network*** se emplea dentro del *address-family* asociado a la VRF que nos interesa, dentro del proceso RIP. Como el *address-family* esta asociado a una VRF, entonces de esta manera se limita la publicación de las rutas para cada VRF, de acuerdo al contexto que les corresponde.

Con esto las rutas que pertenezcan a la VRF serán advertidas por RIP solo por las interfaces asociadas al *address-family* y en consecuencia a la VRF. Todas las demás rutas, ya sea que estén en la tabla de enrutamiento global o en otra VRF no serán advertidas, aunque estén dentro del rango que especifique el comando ***network***.

```
hostname Coyoacán
!
interface serial 0
        description ** Interface dirigida al CE Coyoacán del cliente Autos**
        ip address 10.24.1.5 255.255.255.252
!
interace serial 1
        description ** Interface dirigida al CE Coyoacán del cliente DataCenter**
        ip address 192.168.24.5 255.255.255.252
!
router rip
        version 2
address-family ipv4 vrf Autos
        versión 2
        redistribute bgp 100 metric 1
        network 10.24.1.0
        no auto-summary
exit-address-family
!
address-family ipv4 vrf DataCenter
        version 2
        redistribute bgp 100 metric 1
        network 192.168.24.0
        no auto-summary
exit-address-family
!
router bgp 100
address-family ipv4 vrf Autos
        redistribute rip metric 1
        no auto-summary
        no synchronization
exit-address-family
```

Se ve que en el proceso de bgp, dentro del *address-family* asociado a la VRF de Autos, las rutas almacenadas en esta tabla y aprendidas por RIPv2 serán distribuidas al proceso de BGP.

[56] Rutas dentro de la tabla de enrutamiento además de aquellas interfaces que están conectadas directamente.

Ahora, para definir el proceso que indica como son tratadas las rutas VPN que son aprendidas de las sesiones MP-BGP analizamos el ejemplo anterior.

Dentro del proceso estándar de RIPv2 se debe indicar, bajo el *address-family* correspondiente, la redistribución de las rutas VPNv4 aprendidas de las sesiones MP-BGP hacia los enrutadores CE, mediante el comando ***redistribute.***

4.5.2.5 Asociación de las interfaces a las VRFs

Una vez establecidos los procesos de enrutamiento y las tablas VRF se procede a asociar las interfaces a las VRF's. Esto se logra dentro de la configuración de la interfase con el comando siguiente:

```
Hostname Coyoacán
!
interface serial 0
        description ** Interface dirigida al CE Coyoacán del cliente Autos **
        ip vrf forwarding Autos
        ip address 10.24.1.5 255.255.255.252
```

4.5.2.6 Definición de MP-iBGP

Una vez configurado el PE para que recopile la información de rutas de los clientes, es necesario configurarlo para que se propaguen las rutas a través de la dorsal MPLS/VPN. Para ello se tienen que configurar sesiones de BGP entre los PE's.

MP-BGP es necesario porque las rutas VPNv4 llevan información adicional, además de la dirección IPv4. Por ello la necesidad de extender los atributos que puede transportar BGP mediante MP-BGP. Ahora decimos que son sesiones MP-iBGP porque las sesiones BGP se establecen entre enrutadores pertenecientes al mismo sistema autónomo.

He aquí una tabla de las características de MP-BGP.

MP-iBGP	Características
	Transporta: • Direcciones VPNv4 • Comunidades Extendidas BGP • Información de etiquetas MPLS • Posiblemente atributos estándar de BGP
	Solo se requiere entre los PEs
	Son sesiones BGP internas, ya que los PE's pertenecen al mismo sistema autónomo
	Es necesario ya que las actualizaciones BGP transportarán información adicional además de las direcciones IPv4
	Es una extensión de BGP-4 y transporta rutas que fueron aprendidas de los CE´s por medio de procesos de enrutamiento como RIPv2, BGP-4, OSPF o rutas estáticas configuradas en los PE´s.

Tabla 4.2 Características de MP-BGP

Para establecer MP-iBGP es necesario establecer las sesiones BGP entre los PE's involucrados. Las capacidades de BGP nos permiten indicar las extensiones necesarias para establecer MP-iBGP, además de configurar los contextos de enrutamiento para mantener separada la información de enrutamiento de diferentes clientes VPN.

Para establecer una sesión BGP primero deben ser intercambiadas las capacidades de cada uno de los PE's. Al iniciar una sesión BGP se manda un mensaje OPEN, por medio del cual se intercambian parámetros iniciales de BGP. Este mensaje contiene, entre otras cosas, información referente a:

- Número de Sistema Autónomo
- Parámetros
    - Capacidades
        - Extensiones
            - Multiprotocolo

Las capacidades indican las habilidades que un par o vecino, que habla BGP, puede entender y ejecutar. Cuando se emplean las extensiones multiprotocolo se introducen 2 nuevos atributos opcionales y no transitivos:

- Multiprotocol Reachable NLRI (MP_REACH_NLRI)
- Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI)

El primer atributo anuncia nuevas rutas multiprotocolo además de un bloque de destinos que se consideran alcanzables. El segundo las revoca y tiene un bloque de destinos inalcanzables.

Cuando un PE manda una actualización MP-iBGP, esta contiene información referente a MPLS/VPN y transporta el atributo MP_REACH_NLRI que transporta la siguiente información:

- **Información del *address-family* (AFI, *Address-family Information*)**. La AFI identifica el protocolo de capa de red que se lleva en la actualización. Para MPLS/VPN es de 1.

- **Información del próximo salto (*Next-hop*)**. Tiene la dirección del próximo enrutador camino al destino[57], siendo, para MPLS/VPN, el enrutador PE que anuncia la actualización.

- **NLRI (*Network Layer Reachability Information*)**. Para MPLS el NLRI esta formado por los siguientes tres campos[58]:

Figura 4.27 Formato del campo NLRI

- ✓ **Tamaño:** Indica el tamaño en bits de la etiqueta y el prefijo de dirección. 1 byte.
- ✓ **Etiqueta:** Este campo acarrea una o más etiquetas (corresponden al apilado de etiquetas útil para MPLS/VPN). Cada etiqueta, conocida también como

[57] La dirección del Próximo Salto debe ser del mismo tipo que el Prefijo de dirección incluido en el NLRI. Para que la dirección del Próximo Salto sea del tipo VPNv4, el valor de su RD debe ser cero.
[58] Pudiendo ser más bloques con estos mismos tres campos, es decir más NLRIs.

encabezado *shim*[59] de MPLS, se codifica como 3 bytes donde los primeros 20 bits contienen el Valor de la etiqueta. Los campos son:

- Valor de la etiqueta
- Bits experimentales
- *Bottom of the stack bit*

✓ **Prefijo**: Contiene el RD (64 bits) más el prefijo IPv4 (32 bits)

En relación a la información de los RTs, que como sabemos es una de las comunidades extendidas de BGP, se adjuntan a las rutas BGP, de la misma forma en que se hace con las comunidades estándar de BGP. Las actualizaciones que hace MP-BGP son las encargadas de transportar dichas comunidades extendidas a los demás pares.

Configuración de los enlaces PE a PE con MP-iBGP

Por *default* BGP se configura y se activa para que transporte prefijos *unicast* IPv4. Como en la arquitectura MPLS/VPN sólo se transportan direcciones VPN-IPv4 es necesario deshabilitarlo y habilitar el transporte de dichas direcciones.

Para desactivarlo se emplea el siguiente comando dentro del modo configuración.

```
Coyoacán(config)# router bgp 100
Coyoacán(config-router)# no bgp default ipv4-unicast
```

El *address-family* controla el tipo de sesión BGP, especifica el tipo de rutas (IPv4, VPNIPv4 o ambas) que una sesión entre PE's transportara además de su inserción en las diferentes tablas de un enrutador como son las VRFs, la tabla global o la de los procesos como BGP.

El proceso estándar de configuración de BGP define el *address-family* por *default* y en el se definen aquellos que no son vecinos BGP VPN, es decir aquellos con los que no se entablarán sesiones MP-iBGP. Los vecinos BGP que forman parte de la VPN se definen bajo su correspondiente *address-family*. Así se define un *address-family* en BGP por cada VRF configurada en el PE que anuncie rutas IPv4 y otra *address-family* para transportar direcciones VPN-IPv4 entre los PE's.

Entonces para configurar las sesiones BGP entre los PE's se realiza con el comando ***neighbor*** bajo la configuración BGP estándar o normal.

```
Coyoacán(config)# router bgp 100
Coyoacán(config-router)# neighbor 132.24.23.3 remote-as 100
Coyoacán(config-router)# neighbor 132.24.23.3 update-source loopback0
Coyoacán(config-router)# exit
Coyoacán(config)# router bgp 100
Coyoacán(config-router)# neighbor 132.24.23.1 remote-as 100
Coyoacán(config-router)# neighbor 132.24.23.1 update-source loopback0
```

Con los comandos anteriores solo habilitamos una sesión BGP y sería para transportar rutas IPv4 de la tabla de enrutamiento global aunque faltaría activar ahí mismo dicha sesión. Si se tuviese que hacer se introduciría el siguiente comando.

[59] Descrita en el Capítulo 3.

```
Coyoacán(config-router)# neighbor 132.24.23.1 activate
Coyoacán(config-router)# neighbor 132.24.23.3 activate
```

Aquí tendría que definir todos los vecinos BGP con los cuales se habilitarán sesiones BGP y posteriormente, a través del *address-family* se activarían las sesiones para transportar rutas VPNv4. Para ello es necesario crear un contexto de enrutamiento a fin de intercambiar direcciones VPNv4, y esto se logra mediante el *address-family* dentro del proceso general de BGP.

```
router bgp 100
address-family vpnv4
        neighbor 132.24.23.1 activate
        neighbor 132.24.23.3 activate
```

Como vemos solo es necesario activar la sesión para transportar rutas VPNv4 ya que el vecino ya se había definido en la configuración de la sesión BGP entre los PE's.

Con estas instrucciones queda activado MP-iBGP. Ahora es necesario, en el *address-family* indicar la información adicional que debe intercambiarse. Para mandar la información referente a las comunidades extendidas es necesario el siguiente comando.

```
neighbor 132.24.23.3 send-community both
neighbor 132.24.23.1 send-community both
```

Con esta instrucción habilito el envío de las comunidades estándar y las extendidas pudiendo especificar solo una de ellas ya sea con ***extended*** o **estándard.**

Ahora para indicar a MP-iBGP que tablas o rutas VRF debe advertir, es necesario configurar el *address-family* bajo el proceso BGP con la opción IPv4.

Cada VRF que inyecte rutas a BGP debe ser configurado bajo BGP con su propio *address-family*. Las rutas que pertenezcan a dichas VRF aprendidas por los distintos procesos (RIPv2, OSPF, etc.) deben ser redistribuidas si es que se desea que sean advertidas por MP-iBGP.

A continuación se muestra la configuración del enrutador PE ubicado en Coyoacán que da servicio de VPN a dos clientes.

```
ip vrf  DataCenter
        rd 1:27
        route-target export 100:27
        route-target import 100:27
!
ip vrf Autos
        rd 1 :26
        route-target export 100 :26
        route-target import 100 :26
!
interface loopback0
        ip address 132.24.23.2 255.255.255.255
!
interface serial0
        description ** interface a la VRF Autos **
        ip vrf forwarding Autos
        ip address 10.24.1.5 255.255.255.252
!
```

```
interface serial1
        description ** interface a la VRF DataCenter **
        ip vrf forwarding DataCenter
        ip address 192.168.24.5 255.255.255.252
!
router rip
        version 2
!
address-family ipv4 vrf Autos
        version 2
        redistribute bgp 100 metric 1
        network 10.24.1.0
        no auto-summary
exit-address-family
!
address-family ipv4 vrf DataCenter
        version 2
        redistribute bgp 100 metric 1
        network 192.168.24.0
        no auto-summary
exit-address-family
!
router bgp
        no bgp default ipv4-unicast
        neighbor 132.24.23.1 remote-as 100
        neighbor 132.24.23.1 update-source loopback0
        neighbor 132.24.23.3 remote-as 100
        neighbor 132.24.23.3 update-source loopback0
!
address-family ipv4 vrf Autos
        redistribute rip metric 1
        no auto-summary
        no synchronization
exit-address-family
!
address-family ipv4 vrf DataCenter
        redistribute rip metric 1
        no auto-summary
        no synchronization
exit-address-family
!
address-family vpnv4
        neighbor 132.24.23.1 activate
        neighbor 132.24.23.1 send-community extended
        neighbor 132.24.23.3 activate
        neighbor 132.24.23.3 send-community extended
exit-address-family
!
```

Enseguida se da la configuración necesaria en los otros dos enrutadores PE de la dorsal.

