UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CRITERIOS PARA EL DISEÑO E IMPLEMENTACIÓN DE UNA RED IP-MPLS

T E S I S

PARA OBTENER EL TÍTULO DE:
INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N :

MARIANO AGUILAR ROGEL

CARLOS JESÚS ROJAS HERRERA

ERIK VEGA MAGAÑA

D I R E C T O R D E T E S I S

ING. PABLO CÉSAR DOMÍNGUEZ PÉREZ

C O D I R E C T O R D E T E S I S

ING. RODOLFO ARIAS VILLAVICENCIO

CIUDAD UNIVERSITARIA

AGOSTO 2004

A la Universidad Nacional Autónoma de México, por brindarnos la oportunidad de vivir la experiencia de ser orgullosamente universitarios.

A la Facultad de Ingeniería, por brindarnos la oportunidad de disfrutar plenamente nuestra formación profesional y la experiencia de ser ingenieros universitarios productivos para la sociedad.

Al Ing. Pablo, por abrirnos las puertas en su actividad profesional, por la grata vivencia que representó realizar este trabajo con él, por compartirnos su tiempo, conocimientos y experiencia.

Al Ing. Rodolfo, por introducirnos al mundo de las redes, ayudarnos al desarrollo de esta tesis y apoyarnos para su exitosa terminación.

Al Ing. Adalberto, por su interés en que comprendiéramos a fondo el tema desarrollado y su relación con la realidad, por su tiempo e invaluable ayuda.

A nuestros profesores, quienes con su paciencia, experiencia y dedicación nos infundieron un gran interés y cariño por nuestra profesión.

Mariano, Carlos y Erik

A Dios, por la oportunidad de vivir y conocer el mundo.

A mi familia, por hacerme sentir siempre apoyado y jalar siempre juntos "la carreta".

A mis Padres, por su apoyo, cariño y confianza incondicional, siempre contribuyendo en mis logros. Son una pieza importante en mi ser.

Pa, gracias por enseñarme a comprender esta vida con tu gran ejemplo, por tu cariño y amor. Por todo lo que me has dado, que es "todo" y con nada te lo podré pagar.

Viky, gracias por estar siempre para mi, por tu cariño y tenerme tanta paciencia, por cargarme 9 meses y darme la vida, no tengo palabras para agradecértelo.

Abue Mari, por todo ese amor que siempre me brindas, tus enseñanzas, formación, regaños, tus besos, tu apoyo, tu exquisita comida y simplemente por existir.

A mis hermanos, por convivir conmigo, todas las experiencias que hemos vivido y las que nos faltan.

Roy, por tu forma de ser, tu visión de la vida, por todo el tiempo juntos, por tu cariño. Solo puedo decir que te admiro y respeto.

Lalo, por todas las vivencias, apoyo, por ser tan cuate, por tu cariño y amor. Eres muy importante en mi vida.

A Zais, por todo tu amor, comprensión, ayuda, tiempo, dedicación, cariño y esa inspiración que provocas en mi para seguir adelante. Por llenar de alegria mi vida con esa hermosa sonrisa. ¡Eres mi musa!

A mis amigos Carlos y Erik, por su confianza y apoyo durante la carrera, por tantas cosas que pasamos juntos, tantas aulas, clases, exámenes, trabajos, risas y convivencia extraescolar. Por su incondicional ayuda y comprensión. ¡Son admirables!

A Angélica, Aurora, Lupita, Lupe Rogel, Pedro y sus familias, porque sé que siempre estarán ahí cuando las necesite.

A la Lic. Alicia Berthier, al Ing. Salvador Martinez y al Lic. Jorge Moya, por su apoyo incondicional y sus buenos consejos en mi vida estudiantil y deportiva.

A mis amigos de Pelvis, Edo, Joco, Oli, Fernando, Marco, Pooh, Horus, Joel, Cel, Hertz, Chewy, Samy, Cubicuate, Kot, Gib, José Méndez y todos lo que en este momento no recuerdo, por su amistad, apoyo, confianza y todas esas vivencias que han llenado mi vida y que me dan energía para lograr metas como ésta.

Mariano

A Eva, mi madre, por haber hecho posible que hoy escriba estas líneas, por su incondicional apoyo, inspirante ejemplo, constante aliento e inmenso cariño. Gracias mamá.

A Eva Luz, mi hermana, por su gran cariño, comprensión en los momentos más necesarios, apoyo constante, valioso consejo y sobre todo por ser mi hermanita preferida con la que siempre he contado.

A Carlos, mi abuelo, por su apoyo, ejemplo y guía al generar en mí el interés en el cómo y por qué de las cosas.

A Nayeli, por llenar mi vida con amor, comprensión y cariño, por su paciencia, apoyo y confianza, por impulsarme a ser mejor e inspirar mi vida; esperando con todo el corazón se cumplan nuestras metas y sueños.

A Eric y Mariano, mis compañeros de tesis y amigos, agradeciendo la amistad y confianza depositada en mi a lo largo de esta aventura académica, donde compartimos, más que un salón de clases, un fragmento de nuestra vida.

