UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"REDES PRIVADAS VIRTUALES BASADAS EN MPLS: UN CASO DE NEGOCIOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N :

JOSÉ ELÍAS ESCALANTE LOREDO

GUSTAVO ADOLFO ORTIZ SÁNCHEZ

DIRECTOR DE TESIS: ING. RODOLFO ARIAS VILLAVICENCIO

CO-DIRECTOR: ING. ARMANDO PALMA CABRERA

CIUDAD UNIVERSITARIA, JUNIO 2004

Quiero agradecer ...

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería; *por ser mi segunda casa y haberme convertido en un excelente profesionista, dándome las herramientas suficientes para enfrentar futuros retos. Así como a todos los profesores; por su trabajo y esfuerzo brindado para adquirir dichas herramientas.*

A mi madre y padre; *por su infinito cariño y amor que me han brindado durante toda mi vida, y que sin su apoyo incondicional no me encontraría en este punto de mi vida. Espero de esta forma retribuirles un poco de lo mucho que me han dado.*

A mi hermano Juan Pablo; *por su incomparable amistad y gran compañía que me ha regalado durante todo este tiempo, y al cual lo considero como una de las personas más importantes en mi vida.*

A Nadia del Carmen Cervantes Gil; *por el invaluable amor que me ha demostrado durante todo este tiempo que he compartido con ella, por ser mi inspiración en muchos aspectos pero sobre todo por comprenderme y apoyarme en todo momento.*

A mi director de tesis Ing. Rodolfo Arias Villavicencio y a mi codirector de tesis Ing. Armando Palma Cabrera; *por permitirme realizar este trabajo de tesis con ellos y por haber compartido parte de su gran conocimiento con nosotros.*

A mi compañero de tesis Gustavo A.; *por su gran amistad y por su enorme paciencia al realizar este proyecto de tesis, además por haber compartido grandes momentos inolvidables durante toda la carrera.*

A todos mis compañeros y amigos; *por haberme concedido la fortuna de conocerlos y de compartir muy buenos momentos durante gran parte de mi vida y durante la carrera, en especial a: Arturo Maraboto, Carlos Calzada, Gerardo Sánchez, Raúl Parra, Verónica Santillán, Beatriz Flores, Odette Valenzuela y a todos los que no menciono pero saben que los tengo muy presentes.*

José Elías Escalante Loredo

Quiero agradecer ...

A mi abuela y mi madre.

A mi tío y toda mi pequeña familia, *por supuesto.*

A José Elías, *mi compañero y gran amigo por terminar este viaje y muchos otros; si hubiera querido un hermano me hubiera gustado que fuese como tú. Muchas Gracias*

A Carlos Calzada y Gerardo Sánchez, *mis grandes amigos, porque la escuela no hubiera sido la misma sin ustedes. Gracias por caminar conmigo en este viaje.*

A Beatriz, *"lo cierto es que lo realmente importante ni siquiera se dice".*

A mis compañeros de la Facultad de Ingeniería, *a las generaciones 98-1 y 98-2 de ingeniería en Telecomunicaciones de los cuales aprendí, me acompañaron y ayudé en la medida de mis posibilidades; en especial a Verónica Santillán, Odette Valenzuela, Rogelio Torres, Edson González, Miguel Palomera, Antelma Mercado, Paulo López, Carlos Pérez Roa, y todos lo demás de los cuales no recuerdo el nombre, pero queda el recuerdo.*

A todas las personas que conocí en Telmex en la Red Corporativa de Datos, *en especial a Rodolfo Arias y Armando Palma, gracias por la oportunidad de conocerlos y aprender de ustedes.*

A "Luz de día" y "I miss you", *por ser inspiración, motivación y en su momento compañía, muchas gracias.*

A la Facultad de Ingeniería y a la UNAM *por darme todo, sin pedirme nada a cambio excepto mi constancia. Al Departamento de Telecomunicaciones en especial al Dr. Miguel Moctezuma; al personal que allí labora.*

Gustavo A. Ortiz Sánchez

"Todo debería de ser pensado por un ingeniero hasta el último detalle"

"Los científicos descubren el mundo que existe;
los ingenieros crean el mundo como nunca fue"

- Theodore von Karman

"Un científico puede descubrir una nueva estrella, pero él no puede hacer una.
Tendría que preguntarle a un ingeniero como hacerlo"

- Gordon L. Glegg

"... los ingenieros operan en la interfaz entre la ciencia y la sociedad ..."

- Dean Gordon Brown

"El primer problema de un ingeniero en cualquier situación de diseño
es descubrir cuál es realmente el problema"

Índice

Introducción

En esta ya larga *"era de la informática"*, las redes de computadoras han facilitado en gran medida la comunicación entre los individuos ya sea de forma personal o dentro de una empresa o varias, permitiendo compartir grandes cantidades de información a una velocidad sorprendente. Esta rápida evolución de comunicarse nos ha llevado a mejorar nuestras condiciones de vida, pero sobre todo ha logrado incrementar la productividad empresarial en muchos sectores del mercado.

La aplicación de las tecnologías de la información y de las telecomunicaciones en el ámbito de la gestión empresarial y de la educación principalmente, ha llevado a múltiples organizaciones a preocuparse por mejorarlas y a realizar nuevos diseños.

Conforme las empresas han logrado expandirse, se ha establecido una necesidad de comunicación entre sus nuevas entidades. Dependiendo del tamaño de la empresa se puede considerar conveniente o no, la implementación de su propia red. Basándose en esto, muchas empresas dedicadas a proveer servicios de comunicaciones deciden ofrecer un servicio de conectividad de manera que las empresas que no podían tener su propia red privada, ahora pueden rentar la infraestructura de un Proveedor de Servicios para lograr la comunicación tan buscada.

Es por eso que surgen las Redes Privadas Virtuales (VPNs), éstas constituyen una alternativa económica y flexible para la conexión de empleados, oficinas y delegaciones remotas a la red local central de la empresa. Las empresas pueden desentenderse de la complejidad y costos asociados a la conectividad telefónica y las líneas dedicadas punto a punto.

Sin embargo, una VPN basada en redes públicas puede presentar problemas relacionados con la seguridad de las comunicaciones, el ancho de banda disponible o la Calidad de Servicio – Quality of Service (QoS) requerida. Esto por la propia naturaleza de las redes públicas usadas como soporte a la VPN, ya que se comparte el canal de comunicación con una gran cantidad de usuarios que podrían tener acceso a los datos de la organización si no se empleasen las medidas y protocolos de seguridad adecuados.

Es ahí donde entra en escena la arquitectura MPLS, ya que como se verá más adelante, además de ser un modelo mejorado de enrutamiento, permite la implementación de varios servicios, entre ellos las VPNs. La implementación de VPNs con esta tecnología permite reunir las mejores características de varios protocolos de enrutamiento empleados hasta antes de la creación de MPLS. Podemos decir que obtenemos seguridad por medio del aislamiento de la información que pertenece a cada diferente cliente, además de simplificar el proceso de enrutamiento.

La primer parte de esta tesis presenta un extracto completo de diversos conceptos teóricos relativos a las redes. Entre estos están los implicados en el diseño de una nueva red o actualización de una ya existente mediante el empleo de un método conocido como *Top-Down*. Posteriormente se hablará de los diferentes protocolos de enrutamiento que se continúan empleando; para de esta forma llegar a realizar un análisis minucioso de la arquitectura del protocolo MPLS y emplearla como una alternativa para crear una Red Privada Virtual (VPN) empleando la infraestructura de una empresa proveedora de servicios, y así lograr la comunicación entre los sitios de un cliente. Para finalizar esta parte teórica se complementa el trabajo con un tema interesante y de gran importancia en la transmisión de datos, nos referimos a QoS.

Es importante señalar que a pesar de que el trabajo comienza con conceptos y definiciones fundamentales, es aconsejable que el lector tenga conocimientos de conceptos básicos y características generales de las redes, incluyendo una introducción a la serie de protocolos de comunicaciones que se ven relacionados con éstas, para poder llegar a comprender de una forma más efectiva el contenido de este trabajo.

Dado que dentro de los objetivos de esta tesis está el de resolver un problema de ingeniería aportando una solución viable, toda esta base teórica nos servirá de apoyo para proponer dicha solución.

Se expondrá la problemática de una empresa cuyo campo de trabajo es la de ofrecer servicios de capacitación, y entre sus proyectos tiene contemplado un esquema de actualización tecnológica capaz de soportar los servicios que brinda a otras dependencias.

Es decir, se tratará un caso de negocios, en el cual se tendrá la oportunidad de demostrar el funcionamiento de las Redes Privadas Virtuales basadas en MPLS aplicándose en un problema real, e incluso esta misma solución puede ser aplicada en algún otro giro del sector empresarial que no sea precisamente el educativo como por ejemplo: el financiero, gubernamental o industrial sólo por mencionar algunos.

En la última parte del trabajo se detallará la situación de la empresa *E-Education*, analizando sus requerimientos y posteriormente se dará a conocer la propuesta conocida como *VPN E-Education* diseñada por la empresa *Red Maestra de Datos SysTel (RMDST)* para resolver la situación. Al definir una solución en particular se justificará el diseño del proyecto y se describirán los pasos para implementarlo incluyendo las configuraciones necesarias para lograrlo.

CAPÍTULO UNO
Planteamiento del problema

1.1 Definición del problema.

E-Education es una de las empresas que forman al conocido grupo *Smart Solutions* y el papel que desempeña dentro de éste, es el de brindar capacitación al personal del resto de las empresas del grupo. Sin embargo recientemente la dirección del grupo ha pensado en expandir la oferta de sus servicios más allá del grupo *Smart Solutions* y consolidarse como un fuerte competidor dentro del mercado de capacitación en México. *E-Education* basará su estrategia en aprovechar los adelantos tecnológicos disponibles actualmente lo que permitiría tener costos de operación bajos que se reflejarían en precios atractivos al cliente y esto sin sacrificar el margen de ganancia.

Dentro de los proyectos contemplados en el esquema de actualización tecnológica de *E-Education* se tiene la creación de la *Red E-Education de Siguiente Generación* que de hecho será la base primordial para soportar los nuevos servicios ofrecidos por *E-Education.*

1.2 Propuestas de la solución.

Dentro de las opciones para la solución del problema están las siguientes:

1. Construcción de una red propia con enlaces dedicados.

    a. Ventajas:

        i. Administración de la red.
        ii. Confidencialidad de la información crítica de la empresa.

    b. Desventajas:

        i. Inversión inicial muy alta.
        ii. Costos de operación altos.
        iii. Se requiere de formar recursos de alto nivel que se hagan cargo de la operación de la red, tomando en cuenta los costos en personal que ello implica.

2. Creación de una Red Privada Virtual con la infraestructura ofrecida por un Proveedor de Servicios.

    a. Ventajas:

        i. La operación y el mantenimiento de la red es responsabilidad del proveedor que cuenta con recursos de alto nivel.
        ii. Inversión inicial moderada.
        iii. Costos de operación marginales.
        iv. *E-Education* puede destinar parte de los recursos que ahorre al desarrollo de otras áreas en su negocio.
        v. Cobertura nacional.

    b. Desventajas

        i. Los costos se pueden incrementar en base al nivel de servicios requeridos por la empresa. Tiempo de atención para fallas, mayor ancho de banda, niveles de Calidad de Servicio bajo demanda, etc.

1.3 Resultados esperados.

1. Reducción de costos de operación.

   - Gastos generados por el desplazamiento del personal requerido en el modelo actual de la empresa, tales como: traslado, hospedaje, alimentación, etc.

   - Apertura y/o mantenimiento de centros regionales de capacitación: renta de oficinas, acondicionamiento de aulas, pago de servicios, pago de personal administrativo, etc.

2. Aumento en la productividad de la empresa, dado que sus empleados no emplearán más tiempo en desplazarse hacia el centro de capacitación, ubicado en las oficinas regionales de capacitación.

   - En capacitación: permitirá acceso remoto a materiales de apoyo contenidos en bibliotecas digitales (libros, manuales, vídeos), laboratorios, etc.

   - En tareas administrativas: ayudará a reducir los tiempos para realizar actividades tales como cierres mensuales, pago de nómina, control de asistencia, localización del personal en caso de contingencia, entre otras.

   - En la comunicación: logrará una comunicación ágil entre el personal encargado de la logística de los cursos.

3. Elevar la calidad de los cursos de capacitación y actualización que imparte la empresa.

4. Crear una ventaja competitiva con respecto a otras empresas dirigidas al mismo segmento de mercado.

CAPÍTULO DOS
Planteamiento teórico

2.1 Diseño de redes empleando el método Top-Down.

El método *Top-Down* puede ser definido como un proceso sistemático empleado por diseñadores que desean crear nuevas redes o modificar las ya existentes de una forma eficiente. Lo importante de este método, es que el diseño se enfoca en los requerimientos del cliente así como en sus objetivos técnicos y comerciales incluyendo sus restricciones. Entre algunos de estos requerimientos podemos mencionar: escalabilidad, alta disponibilidad, desempeño, seguridad, rentabilidad, y facilidad de administración de la red. Este proceso sistemático del diseño de redes se enfatiza en la planeación de la evolución de éstas, inclusive antes de su implementación.

Top-Down es una metodología que ayuda a diseñar una perspectiva lógica de la red, incluyendo descripciones de los flujos de tráfico y las topologías, antes de desarrollar la perspectiva física. Es por eso que el diseño de redes comienza en las capas superiores del Modelo de Referencia OSI antes de desplazarse hacia las capas inferiores. Se enfoca en aplicaciones, sesiones y transporte de datos antes de la selección de enrutadores, switches y medios de comunicación que operan en capas inferiores.

Dicho de otra forma, el método *Top-Down* permite primeramente al diseñador obtener una enorme foto del proyecto y después ir detallando dicha foto basándose en los requerimientos y especificaciones técnicas. La parte fundamental del método *Top-Down* y con lo que se comienza un buen diseño de redes es conocer las necesidades y metas del cliente.

2.1.1 Análisis de las metas y restricciones comerciales.

El primer paso en el diseño de redes es analizar las metas comerciales del cliente, entre las cuales se pueden incluir la capacidad de correr aplicaciones de la red para satisfacer los objetivos comerciales de la empresa y la necesidad de trabajar con restricciones como son: los presupuestos, el tener personal de redes limitado, además de un reducido margen de tiempo para la implementación del proyecto.

2.1.1.1 Análisis de las metas comerciales.

El diseño final de la red debe reflejar la estructura empresarial, por lo tanto es buena idea el tener presente como está estructurada la empresa de nuestro cliente: departamentos, relaciones con proveedores, socios, y oficinas remotas. El entender como está conformada la empresa ayuda a localizar las comunidades de mayores usuarios y a caracterizar los flujos de información.

El cliente debe de tener una meta global del proyecto, por lo tanto se le debe requerir una expectativa orientada al negocio que puntualice el propósito de la nueva red.

El que muchos empresarios estén pensando en crear o modificar una red en su empresa se basa en el hecho de que recientemente se ha reconocido la necesidad de aumentar la disponibilidad de las grandes cantidades de datos para los empleados, clientes y socios; ya que de esta forma se pueden tomar decisiones estratégicas más acertadas y en un menor tiempo.

Dentro de las metas comerciales típicas relacionadas con el diseño de redes se pueden mencionar: aumentar ingresos y beneficios, mejorar las comunicaciones empresariales, obtener ciclos cortos en el desarrollo de productos y aumentar la productividad de los empleados, crear asociaciones con otras compañías, expandirse a los mercados en todo el mundo, desplazarse hacia modelos comerciales de redes globales, hacer los datos disponibles para todos los empleados y oficinas para que se puedan tomar mejores decisiones en los negocios, mejorar la seguridad y la confiabilidad de los datos así como de las aplicaciones críticas, y por último ofrecer un mejor soporte y nuevos servicios a los clientes.

Otro punto importante en el comienzo del diseño de la red es determinar su alcance, por eso es necesario saber si el diseño es para la creación de una nueva red o la modificación de una existente. También es necesario preguntar si el diseño es de un sólo segmento, de un conjunto de LANs, de un conjunto de WANs o de toda la red de la empresa.

Ahora es tiempo de enfocarse en las aplicaciones, que es realmente la razón por la cual la red existe. Al inventariar las aplicaciones del cliente se deben incluir tanto aplicaciones actuales como nuevas. Dichas aplicaciones pueden ser:

- **Del usuario:** correo electrónico, transferencia de archivos, terminales remotas, videoconferencia, comercio electrónico, educación a distancia, acceso a base de datos, etc.

- **Del sistema:** autentificación y autorización de usuarios, administración de la red, distribución de software, respaldo de la red, etc.

Entre las cuales se debe de establecer una jerarquía de las extremadamente críticas hasta las no críticas.

2.1.1.2 Análisis de las restricciones comerciales.

Un tema que es difícil de tratar con el cliente y en el cual no se puede opinar del todo es el referente a las políticas de la empresa, en donde es mejor escuchar que hablar. Es necesario conocer este tipo de información, ya que pueden existir una serie de factores totalmente ajenos al trabajo del diseñador que están fuera su alcance y que lleguen a limitar el correcto desarrollo del proyecto. Entre la información que se podría investigar está: la existencia de problemas en las oficinas, las relaciones entre los grupos, así como averiguar si hay personal que no esté de acuerdo con la realización del proyecto.

Otro punto importante es el discutir con el cliente sobre cualquier política referente a protocolos, estándares y proveedores. En muchos casos, una compañía ya tiene seleccionada la tecnología y productos para la nueva red y por lo tanto el diseño de la red debe de encajar con el presupuesto del cliente, se debe tener contemplado: nuevo equipamiento, licencias de software, mantenimiento y soporte, pruebas, capacitación de personal, honorarios y gastos de *outsourcing*[1].

Finalizando con esta parte, se necesita determinar con el cliente una fecha de entrega del proyecto. El diseñador debe de ser capaz de cumplir con este punto, ya que existe la posibilidad de penalización en caso de que no se cumpla.

[1] Es un sistema empleado por grandes empresas, las cuales rentan el servicio de otras empresas para efectuar proyectos pequeños en vez de ellas.

2.1.2 Análisis de las metas y restricciones técnicas.

El análisis de este tipo de metas y restricciones nos ayudará a recomendar a nuestro cliente de una forma más confiable, el tipo de tecnologías que cumplan con sus expectativas. Este tipo de metas técnicas incluyen: escalabilidad, disponibilidad, desempeño, seguridad, administración, facilidad de uso, adaptabilidad, y rentabilidad; como es de esperarse, debe de existir un equilibrio asociado con estas metas.

2.1.2.1 Escalabilidad.

La escalabilidad se refiere a la capacidad de crecimiento que debe soportar nuestro diseño de red. El diseño de la red propuesto debe de ser capaz de adaptarse a incrementos en el uso y en los alcances de la red.

En cuanto a las restricciones en la escalabilidad pueden existir algunos impedimentos inherentes en el tipo de tecnología que se esté empleado en la red.

2.1.2.2 Disponibilidad.

Este término se refiere a la cantidad de tiempo que una red está accesible al usuario y regularmente es un objetivo relevante para el cliente. La disponibilidad está relacionada con la confiabilidad, la cual se refiere a una variedad de cuestiones, incluyendo: precisión, tasa de error, estabilidad y el total de tiempo existente entre fallas. Un ingrediente de la disponibilidad es la recuperabilidad, la cual especifica que tan fácilmente y en que margen de tiempo una red se recupera de problemas. Otro aspecto importante que implica la disponibilidad es la capacidad de recuperación de desastres; un plan de recuperación de desastres incluye un proceso para mantener la información respaldada en un lugar seguro, así como también un proceso para cambiar a tecnologías de respaldo si la principal tecnología es afectada por un desastre.

Se debe alentar al cliente a que especifique los requerimientos para la disponibilidad con precisión. Es también importante especificar el porcentaje del tiempo requerido en la actividad de la red. En caso de requerir un período de inactividad ya sea por mantenimiento, actualización u otro aspecto convendría que no fuera continuo, lo que podría ser un problema, en vez de esto que la inactividad sea esparcida en pequeños intervalos a lo largo de un período.

Un punto muy importante para el cliente es el costo que implica el tiempo de inactividad, ya que esto se ve reflejado en pérdidas de dinero por parte de la empresa. En general, el objetivo de la disponibilidad de una red para el cliente es tener sus aplicaciones con tareas críticas corriendo sin problemas, con un tiempo de inactividad muy pequeño o nulo. Especificando que costo tiene el tiempo de inactividad de una red, nos permitirá clarificar si se soporta una actualización o mantenimiento a la red mientras se encuentra operando.

2.1.2.3 Desempeño de la red.

Cuando se analizan los requerimientos técnicos para el diseño de la red, se debe identificar el criterio del cliente en cuanto al desempeño de la red, incluyendo el rendimiento, fiabilidad, eficiencia, retraso y el tiempo de respuesta. Muchas veces analizar la red existente ayudará a determinar que cambios necesitan hacerse para alcanzar los objetivos de desempeño. Se debe lograr un entendimiento del plan de crecimiento de la red antes de analizar las metas de desempeño.

A continuación se darán algunas definiciones que caracterizan un buen desempeño de la red, tomando en cuenta sus requerimientos y restricciones:

a. Utilización óptima de la red.

La utilización óptima de la red es una medida de que tanto ancho de banda es usado durante un período específico de tiempo. La utilización es comúnmente especificada como un porcentaje de capacidad.

Para redes WAN, una utilización óptima de la red es del 70 por ciento. Muchos clientes tienen varias opciones para reducir la utilización del ancho de banda de la red WAN incluyendo: características avanzadas de protocolos de enrutamiento, compresión, Supresión de Patrones Repetitivos – Repetitive Pattern Supression (RPS), y Detección de Actividad de Voz – Voice Activity Detection (VAD).

b. Rendimiento.

El rendimiento está definido como la cantidad de datos libres de errores que es transmitida por unidad de tiempo. El rendimiento es por lo regular definido para una conexión o sesión específica, pero en algunos casos se puede especificar el rendimiento total de una red. Idealmente, el rendimiento debe ser el mismo que la capacidad de la red, éste depende de métodos de acceso (por ejemplo *token passing* o detección de colisión), de la carga en la red y de la tasa de errores. Cuando se habla del rendimiento en los dispositivos de la red se está refiriendo a la tasa máxima a través de la cual el dispositivo envía paquetes sin tirar ninguno de ellos.

c. Fiabilidad.

La fiabilidad es una meta global en la que los datos recibidos en el destino deben ser los mismos a los datos enviados por la fuente. Causas típicas de errores de datos incluyen, picos de tráfico, problemas de acoplamiento de impedancias, conexiones físicas deficientes, dispositivos descompuestos, y ruido causado por maquinaria eléctrica. Algunas veces, los *bugs*[2] del software pueden causas errores de datos también.

Para enlaces WAN, los objetivos para lograr la fiabilidad o la precisión pueden ser especificados como un umbral en la Tasa de Bits de Error – Bit Error Rate (BER). Para

[2] Se refiere a los errores de escritura en los programas que producen fallas en los sistemas.

LANs un límite aceptable para usarse, es que no debe de haber más de una trama dañada por cada millón de bytes de datos.

d. Eficiencia.

En cuanto a la eficiencia, es una medida de que tan efectiva es una operación en comparación al esfuerzo, energía, tiempo o dinero invertido para producir un resultado esperado. La eficiencia de la red especifica que tanta información adjunta es requerida para enviar tráfico por la red, ya sean avisos por colisiones, redireccionamiento, mensajes de confirmación, grandes encabezados de tramas, etc.

Una forma de que exista un buen desempeño de la red, es que las aplicaciones deben de minimizar la cantidad de ancho de banda utilizado por encabezados usando las tramas más grandes posibles y que la Capa MAC lo permita. Pero hay que tomar también en cuenta que entre más grande sea la trama, más ancho de banda se desperdiciará en la retransmisión. Por eso, como las redes experimentan errores, los tamaños de las tramas están limitados a una eficiencia máxima. Dependiendo la tecnología empleada se puede revisar en tablas el tamaño máximo válido de la trama.

e. Retraso y su variación.

Otro rasgo importante dentro del desempeño de una red, es el retraso y su variación. El uso de aplicaciones interactivas requiere de un mínimo retraso en la recepción de información de realimentación de la red. En adición a esto, usuarios de aplicaciones multimedia requieren de una variación mínima en la cantidad de retraso que experimentan los paquetes. El retraso debe de ser una restricción para aplicaciones de voz y vídeo. Variaciones en el retraso, usualmente llamadas *jitters*, causan interrupciones en la calidad de voz y vídeo. Se debe determinar si el cliente planea correr cualquier aplicación basada en protocolos sensibles al retraso, como Telnet o SNA.

El retraso es relevante para todas las tecnologías de transmisión de datos, de ahí que surja la importancia y necesidad de conocer las bases físicas que lo originan. Este punto es de gran importancia especialmente cuando se trabaja con enlaces satelitales, y cables terrestres largos; ya que el retraso se debe a las grandes distancias que recorren los datos para llegar a su destino. Otro tipo de retraso fundamental es el que existe a la hora de enviar datos digitales en líneas de transmisión, en donde el retraso depende del volumen de datos y de la velocidad que soporte la línea. Adicionalmente a este retraso, existe el que se origina en la conmutación de paquetes, lo cual se refiere a la latencia acumulada cuando los bridges, switches, y enrutadores transmiten datos. La latencia depende de la velocidad de la circuitería interna y del CPU de estos dispositivos, así como de la arquitectura de conmutación de los dispositivos de la red.

El retraso debido a la conmutación de paquetes, también incluye el retraso debido a que en algunos casos los paquetes son enviados a una cola. Alternativamente, para mejorar el desempeño de una red, se pueden usar algoritmos avanzados para encolar, es decir poner a la salida ciertos tipos de paquetes primero, por ejemplo de voz y vídeo.

Así como el retraso es imposible de desaparecer, la variación de éste también, pero se puede jugar con este último para mejorar la transmisión de datos. Las aplicaciones pueden minimizar el *jitter* proveyendo un *buffer*[3] en el cual se almacenen los datos. El empleo de *buffers* reduce el efecto de parpadeo o de interrupciones por que las variaciones en la entrada son más pequeñas que el tamaño total de *buffer* y por consiguiente no hay ninguna variación en la salida. Una buena regla general es que la variación debe ser menor que el uno o dos por ciento del retraso.

f. Tiempo de respuesta.

Los clientes no saben acerca del rendimiento, no entienden la tasa de errores de bits, ni la propagación de retrasos, pero si identifican la cantidad de tiempo para recibir la respuesta de un sistema de la red. También identifican los pequeños cambios en el tiempo de la respuesta esperada y se tornan frustrados cuando ésta es muy larga. Si la respuesta se tarda en llegar menos de 150 [ms], muchos usuarios no lo notarán. Es por eso que es usualmente usada como un valor de tiempo para varios protocolos que ofrecen un transporte de datos seguro. La respuesta en el tiempo de 150 [ms] es un umbral que se emplea en aplicaciones interactivas como por ejemplo: Voz sobre IP (VoIP).

2.1.2.4 Seguridad.

Los clientes necesitan asegurarse de que el diseño ofrece protección contra las pérdidas y daños que puedan sufrir sus datos. Cada compañía tiene sus secretos de negocios, operaciones comerciales y equipo que proteger. La primera tarea en el diseño de seguridad es la planeación. La planeación envuelve el análisis de riesgos y el establecimiento de condiciones de acceso a las fuentes de información y componentes de la red.

Como las compañías se conectan al Internet, necesitan considerar los riesgos adicionales de que gente externa se introduzca a la red de la corporación y le haga algún daño. Clientes que accedan de sitios remotos a través de Redes Privadas Virtuales – Virtual Private Networks (VPNs) necesitan analizar las características de seguridad que el Proveedor de Servicios VPN ofrece. Por otro lado, *hackers*[4] tienen la habilidad de acceder y cambiar datos en la red delicados para la empresa.

Las compañías deben poner especial cuidado en problemas causados por los usuarios de la red que son ineptos o maliciosos. Las compañías reportan que los virus, es la causa más significante de problemas, esto está seguido de actos maliciosos de usuarios internos.

Existen varios requerimientos de seguridad para lograr prevenirse de estos riesgos, un requerimiento primario es proteger recursos (servidores, sistemas de usuario, dispositivos de la red, datos, etc.) de que queden incapacitados, robados, alterados o dañados. Otros requerimientos específicos podrían ser: no permitir a gente externa que acceda a los datos internos, autorizar y autentificar a los usuarios, detectar intrusos y aislar el daño que logren

[3] El buffer es un espacio de memoria para el almacenamiento temporal de datos.
[4] Piratas informáticos.

hacer, autentificar actualizaciones de las Tablas de Enrutamiento recibidas de enrutadores internos o externos, proteger datos transmitidos de sitios remotos a través de VPNs, asegurar físicamente los servidores y dispositivos de la red, proteger aplicaciones y datos de virus, etc.

2.1.2.5 Administración.

Se puede emplear la siguiente terminología de ISO[5] para definir las funciones de administración de una red y que pueden encajar con los requerimientos de un cliente. Entre ellas están:

- La administración de desempeño, que es el análisis del comportamiento del tráfico y de las aplicaciones para optimizar la red.
- La administración de falla que es la detección, aislamiento y corrección de problemas. Los problemas son reportados por los usuarios finales y los administradores.
- La administración de configuración, siendo ésta el control, operación, identificación y colección de datos de los dispositivos administrados.
- La administración de seguridad, que se encarga del monitoreo y pruebas de seguridad así como también de las políticas de protección, mantenimiento y distribución de contraseñas además de otra información de autentificación y autorización.
- La administración de contabilidad, encargada de llevar las cuentas del uso de la red para asignar costos a los usuarios de la red y/o planear cambios en los requerimientos de la capacidad.

2.1.2.6 Funcionabilidad.

Se refiere a la facilidad de uso con la cual los usuarios de la red pueden acceder a la red y sus servicios. Mientras que la administración se enfoca en hacer el trabajo fácil a los administradores, la funcionabilidad se enfoca en hacerlo a los usuarios.

2.1.2.7 Adaptabilidad.

Un buen diseño de red puede adaptarse a nuevas tecnologías y cambios. Estos pueden venir en forma de nuevos protocolos, nuevas prácticas de negocios, nuevas metas fiscales, nueva legislación e innumerables posibilidades. La adaptabilidad de la red afecta a la disponibilidad. Una red que no se puede adaptar no puede ofrecer buena disponibilidad.

Un diseño flexible de la red es también más fácil de adaptarse a patrones de tráfico cambiantes y a requerimientos de Calidad de Servicio. Otro aspecto de la adaptabilidad es que tan rápidamente los dispositivos de la red se pueden adaptar a los problemas y a las actualizaciones.

[5] Organización Internacional para la Normalización – International Organization for Standarization (ISO).

2.1.2.8 Rentabilidad.

La rentabilidad es en parte una meta comercial. El principal objetivo de la rentabilidad es transportar la máxima cantidad de tráfico dado un costo financiero. Dependiendo la aplicación que corra en el sistema final, los bajos costos son usualmente más importantes que la disponibilidad o el desempeño en el diseño de las redes como es el caso de las instituciones educativas. Para las redes empresariales, la disponibilidad es usualmente más importante que los bajos costos.

Para disminuir los costos de operación de una WAN se pueden tener en cuenta los siguientes objetivos: emplear protocolos de enrutamiento para reducir tráfico como es el caso de MPLS[6], que dichos protocolos seleccionen rutas de mínima tarifa, seleccionar tecnologías que asignen dinámicamente ancho de banda, mejorar la eficiencia en los circuitos WAN usando algunas características como compresión, Detección de Actividad de Voz y Supresión de Patrones Repetitivos entre otros.

El segundo aspecto, es el costo de contratación, capacitación y mantenimiento de personal para operar y administrar la red. Para reducir este aspecto, se puede seleccionar equipo que sea fácil de configurar, operar, mantener y administrar; seleccionar un diseño de red que sea fácil de entender y de arreglar; mantener una buena documentación de la red para reducir el tiempo de reparación, seleccionar aplicaciones de red y protocolos que sean fáciles de usar para los usuarios, etc.

2.1.2.9 Equilibrio en las metas.

Se debe de hacer un equilibrio en las metas que se espera del diseño de la red, es decir como existen pros y contras, éstos deben de interrelacionarse unos con otros. Por ejemplo, en la disponibilidad, componentes de redundancia son necesarios, pero aumentan el costo; si se requiere de un riguroso desempeño, circuitos y equipo requerido eleva el costo; reforzar las políticas de seguridad, requiere de monitoreo y de que los usuarios deben olvidarse de la facilidad de uso.

Para ayudarse a analizar los equilibrios que deben de existir, el cliente debe identificar antes que nada un objetivo del diseño de la red que él considere de suma importancia para su empresa. Se deberá priorizar el resto de las metas. Priorizando, se puede ayudar al cliente en el proceso de equilibrar o jerarquizar algunas metas. Se le debe preguntar que tanto quiere gastar en escalabilidad, disponibilidad, desempeño, seguridad, administración, facilidad, adaptabilidad, y rentabilidad. Hacer el equilibrio es más complejo, porque las metas pueden diferir en varias partes de una red.

[6] En una sección posterior se detallará esta importante característica del protocolo MPLS.

2.1.3 Caracterización de la red existente.

Un importante paso en el método de diseño de redes *Top-Down* es examinar la red existente del cliente para juzgar de una mejor forma como se van a cumplir las expectativas de escalabilidad, desempeño, y disponibilidad. Al examinar la red existente se incluye el aprendizaje acerca de la topología y de la estructura física así como evaluar el desempeño de la red. Mediante el desarrollo de un entendimiento de la estructura de la red existente, usos y funcionamiento, se puede determinar si las metas del cliente son realistas.

2.1.3.1 Caracterizando la infraestructura de la red.

Esto significa desarrollar un mapa de la red y conocer la localización de los dispositivos mayores en la red y los segmentos de ésta. También incluye la documentación de nombres y direcciones de los dispositivos mayores y segmentos, así como la identificación de cualquier método estándar para crear los nombres y las direcciones. Documentar los tipos y longitudes de cableado físico, y la investigación en cuanto a las restricciones arquitectónicas y ambientales, son aspectos importantes en la caracterización de la infraestructura de la red.

El ir conociendo las locaciones de los servidores, dispositivos mayores, y segmentos de la red es un buen comienzo en el desarrollo del entendimiento del flujo de tráfico. La meta es obtener un mapa de la red que ya se encuentra implementada. Para desarrollar un dibujo de la red se puede invertir en una buena herramienta que haga diagramas de redes. Algunas compañías ofrecen esta herramienta de dibujo que además automáticamente descubre la red existente. La herramienta aprende acerca de los dispositivos de la red y de las estaciones de trabajo, incluyendo el tipo de CPU, versión del software, memoria, el número de puertos y de tarjetas de red.

Lo que debe incluir un mapa es: información geográfica, como países, estados o provincias, ciudades, campus; conexiones WAN entre países, estados o ciudades, edificios y pisos, conexiones entre edificios y entre campus; indicación del tipo de tecnología LAN o WAN que se esté usando, nombre del Proveedor de Servicios de WANs, la ubicación de enrutadores, switches; localización de VPNs; localización de los servidores mayores, de los mainframes, de las estaciones administradoras de la red; localización de LANs Virtuales – VLANs; topología de algún sistema de seguridad *firewall*[7]; localización de sistemas *dial-in* y *dial-out*; lugar donde residen las estaciones de trabajo y por último una descripción de la topología lógica o la arquitectura de la red.

La topología lógica ilustra la arquitectura de la red, la cual puede ser jerárquica, plana, estructurada, no estructurada, en capas y otras posibilidades. También describe los métodos para conectar dispositivos en una forma geométrica, por ejemplo: estrella, anillo, hub, etc.

Cuando se dibuje el mapa detalladamente, se debe incluir nombres de los sitios mayores, enrutadores, segmentos de red y servidores. También se debe investigar las

[7] Sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada.

direcciones de red que el cliente usa. El esquema de direccionamiento puede influenciar nuestra habilidad para adaptar la red a las nuevas metas de diseño.

También es importante entender el diseño del cableado de la red existente. Documentar esto puede ayudar a realizar un plan para mejorar e identificar cualquier problema potencial. Se debe documentar tipos de cableado en uso así como su longitud y además obtener toda la información acerca del cableado vertical y horizontal

2.1.3.2 Revisando la salud de la red existente.

Es importante analizar el funcionamiento de los segmentos existentes para poder determinar si éstos ayudarán a cumplir con los requisitos del nuevo diseño. Si la red es muy grande se deben analizar los segmentos que pueden interoperar con la nueva red. Se debe poner atención particular al *backbone*[8] de la red y de las redes que conectarán las viejas y nuevas áreas.

Se puede comenzar con un análisis de la utilización de la red. Es una medida de que tanto ancho de banda está en uso durante un intervalo específico de tiempo. En general se debe medir con la suficiente granularidad en el tiempo para poder ver picos en periodos pequeños en el tráfico de la red, así se pueden evaluar de una forma más exacta los requerimientos de la capacidad de los dispositivos o segmentos. Cuando se desarrolla la línea de inicio, usualmente una buena idea es exagerar en la obtención de muchos datos; después se podrán resumir.

También existe una utilización del ancho de banda por parte de los protocolos, por lo tanto se debe medir la utilización de tráfico de tipo broadcast[9] contra el tráfico unicast[10]; y por cada protocolo principal. Algunos protocolos envían tráfico broadcast excesivo, lo cual puede degradar seriamente el desempeño de la red.

Después se puede proceder al análisis de la fiabilidad. Para analizar esto se puede emplear un dispositivo colocado en los seriales, para probar el número de bits dañados comparados con el total. En el caso de tramas una buena regla a seguir es que no debe de haber más de una trama errónea por cada megabyte de datos. Se debe correlacionar la información de estaciones que envían más errores con la información obtenida de la topología de la red para identificar las áreas de ésta que son más propensas a errores, posiblemente debido a ruido eléctrico o problemas de cableado. La fiabilidad también debe incluir una medida de los paquetes perdidos.

Al correlacionar la información acerca de los paquetes perdidos con otras medidas de desempeño, se determina si la pérdida de paquetes indica la necesidad de aumentar el ancho de banda, disminuir los errores empleando la técnica de Verificación por Redundancia Cíclica – Cyclic Redundancy Check (CRC), o actualizar dispositivos de la red.

---

[8] Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a otras redes.

[9] Se envían paquetes de datos a todos los nodos de una red.

[10] Se refiere al envío de paquetes de datos a un sólo destino de red.

En cuanto al análisis de la eficiencia de la red, la meta es maximizar el número de datos en bytes comparados con el número de bytes contenidos en los encabezados y en los paquetes de confirmación enviados por la otra terminal de una conversación. Para examinar los tamaños de las tramas actuales en la red se puede usar un analizador de protocolos.

Otro aspecto de gran importancia en el análisis de la red existente, es el retraso y el tiempo de respuesta. Usando un analizador de protocolos, se puede observar la cantidad de tiempo entre tramas y obtener una estimación áspera del tiempo de respuesta en la Capa de Enlace de Datos y en la Capa de Aplicación.

Una forma muy común para medir el tiempo de respuesta es enviando paquetes ping[11], para poder medir el tiempo del viaje redondo a la hora de enviar una petición y recibir su correspondiente respuesta. También se debe medir el tiempo de respuesta desde el punto de vista del usuario, es decir, una medida de que tanto tiempo toma obtener una respuesta para operaciones típicas. Se debe medir el tiempo de respuesta para protocolos del sistema, por ejemplo las peticiones para una dirección IP mediante el Sistema de Nombres de Dominios – Domain Name System (DNS)[12] o el Protocolo de Configuración Dinámica de Anfitrión – Dynamic Host Configuration Protocol (DHCP).[13] Adicionalmente es de gran de ayuda hacer pruebas de tiempo de respuesta cuando la red está experimentado problemas o cambios.

El paso final para determinar la salud de la red es revisar el funcionamiento de los enrutadores principales. Esto incluye enrutadores que usan una topología jerárquica, enrutadores del *backbone*, y enrutadores que pueden tener roles significativos en el nuevo diseño. Se debe revisar el comportamiento y la salud de un enrutador, esto se hace determinando que tan ocupado se encuentra (utilización del CPU), cuántos paquetes ha procesado, cuántos ha tirado, y el estado de los *buffers* y colas de éste.

2.1.3.3 Herramientas para caracterizar la red existente.

A continuación se mencionan algunas herramientas que ayudan en la caracterización de una red existente:

- **Analizador de protocolos.** Es una herramienta que captura el tráfico de la red, decodifica los protocolos en los paquetes capturados, y provee datos estadísticos para caracterizar carga, errores y tiempo de respuesta. Algunos analizadores incluyen un sistema experto que automáticamente identifica problemas en la red.

- **Herramientas de monitoreo remoto.** Permite obtener datos estadísticos de parámetros de la de Capa de Enlace de datos y de la Capa Física e inclusive se puede

[11] Es usado como una herramienta de diagnóstico para determinar conectividad hasta la Capa 3 del Modelo de Referencia OSI, un ejemplo es determinar si un equipo está activo y donde puede ser contactado, también ayuda a determinar el tiempo de llegada de un aviso de un equipo a otro.
[12] Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones, es decir traduce los nombres de los dominios en direcciones IP.
[13] Es un método estándar para asignar automáticamente direcciones IP a dispositivos en una red.

obtener información hasta la Capa de Aplicación. Esta herramienta permite a los administradores de la red coleccionar datos estadísticos del tráfico.

- **Herramientas Cisco para caracterizar la red existente.** Entre ellos está el Protocolo de Descubrimiento de Cisco – Cisco Discovery Protocol (CDP). El CDP especifica un método en el que los enrutadores y los switches Cisco envían información de configuración de uno a otro en términos regulares. Analizando los datos del CDP se puede ayudar a estudiar la topología de una red existente.

2.1.4 Caracterización del tráfico de la red.

Cuando se habla de la caracterización del tráfico de datos a través de una red, se refiere a la identificación de las fuentes y destinos de dichos flujos, así como a sus direcciones y simetrías. Algo también de gran importancia que se debe considerar al caracterizar el tráfico es su carga, generada por aplicaciones y protocolos, así como su comportamiento, para que de esta forma se puedan seleccionar soluciones adecuadas.