Enrutador PE de Polanco:

```
ip vrf  DataCenter
        rd 1:27
```

```
        route-target export 100:27
        route-target import 100:27
!
ip vrf Autos
        rd 1 :26
        route-target export 100 :26
        route-target import 100 :26
!
interface loopback0
        ip address 132.24.23.3 255.255.255.255
!
interface serial0
        description ** interface a la VRF Autos **
        ip vrf forwarding Autos
        ip address 10.24.2.5 255.255.255.252
!
interface serial1
        description ** interface a la VRF DataCenter **
        ip vrf forwarding DataCenter
        ip address 192.168.25.5 255.255.255.252
!
ip route vrf Autos 10.24.2.0/24 255.255.255.0 serial0
ip route vrf DataCenter 192.168.25.0 255.255.255.0 serial1

router bgp
        no bgp default ipv4-unicast
        neighbor 132.24.23.1 remote-as 100
        neighbor 132.24.23.1 update-source loopback0
        neighbor 132.24.23.2 remote-as 100
        neighbor 132.24.23.2 update-source loopback0
!
address-family ipv4 vrf Autos
        redistribute static
exit-address-family
!
address-family ipv4 vrf DataCenter
        redistribute static
exit-address-family
!
address-family vpnv4
        neighbor 132.24.23.1 activate
        neighbor 132.24.23.1 send-community extended
        neighbor 132.24.23.2 activate
        neighbor 132.24.23.2 send-community extended
exit-address-family
!
```

Por último la configuración del enrutador PE ubicado en el Centro.

```
ip vrf Autos
        rd 100:26
        route-target both 100:26
ip vrf DataCenter
        rd 100:27
        route-target both 100:27
```

```
interface loopback0
        ip address 132.24.23.1 255.255.255.0

interface serial0
        description ** interface a la VRF Autos **
        ip vrf forwarding Autos
        ip address 192.168.25.5 255.255.255.252

interface serial1
        description ** Interface a la VRF DataCenter **
        ip vrf forwarding DataCenter
        ip address 192.168.23.5 255.255.255.252

router rip
        version 2
address-family ipv4 vrf Autos
        version 2
        redistribute bgp 100 metric 1
        network 192.168.25.0
        no auto-summary
exit-address-family

address-family ipv4 vrf DataCenter
        version 2
        redistribute bgp 100 metric 1
        network 192.168.23.0
        no auto-summary
exit-address-family

router bgp 100
        no bgp default ipv4-unicast
        neighbor 132.24.23.2 remote-as 100
        neighbor 132.24.23.2 update-source loopback0
        neighbor 132.24.23.3 remote-as 100
        neighbor 132.24.23.3 update-source loopback0

address-family ipv4 vrf Autos
        redistribute rip
        no auto-summary
        no synchronization
exit-address-family

address-family ipv4 vrf DataCenter
        redistribute rip
        no auto-summary
        no synchronization
exit-address-family

address-family vpnv4
        neighbor 132.24.23.2 activate
        neighbor 132.24.23.2 send-community extended
        neighbor 132.24.23.3 activate
        neighbor 132.24.23.3 send-community extended
exit-address-family
```

En este caso no se recomienda el uso de un enrutador RR (*Route Reflector*) ya que los enrutadores que deben entablar sesiones BGP no son muchos. El RR permite hacer escalable una red que habla BGP cuando esta se conforma por muchos pares BGP. Dicho enrutador provee las rutas disponibles a todos los vecinos con los cuales tenga una sesión habilitada. Cada que se agregue un enrutador a la dorsal, se habilita una sesión BGP exclusivamente con el RR y éste se encargará de anunciar a todos los demás la existencia de un nuevo par.

4.5.3 Características de escalabilidad dentro de la arquitectura de MPLS/VPN

El hecho de que cualquier enrutador PE solo mantenga aquellas rutas VPNv4 que le sean relevantes, hace a la arquitectura MPLS/VPN muy escalable. Si no se almacenan rutas indeseables se ahorra memoria del PE además de evitar la propagación de información que no es necesaria.

El filtro de rutas automático (ARF, *Automatic Route Filtering*) es una característica que esta habilitada por omisión en los PEs y evita que se importe cualquier ruta con un RT que no este configurado en las VRF's del PE. Esto sucede a la entrada del PE. Toda la información con un RT distinto al configurado será desechada. En los RR esta característica esta deshabilitada.

Cuando la topología de la red cambia, ya sea que se agregue un nuevo cliente al servicio VPN o que un cliente VPN agregue un nuevo sitio, será necesario recuperar la información de enrutamiento que previamente fue desechada ya que probablemente para el nuevo sitio si sea relevante.

Para ello se cuenta con otra característica adicional de BGP que ayudará a recuperar la información descartada. Se trata del *Route Refresh*. Esta característica la emplea un PE y es una petición a sus vecinos MP-iBGP de retransmisión de información referente a las rutas VPNv4. Ocurre cuando una configuración en el PE ha cambiado.

La información recibida vuelve a pasar por el filtro de entrada que tienen los PE's, referente a desechar aquella información con un RT diferente al configurado en sus VRF's.

Obviamente esta capacidad de BGP debe ser advertida en el mensaje OPEN y por omisión esta habilitada.

```
sh ip bgp neighbor x.x.x.x
        ...
        neighbor capabilities
                Route Refresh: advertised and received
```

También puede mandar ejecutar el *Route Refresh* por sesión BGP con el siguiente comando.

```
clear ip bgp
```

Para mandar este mensaje a un solo CE perteneciente a una determinada VPN.

```
clear ip bgp * vrf <Nombre de la VRF1>
```

Para mandar este mensaje a un enrutador PE.

```
clear ip bgp * vpnv4 unicast in
```

Además de esto, existe una característica importante que ayuda a manejar o controlar la información de enrutamiento que emite un PE. En lugar de descartar información de enrutamiento innecesaria, se evita que se propague. Esta característica es ORF (*Outbound Route Filtering*) y trabaja en conjunto con el *Route Refresh.*

Esta característica de BGP advierte a sus vecinos que filtros de salida deben emplear. Los filtros ORF se incluyen en el mensaje *Route Refresh* y se resalta las entradas ORF que se clasifican de acuerdo a los siguientes tipos.

Tipo	Valor del tipo	Descripción
NLRI	1	Prevee prefijos de direcciones basados en el filtrado de ruta.
Comunidades	2	Prevee filtrado de rutas basado en las comunidades estandar.
Comunidades Extendidas	3	Prevee filtrado de rutas basado en las comunidades extendidas.
Lista de prefijos	129	Prevee filtrado de rutas basado en una lista de prefijos.

Tabla 4.3 Filtros ORF

Con esto pueden establecerse filtros para evitar la generación de actualizaciones con RT que no sean importables por ciertas VRF's en los PE's.

Capítulo 5. Caso práctico

La propuesta que a continuación se presenta esta orientada a proveer una solución de conectividad entre sitios geográficamente distantes aunado a las necesidades de controlar el tráfico que se pudiera generar.

Como primer punto se describirán las necesidades que requieren un par de empresas a fin de cumplir sus requisitos de interconectividad. Se proveerá un modelo de conexión que les dará, de inicio, el mismo esquema de conexión que el proporcionado por un SP[60] con tecnología *Frame Relay*, pero con las ventajas que conlleva utilizar la tecnología MPLS, que puede proporcionar calidad de servicio, como lo proporcionaría un modelo basado en tecnología FR o ATM.

Después de ello se planteará una solución a través de la implementación de una VPN bajo tecnología de MPLS. Para ello se analizarán los nodos de la red a fin de clasificarlos y asignarles funciones específicas.

Una vez realizada la clasificación se configurarán los nodos en cuestión. Para ilustrar como funciona el esquema de conexión, se describe como es que la información de control de las VPNs viaja a través de la dorsal de red MPLS/VPN.

También se ilustra como viaja la información en una VPN de un sitio a otro a través de una sesión entre dos *host* pertenecientes a la misma *Intranet*.

Este esquema facilitará cualquier esquema de negocios que se proponga la empresa además de que la expansión es una de las ventajas que puede explotar sin necesidad de realizar operaciones tediosas.

[60] SP, *Service Provider*, Proveedor de Servicio

5.1 Análisis de necesidades

5.1.1 Cliente

Se trata de un par de empresas que actualmente poseen una infraestructura de red con tecnología *Frame Relay*, la cual interconecta sus sitios remotos y centrales entre sí. No existe comunicación entre dichas empresas, por lo que los PVCs de FR se emplean para interconectar los sitios pertenecientes a cada *intranet*. A raíz de las desventajas que acarrea este tipo de infraestructuras y de las enormes ventajas que conlleva migrar a una red con tecnología MPLS empleando VPNs, mencionadas en capítulos anteriores, esta empresa ha decidido migrar su red a esta tecnología.

El modelo de conexión actual para la empresa DataCenter es el siguiente:

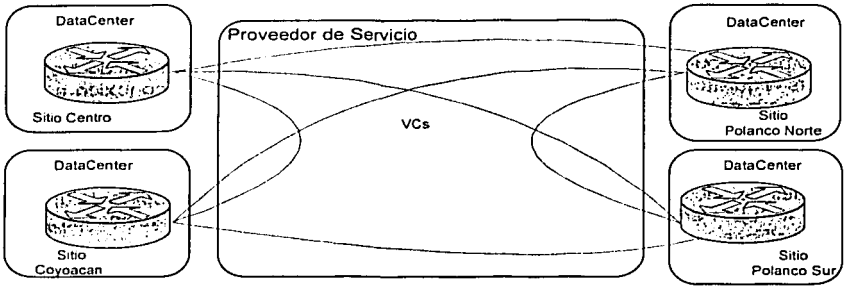


Figura 5.1 Caso práctico: Topología de Red actual del cliente DataCenter

En este caso los tres sitios se interconectan todos con todos, en una topología de tipo malla completa. No hay restricciones.

El modelo de conexión actual para la empresa D. Autos es el siguiente:

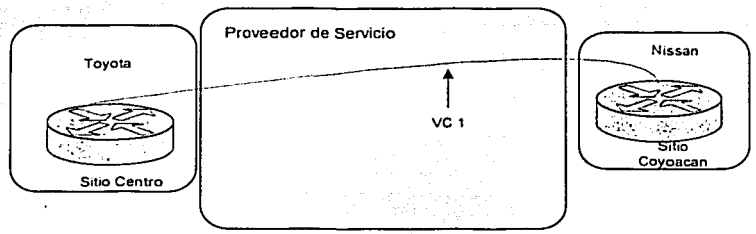


Figura 5.2 Caso Práctico: Topología de Red actual del cliente D. Autos

Igualmente, en este caso ambos sitios tienen conexión total entre sí.

La propuesta de migración del servicio se ilustra con el modelo siguiente, empleando la infraestructura de red de un SP que cuenta con tecnología MPLS.