Carlos

A mi mamá, por el amor, apoyo y compresión que me has dado y por tu ejemplo de superación y de seguir siempre adelante. Doy gracias por tener una mamá como tú. Te quiero mucho ma!

A mi papá, por tu amor, dedicación, esfuerzo y apoyo incondicional en todos lo proyectos que he emprendido, gracias papá.

A mi hermana Adriana, por el cariño y respaldo que me brindaste, por ser lo que eres para mi, mi hermanita consentida a la que tanto quiero.

A mi Madrina, por su apoyo, que siempre ha sido incondicional.

A mi Abuelita, por darme un ejemplo de amor a la vida, y por los momentos divertidos que hemos tenido.

A Mayra, porque siempre me acompaño durante estos años de estudio brindándome su cariño y amistad.

A mis amigos Carlos y Mariano, porque durante la carrera me entregaron su amistad y por su confianza, con quienes compartí experiencias buenas y malas. ¡Gracias!

Erik

CONTENIDO TEMÁTICO

INDICE

OBJETIVO

El objetivo de este trabajo de tesis es mostrar los criterios para la implementación de una red IP con la funcionalidad MPLS, entendiendo como criterios una serie de directrices o secuencias sugeridas para la realización de dicha tarea.

Deseamos poder ofrecer una referencia integral sobre criterios a considerar en la implementación de una red IP-MPLS construida desde el inicio por nosotros.

En el desarrollo del trabajo, propondremos el tipo de red que se desea obtener, las especificaciones para soportar aplicaciones y servicios específicos (VPN's, Voz, Calidad de Servicio, Trafico de datos, Video, Internet) orientándonos al reto de transportar, mas no manipular el tráfico de las aplicaciones del usuario.

El objetivo específico del trabajo es:

Generar una red IP / MPLS escalable, confiable y tolerante a fallas; que asegure la fácil implementación de la tecnología MPLS

Ubicaremos la tesis en el universo de tecnologías WAN de telecomunicaciones. Nuestra propuesta se basa en una recopilación de conceptos teóricos de tecnologías para su aplicación práctica en el diseño e implementación de una red. Su punto de vista se centrará en proponer los elementos de la misma basándonos en consideraciones técnicas que se desarrollan en el transcurso del trabajo, las cuales apoyaremos basados en nuestro criterio y comparación con otras tecnologías.

Se incluirán pasos, recomendaciones, sugerencias, unificación de criterios y metas de implementación de la red, considerando las soluciones tecnológicas actuales y justificando las diferencias y similitudes con estas; dejando de lado las configuraciones o equipos específicos, algoritmos para la optimización de la red y procesos de control de retardo y congestión.

Explicaremos el método de diseño considerando los servicios que ofreceremos, la interconexión de equipos, el esquema de tránsito de datos entre ellos y el funcionamiento básico de algunos protocolos de enrutamiento, las directivas de diseño para la obtención de una red WAN escalable, confiable y

tolerante a fallas que asegure la fácil implementación de la tecnología MPLS, el plan de implementación de la red propuesta y sugerir los puntos a documentar de la misma.

JUSTIFICACIÓN

Se ha propuesto dentro del campo de redes de datos la reducción en el procesamiento de la información para hacer más eficiente el transporte de la información, esto no es nuevo, pero en lo que se había trabajado era en utilizar otro tipo de tecnologías para solucionar este problema, lo cual encarece el servicio.

Aún no existe información o una referencia integral (solo segmentada), que nos diga cuáles son los criterios necesarios para la implementación de una red MPLS. La justificación del desarrollo de esta tesis es la intención de contar con un documento que abarque los aspectos técnicos y prácticos para la implementación de la tecnología MPLS en una red IP.

Actualmente el poder tener transporte de datos de un punto a otro (entre usuarios), desde el enfoque del Proveedor de Servicio, se ha tornado caro e ineficiente. Esto se debe a la falta de un buen diseño de red ocasionado por deficiencias en: Anchos de Banda requeridos, optimización de la conmutación de la información, suficiencia de infraestructura necesaria para ofrecer los tipos de servicios y cobertura del servicio.

Por esta razón las empresas lo que buscan en un Proveedor de Servicio es que cumpla con características como disponibilidad del servicio, jerarquía de tránsito y seguridad de la información.

Otro aspecto a considerar es el uso óptimo de los enlaces, ya que en la mayoría de los casos el usuario no siempre ocupa la totalidad de la capacidad del servicio contratado, significando un desperdicio de recursos y gasto innecesario. Es por ello que se están buscando nuevas formas de reducir los costos compartiendo el enlace por varios usuarios (empresas).

Es importante para el correcto desempeño de la red proyectada tomar en cuenta diversos aspectos como son: protocolos de enrutamiento, tecnologías WAN, administración de la red, robustez de la red (escalabilidad, jerarquía de la información, seguridad, disponibilidad, etc.), entre otros.