2.1.4.1 Caracterización del flujo de tráfico.

Para entender el flujo de tráfico de una red, primero se deben identificar las comunidades de usuarios y los almacenes de datos de las aplicaciones existentes, así como de las nuevas. Es necesario caracterizar las comunidades de usuarios basándose más en sus aplicaciones y uso de protocolos que en sus límites departamentales.

El caracterizar el flujo de tráfico, también requiere de documentar los grandes almacenes de datos, es decir las áreas en la red donde residen los datos de la Capa de Aplicación. Un almacén de datos pude ser un servidor, un cluster de servidores, un mainframe, una unidad de respaldo en cinta, una librería de vídeo digital, o cualquier dispositivo o componente de una red donde se almacene grandes cantidades de datos.

En general medir el comportamiento del flujo de tráfico ayuda a: caracterizar el comportamiento de las redes existentes, planificar el desarrollo de la red y su expansión, cuantificar el desempeño de la red, verificar la Calidad de Servicio de la red, y atribuir el uso de la red a usuarios y aplicaciones determinadas.

El flujo individual de tráfico de la red puede definirse como la información transmitida del protocolo y de la aplicación, entre entidades de comunicaciones durante una simple sesión. El flujo tiene atributos como dirección, simetría, ruta a seguir, opciones de enrutamiento, número de paquetes, número de bytes y direcciones para cada extremo del flujo. Para poder realizar la tarea de caracterizar el tamaño del flujo se puede usar como herramienta un analizador de protocolos. El objetivo de esta herramienta es documentar el flujo en megabytes por segundo entre pares de sistemas autónomos, redes, servidores, y aplicaciones.

El flujo de una red puede ser caracterizado por su dirección y simetría como se mencionó anteriormente; la dirección especifica si los datos viajan en ambos sentidos o solamente en uno, también especifica la ruta que el flujo tomaría para viajar de la fuente al destino a través de la red. La simetría describe si el flujo tiende a tener un desempeño mayor o algún requerimiento de Calidad de Servicio en alguna dirección comparado con el que tendría en otras direcciones. Se conocen varios tipos de flujo, los cuales se describen brevemente a continuación:

a. Flujo de tráfico terminal/host.

Usualmente este flujo es asimétrico, Telnet es un ejemplo de esta categoría, la terminal envía un sólo paquete por cada caracter que el usuario escribe. El host devuelve múltiples caracteres dependiendo de lo que haya escrito el usuario.

b. Flujo de tráfico cliente/servidor.

El flujo es por lo regular bidireccional, y asimétrico. Las peticiones por parte del cliente son usualmente de tamaño menor a 64 bytes, y las respuestas del servidor están en un rango comprendido entre 64 y 1500 bytes o más. El Protocolo de Transferencia de Hiper Texto – Hyper Text Transfer Protocol (HTTP) es probablemente el protocolo cliente/servidor más usado; sin embargo muchas veces el flujo para el tráfico de HTTP no es siempre el que existe entre el navegador de la Web y el servidor Web debido al caching, es decir se almacena en el cliente parte de la información obtenida del servidor.

c. Flujo de tráfico entre parejas (peers).

Es usualmente bidireccional y simétrico, además de que no existe alguna jerarquía entre los dispositivos, cada dispositivo es considerado de igual importancia como cualquier otro, y ningún dispositivo almacena substancialmente más datos que cualquier otro. Un ejemplo de aplicación empleado por parejas, es el empleado en el establecimiento de videoconferencias, muy usadas en juntas de negocios donde la gente se ubica en sitios remotos. Algo que se debe tener muy en cuenta en este tipo de flujo, es que todos los sitios deben tener el mismo requerimiento de Calidad de Servicio. Este último concepto será tratado con mayor profundidad más adelante en el capítulo tres, ya que es importante considerarlo en el diseño de la red.

d. Flujo de tráfico servidor/servidor.

Un servidor requiere establecer una comunicación con otro para realizar un gran número de tareas como son: implementar servicios de directorios, emplear la caché con datos que son muy utilizados, reflejar datos sobre todo en el balanceo de carga y redundancia, respaldar datos, etc. Los servidores requieren emplear entre ellos aplicaciones de administración por varias razones como lo son reforzar políticas de seguridad y actualizar los datos de administración de la red. Generalmente el flujo es bidireccional y la simetría depende de la aplicación, en algunos casos hay una jerarquía de servidores lo que implica que algunos envíen y almacenen más datos que otros.

e. Flujo de tráfico empleado en la computación distribuida.

Al mencionar computación distribuida, nos referimos al empleo de aplicaciones que requieren de múltiples nodos de cómputo, que trabajan juntos para completar un trabajo. Ejemplos de este tipo de computación distribuida son los empleados en los estudios de cine para realizar efectos visuales en las películas, en la industria de los semiconductores, y en la simulación de la ingeniería en la milicia. Los datos pueden viajan a través de un administrador de tareas hacia los nodos de cómputo, así como también entre los nodos. El

caracterizar el flujo de tráfico para las aplicaciones que se emplean en la computación distribuida tal vez requiera de un estudio empleando analizadores de protocolos o un modelo del tráfico potencial empleando un simulador de redes.

Por lo tanto, lo que se debe realizar para poder documentar el flujo del tráfico, ya sea para aplicaciones de la red existentes o nuevas, es caracterizar el tipo de flujo de forma individual para cada aplicación, conocer la lista de comunidades de usuarios y tener en cuenta los almacenes de datos que están asociados con las aplicaciones.

2.1.4.2 Caracterización de la carga del tráfico.

Se puede estimar la carga total para una aplicación, multiplicando la carga del flujo por el número de dispositivos que usan esa aplicación. La investigación que se haga sobre las comunidades de los usuarios y el número de almacenes de datos (servidores) puede ayudar a calcular una demanda del ancho de banda agregado aproximado para cada aplicación. Documentando la localización de las comunidades de los usuarios y los almacenes de datos, puede ayudar a entender la cantidad de tráfico que fluirá de un segmento a otro. Esto puede auxiliar en la elección de las tecnologías del *backbone* y de los dispositivos de la red.

Se deben investigar los patrones de uso de aplicaciones y de los requerimientos de Calidad de Servicio. Algunas aplicaciones no son usadas con mucha frecuencia, pero requieren de una gran parte del ancho de banda cuando son empleadas.

Para documentar los patrones de uso de las aplicaciones, antes se debe identificar el número total de usuarios por aplicación, así como también se debe tomar en cuenta la siguiente información: la frecuencia de las sesiones de aplicaciones, la duración promedio de una sesión de la aplicación y el número de usuarios simultáneos por aplicación.

Se puede ser más exigente en la predicción de la demanda del ancho de banda agregado haciendo algunas suposiciones es decir plantear los peores casos como: asumir que el número de usuarios de una aplicación es igual al número de usuarios simultáneos, creer que todas las aplicaciones son usadas todo el tiempo e imaginarse que cada usuario abre un sesión y ésta dura todo el día, aunque esto llevará a tener un sobre-aprovisionamiento que en muchas ocasiones es imposible de costear.

Para ir refinando las estimaciones de la carga de tráfico causadas por aplicaciones, se necesita realizar una investigación del tamaño de los datos enviados por aplicaciones, de la información adjunta causada por los protocolos también conocida como *overhead* y cualquier carga adicional causada por la inicialización de la aplicación. Para realizar esto, se puede emplear el uso de tablas de tamaños aproximados de los objetos de datos que las aplicaciones transfieren a través de la red, así como también tablas donde se muestre el tráfico estimado de los overheads de varios protocolos.

Otro tipo de estimación de carga de tráfico, es la causada por la reinicialización simultánea de estaciones de trabajo en la red y del inicio nuevamente de sus sesiones. Esta inicialización de estaciones de trabajo puede causar carga significante en las redes al inicio

de la jornada debido al número de paquetes generados que en algunos casos pueden ser paquetes de tipo broadcast.

La última estimación que se debe de tomar en cuenta es la carga de tráfico causada por protocolos de enrutamiento. Estimar este tipo de carga es especialmente importante en una topología que incluye muchas redes del lado de un enlace lento de la WAN, ya que esto puede repercutir en un uso significante del porcentaje del ancho de banda de la misma WAN. Esta estimación también se puede hacer mediante el empleo de tablas donde se relacione anchos de banda con protocolos de enrutamiento.

2.1.4.3 Caracterización del comportamiento del tráfico.

Para seleccionar soluciones apropiadas se necesita entender los modos en que actúan los protocolos y las aplicaciones en adición al análisis del flujo de tráfico y de la carga.

Existen distintos tipos de comportamiento de tráfico como muchas veces es el caso del generado por tramas broadcast y multicast[14]. Una trama broadcast es aquella que va a ser transmitida a todas las estaciones de la LAN, mientras que una trama multicast solamente está dirigida a un subconjunto de estaciones. Dispositivos de la red que operan en la Capa 2 como switches y bridges, envían broadcast y multicast por todos sus puertos. Un enrutador no reenvía ninguno de estos tipos de tramas. Todos los dispositivos de un lado del enrutador son considerados parte de un sólo dominio broadcast.

En adición a la inclusión de enrutadores en el diseño de redes para disminuir el envío de broadcast, también se puede limitar el tamaño del dominio broadcast implementando VLANs. Si más del 20 por ciento del tráfico de la red es broadcast o multicast, la red necesitaría ser segmentada usando enrutadores o VLANs.

Otra posible causa de tráfico pesado causado por broadcast, son las tormentas intermitentes causadas por desconfiguraciones o mal funcionamiento de las estaciones de la red. En general el tráfico broadcast es necesario e inevitable. Protocolos empleados por enrutadores u otros dispositivos usan broadcast y multicast para compartir información acerca de la topología de la red. Los servidores envían sus broadcast y multicast para anunciar sus servicios.

También debe de considerarse en el diseño de la red, su eficiencia, es decir saber realmente si las aplicaciones y los protocolos usan el ancho de banda efectivamente. La eficiencia de la red es afectada por diversos factores como el tamaño de las tramas empleadas en la transferencia de datos, la interacción de protocolos usados por una aplicación, el *Windowing* y el Control de Flujo[15], así como por los mecanismos de recuperación de errores.

[14] Multicast se refiere a los envíos de paquetes o tramas únicos copiados por la red y enviados a un subconjunto específico de direcciones de red.
[15] Ambas técnicas propias de TCP/IP.

El usar el tamaño de la trama máxima soportada por el medio en uso, tiene un impacto positivo en el desempeño de la red. De ser posible se deben usar protocolos que soporten el cálculo de las Unidades Máximas de Transmisión – Maximum Transmission Units (MTUs). Con este tipo de protocolos, el software puede realizar un cálculo dinámico y usar el tamaño de la trama más grande que pueda incursionar a través la red sin requerir de una fragmentación. Existe información disponible con valores predeterminados de gran ayuda al diseñador, para que éste pueda predecir el tamaño de la trama para caracterizar de una mejor forma la carga del tráfico.

Otra forma de entender el tráfico de la red es comprender lo que es el *Windowing* y el Control de Flujo. Por ejemplo un dispositivo TCP/IP envía paquetes de datos en una secuencia rápida, sin esperar una respuesta de confirmación, hasta que el tamaño de su ventana de envío se reduce drásticamente. El tamaño de la ventana de envío de una estación está basada en el tamaño de la ventana de recepción del receptor. Este último establece en cada paquete TCP la cantidad de datos que está dispuesto a recibir. La ventana de recepción del receptor está basada en la cantidad de memoria de éste y en la rapidez que puede procesar los datos recibidos. Para poder optimizar la eficiencia de la red se puede incrementar la memoria y el poder del CPU de las estaciones terminales, lo cual resultará en una ventana de recepción mayor.

2.1.4.4 Caracterización de los requisitos de la Calidad de Servicio.

Dado que existen diferentes clases de aplicaciones, y que estas llegan a solicitar un tipo de servicio en particular por parte de la red, conocer la demanda del ancho de banda para una determinada aplicación no es suficiente, también se necesitan caracterizar parámetros como: el retraso y su variación, tamaños de datos en forma de ráfaga, pérdida de datos, picos y las tasas mínimas de tráfico.[16]

[16] La Calidad de Servicio se analizará con mayor profundidad en la sección 3.4 del siguiente capítulo.

2.2 Tecnología.

2.2.1 Enrutamiento.

El enrutamiento se define como una serie de procesos que son llevados a cabo para transportar la información desde un origen a un destino (figura 2.1), a través de redes interconectadas por enrutadores y otros dispositivos que funcionan como una sola red. Se realiza con base a la dirección IP destino que contenga el encabezado de la información[17] y está asociado a la Capa de Red (Capa 3) del Modelo de Referencia OSI.

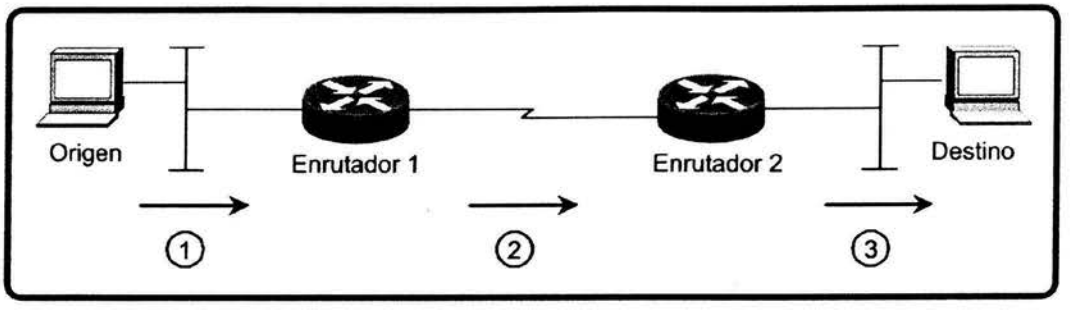


Figura 2.1. Proceso de enrutamiento.

Un enrutador es un dispositivo que determina el siguiente punto de la red a donde será enviada la información, debe de estar conectado al menos a dos redes y elegirá una ruta dependiendo de su visión particular de la red. Crea y mantiene la Tabla de Enrutamiento que es una lista de las rutas disponibles que puede alcanzar, sus condiciones y la forma de llegar a ellas, también conocido como *next-hop*. El enrutador compara el destino de la información con la Tabla de Enrutamiento, y hace una selección, ésta le permitirá saber hacia dónde enviar el paquete.

Comúnmente la información viaja en unidades de información llamadas paquetes. Típicamente un paquete viaja a través de un número no determinado de puntos o nodos[18] antes de arribar a su destino. En cada uno de ellos se toma la decisión de cual será el siguiente salto. Este comportamiento es conocido como salto a salto o *hop-by-hop*.

El proceso de enrutamiento, dentro de un enrutador, consiste de lo siguiente:

1. Se revisa la dirección destino del paquete.

2. Se consulta la Tabla de Enrutamiento.

    a. Si hay una entrada en la Tabla de Enrutamiento:
        - Se envía el paquete.

[17] Encabezado IP, tomado del Request for Comments RFC-791 sección 3.1.
[18] Con este nombre también se denomina a los enrutadores.

b. Si no hay una entrada[19]:
   - Si hay una ruta por omisión (default):
     - Lo envía.
   - Si no hay:
     - Le descarta o lo tira (drop).

Además de las redes alcanzables y el *next-hop*, la Tabla de Enrutamiento contiene la interfase de salida del enrutador, la métrica, distancia administrativa y otras propiedades; esta tabla puede ser creada de tres maneras: estáticamente, dinámicamente y mediante la combinación de ambas.

2.2.2 Enrutamiento Estático.

En el enrutamiento estático las rutas deben de ser creadas manualmente en cada uno de los enrutadores que conforman la red, para todos los destinos deseados, a dichas rutas se les conoce como estáticas. La Tabla de Enrutamiento conformada exclusivamente por este tipo de rutas no responderá a los cambios, que por momentos o permanentemente, se presenten en la red. De presentarse algún cambio de duración significativa, se deberán reconfigurar todas las rutas que resultaron afectadas. En una red de pequeñas dimensiones, no representa mayor problema hacer cambios en el esquema de enrutamiento, sin embargo en una red de proporciones medianas, el mantenimiento de las Tablas de Enrutamiento puede ser una tarea repetitiva e indeseable para el administrador de la red.

Aunque por la topología de la red exista más de una manera para llegar a un destino, el enrutamiento estático no permite utilizar rutas distintas a las configuradas, de tal suerte que si por alguna razón éstas fallan, los paquetes no llegarán a su destino aún cuando existan rutas alternas disponibles.

El enrutamiento estático permite un control preciso sobre hacia donde viaja la información y se preferirá para redes pequeñas y sin enlaces redundantes. Puede además, hacer uso de la Máscara de Subred de Longitud Variable – Variable Length Subnet Mask (VLSM)[20] para hacer sumarización de rutas[21].

[19] Por entrada se entiende, la información referente a una ruta que está en la Tabla de Enrutamiento.
[20] Variable Length Subnet Mask, desarrollado para permitir múltiples niveles de direcciones IP dentro de una sola red, descrito en el RFC-1518; con ello se puede sortear el direccionamiento tradicional basado en clases (Classful), es decir clases A, B y C.
[21] Sumarización de rutas, es una manera de tener una sola dirección IP que representa una colección de direcciones IP cuando se emplea un plan de direccionamiento jerárquico. Descrito en el RFC-1518.

2.2.3 Enrutamiento Dinámico.

Los algoritmos usados por el enrutador para determinar, escoger, compartir la información de la asequibilidad y estado de la red con otros enrutadores y crear la Tabla de Enrutamiento son conocidos como protocolos de enrutamiento dinámico. Su operación puede ser muy compleja, pues en sí mismos contienen los procedimientos necesarios para realizar las siguientes funciones:

- Conocer a los enrutadores adyacentes.
- Determinar la mejor ruta hacia un destino.
- Manejar rutas secundarias o de respaldo.
- Crear la Tabla de Enrutamiento basándose en la información propia y la que recibe de los enrutadores adyacentes.

Cuando la información en los enrutadores es consistente con la topología de la red, se dice que se ha alcanzado la convergencia. El tiempo que le tome al protocolo de enrutamiento llegar a ésta, se conoce como tiempo de convergencia y dependerá de los algoritmos empleados para obtener los destinos, por ello es que cada protocolo tiene un tiempo de convergencia diferente.

Una Tabla de Enrutamiento que haya sido creada exclusivamente en base a algún protocolo de enrutamiento contendrá las rutas que resultaron ser las mejores. Para la elección de las mejores rutas, hacia un destino se usan las métricas, variables asignadas a las rutas que representarán una manera en que estas rutas son clasificadas por preferencia, entre menor sea el valor de la métrica, mejor será la ruta. Se usará una o varias métricas y dependerá de cada protocolo el valor que le asigne a cada una de ellas. Valores comúnmente usados son: número de saltos, retardo, ancho de banda, carga o disponibilidad.

En un enrutador se puede tener configurado más de un protocolo de enrutamiento, lo que nos lleva al caso de tener las mejores rutas que cada protocolo haya calculado hacia un mismo destino. Para obtener la mejor del conjunto, se tiene el parámetro conocido como Distancia Administrativa. Ésta especifica una preferencia sobre la forma en que una ruta fue aprendida. Tiene un significado trascendente local al enrutador y cada protocolo tendrá asignado un valor predeterminado. Los paquetes viajarán sobre trayectorias creadas por protocolos que tengan un valor más pequeño de Distancia Administrativa (ver tabla 2.1).

Fuente de la Ruta	Distancia Administrativa Asociada
Interfase directamente conectada	0
Ruta estática asociada a una interfase	0
Ruta estática asociada a un next-hop	1
Ruta sumarizada de EIGRP	5
eBGP	20
Interna de EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP y RIPv2	120
EGP	140
Externa de EIGRP	170
iBGP	200
Desconocida o Infinito	255

Tabla 2.1 Comparación entre Distancias Administrativas.

Por la manera en que operan los protocolos de enrutamiento puede llegar a presentarse un *loop*, que es la trayectoria cerrada en donde se queda atrapado un paquete, entre dos o más enrutadores en camino a su destino. Son causados por la diferencia en tiempos y trayectorias que una actualización puede seguir antes de arribar a un enrutador en combinación con el algoritmo del protocolo de enrutamiento. Algunas topologías son más susceptibles a este tipo de problemas que otras. Como consecuencia de este problema, los paquetes son descartados, es decir, no llegan a su destino debido a que exceden el valor máximo del campo de Time To Live (TTL) en el encabezado de IP (ver figura 2.2).

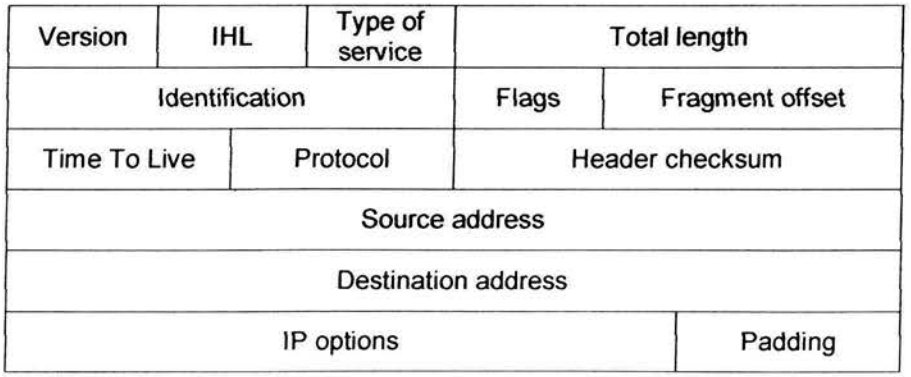


Figura 2.2 Encabezado del protocolo IP versión 4.

Como puede intuirse, los protocolos de enrutamiento dinámico son los responsables de la respuesta automática a los cambios que se presenten en la red, por lo cual se recomienda su uso en redes de mayores proporciones que en el caso del enrutamiento estático. Para este tipo de enrutamiento, el administrador de la red sólo tendrá que definir y configurar la operación del protocolo de enrutamiento. A diferencia del enrutamiento estático, no es posible saber con certeza cómo es que viajan los paquetes a través de la red,

a menos que se cuente con una herramienta que permita tener una idea del comportamiento de los paquetes en la red *(traceroute)*.

La mayoría de los protocolos de enrutamiento caen en alguna de las siguientes clasificaciones:

a. Por el tipo de enrutamiento que realizan:

   - Interior Gateway Protocols (IGPs).
   - Exterior Gateway Protocols (EGPs).

b. Por el tipo de algoritmo empleado para calcular y distribuir sus rutas:

   - Protocolos de Vector Distancia – Distance Vector Protocols (DVPs).
   - Protocolos de Estado de Enlace – Link State Protocols (LSPs).
   - Protocolos Híbridos.
   - Protocolos Path Vector.

2.2.4 Interior Gateway Protocols (IGPs) y Exterior Gateway Protocols (EGPs).

Un conjunto de enrutadores que comparten una misma administración y políticas de enrutamiento se conocen como Sistema Autónomo – Autonomous System (AS).

- A los protocolos que intercambian rutas dentro de un AS son conocidos como Interior Gateway Protocols (IGPs).

- A los protocolos que operan entre ASs se les conocen como Exterior Gateway Protocols (EGPs).

2.2.5 Clasificación por el tipo de algoritmo empleado.

2.2.5.1 Protocolos de Vector Distancia – Distance Vector Protocols (DVPs).

Un Distance Vector Protocol (DVP) realiza actualizaciones de la Tabla de Enrutamiento completa a sus vecinos[22] independientemente de que existan o no cambios en la red. Estas actualizaciones se llevan a cabo con mensajes de tipo difusión (broadcast), que aunado con el hecho de que son periódicas, el protocolo, solamente en su operación, consumirá un porcentaje significativo del ancho de banda del disponible en los enlaces, dejando en un segundo término la información útil a ser transportada. El problema se torna más serio en tanto que la Tabla de Enrutamiento es más grande.

[22] Vecinos son enrutadores con un enlace de datos en común.

Estos protocolos están diseñados para conocer sólo la mejor ruta hacia un destino como resultado de sus algoritmos y esa es la que colocan en su Tabla de Enrutamiento, misma que es enviada a sus vecinos, de tal forma que todos los dispositivos que conforman la red sólo conocen las mejores rutas sin importar que existan otras alternas. Esto puede ocasionar que los paquetes sean descartados si alguna ruta falla y no se ha calculado al menos una nueva hacia un destino en particular.

Para evitar el problema de *loops*, los DVPs utilizan alguna de las siguientes técnicas:

- **Split Horizon.** Con la cual no se enviará una actualización sobre una ruta en particular a través de la interfase por donde se aprendió.

- **Poison Reverse.** Que es una modificación a Split Horizon, que enviará la actualización por la misma interfase a través de la cual aprendió sobre una ruta, pero con una métrica infinita.

- **Count to Infinity.** Con la cual se evita que un paquete vaya de un enrutador a otro de forma interminable, estableciendo el número de saltos máximo a 16. Esto afecta un poco el tiempo de convergencia de la red.

- **Triggered Updates.** Con ella, un enrutador enviará de manera inmediata una actualización en cuanto detecte un cambio. Se utiliza para reducir el tiempo de convergencia de la red.

- **Hold Down Timers.** Introduce un tiempo de desconfianza para la aceptación de información de enrutamiento y así evitar que existan errores en ella.

- **Asynchronous Updates.** Introduce un tiempo aleatorio para realizar las actualizaciones. Comúnmente usada en redes de tipo broadcast, evitando que se generen colisiones entre las actualizaciones que se crean simultáneamente, lo cual impediría que estas llegaran a todos sus destinatarios.

Ejemplos de este tipo de protocolos son IGRP, RIP y RIPv2.

2.2.5.2 Protocolos de Estado de Enlace – Link State Protocols (LSPs).

Estos protocolos cumplen con la misma finalidad que los Distance Vector Protocols (DVPs), pero son totalmente diferentes en su esquema de operación.

Los Link State Protocols (LSPs) tienen una visión de toda la red y no sólo las mejores rutas hacia un destino. Por ello es que resulta más difícil que incurran en errores de *loop* como en el caso de los DVPs. Para tener esta visión de toda la red cada uno de los enrutadores genera información sobre el estado de los enlaces que tiene directamente conectados y la envía a los enrutadores de su *peer*[23].

[23] En este punto, peer es una vecindad o un grupo de vecinos.

Su operación se basa en lo siguiente:

- Cada enrutador establece una relación de adyacencia con cada uno de sus vecinos.
- Cada enrutador envía Link State Advertisements (LSAs) a cada vecino. Un LSA es generado por cada uno de los enlaces del enrutador. Cada enrutador reenvía *(floods)* los anuncios a sus vecinos.
- Cada enrutador hace una copia de todos los LSAs sin modificarlos. Si todo funciona correctamente las bases de datos de todos los enrutadores deberá ser la misma.
- Cuando se ha completado la base de datos topológica es conocida como Link State Database (LSD) y a partir de ella se calculan las rutas que estarán en la Tabla de Enrutamiento.

Cuando un par de enrutadores se encuentran como vecinos, realizan un proceso mediante el cual sincronizan su base de datos hasta que su información sea la misma. Posteriormente deben de establecer ciertos parámetros para poder sincronizar la LSD. La información para lograr la adyacencia es transportada por *Hello Packets*, mismos que sirven como referencia para determinar si un vecino está o no activo, función conocida como *Keepalive*.

El término *flooding* se refiere a la acción que llevan a cabo los enrutadores para enviar los anuncios sobre el estado de los enlaces a todos sus vecinos. Cuando un LSA es recibido se copia y reenvía sin sufrir modificación alguna, excepto al enrutador de donde provino. Así se trata de evitar el problema de *loops* de los DVPs.

Una vez que los enrutadores tienen todos los LSAs incluidos (los de sus vecinos), ejecutan el algoritmo Shortest Path First (SPF)[24] el cual será la base para calcular las rutas a todos los destinos posibles y crear la Tabla de Enrutamiento.

La razón por la cual los LSPs convergen rápidamente, es que envían inmediatamente la información sobre un cambio en el estado de los enlaces cuando éste ocurre y posteriormente realizan los cálculos pertinentes. En contraparte, los DVPs primero calculan las rutas y luego envían su información. Otra diferencia entre ambos es que mientras los LSPs envían pequeñas actualizaciones sobre el estado de los enlaces, los DVPs envían toda la Tabla de Enrutamiento.

Algunos LSPs implementan el uso de áreas; un área es un grupo de enrutadores que pueden constituir una subred. Un AS puede ser dividido en áreas lo que mejorará el desempeño del protocolo, pues cuando se realicen actualizaciones se tendrán que enviar a un número menor de enrutadores, disminuyendo el tráfico entre ellos; se tendrá una LSD sólo para esa área y por lo tanto más pequeña. Los Area Border Routers (ABRs) son enrutadores que conectan al menos a dos áreas diferentes y manejan una base de datos

[24] Algoritmo desarrollado por Dijkstra para la ARPANET.

topológica por cada una. Si un enrutador necesita enviar información a otro en un área diferente, sólo necesita saber como llegar al ABR de su propia área.

Los LSPs pueden usar el VLSM para realizar sumarización de rutas en las actualizaciones y la posibilidad de emplear redes no continuas.

Ejemplos de este tipo de protocolos: OSPF e IS-IS.

2.2.5.2.1 Open Shortest Path First (OSPF)

OSPF es un Link State Protocol, es un protocolo fuente abierta, lo que significa que sus especificaciones son de dominio público, y está descrito por el RFC-1247.

Éste realiza actualizaciones mediante LSAs, que serán enviados a todos los enrutadores dentro de la misma área. Una vez que se ha realizado el proceso de enviar y recibir la información de enrutamiento, usa el algoritmo de SPF para calcular el camino más corto a cada destino.

Además de las características de un LSP, OSPF:

- Es un protocolo *classless*, permite el uso de VLSM.
- Realiza balanceo de carga en enlaces de igual costo.
- Proporciona soporte de autenticación mediante MD5 para enrutamiento más seguro.

OSPF maneja áreas, dentro de cada una de ellas los enrutadores no tendrán información detallada sobre la topología de otras, lo que permitirá manejar una LSD pequeña además de compartirla dentro de la misma.

Cada área tiene un identificador de 32 bits, el Area-ID, que puede ser expresado en forma decimal o en una representación similar a una dirección IP (dotted). El área con el identificador 0 (cero) está reservada y es usada como *backbone*, ésta será la responsable de distribuir la información de enrutamiento entre las áreas de una red, todas y cada una de ellas deberán de tener al menos una conexión física o virtual con el Área 0[25]. Con el nombre de OSPF Autonomous System (OSPF AS) se conocerá al identificador de un conjunto de áreas incluido su *backbone* (dominio).

OSPF emplea Area Border Routers (ABRs)[26] que conectarán una o más áreas con el *backbone* y actúan como punto de comunicación para el tráfico inter-áreas, además mantienen LSDs diferentes para cada una de las áreas conectadas.

La información de enrutamiento de OSPF depende del tipo de redes y del tipo de áreas.

[25] El backbone es también conocido como Área 0.
[26] Los ABRs son revisados en la sección anterior.

OSPF define 5 tipos de redes:

1. **Point-to-Point Networks,** que sólo conectan un par de enrutadores.

2. **Broadcast Networks (conocidas como Broadcast Multi-Access Networks),** como el caso de Ethernet, conectan más de 2 dispositivos y envían un paquete a todos aquellos dispositivos que lo puedan recibir. Estas redes usan Designated Routers (DRs) y Backup Designated Routers (BDRs).

3. **Non-Broadcast Multi-Access (NBMA) Networks,** como Frame Relay y ATM, conectan más de 2 enrutadores pero no realizan broadcast. También usan DRs y BDRs.

4. **Point-to-Multipoint Networks,** se consideran como un conjunto de Point-to-Point Networks por lo que usan DRs y BDRs.

5. **Virtual Link,** que son configuraciones especiales que actúan como Point-to-Point Networks. Son utilizadas para el caso en que un área realice una conexión con el *backbone* a través de otra área, aparentando estar directamente conectada a éste.

Los Designated Routers y Backup Designated Routers son escogidos por OSPF para representar el segmento en donde se encuentran inmersos ante el resto de los que conforman la totalidad de la red. Al representar el área se convertirá en el punto de comunicación entre ésta y otras áreas. Controla el proceso de *flooding*, pues evita que se establezcan adyacencias entre todos los enrutadores del área, sólo estableciéndolas con el DR; para establecer las adyacencias, los enrutadores deben generar LSAs y enviarlos (ver tabla 2.2), mientras se lleva a cabo este proceso no es posible el envío de paquetes a su destino. El BDR sólo es usado en el caso que exista una falla con el DR.

Los LSAs más importantes que OSPF emplea son:

Tipo	Nombre y descripción del LSA
1	Router LSA, generado por todos los enrutadores, enumera el estado de los enlaces del enrutador.
2	Network LSA, generado por el DR, tiene información de los enrutadores de la red.
3	Network Summary LSA, generados por el ABR, contiene las redes sumarizadas que éste puede alcanzar.
4	ASBR Summary LSA (Autonomous System Border Router), generado por el ABR, parecido al tipo 3, excepto que en vez de anunciar redes, anuncia un ASBR.
5	AS External LSA, generados por el ASBR, anuncia un destino externo o una ruta por omisión (default network) por todo el AS.
7	Not-so-Stubby Area LSA, generado por el ASBR, parecido al tipo 5 pero sólo es enviado dentro del área.
8	External Attributes LSA, usando para transportar la información de otros protocolos, por ejemplo de Border Gateway Protocol (BGP).

Tabla 2.2 Tipos de LSAs.

OSPF maneja diversos tipos de áreas y las clasifica de la siguiente manera:

a. Stub Areas.

Son áreas con una sola salida y los enrutadores dentro del área no necesitan saber sobre rutas externas. Los LSAs tipo 5 y 7 no son permitidos en estas áreas.

b. Totally Stubby Areas.

Son áreas que usan la *default route* para alcanzar todas las rutas externas al área. Solamente usan los LSA tipo 1, 2 y 3.

c. Not-so-Stubby Areas.

Son áreas que permanecerán como Stub Areas pero manejan rutas externas permitiendo conocer las redes conectadas al área aún cuando sean de un protocolo diferente. Los LSAs tipos 5 y 8 no son permitidos.

2.2.5.2.2 IS-IS Integrado - Integrated IS-IS.

End System to Intermediate System (ES-IS) es un protocolo que normalmente permite comunicación entre un host y un enrutador y por ende el protocolo que puede emplear un enrutador para comunicarse con otro es Intermediate System to Intermediate System (IS-IS).

IS-IS, es el protocolo de enrutamiento de tipo Connectionless Network Protocol (CLNP) de ISO. Con el fin de soportar la transición de TCP/IP a OSI, se propuso una extensión a este protocolo conocido como IS-IS Integrado o IS-IS Dual, el cual fue diseñado para operar en un ambiente Connectionless Network Service (CLNS), en un ambiente IP, o en uno dual CLNS/IP de ahí su nombre.

Una forma de comprender mejor este protocolo de enrutamiento es mencionando algunas de sus características que lo hacen parecido en su funcionamiento a un protocolo más conocido, OSPF.

Entre los aspectos que tienen en común IS-IS y OSPF podemos mencionar que: ambos mantienen una Link State Database (LSD) de donde el algoritmo SPF calcula los caminos más cortos; usan *Hello Packets* para establecer y mantener adyacencias; emplean áreas que permiten organizar de manera administrativa la topología de la red; tienen la capacidad de facilitar la sumarización de direcciones entre áreas; son protocolos *classless*; eligen a un Designated Router para representar redes broadcast; similar a los LSAs de OSPF, en IS-IS la unidad de datos empleada es el Link State PDU[27] (LSP) que es en sí un paquete. Se tiene definida una entidad que permite la comunicación entre áreas y que comúnmente es otra área que permite el enrutamiento entre éstas.

[27] Protocol Data Unit (PDU). Término OSI equivalente a paquete.

En lo referente a las áreas, en IS-IS los dispositivos (enrutadores y hosts) se encuentran completamente dentro de un área, los bordes son los enlaces y no los enrutadores como es el caso de los ABR de OSPF. Los enrutadores empleados para conectar áreas son conocidos como enrutadores nivel 2, y los que no tienen conectividad a otra área sino que nada más dentro de su propia área son enrutadores nivel 1. Un Sistema Intermedio – Intermediate System (IS) puede ser nivel 1 (L1), nivel 2 (L2) o ambos (L1/L2), éstos últimos pueden ser los análogos a los ABRs, y deben mantener tanto una LSD para el nivel 1 como para el nivel 2.

El *backbone* de IS-IS está formado por el conjunto de enrutadores L2 (incluyendo los enrutadores L1/L2) y sus enlaces de interconexión. Todos los enrutadores dentro de una misma área deben de tener una misma LSD, un enrutador L1 no tiene conocimiento de destinos fuera de su propia área, en caso de querer enviar un paquete a otra área, el enrutador L1 debe enviar su paquete a un enrutador L1/L2, el cual se encargará de lo demás. Los enrutadores L1/L2, mantienen LSDs separadas tanto para L1 como para L2, para calcular separadamente, mediante el algoritmo SPF, las rutas correspondientes a cada nivel en la topología.

Dado que un enrutador IS-IS reside completamente dentro de un área, se le asocia un identificador conocido como Area-ID. Como cada enrutador debe ser único dentro de un dominio de enrutamiento se emplea también un identificador llamado System-ID, que junto con el Area-ID forman un sola dirección conocida como Network Entity Title (NET) o dirección ISO.

2.2.5.2.2.1 Organización Funcional de IS-IS.

Al hablar de la Capa de Red del Modelo de Referencia OSI, se habla en sí de dos subcapas, las cuales tienen tareas muy distintas pero necesarias, unas para poder realizar otras funciones. La subcapa de Subred Independiente provee servicios de red a la Capa de Transporte de una forma coherente y uniforme. La subcapa de Subred Dependiente accesa a los servicios de la Capa de Enlace de Datos. A continuación se mencionarán las funciones de cada una de estas subcapas que forman la Capa de Red, que es donde opera el protocolo de enrutamiento IS-IS.

2.2.5.2.2.2 Funciones de la Subred Dependiente.

Entre las funciones más destacadas en cuanto a enrutamiento se refiere, se tienen: la transmisión y recepción de PDUs a través de una subred adjunta específica; el intercambio de PDUs Hello de IS-IS para descubrir vecinos y establecer adyacencias en la subred; el mantenimiento de dichas adyacencias y también se encarga de la transferencia de PDUs OSI en el proceso de enrutamiento y la transferencia de paquetes IP en el proceso de enrutamiento de IP.

IS-IS define solamente dos tipos de redes: redes Broadcast y redes Punto a Punto. Las Subredes Broadcast son enlaces de datos multi-acceso que soportan multicasting y las Subredes Punto a Punto *(non-broadcast)* pueden ser permanentes como un enlace T1 por ejemplo, o puede establecerse dinámicamente como un SVC de X.25.

Un enrutador IS-IS usa sus PDUs Hello para identificarse a sí mismo, sus funciones o servicios y para describir los parámetros de las interfases a través de las cuales son enviados los *Hello Packets*. Si dos vecinos están de acuerdo con sus respectivas capacidades y parámetros de sus interfaces se convierten en adyacentes. Como es de esperarse se generan adyacencias separadas tanto para nivel 1 como para el nivel 2. Una vez establecida la adyacencia, los *Hello Packets* actúan como *Keepalives*. Cada enrutador envía sus *Hello Packets* con un hold time, informando a sus vecinos el tiempo que deben de esperar para recibir el siguiente *Hello Packet* antes de declararlo muerto.

IS-IS elige un Enrutador Designado (Designated IS) por la misma razón que lo hace OSPF[28]. En vez de hacer que cada enrutador conectado a una LAN anuncie una adyacencia con cada uno de los enrutadores de la red, la red es considerada en su totalidad como un enrutador o pseudonodo. Cada enrutador incluyendo al DR, anuncia un sólo enlace al pseudonodo. El DR también anuncia, como el representante del pseudonodo, un enlace a todos los enrutadores adjuntos.

2.2.5.2.2.3 Funciones de la Subred Independiente.

Las funciones de la subcapa Subred Independiente definen como CLNS envía los paquetes a través de la red CLNP y como estos servicios son ofrecidos a la Capa de Transporte. La función de enrutamiento es en sí dividida en cuatro procesos: actualización, decisión, envío y recepción. Los procesos de envío y recepción como sus nombres lo indican son los responsables de la transmisión y recepción de PDUs.

El proceso de actualización es responsable de la construcción de LSDs L1 y L2, para realizar dichas bases de datos se inunda *(flooding)* un área de LSPs L1, y de LSPs L2 en todas las adyacencias L2.

Una vez que el proceso de actualización ha construido la LSD, el proceso de decisión usa la información de esta base de datos para calcular las rutas más cortas. El proceso usa éstas rutas para construir una Tabla de Enrutamiento. Se realizan cálculos por separado empleando el SPF para rutas L1 y L2.

Las métricas que usa IS-IS para calcular la ruta más corta son:

- **Default,** que debe ser soportada por cada enrutador IS-IS.
- **Delay,** que es opcional y refleja el retardo de la red.
- **Expense,** que es opcional y refleja el costo monetario del uso de la subred.
- **Error,** que refleja la probabilidad de error de la subred.

Cada métrica es expresada como un número entero entre 0 y 63, en caso de que las métricas posean el mismo valor para cada interfaz, se emplea el conteo de saltos como desempate.

[28] Verificar la sección 2.2.5.2.1 de OSPF.

2.2.5.3 Protocolos Híbridos.

2.2.5.3.1 Enhanced Interior Gateway Routing Protocol (EIGRP).

Como su nombre lo indica se trata de una mejora sobre el ya existente Interior Gateway Routing Protocol (IGRP), debida a la necesidad de tener un protocolo de enrutamiento capaz de ser utilizado por redes de proporciones medianas y con topologías diversas. Es compatible con enrutadores que tienen configurado IGRP y se redistribuye automáticamente si se usan números de proceso iguales entre ambos protocolos.

Al igual que su predecesor, EIGRP es un protocolo propietario de Cisco Systems y reúne características de los Link State Protocols con los Distance Vector Protocols, por ello es que se le considera como un protocolo híbrido.

Tal y como sucede con los LSP, EIGRP envía sus actualizaciones por medio de LSAs a sus vecinos por lo que las redes pueden converger más rápidamente, estas son: no periódicas, parciales y limitadas. No periódicas porque no son enviadas en intervalos regulares sino por evento; parciales pues sólo incluyen las rutas que han sufrido cambios; limitadas pues se envían a los enrutadores que fueron afectados por estos cambios. EIGRP no usa más del 50% del ancho de banda de un enlace para su operación, mismo que es susceptible de ser cambiado a algún otro valor.