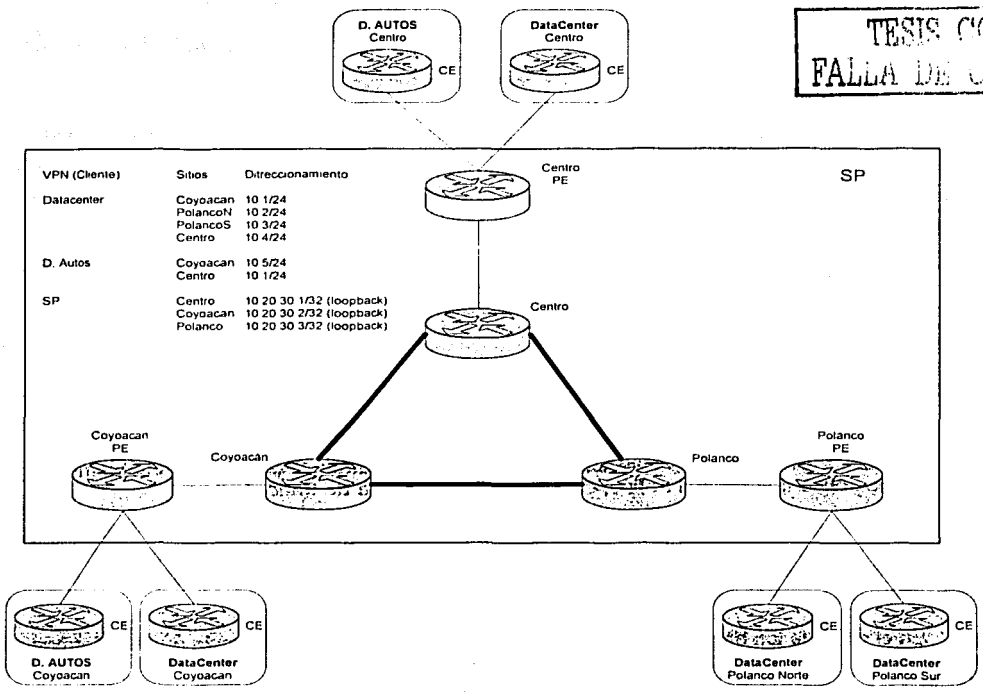


Figura 5.3 Modelo de Red del SP con MPLS

Las siguientes políticas describen la conectividad inter-sitio deseada para este caso particular entre los sitios de DataCenter (DC) y los de D. Autos (DA).

- Cualquier host en el sitio DC-Coyoacan puede comunicarse con cualquier host en el sitio DC-PolancoNorte y DC-PolancoSur y viceversa.
- Cualquier host en el sitio DC-Coyoacan puede comunicarse con cualquier host en el sitio DC-Centro y viceversa.
- Cualquier host en el sitio DC-Centro puede comunicarse con cualquier host en el sitio DC-PolancoNorte y DC-PolancoSur y viceversa.
- Cualquier host en el sitio DA-Coyoacan puede comunicarse con cualquier host en el sitio DA-Centro y viceversa.

En cuanto al enrutamiento para conectar los dispositivos CEs a los PEs, se necesitará ajustar a alguno de los protocolos de enrutamiento IGP que sea soportado por MPLS, en el caso que se requiera enrutamiento dinámico. Así, la elección para escoger el protocolo IGP que ha de emplearse para comunicar los CEs con los PEs, estará determinada por las necesidades de conectividad que presente el cliente.

Los sitios remotos son sitios *stub* por lo que no es necesario que se implementen soluciones de enrutamiento dinámico. Por ello se recomienda para este tipo de sitios que se emplee enrutamiento estático a fin de establecer conectividad entre los CEs y los PEs.

Por otra parte para aquellos sitios "centrales" que tengan, además de aprender rutas de los otros sitios remotos, aplicar algún tipo de políticas de tráfico y que deban proveer algún tipo de recurso a los demás sitios pertenecientes a la misma *Intranet*, será necesario y recomendable implementar como protocolo de enrutamiento con el PE, RIPv2.

5.1.1.1 Tipo de tráfico

En cuanto al tipo de información que manejan ambas empresas podemos establecerla de acuerdo a las aplicaciones que tienen implementadas. Enumeramos las aplicaciones que emplearía el cliente y de las cuales s e deriva el tipo de tráfico.

- Base de datos
- *Active Directory*
- FTP
- WEB

En base a esto podemos clasificar el tráfico como de datos. Por lo que probablemente no sea necesario aplicar políticas al tráfico, o técnicas de ingeniería de tráfico.

Los requisitos de disponibilidad y seguridad para ciertas aplicaciones son necesarios. Por ejemplo para manejar los recursos de las redes LANs que componen cada sitio del cliente, el *Active Directory* de Microsoft, de su sistema operativo Windows .NET, necesita entre otras cosas disponibilidad de recursos para poder realizar sus réplicas de directorio.

En el caso de las bases de datos de la empresa es de suma importancia que la información que viaja entre los sitios se realice en forma segura ya que es información que solo le compete a la empresa y que si alguien la llega a saber puede comprometer los intereses de dicha empresa.

Si bien la transferencia de archivos no es de suma importancia en el sentido de que no se necesita darle prioridad a este tipo de tráfico, si es necesario que exista ancho de banda suficiente para poder hacer los respaldos de información, ya sea de las bases de datos o de algún otro tipo de información de interés para la empresa.

5.1.1.2 Capacidad de enlaces

La capacidad necesaria de los enlaces para comunicar los sitios a la dorsal MPLS/VPN van de acuerdo a la cantidad de tráfico que sea necesario transportar y el costo, por supuesto. Así, se presentan las siguientes tablas.

Tabla 5.1 Enlaces de banda ancha

Capacidad	Ancho de banda (Mbps)[61]	Equivalencias
DS0	0.064	
E1	2.048	32*DS0
E3	34.368	480*DS0
DS3 (T3)	44.736	672*DS0

[61] Incluyen la parte real utilizable por el cliente como la parte usada por los canales de señalización.

OC[62]1	51.84[63]	
STM-1 (OC-3)	155.52	3*OC1
STM-4 (OC-12)	622.08	12*OC1
STM-16 (OC-48)	2488.32	48*OC1

Tabla 5.2 Enlaces de 2 MBPS (E1)

	Rango (Km)	Gasto de instalación (Por tramo)	Renta Mensual (Por tramo)	
			Fijo	Cargo/Km
Local	N.A.	$90,971	$5,321	N.A.
Larga Distancia Nacional	0-81	$12,293	$9,916	$226
	>81-161		$20,830	$168
	>161-805		$39,153	$64
	>805		$55,228	$46

Tabla 5.3 Enlaces Nx64

	Gasto de instalación	Renta mensual por tramo
64 kbps	$12,908	$907
128 kbps	$19,362	$1,725
192 kbps	$25,816	$2,042

La cantidad de tráfico generado en cada sitio VPN se indica en las siguientes matrices de tráfico.

Tabla 5.4 Tráfico generado por D. Autos

Destino / Origen	Coyoacan	Centro
Coyoacan		100 kbps
Centro	100 kbps	

Tabla 5.5 Tráfico generado por DATACENTER

Destino / Origen	Coyoacan	Centro	PolancoN	PolancoS
Coyoacan		32 kbps	32 kbps	-
Centro	56 kbps		56 kbps	56 kbps
PolancoN	32 kbps	32 kbps		32 kbps
PolancoS	-	32 kbps	32 kbps	

De aquí establecemos la capacidad de los enlaces CE-PE necesarios para soportar la carga de tráfico de cada cliente.

Tabla 5.6 Capacidad de enlaces asignado a cada Sitio

Cliente	Enlace	Capacidad
D. Autos	CE_Coyoacan_DA – PE_Coyoacan	2*64Kbps

[62] *Optical Carrier*. Se refiere al nivel físico en SONET de acuerdo con el estándar de la ANSI.
[63] Tasa de línea, no de *payload*.

	CE_Centro_DA – PE_Centro	2*64Kbps
DataCenter	CE_Coyoacan_DC – PE_Coyoacan	64Kbps
	CE_PolancoN_DC – PE_Polanco	2*64Kbps
	CE_PolancoS_DC – PE_Polanco	64Kbps
	CE_Centro_DC – PE_Centro	3*64Kbps

Por cuestiones de costo no se eligen enlaces de alta capacidad, ya que además del costo de instalación se debe cubrir una cuota mensual significativa.

5.1.1.3 Equipo adicional

En cuanto al *hardware* adicional o de renovación que se necesitaría podemos decir que el equipo actual de los clientes es suficiente y realmente no necesita realizar una inversión cuantiosa para poder recibir el servicio.

5.1.2 Proveedor de Servicio

En el caso del SP, este posee una infraestructura de red con tecnología MPLS que esta habilitada para dar, entre otros servicios, el de VPNs.

En cuanto al enrutamiento, dentro de la dorsal MPLS/VPN, por razones de escalabilidad y rendimiento la opción es usar BGP versión 4. Todos los enrutadores PE necesitan transportar las rutas aprendidas de los enrutadores de los clientes, además de la posibilidad de transportar rutas pertenecientes a la Internet, si es que se tienen habilitado. Por estas razones se necesita un protocolo de enrutamiento robusto que pueda soportar los requerimientos actuales y que sea capaz de escalar cuando el tráfico aumente, como BGP-4.

Además, la posibilidad de que los clientes del SP crezca es mucha, lo que lleva a pensar que no todos emplearán los mismos protocolos de enrutamiento para comunicarse con la dorsal del SP y por tanto la necesidad de que la tecnología de enrutamiento que implemente el SP sea capaz de transportar rutas pertenecientes a más de un protocolo de enrutamiento y más de una familia de direcciones, lo que lleva a pensar en una tecnología multiprotocolo. Para cumplir esto, se pueden implementar extensiones multiprotocolo al mismo protocolo BGP-4, sin necesidad de alterar su funcionamiento normal.

5.1.2.1 Capacidad de enlaces

En cuanto a la capacidad de conexión con que cuenta dicho proveedor podemos decir que cada enlace dentro de la dorsal tiene una capacidad de 34.368 Mbps (E3), suficiente para transportar el tráfico de los usuarios existentes y para satisfacer sus necesidades de expansión de muchos clientes más. La capacidad de los enlaces que conectan cada uno de los enrutadores P deben de soportar el tráfico originado por todos los clientes a la hora pico. El *hardware* con el que cuenta actualmente soporta los requerimientos necesarios por lo que no hay necesidad de actualizar o realizar un gasto adicional.

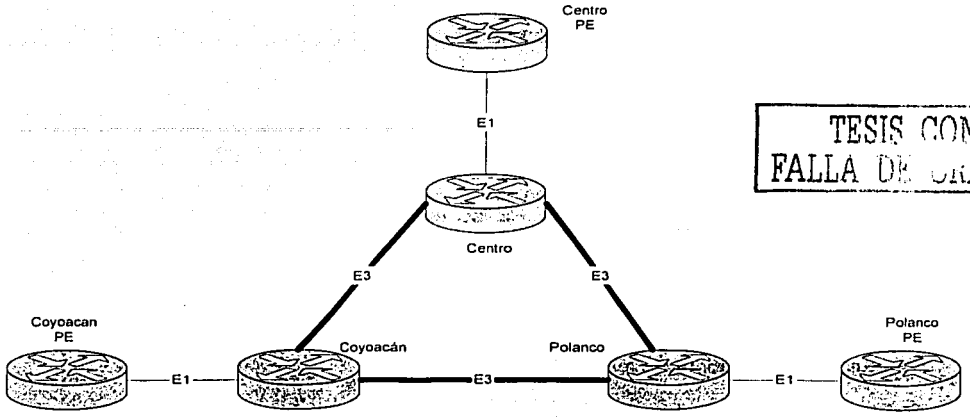


Figura 5.4 Capacidad de los enlaces Enrutadores P y Enrutadores PE

Tabla 5.7 Enlaces en la dorsal de red

Enlace	Capacidad
Backbone	E3
No Backbone	E1

Los enlaces están orientados a ofrecer una solución al transporte de datos de los clientes a través de la dorsal y solo proveen conexiones punto a punto hacia un solo proveedor.

En cuestiones de administración no necesitará algún tipo de acuerdo con el cliente ya que esta tarea la tiene asignada completamente el Proveedor de Servicio. Será parte del servicio vendido.

En cuanto a la tecnología que usa el SP para administrar las etiquetas que conforman las LSP, el proveedor ha considerado emplear LDP para establecer y mantener las LSPs[64].