Existe la necesidad de crear una red que ofrezca servicios altamente demandantes de recursos de la red a bajo costo, para que sea accesible desde particulares, pequeños negocios hasta grandes corporativos.

Podemos mencionar que actualmente la mayor parte de las redes están soportadas bajo el protocolo IP, siendo este compatible con redes MPLS. Este tipo de red se encuentra en expansión debido a los bajos costos de implementación y administración de la misma, así como las ventajas ofrecidas por MPLS.

La relevancia de la implementación de MPLS en la red, es tener la capacidad de proporcionar redes multiservicio, en las cuales se pueda soportar cualquier aplicación de forma eficiente, asegurando al usuario que su información será transportada exitosamente proporcionándole Calidad de Servicio y alta disponibilidad, mientras que el Proveedor de Servicio tendrá la posibilidad de implementar herramientas como Ingeniería de Trafico y una eficiente administración de la red.

REQUISITOS DE LA RED (CONSIDERACIONES INICIALES)

En este capítulo trataremos las consideraciones iniciales de servicios y parámetros a ofrecer por una red IP convencional considerando, clasificando y organizando los servicios que comúnmente son requeridos de ésta y entendiendo las necesidades que requieren solución para posteriormente contar con una base de requerimientos sólida de la cual poder partir al crear una red que cumpla con todos los requisitos planteados en el propio capítulo. Los puntos presentados se analizan desde la óptica del Proveedor de Servicios ya que será el encargado de proponer y asegurar un nivel de servicio en el tránsito de la información al usuario que convenga a ambas partes.

I.1 CONDICIONES DE SERVICIO

Se presentan aspectos fundamentales en el proceso de diseño de la arquitectura de una red WAN, y se comprenden en subcapítulos enfocados a conjuntos de consideraciones divididos como sigue:

Consideraremos las necesidades en la red, ya que en ellas se basa el desarrollo y las posibilidades de implementación de procesos de diseño posteriores, así, los requerimientos de la red se retoman como un proceso sistemático (también conocido como mejores prácticas en el diseño de red), el cual ayudará a obtener los resultados esperados en el diseño final de la red del Proveedor de Servicios, considerando las tecnologías y pasos de diseño tratados en capítulos posteriores, y en especial MPLS (razón de esta tesis) son implementados y administrados por éste.

Posteriormente nos enfocaremos a las necesidades de tráfico que serán resueltas al cliente con los criterios implementados por el operador, en esta parte también consideraremos el impacto técnico y de negocios que se obtendrá en el servicio ofrecido al cliente.

I.1.1 PROVEEDOR DE SERVICIO

El primer paso es **identificar el negocio de la red como Proveedor y las metas técnicas de la misma**, ya que cuando se diseña una red para soportar el tráfico de un

cliente se deben identificar los problemas potenciales, como resolverlos y cuales son las metas para este proyecto de diseño de red.

Es fundamental encontrar las metas técnicas y de negocios que tendrá la red, por ejemplo, qué clase de aplicaciones transitarán por la red, los requerimientos de negocios que lo ocasionan y la disponibilidad que es requerida para soportar a los usuarios que utilizarán la red.

Definir con precisión las metas que se tienen como Proveedor al comenzar a diseñar la red es esencial antes de emprender el trabajo de diseño como tal, dado que son críticas para un final de proyecto satisfactorio, considerando las necesidades de los usuarios a los que se brindará el servicio de la red en proceso de diseño. Esto es benéfico para fases posteriores de diseño, ya que si desde el inicio se comprende la orientación que se le quiere dar a la red de manera adecuada, pensando qué metas y clientes son buscadas por el Proveedor de Servicio, se asegura que los usuarios quedarán conformes con el servicio proporcionado y no se tendrá ningún problema en conseguir clientes y cubrir sus necesidades.

Negocios

Los aspectos de negocios que un Proveedor pretende lograr se centran en satisfacer las necesidades del mercado, proponiendo soluciones que sean técnicamente sustentables en relación al costo al que se ofrecerán al cliente y a la utilidad que se recuperará considerando la inversión y la utilización de la infraestructura necesaria. Algunos de estos aspectos pueden sintetizarse en:

- Incrementar el rédito y beneficio de la compañía operadora de la red.
- Reducir los costos en telecomunicaciones y mantenimiento.
- Mejorar la seguridad, sensitividad y propiedad de los datos que transitan.
- Proveer el mejor servicio de soporte técnico al consumidor.
- Hacer fácil de seguir el acceso a los datos a todos los clientes, considerando una amplia cobertura geográfica.
- Ofrecer interconectividad entre diferentes redes y clientes.
- Hacer la red operativa, rentable, confiable y con un buen desempeño.
- Ofrecer una amplia Cartera de Servicios.
- Reducir costo hacia el cliente.

Técnicos

Dependiendo de las metas que Proveedor en la fase de diseño haya propuesto para la red, deberán seleccionarse las tecnologías para la misma.