EIGRP tiene cuatro componentes:

a. Protocol Dependent Modules.
b. Reliable Transport Protocol (RTP).
c. Neighbor Discovery/Recovery.
d. Diffusing Update Algorithm (DUAL).

a. Protocol Dependent Modules.

EIGRP tiene módulos para IP, IPX y AppleTalk que son responsables de las tareas de enrutamiento de cada protocolo. Cada uno de ellos es responsable de encapsular los protocolos en su respectivo protocolo de Capa 3.

b. Reliable Transport Protocol.

El RTP, se encarga de la entrega y recepción confiable de los paquetes de EIGRP. La entrega se hace utilizando la dirección multicast 224.0.0.10. Cada vecino que reciba un paquete dirigido a ésta, mandará una confirmación pero hacia la dirección unicast que originó el anuncio.

El RTP usa múltiples tipos de paquetes, todos ellos identificados por el número 88 en el campo de Protocol del encabezado IP:

- **Hello Packets,** que se usan para el proceso de descubrimiento de vecinos.
- **Acknowledgments;** que son iguales a los *Hello Packets* pero sin información.

- **Updates,** que transportan la información de enrutamiento. Estos paquetes son sólo transmitidos cuando los enrutadores requieren información.
- **Queries y Replies,** que son usados para cálculos del protocolo.
- **Request,** usado sólo por versiones antiguas de EIGRP.

c. Neighbor Discovery/Recovery.

Debido al tipo de actualización de EIGRP, es necesario saber sobre el estado de los enrutadores. Con la información de cada vecino se genera la Tabla de Vecinos. Para saber sobre los vecinos se emplean los *Hello Packets* que son enviados cada 5 segundos menos un tiempo aleatorio para evitar colisiones, en el caso de enlaces punto a punto los *Hello Packets* serán enviados cada 60 segundos.

d. Diffusing Update Algorithm (DUAL).

EIGRP usa DUAL para calcular las mejores rutas y distribuirlas, manteniendo la red libre de *loops*. Usa ciertos conceptos para su operación tales como Adyacencia, Feasible Distance, Feasible Successor y Successor.

La Adyacencia se refiere al hecho de que exista un enlace virtual entre dos vecinos a través de un enlace de datos. Cuando ya está establecida, el enrutador recibirá actualizaciones desde sus vecinos.

La Feasible Distance es la menor métrica calculada hacia cada uno de los destinos. La Feasibility Condition (FC) es aquella con la cual se compara si la distancia reportada es menor que la Feasible Distance del enrutador. Si la distancia anunciada de un vecino a un destino cumple con la FC el vecino se convierte en un Feasible Successor para ese destino.

Para cada destino en la Tabla Topológica, la ruta con la menor métrica hacia un destino es elegida y puesta en la Tabla de Enrutamiento. El vecino que anunció esa ruta será el Successor o el siguiente salto para los paquetes dirigidos a ese destino.

EIGRP es un protocolo *classless*, en las actualizaciones sobre una ruta se incluye la máscara de red con la cual se configuró, permitiendo el uso del VLSM para sumarizar las rutas hacia un destino.

2.2.5.4 Border Gateway Protocol (BGP).

BGP es un protocolo de enrutamiento Inter-Sistemas Autónomos, definido por el RFC-1771, actualmente es usado para intercambiar información de enrutamiento en Internet, debido a que maneja varios parámetros de ruta para definir políticas sobre las trayectorias permitidas para el envío de datos y mantiene un escenario estable de enrutamiento. La versión 4 es la que actualmente se usa y comúnmente es referida como BGP-4.

Para su operación establece una conexión única, basada en direcciones unicast, con cada uno de sus vecinos de BGP. Asegura la confiabilidad de dicha conexión usando TCP

(mediante el puerto 179), por ello se deben establecer comunicaciones individuales con cada *peer*[29].

Para calcular la mejor ruta BGP no usa una métrica como en el caso de EIGRP u otros protocolos, emplea una serie de parámetros llamados atributos de ruta *(path attributes).* Uno de ellos es el AS_Path, que contiene la lista de números de AS a través de los cuales un paquete debe de pasar para llegar a su destino. Debido a este parámetro, BGP es considerado como un protocolo de enrutamiento Path Vector.

La ruta más corta a un destino es aquella que contiene el menor número de ASs en la lista del AS_Path. Éste cumple con otra función importante, la de evitar *loops*; mediante la revisión de los números en el AS_Path, si un identificador es detectado dos veces, la actualización no será aceptada.

BGP no tiene conocimiento detallado de las topologías dentro de cada AS, para ello se emplea un IGP. Cuando en una topología existen enlaces paralelos y de igual costo hacia un destino BGP, más específicamente eBGP, selecciona sólo una ruta, difiriendo de otros protocolos de enrutamiento que pueden hacer balanceo de carga en situaciones similares.

Cuando un enrutador que usa BGP intercambia información de enrutamiento con otro enrutador que tiene el mismo identificador de AS, es conocido como Internal BGP (iBGP). Pero si el identificador de AS es diferente, entonces se conoce como External BGP (eBGP). Los eBGP *peers* generalmente están directamente conectados; los enrutadores iBGP no necesitan estar directamente conectados para establecer su conexión, pueden lograrlo a través de otros que incluso no operen con BGP. Existen atributos propios para eBGP e iBGP; algunos de ellos sólo tienen sentido en iBGP y viceversa.

Las actualizaciones son incrementales y parciales. Incrementales pues éstas tienen números consecutivos y sustituyen a la anterior; parciales pues sólo envían la información sobre los cambios en la red. Debido a que no hay actualizaciones periódicas BGP utiliza mensajes *Keepalive* para verificar el estado de la conexión establecida.

2.2.5.4.1 Tipos de mensajes de BGP.

BGP usa 4 tipos de mensajes en su operación:

a. Open.
b. Keepalive.
c. Update.
d. Notification.

[29] En este punto, por peer entenderemos a un enrutador que use BGP con el que se haya establecido una conexión.

a. Mensaje Open.

Cada vecino los usa para identificarse a sí mismo y especificar los parámetros operacionales de BGP. Éste contiene la siguiente información:

- Versión BGP.
- Número de AS.
- Identificador BGP.

b. Mensaje Keepalive.

Verifican el estado de la conexión establecida y son enviados cada 60 segundos (en la implementación Cisco).

c. Mensaje Update.

Anuncia las rutas factibles o viables, e incluye la siguiente información:

- Network Layer Reachability Information (NLRI).
- Path Attribute.
- Withdrawn Routes.

d. Mensaje Notification.

Son enviados cuando ocurre un error y provoca que BGP cierre una conexión entre *peers*.

2.2.5.4.2 Atributos de Ruta (Path Attributes).

Un Path Attribute es una característica que se envía en los mensajes Update de BGP. Son usados para proveer la información necesaria para el enrutamiento, sirven de igual manera para establecer y comunicar políticas de enrutamiento.

Todos ellos se pueden clasificar en alguna de las siguientes categorías:

- Bien Conocidos Obligatorios.
- Bien Conocidos Discrecionales.
- Opcionales Transitivos.
- Opcionales No-Transitivos.

Los Bien Conocidos son reconocidos por todas las implementaciones de BGP, mientras que los Opcionales pueden ser o no soportados (reconocidos) por todas las implementaciones de BGP.

Los Obligatorios deben de ser incluidos en todas las actualizaciones que realice BGP, mientras que los Discrecionales pueden ser o no enviados en las actualizaciones.

Transitivos, porque la implementación de BGP podrá aceptar el atributo y enviarlo a otros *peers* de BGP. No-Transitivos, pues el atributo podrá ser ignorado pero servirá para poder aplicar o distribuir ciertas políticas.

A continuación se mencionan algunos de los atributos más importantes:

Origin Attribute.

Éste especifica el origen de una actualización. Cuando BGP tiene múltiples rutas hacia un destino, toma este atributo como factor para escoger una. Los orígenes pueden ser: IGP, EGP o Internet. Es un atributo Bien Conocido Obligatorio.

AS_Path Attribute.

Éste usa una secuencia de números para describir todos los ASs por los cuales ha pasado la actualización, empezando con el más reciente y finalizando con el AS que la originó. Cada enrutador BGP suma su propio identificador de AS a la lista cuando la actualización es enviada a otro AS. Es un atributo Bien Conocido Obligatorio.

Next-Hop Attribute.

Es la dirección IP del enrutador que es el *next-hop* para alcanzar un destino. Es un atributo Bien Conocido Obligatorio.

Local_Pref Attribute.

Es usado sólo en actualizaciones entre iBGP *peers*. Indica un grado de preferencia sobre diferentes rutas hacia un destino, se toma la ruta con mayor valor. Es un atributo Bien Conocido Discrecional.

Multi_Exit_Disc Attribute.

En contraparte del Local_Pref Attribute, le permite a un AS informar a otro sobre su punto de ingreso al mismo. Si todas las rutas que ingresan son iguales hará una comparación de los MED y el que tenga menor valor será utilizado. Este atributo es Opcional No-Transitivo.

Community Attribute.

Está diseñado para simplificar la aplicación de políticas. Provee una forma de agrupar destinos, llamados comunidades, mismos a los que se les pueden aplicar políticas de enrutamiento. Este atributo es Opcional Transitivo.

Originator_ID.

Éste es generado y usado por los Route Reflectors (RR) para evitar los *loops* de enrutamiento. Este atributo es Opcional No-Transitivo.

2.2.5.4.3 Sincronización entre iBGP y un IGP.

Por las características antes mencionadas de BGP de poder operar dentro de un AS para distribuir rutas, se podría pensar que no es necesario un IGP y exclusivamente tener BGP en los enrutadores. Esto no es totalmente cierto, pues BGP necesitará de un IGP para poder realizar el envío de paquetes correctamente a su destino, de lo contrario, se tendrían que mantener rutas estáticas en los enrutadores para llevar a cabo esta tarea.

Un iBGP *peer* no redistribuirá una ruta aprendida a través de otro iBGP *peer* a un tercero dentro del mismo AS, sólo lo hará con enrutadores pertenecientes a otro AS. Por ello es importante mantener una topología de malla total *(full mesh)* entre los enrutadores del AS, esto es útil para:

- Prevenir los *loops* de enrutamiento de BGP dentro del AS.
- Asegurar que todos los enrutadores sepan cómo enviar los paquetes en camino a su destino de BGP.

La sincronización entre un IGP y BGP se puede entender de la siguiente manera:

Antes de que una ruta que se aprendió de un vecino de iBGP sea puesta en la Tabla de Enrutamiento o anunciada a un BGP *peer*, ésta debe de ser conocida a través de un IGP.

Sin embargo así como está descrita anteriormente la sincronización, pueden existir problemas en el envío de paquetes a su destino correctamente, dado que el enrutador en su IGP puede no tener un *next-hop* para los destinos enlistado en la Tabla de Enrutamiento de BGP. Es posible que exista una manera de mantener rutas de BGP usando solamente al IGP para establecer las conexiones de los BGP *peers*.

Si no se realiza la sincronización entre el IGP y el BGP, es posible que las rutas de BGP puedan ser aprendidas por enrutadores vecinos de iBGP. De esta manera se pueden enviar correctamente los paquetes a su destino.

BGP necesita una topología *fully meshed* por lo cual la sincronización debe deshabilitarse permitiendo que las rutas anunciadas por otros enrutadores puedan entrar a la Tabla de Enrutamiento sin informar al IGP. Otro caso en que la sincronización puede deshabilitarse es cuando un AS no cursará tráfico de otros ASs, entonces no será necesaria esta operación permitiendo a BGP converger más rápidamente y anunciar menos rutas a través del IGP.

BGP mantiene cierta independencia con el IGP, cuando ocurren cambios a nivel de BGP, el IGP no necesita saber de los mismos pues sólo sirve para el envío correcto de paquetes, sólo BGP realiza los ajustes necesarios en su información. Cuando ocurre un cambio en el IGP, BGP puede seguir operando normalmente.

Cuando iBGP intente crear una topología *fully meshed*, se crea otro problema: puede resultar muy difícil establecer todas las conexiones necesarias, si es que se trata de una red de grandes proporciones, por ello BGP tiene cuatro características que posibilitan manejar este problema:

a. Peer Groups.
b. Communities.
c. Route Reflectors.
d. Confederations.

a. Peer Groups.

Regularmente en redes de BGP es necesario aplicar ciertas políticas de un enrutador a un conjunto de éstos, lo que se puede realizar haciendo uso de *peer* groups, que simplificará la configuración y la administración del grupo de enrutadores que compartirán políticas comunes.

Un *Peer Group* está definido en un enrutador por el nombre y el conjunto de políticas a ser aplicadas, posteriormente éste se agregará al *Peer Group*. El uso de *Peer Groups* puede mejorar el desempeño de un enrutador, pues en vez de consultar constantemente una base de datos con las políticas de enrutamiento para cada actualización, el enrutador puede consultar la base de datos sólo una vez y crear una única actualización y enviando luego copias a todos los enrutadores dentro del *Peer Group*. Más políticas pueden ser aplicadas a uno o más miembros del *Peer Group*, si éste es el caso se puede aplicar directamente al enrutador, además de las políticas compartidas del grupo.

b. Communities.

Mientras que los *Peer Groups* aplican un conjunto de políticas a un grupo de enrutadores, las Communities, aplican políticas a un grupo (conjunto) de rutas. Se pueden establecer más de un valor de Community para una ruta, y gracias a ello se pueden ajustar las políticas basadas en los atributos contenidos en las actualizaciones.

c. Route Reflectors.

Los Route Reflectors (RR) ofrecen una alternativa al problema de tener que establecer conexiones con todos y cada uno de los BGP *peers*. Si un enrutador dentro de un AS, es configurado para ser RR el resto de los iBGP *peers*, conocidos como clientes, establecerán conexiones exclusivamente con el RR en lugar de hacerlo con todos y cada uno de los clientes. En su totalidad el RR y sus clientes son conocidos como cluster.

Las rutas de un iBGP pueden ser anunciadas (reflejadas) a otro cliente a través del RR; un cliente puede establecer conexiones con otros enrutadores de un AS diferente, pero dentro del AS con el único enrutador que pueden establecer conexión es con el RR. Este último puede establecer conexiones con enrutadores internos y externos al AS y pueden reflejar las rutas a sus clientes.

La funcionalidad del RR sólo debe ser entendida por él mismo, así los demás enrutadores, desde su perspectiva, estarán estableciendo conexión con un iBGP *peer*. Esto es una funcionalidad muy atractiva, pues los enrutadores con implementaciones básicas de BGP pueden continuar siendo clientes dentro de un cluster.

El propósito principal de los RR es reducir el número requerido de conexiones para establecer vecinos proponiendo sólo un punto de peering para múltiples vecinos, lo cual, por sí mismo, introduce un sólo punto de falla dentro del sistema, es por ello que incluir otro RR en la red resulta altamente recomendable, en caso de que uno de los RRs falle, el o los restantes podrán mantener las sesiones de BGP y por tanto el enrutamiento se puede llevar a cabo de forma normal.

Todo RR dentro del AS necesita tener configurado un Cluster-ID para que cualquier otro RR pueda reconocer sus actualizaciones dentro del mismo. Existe también el Cluster-List que servirá para identificar la ruta por donde provino una actualización. Usando este atributo un RR puede identificar si la información de enrutamiento ha caído en un *loop* y por lo tanto deba ser descartada.

Si un RR recibe múltiples rutas a un mismo destino, ésta será anunciada dependiendo del origen de la misma:

- Si fue aprendida desde un iBGP *peer* no cliente, será reflejada sólo a los clientes.
- Si fue aprendida de un cliente, será reflejada a todos los clientes y no clientes, excepto al cliente que la originó.
- Si fue aprendida desde un eBGP *peer*, es reflejada a todos lo clientes y los no clientes.

d. Confederations.

El uso de Confererations es otra solución de BGP, pero su uso está fuera del alcance del presente documento.

CAPÍTULO TRES
VPNs basadas en MPLS

3.1 Multiprotocol Label Switching (MPLS).

3.1.1 Introducción.

Como hasta ahora hemos visto, el envío de paquetes hacia un destino determinado se realiza única y exclusivamente basado en la dirección IP destino contenida en cada uno de ellos. Además la decisión de qué ruta se ocupará para el enviar los paquetes se realiza *hop-by-hop*. Esto continua funcionando correctamente, pero desde hace algún tiempo la Internet Engineering Task Force (IETF) en conjunto con empresas vendedoras de enrutadores, comenzaron a desarrollar mejores métodos para el envío de paquetes, nuevas técnicas y arquitecturas, que permitan más flexibilidad y nuevas posibilidades a las redes ya existentes.

Un ejemplo de problemática en el envío tradicional de paquetes se presenta cuando ocurre un cambio en la información de enrutamiento, ésta se debe llevar a todos los dispositivos en la red, lo cual involucra un tiempo de convergencia de la misma pero además otra particularidad: se realizan cambios en la Tabla de Enrutamiento y por lo tanto

los paquetes cambian las rutas hacia sus destinos, afectando de manera sensible el desempeño de los enrutadores.

Es deseable entonces que mediante algún mecanismo menos susceptible a este tipo de cambios, se realice el envío. Este mecanismo agregaría una etiqueta al frente de cada paquete y realizar el enrutamiento basado en ésta, haciendo de ella un índice dentro de una tabla interna, encontrar la interfase de salida correcta se vuelve una simple búsqueda en la misma. Usando esta técnica, el enrutamiento se puede llevar a cabo rápidamente, con la posibilidad de reservar recursos a lo largo de la trayectoria hacia su destino. Cualquier cambio que se realice será comunicado a través de un nuevo juego de etiquetas. El impacto en los enrutadores se debe reducir, pues sólo se realiza un intercambio de etiquetas, sin la necesidad de recurrir a procesos más complejos.

Hay que notar que dicha tecnología no substituye al enrutamiento tradicional, simplemente lo simplifica y hace más eficiente el envío de paquetes.

Con la introducción de dichas etiquetas, un Proveedor de Servicios – Service Provider (SP) puede implementar otro tipo de mejoras basados en éstas, permitiendo incrementar sus niveles de servicio.

Esta nueva idea tiene varios nombres propietarios; la IETF comenzó a normalizar la idea bajo el nombre de Multiprotocol Label Switching (MPLS), que está descrito en el RFC-3031 y algunos otros. Esta tecnología emergente introduce una arquitectura que permite realizar el intercambio de etiquetas (label switching) combinando la rapidez del envío de paquetes de Capa 2 con los beneficios tiene el enrutamiento de Capa 3.

MPLS asigna etiquetas a los paquetes para que sean transportados a través de redes basadas en paquetes o basadas en celdas[1]. El mecanismo para el envío de los paquetes por toda la red es el intercambio de etiquetas (label swapping) en donde los paquetes acarrean etiquetas de tamaño fijo que le indica a los nodos de envío (enrutadores) a lo largo de la trayectoria, cómo procesarlos y enviarlos.

El primer problema que surgió con esta nueva tecnología es ¿en dónde se debe poner la etiqueta? Debido a que los paquetes IP puro no fueron diseñados para circuitos virtuales, no tienen un campo especial que permita el acomodo de la etiqueta, por ello el encabezado MPLS es puesto al frente del encabezado IP y antes del encabezado de la Capa Física.

MPLS brinda la posibilidad de que un paquete puede acarrear una pila (stack) completa de etiquetas en él, lo que permitirá obtener mejoras importantes en la red que se habilite para manejar esta tecnología, siendo las más importantes: Ingeniería de Tráfico (Traffic Engineering), Redes Privadas Virtuales (Virtual Private Networks) y Túneles Recursivos.

[1] El presente documento sólo hará referencia a redes basadas en paquetes, la operación basada en celdas está fuera del alcance del mismo.

3.1.2 Arquitectura del MPLS.

Nueva terminología es introducida en este punto para describir el funcionamiento de MPLS.

Un Label Switch Router (LSR) es un enrutador que realiza el envío de paquetes basado en etiquetas. Tiene la capacidad de asignar y distribuir asociaciones de etiquetas a otros LSRs dentro de la red MPLS.

Un Edge-LSR es un enrutador que además de las funciones de un LSR tiene otras dos importantes funciones, la de imponer (push) y retirar (pop) etiquetas a los paquetes en los puntos de entrada y salida al dominio MPLS. Al imponer puede tratarse de una sola etiqueta o una pila de ellas; al retirar se hará con la última etiqueta de la pila.

El Edge-LSR puede realizar el envío de paquetes IP sin MPLS, también etiquetar paquetes y enviarlos a nodos con MPLS o bien puede retirar la etiqueta, buscar en la Tabla de Enrutamiento y enviar el paquete por la interfase correspondiente. En la figura 3.1 podemos observar la arquitectura de un Edge-LSR.

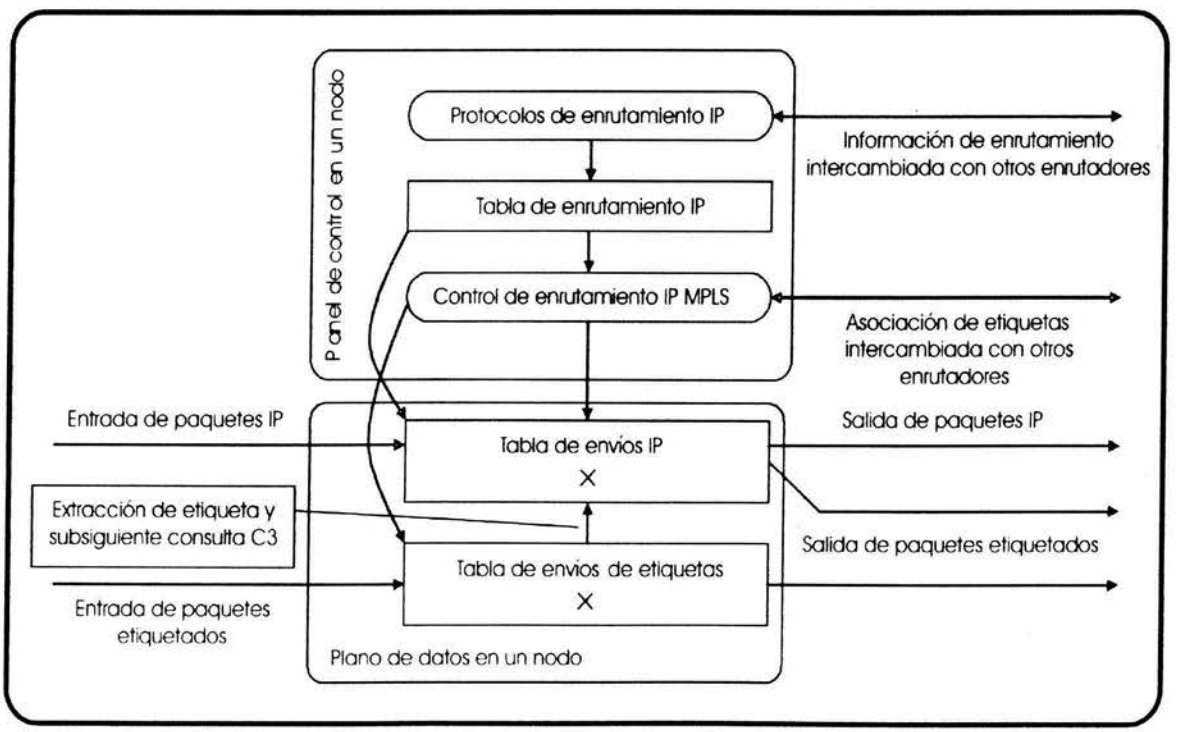


Figura 3.1 Arquitectura de un Edge-LSR.

Las etiquetas sólo tienen significado local; dos enrutadores diferentes pueden crear paquetes sin relación alguna con la misma etiqueta y transmitirlos hacia un mismo enrutador para que éste los envíe por una misma interfase de salida.

Para realizar el envío de los paquetes etiquetados los nodos necesitan conocer los destinos de éstos, lo cuál es llevado a cabo mediante la Forwarding Equivalence Class (FEC), que simplemente es cuando los enrutadores agrupan diferentes flujos de información que tengan como destino a un mismo enrutador o una LAN y usan la misma etiqueta para ellos. Los paquetes se enviarán de la misma manera y por la misma ruta. Con MPLS un paquete es asignado a una FEC en particular, sólo una vez, por el nodo en el cuál se entra al dominio MPLS.

El identificador que le asigna a un paquete la FEC a la que pertenece será la etiqueta propiamente dicha que se le coloca al paquete IP junto con otra información útil para MPLS y forma parte del Encabezado MPLS – MPLS Label Stack Header.

3.1.3 Envío de paquetes en MPLS y los Label Switched Paths (LSPs).

Los paquetes que viajan en una red MPLS tienen un punto de ingreso y uno de egreso, estos puntos serán LSRs, así mismo serán los extremos de un Label Switched Path (LSP). Éste está formado de un conjunto de LSRs a través de los cuales un paquete etiquetado debe viajar para llegar a su destino dentro de una FEC determinada. El LSP es unidireccional, de tal modo que se debe usar un LSP diferente para el regreso del tráfico perteneciente a la FEC, las trayectorias de ambos pueden no coincidir. El LSP es creado antes de cursar tráfico alguno por el mismo. Mientras el paquete atraviesa la red MPLS, cada LSR intercambia (swapping) la etiqueta de origen (ingreso) por una etiqueta de salida (egreso) hasta el último LSR de la LSP. En la figura 3.2 se esquematiza tanto el intercambio de la etiqueta como su retiro por parte de un LSR.

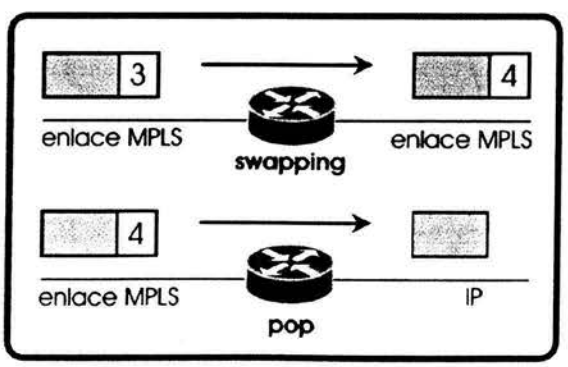


Figura 3.2 Intercambio y retiro de etiqueta.

Cada LSR contiene dos tablas que contienen la información que MPLS necesita para su operación. La Label Information Base (LIB) contiene todas las etiquetas asignadas por el LSR y los mapas de las etiquetas asignadas y recibidas de cualquier vecino. La Label Forwarding Information Base (LFIB) es usada para el envío de paquetes y contiene sólo aquellas etiquetas en uso por el LSR que la contiene.

3.1.4 Encabezado MPLS – MPLS Label Stack Header.

En la sección 3.1.1 se hizo referencia a la posición que debe tener el Encabezado MPLS – MPLS Label Stack Header, entre el encabezado de Capa 2 y el de Capa 3 como se muestra en la figura 3.3.

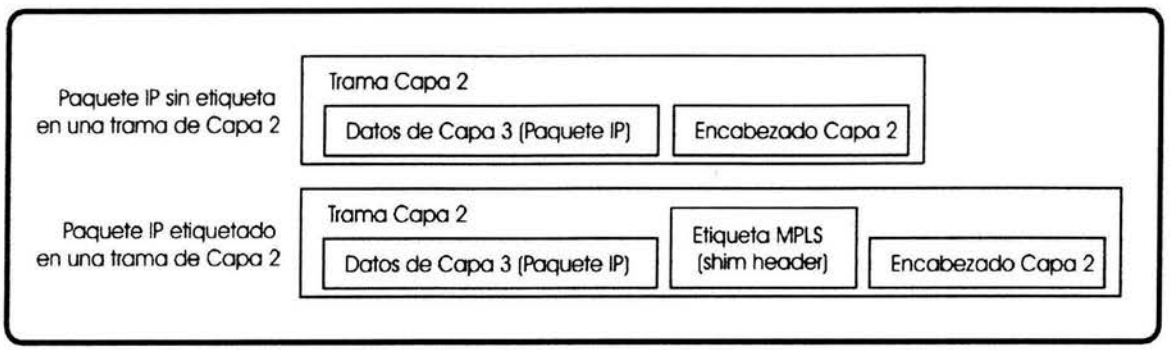


Figura 3.3 Posición de la etiqueta de MPLS en una trama de Capa 2

Debido a que el encabezado MPLS es insertado en este lugar, también es conocido como *shim label*. El encabezado contiene: la etiqueta MPLS de 20 bits; un campo de Class of Service (CoS) de 3 bits, que también son conocidos como bits experimentales (Exp) en documentación de la IETF; 8 bits que corresponden al campo de Time To Live (TTL) con función similar a la del encabezado IP y un bit para el campo de Bottom-of-Stack. El encabezado se ilustra en la figura 3.4.

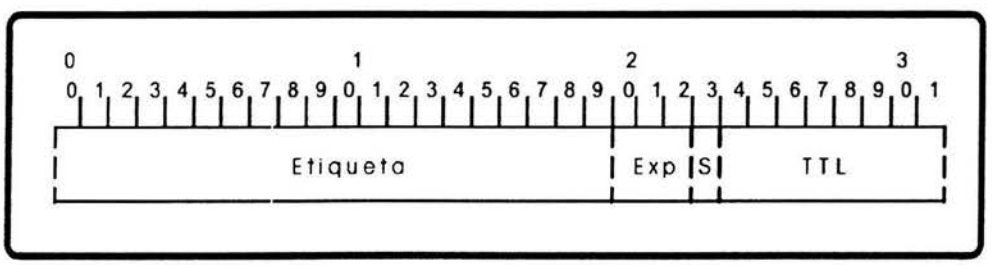


Figura 3.4 Encabezado de una pila de etiquetas MPLS.

Este último bit, el Bottom-of-Stack, hace posible la existencia de una pila de etiquetas MPLS en un sólo paquete. Este bit es igual a uno para la última etiqueta de la pila y cero para el resto de las etiquetas.[31] Algunas aplicaciones de MPLS hacen uso de esta característica, como se verá en su momento en este documento.

[31] Tomado del RFC-3032, sección 2.1.

3.1.5 Intercambio de etiquetas en el Frame-mode de MPLS.

Cuando un paquete etiquetado llega a un enrutador con MPLS configurado, la etiqueta es comparada con la LFIB y éste es enviado por la interfase adecuada, realizado el reemplazo o retiro de la etiqueta como se muestra continuación (figura 3.5).

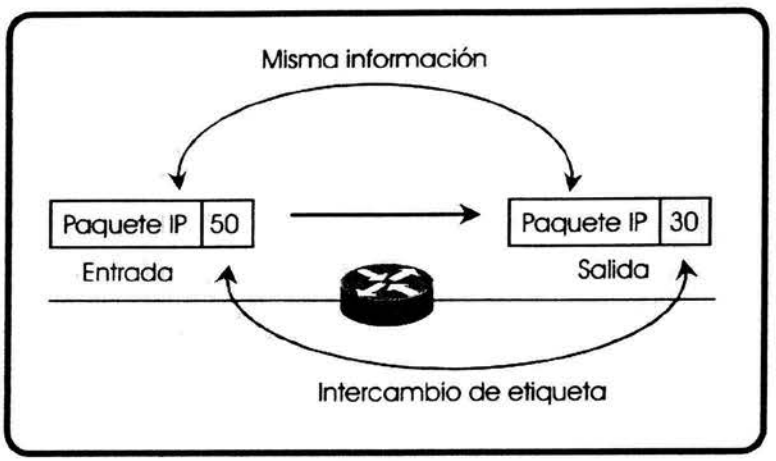


Figura 3.5 Intercambio de etiqueta.

Un LSR puede realizar cualquiera de las siguientes acciones:

Pop Tag	Remueve la última etiqueta y envía el paquete estando o no etiquetado.
Swap Tag	Reemplaza la última etiqueta del encabezado por otra con valor diferente.
Push Tag	Impone una etiqueta o un conjunto de etiquetas.
Aggregate	Quita la última etiqueta y realiza una búsqueda en la Tabla de Enrutamiento para el envío correspondiente.
Untag	Quita la última etiqueta y envía el paquete al *next-hop* correspondiente.

Tabla 3.1 Acciones de un LSR.

3.1.6 Envío de paquetes MPLS que contiene una pila de etiquetas.

Sin importar que el paquete contenga una pila de etiquetas o una sola etiqueta, el envío de paquetes es realizado de la misma manera. En cualquier caso la decisión de envío se basa en la última etiqueta (superior de la pila) que contenga el paquete, ignorando el resto si se trata de una pila. Esto permite que los Edge-LSR puedan realizar la clasificación de los paquetes de acuerdo a un conjunto de reglas sin que de ello tengan conocimiento los enrutadores que se encuentran en la dorsal (core) de la red. La forma en que se realiza el intercambio de etiquetas con la pila de etiquetas de MPLS se puede observar de forma gráfica en la figura 3.6.

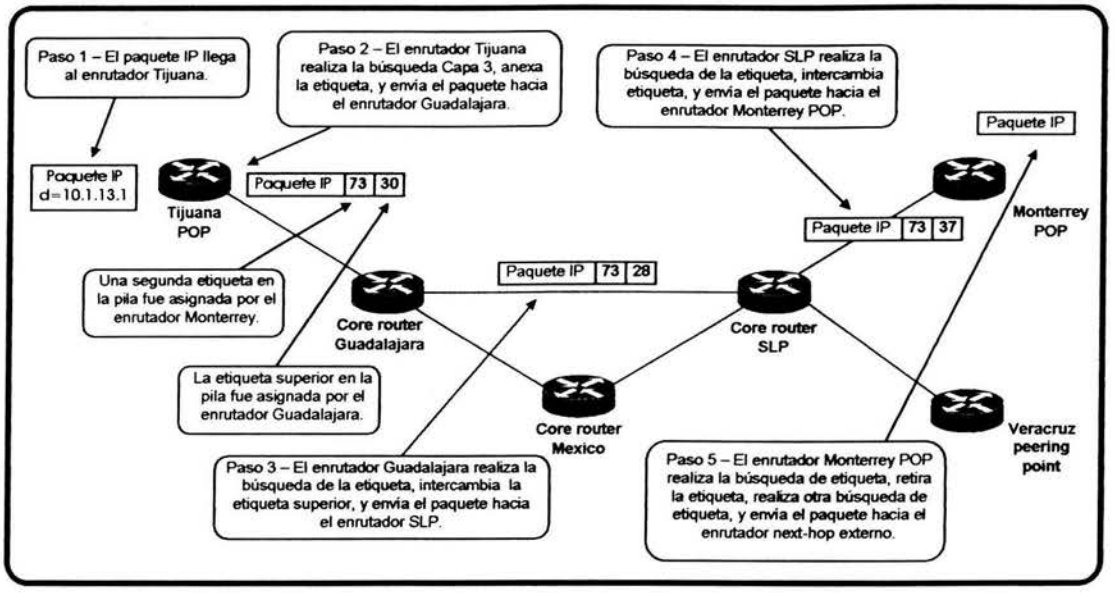


Figura 3.6 Intercambio de etiquetas con la pila de etiquetas de MPLS.

3.1.7 Distribución de las Asociaciones de Etiquetas – Label Binding Propagation.

El intercambio de asociaciones de etiquetas para direcciones unicast se realiza mediante el *Tag Distribution Protocol* (TDP) propietario de Cisco o el *Label Distribution Protocol* (LDP) desarrollado por la IETF.

Cuando se configura MPLS en alguna interfase, el TDP o el LDP inician el proceso para crear la LIB. El enrutador entonces intenta conocer a otros LSRs a través de paquetes llamados *Hello Packets*, que son enviados como paquetes broadcast o multicast, realizando el descubrimiento de los LSR vecinos automáticamente. Una vez que el LSR es encontrado, se establece una sesión mediante TCP, con los puertos 711 para TDP y 646 para LDP.

3.1.8 Asociaciones de etiquetas y su distribución.

Tan pronto como la LIB es creada, una etiqueta es asociada a cada una de las FECs que conozca el enrutador. Para el caso de la operación de MPLS en Frame-mode, el método para establecer y distribuir las etiquetas es llamado Control Independiente – Independent Control con Distribución de Bajada de Etiquetas sin Solicitud – Unsolicited Downstream Label Distribution y de Retención Liberal – Liberal Retention.

Control Independiente de la asociación de etiquetas, pues el LSR reconoce una FEC en particular y toma la decisión de poner una etiqueta independientemente a la distribución

de las asociaciones a sus vecinos, en otras palabras, la impone sin importar si ha recibido una etiqueta con el mismo valor de un vecino o no.

Sin Solicitud (unsolicited), pues el LSR asigna la etiqueta y envía su mapa de asociaciones al siguiente vecino (upstream neighbor) sin importar si éste necesita o no la etiqueta. Existe también la distribución bajo demanda (on demand) cuando el LSR asigna la etiqueta sólo cuando el siguiente vecino se lo solicita.

De Bajada *(downstream)* cuando el LSR asigna una etiqueta en el sentido contrario al cual la etiqueta fue solicitada. Toda asociación es anunciada inmediatamente al resto de los enrutadores a través de las sesiones ya existentes de TDP o LDP.

Un LSR adyacente recibe el mapa de etiquetas y lo almacena en su LIB y lo usa en su LIB o en la LFIB, si el mapa fue recibido desde el *downstream neighbor*, que es el *next-hop* para una FEC en particular. Este método de almacenamiento es conocido como Modo de Retención Liberal – Liberal Retention Mode que es opuesto al modo de Retención Conservativo – Conservative Retention Mode donde el LSR retiene las etiquetas asignadas a un prefijo por sus enrutadores *downstream*.

3.1.9 Retiro de Etiquetas en el Penúltimo Salto – Penultimate Hop Popping.

Cuando un paquete etiquetado llega a un enrutador es probable que se requiera quitar la etiqueta y mandarlo a su destino final en un mismo punto, es decir, es necesario realizar una doble búsqueda para saber qué hacer con el paquete y con ello se agrega complejidad a las operaciones en un mismo enrutador. Esto dio pauta para que el Retiro de Etiqueta en el Penúltimo Salto – Penultimate Hop Popping haya sido introducido en la arquitectura de MPLS.

Con esta técnica el Edge-LSR puede pedirle a su antecesor *(downstream)* de un LSP determinado que elimine la etiqueta superior de la pila de un paquete que haya sido identificado para un destino a través de ese Edge-LSR en específico y así reducir la carga de trabajo. La figura 3.7 ilustra este ejemplo.

Esta técnica no afecta la lógica del intercambio de etiquetas ya revisada.

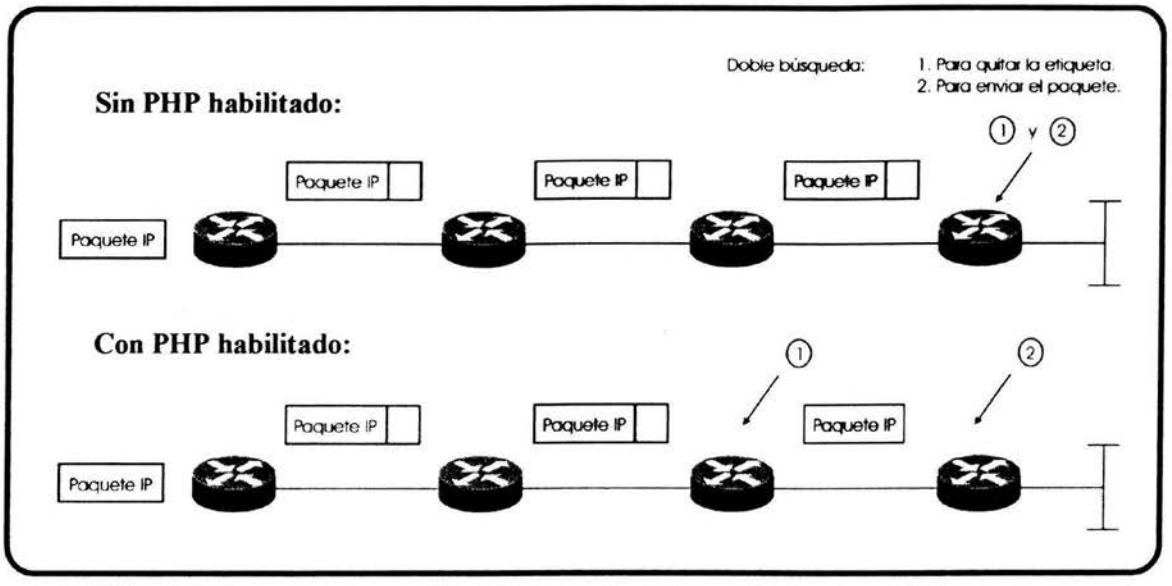


Figura 3.7 Funcionabilidad de PHP.

3.1.10 Encapsulación de MPLS a través de enlaces Ethernet.

Como consecuencia del uso de MPLS en una red, tenemos que los paquetes aumentan su tamaño, debido a la adición de etiquetas al paquete IP. Cada encabezado de MPLS (uno por etiqueta) tiene un tamaño fijo de 4 octetos (32 bits) de longitud. Si bien el encabezado MPLS no es un aumento muy grande, es muy significativo cuando se trata de enviar los paquetes a través de enlaces Ethernet. Independientemente de la implementación que se trate Ethernet, Fast Ethernet o Gigabit Ethernet, cada una de ellas tiene un tamaño máximo de frame igual a 1518 octetos con un campo de datos que va desde los 46 a los 1500 octetos lo que significa que si un paquete con este campo igual a 1500 octetos es etiquetado, el frame necesita ser enviado con un tamaño de 1504 octetos. Debido a la restricción en el tamaño de los frames a través de redes Ethernet es porque el MTU es más pequeño que el del tamaño del paquete en cuestión. En un segmento Ethernet, un paquete con longitud mayor al MTU es considerado como un error, conocidos como Giant y por lo tanto sería descartado.

Para evitar que este tipo de paquetes etiquetados se pierdan, a través de las redes Ethernet, Cisco introdujo algunos cambios en su implementación de MPLS que permiten a un puerto Ethernet de un enrutador soportar estos paquetes que son más grandes de 1500 octetos. Esto es logrado aumentando el MTU del puerto hasta 1526 octetos, que es el tamaño de un frame Ethernet, 8 octetos más para 2 niveles de encabezados MPLS. El total de niveles de etiquetas propuesto por Cisco es adecuado en este momento para la introducción de MPLS y de VPNs con MPLS, para aplicaciones que utilicen más de 2 etiquetas, no hay que olvidar aumentar la longitud del MTU, en 4 bytes por cada etiqueta adicional.