5.2 Estrategia para la implementación de MPLS/VPN

Considerando que el SP ya tiene capacidad para brindar el servicio de VPNs empleando tecnología de MPLS, realizamos un esquema que definiría los pasos a seguir para la implementación del servicio a los dos clientes mencionados anteriormente.

Los pasos a seguir son:

- Clasificación de los nodos para la activación de funcionalidades.
- Implementación (Configuración de cada uno de los nodos).
- Esquema de seguimiento de la información de control para el correcto funcionamiento del servicio.

[64] Recordar que si se tiene habilitado LDP y RSVP al mismo tiempo, el segundo método tiene preferencia.

5.2.1 Clasificación de los nodos para la activación de funcionalidades

Para la dorsal de red del proveedor podemos clasificar los nodos de red en tres tipos:

- Enrutadores PE. Estos enrutadores son lo que sirven como punto de acceso a la dorsal del SP. Principalmente van a intercambiar información de enrutamiento con los CEs a través de enrutamiento estático o dinámico, según las necesidades del cliente. También entablarán sesiones BGP con cada par o enrutador PE perteneciente a la dorsal de red. Como nodos MPLS los enrutadores PE se encargan de etiquetar los paquetes IP al momento de entrar al dominio MPLS así como desetiquetarlos cuando abandonan dicho dominio.

- Enrutadores P. Cualquier enrutador que no tenga contacto directo con algún dispositivo de red perteneciente al cliente estará clasificado como enrutador P. En el caso de la arquitectura MPLS, sus funciones se limitarán a los procesos relacionados con la conmutación de etiquetas.

- Enrutadores CE. Son los dispositivos pertenecientes a los clientes que les brindarán conexión con los enrutadores de acceso del SP, en este caso los PEs.

Enrutadores PE

En este caso particular, se ha adjuntado un enrutador PE, perteneciente al SP, a cada sitio que necesita enviar o recibir rutas a otro sitio de su misma *intranet*. Una de las ventajas de la arquitectura MPLS/VPN es que los PEs no necesitan almacenar las rutas de todas las VPNs sino solo aquellas rutas de cada VPN que tenga configurada (anunciadas por otros PE's) y de los sitios que tienen conectados directamente (configuradas estáticamente en el PE, o bien anunciadas dinámicamente por los CE's).

En cuanto a la información de enrutamiento que fluye de un CE al PE de ingreso, un enrutador PE realiza lo siguiente:

- Mantiene una tabla VRF por cada uno de los sitios conectados directamente a el. En el caso del PE ubicado en Polanco, este se debe configurar para asociar múltiples sitios a una misma VRF.

- Checa todas las rutas contra la política de importación configurada localmente para cada protocolo de enrutamiento que se ejecute entre las interfases del PE y del CE. Si la ruta pasa el filtro, el prefijo de dirección se instala en la VRF correspondiente como ruta IPv4.

- Verificar que los otros PEs que tengan configuradas las mismas VPNs estén anunciando al PE en proceso de configuración, las rutas de los CEs que tengan directamente conectados.

- Antes de que el PE advierta la ruta, se le asigna una etiqueta MPLS.

- Verificar que se estén anunciando las rutas de CEs directamente conectados, a los PEs correspondientes.

Enrutador PE Centro y PE Coyoacan. El enrutador PE Centro tiene conectados a el 2 sitios en los cuales se encuentran los servidores primarios a los cuales deben de acceder los demás sitios. Para cubrir las necesidades se desarrollará RIPv2 en conjunto con los CEs indicados.

La configuración de enrutador PE Coyoacan será la misma en cuanto a la forma de comunicarse con los otros PEs. La única diferencia será el modo en que ambos aprenderán rutas de sus respectivos enrutadores CEs ya que el enrutador PE Coyoacan empleará enrutamiento estático para comunicarse con los CEs conectados a el.

Enrutador PE Polanco. En este nodo, el enrutamiento será estático y solo cabe hacer notar que se necesitará asociar dos sitios a una misma VRF.

Enrutadores P

Los enrutadores P únicamente tendrán funciones relacionadas con la conmutación de etiquetas y los procesos para mantener las LSP. La información de las VPNs no será almacenada por estos enrutadores ya que ellos se limitarán a reenviar los paquetes atendiendo solo a la información de la pila de etiquetas de MPLS/VPN.

Enrutadores CE

Serán enrutadores que ya estarán enviando todo el tráfico a una ruta por *default* que apunta hacia el PE al que se conectan, o bien estarán usado enrutamiento dinámico con RIPV2.

5.2.2 Arquitectura de Red

El dominio o sistema autónomo que tiene asignado el SP para su dorsal de red es el 65350. Con esto podemos establecer los valores de RT que se emplearán para configurar las políticas de RT que nos servirán para cubrir los requerimientos de conectividad inter-sitio requeridas por ambos clientes.

Tabla 5.8 Asignación de RD y RT

Cliente VPN	Número de Sistema Autónomo	Valor único	RD	RT
D. Autos	65350	100	65350:100	65350:100
DataCenter	65350	101	65350:101	65350:101

5.2.2.1 Sesiones BGP

El SP solo necesita configurar sesiones lógicas de malla completa entre los enrutadores PE. Para ello emplea las direcciones *loopback* de cada enrutador PE. En este caso todos los enrutadores que conforman el *backbone* no necesitan conocer las rutas BGP por lo que ellos no están considerados para ser *peers* BGP.

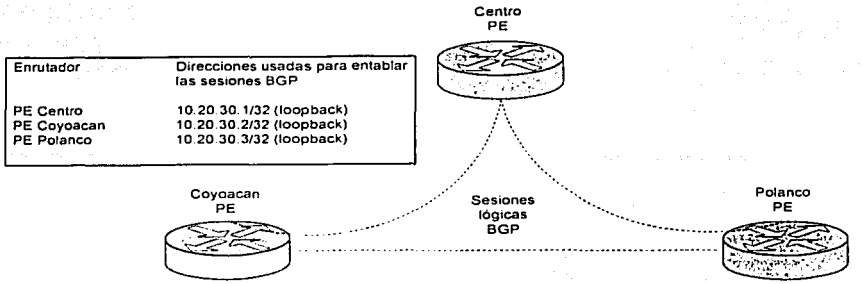


Figura 5.5 Sesiones lógicas BGP entre PEs

Los tres enrutadores PE intercambiaran rutas VPNv4 y posiblemente direcciones IPv4.

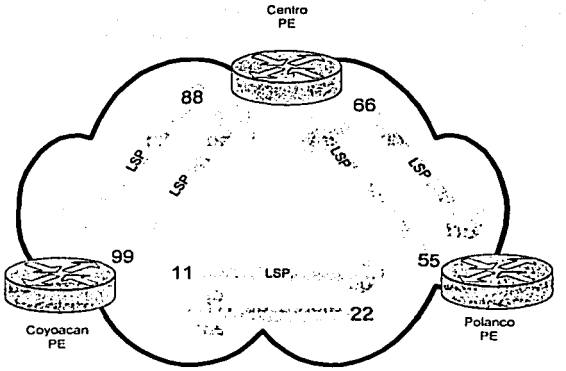


Figura 5.6 *Label Switched Paths*

5.2.3 Implementación (Configuración de cada uno de los nodos)

A continuación se presenta la configuración de cada uno de los enrutadores PE involucrados en la provisión del servicio de VPNs.

Enrutadores PEs

PE Coyoacan

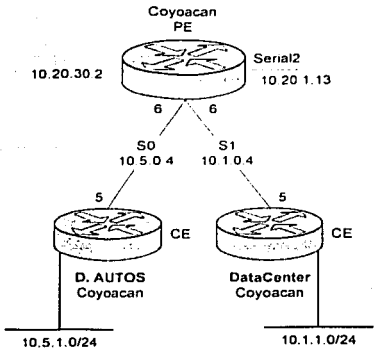


Figura 5.7 Diagrama de conexión Enrutador PE Coyoacan

```
hostname PE_Coyocan
!
ip cef
!
ip vrf Autos
        rd 65350:100
        route-target import 65350:100
        route-target export 65350:100
!
ip vrf DataCenter
        rd 65350:101
        route-target import 65350:101
        route-target export 65350:101
!
interface loopback0
        ip address 10.20.30.2 255.255.255.255
!
interface serial0
        ip vrf forwarding Autos
        ip address 10.5.0.6 255.255.255.252
!
interface serial2
        ip address 10.20.1.13 255.255.255.252
        tag-switching ip
!
interface serial1
        ip vrf forwarding DataCenter
        ip address 10.1.0.6 255.255.255.252
!
ip route vrf Autos 10.5.1.0 255.255.255.0 serial0
ip route vrf DataCenter 10.1.1.0 255.255.255.0 serial1
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
```

```
router bgp
        no bgp default ipv4-unicast
        neighbor 10.20.30.3 remote-as 65350
        neighbor 10.20.30.3 update-source loopback0
        neighbor 10.20.30.1 remote-as 65350
        neighbor 10.20.30.1 update-source loopback0

address-family ipv4 vrf Autos
        redistribute static
exit-address family
!
address-family ipv4 DataCenter
        redistribute static
exit-address family
!
address-family vpnv4
        neighbor 10.20.30.3 activate
        neighbor 10.20.30.3 send-community both
        neighbor 10.20.30.1 activate
        neighbor 10.20.30.1 send-community both
exit-address family
!
ip classless
```


Enrutador PE Polanco

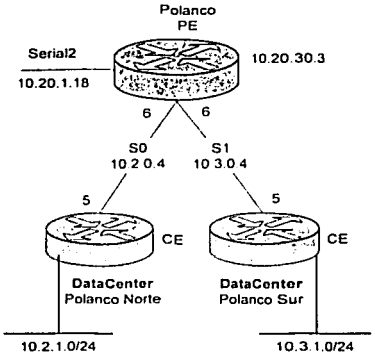


Figura 5.8 Diagrama de conexión Enrutador PE Polanco

```
hostname PE_Polanco
!
!
ip cef
!
!
ip vrf DataCenter
        rd 65350:101
```

```
        route-target import 65350:101
        route-target export 65350:101
!
!
interface loopback0
        ip address 10.20.30.3 255.255.255.255
!
interface serial0
        ip vrf forwarding DataCenter
        ip address 10.2.0.6 255.255.255.252
!
interface serial1
        ip vrf forwarding DataCenter
        ip address 10.3.0.6 255.255.255.252
!
interface serial2
        ip address 10.20.1.18 255.255.255.252
        tag-switching ip
!
!
ip route vrf DataCenter 10.2.1.0 255.255.255.0 serial0
ip route vrf DataCenter 10.3.1.0 255.255.255.0 serial1
!
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
!
router bgp
        no bgp default ipv4-unicast
        neighbor 10.20.30.2 remote-as 65350
        neighbor 10.20.30.2 update-source loopback0
        neighbor 10.20.30.1 remote-as 65350
        neighbor 10.20.30.1 update-source loopback0

address-family ipv4 DataCenter
        redistribute static
exit-address family
!
!
address-family vpnv4
        neighbor 10.20.30.2 activate
        neighbor 10.20.30.2 send-community both
        neighbor 10.20.30.1 activate
        neighbor 10.20.30.1 send-community both
exit-address family
!
!
ip classless
```