Es recomendable que las metas técnicas y requerimientos sean especificados tan claramente como sea posible desde la primera etapa del diseño WAN. Por lo anterior, como sucede con las decisiones fundamentales, el apresurarse en el desarrollo del diseño de la red es poco recomendable; es más redituable pensar y entender lo que se desea lograr técnicamente y planear la red para lograrlo.

Este trabajo dará frutos cuando se comience el diseño lógico y físico. Las metas técnicas mas típicas incluyen:

Escalabilidad

Es la habilidad de la red WAN de continuar funcionando bien aun cuando ésta cambie de tamaño o capacidad para soportar los requerimientos de tráfico o aplicaciones circulantes por la red del Proveedor. Debe considerarse que típicamente el redimensionamiento es a un gran tamaño y capacidad.

El ambiente de negocios de los clientes hoy en día es dinámico y cambia rápidamente, y existe la necesidad de agregar capacidad rápidamente, soportar nuevas aplicaciones y conectarse con puntos remotos para ofrecer completa interconectividad rápida y confiable. Dicho lo anterior, la escalabilidad es siempre la mayor preocupación y la meta primaria para el diseño de la red de una empresa Proveedora de Servicios WAN.

Se encuentra relacionada en cierta forma con el rendimiento y no constituye un problema si la red está bien diseñada y cuenta con esquemas razonables y coherentes; no obstante, sin la realización de la prueba de carga del sistema en un escenario real, no se puede afirmar que un determinado sistema es o no lo suficientemente escalable.

La escalabilidad nunca termina; el diseño debe reflejar e integrar que en cada modificación y decisión de implementación se piensa en el proceso entero. En el aspecto de previsión de ventas, es indispensable pensar cuánto los clientes crecerán y cuántos más se agregarán a corto (próximos 12 meses), mediano (próximos 24 meses) y largo plazo (más de 24 meses); los puntos importantes son:

- Tráfico: Cuánto tráfico se espera agregar a la red en corto y mediano plazo.

- Enrutadores: Cuántos enrutadores más serán agregados en la red en corto y mediano plazo.
- Aplicaciones: Cuántas y cuáles aplicaciones para red nuevas serán introducidas.
- Ancho de banda: Cuánto Ancho de Banda será necesario para soportar las nuevas aplicaciones y tráfico.
- Enlaces y conectividad: Cuantos enlaces físicos serán agregados en la red para obtener la conectividad requerida en corto y mediano plazo.
- Conexión con otros ISPs: Cuantos proveedores serán conectados a la red en mediano y largo plazo.

Disponibilidad

Es la segunda meta técnica más importante para el Proveedor, ya que se requiere por regla general de una gran disponibilidad de la red WAN. Esto hace referencia a la cantidad de tiempo que la red es utilizable por los usuarios que han contratado los servicios de la red.

Puede expresarse como un porcentaje de tiempo por año, mes, semana, día, etc., comparado con el total del tiempo para el periodo seleccionado. A diferencia de la escalabilidad, la disponibilidad puede ser definida numéricamente, haciendo mucho más fácil la evaluación si el diseño y servicio ofrecido por una red es satisfactorio o no. Dependiendo de la esencia del negocio, o variedad de éstos por parte de los clientes, el requerimiento de la disponibilidad varía grandemente.

Es muy importante proponer una disponibilidad razonable y realista, dado que se relacionara directamente con el costo solicitado por proporcionar el servicio. Deben tomarse en cuenta:

- La naturaleza de negocios a la que se enfocará la red.
- La utilización real de la red.
- Clases de usuarios que cuentan con la red de manera indispensable (políticas de contratación).
- Consecuencias políticas y de negocios si la red se viene abajo.
- Cuánto dinero perderá la compañía por hora en que la red este abajo.

• Si se tiene suficiente capacidad para soportar todos los circuitos WAN redundantes y el equipo necesario.

Tráfico

El tráfico mide cuanto Ancho de Banda es usado durante un periodo de tiempo específico por los clientes del operador, así como la posibilidad de soportar las peticiones de tráfico por parte de los clientes (previstas desde el momento del ofrecimiento de venta del servicio). Para circuitos WAN en el punto de utilización óptima de la red no es recomendable considerar agregar más capacidad si el ancho de banda utilizado del segmento de la red es menor al 70 u 80% de la capacidad total en función de los niveles de servicio ofrecidos.

Es probable que éste sea el aspecto en el que debe tenerse mayor consideración, dado que el funcionamiento de la red se considerará como satisfactorio si la cantidad de tráfico para la que fue planeada puede transitar sin problemas por ella; dicha estimación debe realizarse antes de proponer cualquier solución de diseño para la red del Proveedor de Servicio. En cuanto a las aplicaciones que transitarán por la red, deberán evaluarse aquellas que saturen los enlaces y decidir la forma en que se tratará con ellas. Es recomendable evaluar el peor caso, es decir, cuando la capacidad de tráfico de la red pudiera ser rebasada por las peticiones de los usuarios.