3.1.11 Operación de MPLS con BGP.

Típicamente una etiqueta es asociada a cada prefijo IP (anuncios sumarizados) en la Tabla de Enrutamiento de cada LSR, con excepción de las rutas aprendidas a través de BGP. El Edge-LSR de ingreso usa la etiqueta asociada al *next-hop* de BGP para etiquetar los paquetes a ser enviados a los destinos de BGP, lo cual brinda nuevas posibilidades en el diseño. Usualmente se debe tener configurado BGP en cada enrutador de la dorsal (core) de la red de un Proveedor de Servicios – Service Provider (SP) para realizar correctamente el envío de paquetes hacia destinos BGP. De no ser el caso antes propuesto, los enrutadores de la dorsal no podrían enviar los paquetes a su destino como se esquematiza en la figura 3.8.

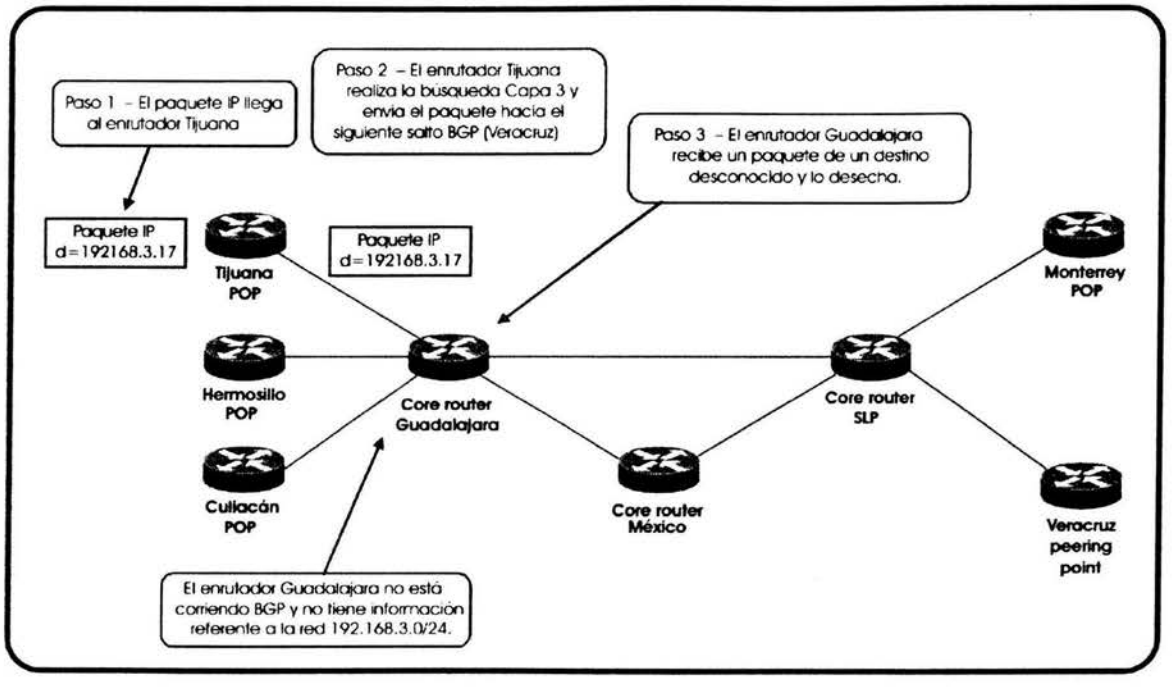


Figura 3.8 Pérdida de conectividad en redes que no tienen BGP en los core routers.

Si en algún punto de la red se realiza sumarización, ya sea manual o automáticamente, un subconjunto de redes será representada por una entrada y dado que una etiqueta es asignada a cada prefijo o entrada de la Tabla de Enrutamiento, se creará una etiqueta que represente muchos destinos.

Cuando un paquete con una etiqueta cuyo destino sea una de las subredes sumarizadas, al arribar al enrutador anterior *(downstream)* al que realizó la sumarización removerá la etiqueta, de acuerdo con el PHP, esto puede causar un problema; El enrutador que realizó la sumarización buscará el destino que contiene el paquete en la segunda etiqueta y al no poder encontrar ese destino en sí mismo, el enrutador puede tirar el paquete. Por lo cual es muy recomendable no realizar sumarización de rutas para las direcciones IP utilizadas como *next-hop* de BGP.

Sin embargo si se habilita MPLS, un Edge-LSR puede etiquetar un paquete para un destino BGP, y transportarlo a su destino correctamente, cómo si éste fuera un paquete etiquetado común y corriente con la etiqueta asociada con el *next-hop* de BGP. Dado que el *next-hop* de BGP siempre es anunciado por el IGP de la red, todos los enrutadores intermedios deben de tener un mapa de las etiquetas a ser usadas para alcanzar ese destino sin la necesidad de tener configurado BGP en toda la trayectoria (ver figura 3.9).

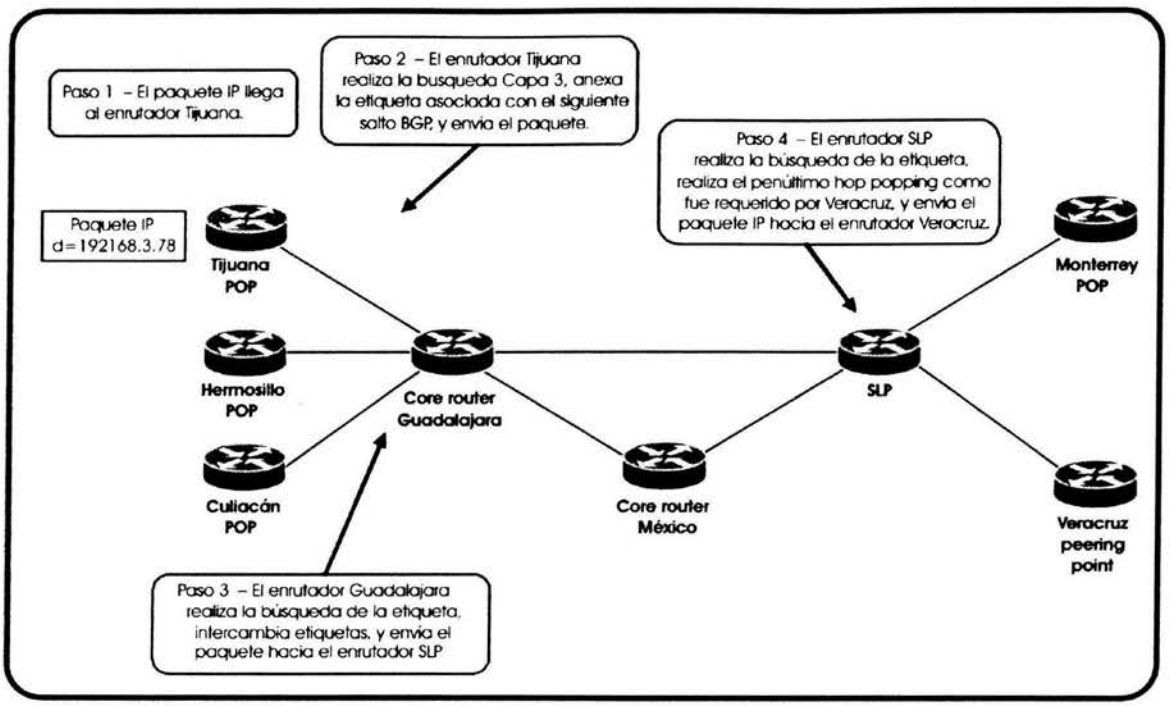


Figura 3.9 Propagación de paquetes hacia destinos BGP en una red habilitada con MPLS.

Al remover BGP de los enrutadores de la dorsal, se reducen los requisitos de operación tanto en memoria para almacenar las rutas así como en el CPU de los enrutadores para realizar el proceso de actualización de rutas de BGP. Por lo anterior el uso de MPLS, aún en redes basadas únicamente en *backbones* de IP puro es bastante recomendable.

3.2 Redes Privadas Virtuales – Virtual Private Networks (VPNs).

Una Red Privada Virtual puede ser definida como una red en la cual la conectividad entre múltiples sitios de un cliente es instalada (deployed) sobre una infraestructura compartida con la misma seguridad y acceso que una Red Privada basada en tecnologías WAN convencionales.

Con nuevas tecnologías que soportan VPNs, se podría pensar que es un concepto de reciente creación, lo cual no es cierto. El concepto VPNs ha sido conocido por más de una década en el mercado de las redes de datos. Estas nuevas tecnologías han permitido crear VPNs más eficientes, escalables pero sobre todo rentables.

3.2.1 Introducción y evolución.

Las primeras redes de computadoras fueron implementadas con líneas dedicadas y con conexiones dial-up. Lo que permitía tener un alto grado de privacidad; sin embargo no eran rentables. Nuevas tecnologías aparecieron, las primeras redes virtuales estaban basadas en X.25 y Frame Relay; posteriormente en ATM. Las VPNs cuentan con un número de componentes bien definidos: los equipos del cliente y los equipos del Proveedor de Servicios.

- El Proveedor de Servicios – Service Provider (SP) es una organización que posee la infraestructura para proveer líneas dedicadas emuladas a sus clientes. Ofrece a los clientes un servicio de Red Privada Virtual (VPN).

- El cliente se conecta a la red del Proveedor de Servicios a través del Customer Premises Equipment (CPE), que es un dispositivo terminal, puede ser un bridge o un enrutador. También es conocido como equipo Customer Edge (CE).

- El equipo que se conecta al CE pero que pertenece al Proveedor de Servicio es conocido como equipo Provider Edge (PE).

- El Proveedor de Servicio tiene usualmente equipo adicional en el core (centro) de la red, estos equipos son llamados **Equipos-P**, por ejemplo P-switches, P-routers (ver figura 3.10).

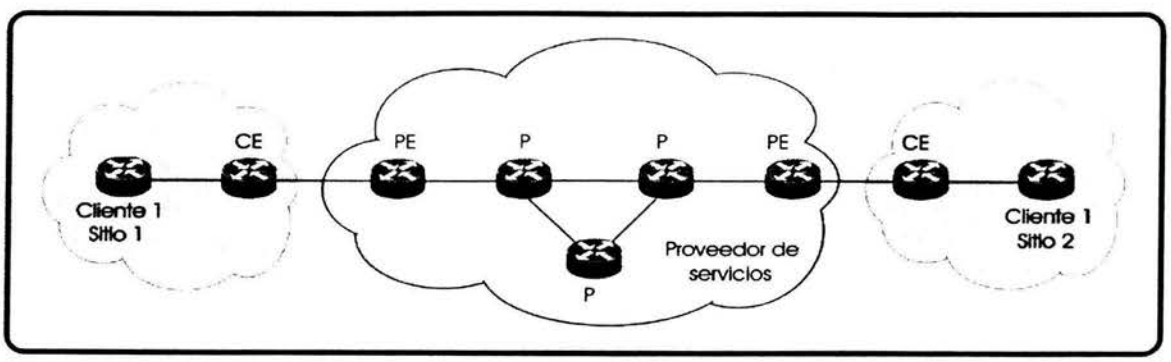


Figura 3.10 Equipos del cliente y del Proveedor de Servicios en una VPN

3.2.2 Implementaciones.

Dos implementaciones de VPNs han ganado popularidad:

- El modelo *Overlay*, en donde el Proveedor de Servicios provee líneas dedicadas emuladas al cliente.
- El modelo Peer-to-Peer en donde el Proveedor de Servicios intercambia información de enrutamiento con el cliente, el proveedor lleva la información entre los diferentes sitios del cliente sin involucrarlo.

3.2.2.1 Modelo Overlay de VPNs.

Este modelo es el más fácil de entender, pues separa claramente el equipo que pertenece al cliente y el que pertenece al Proveedor de Servicios, como se puede apreciar en la figura 3.11.

1. El Proveedor de Servicios le brinda al cliente un conjunto de líneas dedicadas.

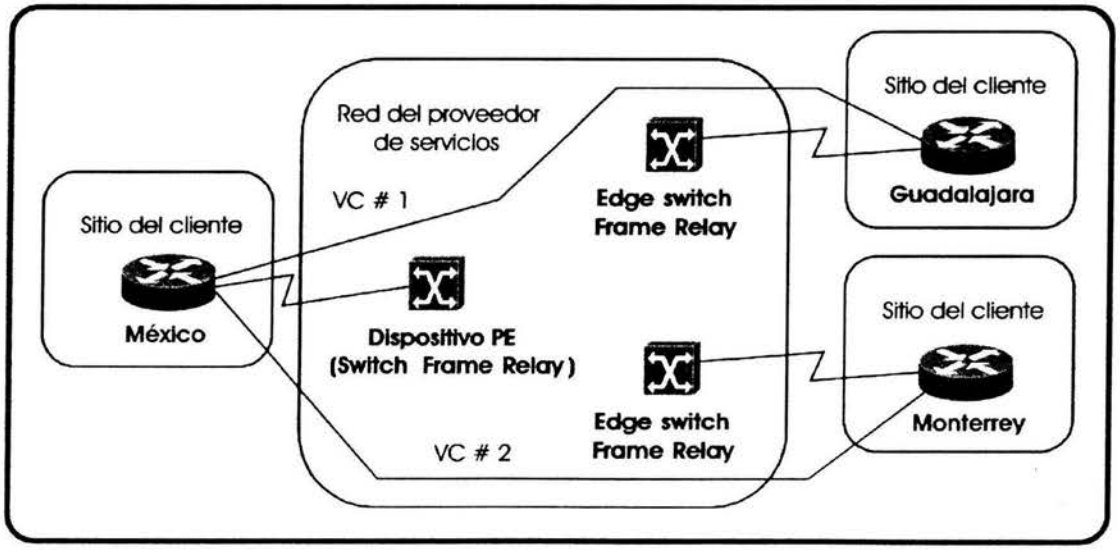


Figura 3.11 Ejemplo de una red VPN Overlay.

2. El cliente puede establecer comunicación entre sus equipos (CPE) a través de los circuitos virtuales brindados por el Proveedor de Servicios. La información del protocolo de enrutamiento entre los equipos del cliente que viaja por la infraestructura del Proveedor de Servicios no es conocida por él. La figura 3.12 muestra la topología de enrutamiento de la red VPN de la figura 3.11.

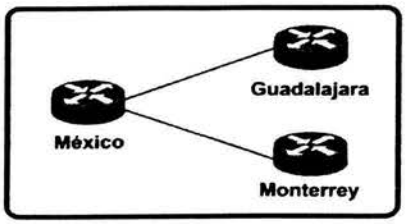


Figura 3.12 Enrutamiento en un ejemplo de una red VPN Overlay.

Las VPNs basadas en este modelo pueden ser implementadas con varias tecnologías WAN de Capa 2 tales como: Frame Relay, ATM, X.25, etc. Últimamente también han sido implementadas con IP-over-IP Tunneling en *backbones* de IP privadas y en Internet. Los dos métodos más usados para ello son el Generic Route Encapsulation (GRE) e IP Security (IPSec). Este modelo a pesar de su sencillez tiene desventajas:

- Es idóneo para configuraciones con enlaces no redundantes con pocas centrales y muchos sitios remotos, pero su administración se puede complicar si se trata de una configuración de malla.

Para tener un enrutamiento óptimo se requiere tener una topología *full mesh* en el *backbone*.

3.2.2.2 Modelo Peer-to-Peer de VPNs.

Este modelo es más reciente que el *Overlay*. En este modelo, el dispositivo PE-router, intercambia información de enrutamiento directamente con el CPE router (ver figura 3.13).

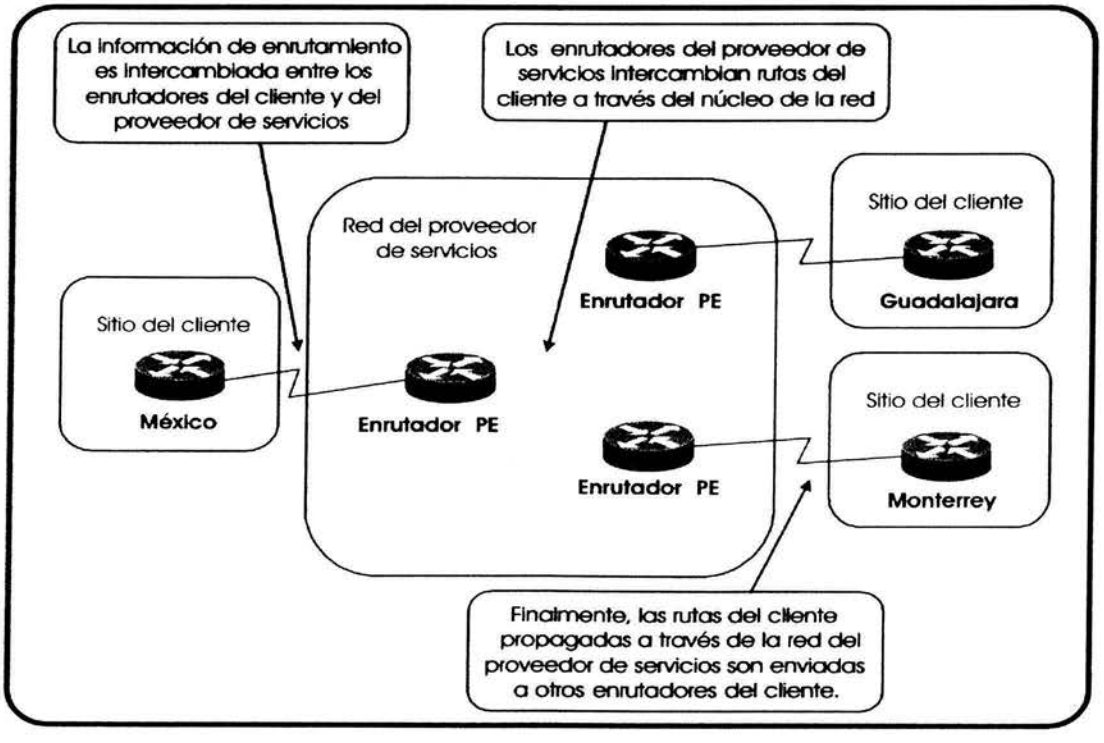


Figura 3.13 Ejemplo de una red VPN Peer-to-Peer.

El modelo además brinda ventajas sobre el modelo *Overlay*:

- El enrutamiento se vuelve sencillo para el cliente, pues sólo tiene que intercambiar la información de enrutamiento con sólo un (o unos) PE-router.
- El enrutamiento entre los clientes siempre es óptimo, debido a que los P-routers conocen la topología de los clientes y establecen el enrutamiento óptimo entre sitios.
- Agregar un nuevo sitio es más sencillo porque el proveedor de servicio sólo tiene que hacer los cambios y configuraciones para el PE-router en donde se agregará dicho nuevo sitio.

Existen dos opciones de implementación para el modelo de VPN Peer-to-peer.

- Shared-router, donde varios clientes de una VPN comparte un mismo PE-router.
- Dedicated-router, donde cada cliente de una VPN tiene un PE-router dedicado.

3.3 MPLS VPNs.

3.3.1 Uso de CEF.

En implementaciones en donde se usará exclusivamente equipo Cisco, la información necesaria para la creación de la LIB de MPLS se basa en la información que proporciona Cisco Express Forwarding (CEF); por ello es fundamental su habilitación. CEF es una tecnología de Capa 3, propietaria de Cisco Systems, para el envío de paquetes; optimiza el rendimiento y escalabilidad de una red con grandes y dinámicos patrones de tráfico, tales como aplicaciones basadas en Web o sesiones interactivas.

Ofrece beneficios tales como:

- Rendimiento mejorado, usa menos el CPU del enrutador, que puede ser empleado para servicios dedicados de Capa 3 como QoS y encriptación.
- Escalabilidad, ofrece capacidad completa para el envío de paquetes para cada tarjeta del enrutador.
- Capacidad, provee un nivel inmejorable de consistencia para el envío y estabilidad en redes dinámicas de gran tamaño.

CEF se puede usar en cualquier parte de la red pues brinda el rendimiento necesario para el crecimiento y escalabilidad del tráfico de la red.

3.3.2 Habilitar MPLS.

El tamaño de la implementación de MPLS puede ser desde un sólo enlace hasta toda la red, y desde un número pequeño hasta todas las subredes (destinos) posibles en la red.

En nuestro caso debido a que se usará exclusivamente equipo Cisco, se habilitará la funcionalidad de Tag-Switching y no MPLS como tal (LDP); Tag-Switching es una tecnología para el envío de paquetes de alto desempeño, propietaria de Cisco Systems que permite la asignación de etiquetas a las tramas para que sean transportadas en redes basadas en paquetes o en celdas. Esto es que los LSR puedan crear una relación basada en TDP/LDP (según sea el caso) con cualquier otro LSR adyacente y para distribuir las asociaciones de etiquetas a través de las sesiones de TCP.

Si no se desea etiquetar una FEC en particular existe un mecanismo para filtrar un anuncio de los mapas de etiquetas para que un LSR vecino no reciba dicho mapa. Sin el mapa, este LSR no puede hacer el envío basado en etiquetas hacia la FEC y por lo tanto debe enrutar los paquetes mediante la Tabla de Enrutamiento convencional. Esto se lleva a

cabo mediante una lista de acceso que permitirá comparar el identificador de TDP/LDP de un nodo vecino.

Es importante asegurar que para el identificador se empleen direcciones estables, por lo que se recomienda el uso de direcciones *loopback*. En el caso de que se usen varias *loopbacks*, se deberá especificar cuál se usará como identificador.

Un punto que debe considerarse en este momento, es mencionado previamente en la sección 3.1.10, y es el posible problema ocasionado por interfaces cuyo MTU es igual a 1518 que corresponde al MTU de una interfase Ethernet, al agregar el encabezado de MPLS se excede este valor y por lo tanto estos paquetes se descartarán. Para evitar este problema se ha previsto incrementar el valor de MTU para esas interfaces dentro de la configuración de Tag Switching en particular a 1524 bytes.

3.3.3 Creación de la VPN.

Una Red Privada Virtual – Virtual Private Network (VPN) es en esencia, una colección de sitios compartiendo información de enrutamiento, así un sitio puede pertenecer a más de una VPN si puede mantener las rutas de cada una de ellas separadas.

Con la introducción de MPLS, se dispone ahora de la capacidad para construir un escenario que combine una VPN basada en el modelo *Overlay*, con beneficios tales como seguridad y aislamiento, con los del enrutamiento simplificado que se obtiene con la implementación del modelo Peer-to-Peer. Este nuevo escenario es conocido como Red Privada Virtual basada en MPLS (MPLS/VPN por sus siglas en inglés). Con esta nueva arquitectura, es posible la creación una red privada sobre una infraestructura pública.

El *backbone* MPLS (administrado por el Proveedor de Servicios) está compuesto de PE-routers (Edge LSRs) y P-routers (Core-LSRs). Los PE-routers se conectarán a uno o más CE-routers (ver figura 3.14). Los PE-routers usan MPLS en sus enlaces con los P-routers, e IP puro en los enlaces con los CE-routers.

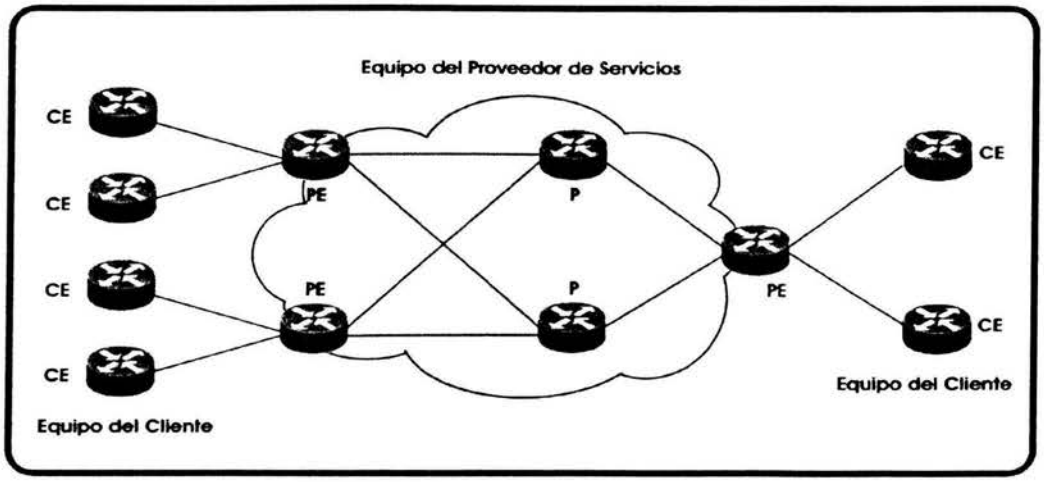


Figura 3.14 Estructura típica de una VPN basada en MPLS.

Cada PE-router usa como único identificador una dirección *loopback*, que debe ser propagada a través del *backbone* de MPLS usando un IGP, común entre ellos, que puede ser EIGRP, OSPF o IS-IS.

Todos los PE-routers, establecen sesiones de MultiProtocol Internal-BGP (MP-iBGP)[32] para poder intercambiar la información de enrutamiento relacionada con los sitios conectados así como de las VPNs. Son sesiones de iBGP, pues pertenecen al mismo AS y deben de existir entre todos y cada uno de los PE-routers, formando una topología de malla completa *(full mesh)*. Los P-routers, no utilizan BGP y no tienen conocimiento alguno de las VPNs (ver figura 3.15).

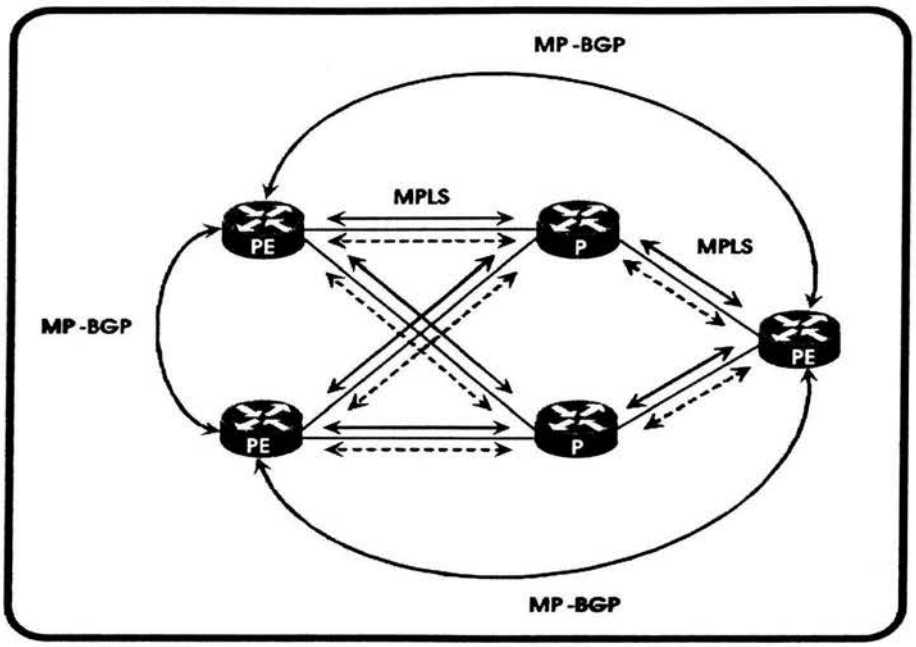


Figura 3.15 Tipos de enrutamiento empleados en la VPN basada en MPLS.

Por cuestiones de escalabilidad de la red, debido al número de sesiones que se pueden establecer entre PE-routers, se introducirán Route Reflectors (RRs), que reflejarán las rutas internas de BGP (iBGP).

Algunas razones para utilizar BGP como el protocolo que ha de transportar las rutas de la VPN son:

- El número de rutas puede ser grande.
- Es multiprotocolo y puede intercambiar información entre enrutadores que no estén directamente conectados.
- Puede transportar información adicional a una ruta, como si fuera un atributo.

[32] Descrito por el RFC-2283.

Las extensiones MP-BGP permiten transportar rutas de varias address-families, mediante el Route Target y Route Distinguisher.

Cuando un PE-router recibe una dirección destino es asociada con uno o más Target VPN, que en BGP son transportados como atributos de rutas, conocidos como Route Targets.

Cualquier ruta asociada con un Route Target, debe de ser distribuida a cada PE-router que tenga una tabla de envío asociada con este atributo. Cuando la ruta es recibida por un PE-router, es elegible para ser utilizada por cada PE-router en cada uno de los sitios que estén asociados con el Target VPN.

El PE-router descartará cualquier ruta VPN-IPv4 que no tenga un Route Target configurado para ser importado en cualquiera de sus VRFs conectadas. Cada VRF tiene políticas para importar o exportar anuncios, basados en este atributo.

El Route Target es lo más cercano a un identificador de VPN en la arquitectura MPLS/VPN, es una entidad de 64 bits, será el factor que decida que enrutadores deben recibir la ruta en cuestión.

Para crear VPNs basadas en IP con una implementación Peer-to-Peer, se requiere un espacio de direccionamiento estrictamente único. Cuando dos clientes quieren crear una VPN en un mismo *backbone* de MPLS, y tienen el mismo espacio de direccionamiento, será necesario poder identificar las rutas que le pertenecen a cada uno, ello requerirá que se usen direcciones VPN-IPv4.

Una dirección VPN-IPv4 comprende 12 bytes, comenzando por el Route Distinguisher (RD) de 8 bytes y una dirección IP de 4 bytes (ver figura 3.16). El PE-router se encargará de crear una dirección VPN-IPv4 única, a partir de los datos necesarios.

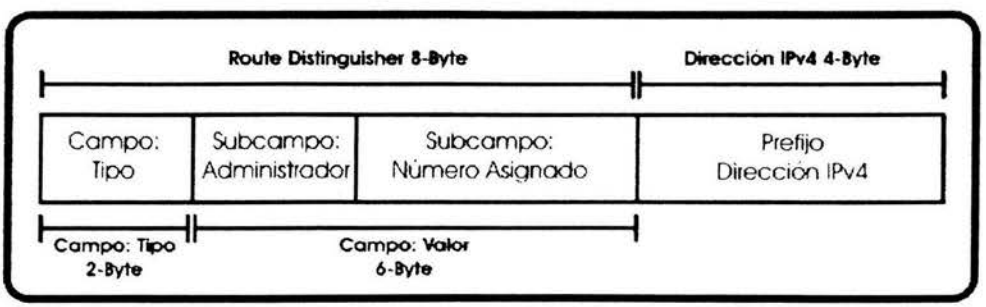


Figura 3.16 Dirección VPN-IPv4.

Esto asegura que el mismo espacio de direccionamiento pueda ser usado por dos VPNs diferentes, además de poder utilizar dos rutas completamente diferentes a destinos particulares de cada VPN. Que los espacios de direccionamiento se encimen, resulta de emplear direcciones IP privadas[4] en las redes de los clientes.

[4] Para más información consultar el RFC-1918.

El RD no contiene información acerca del origen de la ruta o acerca del conjunto de VPNs en las cuales se distribuirá la ruta. Su propósito es crear rutas distintas hacia un mismo prefijo de IPv4. Un RD consiste de:

- El campo de Tipo determina la longitud de los otros dos campos.
- El campo de Administrador identifica a una autoridad del número asignado, que puede ser una dirección IPv4 (4 bytes) o un número de AS (2 bytes).
- El campo de Assigned Number contiene un número asignado por el Proveedor de Servicios.

El PE-router tiene que ser configurado para asociar las rutas del CE-router con un RD en particular.

Los CE-routers y PE-routers intercambiarán información de enrutamiento a través de eBGP, OSPF, RIPv2 o enrutamiento estático. El CE-router, a su vez, puede tener configurado cualquier protocolo de enrutamiento. Los PE-routers deben mantener tablas de rutas separadas, una global con todas las rutas de los PE-routers y P-routers; otra que es la combinación entre la Tabla de Enrutamiento de la VPN y la Tabla de Enrutamiento asociada también llamada Instancia de Envío y Enrutamiento de la VPN – VPN Routing and Forwarding Instance conocida como VRF. Ésta es una colección de rutas que deben de estar disponibles para un sitio en particular o un conjunto de ellos (CE-routers). Esas rutas pueden pertenecer a más de una VPN.

Todos los sitios que comparten la misma información de enrutamiento que pueden comunicarse directamente con otros y están conectados al mismo PE-router pueden ser puestos en una VRF común. En el caso de que un CE-router tiene como único punto de comunicación hacia el *backbone* de MPLS un PE-router, entonces por simplicidad, se empleará una ruta estática hacia éste, mismo que se encargará a redistribuirla al resto de equipos de la VPN a través de BGP, más correctamente y de acuerdo con lo explicado anteriormente a través de sesiones de iBGP.

3.3.4 VPN Packet Forwarding.

Con la introducción de MPLS el envío de paquetes se puede simplificar, cada paquete de la VPN es etiquetado en el punto de ingreso (por un PE-router de ingreso) con una etiqueta única, que identifica este punto de ingreso en particular y es enviado a través de la red. Todos los enrutadores en la red enviarán el paquete únicamente intercambiando las etiquetas sin tener conocimiento del contenido del paquete.

Cada PE-router usa como único identificador una dirección *loopback*, que debe ser propagada a través de la Red P[5] usando un IGP en común, que puede ser EIGRP, OSPF o

[5] Se refiere a la red conformada únicamente por P-routers.

IS-IS. Esa dirección es usada también como el *next-hop* de BGP para todas las rutas de VPNs que anuncie ese PE-router. Los PE-routers, establecen sesiones de MP-iBGP para poder intercambiar la información de enrutamiento relacionada con los sitios de una VPN.

Los P-routers, no utilizan BGP y no tienen conocimiento alguno de las VPNs. Una etiqueta es asignada por cada P-router para un destino y es llevada a sus demás vecinos. Todos los demás PE-routers reciben la asociación de etiquetas con el punto de egreso a través del proceso de distribución de etiquetas de MPLS. Después de que la etiqueta para el punto de egreso (PE-router de egreso) es recibida por el punto de ingreso (PE-router de ingreso), los paquetes de la VPN pueden empezar a ser enviados. La figura 3.17 nos muestra el proceso de envío de paquetes a través de la VPN en sus pasos preparatorios.

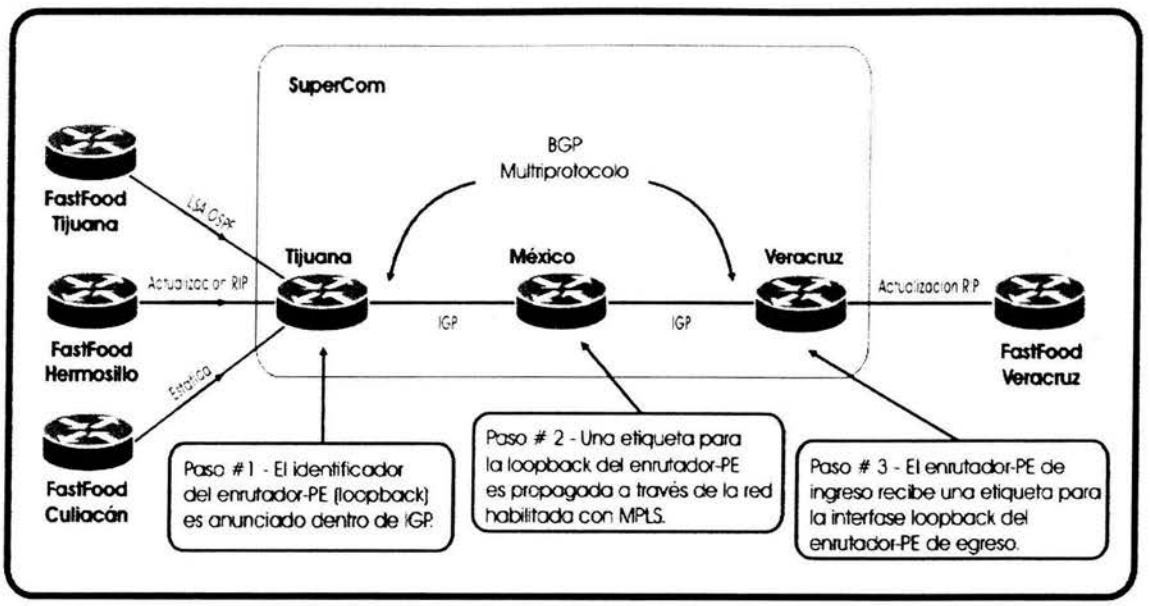


Figura 3.17 Envío de paquetes a través de la VPN (pasos preparatorios).

Cuando el PE-router de egreso recibe un paquete de una VPN, con una etiqueta no tiene información que le indique a cuál VPN va dirigido. Para poder establecer la comunicación entre sitios de la VPN, un segundo juego de etiquetas es introducido.

Cada PE-router asigna una única etiqueta para cada enrutador en cada VRF, estas etiquetas son propagadas junto con las rutas que les corresponden a través de MP-iBGP a los demás PE-routers. Estos reciben las actualizaciones y las ponen en sus VRFs respectivas, además ponen la etiqueta asignada por el PE-router de egreso también en la VRF.

Entonces, el paquete de la VPN es recibido, se compara con la VRF y el PE-router de egreso le asigna una etiqueta con la dirección destino y es enviado. Otra etiqueta, apuntando al PE-router de egreso es agregada y se obtiene de la Tabla de Envío Global. Ambas etiquetas son puestas en la pila de etiquetas del encabezado de MPLS, al frente del paquete de la VPN.

Todos los P-routers de la red envían el paquete de la VPN basados únicamente en la etiqueta más exterior, que apunta al PE-router de egreso. Debido a que el envío normal de paquetes basado en MPLS no permite a estos equipos ver más allá de la primera etiqueta, no estarán al tanto de la segunda etiqueta o del paquete que pertenece a una VPN en particular.

El PE-router de egreso recibirá el paquete etiquetado, retirará la primera etiqueta y realizará una búsqueda en la segunda etiqueta, que únicamente identificará la VRF destino y en algunas ocasiones la interfase de salida en ese enrutador. Una segunda búsqueda puede ser llevada a cabo en la VRF, para poder enviar el paquete al CE-router adecuado. Este proceso introduce un retardo significativo en el envío de paquetes, por ello es que se usa la técnica del Penultimate Hop Popping (PHP)[6].

[6] Para más detalles, referirse a la sección 3.1.9.

3.4 Calidad de Servicio – Quality of Service (QoS).

Una red de comunicaciones conforma el segmento principal de cualquier organización exitosa. Estas redes transportan una multitud de aplicaciones y datos que tienen estrictos requerimientos en términos de ancho de banda y otros recursos de la red. Entre algunas de estas aplicaciones principales tenemos: videoconferencia en tiempo real, vídeo fluido, educación a distancia, transacciones financieras seguras, aplicaciones de comercio entre otras. Estas aplicaciones tienen diferentes requerimientos en cuanto a retraso, variación del retraso *(jitter)*, ancho de banda y la pérdida de paquetes. Estos cuatro parámetros forman la base de lo que se conoce como Calidad de Servicio – Quality of Service (QoS).

Las aplicaciones que tienen un uso intensivo del ancho de banda de la red implican un aumento en el uso de los recursos de ésta misma, pero también complementan y mejoran cada proceso del negocio. Las redes deben proveer servicios seguros, predecibles, cuantificables y algunas veces garantizados. Es por eso importante, que la red IP debe ser diseñada para proveer la QoS requerida por las aplicaciones de la empresa.

Cuando se habla de Calidad de Servicio (QoS) en redes IP, se habla de una determinada inteligencia existente en los dispositivos que manejan de una forma preferente el tráfico. La Calidad de Servicio se define como esos mecanismos o técnicas que permiten al administrador de la red tener control sobre el ancho de banda, el retraso, el *jitter*, y la pérdida de paquetes en la red. Estas habilidades que posee QoS permiten a los proveedores dividir o clasificar de alguna forma el tráfico que entra a la red IP y darle prioridad a determinadas Clases de Servicio bajo condiciones de congestión en la red, asignando distintos valores de ancho de banda predefinidos.

La Internet Engineering Task Force (IETF) ha definido dos modelos para implementar QoS, estos son Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ). IntServ obedece a un modelo de QoS empleando una señalización de extremo a extremo, en el cual los hosts finales le indican a la red IP sus necesidades de QoS para la reservación de ancho de banda y de otros recursos. DiffServ trabaja en un modelo de QoS proveído, en el cual los elementos de la red son configurados para dar servicio a múltiples clases de tráfico con diversos requerimientos de QoS.

En un sentido tangible, QoS es implementado mediante varios mecanismos como son: protocolos de señalización, mecanismos de control o monitoreo de flujos de tráfico *(policing)* y de configuración o de conformado de tráfico *(shaping)*, mecanismos de control de congestión, y mecanismos de eficiencia de enlace.

3.4.1 Servicios Integrados (IntServ).

En esta sección se describirá el modelo de QoS conocido como IntServ, posteriormente en las dos secciones siguientes se detallará el protocolo empleado por IntServ (RSVP) y de su implementación en MPLS.

El modelo IntServ provee una solución de QoS mediante una señalización de extremo a extremo, logrando mantener un estado, y mediante el control de admisión a cada elemento de la red. IntServ especifica un número de Clases de Servicio designadas para cumplir con las necesidades de los diferentes tipos de aplicaciones. En este modelo también se emplean protocolos para lograr la señalización, como es el caso del Resource Reservation Protocol (RSVP) que es usado para hacer peticiones de QoS empleando las Clases de Servicio IntServ.

IntServ trabaja con dos tipos de especificaciones principalmente. La primera se llama especificación de tráfico (Tspec), en la cual se define el tipo de tráfico de una aplicación que ingresa a la red, por lo tanto se requiere que los elementos de la red (enrutadores y switches) realicen funciones de control y monitoreo *(policing),* verificando que el tráfico está de acuerdo con su Tspec. En caso de que los paquetes no concuerden con los valores del Tspec, estos serán dados de baja. También se define una especificación de reservación (Rspec), la cual solicita el nivel de QoS así como la reservación de los recursos de la red, para este caso se requiere que los elementos de la red realicen funciones tal como el control de admisión, para comprobar si existen suficientes recursos para satisfacer la petición de QoS. Si los recursos son escasos, la petición de QoS será denegada. IntServ también requiere que los elementos de la red realicen la clasificación de paquetes que requieren de un nivel específico de QoS, así como también de mecanismos de encolamiento *(queuing)* y de planificación *(scheduling).*

Existen dos Clases de Servicio en IntServ, el Servicio Garantizado y el de Carga Controlada. Estas Clases de Servicios se solicitan vía RSVP, suponiendo que todos los elementos de la red a lo largo de la ruta soportan este protocolo desde el origen hasta su destino.