Enrutador PE Centro

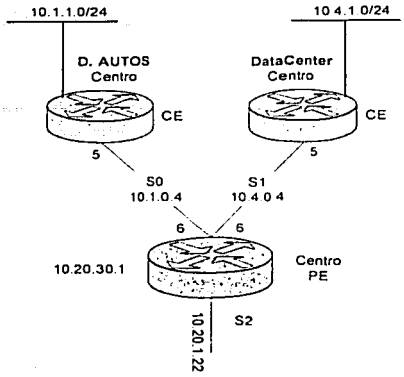


Figura 5.9 Diagrama de conexión Enrutador PE Centro

```
hostname PE_Centro
!
ip cef
!
ip vrf Autos
        rd 65350:100
        route-target import 65350:100
        route-target export 65350:100
!
ip vrf DataCenter
        rd 65350:101
        route-target import 65350:101
        route-target export 65350:101
!
interface loopback0
        ip address 10.20.30.1 255.255.255.255
!
interface serial0
        ip vrf forwarding Autos
        ip address 10.1.0.6 255.255.255.252
!
interface serial1
        ip vrf forwarding DataCenter
        ip address 10.4.0.6 255.255.255.252
!
interface serial2
        ip address 10.20.1.22 255.255.255.252
        tag-switching ip
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
```

```
router rip
        version 2
!
address-family ipv4 vrf Autos
        version 2
        redistribute bgp 65350 metric 1
        network 10.1.0.0
        no auto-summary
exit-address-family
!
address-family ipv4 vrf DataCenter
        version 2
        redistribute bgp 65350 metric 1
        network 10.4.0.0
        no auto-summary
exit-address-family
!
router bgp
        no bgp default ipv4-unicast
        neighbor 10.20.30.2 remote-as 65350
        neighbor 10.20.30.2 update-source loopback0
        neighbor 10.20.30.3 remote-as 65350
        neighbor 10.20.30.3 update-source loopback0
!
address-family ipv4 vrf Autos
        redistribute rip metric 1
        no auto-summary
        no synchronization
exit-address-family
!
address-family ipv4 vrf DatCenter
        redistribute rip metric 1
        no-auto-summary
        no synchronization
exit-address-family
!
address-family vpnv4
        neighbor 10.20.30.2 activate
        neighbor 10.20.30.2 send-community both
        neighbor 10.20.30.3 activate
        neighbor 10.20.30.3 send-community both
exit-address-family
!
ip classless
```

Enrutadores CEs

CE Coyoacan D. Autos

```
hostname CE_Coyoacan_DA
!
ip subnet-zero
!
```

```
interface serial0
        ip address 10.5.0.5 255.255.255.252
!
interface ethernet0
ip address 10.5.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial0
end
```

CE Coyoacan DATACENTER

```
hostname CE_Coyoacan_DC
!
ip subnet-zero
!
interface serial1
        ip address 10.1.0.5 255.255.255.252
!
interface ethernet0
ip address 10.1.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial1
end
```

CE Polanco Norte DATACENTER

```
hostname CE_PolancoNorte_DC
!
ip subnet-zero
!
interface serial0
        ip address 10.2.0.5 255.255.255.252
!
interface ethernet0
ip address 10.2.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial0
end
```

CE Polanco Sur DATACENTER

```
hostname CE_PolancoSur_DC
!
ip subnet-zero
!
interface serial1
        ip address 10.3.0.5 255.255.255.252
!
interface ethernet0
```

```
ip address 10.3.1.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial1
end
```

CE Centro D. Autos

```
hostname CE_Centro_DA
!
ip subnet-zero
!
interface serial0
        ip address 10.1.0.5 255.255.255.252
!
interface ethernet0
ip address 10.1.1.254 255.255.255.0
!
router rip
        version 2
        network 10.1.0.0
        no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial0
end
```

CE Centro DATACENTER

```
hostname CE_Centro_DC
!
ip subnet-zero
!
interface serial1
        ip address 10.4.0.5 255.255.255.252
!
interface ethernet0
ip address 10.4.1.254 255.255.255.0
!
router rip
        version 2
        network 10.4.0.0
        no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 serial1
!
end
```

Enrutadores Ps

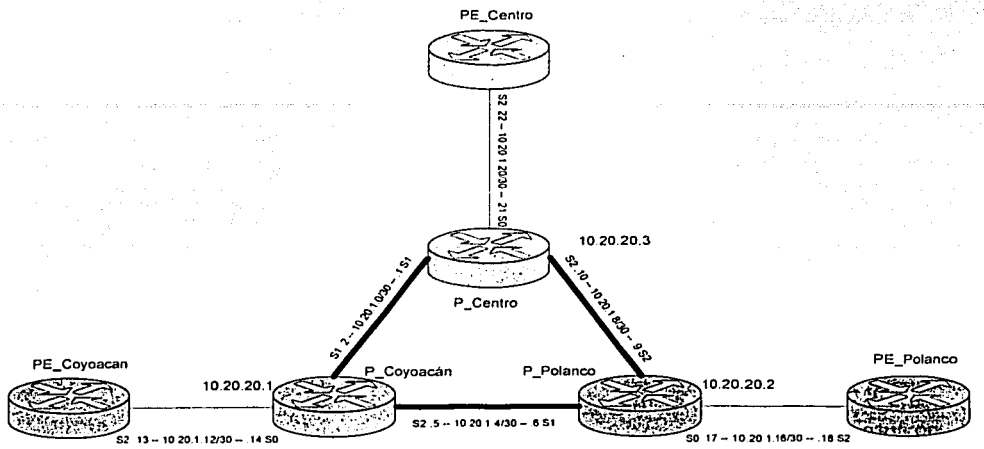


Figura 5.10 Topología del *backbone*

P Coyoacan

```
hostname P_Coyoacan
!
!
ip cef
!
interface loopback0
        ip address 10.20.20.1 255.255.255.255
!
interface serial0
        ip address 10.20.1.14 255.255.255.252
        tag-switching ip
!
interface serial1
        ip address 10.20.1.2 255.255.255.252
        tag-switching ip
!
interface serial2
        ip address 10.20.1.5 255.255.255.252
        tag-switching ip
!
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
!
```

P Polanco

```
hostname P_Polanco
!
ip cef
!
interface loopback0
        ip address 10.20.20.2
!
interface serial0
        ip address 10.20.1.17 255.255.255.252
        tag-switching ip
!
interface serial1
        ip address 10.20.1.6 255.255.255.252
        tag-switching ip
!
interface serial2
        ip address 10.20.1.9 255.255.255.252
        tag-switching ip
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
```

P Centro

```
hostname P_Centro
!
ip cef
!
interface loopback0
        ip address 10.20.20.3
!
interface serial0
        ip address 10.20.1.21 255.255.255.252
        tag-switching ip
!
interface serial1
        ip address 10.20.1.1 255.255.255.252
        tag-switching ip
!
interface serial2
        ip address 10.20.1.10 255.255.255.252
        tag-switching ip
!
router eigrp 124
        network 10.20.0.0
        no auto-summary
!
```

5.3 Esquema de seguimiento de la información de control para el correcto funcionamiento del servicio

En este punto se hará un análisis de la información de control de la VPN así como de la de MPLS para el caso tratado.

5.3.1 Distribución de la información de enrutamiento VPN

Antes de poder enviar tráfico VPN de un sitio remoto a otro primero es necesario distribuir la información de enrutamiento VPN entre los sitios a través de la dorsal de red.

5.3.1.1 Distribución de rutas del CE al PE

PE Coyoacan

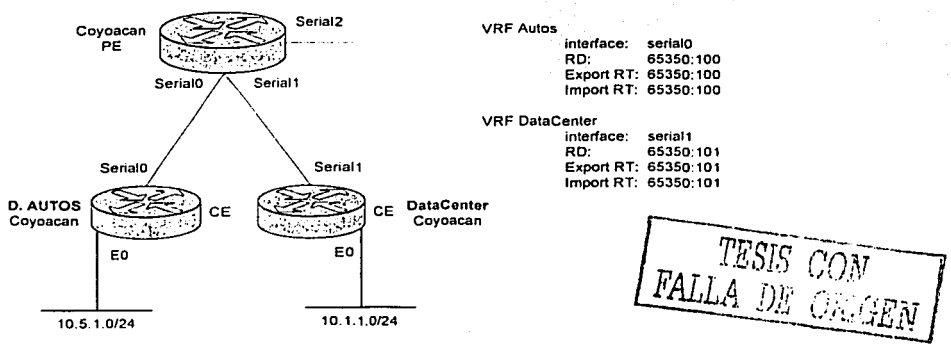


Figura 5.11 Esquema de configuración Enrutador PE Coyoacan

El enrutador PE de Coyoacan hizó la siguiente asignación de etiquetas a las rutas aprendidas de los siguientes sitios:

Tabla 5.9 Etiquetas asignadas Enrutador PE Coyoacan

Sitio	Prefijo	Etiqueta
Coyoacan Autos	10.5.1/24	1001
Coyoacan DataCenter	10.1.1/24	1002

Estas etiquetas son las que pertenecen a la VPN y en las tablas siguientes aparecen en la columna de *Bottom Label*. Las etiquetas que aparecen en las tablas siguientes en la columna de Top Label, son las que están asociadas a las direcciones de *loopback* de los PE destino y son las que permiten trasportar los paquetes de un PE a otro.

El enrutador instaló dos rutas MPLS, para que cuando arrive un paquete de la dorsal de red con cualquiera de esas etiquetas, el enrutador PE pueda realizar una operación de extracción de etiqueta y envie el paquete IPv4 directamente al CE correspondiente.

Tabla 5.10 Tabla de envío MPLS Enrutador PE Coyoacan

Input Interface	Label	Action	Output Interface
Serial2	1001	Pop	Serial0
Serial2	1002	Pop	Serial1

Las tablas VRFs del enrutador PE son:

Tabla 5.11 Tabla VRF Autos

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.5.1/24	Direct	Serial0	1001	-

Tabla 5.12 Tabla VRF DataCenter

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1.1/24	Direct	Serial1	1002	-

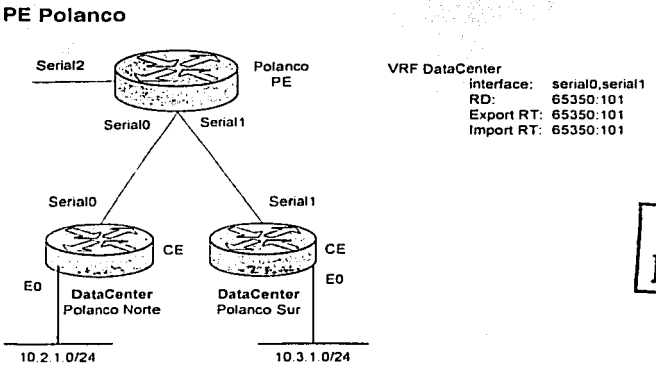


Figura 5.12 Esquema de configuración Enrutador PE Polanco

El enrutador LER de Polanco hizó la siguiente asignación de etiquetas a las rutas aprendidas de los siguientes sitios:

Tabla 5.13 Etiquetas asignadas Enrutador PE Polanco

Sitio	Prefijo	Etiqueta
PolancoN DataCenter	10.2.1/24	1003
PolancoS DataCenter	10.3.1/24	1004

El enrutador instaló dos rutas MPLS, para que cuando arribe un paquete de la dorsal de red con cualquiera de esas etiquetas, el enrutador PE pueda realizar una operación de extracción (*pop*) de etiqueta y envíe el paquete IPv4 directamente al CE correspondiente.

Tabla 5.14 Tabla de envio MPLS Enrutador PE Polanco

Input Interface	Label	Action	Output Interface
Serial2	1003	Pop	Serial0
Serial2	1004	Pop	Serial1

Las tablas VRFs del enrutador PE son:

Tabla 5.15 Tabla VRF DataCenter

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.2.1/24	Direct	Serial0	1003	-
10.3.1/24	Direct	Serial1	1004	-

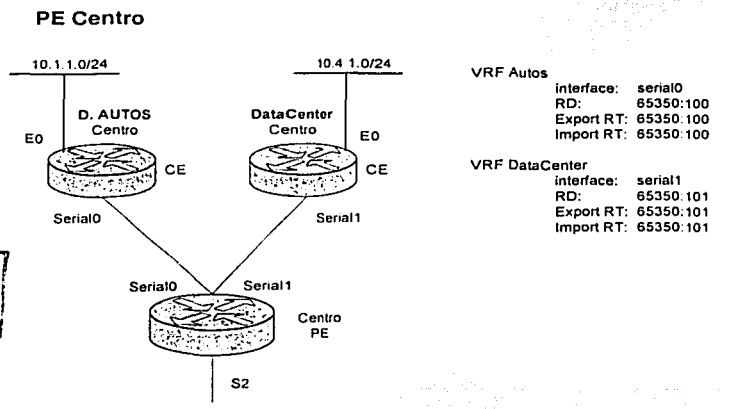


Figura 5.13 Esquema de configuración Enrutador PE Centro

El enrutador PE del Centro hizo la siguiente asignación de etiquetas a las rutas aprendidas de los siguientes sitios:

Tabla 5.16 Etiquetas asignadas Enrutador PE Centro

Sitio	Prefijo	Etiqueta
Centro Autos	10.1.1/24	1005
Centro DataCenter	10.4.1/24	1006

El enrutador instaló dos rutas MPLS, para que cuando arribe un paquete de la dorsal de red con cualquiera de esas etiquetas, el enrutador PE pueda realizar una operación de extracción de etiqueta y envie el paquete IPv4 directamente al CE.