Transmisión libre de errores

Es la cantidad de datos libres de errores transmitidos por unidad de tiempo. Es importante no confundirlo con capacidad, que es una constante y determinada por tecnologías de capa física, mientras que la transmisión libre de errores es una variable determinada por diversos factores como el método de acceso de los paquetes, carga de la red y tasa de errores. La forma mas popular de medir la transmisión libre de errores es en Paquetes por Segundo (PPS). Dicha cifra está en estrecha relación con el tamaño del *frame* utilizado por la tecnología de capa 2 del MROSI. Éste es uno de los parámetros más representativos de la calidad de servicio que se proporciona al cliente, pese a no ser de evidente observación.

Retardo

También conocido como Latencia, es otro parámetro que mide el funcionamiento de la red, especialmente para aplicaciones interactivas con el usuario, como Videoconferencia o Voz sobre IP. En estos casos, los usuarios podrán percibir muy

fácilmente el Retardo en la red y en consecuencia quejarse acerca del funcionamiento de la misma. El Retardo es causado por muchas razones y algunos simplemente no pueden evitarse.

Para determinar una meta realista para cuanto Retardo es tolerable en el ambiente del cliente, se tiene que investigar y entender completamente que aplicaciones están corriendo en la red y que clase de requerimientos de Retardo existen para cada aplicación.

Obviamente una forma de resolver el problema de Retardo es agregar más Ancho de Banda en la red. Sin embargo el presupuesto es una gran preocupación, por lo que tecnologías como prioridad en la petición, estrategias de encolamiento (*priority queuing*), compresión y manejo de tráfico (*traffic shaping*) ayudan grandemente al mejoramiento del comportamiento de la red.

El Proveedor es quien debe establecer el Retardo máximo que presentará la red y cuánto puede ofrecer al cliente. Es difícil ajustarse totalmente a las aplicaciones de los clientes. Actualmente en México se ofrece un retardo en red máximo de 150 [ms] y es escalado de acuerdo a la topología de la red.

Seguridad

Entre todas las metas técnicas la Seguridad ha incrementado en importancia dado que los clientes mantienen conectadas sus redes internas privadas al Internet. Sin embargo, la Seguridad concerniente deberá ser cuidadosamente integrada en cada paso del diseño y planeación de la red. El Proveedor debe asegurarse de poder cumplir con las Políticas de Seguridad del cliente. Deben hacerse tantos cuestionamientos como sea posible para entender los riesgos asociados con la implementación de una red no segura, y determinar cuán sensible es la información. Deben estimarse las consecuencias si alguien penetra en la red y extrae datos, tanto para los clientes a los que se les brinda el servicio, como a la red misma del Proveedor, observando siempre las posibles fuentes de ataques (intencionales o no), las cuales podrán ser externas o de los mismos usuarios de la red.

Desempeño

El requerimiento para esto puede ser desde un pobre compromiso con el cliente, hasta una alta exigencia en los parámetros que se han contratado por parte de los usuarios, normalmente dependiente del tipo de servicio contratado por el usuario (en

caso que estén disponibles distintos tipos en el ofrecimiento del Proveedor); además habrá que tomar en cuenta las recomendaciones y obligaciones emitidas por los organismos reguladores de esta clase de servicios, así como los estándares que internacionalmente se esperará que cumpla cualquier Proveedor de Servicios.

En general, debe definirse especificándose en términos precisos y técnicos utilizando parámetros de red como tráfico, velocidad, utilización, seguridad y retardo, los cuales indican la salud de una red de un operador. Existen herramientas de administración disponibles para recolectar y analizar esta información.

1.2.1 EL CLIENTE

Debemos identificar el **tipo de negocio** de los clientes de la red para considerar los requerimientos de red que necesitarán en función de las aplicaciones que utilicen mayoritariamente, así como sus **metas técnicas**, que serán impactadas por la calidad del servicio que la red les brinde, ya que cuando se solicita el servicio de red por un cliente, éste tiene en mente problemas potenciales, requerimientos y metas a ser resueltas por un servicio de red a ser proporcionado.

Es recomendable entender al cliente y encontrar sus metas técnicas y de negocios, con el fin de poder cumplir con el servicio contratado y seguir ofreciendo diferentes alternativas de planes de servicio para las necesidades cambiantes del cliente.

Definir con precisión las metas de los servicios a ofrecer al cliente es esencial antes de comenzar el trabajo de diseño de la red del Proveedor, dado que son críticas para un final satisfactorio del proyecto.

Negocios

En la mayoría de los casos la elección de un servicio de red se hace en conjunto con definir las estructuras corporativas de la empresa. Es aconsejable entender cómo la compañía del cliente esta estructurada en departamentos, líneas de negocios, compañías y oficinas remotas. Esto ayuda a localizar e identificar todas las comunidades más grandes de usuarios, a caracterizar el tráfico que fluirá en la red e identificar el mercado de usuarios más significativo.