En el Servicio Garantizado *(Guaranteed Service)* se proporciona un nivel de ancho de banda y un límite en el retardo, garantizando la no existencia de pérdidas en colas. Está pensado para aplicaciones con requerimientos en tiempo real, tales como ciertas aplicaciones de audio y vídeo. Cada enrutador caracteriza el servicio garantizado para un flujo específico asignando un ancho de banda y un espacio en *buffer.*

A diferencia del anterior, este Servicio de Carga Controlada *(Controlled Load Service)* no ofrece garantías en la entrega de los paquetes. Así, será adecuado para aquellas aplicaciones que toleren una cierta cantidad de pérdidas y un retardo mantenidos en un nivel razonable. Los enrutadores que implementen este servicio deben verificar que el tráfico recibido siga las especificaciones dadas por el Tspec, y cualquier tráfico que no las cumpla será reenviado por la red, como tráfico de Mejor Esfuerzo *(Best Effort).*

3.4.1.1 Resource Reservation Protocol (RSVP).

RSVP es un protocolo de señalización que emplea IntServ, intentando proveer un servicio lo más cercano posible a la emulación de circuitos en redes IP, permitiendo a las aplicaciones señalizar sus requerimientos de QoS a la red. RSVP es la tecnología más compleja para ofrecer Calidad de Servicio, representado la técnica más alejada del servicio de mejor esfuerzo, proveyendo el nivel más alto de QoS. RSVP permite a las aplicaciones reservar de manera dinámica el ancho de banda. Al trabajar de esta forma y teniendo una reservación de recursos en cada uno de los enrutadores entre el origen y el destino, cada enrutador habilitado con RSVP necesita guardar información de cada una de las sesiones de RSVP, lo cual puede afectar el desempeño del enrutador.

Su forma de trabajar es la siguiente, las aplicaciones señalizan sus requerimientos de QoS, posteriormente la red reconoce la petición de QoS con una respuesta de éxito o de falla. RSVP transporta información de clasificación, incluyendo las direcciones IP fuente y destino así como los números de los puertos UDP, de esta manera los flujos con un requerimiento particular de QoS pueden ser reconocidos dentro de la red. RSVP también transporta las especificaciones Tspec y Rspec, así como información de la Clase de Servicio deseada, y lo hace de la aplicación hacia cada elemento de la red a lo largo de toda la ruta entre el emisor y el receptor.

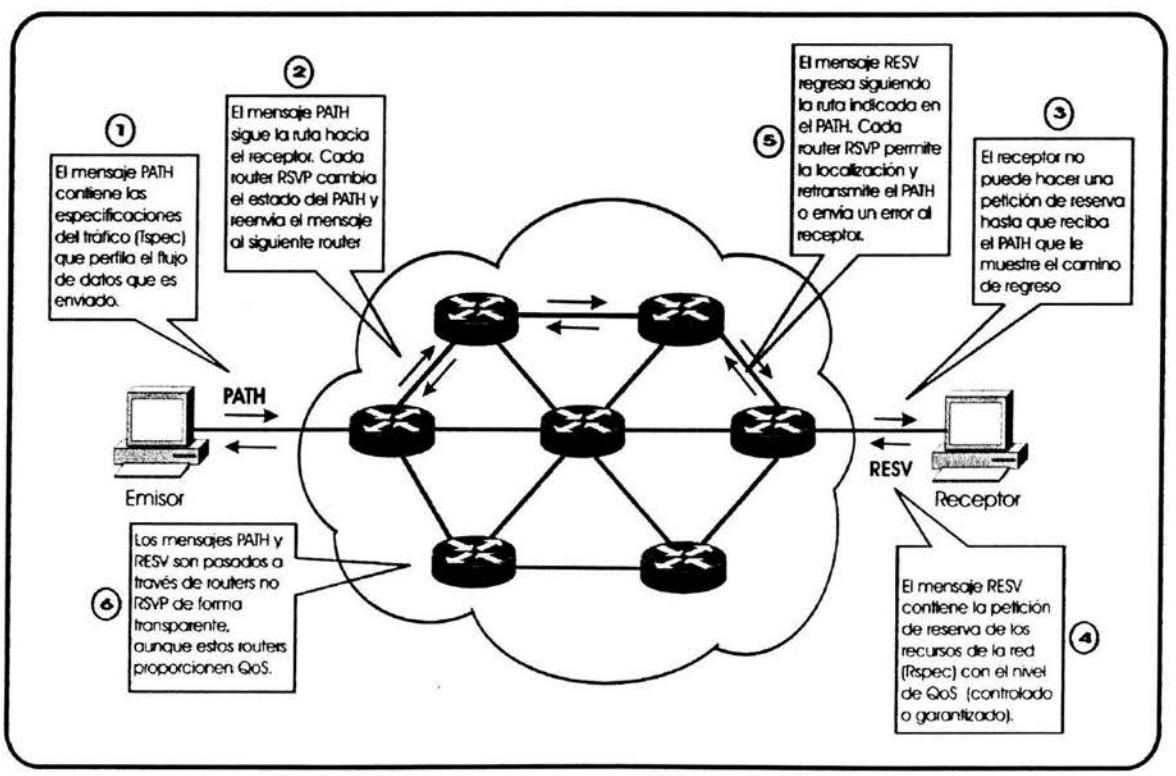


Figura 3.18 Intercambio de mensajes en RSVP.

RSVP transporta esta información usando dos tipos de mensajes: PATH y RESV (figura 3.18). El primero viaja del emisor a uno o más receptores e incluye Tspecs y la

información de clasificación proveída por el emisor. Cabe agregar que pueden existir múltiples receptores dado que RSVP fue diseñado para aplicaciones multicast. Cuando este mensaje le llega al receptor, éste envía el mensaje RESV de regreso al emisor, identificando la sesión para la cual está hecha la reservación. Este mensaje incluye un Rspec indicando el nivel de QoS requerida por el receptor. También incluye información respecto a cuales emisores están autorizados para utilizar los recursos asignados para el flujo. RSVP realiza sus reservaciones de una forma unidireccional.

Al establecer la ruta, los enrutadores pueden identificar los paquetes pertenecientes a la reservación inspeccionando cinco campos de los encabezados IP y del protocolo de transporte. Estos son las direcciones IP y puertos tanto del destino como de la fuente, así como el número de protocolo; al conjunto de estos paquetes identificados de esta forma son llamados Flujos Reservados. Los paquetes de este flujo son monitoreados para asegurarse de no generar más tráfico que el especificado. Estos paquetes también reciben un encolamiento y planificación *(scheduling)* adecuados para alcanzar la QoS deseada.

RSVP fue diseñado para soportar reservación de recursos para microflujos de aplicaciones individuales. A condición de que sea señalizado usando RSVP y que los recursos estén disponibles. Cada elemento en la red a lo largo de la ruta, incluyendo a los Sistemas Finales (end systems), necesitan conocer muy bien el protocolo RSVP y ser capaces de señalizar la QoS requerida. La información del estado para cada reservación necesita ser mantenida por cada elemento de la red. La reservación en cada dispositivo es suave (soft), lo cual significa que necesita ser renovada periódicamente.

RSVP puede hacer reservaciones para tráfico agregado. Esto forma la base de la implementación de RSVP en MPLS, en donde los paquetes pertenecientes a un Flujo Reservado pueden ser definidos como pertenecientes a una Forwarding Equivalence Class (FEC) particular. Las ligaduras de etiqueta pueden ser creadas para asociar etiquetas con instancias FEC. Estas etiquetas pueden ser distribuidas usando el protocolo *Label Distribution Protocol* (LDP).

3.4.2 Implementación de IntServ en MPLS.

MPLS puede ser habilitado en los Label Switching Routers (LSRs) mediante la asociación de etiquetas con flujos que tengan reservaciones RSVP. Los paquetes a los cuales se le hizo una reservación RSVP pueden ser considerados como Forwarding Equivalence Classes (FECs), como se había mencionado anteriormente. Una etiqueta puede identificar cada FEC. Las ligaduras creadas entre las etiquetas y los flujos RSVP deben ser distribuidas entre los LSRs.

Así, después de que el emisor envía su mensaje RSVP PATH a través de la red, el host responde con un mensaje RSVP RESV estándar. El primer LSR visto desde el receptor recibe el mensaje RESV y le asigna una etiqueta tanto en la entrada como en la salida del enrutador, y posteriormente envía el mensaje RESV con su correspondiente etiqueta hacia el enrutador siguiente en dirección hacia el emisor, hasta llegar a éste. De esta forma se

establece un Label Switched Path (LSP), a través de la ruta RSVP, y cada LSR puede asociar los recursos QoS con el LSP. Por lo tanto cuando un LSR recibe un paquete de otro enrutador, puede buscar el valor de su etiqueta en su LFIB y reconocer los mecanismos relacionados con la QoS asociados a este paquete, como su monitoreo y encolamiento.

3.4.3 Precedencia IP – IP Precedence.

El tratamiento de QoS que hace RSVP a los flujos de datos descrito en el apartado anterior no es escalable y por lo tanto resulta compleja su implementación, es por eso que surge Precedencia IP – IP Precedence.

La Precedencia IP fue definida por la IETF como una forma simplificada de brindar QoS en IP mediante la adopción de un modelo agregado para flujos, clasificando varios flujos en clases agregadas y proveyendo la apropiada QoS a los flujos clasificados.

Los paquetes son clasificados en el límite de la red en una de las ocho diferentes clases existentes. Esto logrado mediante el empleo de tres bits de precedencia en el campo Type of Service (ToS) del encabezado IP. Así, de esta forma los paquetes entran en alguna de las ocho clases (ver tabla 3.2), y en caso de congestión, los paquetes de menor precedencia serán tirados a favor de los de mayor precedencia. Además, cada paquete es marcado para recibir uno de los dos niveles de retraso[7], de rendimiento y de confiabilidad antes de su envío (ver figura 3.19).

Figura 3.19 Contenido del campo Type of Service del encabezado IPv4.

Tan pronto los paquetes son marcados con la apropiada Precedencia IP, cualquier nodo de la red a lo largo de la ruta conoce el nivel relativo de prioridad que le corresponde y así podrá aplicar preferencia en el envío a paquetes con alta prioridad. El esquema de Precedencia IP, sólo permite la especificación de una prioridad relativa, y no tiene estipulado ningún tipo de precedencia a la hora de tirar paquetes con un nivel de prioridad similar.

[7]Para poder consultar detalladamente esta información se puede referir al RFC-791.

Número	Valor	Tipo de Precedencia
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash Override
5	101	Critical
6	110	Internet Control
7	111	Network Control

Tabla 3.2 Valores de Precedencia IP

3.4.4 Servicios Diferenciados (DiffServ).

En este modelo, DiffServ también describe un conjunto de funciones para ofrecer QoS a aplicaciones críticas de extremo a extremo en una red IP. DiffServ es un modelo de servicio múltiple que puede satisfacer una gran variedad de requerimientos de QoS. Con DiffServ, la red trata de entregar un tipo de servicio particular basado en la QoS especificada por cada paquete. La forma de hacer esto es dividiendo el tráfico en un determinado número de clases y asignando recursos por clase. La red emplea las especificaciones de QoS para clasificar, marcar, configurar y monitorear tráfico, así como para realizar funciones de encolamiento. Los Servicios Diferenciados son apropiados para Flujos Agregados dado que realiza una clasificación del tráfico de niveles severos.

Para poder clasificar el tráfico en clases, se pone en uso el campo ToS del encabezado IP, marcando los distintos paquetes con seis bits, que en conjunto reciben el nombre de Differentiated Services Code Point (DSCP). Este modelo es similar al de Precedencia IP e inclusive se pueden mapear los distintos niveles de éste a las clases DSCP (ver tabla 3.3).

Precedencia IP	DSCP
IP Precedence 0	DSCP 0
IP Precedence 1	DSCP 8
IP Precedence 2	DSCP 16
IP Precedence 3	DSCP 24
IP Precedence 4	DSCP 32
IP Precedence 5	DSCP 40
IP Precedence 6	DSCP 48
IP Precedence 7	DSCP 56

Tabla 3.3 Mapeo de niveles de Precedencia IP a clases DSCP.

Así, de esta forma los elementos de la red a lo largo de la ruta examinan el valor del campo DSCP y determinan la QoS requerida por el paquete. Esto es conocido como Per-Hop Behavior (PHB). Cada elemento de la red tiene una tabla que mapea el DSCP encontrado en un paquete hacia el PHB para determinar como debe de ser tratado el paquete. El DSCP es un número o valor llevado en el paquete, y los PHBs son acciones específicas que se aplican a los paquetes. Una colección de paquetes que tienen el mismo

valor DSCP en su encabezado, y cruzan por un mismo elemento de la red en una dirección particular, es llamado un Behavior Agregate (BA). PHB se refiere al comportamiento o a la forma en como un nodo tratará a un paquete perteneciente a un BA en cuanto a su planificación *(scheduling)*, encolamiento *(queuing)*, monitoreo *(policing)*, o configuración *(shaping)*.

En la actualidad se disponen de cuatro estándares de implementación PHB.

a. Default PHB.
b. Class Selector PHB.
c. Expedited Forwarding (EF) PHB.
d. Assured Forwarding (AF) PHB.

a. Default PHB.

El Default PHB resulta ser el estándar de envío de paquetes de IP conocido como Mejor Esfuerzo *(Best Effort)*. Los paquetes que tienen este tipo de trato, así como cualquier otro paquete que no sea mapeado a uno de los cuatro tipos de tratamiento, poseen un valor DSCP en sus encabezados de 000000.

b. Class-Selector PHB.

Con el fin de conservar una compatibilidad con el esquema de Precedencia IP, se definen los valores DSCP de la forma xxx000. Tales valores DSCP son llamados Class-Selector Codepoints. El PHB asociado con un Class-Selector Codepoint es conocido como Class-Selector PHB. Estos PHBs, conservan casi el mismo comportamiento de envío que el que implementan los nodos en la clasificación y en el envío basada en Precedencia IP. Estos PHBs aseguran que los nodos adaptados a DiffServ puedan coexistir con los nodos que conocen IP Precedence.

c. Expedited Forwarding (EF) PHB.

El marcado DSCP de una clase como EF resulta en el envío agilizado con retardo mínimo y con pocas pérdidas. Estos paquetes tienen una prioridad mayor en el envío sobre otros. El PHB EF en el modelo DiffServ satisface las necesidades de pocas pérdidas de paquetes, poca latencia, bajo *jitter*, y de ancho de banda garantizado. EF puede ser implementado usando encolamiento prioritario, junto con un limitador de la tasa de envío. A pesar de que el implementar PHB EF en una red DiffServ provee un Servicio Premium, éste debe de estar dirigido hacia las aplicaciones más críticas, porque si existe congestión, no es posible dar el mismo trato a todo el tráfico con una alta prioridad. El valor DSCP recomendado para EF es 101110.

d. Assured Forwarding (AF) PHB.

El envío asegurado o Assured Forwarding (AF) es casi equivalente al Servicio de Carga Controlada disponible en el modelo de Servicios Integrados. AF PHB define un método con el cual se puede ofrecer un envío garantizado a los BAs. Este método consiste

en clasificar los paquetes en cuatro clases AF y a cada clase asignarle tres niveles o preferencias de desecho en caso de que se requiera tirar paquetes debido a la existencia de congestión o se exceda el ancho de banda asignado. Lo cual se logrará marcado paquetes con su respectivo valor DSCP según sea el caso (ver tabla 3.4).

Precedencia de desecho de paquetes	Clase 1	Clase 2	Clase 3	Clase 4
Baja	(AF11) 001010	(AF21) 010010	(AF31) 011010	(AF41) 100010
Mediana	(AF12) 001100	(AF22) 010100	(AF32) 011100	(AF42) 100100
Alta	(AF13) 001110	(AF23) 010110	(AF33) 011110	(AF43) 100110

Tabla 3.4 Diferentes valores de DSCP para un AF PHB.

3.4.4.1 Arquitectura de los Servicios Diferenciados.

Una región DiffServ (DS) está compuesta de uno o más dominios DS. Cada dominio a su vez es configurado usando el DSCP y los diferentes PHBs, además este dominio está conformado de nodos de ingreso DS, nodos internos DS ubicados en el centro (core), y nodos de egreso DS. Toda la ruta que un paquete viaja debe de estar habilitada con DiffServ.

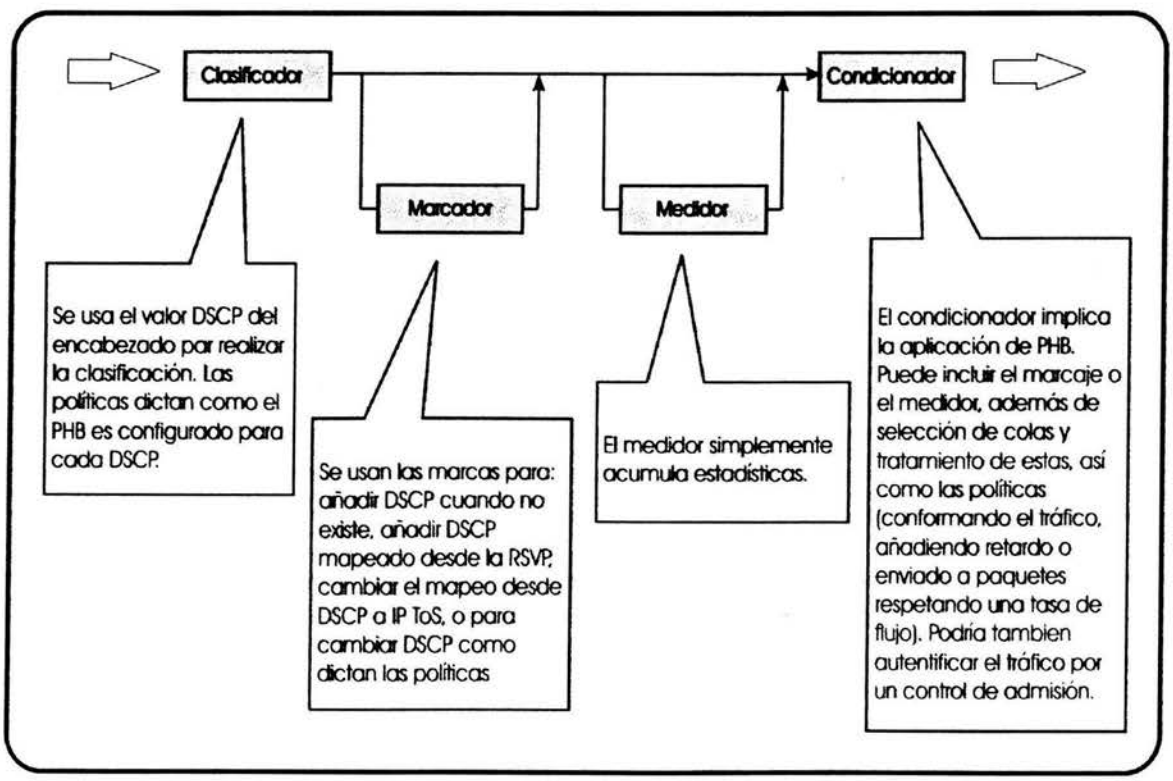


Figura 3.20 Arquitectura de DiffServ. Esta funcionalidad está activada en cada enrutador habilitado para ofrecer DiffServ, aunque no todas las funciones se utilizan al mismo tiempo. Casi todos los enrutadores de los extremos la utilizan, no tanto los enrutadores internos.

Los nodos de ingreso DS o de egreso también se conocen como nodos fronterizos DS, este tipo de nodos conectan los dominios DS entre si. Típicamente, el nodo fronterizo DS realiza el acondicionamiento del tráfico antes de que entre en un dominio, este acondicionador de tráfico clasifica los paquetes entrantes en agregados predefinidos basados en el contenido de alguna porción del encabezado, los mide revisando que se cumplan los parámetros de tráfico o los marca apropiadamente escribiendo o rescribiendo el DSCP, para que finalmente los configure (emplear el *buffer* para lograr una tasa de flujo determinada) o en caso de congestión tire los paquetes (ver figura 3.20). En el caso de los nodos internos DiffServ, implementan el apropiado PHB empleando técnicas de monitoreo o control *(policing)*, de configuración *(shaping)* y algunas veces remarcando los paquetes dependiendo de sus políticas.

3.4.4.2 Mecanismos DiffServ.

El modelo DiffServ solamente define el uso del DSCP y los PHBs, estos últimos simplemente describen el trato que un nodo le dará a un paquete en el envío; pero el modelo no especifica como esos PHBs son implementados. Una variedad de técnicas de encolamiento, *policing* o monitoreo, medición, y *shaping* o conformado deben ser usadas para acondicionar el tráfico, y de esta forma cumplir con la Calidad de Servicio solicitada.

3.4.4.2.1 Control de Tráfico (Traffic Policing).

Se utiliza la Tasa de Acceso Comprometida – Committed Access Rate (CAR) en el acondicionamiento del tráfico y en la provisión de PHB para clases AF en los bordes y en el centro (core) de un dominio DS.

El CAR realiza funciones tal como la de limitar la tasa de transmisión tanto en la entrada como en la salida de una interfase o subinterfase basándose en un conjunto de criterios flexibles. CAR también emplea acciones configurables, como son la transmisión y el desecho de paquetes, la configuración de la precedencia o la configuración del grupo de QoS, basándose en si el tráfico conforma o excede la tasa límite.

Principalmente CAR nos ofrece dos ventajas, la primera es que se puede administrar el ancho de banda a través del límite de la tasa. Esta función nos permite controlar la tasa máxima para transmitir tráfico o recibirlo en una interfase. Por lo regular CAR es configurado en las interfases de los bordes de una red para limitar el tráfico entrante o saliente. Los paquetes son medidos, y diferentes acciones son tomadas, dependiendo si el paquete en cuestión conforma, viola o excede la tasa promedio configurada. Un paquete puede ser transmitido, tirado, o remarcado con diferente valor de prioridad.

La otra ventaja radica en que nos ayuda a realizar una clasificación de los paquetes. Esta función nos permite particionar la red en múltiples niveles de prioridad o de clases de

servicio. Los dispositivos de la red usan estas clasificaciones para determinar como debe de ser tratado el tráfico.

3.4.4.2.2 Conformado de Tráfico (Traffic Shaping).

La razones principales por la que se debe de usar el conformado o configuración de tráfico es para tener un control de acceso al ancho de banda disponible, para asegurar que el tráfico conforma o cumple con las políticas establecidas y para regular el flujo de tráfico de manera que se pueda evitar la congestión que ocurre cuando el tráfico enviado excede sus límites. El conformado de tráfico suaviza el tráfico mediante el almacenamiento de éste, cuando está por encima de su tasa configurada, en una cola.

Existen varios mecanismos de conformado pero en este momento sólo nos interesa mencionar el Generic Traffic Shaping (GTS) que proporciona un servicio de *buffer* a los paquetes, en vez de simplemente tirarlos en caso de congestión. GTS es un mecanismo de control del flujo del tráfico en una interfase determinada. Reduce la circulación de salida para evitar la congestión obligando a determinado tráfico a una tasa de bits particular mientras se encolan las ráfagas del citado tráfico. Para forzar el tráfico a una tasa de bits particular se emplea el mecanismo *token bucket* (ver figura 3.21).

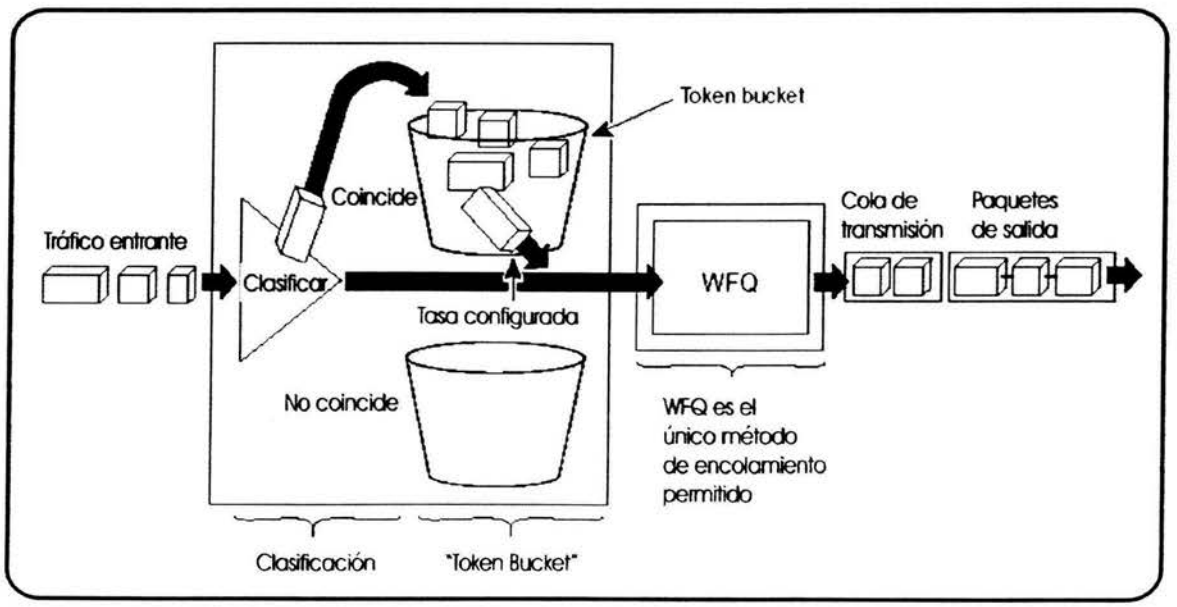


Figura 3.21 Generic Traffic Shaping.

Así de esta manera el conformado o configurado de tráfico permite su control a la salida de una interfase a manera de corresponder su transmisión con la velocidad de la interfase destino y asegurar que el tráfico conforma las políticas establecidas. Este mecanismo conocido como Traffic Shaping ayuda a eliminar los cuellos de botella en topologías con tasa de datos desiguales.

3.4.4.2.3 Ejecución de PHB.

PHB es puesta en ejecución en los enrutadores del núcleo dependiendo del valor DSCP marcado en el encabezado del paquete. Expedited Forwarding (EF) PHB es implementado usando un mecanismo de encolamiento conocido como Low Latency Queuing (LLQ), y Assured Forwarding (AF) PHB puede ser implementado mediante una combinación de Class-Based Weighted Fair Queuing (CBWFQ) y Weighted Random Early Detection (WRED) o CAR.

LLQ ofrece un encolamiento prioritario estricto para tráfico sensible al retardo como VoIP a lo largo de la ruta de datos. LLQ debe ser implementado en cada salto. Este encolamiento prioritario es controlado con el fin de asegurar que el exceso de tráfico sensible al retardo no interfiera con tráfico de otras clases.

Para situaciones en las que es deseable proporcionar un tiempo de respuesta consistente a cualquier tipo de usuarios sin necesidad de aumentar el ancho de banda de forma excesiva, la solución es Weighted Fair Queuing (WFQ). Es un algoritmo de encolamiento basado en el flujo que realiza dos tareas simultáneamente: sitúa el tráfico interactivo a principio de la cola para reducir el tiempo de respuesta y permite así compartir el resto del ancho de banda entre flujos que requieren gran ancho de banda. WFQ asegura que las colas no se quedarán sin ancho de banda, proporcionando a ese tráfico un servicio predecible. Así mismo, las ráfagas de tráfico de bajo volumen (la mayoría del tráfico) reciben servicio preferencial, transmitiéndolas rápidamente. Las ráfagas de tráfico de gran volumen compartirán la capacidad restante de forma proporcional entre ellos.

WFQ ha sido diseñado para minimizar en esfuerzos al configurar, adaptándose automáticamente a las condiciones cambiantes del tráfico de la red. WFQ es eficaz pues permite que se pueda asignar cualquier cantidad de ancho de banda para flujos de tráfico de baja prioridad si no está presente ningún flujo de alta prioridad. WFQ, además, trabaja con las técnicas IP Precedence y DSCP para proporcionar QoS diferenciada así como servicios garantizados.

CBWFQ extiende la funcionalidad de WFQ de proveer soporte a clases de tráfico definidas por el usuario. CBWFQ permite distribuir el ancho de banda entre varias clases definidas. El ancho de banda debe ser asignado a cada clase en una base absoluta o como un porcentaje del ancho de banda de la interfase o subinterfase a las cuales se les aplicaría esta política. Dentro de una clase AF, los paquetes pueden ser tirados en base a un esquema de precedencia de desecho usando WRED.

Ahora nos referiremos a las técnicas de prevención de congestión, las cuales supervisan las cargas de tráfico de la red en un esfuerzo por anticiparse y evitar la congestión de los comunes cuellos de botella de la red, como opuesto a técnicas que operan para controlar la congestión de la red después de que ésta ocurre.

Los algoritmos de detección temprana al azar son diseñados para evitar la congestión entre redes antes de que ésta se vuelva un problema. Random Early Detection (RED) supervisa la carga de tráfico en diferentes puntos de la red y descarta paquetes de forma estocástica si

aumenta el nivel de congestión. El resultado es que la fuente detecta esta situación, retardando su transmisión.

WRED (Weighted Random Early Detection) combina las capacidades de RED con IP Precedence. Esta combinación mantiene tráfico preferencial que maneja como paquetes de prioridad más altos. Puede desechar selectivamente el tráfico de menor prioridad cuando el interfaz empieza a congestionarse y proporciona características de gestión distintas para las diferentes clases de servicio. Pero WRED también permite RSVP, ofreciendo Servicios Integrados de QoS de carga controlada.

3.4.5 Modular QoS CLI.

El Modular QoS Command Line Interface (MQC) es un mecanismo de aprovisionamiento del software IOS (Internetworking Operating System). El Modular QoS CLI consiste en los siguientes tres elementos:

- Mapas de Clases.
- Mapas de Políticas.
- Políticas de Servicio.

Un Mapa de Clase clasifica el tráfico en una interfase ya sea de salida o de entrada. El Mapa de Clase define los criterios a usar para diferenciar el tráfico. Por ejemplo, se puede usar el Mapa de Clase para diferenciar tráfico de voz del tráfico de datos.

Un Mapa de Políticas define acciones QoS, las controla y las asocia a Mapas de Clase. En un Mapa de Políticas se pueden definir acciones QoS como el Traffic Policing y el CBWFQ.

Por ultimo tenemos las Políticas de Servicio, las cuales adjuntan Mapas de Políticas a una interfase y especifican la dirección (ya sea a la entrada o a la salida) en que la política debe ser aplicada. Una interfase puede tener diferentes Mapas de Políticas para paquetes que llegan a ésta o para paquetes que salen.

Para configurar QoS en una interfase usando MQC, se realiza mediante los siguientes pasos (ver figura 3.22).Cabe señalar que los dos primeros pasos se configuran a nivel global mientras que el tercer paso se configura a nivel de interfase.

1. Se define la clase de tráfico usando el comando class-map.

2. Se crea la política de tráfico usando el comando policy-map y se asocia la clase de tráfico con la política.

3. Por último se adjunta la política de tráfico y se asocia la clase de tráfico a la interfase usando el comando service-policy.

MQC forma la base para proveer DiffServ, y todos los mecanismos QoS son parte de los Mapas de Clases (clasificación) o Mapas de Políticas (control, conformado, encolamiento, evasión de congestión, marcado de paquetes, o marcado de CoS Capa 2).

Los paquetes que entran a un dominio DS pueden ser medidos, marcados, conformados, o controlados para implementar las políticas de tráfico. En el software IOS, la clasificación y marcado son hechos mediante el uso de Mapas de Clases MQC. La medición se hace empleando una algoritmo *token bucket*, el conformado es hecho con GTS, y el control es hecho mediante un control basado en clases o con CAR.

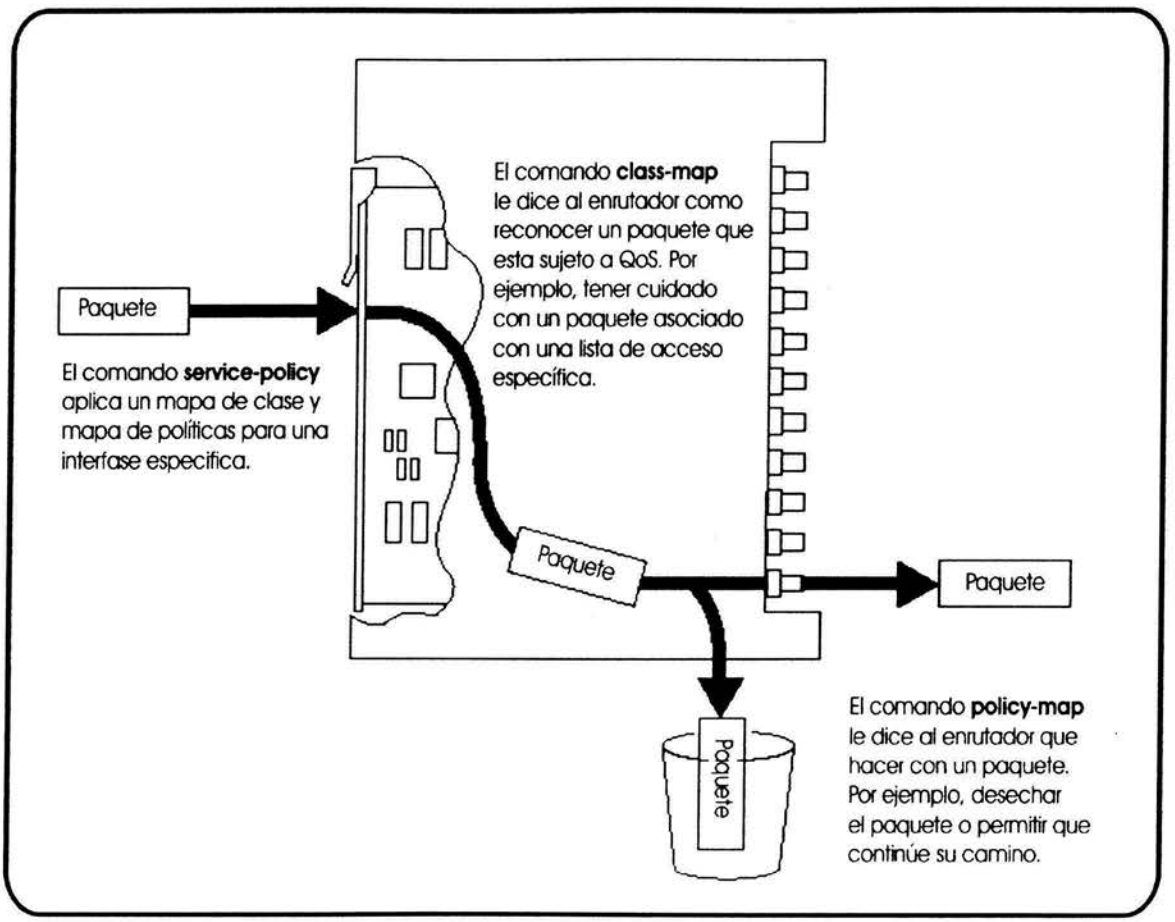


Figura 3.22 Proceso de configuración de QoS en una interfase.

3.4.6 Implementación de DiffServ en MPLS.

Los MPLS LSRs no examinan el contenido del encabezado IP ni el valor del campo DSCP como es requerido por DiffServ. Esto significa que el PHB apropiado debe ser determinado del valor de la etiqueta. El encabezado de MPLS tiene un campo de tres bits llamado Exp, que fue originalmente definido como de uso experimental. Este campo soporta ocho diferentes valores y es usado por MPLS para dar soporte a ocho clases de DiffServ.

Los bits de Precedencia IP o los tres primeros bits del campo DSCP son copiados al campo Exp de MPLS en el borde de la red. Cada LSR a lo largo del LSP mapea los bits del Exp hacia un PHB. El Proveedor de Servicio también puede configurar una CoS en el paquete dentro de MPLS. Esta característica permite al Proveedor de Servicio configurar el campo Exp de MPLS en vez de sobrescribir el valor en el campo de Precedencia IP del cliente. Esto deja el encabezado IP intacto y disponible para el uso del cliente. La CoS configurada por el cliente no cambia cuando el paquete atraviesa el *backbone* de MPLS. Los LSPs creados de esta forma son conocidos como E-LSPs o Exp-LSPs. Un E-LSPs puede soportar hasta ocho PHBs (ver figura 3.23).

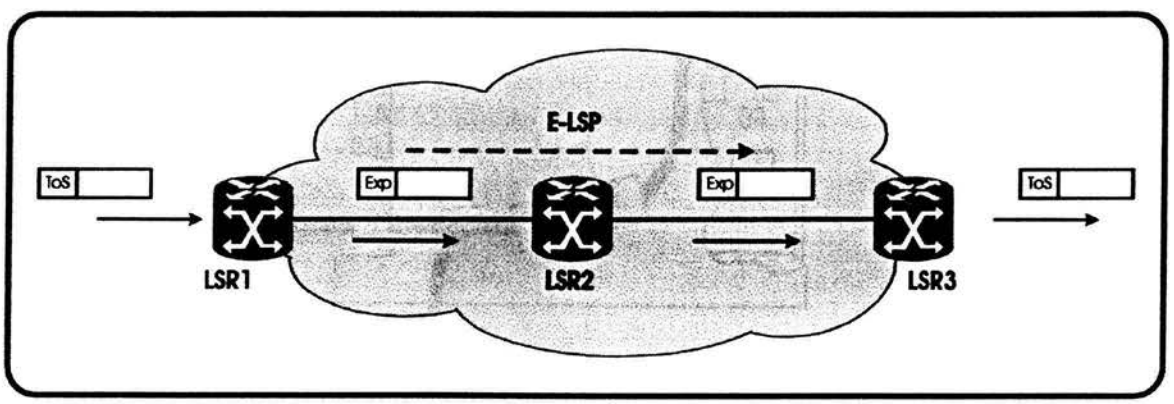


Figura 3.23 MPLS E-LSP.

Si se desean más de 8 PHBs en la red de MPLS, se usan los Label LSPs (L-LSPs), en cuyo caso el PHB del LSR es inferido de la etiqueta. Sólo un PHB puede ser posible por cada L-LSP, excepto para los Servicios Asegurados (AF DiffServ). En el caso de AF DiffServ, los paquetes comparten un PHB en común que puede ser agregado a una FEC, el cual a su vez es asignado a un LSP. Esto se conoce con el nombre de Clase de Planificación PHB (PHB Scheduling Class). La preferencia de tirado es codificada en la parte de los Exp bits del encabezado. Y ésta es la forma en como se logran implementar los Servicios Diferenciados en una red MPLS mediante el empleo de sus etiquetas (ver figura 3.24).

Para concluir esta parte del capítulo se puede decir que todos los modelos mencionados con sus respectivos mecanismos nos ayudan a satisfacer las necesidades de QoS en una red. Y estas necesidades de QoS están dictadas directamente por las aplicaciones y los usuarios a los cuales dará servicio la red cómo se comentó anteriormente.

Sin embargo las necesidades por QoS varían de cliente a cliente y de aplicación a aplicación, ya que no todas las aplicaciones requieren de los mismos recursos, por presentar diferente sensibilidad a los distintos parámetros que conforman la Calidad de Servicio. Como se ha podido deducir, el ofrecer niveles de servicio en redes basadas en IP necesariamente se basa en resolver problemas de administración de tráfico, pero sobre todo de administración del ancho de banda que resulta ser el recurso más importante y caro en la red.

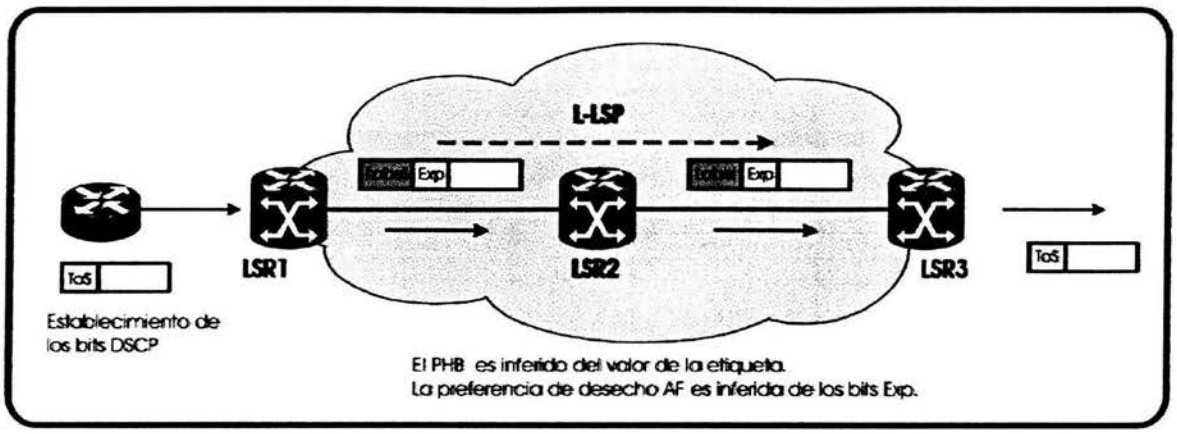


Figura 3.24 MPLS L-LSP.

En general los mecanismos empleados por el modelo DiffServ logran satisfacer todas estas necesidades a las que nos referimos, ya que el modelo IntServ está en desuso, dado que DiffServ ofrece QoS de una forma menos compleja que la de IntServ. Esta complejidad se basa en sus desventajas entre las que podemos mencionar la necesidad de actualizar mensajes para mantener un estado y que aumenta el *overhead* en redes de gran tamaño al mantener precisamente este estado con su respectiva señalización; y tal vez la más importante de sus desventajas es que realiza la clasificación, monitoreo *(policing)*, encolamiento y planificación *(scheduling)* por flujos, lo que provoca un *overhead* cuando se trata de un gran número de estos.

En la actualidad se está trabajando en una integración de IntServ/RSVP-DiffServ que tendrá mucho que ofrecer como una alta escalabilidad y una solución más que eficiente para nuestras necesidades de Calidad de Servicio.