Tabla 5.17 Tabla de envio MPLS Enrutador PE Centro

Input Interface	Label	Action	Output Interface
Serial2	1005	Pop	Serial0
Serial2	1006	Pop	Serial1

Las tablas VRFs del enrutador PE son:

Tabla 5.18 Tabla VRF Autos

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1.1/24	Direct	Serial0	1005	-

Tabla 5.19 Tabla VRF DataCenter

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.4.1/24	Direct	Serial1	1006	-

5.3.1.2 Distribución de rutas a través de la dorsal de red de PE a PE

Para realizar esta tarea se emplean las sesiones habilitados de MP-iBGP. La información es enviada por cada PE a cada uno de sus pares MP-iBGP.

Anuncios de ruta de los PE de Ingreso

PE Coyoacan

Destination 65350:100:10.5.1/24
Label 1001
BGP Next-Hop 10.20.30.2
RT 65350:100

Destination 65350:101:10.1.1/24
Label 1002
BGP Next-Hop 10.20.30.2
RT 65350:101

PE Polanco

Destination 65350:101:10.2.1/24
Label 1003
BGP Next-Hop 10.20.30.3
RT 65350:101

Destination 65350:101:10.3.1/24
Label 1004
BGP Next-Hop 10.20.30.3
RT 65350:101

PE Centro

Destination 65350:100:10.1.1/24
Label 1005
BGP Next-Hop 10.20.30.1
RT 65350:100

Destination 65350:101:10.4.1/24
Label 1006
BGP Next-Hop 10.20.30.1
RT 65350:101

Instalación de rutas en los PEs de egreso

Los enrutadores PE instalan las siguientes rutas

PE Coyoacan

PE Coyoacan instala las siguientes rutas de su par PE Polanco en la VRF DataCenter.

Destination 65350:101:10.2.1/24
Label 1003
BGP Next-Hop 10.20.30.3
RT 65350:101

Destination 65350:101:10.3.1/24
Label 1004
BGP Next-Hop 10.20.30.3
RT 65350:101

PE Coyoacan instala las siguientes rutas de su par PE Centro en la VRF Autos.

Destination 65350:100:10.1.1/24
Label 1005
BGP Next-Hop 10.20.30.1
RT 65350:100

PE Coyoacan instala las siguientes rutas de su par PE Centro en la VRF DataCenter.

Destination 65350:101:10.4.1/24
Label 1006
BGP Next-Hop 10.20.30.1
RT 65350:101

Después que las rutas han sido intercambiadas, el contenido de las tablas VRF del enrutador PE Coyoacan son:

Tabla 5.20 Tabla VRF Autos Enrutador PE Coyoacan

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.5.1/24	Direct	Serial0	1001	-
10.1.1/24	10.20.30.1	Serial2	1005	99

Tabla 5.21 Tabla VRF DataCenter Enrutador PE Coyoacan

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1.1/24	Direct	Serial1	1002	-
10.2.1/24	10.20.30.3	Serial2	1003	11
10.3.1/24	10.20.30.3	Serial2	1004	11
10.4.1/24	10.20.30.1	Serial2	1006	99

PE Polanco

PE Polanco instala las siguientes rutas de su par PE Coyoacan en la VRF DataCenter.

Destination 65350:101:10.1.1/24
Label 1002
BGP Next-Hop 10.20.30.2
RT 65350:101

PE Polanco instala las siguientes rutas de su par PE Centro en la VRF DataCenter.

Destination 65350:101:10.4.1/24
Label 1006
BGP Next-Hop 10.20.30.1
RT 65350:101

Después que las rutas han sido intercambiadas, el contenido de la tabla VRF del enrutador PE Polanco es:

Tabla 5.22 Tabla VRF DataCenter

Destination	BGP Next-Hop Direct	Interface	Bottom Label	Top Label
10.2.1/24	Direct	Serial0	1003	-
10.3.1/24	Direct	Serial1	1004	-
10.1.1/24	10.20.30.2	Serial2	1002	22
10.4.1/24	10.20.30.1	Serial2	1006	55

PE Centro

PE Centro instala las siguientes rutas de su par PE Coyoacan en la VRF Autos.

Destination 65350:100:10.5.1/24
Label 1001
BGP Next-Hop 10.20.30.2
RT 65350:100

PE Centro instala las siguientes rutas de su par PE Coyoacan en la VRF DataCenter.

Destination 65350:101:10.1.1/24
Label 1002
BGP Next-Hop 10.20.30.2
RT 65350:101

PE Centro instala las siguientes rutas de su par PE Polanco en la VRF DataCenter.

Destination 65350:101:10.2.1/24
Label 1003
BGP Next-Hop 10.20.30.3
RT 65350:101

Destination 65350:101:10.3.1/24
Label 1004
BGP Next-Hop 10.20.30.3
RT 65350:101

Después que las rutas han sido intercambiadas, el contenido de la tabla VRF del enrutador PE Centro es:

Tabla 5.23 Tabla VRF Autos Enrutador PE Centro

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1.1/24	Direct	Serial0	1005	-
10.5.1/24	10.20.30.2	Serial2	1001	88

Tabla 5.24 Tabla VRF DataCenter Enrutador PE Centro

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.4.1/24	Direct	Serial1	1006	-
10.1.1/24	10.20.30.2	Serial2	1002	99
10.2.1/24	10.20.30.3	Serial2	1003	66
10.3.1/24	10.20.30.3	Serial2	1004	66

5.3.1.3 Distribución de rutas de PE a CE

Después de pasar los respectivos filtros para distribuir las rutas de los PEs de egreso hacia los CEs, las tablas de enrutamiento en los CE quedan.

Tabla 5.25 Tabla de enrutamiento Enrutador CE Autos Coyoacan

Destination	Next-Hop	Interface
10.5.1/24	Direct	E0
0.0.0.0/0	10.5.0.6	Serial0

Tabla 5.26 Tabla de enrutamiento Enrutador CE DataCenter Coyoacan

Destination	Next-Hop	Interface
10.1.1/24	Direct	E0
0.0.0.0/0	10.1.0.6	Serial1

Tabla 5.27 Tabla de enrutamiento Enrutador CE DataCenter PolancoN

Destination	Next-Hop	Interface
10.2.1/24	Direct	E0
0.0.0.0/0	10.2.0.6	Serial0

Tabla 5.28 Tabla de enrutamiento Enrutador CE DataCenter PolancoS

Destination	Next-Hop	Interface
10.3.1/24	Direct	E0
0.0.0.0/0	10.3.0.6	Serial1

Tabla 5.29 Tabla de enrutamiento Enrutador CE Autos Centro

Destination	Next-Hop	Interface
10.1.1/24	Direct	E0
0.0.0.0/0	10.1.0.6	Serial0

Tabla 5.30 Tabla de enrutamiento Enrutador CE DataCenter Centro

Destination	Next-Hop	Interface
10.4.1/24	Direct	E0
0.0.0.0/0	10.4.0.6	Serial1

5.3.2 Esquema de pruebas para comprobación de operación de red

Las pruebas se limitan a la verificación de que un *host* en un sitio puede comunicarse con otro, perteneciente a la misma VPN pero que se encuentra en otro sitio.

Para lograrlo podemos hacerlo a través de tres sencillas aplicaciones.

- Telnet
- Ping
- Trace

Sin embargo, aquí se presenta un esquema que simula el viaje de un paquete IP de un sitio a otro. Este paquete podría ser de una sesión de telnet o de un simple *echo* ICMP.

5.3.2.1 Envío de tráfico VPN a través de la dorsal de red MPLS/VPN

Cuando un *host* (10.5.1.201) del sitio D. Autos ubicado en Coyoacan quiere comunicarse con su servidor (10.1.1.1) que esta en el sitio D. Autos ubicado en el Centro sucede lo siguiente.

El paquete IPv4 llega al CE D. Autos Coyoacan. Este realiza una revisión (*lookup*) de ruta *longest-match* en su tabla de envío IP. La mejor entrada en dicha tabla que iguala la dirección destino IP del paquete es la ruta por default:

Destination	Next-Hop	Interface
0.0.0.0/0	10.5.0.6	Serial0

Después de realizar el *lookup*, el dispositivo CE envía el paquete IPv4 al enrutador PE por la interface Serial0.

El enrutador PE recibe el paquete y realiza un *longest-match lookup* contra la tabla VRF asociada con la interface por donde llego la ruta. La entrada en la VRF Autos que más se parece a la dirección destino del paquete es.

Destination	BGP Next-Hop	Interface	Bottom Label	Top Label
10.1.1/24	10.20.30.1	Serial2	1005	99

Como la interface Serial2 no esta asociada a ninguna VRF, el paquete debe viajar al menos un salto en la dorsal de red MPLS/VPN para llegar a su destino. En enrutador crea un encabezado MPLS y le coloca la etiqueta MPLS con valor 1005 en el apilado de etiqueta MPLS. Después le coloca la etiqueta 99 que indica la LSP del PE Coyoacan a el PE Centro, siendo esta la última etiqueta.

El paquete es enviado hacia el primer LER (primer enrutador P) de la LSP. La dorsal de red intercambia (*swapping*) el valor de la etiqueta última del paquete etiquetado a través de la LSP hasta que alcanza el penúltimo enrutador hacia el PE Centro. La última etiqueta es extraída por el penúltimo enrutador y el paquete es enviado con una sola etiqueta hacia el enrutador PE Centro.

Cuando el PE Centro recibe el paquete sobre la interface serial2 este realiza un *lookup* en la tabla de envío MPLS. La entrada exacta que corresponde con la etiqueta del paquete entrante es.

Input Interface	Label	Action	Output Interface
Serial2	1005	Pop	Serial0

El enrutador PE Centro retira la etiqueta del paquete y lo envía como paquete IPv4 hacia el CE Autos.

Cuando el paquete arriba a este último dispositivo se realiza un *longest-match lookup* en la tabla de envío IP. La entrada que más se parece a la dirección destino del paquete en la tabla de envío del CE es.

Destination	Next-Hop	Interface
10.1.1/24	Direct	E0

Después de este último *lookup* el CE envía el paquete IPv4 hacia el servidor con dirección 10.1.1.1. A continuación se ilustra este proceso.