En la etapa temprana de diseño de red del operador, comúnmente se pierde mucho tiempo desarrollando especificaciones técnicas perdiendo de vista la importancia de

entender las metas de negocios del cliente, el cual finalmente será el consumidor del servicio.

Algunas de las metas de negocios típicas requeridas por el cliente son:

- Incrementar el rédito y beneficio de la compañía.
- Incrementar la productividad de los empleados y mejorar la comunicación corporativa.
- Reducir los costos en telecomunicaciones y redes.
- Contar con acceso en cualquier sitio.
- Hacer la red propia operativa y rentable.
- Contar con soporte técnico y pronta resolución de fallas por parte del Proveedor.

Técnico

Una vez entendidas bien las metas de negocio que el cliente espera solucionar con la contratación del servicio de red, se podrá encarar el reto de proponer esquemas de servicio al cliente para solucionar sus metas técnicas. Es recomendable que las metas técnicas y requerimientos sean especificados tan claramente como sea posible desde la primera etapa del diseño WAN.

Las metas técnicas buscadas por los clientes mas típicas incluyen:

Costo

Este es uno de los puntos que ofrecen más limitaciones en la propuesta de cualquier servicio de red, dado que tanto el cliente al contratar el servicio tiene límite de presupuesto, sin embargo, el ánimo de cualquier diseño es encontrar el punto óptimo en el cual puedan convivir los intereses de ambas partes sin sacrificar la satisfacción de sus necesidades.

Cobertura

Hace referencia al alcance que tendrá la red, es decir, hasta donde podrá contarse con el servicio con la calidad acordada en el contrato del enlace de red; desafortunadamente desde el punto de vista económico el nivel de cobertura está relacionado directamente con el costo del arrendamiento del servicio WAN. El cliente busca la mayor cobertura disponible, asegurando que su interconexión de equipos quedará respaldada.

Escalabilidad

Es la facilidad que tendrá la red del cliente de cambiar de tamaño o volumen perteneciendo al mismo servicio del operador, con el fin de soportar el aumento en los requerimientos de tráfico o aplicaciones de la empresa cliente, por lo anterior, el que el Proveedor ofrezca escalabilidad sencilla es siempre la mayor preocupación y la meta primaria para la contratación del servicio de red de una empresa. Es recomendable se monitoreen las expectativas de crecimiento del cliente para que el Proveedor sugiera la mejor opción de enlace para poder cumplir con lo prometido al cliente al momento de la contratación; los puntos importantes son:

- Usuarios: Cuántos usuarios nuevos se espera agregar en la red de trabajo de la compañía en corto y mediano plazo.
- Servidores: Cuantos servidores más serán agregados en corto y mediano plazo.
- Aplicaciones: Cuántas y cuáles aplicaciones para red nuevas serán introducidas.
- Ancho de Banda: Cuánto Ancho de Banda será necesario para soportar esas nuevas aplicaciones y usuarios.
- Sitios: Cuantos sitios serán agregados en la red en corto y mediano plazo.
- Compañías externas: Cuantas compañías externas serán unidas a la red en corto y mediano plazo.

Disponibilidad

Es un aspecto básico buscado por los clientes, ya que representa el aprovechamiento real que podrá hacer del servicio de red contratado. Adicionalmente, al ser un parámetro mensurable, es mayor el compromiso del Proveedor, así como la capacidad de comparación del cliente entre ofrecimientos de distintos Proveedores de Servicio. Dependiendo de la esencia del negocio del cliente, el requerimiento de la disponibilidad varía grandemente. Comúnmente, la petición de disponibilidad por parte del usuario será la mayor posible. Las variables que influyen la Disponibilidad requerida por el cliente son principalmente:

- Contar con una respuesta rápida por parte del Proveedor en caso de fallas.
- Las consecuencias políticas y de negocios si la red se viene abajo.

- La cantidad de dinero que perderá la compañía por hora en que la red este abajo.
- Si se tiene suficiente presupuesto para pagar todos los circuitos WAN redundantes necesarios (solución más simple, pero más cara).

Tráfico

Es la cantidad de información que el usuario espera transitar por la red del Proveedor, por lo tanto, es la capacidad del servicio de red que contrata. El servicio debe ofrecer la flexibilidad necesaria para que el usuario pueda agregar Ancho de Banda cuando sus necesidades de tráfico aumenten, sin afectar la red del Proveedor.

Transmisión libre de errores

Este punto no es evidente para el usuario, ya que la mayoría de las aplicaciones que transitan información por la red se aseguran de obtener la información completa y libre de errores, además de considerar que la aplicación puede ser sensible a las pérdidas, como datos críticos o enlaces de Voz o Video. Este parámetro es de suma importancia para evaluar la calidad del servicio proporcionado por el Proveedor y las deficiencias en este parámetro a ser soportadas dependerán del negocio del cliente.