Cabe mencionar que para poder soportar las implementaciones de QoS en una red se debe tomar muy en cuenta el tipo de hardware que se empleará para ello, es por eso que se requiere de dispositivos que puedan realizar las actividades mencionadas anteriormente, como son: gestión de tráfico, evitar congestión en la red, realizar el conformado y monitoreo de tráfico *(traffic shaping y traffic policing)*, habilidad para manejar los Servicios Diferenciados y los requerimientos en encolamiento entro otros.

CAPÍTULO CUATRO
Análisis de la propuesta

4.1 Solución para E-Education.

Para empresas que requieren de los servicios que una red les puede proveer sin importar el giro al que se esté enfocada (educativo, industrial, gubernamental, investigación, comercial, etc.), actualmente puede encontrar una gran variedad de alternativas para satisfacer sus necesidades de comunicación.

Entre estas alternativas podemos incluir la creación de una red propia, el arrendamiento de la solución completa por parte de un Proveedor de Servicios de este tipo, o inclusive se puede emplear un esquema híbrido en el cual el cliente puede comprar equipo que crea conveniente y al mismo tiempo rentar el equipo y los servicios de un proveedor.

La empresa *E-Education* decide tomar en cuenta la alternativa de un modelo híbrido, donde integrará parte de equipo adquirido por ésta y la renta de servicios; y es aquí donde se habla de implementar una Red Privada Virtual empleando la arquitectura MPLS en un Proveedor de Servicios que en este caso será la *Red Maestra de Datos SysTel (RMDST).*

Siendo ésta la opción elegida al tomar en cuenta su cobertura, menores costos, mejores tiempos de implementación y su experiencia en el manejo de redes a nivel nacional. La evaluación y confrontación de las diversas propuestas que se le plantearon a la empresa *E-Education* por los distintos proveedores queda fuera del alcance del presente análisis dado que *E-Education* es la única entidad a quien concernía este proceso.

En esta parte del trabajo, como primer punto se describirán las diferentes necesidades de la empresa *E-Education* sobre el servicio de red, incluyendo las aplicaciones principales que se requieren para poder lograr la capacitación a distancia.

Posteriormente se dará a conocer la propuesta que nosotros planteamos y creemos que puede resolver la situación de *E-Education.* Esta corresponde a la proporcionada por una empresa líder en el mercado de telecomunicaciones *(RMDST)* dedicada al diseño e integración de soluciones corporativas de comunicación de datos, voz y vídeo; que inclusive forma parte del grupo *Smart Solutions.*

Esta propuesta de la solución al problema de *E-Education* incluye en su estructura una descripción funcional del proyecto, elementos que la conforman incluyendo el equipo a emplear así como su topología y el presupuesto que implica el adquirir o arrendar el hardware así como los servicios de transmisión de datos.

Después se discutirá el por qué esta solución fue propuesta revisando aspectos característicos de un proyecto a evaluar como pueden ser: cobertura, escalabilidad, disponibilidad, desempeño de la red, seguridad, administración, facilidad de uso, adaptabilidad y rentabilidad. Por último se hablará de la implementación de este proyecto y las fases que éste conlleva.

4.2 Necesidades de E-Education.

Como se mencionó en el primer capítulo del presente trabajo, *E-Education* es una empresa cuya principal actividad es brindar capacitación a las diversas empresas del grupo *Smart Solutions* a través de los múltiples planteles con que cuenta a lo largo de toda la República Mexicana.

La empresa *E-Education* con el fin de mantenerse a la vanguardia en el proceso educativo y con el objetivo de ofrecer un mejor servicio y optimizar su operación, ha decidido desarrollar nuevos programas de capacitación, dentro de los cuales podemos encontrar el denominado *Capacitación a Distancia,* programa que contempla el acceso a diferentes aplicaciones como son bibliotecas electrónicas, módulos de centro de consulta y videoconferencia en línea, a través de una red de telecomunicaciones que permita ofrecer servicios convergentes de voz, datos y vídeo, o bien por Internet.

Las aplicaciones desarrolladas para estos proyectos requieren de una red de comunicaciones que les garantice, además de la entrega íntegra de su información, tiempos de respuesta muy pequeños dado que algunas de ellas requieren interacción de los usuarios en tiempo real.

4.2.1 Aplicaciones.

A continuación se mencionarán las aplicaciones principales requeridas por la empresa *E-Education* para lograr la capacitación a distancia.

a. Sistema SCIEINTT.

Este sistema permite a los usuarios consultar por medio del navegador de su PC una base de datos centralizada, la cual contiene toda la información referente a los cursos ofrecidos por *E-Education*. El tráfico de esta aplicación es únicamente de Web y se transmite en ráfagas cada vez que una solicitud es resuelta.

b. Sistema de educación a distancia LearnLinc.

Ésta es la principal aplicación en la red dado que es el corazón del negocio de *E-Education*. Este es un sistema que permite, mediante la instalación de un cliente en cada PC participante, la realización de audio-conferencias enriquecidas con servicios como compartición de documentos, pizarra, chat, vídeo sobre demanda, etc. Las PCs cliente estarán localizadas en cada uno de los 10 nodos, que la red *E-Education* planea tener en su primera fase, en una sala denominada "aula de educación a distancia".

Como información adicional se tiene que en una audioconferencia el ancho de banda requerido por llamada es de alrededor de 30 kbps mientras que la solicitud de vídeo sobre demanda requiere de aproximadamente 400 kbps.

c. Sistema de videoconferencia H.323.

En este caso se pretende tener una sala con equipo de videoconferencia por cada uno de los 10 nodos que se integrarán a la red en su primera fase. Cada sistema generará en promedio por evento, flujos de 480 kbps.

Los requerimientos de esta aplicación además del ancho de banda son los que se indican en la tabla 4.1.

Requerimientos de la red	
Retardo total de extremo a extremo (latencia).	Menor o igual a 150 [ms].
Variabilidad del retardo *(jitter)*.	Menor o igual a 150 [ms].
Pérdida de paquetes.	Menor o igual al 1 %.

Tabla 4.1 Requerimientos mínimos de la red para el adecuado funcionamiento del sistema H.323

4.2.2 Conexión a redes externas.

Otra de las necesidades de *E-Education* es el poder tener acceso a Internet, ya que es requerido tanto por el sistema de videoconferencia como por la aplicación LearnLinc. Así de esta forma se puede tener acceso a sitios Web durante la impartición de un curso y se

puede permitir acceso a personas que no pueden tomar el evento en las instalaciones de *E-Education*, se espera que estos sean en su mayoría clientes de otras empresas del grupo.

También se requiere de acceso a Internet 2, dado que esta red de cómputo con capacidades avanzadas y de reciente desarrollo permite compartir mayores cantidades de información empleando elevadas velocidades en aplicaciones de alta tecnología así como en el acceso a grandes bases de datos. Algunas de las aplicaciones en desarrollo son: bibliotecas digitales, laboratorios virtuales, manipulación a distancia y visualización de modelos 3D; aplicaciones todas ellas que no serían posibles de desarrollar con la tecnología del Internet de hoy.

Tanto para la conexión al Internet como al Internet 2 se debe integrar un esquema de seguridad que permita mantener la integridad de los recursos de *E-Education*.

4.2.3 Cobertura.

E-Education al ser una empresa líder en el sector de capacitación requiere que sus servicios estén al alcance del mayor número de clientes posibles, es por eso que la cobertura que requiere esta empresa nacional es muy amplia, tendiendo a cubrir las ciudades más importantes en la República Mexicana.

Por el momento la empresa requiere que sus servicios estén presentes en 10 sitios estratégicos para su negocio tratando de cubrir en una primera etapa gran parte del territorio nacional. Posteriormente se pretende ampliar la cobertura de la red de servicios hasta 60 nodos, cabe mencionar que esto se contemplaría en etapas posteriores que no se toman en cuenta en este proyecto.

En la tabla 4.2 se enlistan los diez sitios que serán dados de alta en el proyecto y en los cuales se piensa que lograrán el objetivo de la empresa *E-Education*.

▪ Azcapotzalco	▪ Hermosillo
▪ Coyoacán	▪ Monterrey
▪ Cuernavaca	▪ Puebla
▪ Culiacán	▪ Querétaro
▪ Guadalajara	▪ San Luis

Tabla 4.2 Sitios considerados por E-Education estratégicos para brindar sus servicios y que serán los primeros en integrarse a la VPN E-Education.

Se muestra en la figura 4.1 un esquema donde se puede apreciar la cobertura requerida para el proyecto de la empresa *E-Education* en una fase inicial.

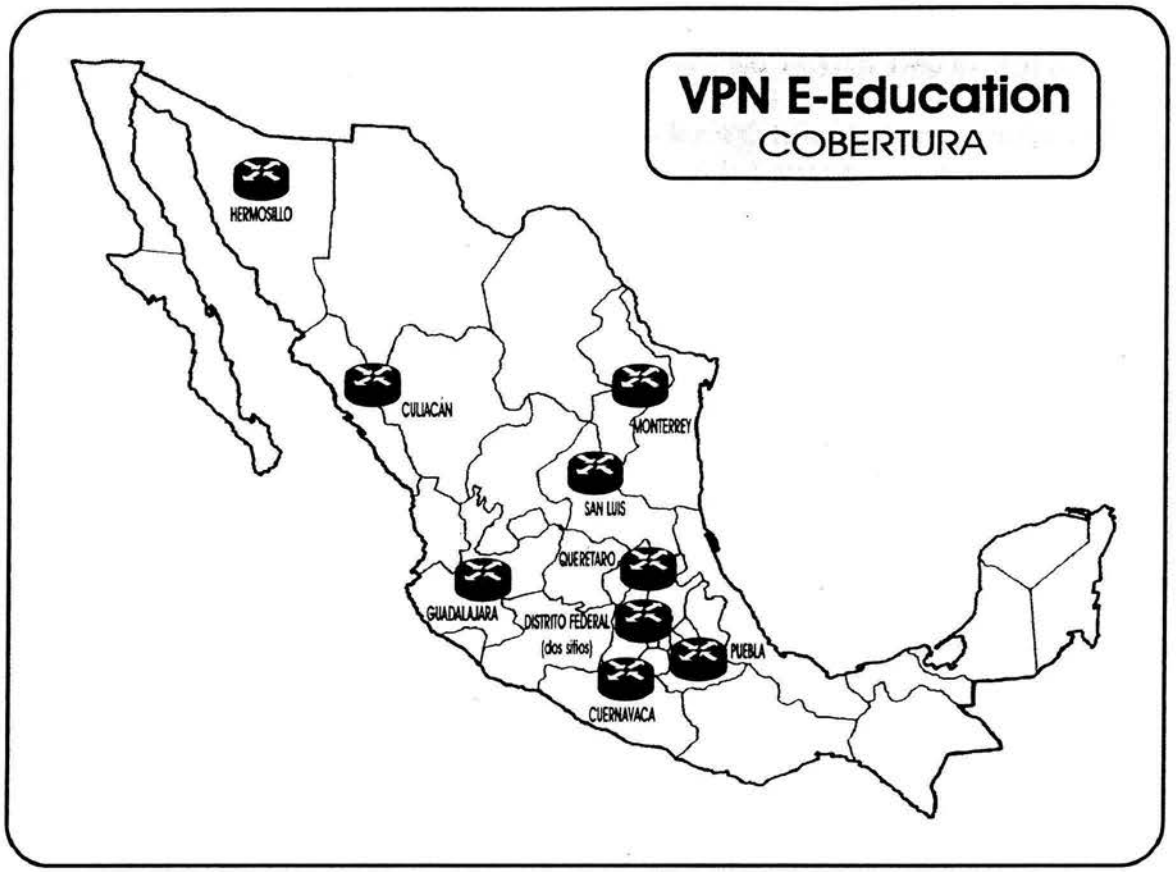


Figura 4.1 Cobertura de los servicios de E-Education.

4.3 Propuesta de la Red Maestra de Datos SysTel (RMDST).

La *Red Maestra de Datos SysTel* es el área encargada de ofrecer los servicios de administración, diseño y mantenimiento de la red interna de datos de la empresa *SysTel*, la cual también es considerada como una empresa líder en el mercado de las telecomunicaciones.

SysTel orienta todos sus recursos tecnológicos, humanos y financieros, a consolidar su liderazgo en el mercado, proveyendo servicios avanzados de telecomunicaciones en todas las regiones de nuestro país, buscando además nuevos horizontes en el plano internacional, para confirmarse como una de las empresas de telecomunicaciones de más rápido y mayor crecimiento a nivel mundial.

Después de que la *RMDST* analizó las necesidades principales de *E-Education* sobre el servicio de red; propone una solución estableciendo la factibilidad de implementarla y el impacto que esta tendría sobre la *Red Maestra de Datos SysTel (RMDST).*

Esta propuesta se orienta en aprovechar las ventajas que en cuanto a amplia cobertura, estabilidad y capacidad puede proporcionar la *RMDST* para crear una Red Privada Virtual que sea capaz de brindar los servicios de red requeridos por *E-Education.* Se propone un

diseño orientado a satisfacer estas necesidades y establece las modificaciones necesarias en la infraestructura de la *RMDST* para su implementación

Como ya se explicó en el apartado 4.2.1 referente a las aplicaciones requeridas por *E-Education*, LearnLinc es la principal aplicación en la red, ya es la que va a permitir la realización de audio-conferencias enriquecidas con otros servicios como el vídeo sobre demanda por ejemplo. La *RMDST* propone como parte de su proyecto, que en cada uno de los 10 nodos propuestos se instalen de 12 a 16 PCs y puedan tenerse un máximo de 10 eventos simultáneos. Entre los requerimientos específicos para esta aplicación tenemos que el ancho de banda del enlace de acceso a la red en cada nodo de *E-Education* será de 1984 kbps, lo cual limitará el número máximo de eventos simultáneos que estén recibiendo vídeo desde el servidor central a 5, siempre y cuando no esté en uso el sistema de videoconferencia H.323 (descrito en el apartado 4.2.1), en cuyo caso el número máximo sería de 4.

Dado que la aplicación, al menos en su fase inicial funcionará con direcciones unicast por limitaciones tecnológicas dentro de la *RMDST*, se debe optimizar el uso del ancho de banda mediante el uso de un servidor esclavo local en cada aula de educación a distancia. Supóngase que en un aula de educación a distancia se tienen tres participantes del mismo evento, en este caso el servidor estaría enviando tres flujos de datos (audio, vídeo o datos) uno por cada participante lo que ocasiona un uso ineficiente del ancho de banda que finalmente es un recurso limitado. Agregando un servidor esclavo local en la sala de Educación a Distancia éste se sincroniza con el servidor central y a través de la red sólo viaja un flujo de datos independientemente del número de participantes en un evento particular. La replica del flujo se haría de manera local donde el ancho de banda disponible permite tener "n" copias del flujo original. Por supuesto *E-Education* tendrá que evaluar cuales son las implicaciones que tiene el agregar los servidores esclavos ya que cualquier costo que se pudiera generar correría por su cuenta. En una fase posterior, una vez hechas las actualizaciones necesarias en la *RMDST*, se podría migrar la aplicación del uso de direcciones unicast a multicast.

Otro punto que también cabe señalar en esta introducción a la propuesta de la *RMDST*, es que para el desarrollo de actividades diversas relacionadas con los servicios de capacitación que *E-Education* brinda a *SysTel* es necesario permitir el acceso hacia algunos recursos ubicados dentro de la *RMDST*. El diseño de la interconexión y las políticas de seguridad que se aplicarán serán definidas por la *RMDST*.

4.3.1 Descripción funcional.

Tomando la información de las secciones anteriores la *RMDST* sugiere la implementación de una Red Privada Virtual, esto es, aprovechando la infraestructura de la *RMDST* se creará mediante el protocolo MPLS una red lógica totalmente independiente que brindará servicios de comunicación a las aplicaciones de *E-Education*. Las ventajas que ofrece esta solución son, entre otras, las siguientes:

- Redes totalmente independientes.
- No existe mezcla de tráfico entre redes.

- El cliente puede mantener su propio esquema de direccionamiento.
- Reducción de costos en enlaces, dado que sólo se rentan enlaces locales.
- Disponibilidad de una red de transporte con cobertura nacional, gran capacidad y tiempos de respuesta mínimos.

La solución propuesta denominada en adelante *Red Privada Virtual E-Education* o *VPN E-Education* se muestra en la figura 4.2. Este proyecto será implementado en tres fases, los sitios que serán integrados a la VPN en cada fase son determinados por *E-Education* de acuerdo a la importancia que para ellos represente. Durante la primera fase se integrarán los principales edificios de *E-Education* y sobre ella nos enfocaremos.

Si bien esta propuesta incluye el equipamiento que permitiría tener servicios de telefonía sobre la red, no se recomienda sea adquirido para la primera fase dado que aun no se conocen en detalle los requerimientos que *E-Education* pudiera tener a este respecto. El fin que se persigue al mencionarlo es el de tomar en cuenta el costo aproximado de la solución para fines de programación presupuestal.

Se recomienda que la solución de telefonía sea discutida más ampliamente entre *E-Education* y la *RMDST*, en caso de determinarse que *E-Education* requiere de esta solución se programe su implementación para la segunda fase del proyecto.

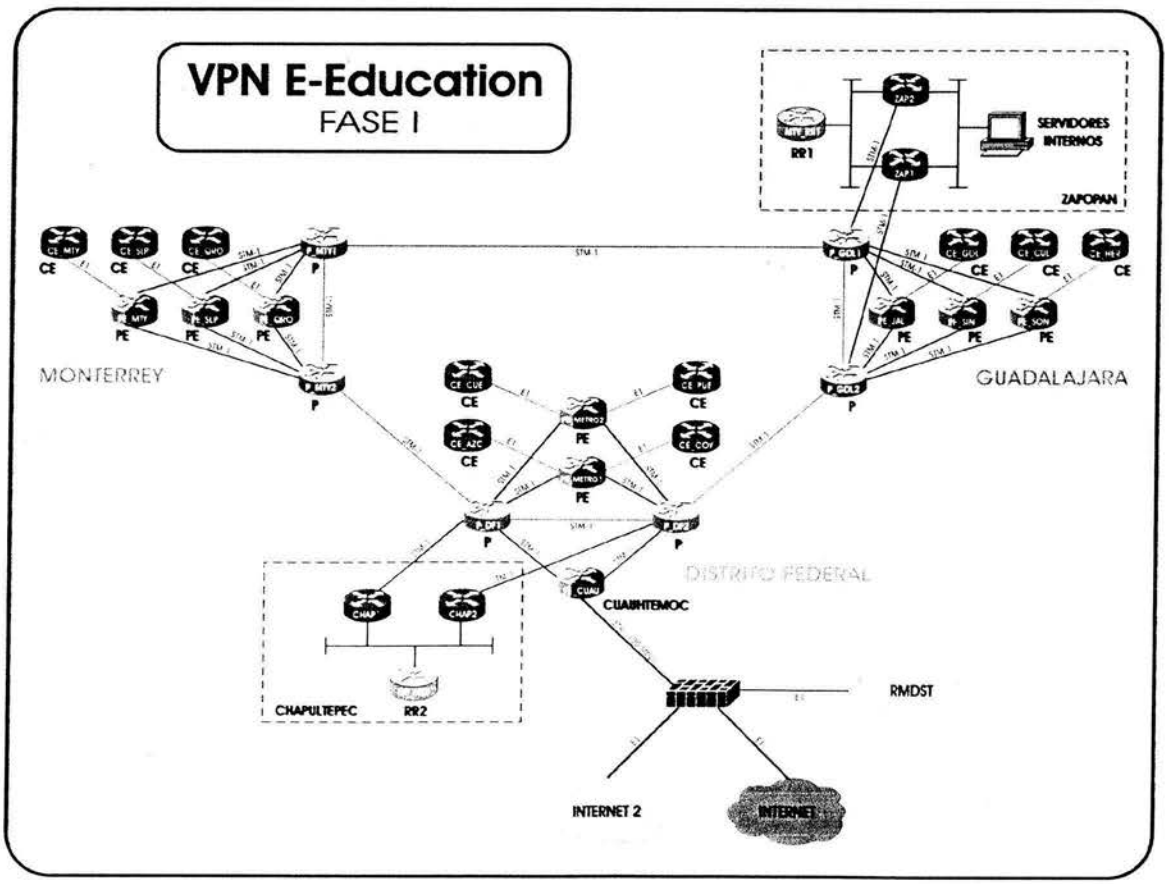


Figura 4.2 Solución propuesta por la RMDST para E-Education en su fase I.

4.3.2 Topología de la solución.

La *VPN E-Education* estará formada por los nodos Chapultepec y Zapopan, además de los edificios de *E-Education*, incluyendo aquellos que actualmente son nodos de la *RMDST* los cuales por cierto serán migrados al nuevo esquema.

Zapopan será parte de la *VPN E-Education* por ser el sitio en que se instalarán los principales servidores de *E-Education*. En la fase I se integrarán a la VPN los siguientes sitios (tabla 4.3):

- Cuauhtémoc (sitio central)
- Azcapotzalco
- Coyoacán
- Cuernavaca
- Culiacán
- Guadalajara
- Hermosillo
- Monterrey
- Puebla
- Querétaro
- San Luis

Tabla 4.3 Sitios que se integrarán a la VPN E-Education en su fase I.

4.3.3 Facilidades de transmisión.

Para los nodos de la VPN se utilizarán enlaces de 2.048 Mbps (E1). Con esto se dará servicio a la aplicación LearnLinc y al sistema de videoconferencia H.323 con la advertencia indicada anteriormente de tener un máximo de 5 eventos simultáneos haciendo transferencias de vídeo.

Para el caso de Cuauhtémoc se sugiere:

- Un enlace E3 conectado al nodo dorsal Cuauhtémoc de la *RMDST*.
- Un enlace E3 conectado al nodo dorsal Vallejo de la *RMDST* para tráfico diferente al de Internet 2 y en caso de contingencia como respaldo del enlace conectado al nodo dorsal Cuauhtémoc.
- Un enlace E3 ATM dedicado para conexión directa al Internet 2.
- Un enlace E1 dedicado para conexión directa al Internet.

Para poder tener acceso a Internet 2, por recomendación directa de la Corporación Universitaria para el Desarrollo de Internet (CUDI)[8] se requiere instalar en el nodo Cuauhtémoc un equipo capaz de recibir un enlace E3 con tecnología ATM.

El nodo central Cuauhtémoc forma parte del esquema de conexión seguro entre *E-Education*, la *RMDST*, el Internet y el Internet 2. Este esquema se describe completamente más adelante en el presente capítulo.

[8] El CUDI es una Asociación Civil que tiene por objeto promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México.

Respecto al nodo Zapopan, éste cuenta con un par de enlaces STM-1, donde uno es respaldo del otro. Al interior de Zapopan se cuenta con una arquitectura basada en switches de alta velocidad.

4.3.4 Equipamiento.

Para los nodos a ser integrados a la VPN en su primera fase, excepto Cuauhtémoc, se utilizarán enrutadores Cisco 3640 con 1 puerto Fast Ethernet, 1 puerto WAN y 2 puertos de voz analógicos.

En cuanto al nodo central Cuauhtémoc, el equipamiento necesario se describe más adelante en este capítulo, en el que se explica el detalle del esquema de conexión seguro.

Para el nodo Zapopan no se solicita equipo ya que se utilizará la infraestructura de la *RMDST*.

El detalle del equipamiento necesario para la requisición se incluye en la sección "Costos de implementación de la fase I del proyecto".

4.3.5 Sistema de administración de la red.

Se sugiere la adquisición de la herramienta de administración Resource Manager Essentials de Cisco Works.

Resource Manager Essentials (RME) es una suite de aplicaciones basadas en Web que ofrecen soluciones de administración para switches, servidores de acceso y enrutadores Cisco. La interfaz de RME permite fácil acceso a la información crítica de la red y simplifica las tareas administrativas altamente demandantes de tiempo mediante los siguientes componentes:

- Administrador de inventario.
- Auditor de cambios.
- Administrador de configuración de dispositivos.
- Administrador de imágenes de software.
- Administrador de disponibilidad.
- Analizador syslog.

Los detalles de las especificaciones del software y las características de la estación de trabajo necesaria se incluyen en la sección 4.3.7.

4.3.6 Esquema seguro de conexión.

Para mantener la integridad de los recursos de *E-Education* y la *RMDST*, mientras se brinda el servicio de acceso al Internet y al Internet 2, se requiere de la implementación de un esquema seguro de interconexión. Para ello la *RMDST* ha diseñado el Nodo de Acceso Seguro (NAS) para *E-Education* en el que se recibirán los enlaces al Internet y al Internet 2 y además se interconecten la *VPN E-Education* y la *RMDST*.

Respecto a la seguridad de la *VPN E-Education* se deben considerar los puntos de interconexión con redes externas, entre las que se incluyen:

- *RMDST*
- Internet
- Internet 2

En la siguiente figura 4.3 se muestra el esquema de interconexión de la VPN *E-Education.*

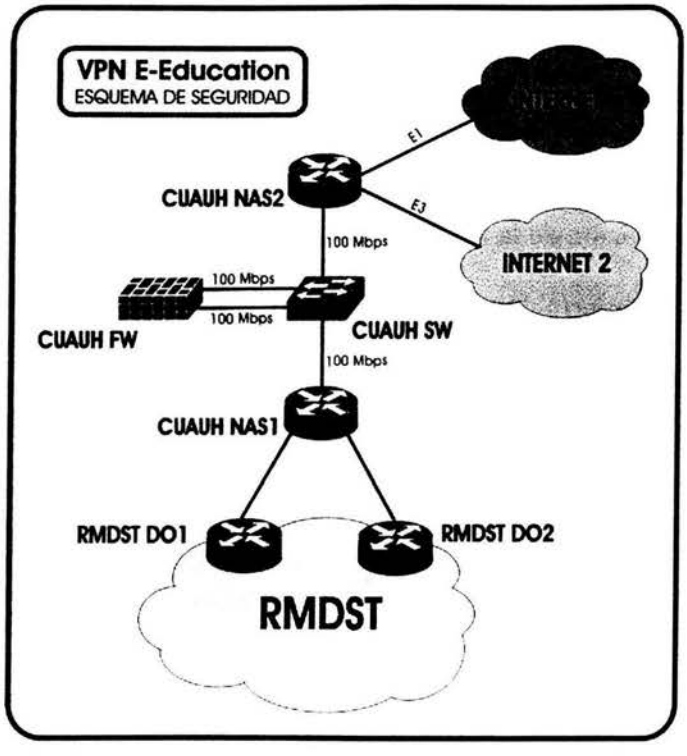


Figura 4.3 Esquema de Seguridad de Red para la VPN E-Education.

Entre las observaciones más importantes que se deben hacer respecto a este esquema de seguridad de red están:

- En Cuauhtémoc se conectarán dos enlaces E3 locales entre los enrutadores dorsales de la *RMDST* y la red de *E-Education.* El primer enlace será para el tráfico de la VPN de *E-Education* y el segundo para el tráfico entre *E-Education* y *RMDST.*

- Por medio de un *firewall* se controlará el paso de tráfico entre *E-Education* y las redes Internet e Internet2. Se propone un *firewall* PIX-525 de Cisco con una tarjeta de 4 puertos Fast Ethernet.

- La gestión y administración de los equipos de red de *E-Education* se realizará por personal de la *RMDST.*

- La interconexión entre *RMDST* e *E-Education* solamente se podrá realizar en Cuauhtémoc. No podrán existir otros puntos de interconexión.

- Se podrá difundir la red de *E-Education* dentro de la *RMDST* y viceversa.

Los costos estimados para implementar este sistema de seguridad se comentarán en la siguiente la sección.

4.3.7 Costos de implementación de la fase I del proyecto.

Para la implementación del proyecto, los costos se dividen en dos clasificaciones, una es la inversión inicial necesaria en infraestructura y se cuenta una sola vez y la segunda son los gastos recurrentes ocasionados por la operación de la red, en este caso se refieren básicamente a la renta de las facilidades de transmisión y del servicio de acceso a Internet. Las tablas 4.4 a la 4.13 muestran la descripción de ambos costos.

En la sección 4.3.8 se muestran las tablas donde se distribuyen los gastos de la implementación de la fase I del proyecto entre *E-Education* y la *RMDST*.

La tabla 4.4 indica el equipamiento necesario para los 10 sitios remotos que se integrará a la red en la primera fase. El costo viene dado en dólares americanos y correrá por parte del cliente que en este caso es *E-Education*.

Descripción	Precio Unitario	Cantidad Requerida	Total
Cisco 3600 4-Slot Modular Router-AC with IP Software	$6,500	10	$65,000
1-10/100 Ethernet 2 WAN Card Slot Network Module	$2,300	10	$23,000
1-Port Serial WAN Interface Card	$400	10	$4,000
V.35 Cable, DTE, Male, 10 Feet	$100	10	$1,000
Two-Slot Voice/Fax Network Module	$ 1,700	10	$17,000
Two-Port Voice Interface Card-FXS	$400	10	$4,000
24 Port, 10/100 Autosensing, Autonegotiating Catalyst Switch	$1,995	10	$19,950
Total			**$133,950**

Tabla 4.4 Costo de equipo de comunicaciones para sitios remotos (fase I).

La tabla 4.5 indica el costo de la actualización de memoria necesaria en los enrutadores de la *RMDST* que recibirán las conexiones de los nodos de la VPN *E-Education*. Este crecimiento en memoria es necesario para poder activar los procesos necesarios para la creación de la VPN en el enrutador sin afectar su desempeño. Dentro de la arquitectura de una VPN basada en MPLS estos enrutadores cumplirán la función de enrutadores PE y es así como se les denominará de aquí en adelante. El costo viene dado en dólares americanos y será cubierto por la *RMDST* dado que es parte de la infraestructura de la empresa que proporciona el servicio que está brindando.

Descripcion	Precio Unitario	Cantidad Requerida	Total
RSP 128MB DRAM Upgrade Kit	$2,400	8	$19,200
RSP2 Flash Card: 32MB Kit	$700	8	$5,600
Total			**$24,800**

Tabla 4.5 Costo de actualización de enrutadores PE de la RMDST.

La tabla 4.6 indica el costo del hardware y software necesario para la implementación del sistema de administración que será utilizado en la red. El costo está especificado en dólares americanos. Es importante reiterar que este sistema debe estar listo para entrar en operación antes de que se comience con la fase I del proyecto.

Descripcion	Precio Unitario	Cantidad Requerida	Total
Dual 10/100 Ethernet Router with 2 WIC Slots, 1 NM Slot	$3,095	1	$3,095
1-Port Channelized E1/ISDN-PRI Unbalanced Network Module	$2,600	1	$2,600
Servidor SUN Ultra 80 para el soporte de Cisco Works 2000	$32,000	1	$32,000
CiscoWorks2000 Routed WAN Management Solution (RWAN) 1.1	$15,000	1	$15,000
Total			**$52,695**

Tabla 4.6 Costo del Hw y Sw necesarios para el sistema de gestión de la red.

La tabla 4.7 indica el costo de instalación de los enlaces E1 que darán acceso a los nodos de *E-Education* a la *RMDST*. El monto viene dado en dólares americanos, de acuerdo al tiempo que se contrate es posible obtener algún descuento y dado que forma parte de la instalación de *E-Education*, correrá por cuenta de éste.

Descripcion	Precio Unitario	Cantidad Requerida	Total
Instalación de E1 por tramo	$8,050	20	$161,000
Total			**$161,000**

Tabla 4.7 Costo de instalación de enlaces E1 para acceso a la RMDST

La tabla 4.8 indica el costo de instalación de un enlace E1 para acceso al Internet y viene dado en dólares americanos. Esto no incluye la renta del servicio únicamente la instalación del enlace, de acuerdo al tiempo que se contrate es posible obtener algún descuento.

Descripcion	Precio Unitario	Cantidad Requerida	Total
Instalación de E1 por tramo	$8,050	2	$16,100
Total			**$16,100**

Tabla 4.8 Costo de instalación de enlace E1 para acceso a Internet

La tabla 4.9 indica el costo de instalación de un enlace E3 para acceso al Internet 2 así como para acceso a la *RMDST* y viene dado en dólares americanos, de acuerdo al tiempo que se contrate es posible obtener algún descuento.

Descripción	Precio Unitario	Cantidad Requerida	Total
Instalación de E3 por tramo	$40,755	2	$81,510
Total			**$81,510**

Tabla 4.9 Costo de instalación de enlace E3 para acceso a Internet y a la RMSDT.

De la tabla 4.10 a la 4.13, además de detallar el equipo que se implementará en el esquema de seguridad de red, muestran los costos aproximados en dólares, considerando fuentes de AC y precios de lista sin descuento.

Descripción	Precio Unitario	Cantidad Requerida	Total
24-Port 10/100 Switch	$1,995	1	$1,995
Total			**$1,995**

Tabla 4.10 Costo de equipo CUAUH SW.

Descripcion	Precio Unitario	Cantidad Requerida	Total
PIX 525 Unrestricted (Chassis, Software, Two 10/100 Ports)	$22,000	1	$22,000
PIX 4-Port 10/100 Ethernet Interface	$1,000	1	$1,000
Total			**$23,000**

Tabla 4.11 Costo de equipo CUAUH FW.

Descripción	Precio Unitario	Cantidad Requerida	Total
7204VXR +NPE-400,ISA, I/O Contr w/2FE-Ports +IPSEC 56	$20,000	1	$20,000
2-Port E3 Serial Port Adapter with E3 DSUs	$18,000	1	$18,000
4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)	$8,000	1	$8,000
2-port T1/E1 moderate capacity enhanced voice PA	$8,000	1	$8,000
Versatile Interface Processor 2, Model 50	$15,000	1	$15,000
Total			**$69,000**

Tabla 4.12 Costo de equipo CUAUH NAS1.

Descripcion	Precio Unitario	Cantidad Requerida	Total
7204VXR+NPE-400,ISA, I/O Contr w/2FE Ports+IPSEC 56	$20,000	1	$20,000
1-Port ATM Enhanced E3 Port Adapter	$8,000	1	$8,000
4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)	$8,000	1	$8,000
Total			**$36,000**

Tabla 4.13 Costo de equipo CUAUH NAS2.

La tabla 4.14 indica el costo total del equipamiento necesario para la implementación del Nodo de Acceso Seguro de *E-Education* que será ubicado en Cuauhtémoc.

Equipo	Costo
CUAUH SW.	$1,995
CUAUH FW.	$23,000
CUAUH NAS1.	$69,000
CUAUH NAS2.	$36,000
Total	**$129,995**

Tabla 4.14 Costo total del equipamiento para el Nodo de Acceso Seguro E-Education Cuauhtémoc.

Hasta aquí se han definido todos los gastos del equipo de comunicaciones y el sistema de administración. Estos gastos constituyen la inversión inicial necesaria para la implementación de la fase I del proyecto. En cada parte de la cotización se especificó por parte de quien correrían los gastos, ya sea *E-Education* o la *RMDST*.

A continuación en las tablas 4.15, 4.16 y 4.17 se indican los costos recurrentes de la renta mensual de enlaces de acceso a la VPN y la renta mensual del servicio de Internet y la renta del enlace de acceso al Internet 2. Los costos vienen dados en dólares americanos.

Los gastos de la renta de enlaces para acceso a la VPN, al Internet 2 al igual que la renta del servicio de acceso al Internet corren por cuenta de la *RMDST*.

Descripcion	Precio Unitario	Cantidad Requerida	Total
Renta mensual Lada enlace de 2 Mbps por tramo	$470	10	$4,700
Total			**$4,700**

Tabla 4.15 Renta mensual de Lada enlaces de 2 Mbps para nodos de la fase I.

Descripcion	Precio Unitario	Cantidad Requerida	Total
Renta mensual de enlace E1	$290	1	$290
Renta mensual de puerto E1	**$1,950**	**1**	**$1,950**
Renta mensual del servicio de acceso a Internet	$1,950	1	$1,950
Total			**$4,190**

Tabla 4.16 Renta mensual del servicio de acceso a Internet

Descripción	Precio Unitario	Cantidad Requerida	Total
Renta mensual de enlace E3	$4,940	1	$4,940
Total			**$4,940**

Tabla 4.17 Renta mensual del enlace de acceso al Internet 2.

4.3.8 Resumen de costos.

Para obtener el costo total de implementación del proyecto en su primera fase se toma la suma de los totales de las tablas 4.4 a la 4.9 y la 4.14, el cual se muestra en la tabla 4.18. Este costo total será dividido entre la *RMDST* y *E-Education*. La parte que corresponde a la *RMDST* y a *E-Education* se muestra en las tablas 4.19 y 4.20 respectivamente.

Descripción	Total
Equipamiento para 10 sitios foráneos	$133,950
Actualización de memoria de 8 PEs	$24,800
Sistema de gestión	$52,695
Instalación de enlaces E1 de acceso a la RMDST	$161,000
Instalación de enlace para acceso a Internet	$16,100
Instalación de enlace para acceso a Internet 2	$81,510
Equipamiento para el NAS E-Education Cuauhtémoc	$129,995
Total	**$600,050**

Tabla 4.18 Costo total del proyecto en su fase I.

Descripción	Total
Actualización de memoria de 8 PEs	$24,800
Instalación de enlaces E1 de acceso a la RMDST	$161,000
Instalación de enlace para acceso a Internet	$8,050
Instalación de enlace para acceso a Internet 2	$81,510
Sistema de gestión	$52,695
Total	**$328,055**

Tabla 4.19 Costo del proyecto para la RMDST.

Descripción	Total
Equipamiento para 10 sitios foráneos	$133,950
Equipamiento para el NAS E-Education Cuauhtémoc	$129,995
Total	**$263,945**

Tabla 4.20 Costo del proyecto para E-Education.

Cabe señalar que lo anterior fue referido a la implementación física de los dispositivos y enlaces a emplear, falta incluir los gastos de la renta mensual de los enlaces, de los cuales *E-Education* se encargará de cubrir, estos se muestran en la tabla 4.21.

Descripcion	Precio Unitario	Cantidad Requerida	Mensual	Semestral	Anual
Renta mensual Lada enlace de 2 Mbps por tramo para nodos de la fase I	$470	10	$4,700	$25,380	$47,940
Renta mensual del servicio de acceso a Internet incluyendo puerto, enlace y servicio	$4,190	1	$4,190	$22,626	$42,738
Renta mensual de enlace E3 de acceso al Internet 2	$4,940	1	$4,940	$26,676	$50,388
Total			**$13,830**	**$74,682**	**$141,066**

Tabla 4.21 Renta mensual de los todos los enlaces.

En la tabla 4.21 podemos observar el gasto que implica la renta de los enlaces ya sea mensual, semestral o anual; precios que ya incluyen un descuento según la cantidad de tiempo que se puede rentar.

La implementación del proyecto se llevará a cabo en tres fases. Antes de comenzar cualquiera de las fases deberán cumplirse totalmente las tareas previas necesarias indicadas por la *RMDST*. A manera de ejemplo se listan a continuación las tareas que deberán cumplirse antes de comenzar con la fase I y los responsables de llevarlas a cabo (tabla 4.21).

Tareas	Responsable
Solicitud de compra de equipo de comunicaciones.	RMDST y E-Education
Solicitud de compra del sistema de administración.	RMDST y E-Education
Solicitud de enlaces.	RMDST
Recepción e Instalación de equipos.	RMDST y E-Education
Recepción y puesta en operación del sistema de administración.	RMDST
Recepción de enlaces.	RMDST
Elaboración del plan de trabajo para la implementación de la fase I.	RMDST
Configuración de equipos en fase I.	RMDST y E-Education

Tabla 4.21 Tareas que deben cumplirse antes de comenzar la fase I y los responsables de realizarlas.

Una vez cubiertas estas tareas previas se procederá a la implementación de la VPN en su primera fase, realizándose inclusive una serie de pruebas para validar el correcto funcionamiento de la red para posteriormente liberarla para su entrada en producción.

La integración de cualquier nuevo nodo posterior a la fase I deberá ser solicitada a la *RMDST* por medio de la Gerencia de Servicio a Clientes.

4.3.9 Justificación de la propuesta de la RMDST.

Como se mencionó al principio de este capítulo se justificará la selección de la propuesta que se ha venido planteando, es por eso que a continuación se mencionarán las razones por las cuales se considera este proyecto como uno de los más completos y que

creemos, puede llegar a solucionar la problemática de la empresa y por ende cubrir las metas tanto técnicas como comerciales de esta misma.

Comenzaremos mencionando que esta solución nos ofrece en cuanto a cobertura se refiere, una zona muy amplia en la que la empresa podrá compartir sus servicios de capacitación, es decir con la implementación de esta VPN empleando la infraestructura de la *RMDST* se pueden llegar a cubrir los principales edificios de *E-Education.* Al iniciar el proyecto se comenzará con 10 sitios, los cuales como se describió anteriormente están distribuidos estratégicamente, y que al ampliarse el proyecto mediante las fases posteriores se podrá llegar a tener una gran cobertura sobre la mayor parte de la República (ver figura 4.1).

Este modelo de red nos permite ampliarla de una forma más eficaz que si empleáramos otra topología u otra tecnología ajena a las VPNs basadas en MPLS. Así de esta forma su escalabilidad y adaptabilidad a los cambios no es tan compleja. Si el cliente así lo requiriera podría expandir su red estableciendo más nodos realizando movimientos mínimos. El proveedor simplemente tendría que instalar un enlace del enrutador del cliente (enrutador CE) al enrutador PE que forma parte de la infraestructura rentada, obviamente realizando las configuraciones necesarias para el levantamiento de este nuevo sitio.

La implementación de este esquema no es muy compleja, inclusive la administración de la red generalmente queda en manos del Proveedor de Servicios quitándole un peso de encima al cliente y evitándole gastos en personal encargado de realizar esta tarea así como capacitarla.

Se propuso un esquema de conexión seguro implicando el uso de un *firewall*, lo cual siendo un punto a favor ayuda a mantener la seguridad e integridad de la información que viaja a través de la VPN.

Tal vez uno de los puntos más importantes y que ha llegado a ser un elemento definitivo en la elección de proyectos en concursos es el referido a los costos. El dinero es un factor muy importante en muchas empresas y es por eso que además de querer obtener altos beneficios de sus proyectos, estas también desean que sean rentables. El principal objetivo de la rentabilidad es transportar la máxima cantidad de tráfico dado un costo financiero.