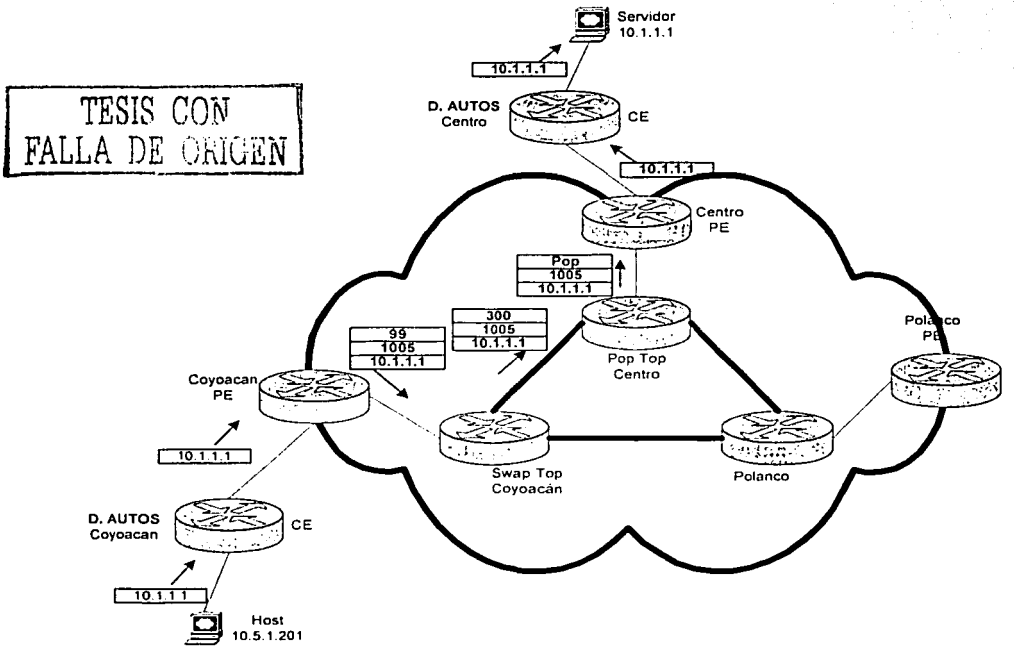


Figura 5.14 Envío de tráfico VPN a través de la dorsal de red MPLS/VPN

Conclusiones

En la actualidad es muy frecuente escuchar el término VPN, debido a la gran demanda de redes privadas por parte de empresas y organismos, y dada su fuerte inserción en el mercado de los Proveedores de Servicio (SP, *Service Providers*).

En muchos lugares se han percatado que las IP VPNs gestionadas representan un sustituto efectivo para las redes de área extensa (WAN, *Wide Area Network*) tradicionales, compuestas por una amalgama de tecnologías diferentes. Gracias a MPLS, las IP VPNs pueden ofrecer control de tráfico y calidad de servicio demostrando ser en la actualidad más escalables y económicas que las tecnologías FR y ATM.

Tradicionalmente, las VPNs no se consideraban como herramientas críticas para los negocios, dado que no podían igualar la calidad de servicio que garantizaban las líneas privadas. Dentro de la variedad de IP VPNs, las basadas en el protocolo IPSec, podían utilizarse para crear una WAN económica utilizando la Internet como medio de transporte. No obstante, este tipo de redes venían limitadas por el enfoque que supone la tecnología IP, del mejor esfuerzo (*best effort*), para transportar el tráfico. Esta tecnología no es aceptable para aplicaciones sensibles a retardos. Además de que resulta difícil monitorizar el tráfico de red a diferencia de los servicios WAN tradicionales.

El nuevo estándar MPLS, permite crear VPNs dentro de la red IP privada y compartida del SP. Gracias a ello, los usuarios empresariales pueden obtener beneficios en el recorte de costos que ofrece una infraestructura de red compartida y beneficiarse simultáneamente de un tráfico con unos niveles garantizados de latencia, pérdidas de paquetes, *jitter*, algo crucial para aplicaciones de tiempo real sobre IP, así como aplicaciones empresariales de misión crítica.

MPLS ha venido a impulsar las VPNs, en el enfoque de las empresas ya que son redes más económicas y rápidas, menos complejas, así como más adaptables y flexibles que las que pueda ofrecer cualquier tecnología WAN.

Desde el punto de vista del cliente, uno de los factores que debe considerar antes de seleccionar entre tecnología VPN es la aplicación ó función principal que desarrollará.

Entre las principales aplicaciones que utilizan las VPNs tenemos:

- Acceso remoto
- Conectividad sitio a sitio
- *Extranets*

En definitiva, a medida que las empresas y los negocios entran en el modelo de la globalización, las necesidades de comunicación remota a sitios centralizados de las propias

empresas se van haciendo más urgentes, provocando la demanda de tecnologías que brinden dicho servicio de manera confiable y segura.

El esquema de conectividad MPLS/VPN provee las siguientes ventajas de escalabilidad en relación a otros esquemas:

- Es muy escalable comparado con los modelos *Overlay*, ya que no son necesarios los circuitos virtuales que se configuran para brindar conectividad entre todos los equipos de frontera del proveedor de servicios.
- Los recursos de los enrutadores de acceso no se malgastan ya que estos mantienen exclusivamente una tabla de enrutamiento de las redes directamente conectadas y de las redes de los sitios que pertenecen a la misma VPN.
- Facilita el uso de direccionamiento privado para las empresas ya que dicho esquema provee soporte para el traslape de direcciones IP.
- La administración de red se vuelve simple ya que el SP no tiene una dorsal de red individual por cada cliente VPN.
- El asignamiento del RD provee la suficiente independencia para formar direcciones IP únicas dando a los SPs libertad para manejar su propio espacio de numeración IP.
- La característica de ORF reduce la cantidad de información distribuida a través de la dorsal de red del SP además de conservar los recursos de procesamiento de paquetes del enrutador.
- La dificultad de entablar sesiones MP-iBGP de mallas completas se soluciona con el desarrollo de RR[65].
- La arquitectura de MPLS permite aplicar servicios diferenciados, como son la capacidad de ofrecer distintos tratos a diferentes agregados de tráfico.
- El acceso a Internet se puede dar sin tener que replicar las rutas de Internet en las VRFs.

Estas ventajas se ven reflejadas en el incremento de velocidad para el transporte de paquetes de un lado al otro de la dorsal de red debido a que los paquetes son conmutados basándose en la revisión exclusivamente de valores de etiquetas, eliminando el proceso que realiza cada nodo de revisar en cada paquete la dirección destino.

El esquema implementado permite al SP:

- Ofrecer al cliente la posibilidad de expandirse cuando lo requiera realizando movimientos mínimos.
- Reducir costos en cuanto a sus implementaciones físicas.
- Ofrecer este servicio a múltiples clientes potenciales de VPNs con la misma infraestructura de red.
- Brindar con la misma infraestructura múltiples servicios derivando en ahorro de tiempo para la administración de dichos servicios así como mayor integración y escalabilidad.

La implementación del esquema es sencilla además de que la administración de este servicio generalmente recae en el SP lo que ocasiona que el cliente evite:

- Realizar gastos en la capacitación de su personal de red.
- Mantener un centro de administración para su servicio de VPNs.

En cuanto a la relación costo/beneficio, esta se mantiene en un nivel óptimo considerando que:

- El esquema MPLS/VPN se implementa en la infraestructura del SP, lo que independiza al servicio de VPN del equipamiento y la carga administrativa por parte del cliente.

[65] *Route Reflector*

- Al no requerirse un *hardware* específico ni "poderoso" para realizar funciones complejas e intensivas como la encriptación y/o autenticación de los datos, se disminuyen fuertemente los costos de la solución.
- En cuanto a la información de enrutamiento, el SP mantiene un conocimiento total de todos los sitios de una VPN y, de manera ágil y dinámica, se le informa a los CEs[66]. De esta forma la carga administrativa y compleja que implica el control de enrutamiento en el lado del cliente se transforma en algo sencillo, preciso y eficiente.

Estos beneficios determinan una óptima relación costo/beneficio, manteniendo un alto grado de rendimiento, siendo flexible y escalable para futuras necesidades, soportando distintas Clases de Servicio (CoS) para servir eficientemente las aplicaciones requeridas.

Al respecto de la implementación práctica desarrollada en el presente trabajo, podemos destacar lo siguiente.

- Lo primero en considerar fue el modelo de conexión requerido por el cliente, ya que en base a esto, fueron establecidas las políticas de comunicación entre los sitios de los clientes, además de que con esta información se ubicaron los puntos de acceso de la dorsal de red del Proveedor de Servicio.
- El dimensionamiento de los enlaces necesarios para interconectar el *backbone* fue importante debido a que este afecta directamente la capacidad del SP para que a futuro pueda brindar más servicios de los que ahora se necesitan, sin necesidad de actualizar o expandir la capacidad de dichos enlaces.
- Igualmente, el dimensionamiento de los enlaces para conectar los sitios de los clientes al *backbone* fueron realizadas en base a los requerimientos de transporte de tráfico de las aplicaciones de estos, considerándose además los costos de implementación y renta de los enlaces, asegurando así una solución con la mejor relación costo/beneficio.
- El servicio primario que el cliente requería, fue conectividad sitio a sitio todos con todos y gracias al esquema de MPLS/VPN, la configuración de los dispositivos de red para dar esta conectividad fue sencilla. Además es escalable dado que en el momento en el que se pretenda cambiar la topología a "hub & spoke" u alguna otra, no se tienen que realizar cambios en el diseño de red ya que la flexibilidad de dicho esquema permite realizar este tipo de cambios sin afectar el modo de operación del esquema.
- Por otra parte, al ser un servicio gestionado totalmente por el SP, en éste caso, el costo para los clientes no incluye la compra de equipo adicional (a diferencia de otras tecnologías), ni el soporte técnico que representa la administración de una red. Se trata, pues de una solución viable para aquellas empresas que no cuentan con los recursos para poder desplegar su propia red de servicios WAN.
- Las aplicaciones que ejecutan los clientes disponen de la tecnología suficiente de parte del SP para, en dado caso que lo requieran, usar aplicaciones en tiempo real, ya que MPLS tiene la capacidad de montar servicios diferenciados, de manera que se puede asignar clases de servicio de acuerdo a la aplicación que lo necesite. E igualmente, implementarlo es una tarea relativamente fácil dentro del dominio MPLS.
- El equipo del SP debe tener las características necesarias para soportar la tecnología usada, MPLS, además de contar con suficientes recursos para tener buen rendimiento al momento de dar servicio al cliente, como capacidad de procesamiento y memoria.
- Algo que no se ha especificado es que al momento de realizar los contratos con los SPs para obtener el servicio de MPLS/VPN es necesario revisar el SLA[67] (*Service Level Agreement*), mediante el cual el SP se compromete a dar el rendimiento requerido para las aplicaciones del cliente.

[66] CEs, Dispositivos de frontera perteneciente al cliente.

[67] Los SLAs ofrecen garantías de latencia máxima esperada, variación de latencia, entrega de paquetes y disponibilidad de ancho de banda.

- También es importante mencionar que la carga que representa a los dispositivos de red para la ejecución de MPLS no es significativa.

Respecto a las expectativas de las redes VPNs MPLS se piensa que su expansión es un hecho debido a la demanda de redes gestionadas y a que las empresas siguen desplegando un gran número de aplicaciones distribuidas de misión crítica, muchas de las cuales están basadas en IP. Todas ellas requieren amplia compatibilidad con redes IP para que las empresas con múltiples sitios puedan aprovecharlas al máximo.

Otro aspecto importante que determina el crecimiento de las redes VPN MPLS consiste en el hecho de que la separación tradicional entre voz y datos está desapareciendo gracias a las empresas que desean emplear la misma red para ambos tipos de tráfico, permitiendo reducir los costos relacionados con la implementación de redes separadas para cada tipo de información. A medida que las empresas sigan desplegando este tipo de redes convergentes en un número cada vez mayor de sitios, las VPNs MPLS se vuelven imprescindibles para interconectar las redes de forma transparente. A su vez, esto permite a las empresas realizar llamadas de voz y videoconferencias entre sitios sobre una red convergente.

Aunque las VPNs MPLS compiten directamente con las tecnologías de red tradicionales existentes como ATM o *Frame Relay*, también puede recurrirse a utilizarlas de modo conjunto. Por ejemplo, las empresas podrían utilizar una WAN MPLS basada en una combinación de tecnologías de acceso tradicionales y nuevas. De este modo, las empresas podrían conservar las inversiones realizadas en tecnologías tradicionales y desplegar nuevas tecnologías de acceso cuando fueran necesarias.

Sin embargo, la tendencia es que MPLS siga adentrándose profundamente en el mercado del ATM y FR, llevando un camino importante ya recorrido para convertirse en el estándar de facto para el núcleo de red. Y para aquellas empresas que no requieran mayor calidad de servicio, pero que sí se vean en la obligación de permitir a sus usuarios conectarse de forma segura a la red corporativa, deberán emplear las IP VPNs basadas en IPSec.