Retardo

Similar al parámetro anterior, es difícilmente detectado por el usuario, sin embargo, un incremento en Retardo se observará evidentemente en aplicaciones interactivas con el usuario, como Videoconferencia o Voz sobre IP. Es un parámetro importante en las aplicaciones sensibles al retardo en la red, y aunque el retardo es causado por muchas razones y algunos retardos simplemente no pueden ser prevenidos, debe hacerse un esfuerzo por satisfacer las necesidades más comunes que las aplicaciones de los usuarios requieran.

Obviamente, una forma de resolver el problema de retardo es que el usuario contrate un enlace con un mayor Ancho de Banda, sin embargo, ésta no siempre es una opción viable para el cliente, por lo que el Proveedor podrá ofrecer alguna alternativa para optimizar el uso de su Ancho de Banda contratado.

Seguridad

Dado que las empresas necesitan conectar sus redes internas privadas al Internet, así como facilitar la información a sus trabajadores remotos, la seguridad concerniente deberá ser cuidadosamente integrada en cada paso del diseño y

planeación de la red. El cliente busca un servicio de red que solucione su pensamiento corporativo de políticas de seguridad. En función del servicio de red contratado, deben entenderse los riesgos asociados con la implementación de una red no segura; determinar cuán sensible es la información y dónde será guardada; cuáles son las consecuencias si alguien penetra en la red y extrae esos datos, etc.

Desempeño

El punto de partida de desempeño puede ir desde una vaga definición dada por las necesidades del servicio proporcionado por la empresa hasta específicamente técnicas, como la enumeración de parámetros de la red como tráfico o velocidad. En general el cliente deberá considerar si el servicio de red satisface sus necesidades de transporte de datos. En general este parámetro puede definirse especificando en términos precisos y técnicos utilizando medidas como seguridad, utilización, tráfico y retardo, los cuales indican la salud del servicio de red proporcionado a una empresa.

1.2 SERVICIOS A OFRECER POR LA RED

Como parte esencial de la propuesta de una red, deben ser determinadas y seleccionadas las capacidades y requerimientos de la misma, así como las capacidades específicas de los servicios que serán ofrecidos a los usuarios de ésta.

A continuación se sugieren capacidades que deseablemente deberán existir en la red, así como los compromisos del Proveedor con el cliente en función del tipo de servicio contratado.

En general, entregar el Ancho de Banda necesario a las aplicaciones WAN es una tarea difícil por las limitaciones de capacidad de los enlaces, por lo que el implementar aplicaciones multimedia a través de una red WAN es un reto. Una opción al necesitar Ancho de Banda adicional es revisar las tecnologías de conmutación de circuitos disponibles.

Una manera de mejorar la utilización de enlaces es agendar su uso apropiadamente, como en el caso de aplicaciones bajo demanda (como Videoconferencia), que típicamente consumen Ancho de Banda WAN durante las horas hábiles, pero otras aplicaciones (como aplicaciones de servidores de video) pueden ser agendados para que consuman el Ancho de Banda en horas no hábiles.

1.2.1 QoS –QUALITY OF SERVICE- (CALIDAD DE SERVICIO)

Definición

QoS es definida como la medida del desempeño de un sistema de transmisión que refleja la calidad de transmisión y disponibilidad de servicio. La disponibilidad de servicio es un elemento crucial en que se fundamenta la QoS.

Es la tecnología clave que posibilita la convergencia en la red de Voz, Video y Datos, y es necesaria por que estas aplicaciones tienen estrictos requerimientos de servicio de infraestructura de red, los cuales superan los requerimientos de tráfico de datos genérico, ya que si no cuentan con prioridad en el servicio por parte de los

dispositivos de la red, entonces la calidad de estas importantes aplicaciones podría rápidamente degradarse hasta el punto de no poder utilizarse.

Proceso de Administración

Implementar una solución de QoS no es una tarea definida en un solo momento, e implementada con la aplicación de una política. Una aplicación satisfactoria de QoS es seguida por monitoreo de los niveles de servicio y ajustes periódicos y puesta a punto de las políticas de QoS, como se muestra en la figura.

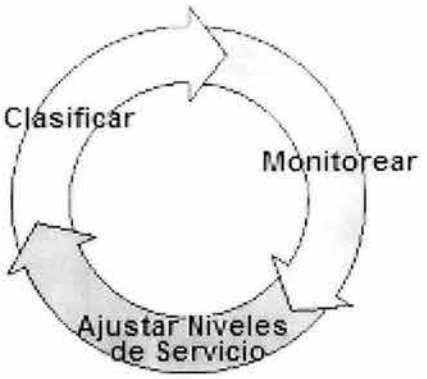


Figura 1.2.1- Ciclo Administrativo de QoS

El monitorear y adaptar las políticas de QoS a los cambios de negocios eficientemente se realiza a través de la administración de las soluciones de QoS.

El monitoreo en corto plazo es útil para verificar que las políticas de QoS aplicadas están teniendo el efecto deseado, mientras que el monitoreo a largo plazo, o tendencia, es necesario para determinar si el Ancho de Banda provisto es aún adecuado para las necesidades cambiantes.