La implementación de VPNs basadas en MPLS permite al cliente ahorrarse no sólo la instalación del equipo sino también una serie de servicios necesarios. En nuestro caso los costos del hardware y software necesarios para el sistema de gestión de la red son absorbidos por el Proveedor de Servicios (SP) ya que cuenta actualmente con esa infraestructura de gestión, por lo tanto este servicio se le ofrece al cliente por parte de la *RMDST* como un valor agregado. Y lo más importante y que hace de esto un proyecto atractivo es que la propuesta de la *RMDST* sólo cobrará la renta mensual entre los enrutadores del cliente y los PEs.

CAPÍTULO CINCO
Implementación de la VPN

5.1 Introducción.

Con la introducción de MPLS en la red del Proveedor de Servicios, es posible trasportar cualquier tipo de tráfico manteniendo la confidencialidad del mismo, a través de una red pública de datos, creando una Red Privada Virtual basada en MPLS.

Es necesario conocer y establecer el procedimiento mediante el cual se agregarán nodos a la Red Privada Virtual; a continuación se muestran los procedimientos necesarios para la implementación de MPLS en la red de la *RMDST*:

En seguida se presentarán las configuraciones para la configuración básica del PE; así mismo la configuración entre el PE y CE usando únicamente Enrutamiento Estático.

5.2 Adición y configuración de un nuevo PE.

5.2.1 Requisitos de hardware y software.

Para poder implementar MPLS en los equipos de la *RMDST* los nodos PE deberán de cumplir con los mínimos requisitos siguientes:

- Tener físicamente 128 MB de memoria RAM y un mínimo de 16 MB de memoria FLASH.
- El IOS mínimo que se necesita para poder emplear cualquiera de las siguientes funcionalidades es de la Main Line 12.0S, la versión mínima será 12.0(22)S; sin embargo ésta podrá cambiar en función del hardware, principalmente por la plataforma[9]

5.2.2 Adición de un nuevo PE para agregar un CE.

La figura 5.1 muestra el esquema típico para la adición de un nuevo PE a la Red Dorsal de MPLS ya existente.

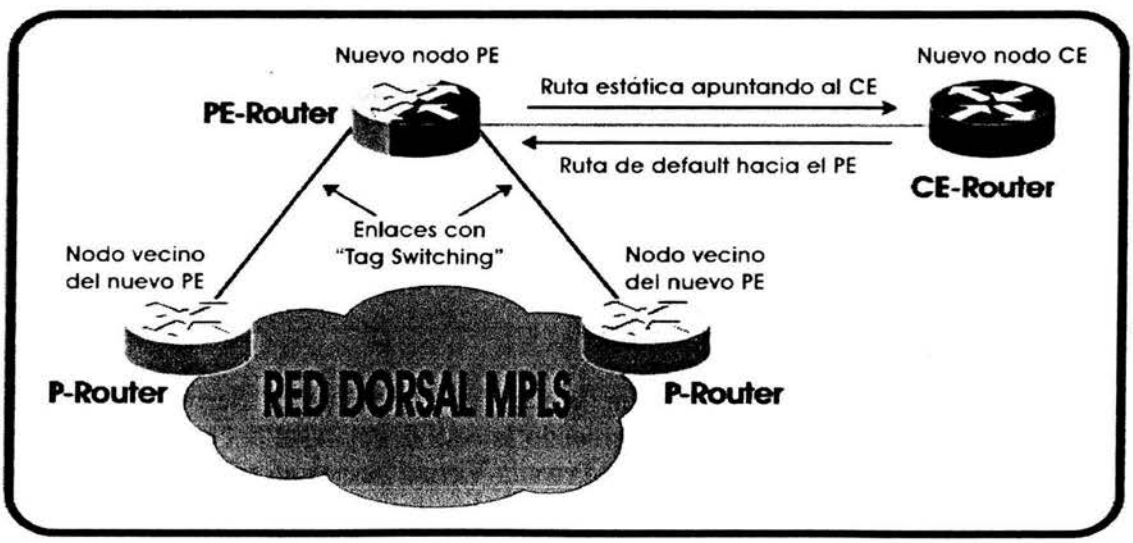


Figura 5.1 Esquema de conexión de un PE a un CE.

5.2.3 Activación de CEF en el PE.

Como se había mencionado en la sección 3.3.1 es necesaria la activación de CEF en todos los enrutadores que realizarán manejo de etiquetas (imposición, retiro e intercambio), esto debido a que en la implementación de Cisco Systems para esta tecnología la tabla que emplea CEF será el origen para la creación de la Tabla de Adyacencias de MPLS, por lo cual es un requisito indispensable.

[9] Esto se puede corroborar usando el Feature Navigator de Cisco Systems. http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp.

La modalidad de CEF empleado en los PE dependerá de la plataforma de los mismos, se recomienda que se verifique la operabilidad del mismo usando la herramienta Feature Navigator (propiedad de Cisco Systems) si es necesario emplear otras plataformas distintas a las que a continuación se mencionan.

Existen dos principales modalidades para emplear CEF en las plataformas de Cisco Systems:

1. CEF centralizado, en el cual las tareas son realizadas por el procesador central del equipo; es necesario contar el IOS mínimo igual a 12.0(22)S.

2. CEF distribuido, en el cual las tareas son realizadas de manera individualizada por cada tarjeta; es necesario contar el IOS mínimo igual a 12.1(14)S.

Cualquiera de las opciones que se escoja es posible activar o desactivar CEF a nivel interfase; para habilitar CEF en un enrutador se debe de seguir con los siguientes pasos:

- En el modo de configuración global:

```
! Para el modo centralizado
!
ip cef
!

! Para el modo distribuido
!
ip cef distributed
!
```

- En modo de configuración por interfase:

```
! Para tarjetas FSIP
!
ip route-cache
!

! Para tarjetas VIP
!
ip route-cache distributed
!
```

5.2.4 Migración hacia MPLS en los enlaces de los enrutadores P y PE.

Para la imposición, retiro y manipulación de etiquetas, Cisco Systems emplea Tag-Switching y la norma MPLS; por el momento se preferirá la primera hasta que la implementación de MPLS madure dentro del IOS. Por ello cuando se elija una IOS para manipular etiquetas se buscará esta funcionalidad.

Para configurar Tag-Switching en un enrutador se hará de la siguiente manera:

i. Para la creación de la Tabla de Adyacencias, mediante el Tag Distribution Protocol, se empleará una interfase loopback10 definida con anterioridad en toda la red (Router ID) y que será conocida usando el mismo IGP que la red esté actualmente usando.

ii. Se definirá un filtro que permitirá exclusivamente la distribución de las etiquetas asociadas a esta VPN a través de la interfase loopback222.

iii. Para los enlaces E1 el MTU en MPLS se definirá fijo a un tamaño de 1524 bytes y se configurará en cada uno de los enlaces de los vecinos de la red dorsal. Este valor se debe a la explicación de la sección 3.1.10; cabe recordar que para enlaces con MTU mayor a 1518 no será necesario este comando.

Se necesitarán los siguientes comandos:

- En el modo de configuración global:

```
! Definición del Router ID para en el TDP usando una interfase loopback
!
tag-switching tdp router-id loopback10
!
```

- En el modo de configuración por interfase:

```
! Se configura en los enlaces entre Ps y entre PEs
!
tag-switching ip
!
```

Para los enlaces seriales con requisitos específicos de MTU:

```
!
tag-switching mtu 1524
!
```

Creación del filtro para la distribución de etiquetas en el modo de configuración global:

```
!
interface loopback222
ip address 10.222.1.x
!
access-list 22 permit 10.222.1.0 0.0.0.255
!
no tag-switching advertise-tags
tag-switching advertise-tags for 22
!
```

En este momento es posible verificar el funcionamiento de Tag-Switching con los siguientes comandos:

```
show tag-switching forwarding-table

Router#show tag-switching forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Untagged    10.10.1.3/32     0          Se2/0       point2point
17     Pop tag     10.222.1.3/32    0          Se2/0       point2point
18     Untagged    10.0.0.8/30      0          Se2/0       point2point
19     Untagged    10.10.1.5/32     0          Et0/0       192.168.2.2
20     Untagged    10.222.1.5/32    10949      Et0/0       192.168.2.2
21     Untagged    10.10.1.1/32     0          Se3/0       point2point
22     Pop tag     10.222.1.1/32    0          Se3/0       point2point
23     Untagged    10.10.1.4/32     0          Se2/0       point2point
24     25          10.222.1.4/32    1120       Se2/0       point2point
```

Hay que prestar atención a la columna "Outgoing tag or VC" allí deberán aparecer las asociaciones con etiquetas pertenecientes a las loopback222, ya sean Pop tag, Untagged o el número de etiqueta que le corresponde.

5.2.5 Configuración de la VPN.

Una parte importante en la implementación de la VPN es el uso de MP-BGP, descrito en la sección 3.3.3 la comunicación entre CEs de la misma VPN se logra a través de la transferencia de información entre los PEs mediante MPLS y de MP-BGP.

La principal ventaja de MP-BGP es que proporciona dos importantes elementos para lograr la VPN:

i. Se pueden configurar diferentes VPNs gracias al uso de VRFs.

ii. Diferentes clientes pueden usar el mismo direccionamiento gracias a los Route Distinguishers.

Como consecuencia de la complejidad que puede alcanzar la administración y configuración de una VPN debido al uso de MP-BGP, se ha optado el uso de Route Reflectors, de tal suerte que cuando un PE se quiera comunicar con otro de la misma VPN usará la información que el RR le reenvíe.

Para lograr simplicidad, es posible utilizar el concepto de peer-groups, que permite simplificar las configuraciones si se tienen políticas idénticas para un mismo grupo de PEs.

La implementación de la VPN seguirá los siguientes lineamientos:

1. La VRF tomará el nombre de EEDUC.

2. Los identificadores Route Distinguisher (RD) y Route Target (RT) tendrán el mismo valor para poder propagarlos correctamente, cuyos valores serán a 10.69.0.0 para el RD y 10.69.0.0:1 para el RT.

3. En una etapa inicial existirán un par de Route Reflectors cuyas direcciones *loopback* serán: 10.222.1.5 y 10.222.1.6.

```
! Definición de la VRF
!
ip vrf EEDUC
 rd 10.69.0.0:1
 route-target import 10.69.0.0:1
 route-target export 10.69.0.0:1
!


!Configuración de BGP para los Route Reflectors
!
interface loopback10
 ip address 10.10.5.1 255.255.255.255
!
interface Loopback222
 ip address 10.222.1.5 255.255.255.255
!
router bgp 5555
 no synchronization
 bgp router-id X
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor EEDUC peer-group
 neighbor EEDUC remote-as 5555
 neighbor EEDUC update-source Loopback222
 no auto-summary
 !


! Configuración del bloque para enrutamiento
!
address-family vpnv4
neighbor ip_del_PE_agregado active
 neighbor ip_del_PE_agregado send-community both
 neighbor ip_del_PE_agregado peer-group EEDUC
 no auto-summary
  exit-address-family
!
```

```
! Configuración para los PEs
!
interface loopback10
 ip address 10.10.1.X 255.255.255.255
!
!
route-map loopback222
 set ip next-hop ip_de_loopback222
!
!
router bgp 5555
 no synchronization
 bgp router-id 10.10.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor ip_del_RR_principal remote-as 5555
 neighbor ip_del_RR_principal update-source Loopback222
 neighbor ip_del_RR_respaldo remote-as 5555
 neighbor ip_del_RR_respaldo update-source Loopback222
 no auto-summary
!
!
address-family ipv4 vrf EEDUC
redistribute static
 no auto-summary
 no syncronization
 exit-address-family
!
address-family vpnv4
 neighbor ip_del_RR_principal active
 neighbor ip_del_RR_principal send-community both
 neighbor ip_del_RR_principal route-map loopback222 out
 neighbor ip_del_RR_respaldo active
 neighbor ip_del_RR_respaldo send-community both
 neighbor ip_del_RR_respaldo route-map loopback222 out
 bgp scan-time import 5
 bgp scan-time 10
 no auto-summary
 exit-address-family
!
```

5.2.6 Comandos para verificar operación de BGP.

Después de haber configurado correctamente los parámetros para la operación de BGP aparecerá en el puerto de consola del enrutador el siguiente mensaje:

```
%BGP-5-ADJCHANCE: neighbor x.x.x.x Up
```

Si se ha establecido una sesión remota usando TELNET, previamente se deberá usar el comando

```
terminal monitor
```

Posteriormente establecida la sesión de BGP, pueden obtenerse más detalles de dicha sesión mediante el siguiente comando:

```
show ip bgp neighbors
```

En el despliegue buscar la línea:

```
BGP state = Established, up for *****
```

Tal y como se muestra a continuación:

```
Router#show ip bgp neighbors
BGP neighbor is 10.222.1.5,  remote AS 5555, internal link
  BGP version 4, remote router ID 10.222.1.5
  Last read 00:00:50, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: received
    Address family VPNv4 Unicast: advertised and received
```

5.2.7 Asignación de puertos a la VPN en el PE.

En esta sección se analizará la configuración para los nuevos equipos CE que se agreguen a la VPN. En la mayoría de los casos la siguiente configuración se aplicará a interfases seriales, pero puede ser aplicada a cualquier interfase en común entre un PE y el nuevo CE.

```
!
! Definición de una interfase para la VPN en el PE
interface X
 ip vrf forwarding EDDUC
 ip address dirección_ip máscara_asignada
!
```

En el caso particular de que existan enlaces paralelos entre el PE y el CE, todos ellos deberán ser agregados a la VPN.

5.2.8 Verificación de la correcta asignación de puertos.

Para llevar a cabo esta tarea se usará el siguiente comando:

```
show ip vrf
```

```
Router#show ip vrf
  Name                              Default RD          Interfaces
  EEDUC                             10.69.0.0:1         Serial2/0
                                                        Loopback69
```

5.2.9 Adición de un CE a un PE existente.

Como se mencionó en la sección 3.3.3 la comunicación entre el PE y el CE puede ser llevada a cabo de distintas maneras; por simplicidad de administración así como por la topología empleada, que se muestra en la figura 5.1 se utilizarán rutas estáticas en ellos. En el PE se configurará una ruta que englobe al segmento al que pertenece el CE; en el CE se usará una ruta por default de tal suerte que el PE se convertirá en el único punto de salida para éste:

```
! Definición de una interfase para la VPN en el PE
interface X
 ip vrf forwarding EEDUC
 ip address dirección_ip máscara_asignada
!
```

En el modo de configuración global:

```
! Configuración de la ruta estática en el PE para el segmento del CE
!
ip route vrf EEDUC segmento_del_CE máscara_asignada  interfase_hacia_el_CE
!

! Configuración en el CE de la ruta por default hacia el PE
!
ip route 0.0.0.0 0.0.0.0 interfase_hacia_el_PE
ip classless
!
```

5.2.10 Configuración de los parámetros para QoS.

Para asegurar que el tráfico perteneciente a la VPN sea transportado con un nivel de preferencia sobre el resto, se etiquetará para que tenga una Calidad de Servicio distinto al resto, adicionalmente para enviar el tráfico hacia la red dorsal; en ambos casos se utilizará Class Based Weighted Fair Queuing (CBWFQ).

En el modo de configuración global

```
! ACLs para la selección de tráfico
!
access-list 120 permit ip any any
!
!Definición de la clase que lo etiqueta
!
class-map match-all ALLTRAFFIC
  match access-group 120
 class-map match-all ALTA
  match mpls experimental topmost 3
 class-map match-all MEDIA
  match mpls experimental topmost 2
!
policy-map QOS
  class ALLTRAFFIC
   set dscp cs3
!
 policy-map QOSCORE
  class ALTA
   priority 512
   police cir 512000 bc 16000 be 16000
     conform-action transmit
     exceed-action set-mpls-exp-topmost-transmit 2
  class MEDIA
   bandwidth 512
   police cir 512000 bc 16000 be 16000
     conform-action transmit
     exceed-action set-mpls-exp-topmost-transmit 1
  class class-default
   fair-queue
!
```

5.2.11 Aplicación de QoS en las interfases del PE.

En modo de configuración de la interfase para la etiquetación de paquetes:

```
!
 ip vrf forwarding EEDUC
 ip address ip_correspondiente_interfase
 service-policy input QOS
!
```

```
Para el envío de paquetes
```

```
!
 ip address ip_correspondiente_interfase
 service-policy output QOSCORE
!
```

5.2.12 Verificación final del funcionamiento de la VPN.

Para verificar el funcionamiento correcto de la VPN hasta la capa del Modelo de Referencia del modelo OSI, se empleará el comando ping pero con capacidades para VPN:

```
ping vrf identificador_de_la_vrf
```

Desde cualquier enrutador PE:

```
ping vrf EEDUC 10.69.1.1 ! dirección de uno de los RR

ping vrf EEDUC 10.69.1.X ! dirección del CE recién agregado
```

Desde el CE recién agregado

```
ping vrf EEDUC 10.69.1.1 ! dirección del RR
```

De ser posible se corroborará el correcto funcionamiento utilizando las aplicaciones, que será el objetivo final de la VPN.

5.2.13 Configuraciones usadas para la VPN.

A continuación se muestra el resumen de las configuraciones usadas para la creación de la VPN, se incluyen las configuraciones de un RR, un PE y finalmente del CE, propiedad de cliente.

5.2.14 Configuración del Route Reflector.

```
r_220RR#sh run
Building configuration...

Current configuration : 1773 bytes
!
version 12.2
!
hostname r_220RR
```

```
!
logging queue-limit 100
!
clock timezone PST -8
ip subnet-zero
no ip domain lookup
!
ip vrf EEDUC
 rd 10.69.0.0:1
 route-target export 10.69.0.0:1
 route-target import 10.69.0.0:1
!
ip cef
mpls ldp logging neighbor-changes
no tag-switching advertise-tags
tag-switching advertise-tags for 22
tag-switching tdp router-id Loopback10
!
!
interface Loopback10
 ip address 10.10.1.5 255.255.255.255
!
interface Loopback222
 ip address 10.222.1.5 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 tag-switching mtu 1524
 tag-switching ip
!
router eigrp 10
 network 10.0.0.0
 network 192.168.2.0
 no auto-summary
!
router bgp 5555
 no synchronization
 bgp log-neighbor-changes
 neighbor EEDUC peer-group
 neighbor EEDUC remote-as 5555
 neighbor EEDUC update-source Loopback222
 neighbor 10.222.1.1 peer-group EEDUC
 neighbor 10.222.1.4 peer-group EEDUC
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.222.1.1 activate
 neighbor 10.222.1.1 route-reflector-client
 neighbor 10.222.1.1 send-community both
 neighbor 10.222.1.4 activate
 neighbor 10.222.1.4 route-reflector-client
 neighbor 10.222.1.4 send-community both
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf EEDUC
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
no ip http server
!
```

```
!
access-list 22 permit 10.222.1.0 0.0.0.255
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

5.2.15 Configuración del Router PE.

```
r_170#sh run
Building configuration...

Current configuration : 2224 bytes
!
version 12.2
!
hostname r_170
!
ip subnet-zero
!
ip vrf EEDUC
 rd 10.69.0.0:1
 route-target export 10.69.0.0:1
 route-target import 10.69.0.0:1
!
ip cef
mpls ldp logging neighbor-changes
no tag-switching advertise-tags
tag-switching advertise-tags for 22
tag-switching tdp router-id Loopback10
!
!
 class-map match-all ALLTRAFFIC
  match access-group 120
 class-map match-all ALTA
  match mpls experimental topmost 3
 class-map match-all MEDIA
  match mpls experimental topmost 2
!
!
 policy-map QOS
  class ALLTRAFFIC
   set dscp cs3
!
 policy-map QOSCORE
  class ALTA
   priority 512
   police cir 512000 bc 16000 be 16000
     conform-action transmit
     exceed-action set-mpls-exp-topmost-transmit 2
  class MEDIA
   bandwidth 512
   police cir 512000 bc 16000 be 16000
     conform-action transmit
     exceed-action set-mpls-exp-topmost-transmit 1
  class class-default
   fair-queue
!
```

```
!
interface Loopback10
 ip address 10.10.1.1 255.255.255.255
!
!
interface Loopback222
 ip address 10.222.1.1 255.255.255.255
!
interface Serial2/0
 ip vrf forwarding EEDUC
 ip address 172.16.1.1 255.255.255.252
 service-policy input QOS
!
interface Serial3/0
 ip address 10.0.0.1 255.255.255.252
 service-policy output QOSCORE
 tag-switching mtu 1524
 tag-switching ip
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
router bgp 5555
 no synchronization
 bgp router-id 10.10.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.222.1.5 remote-as 5555
 neighbor 10.222.1.5 update-source Loopback222
 no auto-summary
 !
 address-family ipv4 multicast
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.222.1.5 activate
 neighbor 10.222.1.5 send-community both
 neighbor 10.222.1.5 route-map loopback222 out
 no auto-summary
 exit-address-family
 !
 address-family ipv4
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf EEDUC
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route vrf EEDUC 192.168.2.0 255.255.255.0 Serial2/0
no ip http server
!
!
access-list 22 permit 10.222.1.0 0.0.0.255
access-list 120 permit ip any any
!
```

```
route-map loopback222 permit 10
 set ip next-hop 10.222.1.1
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

5.2.16 Configuración del Router CE.

```
r_160#sh run
Building configuration...

Current configuration : 614 bytes
!
hostname r_160
!
interface Ethernet0
 ip address 192.168.2.1 255.255.255.0
!
interface Serial2/0
 ip address 172.16.1.2 255.255.255.252
!
interface Serial3/0
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
no ip http server
!
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Como se puede apreciar en las configuraciones, mientras que la configuración del RR es la más grande, pues éste contiene información de todos los vecinos para la VPN, el PE solamente tiene que formar vecindad con los RR de la red. El CE, propiedad del cliente no sabe acerca de la VPN y no necesitará configuraciones especiales.

5.2.17 Usando un Protocolo de Enrutamiento entre PE y CE.

Es posible que el cliente tenga varios segmentos IP que quiera anunciar al resto de los equipos que pertenecen a su red, como antes se había revisado todas ellas se pueden anunciar usando rutas estáticas, pero por comodidad usar un Protocolo de Enrutamiento como RIPv2, OSPF, BGP o EIGRP. Es posible transportar las rutas de esos protocolos

dentro de la VPN y llevarlas al resto de los sitios del cliente, sin que ellas interfieran con la operación de la VPN.

En el caso de que las rutas sean aprendidas usando BGP desde el CE-router la redistribución no es necesaria dado que es llevada a cabo automáticamente, aunque el contexto de enrutamiento (proceso de BGP) y la configuración de vecinos debe de ser configurada dentro del mismo proceso de BGP usando un *address-family* diferente.

Por lo tanto hay dos requisitos básicos para este esquema, el primero será configurar las sesiones de MP-iBGP entre los PE-routers; el segundo es la configuración de BGP entre los PE-routers y los CE-routers.

En la mayoría de los casos el PE y el CE deben de estar directamente conectados, dado que establecen una sesión de eBGP. Si la versión de IOS lo permite es posible utilizar multi-hop para que estos no estén directamente conectados.

A continuación se muestran las configuraciones en el PE y el CE para que el cliente pueda usar BGP entre los sitios de su red. Se ha considerado usar BGP dado que es un protocolo de fuente abierta y que puede ser empleado aún entre enrutadores de diferentes marcas a Cisco.

```
!
!Configuración en el PE
!
router bgp 5555
 no synchronization
 no bgp default ipv4-unicast
 neighbor ip_del_RR remote-as 5555
 neighbor ip_del_RR update-source Loopback222
 no auto-summary
 !
 address-family ipv4 vrf EEDUC
 neighbor ip_del_CE remote-as YYYY
 neighbor ip_del_CE activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 !
```

Como se puede apreciar dentro de la configuración de la VRF a ser transportada por BGP se han removido los comandos *redistribute connected* y *redistribute static* y se han puestos los comandos:

```
neighbor ip_del_CE remote-as YYYY
neighbor ip_del_CE activate
```

Donde el remote AS es que el cliente ocupa actualmente, mismo que puede ser público u homologado o privado.

```
!
¡Configuración del CE
!
router bgp YYYY
 no synchronization
 no bgp default ipv4-unicast
 neighbor ip_del_PE remote-as 5555
 no auto-summary
!
```

Como puede apreciarse la configuración es la típica empleada si es que se tuviera un vecino normal de BGP.

Estas configuraciones pueden ser empleadas en todo momento, aunque se recomienda usarla sólo en alguna de las siguientes configuraciones:

1. Cuando el cliente tenga muchos segmentos de red diferentes que no puedan ser sumarizadas para anunciar a sus vecinos, esto evitará tener rutas estáticas en el PE-router apuntando al CE-router.

2. Cuando el cliente tenga enlaces a diferentes PE-routers en esquemas de redundancia.

Es importante recalcar que al emplear BGP como Protocolo de Enrutamiento se obtienen una base sólida e idónea para ejecutar entre los equipos, sin embargo hay que observar que los recursos del PE pueden verse agotados al tener diferentes instancias de BGP corriendo en el mismo equipo.

5.3 Fase I: Migración de los 10 sitios críticos para el cliente dentro de la VPN E-Education.

5.3.1 Fase IA-1: Activación de MPLS México – Monterrey y Monterrey – Monterrey.

A continuación se muestran los enlaces que en los que se activará MPLS que pertenecen a la red dorsal, dichos enlaces son STM-1 entre los equipos P_DF1 y P_MTY2, así mismo entre los equipos P_MTY1 y P_MTY2.

La tabla 5.1 muestra la relación de interfaces, dirección IP y equipo en los cuales se activará Tag-Switching.

Enrutador	Interfase	Dirección IP
P_DF1	POS 1/0/1	10.0.0.18
P_MTY2	POS 1/1/1	10.0.0.17
P_MTY2	POS 1/1/2	10.0.0.14
P_MTY1	POS 1/0/1	10.0.0.13

Tabla 5.1 Relación de interfaces en donde se habilitará Tag-Switching en la Fase 1A-1

Para la configuración de estos enlaces, revise la sección 5.2.4 "Migración hacia MPLS en los enlaces de los enrutadores P y PE".

Posterior a la activación se tendrá un período de observación de 48 horas debida a la criticidad de los enlaces involucrados. Si durante el período no se presenta ninguna falla se procederá a la siguiente activación.

5.3.2 Fase IA-2: Activación de MPLS Guadalajara – Monterrey y Guadalajara – Guadalajara.

A continuación se muestran (tabla 5.2) los enlaces que en los que se activará MPLS que pertenecen a la red dorsal, dichos enlaces son STM-1 entre los equipos P_MTY1 y P_GDL1, así mismo entre los equipos P_GDL1 y P_GDL2.

Enrutador	Interfase	Dirección IP
P_MTY1	POS 1/0/2	10.0.0.9
P_GDL1	POS 1/0/1	10.0.0.10
P_GDL1	POS 1/0/2	10.0.0.5
P_GDL2	POS 1/1/1	10.0.0.6

Tabla 5.2 Relación de interfases en donde se habilitará Tag-Switching en la Fase IA-2.

Para la configuración de estos enlaces, revise la sección 5.2.4 "Migración hacia MPLS en los enlaces de los enrutadores P y PE".

Posterior a la activación se tendrá un período de observación de 48 horas debida a la criticidad de los enlaces involucrados. Si durante el período no se presenta ninguna falla se procederá a la siguiente activación.

5.3.3 Fase IA-3: Activación de MPLS Guadalajara – México y México – México.

En esta fase se finaliza con la activación de Tag-Switching en los enlaces que pertenecen a la dorsal. Se habilitará entre los equipos P_GDL2 y P_DF2 asi como entre P_DF2 y P_DF1 (ver tabla 5.3).

Enrutador	Interfase	Dirección IP
P_GDL2	POS 1/1/2	10.0.0.1
P_DF2	POS 1/0/1	10.0.0.2
P_DF2	POS 1/0/2	10.0.0.22
P_DF1	POS 1/0/2	10.0.0.21

Tabla 5.3 Relación de interfases en donde se habilitará Tag-Switching en la Fase IA-3.

En este punto toda la red dorsal estará habilitada para poder usar MPLS, por lo cual las pruebas mencionadas en la sección de configuración deberán de ser correctas.

Se recomienda un período de observación de 72 horas después de completar las Fases IA–1, IA–2 y IA–3. Si durante este período no ha presentado ninguna eventualidad, entonces se procederá con la siguiente parte de la implementación de la VPN.

5.3.4 Fase IB: Puesta en operación del Route Reflector DF_RR2.

Como primer paso para la creación de la VPN será necesario de establecer las sesiones de MP-BGP, de tal suerte que las todas las rutas externas a la dorsal puedan ser distribuidas correctamente entre los enrutadores de frontera, PE-routers. Los pasos para la configuración a emplear puede revisarse en "Configuración de la VPN" en la sección 5.2.5.

Una vez puesto en operación este equipo, se recomienda hacer pruebas para verificar la conectividad con los equipos P de la red dorsal. Habrá un período de observación de 24 horas en este equipo antes de la puesta en operación del segundo Route Reflector, MTY_RR1.

5.3.5 Fase IC: Puesta en operación del Route Reflector MTY_RR1

La puesta en operación del segundo Route Reflector MTY_RR1 se llevará una vez que expire el período de observación del Route Reflector ubicado en la Ciudad de México DF_RR2. Los pasos para la configuración a emplear puede revisarse en "Configuración de la VPN" en la sección 5.2.5.

Igual que en la puesta en operación del primer Route Reflector habrá un período de observación de 24 horas. En este punto es posible observar el funcionamiento de los dos Route Reflectors operando bajo BGP. Las pruebas recomendadas aparecen en la misma sección que contiene la configuración a seguir para estos equipos.

5.3.6 Fase ID: Configuración de MPLS en los enlaces entre los PE-routers y los P-router.

En este punto la configuración de MPLS entre los P-routers, correspondiente a la Fase 1A debe de estar terminada; sin embargo los enlaces entre los equipos PE-router y los P-routers está pendiente. De tal suerte que la configuración para estos enlaces se dará en la misma manera que la Fase antes mencionada; se deberán de seguir los pasos mencionados en la sección 5.2.4 "Migración hacia MPLS en los enlaces de los enrutadores P y PE".

5.3.7 Fase IE: Integración de PEs piloto.

Después de la puesta en operación de los dos Route Reflectors, se agregará esta subfase en la cual se configurarán 3 equipos PE de acuerdo con la sección 5.2.5 "Configuración de la VPN". Se tendrá una interfase *loopback* temporal, se ha escogido que sea la loopback69.

Los equipos seleccionados para ser los pilotos en esta subfase de prueba serán lo siguientes (tabla 5.4):

Enrutador	Direccion IP de loopback69
PE_METRO1	10.69.1.1
PE_GDL2	10.69.1.12
PE_MTY1	10.69.1.14

Tabla 5.4 Enrutadores PEs piloto.

Las interfases *loopback* quedarán configuradas como a continuación de muestra:

```
interface Loopback69
 ip vrf forwarding EEDUC
 ip address 10.69.1.1 255.255.255.255
```

Dicha interfase se integrará temporalmente a la VPN EEDUC para verificar la correcta propagación de las rutas a través de MP-BGP. Para realizar las pruebas mencionadas en la sección en donde se encuentran las configuraciones, habrá que agregar lo siguiente:

```
address-family ipv4 vrf EEDUC
 redistribute connected
exit-address-family
```

Al finalizar las pruebas pertinentes la interfase loopback69 así como la configuración que la incluye en la VRF, será removida de la configuración de dichos equipos, pues únicamente se configurará para verificar la funcionalidad de la VPN y no será necesaria para la puesta en operación de todos los equipos de la VPN.

Estos enrutadores se tendrán bajo observación por un período de 24 horas dentro de las cuales se realizaran prueba de conectividad entre los 3 equipos.

5.3.8 Fase IF: Integración de CEs piloto.

De común acuerdo con el cliente previamente al inicio de esta etapa los trabajos de migración no se comenzarán en tanto los requisitos en cuanto a instalaciones (eléctricas, de espacio y funcionamiento) definidas por la *RMDST* no sean cumplidas al 100%. Para ello personal en cada una de las regiones asistirá a cada uno de los sitios propuestos para hacer el reconocimiento y levantamiento de los mismos para confirmar que los trabajos pueden comenzar sin contratiempos. Así mismo la *RMDST* deberá de realizar todos los trámites necesarios de tal suerte que los enlaces entre los equipos PE-routers y los CE-routers estén listos para cuando se haga el levantamiento final antes de la puesta en operación de la red.

Las configuraciones pertinentes estarán basadas en su totalidad en la documentación prevista en el presente documento, las configuraciones serán adecuadas a las necesidades y equipamiento existente en cada Región esto es, la direcciones IP pertenecientes al sitio y los segmentos del cliente a ser anunciados por los PE-router a través de la ruta estática que pertenece a la VRF; se han presentado configuraciones modelo y típicas que ejemplifican en la totalidad los pasos y escenarios posibles.

Se escogerán 3 sitios que serán integrados a la VPN como prueba piloto, previo a una migración masiva de CE a lo largo de todo el país.

A continuación se muestra la relación de los 3 sitios CE piloto y los enrutadores PE a los cuales se agregarán estos (tabla 5.5):

Enrutador CE	Enrutador PE
CE_COY	PE_METRO1
CE_PUE	PE_METRO2
CE_QRO	PE_QRO

Tabla 5.5 Sitios CE para pruebas piloto.

La configuración necesaria para la asignación de puertos en los equipos PE, se describe en la sección 5.2.7 "Asignación de puertos a la VPN en el PE". La configuración en los equipos CE pilotos deberán seguir la configuración descrita en el apartado 5.2.9 "Adición de un CE a un PE existente".

Después de que las pruebas pertinentes se hayan realizado entre los equipos CE del cliente, se establecerá un período de observación de 48 horas, mismos que servirán para continuar con las pruebas que el cliente considere necesarias.

5.3.9 Fase IG: Puesta en operación del Nodo de Acceso Seguro en el nodo Cuauhtémoc.

El Nodo de Acceso Seguro ubicado en la Zona Metropolitana, correrá a cargo de la empresa MAXSEC, la cual se ha subcontratado para que ponga en funcionamiento el esquema de conexión a redes externas. Los tiempos, documentación relativa a esa migración no se contemplan dentro de este documento, por ser de carácter técnico y fuera del alcance del presente.

5.3.10 Fase IH: Integración masiva de CEs.

Concluida la adición de los 3 sitios piloto y habiendo transcurrido el período de pruebas sin mayor contratiempo, se integrarán todos los sitios restantes programados para la Fase 1 del proyecto a la VPN; Los PE-routers a los que se conectarán los CE-routers fueron determinados con anterioridad basados en la cercanía del segundo al primero, así los enlaces entre ellos serán de la menor distancia posible y la renta mensual no incluya gastos por Larga Distancia. Se ha previsto el caso de que existan dos PE-router en la misma zona geográfica y a la misma distancia, el criterio que se adoptó para esta situación es la carga de tráfico que se presente en el nodo de ingreso a la VPN. Con estos criterios previamente revisados y concensados, se ha construido la tabla 5.6 que se muestra a continuación:

Enrutador CE	Enrutador PE
CE_CUE	PE_METRO2
CE_AZC	PE_METRO1
CE_MTY	PE_MTY
CE_SLP	PE_SLP
CE_GDL	PE_JAL
CE_CUL	PE_SIN
CE_HER	PE_SON

Tabla 5.6 Relación de los CE restantes pertenecientes a la Fase I.

Al igual que los sitios piloto, se seguirán las recomendaciones de las secciones "Asignación de puertos a la VPN en el PE" y "Adición de un CE a un PE existente" respectivamente.

5.4 Fase II: Integración de nuevos CEs.

En esta etapa se integrarán todos los sitios restantes programados en el proyecto. El alcance del presente documento no contempla el seguimiento sitio a sitio en la Fase II, sin embargo la migración de todos los sitios restantes se llevará a cabo conforme a lo previsto durante la Fase IH, así mismo se seguirán los pasos en la sección 5.2.9 "Adición de un CE a un PE existente".

Conclusiones

Gran parte del presente trabajo está dedicada al entendimiento de fundamentos teóricos, para que basados en éstos se logre el objetivo principal, que es el de realizar un diseño de una solución que resuelva un problema de ingeniería enfocado a las redes de datos. La información que se logra recopilar en este documento nos ayuda a entender, diseñar e implementar una VPN empleando la red de un Proveedor de Servicios *(RMDST)* auxiliándose de la arquitectura MPLS, para de esta forma lograr la interconectividad entre las distintas sedes de una empresa de capacitación *(E-Education)*.

El uso de las redes de datos en las compañías de cualquier tamaño así como de cualquier ramo, comienza a ser una necesidad, por lo que la demanda de estos servicios va en aumento constantemente; sin embargo crear una Red Privada era caro y no todas las empresas podían costearla pese a ser de gran ayuda para sus negocios.

Tratando de resolver este problema se introducen nuevas tecnologías como IPSec que dieron paso a crear Redes Privadas Virtuales que abarataron los costos de las redes corporativas, sin embargo por las mismas características de esta tecnología, encriptar el contenido de los paquetes y la detección de diferencias de ellos para verificar su integridad no permitían brindar opciones de Calidad de Servicio que garantizaran que el trafico más importante para la empresa fuera transportado con preferencia sobre el resto del tráfico. Adicionalmente se requería equipo especializado o programas que lo hicieran eficientemente, lo que implicaba costos adicionales regularmente cubiertos por el usuario final.

Con la introducción de MPLS en la red dorsal de un Proveedor de Servicios se permite crear túneles dentro de la misma red en base al intercambio de etiquetas que se le agregan a los paquetes IP, permitiendo un envío más rápido y eficiente basado en ellas y no en las técnicas convencionales. Esto hace que la red sea más ágil, dado que se elimina el proceso que realizaba cada nodo de la red, el de revisar en cada paquete la dirección a la cual se dirigía.

Esto aunado con las nuevas características que proporcionan las extensiones de multiprotocolo de BGP, MP-BGP es posible crear múltiples instancias de enrutamiento en un mismo equipo lo que permitirá tener múltiples VPNs en un mismo equipo, esto como resultado final crea la posibilidad de usar una Red Pública de Datos, que le pertenece a un Proveedor de Servicios, para tener VPNs independientes y con el mismo nivel de seguridad que se obtiene con enlaces dedicados tales como Frame-Relay o enlaces de ISDN.

Además permite utilizar técnicas de Calidad de Servicio directamente en los paquetes lo que permite incluso manejar aplicaciones que son sensibles al retardo tales como Voz

sobre IP (VoIP). Es decir MPLS permite el empleo de Servicios Diferenciados para ofrecer distintos tratos a diferentes tipos de flujos de tráfico a través de la red.

Cómo se puede revisar a lo largo del presente documento, el usuario final no tiene que usar equipo o programas especializados; las configuraciones son idénticas como si se tratará de un enlace permanente y dedicado, el mayor cambio en arquitectura e implementación es por parte del Proveedor de Servicios por lo que es más sencillo y transparente para el usuario final adoptar esta nueva tecnología. Esta facilidad que se permite en la escalabilidad hace que el usuario logre integrar nuevos nodos a la red (expandir su negocio) cuando lo desee y realizando esto en pocos pasos. Además de que en la mayoría de los casos la gestión de la red no recae en el cliente sino en el SP.

Por lo tanto se puede llegar a la conclusión de que la implementación de VPNs basadas en MPLS permite a las empresas tener a su alcance redes de datos más económicas, con un grado de complejidad menor, con una gran capacidad de adaptación además de ser más flexibles y rápidas. Características por las que se inclinaría cualquier empresa que esté involucrada en el negocio de la capacitación como es el caso de *E-Education.*

Las tablas donde se ven reflejados los costos que implican implementar una red de este tipo, nos dan una mejor idea de la reducción de costos al dividir los gastos entre la empresa que contrata el servicio y el Proveedor de Servicios; y a medida que se implementen por más Proveedores de Servicios éstos se verán reducidos aún más. Estas técnicas comenzaban a ser estudiadas e implementadas hace casi dos años, pero hoy son una realidad a nivel mundial incluyendo su uso nuestro país, así Proveedores de Servicios como Telmex o ATT proporcionan este servicio a la par de los enlaces dedicados, siendo la creación de Redes Privadas Virtuales hoy más común que la instalación de Enlaces Dedicados.

Adicional a estos cambios, se tiene que con la introducción de nuevos avances tecnológicos tales como Multicast, es posible reducir los flujos duplicados de información y hacer uso más eficiente de la capacidad de los enlaces existentes tales como reproducción de un vídeo que puede ser atendido por muchas personas de manera simultanea. Esta aplicación que se menciona aunado al empleo de Multicast y de las VPNs está adquiriendo actualmente mucho interés por parte de redes corporativas donde aplicaciones como capacitación a distancia están permitiendo una reducción de costos atractiva.

El empleo de este tipo de tecnología (MPLS sobre VPNs) ha llevado a muchas empresas a cubrir sus metas técnicas y comerciales casi por completo, por lo que cada día más empresas llegan a convencerse de que es una opción muy completa y con un gran futuro. Por lo que MPLS está siendo integrada en el mercado de una forma muy rápida y se está convirtiendo en un estándar para ser implementada en los backbones de SPs.

Lo que se logró con el presente trabajo fue mostrar desde el punto de vista de un diseñador de redes todas las variables que se encuentran en juego para lograr obtener éxito en un proyecto de este tipo. Es decir, el ingeniero debe observar el proyecto de una manera integral, basándose en los objetivos de la empresa, y además de tomar en cuenta las aplicaciones que se requieren y el diseño de la red en general, debe tener presente puntos

ajenos a lo técnico referentes a: presupuestos, tiempos de implementación, alcances de los proyectos en cada una de sus fases, personal limitado para trabajar en éstos, gente que se verá o no beneficiada con el nuevo proyecto, etc.

Es por eso necesario el empleo de algún método que ayude a lograr integrar todas estas variables permitiendo al ingeniero (diseñador) obtener resultados satisfactorios para la empresa. Al inicio de este trabajo se demostró que el método *Top-Down* permite lograr esto, primero el diseñador obtiene una enorme foto del proyecto y después la va detallando basándose en los requerimientos y especificaciones técnicas. La mayoría de las veces el éxito de proyectos relacionados con el diseño de redes y que además es considerado parte fundamental del método *Top-Down* es el conocimiento de las necesidades y metas del cliente, ya sean comerciales, técnicas o inclusive ambas.

Por último, entre los beneficios más relevantes con los que una empresa obtiene al emplear este tipo de métodos se pueden mencionar: aumentar ingresos y beneficios, mejorar las comunicaciones empresariales, obtener ciclos cortos en el desarrollo de productos y aumentar la productividad de los empleados, crear asociaciones con otras compañías, expandirse a los mercados en todo el mundo, desplazarse hacia modelos comerciales de redes globales, hacer los datos disponibles para todos los empleados y oficinas para que se puedan tomar mejores decisiones en los negocios, mejorar la seguridad y la confiabilidad de los datos así como de las aplicaciones críticas, y para finalizar ofrecer un mejor soporte y nuevos servicios a los clientes.

Apéndice A. Comandos de MPLS – VPNs

A continuación se describen brevemente algunos de los comandos empleados para la configuración de MPLS VPNs:

`ip cef`
Habilita el Cisco Express Forwarding (CEF) en la tarjeta del procesador del enrutador.

`ip cef distributed`
Habilita la operación CEF distribuida (dCEF). Distribuye información CEF a las tarjetas de la línea (line cards). Las tarjetas de la línea realizan envío expreso.

`ip vrf EEDUC`
Configura una Tabla de Enrutamiento de una instancia de enrutamiento/envío de una VPN (VRF). Este comando crea una Tabla de Enrutamiento VRF y una tabla CEF. Asociado a estas tablas existe un valor distinguidor de ruta (route distinguisher).

`rd 10.193.0.0:1`
Este comando crea Tablas de Enrutamiento y de envío para una instancia de enrutamiento/envío de una VPN. También especifica un distinguidor de ruta (route distinguisher) por default para una VPN.

`route-target export 10.193.0.0:1`
Se usa para crear una comunidad extendida route-target para una VRF. Exporta información de enrutamiento hacia la comunidad extendida de la VNP destino.

`route-target import 10.193.0.0:1`
Importa información de enrutamiento de la comunidad extendida de la VNP destino.

`no tag-switching advertise-tags`
Deshabilita la distribución de etiquetas usando *Tag Distribution Protocol* TDP, con sus valores por omisión.

`no mpls advertise-labels`
Sirve para impedir la distribución de etiquetas (de entrada) asignadas localmente por medio del *Label Distribution Protocol* (LDP).

`tag-switching advertise-tags for loopback111`
`mpls ldp advertise-labels for loopback111`
Sirve para controlar la distribución de etiquetas localmente asignadas por medio del LDP. Al emplear *for*, se especifica cuales destinos debe tener sus etiquetas anunciadas.

tag-switching tdp router-id Loopback666
mpls ldp router-id Loopback666
Especifica una interfase preferida para determinar la ID del enrutador LDP.

interface Serial10/1/1
Este comando se usa para especificar una interfase serial creada en un controlador T1 canalizado o E1 canalizado. Se requiere del número de la ranura y del número del puerto donde el controlador E1 o T1 canalizado está localizado.

tag-switching mtu 1524
Se usa para invalidar o pasar por alto la máxima unidad de transmisión (MTU) por interfase. El mínimo es 128 bytes y la máxima depende del tipo de interfase.

tag-switching ip
Este comando es empleado para permitir el intercambio de etiquetas de paquetes IPv4. El intercambio dinámico de etiquetas es permitido por este comando, esto es, la distribución de etiquetas basada en protocolos de enrutamiento.

router bgp 666
Este comando es para configurar un proceso de enrutamiento BGP 666 es el número de un sistema autónomo que identifica al enrutador a otros enrutadores BGP y que etiqueta la información de enrutamiento que es pasada a lo largo de éste. Este comando permite configurar un centro (core) de enrutamiento distribuido que automáticamente garantice el intercambio libre de *loops* de la información de enrutamiento entre sistemas autónomos.

no synchronization
Habilita el software Cisco IOS para anunciar una ruta de la red sin esperar por el IGP. Esta función permite a enrutadores y servidores de acceso dentro de un sistema autónomo a tener la ruta antes de que BGP la haga disponible a otros sistemas autónomos.

bgp router-id 10.111.7.24
Configura una ID fija de un enrutador como un identificador de un enrutador que trabaja con BGP. Una interfase *loopback*, si existe configurada una, es más efectiva que una interfase fija como identificador porque no existe un enlace físico que sufra una caída.

no bgp default ipv4-unicast
Se emplea para permitir la familia de direcciones unicast IP versión 4 (IPv4) en todos los vecinos.

bgp cluster-id 221933310
Se emplea para configurar el ID de un cluster si el cluster BGP tiene más de un reflector de rutas (route reflector). Un route reflector junto con sus clientes forma un cluster. Usualmente un cluster de clientes tendrá un sólo route reflector. En ese caso, el cluster es identificado por el ID del enrutador del route reflector. Con el fin de incrementar redundancia y evitar un sólo punto de falla, un cluster debe de tener más de un route reflector. En este caso, todos los route reflectors en el cluster deben ser configurados con un

ID de 4 bytes, para que un route reflector pueda reconocer actualizaciones de route reflectors del mismo cluster.

bgp log-neighbor-changes
Este comando permite realizar un registro de los cambios de estado de un vecino BGP y reinicializaciones para la solución de problemas de conectividad de la red así como de la medición de estabilidad de la red.

neighbor EEDUC peer-group
Sirve para crear un *Peer Group* BGP o multiprotocolo BGP. Usualmente cuando se habla BGP o multiprotocolo BGP, varios vecinos son configurados con las mismas políticas de actualización. Vecinos con las mismas políticas de actualización pueden ser agrupados en peer groups para simplificar la configuración y hacer las actualizaciones más eficientes.

neighbor EEDUC remote-as 666
Se usa para agregar una entrada a la tabla de vecinos BGP o Multiprotocolo BGP.

neighbor EEDUC update-source Loopback666
Se usa para que el software Cisco IOS permita sesiones BGP para usar cualquier interfase para conexiones TCP.

neighbor EEDUC activate
Se emplea para intercambiar información con un vecino BGP.

neighbor 10.111.7.27 remote-as 666
Se usa para agregar una entrada a la tabla de vecinos BGP o multiprotocolo BGP.

neighbor 10.111.7.27 update-source Loopback666
Se usa para que el software Cisco IOS permita sesiones BGP para usar cualquier interfase para conexiones TCP.

no auto-summary
Para desactivar la restauración el comportamiento por default de la sumarización automática de rutas de subredes en rutas a nivel de red. También se usa para enviar información de enrutamiento de subprefijos a través de los límites de redes classful.

address-family ipv4 vrf EEDUC
Para entrar al modo de configuración de familia de dirección (address family configuration mode) para configurar sesiones de enrutamiento como BGP que usa el estándar de los prefijos de las direcciones IP versión 4. Este comando pone al enrutador en el modo de configuración address family, donde se pueden configurar sesiones de enrutamiento que usan el estándar de prefijos de direcciones IP versión 4.

redistribute static
Redistribuye rutas de un dominio de enrutamiento hacia otro.

default-information originate
Se usa para controlar la redistribución de un protocolo o red dentro de BGP. Este comando debe ser usado si el operador de la red necesita controlar la redistribución de rutas por default.

exit-address-family
Se usa para salir del modo de configuración family address. Puede ser abreviado por exit.

address-family vpnv4
Se emplea para entrar al modo de configuración family address y poder configurar sesiones de enrutamiento, como BGP, que usa el estándar de prefijos de direcciones Virtual Private Network (VPN) versión 4.

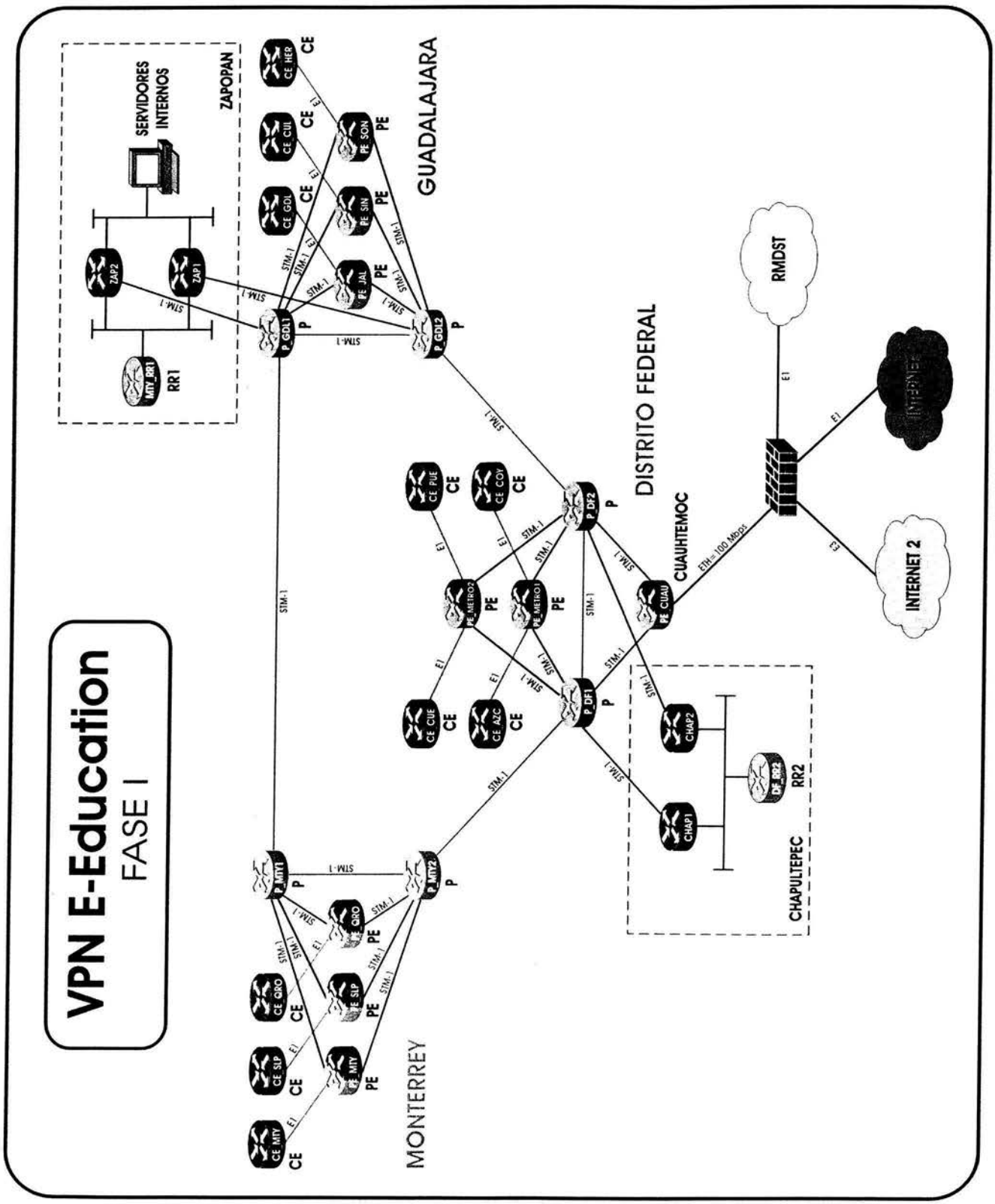
neighbor 10.111.7.27 activate
Se emplea para intercambiar información con un vecino BGP.

exit-address-family
Se usa para salir del modo de configuración family address. Puede ser abreviado por exit.

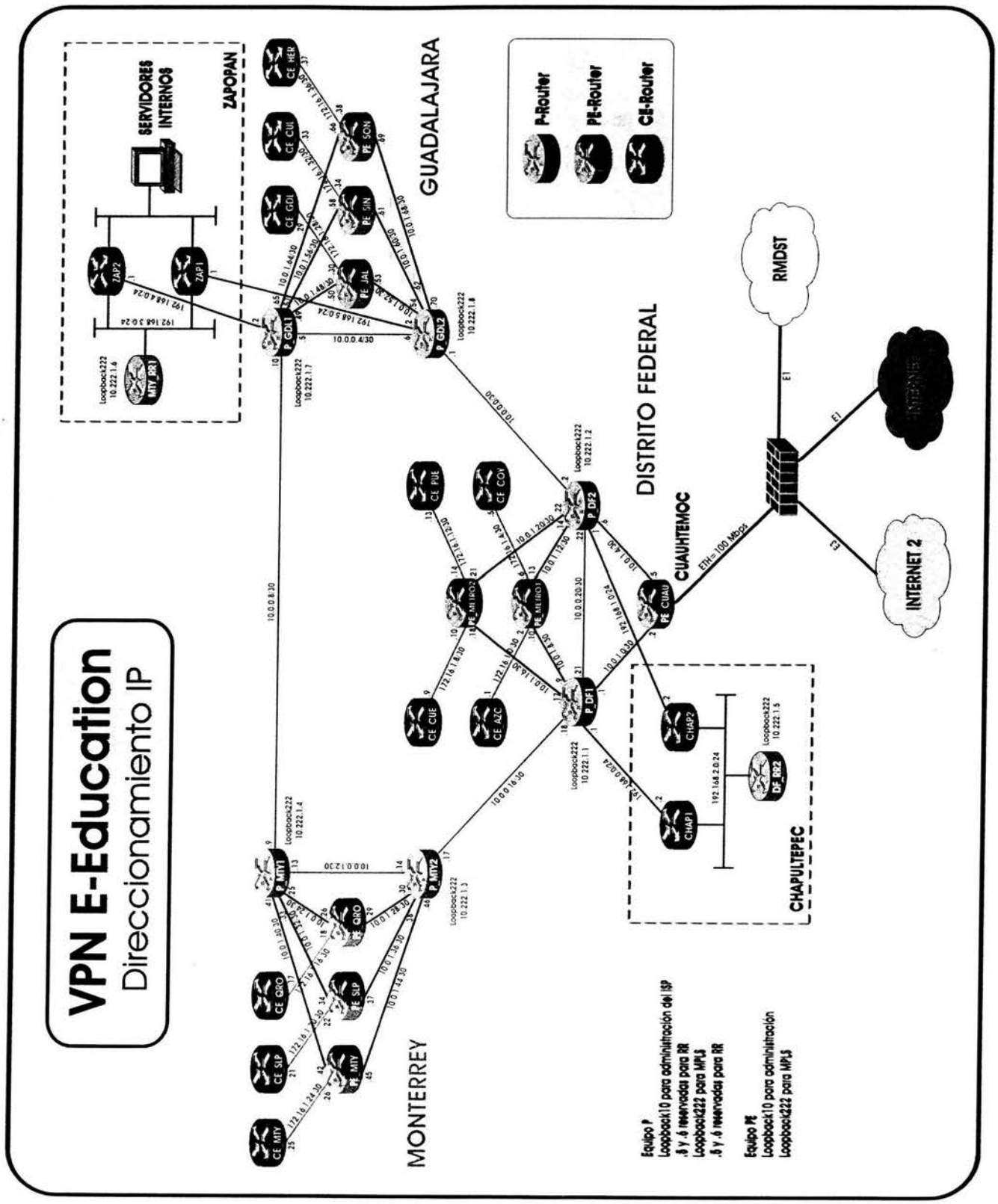
ip route vrf EEDUC 10.128.0.0 255.128.0.0 Serial5/0/0
Es usado para establecer rutas estáticas para una VRF. Se usa una ruta estática cuando el Software Cisco IOS no puede construir dinámicamente una ruta al destino.

ip route vrf EEDUC 10.193.0.0 255.255.254.0 Serial5/0/0
Es usado para establecer rutas estáticas para una VRF. Se usa una ruta estática cuando el Software Cisco IOS no puede construir dinámicamente una ruta al destino.

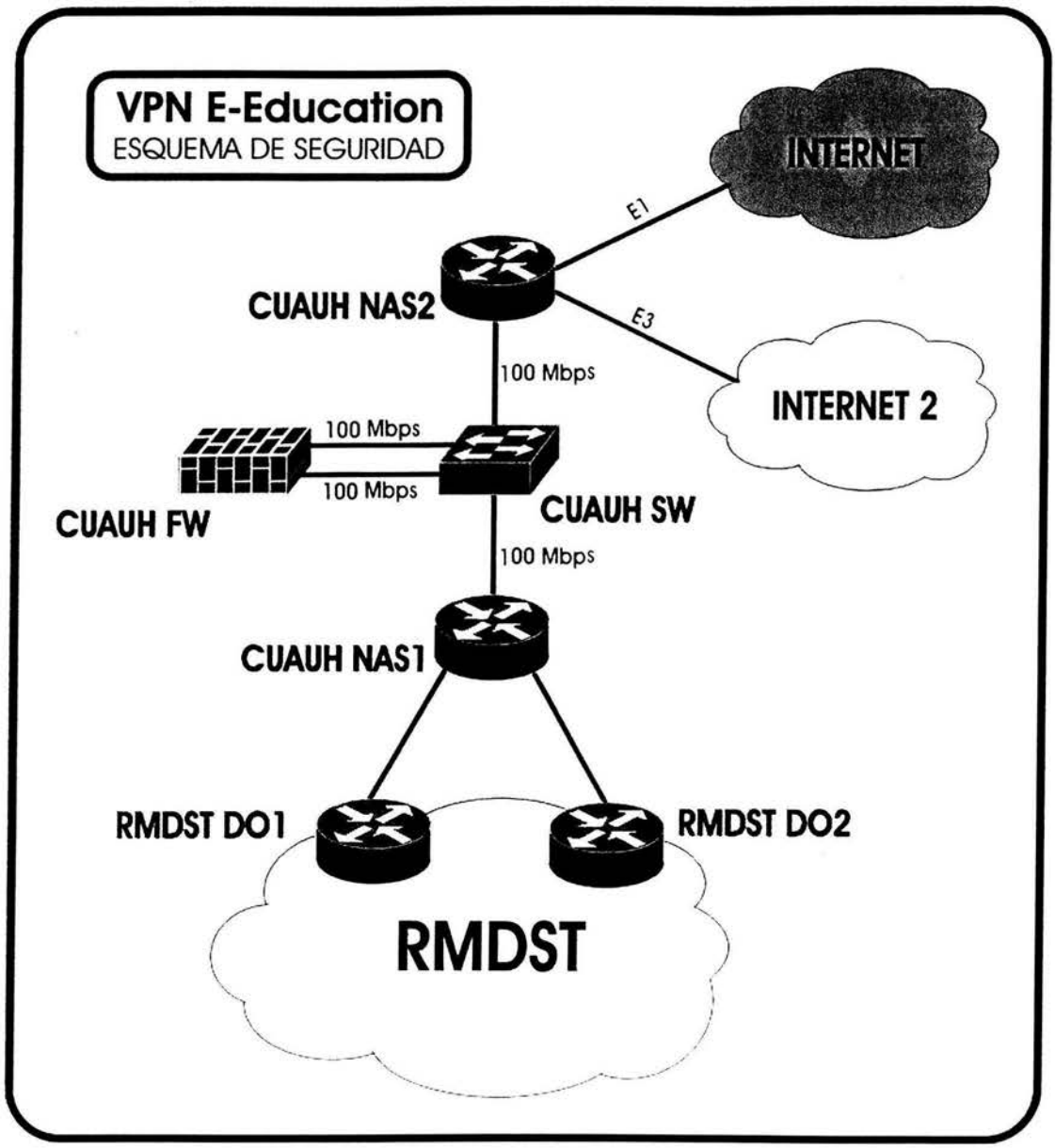
Apéndice B1. Mapa de la VPN E-Education



Apéndice B2. Direccionamiento VPN



Apéndice B3. Esquema de seguridad



Glosario de términos y acrónimos

A

ABR (Area Border Router). Es el enrutador que conecta al menos a dos áreas diferentes.

Ancho de Banda (Bandwidth). Cuando nos referimos a un sistema de comunicación digital, el ancho de banda es la cantidad de datos que pueden ser transmitidos en una cantidad de tiempo fija, a través de una red de comunicación.

AS (Autonomous System). Sistema Autónomo. Es un conjunto de enrutadores que comparten una misma administración y políticas de enrutamiento.

ATM (Asynchronous Transfer Mode). Modo de Transferencia Asíncrona. Estándar internacional para transmisión de celdas en el que múltiples tipos de servicios (voz, vídeo o datos) se transmiten en celdas de longitud fija. Estas permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retrasos de tránsito. ATM está diseñado para aprovechar los medios de transmisión de alta velocidad.

B

Backbone. Parte de una red (un segmento de alta velocidad o una serie de conexiones) que forma una ruta principal dentro de una red, para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.

BER (Bit Error Rate). Tasa de Bits de Error. Se refiere a la proporción de bits recibidos que contienen errores.

Broadcast. Es la difusión de paquetes a todos los nodos de una red. Estos paquetes se identifican mediante una dirección bien definida.

Buffer. Es un espacio de memoria para el almacenamiento temporal de datos.

Bugs. Son errores de escritura en los programas que producen fallas en los sistemas.

C

Caching. Es un proceso en el cual se accesa frecuentemente a datos dejados a la mano, en vez de estar buscándolos constantemente en el lugar donde están almacenados.

CAR (Committed Access Rate). Tasa de Acceso Comprometida. Empleada en el acondicionamiento del tráfico. El CAR realiza funciones tal como la de limitar la tasa de transmisión tanto en la entrada como en la salida de una interfase o subinterfase basándose en un conjunto de criterios flexibles.

CDP (Cisco Discovery Protocol). Protocolo de Descubrimiento de Cisco. Herramienta Cisco para caracterizar una red existente.

Cisco Express Forwarding (CEF). Es una tecnología de Capa 3, propietaria de Cisco Systems, para el envío de paquetes; optimiza el rendimiento y escalabilidad de una red con grandes y dinámicos patrones de tráfico, tales como aplicaciones basadas en Web o sesiones interactivas.

Classful. Sigue el esquema clásico de las Clases para direccionamiento IP, dichas clases son A, B, C, D y E.

Classless. Permite el uso de VLSM, con lo cual es posible evitar el uso estricto de las Clases para direccionamiento IP.

CLNP (Connectionless Network Protocol). Protocolo de Red No Orientado a Conexión. Protocolo de la Capa de Red OSI que no requiere un circuito para establecese antes de que se transmitan los datos.

Colisión. En Ethernet, es el resultado de dos nodos que transmiten simultáneamente. Las tramas de los dos dispositivos chocan y se dañan cuando se encuentran en los medios físicos.

Convergencia. Se refiere cuando la información en los enrutadores es consistente con la topología de la red.

CPE (Customer Premises Equipment). Dispositivo terminal que puede ser un bridge o un enrutador, con el cual el cliente se conecta a la red del Proveedor de Servicios. También es conocido como equipo CE (Customer Edge).

CRC (Cyclic Redundancy Check). Verificación por Redundancia Cíclica. Técnica de verificación de errores en la cual el receptor de la trama calcula un residuo dividiendo el contenido de la trama por un divisor binario primo y compara el residuo calculado en el valor almacenado en la trama por el nodo emisor.

CUDI (Corporación Universitaria para el Desarrollo de Internet). Es una Asociación Civil que tiene por objeto promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México.

D

DHCP (Dynamic Host Configuration Protocol). Protocolo de Configuración Dinámica de Anfitrión. Es un método estándar para asignar automáticamente direcciones IP a dispositivos en una red.

Dial-up. Conexión a una red por medio de un módem a través de la línea telefónica.

Dirección IP. Identificador de 32 bits asignada a dispositivos que usan TCP/IP. Corresponde a una de las cinco clases y se escribe en forma de 4 octetos separados por puntos. Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Se emplea para identificar una entidad única, como un proceso o dispositivo de red en particular.

Distancia Administrativa. Ésta especifica una preferencia sobre la forma en que una ruta fue aprendida. Tiene un significado trascendente local al enrutador y cada protocolo tendrá asignado un valor predeterminado.

DNS (Domain Name System). Sistema de Nombres de Dominios. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones, es decir traduce los nombres de los dominios en direcciones IP.

E

Edge-LSR. Es un enrutador que además de las funciones de un LSR tiene otras dos importantes funciones, la de imponer (push) y retirar (pop) etiquetas a los paquetes en los puntos de entrada y salida al dominio MPLS.

Enrutador (router). Es un dispositivo que determina el siguiente punto de la red a donde será enviada la información, debe de estar conectado al menos a dos redes y elegirá una ruta dependiendo de su visión particular de la red.

Enrutamiento. Se define como una serie de procesos que son llevados a cabo para transportar la información desde un origen a un destino, a través de redes interconectadas por enrutadores y otros dispositivos que funcionan como una sola red.

Equipos-P. El proveedor de servicio tiene usualmente equipo adicional en el core (centro) de la red, estos equipos son llamados Equipos-P., por ejemplo P-switches, P-routers.

Ethernet. Protocolo para redes LAN. Define las reglas a ser usadas para la transmisión y recepción de información.

F

Firewall. Sistema diseñado para prevenir el acceso no autorizado a/o desde una red privada, en general para intrusos desde el Internet.

Flooding. El término que se refiere a la acción que llevan a cabo los enrutadores para enviar los anuncios sobre el estado de los enlaces a todos sus vecinos.

Forwarding Equivalence Class (FEC). Es cuando los enrutadores agrupan diferentes flujos de información que tengan como destino a un mismo enrutador o una LAN y usan la

misma etiqueta para ellos. Los paquetes se enviarán de la misma manera y por la misma ruta.

Full-mesh. Topología de malla completa.

GRE (Generic Route Encapsulation). Encapsulamiento de Enrutamiento Genérico. Protocolo de tunneling desarrollado por Cisco que puede encapsular una gran variedad de tipos de paquetes de protocolos dentro de los túneles IP, creando un enlace de punto a punto virtual para los enrutadores Cisco en puntos remotos de una internetworking IP.

G

GTS (Generic Traffic Shaping). Mecanismo que proporciona un servicio de *buffer* a los paquetes, en vez de simplemente tirarlos en caso de congestión.

H

Hackers. Son intrusos que entran en los sistemas sin tener autorización. Son considerados piratas informáticos.

Hello Packets. Paquetes que transportan información para lograr la adyacencia entre enrutadores.

Hop-by-hop. Salto a salto es el comportamiento de un paquete que viaja a través de un número no determinado de puntos o nodos antes de arribar a su destino. En cada uno de ellos se toma la decisión de cual será el siguiente salto.

HTTP (Hyper Text Transfer Protocol). Protocolo de Transferencia de Hiper Texto. Protocolo que sirve para incursionar en los sitios de WWW en el Internet.

I

IETF (Internet Engineering Task Force). Fuerza de Tareas de Ingeniería de Internet. Fuerza de tareas compuesta por más de 80 grupos de trabajo responsables por el desarrollo de estándares de Internet.

IGRP (Interior Gateway Routing Protocol). Protocolo de Enrutamiento de Gateway Interior. Protocolo IGP propietario de Cisco para manejar los problemas relacionados con el enrutamiento de redes heterogéneas de gran envergadura.

Internet. Es una colección de redes autónomas interconectadas usando protocolos de Internet para entregar una variedad de servicios incluyendo Web, e-mail, vídeo, audio y datos.

Internetwork. Agrupamiento de redes interconectadas por enrutadores y otros dispositivos que funciona (en general) como una sola red.

IOS (Internetworking Operating System). Sistema operativo usado por Cisco Systems en sus equipos.

IP (Internet Protocol). Protocolo de Internet. Es un protocolo de la Capa de Red (Capa 3) que ofrece un servicio de internetwork no orientada a conexión. IP brinda funciones de direccionamiento, definición de enrutamiento y conexión de extremo a extremo.

Ipsec (IP Security). Seguridad IP. Protocolo de seguridad IP que facilita la construcción de redes privadas virtuales sobre Internet. Proporciona confidencialidad, autenticidad del remitente, integridad de los datos transmitidos y protección contra reenvíos no autorizados de datos.

ISO (Internacional Organization for Standardization). Organización Internacional para la Normalización. Es una organización que tiene a su cargo una amplia gama de estándares incluidos aquellos referidos al internetworking.

J

Jitter. Variación en el retraso.

K

Keepalive. Función de los protocolos de enrutamiento que sirve como referencia para determinar si un vecino está o no activo.

L

LAN (Local Area Network). Red de Área Local. Es una red de datos de corta distancia, formada por computadoras y dispositivos periféricos enlazados entre si y ubicados en un área relativamente limitada como puede ser entre edificios, entre campus o en un mismo piso. Este tipo de redes permite conexiones de alta velocidad entre dispositivos con tasas de transferencia de hasta 10 Gbps.

Latencia. Es el retraso entre el tiempo que un dispositivo solicita acceso a una red y el tiempo en que se le otorga el permiso para trasmitir. También se considera como el retraso entre el tiempo en que el dispositivo recibe una trama y el tiempo en que la trama se envía al puerto destino.

LDP (Label Distribution Protocol). Protocolo empleado para el intercambio de asociaciones de etiquetas para direcciones unicast cuyo propietario es la IETF.

LFIB (Label Forwarding Information Base). Es usada para el envío de paquetes y contiene sólo aquellas etiquetas en uso por el LSR que la contiene.

LIB (Label Information Base). Contiene todas las etiquetas asignadas por el LSR y los mapas de las etiquetas asignadas y recibidas de cualquier vecino.

LLQ (Low Latency Queuing). Mecanismo que ofrece un encolamiento prioritario estricto para tráfico sensible al retardo como VoIP a lo largo de la ruta de datos.

Loop. Es la trayectoria cerrada en donde queda atrapado un paquete, entre dos o más enrutadores en camino a su destino.

Loopback. Es una internase lógica que se configura en un enrutador que siempre está activa al contrario de una interfase física.

LSA (Link State Advertisement). Paquete broadcast utilizado por los protocolos estado de enlace que contiene información acerca de vecinos y costos de ruta.

LSD (Link State Database). Es una base de datos topológica.

LSP (Link State PDU). Es la unidad de datos empleada en IS-IS.

LSR (Label Switch Router). Es un enrutador que realiza el envío de paquetes basado en etiquetas.

M

MAC (Media Access Control). Control de Acceso al Medio. Parte más baja de la Capa de Enlace de Datos.

MD5 (Message Digest 5). Es un algoritmo utilizado para la autenticación de mensajes en SNMP. MD5 verifica la integridad de la comunicación, autentifica el origen y verifica la puntualidad.

Métricas. Son variables asignadas a las rutas que representarán una manera en que estas rutas son clasificadas por preferencia, entre menor sea el valor de la métrica, mejor será la ruta.

Modelo de Referencia OSI. Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales.

MPLS (Multi Protocol Label Switching). Es un protocolo mediante el cual se envían paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes de IP.

MTU (Maximum Transmission Unit). Unidad Máxima de Transmisión. Tamaño máximo de paquetes, en bytes, que puede manejar una interfase en particular.

Multicast. Se refiere a los envíos de paquetes o tramas únicos copiados por la red y enviados a un subconjunto específico de direcciones de red.

N

Next-hop. Otra forma en que se le conoce al enrutador.

O

OSI. (Open System Interconnection). Sistema de Interconexión Abierta.

Outsourcing. Es un sistema empleado por grandes empresas, las cuales rentan el servicio de otras empresas para efectuar proyectos pequeños en vez de ellas.

Overhead. Información adjunta a un aviso de la red para garantizar una transmisión sin errores al destino correcto.

P

PDU (Protocol Data Unit). Término OSI equivalente a paquete.

PE (Provider Edge). Es el equipo que se conecta al CE pero que pertenece al Proveedor de Servicio.

Peer. Es una vecindad o un grupo de vecinos. También conocido como pareja de dispositivos (por ejemplo de enrutadores).

Ping. Es usado como una herramienta de diagnóstico para determinar conectividad hasta la Capa 3 del Modelo de Referencia OSI, un ejemplo es determinar si un equipo está activo y donde puede ser contactado, también ayuda a determinar el tiempo de llegada de un aviso de un equipo a otro.

Política. Es una regla que gobierna la administración de recursos.

Protocolo. Es la descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.

Q

QoS (Quality of Service). Calidad de Servicio. Medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

R

RED (Random Early Detection). Mecanismo que supervisa la carga de tráfico en diferentes puntos de la red y descarta paquetes de forma estocástica si aumenta el nivel de congestión.

RFC (Request for Comments). Petición de Comentarios. Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. La mayoría de las RFCs documentan especificaciones de protocolos.

RIP (Routing Information Protocol). Protocolo de Información de Enrutamiento. IGP común de las redes de datos. RIP utiliza el número de saltos como métrica de enrutamiento. Desarrollado por la IETF. Actualmente se emplea la versión 2, RIPv2.

RPS (Repetitive Pattern Supression). Supresión de Patrones Repetitivos.

RSVP (Resource Reservation Protocol). Es un protocolo para lograr la señalización, es usado para hacer peticiones de QoS empleando Clases de Servicio.

S

SNA (System Network Architecture). Arquitectura de Redes de Sistema. Arquitectura de red grande, compleja, con gran cantidad de funciones. Similar en algunos aspectos al Modelo de Referencia OSI, pero con varias diferencias.

SNMP (Simple Network Management Protocol). Protocolo Simple de Administración de Redes. Es un protocolo de administración de red que se utiliza casi exclusivamente en redes TCP/IP. SNMP suministra un medio para supervisar y controlar los dispositivos de red (enrutadores, switches, hubs, etc.), y para administrar configuraciones, recoger estadísticas, el desempeño y la seguridad.

SP (Service Provider). Proveedor de Servicios. Es una organización que posee la infraestructura para proveer líneas dedicadas emuladas a sus clientes.

SPF (Shortest Path First). Algoritmo de enrutamiento que realiza iteraciones sobre las longitudes de las rutas para determinar el árbol de extensión de ruta más corta. A veces denominado algoritmo de Dijkstra.

Sumarización. Es una manera de tener una sola dirección IP que representa una colección de direcciones IP cuando se emplea un plan de direccionamiento jerárquico.

SVC (Switched Virtual Circuit). Circuito Virtual Conmutado. Circuito que se establece de forma dinámica a pedido y que se desconecta cuando la transmisión se completa.

T

Tabla de Enrutamiento. Es una lista de las rutas disponibles que puede alcanzar un enrutador, sus condiciones y la forma de llegar a ellas.

TCP (Transmission Control Protocol). Protocolo de Control de Transporte. Protocolo de la Capa de Transporte orientado a conexión que proporciona una transmisión confiable de datos full dúplex.

TDP (Tag Distribution Protocol). Protocolo de tipo orientado a conexión para distribuir las etiquetas usadas en Tag-Switching, cuyo propietario es Cisco.

Telnet. Programa que permite la conexión con otro ordenador a través del Internet o por línea telefónica.

Tiempo de convergencia. Es el tiempo que le toma al protocolo de enrutamiento llegar a la convergencia y dependerá de los algoritmos empleados para obtener los destinos.

Token passing. Es un protocolo que permite a una determinada terminal transmitir en una red. Esto lo logra mediante el empleo del *token*, el cual es una trama que contiene información de control. La posesión de éste permitirá al dispositivo de la red transmitir datos.

Topología. Es una disposición física de nodos de red y medios dentro de una estructura de redes.

ToS (Type of Service). Tipo de Servicio. Campo dentro de un datagrama IP que indica la forma en que se debe administrar el datagrama.

TTL (Time to Live). Campo del encabezado IP que indica cuantos saltos más en la red son permitidos antes de que el paquete sea desechado (descartado).

U

Unicast. Se refiere al envío de paquetes de datos a un sólo destino de red.

V

VAD (Voice Activity Detection). Detección de Actividad de Voz. Es una tecnología que reconoce cuando una persona habla y cuando permanece en silencio para suprimir el envío de ruido innecesario a través de la línea de comunicaciones.

Vecinos. Son enrutadores con un enlace de datos en común.

VLAN (Virtual Local Area Network). LAN Virtual. Grupo de dispositivos de una LAN que están configurados (usando software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, de hecho, están ubicados en una serie de segmentos de LAN distintos. Debido a que las VLANs están basadas en conexiones lógicas en lugar de físicas, son sumamente flexibles.

VLSM (Variable Length Subnet Mask). Máscara de Subred de Longitud Variable. Fue desarrollado para permitir múltiples niveles de direcciones IP dentro de una sola red, con ello se puede sortear el direccionamiento tradicional basado en clases.

VoIP (Voice over Internet Protocol). Protocolo de Voz en Internet. Transmisión digital de voz a través de Internet.

VPN (Virtual Private Network). Red Virtual Privada. Es un sistema de telecomunicaciones consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente los recursos de una red de acceso público, es una extensión de la red privada de una organización usando una red de carácter público.

VRF (VPN Routing and Forwarding Instance). Instancia de Envío y Enrutamiento de la VPN. Es la combinación entre la Tabla de Enrutamiento de la VPN y la Tabla de Enrutamiento asociada.

W

WAN (Wide Area Network). Red de Área Amplia. Es una red de comunicación de datos que enlaza usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicios comunes.

Web. Red de documentos HTML intercomunicados y distribuidos entre servidores del mundo.

WFQ (Weighted Fair Queuing). Es un algoritmo de encolamiento basado en el flujo que realiza dos tareas simultáneamente: sitúa el tráfico interactivo a principio de la cola para reducir el tiempo de respuesta y permite así compartir el resto del ancho de banda entre flujos que requieren gran ancho de banda.

Bibliografía

- **"Internetworking Technologies Handbook".**
  Chapter 45. Open System Interconnection Routing Protocol.
  Chapter 46. Open Shortest Path First.
  Chapter 48. Resource Reservation Protocol.
  Chapter 49. Quality of Service Networking.
  Cisco Systems, Inc.
  Cisco Press.

- **"Tecnologías de Interconectividad de Redes".**
  Merilee Ford.
  Prentice Hall.
  Cisco Systems, Inc.
  1998.

- **"Communications for Cooperating Systems OSI, SNA and TCP/IP".**
  R. J. Cypser.
  Addison-Wesley.
  1991.

- **"Redes de Computadoras. Protocolos, Normas e Interfases".**
  Uyless Black.
  Microbit.
  2ª Edición.
  1997.

- **"Academia de Networking de Cisco Systems: Guía del Primer Año".**
  Cisco Networking Academy Program.
  Cisco Systems, Inc.
  Cisco Press.
  2ª Edición.
  2003.

- **"Academia de Networking de Cisco Systems: Guía del Segundo Año".**
  Cisco Networking Academy Program.
  Cisco Systems, Inc.
  Cisco Press.
  2ª Edición.
  2003.

- **"Redes de Computadoras e Internet".**
  Álvaro Gómez Vieites, Manuel Veloso Espiñeira.
  Alfaomega.
  2003.

- **"Top-Down Network Design".**
  Priscilla Oppenheimer
  Cisco Systems, Inc.
  Cisco Press.

- **MPLS and VPN Architectures.**
  Ivan Pepelnjak, Jim Guichard.
  Cisco Systems, Inc.
  Cisco Press.

- **"Cisco IOS Quality of Service Solutions".**
  Configuration Guide.
  Release 12.3.
  Cisco Systems, Inc.

- **Data Sheet: "Cisco IOS Software: Quality of Service".**
  Cisco Systems, Inc.
  2000.

- **"Catalyst 2948G-L3 and Catalyst 4908G-L3 Software Feature and Configuration Guide".**
  Chapter 9 Configuring Quality of Service.
  Cisco IOS Release 12.0(7)W5(15d).
  Cisco Systems, Inc.

- **White Paper: "DiffServ: The Scalable End-to-End QoS Model".**
  Cisco Systems, Inc.
  2001.

- **"Implementing DiffServ for End-to-End Quality of Service".**
  Cisco IOS Release 12.1 (5) T.
  Cysco Systems, Inc.

- **"Committed Access Rate".**
  Cisco IOS Release 11.1 (17) C.
  Cisco Systems, Inc.

- **White Paper "Cisco IOS MPLS Quality of Service".**
  Cisco Systems, Inc.
  1992 – 2001.

- **"Low Latency Queuing".**
  Cisco IOS Release 12.0 (7) T.
  Cisco Systems, Inc.

- **"Class-Based Weighted Fair Queuing".**
  Cisco IOS Release 12.0 (5) T.
  Cisco Systems, Inc.

- **"Modular Quality of Service Command-Line Interface Overview".**
  Cisco IOS Quality of Service Solutions Configuration Guide.
  Cisco Systems, Inc.

- **"MPLS Quality of Service Enhancements".**
  Release 12.0 (14) ST.
  Cisco Systems, Inc.

- **"MPLS Quality of Service (QoS)".**
  Cisco IOS Release 12.0 (22) S.
  Cisco Systems, Inc.

- **White Paper: "MPLS – An Introduction to Multiprotocol Label Switching".**
  Nortel Networks.
  2001.

- **"MPLS Virtual Private Networks".**
  Cisco IOS Release 12.0 (5) T.
  Cisco Systems, Inc.

- **"Quality of Service Concepts".**
  Cisco IP Solution Center, 3.0: Quality of Service Management User Guide, 3.0.
  Cisco Systems, Inc.

- **"Quality of Service Configuration Overview".**
  Cisco 10000 Series Internet Router Quality of Service Configuration Guide.
  Cisco Systems, Inc.

- **Q&A: "Quality of Service for Multi-Protocol Label Switching Networks".**
  Cisco Systems, Inc.
  1992 – 2001.

- **"Traffic Shaping".**
  Catalyst 4224 Access Gateway Switch Software Configuration Guide.
  Cisco Systems, Inc.

- **"Policing and Shaping Overview".**
  Cisco IOS Quality of Service Solutions Configuration Guide.
  Cisco Systems, Inc.

- **"Dictionary of Internetworking Terms and Acronyms".**
  Cisco Systems, Inc.

- **Request for Comments (RFCs):**

RFC-791	RFC-1918
RFC-1247	RFC-2283
RFC-1518	RFC-3031
RFC-1771	RFC-3032

Los RFCs anteriores pueden ser consultados en las siguientes direcciones de Internet:

http://www.ietf.org/rfc.html
http://www.rfc-es.org/

Referencias en Internet:

http://www.cisco.com

http://qos.iespana.es/qos/

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl

http://www.juniper.net/solutions/literature/white_papers/200012.pdf

http://www.ifxnetworks.com/document/IFX_MPLSWhitePaper_sp.pdf

http://members.fortunecity.com/redesteleunam/

http://www.juniper.net/techpubs/software/junos/junos57/swconfig57-vpns/html/

http://www.nanog.org/mtg-0102/ppt/retana/

http://www.fi.upm.es/~jgarcia/Curso_MPLS/

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

http://www.argo.es/~jcea/artic/vpn1.htm