Glosario

ACL - Access Control List

Típicamente encontradas en elementos de red, permiten o deniegan el procesamiento de ciertos paquetes identificados por su dirección IP, puerto destino, etc.

ASN - Autonomous System Number

Número de Sistema Autónomo.

ATM - Asynchronous Transfer Mode

Modo de transferencia de alta velocidad basado en conmutación de celdas de tamaño fijo para transmitir datos, voz y video. Es asíncrono en el sentido de que la repetición de las celdas que contienen información de un solo usuario no es necesariamente periódica.

BGP - Border Gateway Protocol

Es un protocolo IP usado para intercambiar información de enrutamiento entre dominios de redes.

Componente de control - Control Component

Es una función realizada por un enrutador que hace y mantiene una tabla de envío y trabaja con otros componentes de control de otros nodos para distribuir la información de enrutamiento.

Componente de envío - Forwarding Component

Proceso de envío realizado por un enrutador que emplea una tabla de envío de etiquetas para enviar los paquetes entrantes a la red.

CPE - Customer Premises (o Provided) Equipment

Es el equipo ubicado en las instalaciones del cliente semejante a los sistemas de teléfono, modems, enrutadores y terminales. Para el caso de MPLS VPS se trata de enrutadores.

DLCI - Data Link Control Identifier

Etiqueta empleada por las redes FR para identificar cada circuito virtual de FR.

Dominio de enrutamiento - Routing Domain

Parte de una red que es controlada por un protocolo de enrutamiento específico.

Edge LSR - Edge Label Switch Router

Enrutador carrier-class localizado en la frontera de la red del carrier, el cual primero clasifica los paquetes IP y luego les asocia etiquetas.

EIGRP - Enhanced Interior Gateway Routing Protocol

Versión mejorada de IGRP desarrollada por CISCO. Provee capacidades de convergencia superiores además de gran eficiencia y combina las ventajas de los protocolos *link-state* con los *distance-vector*.

Enrutador

Dispositivo de capa 3 (capa de red) que mantiene una tabla de envío y enruta los paquetes a través de la red.

Enrutamiento - Routing

Acción de mover la información a través de la red desde un origen hasta un destino.

Enrutamiento explícito

La habilidad para seleccionar una ruta específica basándose en una política específica, en calidad de servicio o en la membresía de una red privada virtual y no en la ruta más corta o en la dirección destino.

FEC - Forwarding Equivalente Class

Grupo de paquetes que son tratados de igual forma cuando son transportados en la red.

Forwarding - Envío

Proceso de transmitir un paquete a través de una interfase hacia su destino sobre un enrutador o *switch*.

Frame Relay

Protocolo de transmisión de datos de lata velocidad usado por las redes WANs. Usado para interconectar redes LANs entre grandes distancias.

GRE - Generic Routing Encapsulation

Protocolo Genérico de Encapsulación para la formación de túneles IP.

IETF - Internet Engineering Task Force

Organización que provee la coordinación de estándares y especificaciones de desarrollo para redes TCP/IP.

IGP - Interior Gateway Protocol

Protocolo de Internet usado para intercambiar información de enrutamiento dentro de sistemas autónomos. Como ejemplos tenemos: IGRP, OSPF y RIP.

IP - Internet Protocol

Protocolo de capa 3 (capa de red) que contiene información de direccionamiento y alguna información de control que permite al paquete ser enrutado.

ISIS - Intermediate System - Intermediate System

Protocolo OSI de enrutamiento jerárquico de estado de enlace (*link-state*) donde los sistemas intermedios (enrutadores) intercambian información de enrutamiento basándose en una métrica única para determinar la topología de la red.

ISP - Internet Service Provider

Compañía que provee servicios de acceso a Internet a empresas o individuos.

Jitter

Variación del retardo.

Label - Etiqueta

Identificador de tamaño fijo que se usa para determinar como se envía un paquete.

Label Binding

Asociación entre una etiqueta y una FEC la cual ha sido advertida a los vecinos para establecer una ruta conmutada de etiquetas.

Label Switching

Termino genérico usado para describir el envío de paquetes IP usando algoritmos de envío de intercambio de etiquetas bajo el control de los algoritmos de enrutamiento de capa de red.

LDP - Label Distribution Protocol

Protocolo definido por la IETF diseñado para distribuir y marcar los cambios a etiquetas asignadas localmente y las FECs asociadas con ellas entre los LSRs adyacentes.

LER - Label Edge Router

Dispositivo de frontera de dominio MPLS encargado de etiquetar los paquetes entrantes al dominio y quitar las etiquetas de los paquetes etiquetados a su salida.

LSP - Label Switching Path

Conexión entre dos enrutadores que usan MPLS para transportar paquetes.

LSR - Label Switch Router

Es un dispositivo que soporta tanto los componentes de control estandar IP, como los protocolos de enrutamiento, y los componentes de envío de intercambio de etiquetas.

MPLS - Multiprotocol Label Switching

Estándar de conmutación de etiquetas desarrollado por un grupo de la IEFT.

NLRI - Network Layer Reachability Information

Información que describe una ruta y como llegar a ella. Se envía en los mensajes de actualización de BGP. Podría decirse que es un prefijo, en ese contexto. Un mensaje de actualización de BGP acarrea uno o más prefijos NLRI y los atributos de una ruta para los prefijos NLRI; los atributos de la ruta incluyen la dirección gateway del Próximo Salto BGP, valores de comunidades, entre otros.

OSPF - Open Shortest Path First

Protocolo de enrutamiento IP de estado de enlace.

PVC - Permanent Virtual Circuit

Circuito virtual que siempre esta disponible.

QoS - Quality of Servide

Se refiere a la capacidad para diferenciar entre el tráfico y los tipos de servicio para que uno o más clases de tráfico puedan ser tratados en forma diferente entre sí.

RIP - Routing Information Protocol

Protocolo de enrutamiento IGP que emplea la cuenta de saltos como métrica.

RD - Route Distinguisher

Valor de 8 bytes que es concatenado a una dirección IPv4 y sirve para crear direcciones VPNv4 únicas.

RSVP - Resource Reservation Protocol

Protocolo diseñado para reservar recursos de red y que provee calidad de servicio garantizado a ciertas aplicaciones.

RT - Route Target

Atributo de ruta que permite asociarla a una o a varias MPLS-VPNs específicas.

SNPA - Subnetwork Points of Attachment

Dirección de capa de enlace (como una dirección Ethernet, dirección X.25 o direcciones FR DLCI). Las direcciones SNPA se emplean para configurar una ruta CLNS para una interface.

SVC - Switched Virtual Circuit

Conexión entre dos puntos finales empleado por tecnologías de capa 2 que son orientadas a conexión como ATM o FR y que son ser dinámicamente establecidos.

Switching

Término general para la conmutación de paquetes, celdas o frames.

TCP - Transmisión Control Protocol

Protocolo de entrega confiable, ubicado en la capa 4 del modelo de referencia OSI, para la entrega de flujos de datos.

ToS - Type of Service

Grupo de bits en el encabezado IP que especifican un Tipo de Servicio.

Túnel

Conexión segura que habilita la transmisión de información encapsulada (regularmente en IP) y/o encriptada.

VIP - Versatile Interface Processor

Son tarjetas con 1 o 2 ranuras para conectar adaptadores de puertos en enrutadores CISCO (solo las series 7000, 7500 y 12000)

VPI/VCI - Virtual path Identifier / Virtual Channel Identifier

Campo en el encabezado ATM empleado para identificar el circuito virtual al cual una celda pertenece.

VPN - Virtual Private Network

Red Privada Virtual. Habilita enviar información en forma segura entre dos equipos ocupando la red pública o compartida de un SP.

VRF - Virtual Routing and Forwarding Instance

Una VRF consiste de una tabla de enrutamiento, una tabla de envio derivada, un bloque de interfaces que usan la tabla de envío y un bloque de reglas y protocolos de enrutamiento que determinan lo que la en la tabla de enrutamiento. En general, una VRF incluye la información de enrutamiento que define un sitio de cliente VPN que es agregado a un enrutador PE.

WAN - Wide Area Network

Es una red que se expande en un área geográfica amplia.

Bibliografía

Libros de Texto

- Internetworking Technologies Handbook, CISCO.
- MPLS and VPN Architectures, Jim Guichard y Ivan Pepelnjak, Cisco Press, USA, 2000. Capitulo 1, 2, 3, 7, 8 y 9.
- Multiprotocol Label Switching Architecture, E. Rosen, et al., January 2001.
- MPLS and Label Switching Networks, U. Black, ISBN 0130158232, Prentice Hall, 2001.
- User Guide for VPN Monitor, Apéndice A.

En la Internet

• Why Don't RIP and IGRP Support Variable-Length Subnet Mask? • Enhanced EIGRP • IGRP • OSPF • BGP-4 • Routing Basis • Open System Interconnection Routing Protocol • RIP • MPLS Virtual Private Networks (VPNs) • MPLS Architecture Overview (Presentación) • MPLS-QoS (Presentación) • Introduction to MPLS-BGP-VPN (Presentación) • MPLS-VPN Deployment Guidelines (Presentación) • MPLS-VPN Architecture Overview (Presentación)	www.cisco.com

• Intranets and Virtual Private Networks • Multiprotocol Label Switching • A comparison of MPLS Traffic-Engineering Initiatives • Virtual Private Networks • Glosario • Frame Relay and ATM WAN Technology • Introduction to Cisco MPLS VPN Technology	www.iec.org
• MPLS - An introduction to multiprotocolo label switching	www.nortelnetworks.com
• Las redes privadas virtuales	http://www.iies.es/
• Definiciones	http://www.cft.gob.mx/html/4_tar/globalcrossinglanding/GC-PL.html#R
• VPNs	www.servisoft.es/files/
• BGP/MPLS VPN • VPNv4 address family	http://www.ensc.sfu.ca/~ljilja/cnl/presentations/tony/BGP-MPLS-VPN/
• Estrategia de Cisco en el desarrollo de MPLS • Multi-Protocol Border Gateway • Protocol and IPv6 • RIP and EIGRP. Selecting IP Routing Protocols • Configuring MPLS and VPN • VPN Concepts • Which VPN solution is right for you? • Configuring a basic MPLS VPN • Multiprotocol BGP • BGP Update	www.cisco.com
• Layer 2 VPNs	www.ietf.org
• Enrutamiento	www.inf.utfsm.cl/~jcanas

White Papers

- Current Análisis. Tendencias emergentes en servicios de IP VPN. Ventajas para clientes derivadas de la aparición de productos más flexibles y con más funcionalidad. Compilado para EasyNet.
- Infonetics Research. Managed VPNs, Enhanced Revenue Opportunities for Service Providers, March 2002.
- IDC. Why IP Virtual Private Networks? Six key Benefits, December 2000.
- IFX Networks. MPLS/VPN.
- MIB para la arquitectura de servicios diferenciados (diffserv).
- Juniper Networks. Chuck Semeria, RFC 2547bis: BGP/MPLS VPN Fundamentals, 2001.
- NortelNetworks. MPLS - An Introduction to Multi Protocol Label Switching. USA, 2001.

- Marconi. Agregando más Valor a IP con Redes Orientadas a Conexión.

Internet Drafts

- RFC 791 - Internet Protocol
- RFC 1771 - Border Gateway Protocol 4 (BGP-4)
- RFC 1997 - BGP Communities Attribute
- RFC 2547 - BGP/MPLS VPNs
- RFC 3036 - LDP Specifications
- RFC 3107 - Carrying Label Information in BGP4
- RFC 3031 - Multiprotocol Label Switching Architecture
- RFC 2858 - Multiprotocol Extensions for BGP-4
- RFC 2475 - An Architecture for Differentiated Services
- RFC 3289 - Management Information Base for the Differentiated Services Architecture

Contacto

Cualquier aclaración con este documento favor de dirigirse al autor.

Ing. Jonathan Mora Cuevas.
e-mail: jon@hertz.fi-b.unam.mx
jmcplayer@hotmail.com
Tel. domicilio: 56-32-45-39

Octubre 2003.