Por ejemplo, al actualizar una aplicación se puede causar que el Ancho de Banda provisto sea excedido, o bien los objetivos de negocios pueden cambiar periódicamente generando necesidad de revisión de las prioridades generales.

Parámetros

Antes de implementar cualquier QoS satisfactoriamente, la infraestructura de la red debe estar diseñada para ser altamente disponible.

Debemos considerar que las aplicaciones de datos y multimedia tienen diferentes requerimientos de servicios. A diferencia de los servicios tradicionales como File Transfer Protocol (FTP) o Simple Mail Transfer Protocol (SMTP), cuyas Variaciones en Retardo siempre pasan desapercibidas, los datos de Audio y Video son utilizables solo si son entregados dentro de un periodo de tiempo especificado. La entrega retrasada solo impide la utilidad de otra información en el flujo de la red. En general el Retardo y Variación de Retardo son dos fuerzas primarias trabajando contra la entrega oportuna de información.

La calidad de la transmisión esta determinada por la Disponibilidad y Pérdidas, adicionalmente por los siguientes factores, los cuales son manejados en diversos puntos por los mecanismos de la red.

Retardo

También llamado Latencia, es la cantidad de tiempo que toma a un paquete alcanzar el extremo receptor después de ser transmitido desde el extremo transmisor. Este periodo de tiempo es conocido como "*end-to-end-delay*" y puede ser descompuesto en dos áreas:

- *Retardo de la Red Fijo*: Incluye el tiempo de codificación / decodificación (para voz y video), así como una cantidad finita de tiempo requerida por los pulsos ópticos / eléctricos para atravesar el medio en ruta a su destino.
- *Retardo de la Red Variable*: Generalmente se refiere a las condiciones de la red, como la congestión, que puede afectar el tiempo conjunto requerido para transitar.

En redes de datos transportando Voz y Video, existen tres tipos de retardo:

- *Retardo en Paquetización*: Cantidad de tiempo que le toma muestrear y codificar las señales de Voz y Video analógicos y convertirlos en paquetes.
- *Retardo en Señalización*: Cantidad de tiempo que toma colocar los bits de paquetes de datos en el medio físico.
- *Retardo en Propagación*: Cantidad de tiempo que toma transmitir los bits de un paquete a través del cableado físico.

La red, por su parte, contribuye al retardo principalmente con:

- *Retardo de Propagación* (*Propagation delay*): La cantidad de tiempo que le toma a la información viajar la distancia de la línea. La propagación del Retardo es mayormente determinada por al velocidad de la luz, por consiguiente, el factor de retardo de propagación no es afectado por la tecnología de red que ser emplea.
- *Retardo de Transmisión* (*transmition delay*): La cantidad de tiempo que le toma a un paquete cruzar el medio. El retardo en la transmisión es determinado por la velocidad del medio y el tamaño del paquete.
- Retardo de Guardar y Enviar (*Store-and-forward delay*): La cantidad de tiempo que le toma a un dispositivo de red el enviar un paquete que es recibido.
- *Retardo de procesamiento* (*Processing delay*): El tiempo requerido por el dispositivo de red para encontrar la ruta, cambiar el encabezado y otras tareas de conmutación. En algunos casos el paquete también necesitará ser manipulado. Todos estos pasos pueden contribuir al retardo en el procesamiento.

Variación en el Retardo

Variación en el retardo ("*jitter*") es la diferencia en el retardo *end-to-end* entre paquetes. Por ejemplo, si un paquete requiere 100 [ms] para atravesar la red del extremo transmisor al extremos receptor, y el paquete siguiente requiere 125 [ms] para realizar el mismo trayecto, entonces la variación en el retardo es calculado como 25 [ms]. Es particularmente descriptivo en las comunicaciones de audio debido a que puede causar efectos desagradables que el usuario podría notar. Muchas aplicaciones multimedia son diseñadas para minimizar ésta variación.

Cada estación final en VoIP o conversación de Video sobre IP tiene un "*jitter buffer*", o memoria de variación de retardo con el fin de suavizar los cambios en los tiempos de llegada conteniendo voz. Desde este *buffer* el software o hardware obtiene los datos a desplegar o retransmitir. Es dinámico y puede ajustarse normalmente por más de 30 [ms] de cambio promedio en la llegada de los paquetes. El uso de *buffers* no garantiza la anulación de discontinuidades, debido a que éstas son impredecibles. Se acompaña su uso con técnicas para minimizar el *jitter*.

Convergencia

La convergencia de la red en el caso de una falla es un factor de gran importancia a considerar en el diseño de una red. Específicamente se debe razonar lo que sucede en el instante de la falla y lo que acontece cuando el dispositivo es restaurado. El comportamiento de la red es un poco diferente en estos dos escenarios.

Redundancia

Para asegurar la continuidad del servicio con la calidad proyectada, deben existir métodos para hacer llegar el tráfico a su destino pese a la posible presencia de fallas en enlaces o equipos. Con este fin, redundancia es agregada a la red, asegurando que cualquier falla en ella no interrumpirá el paso de datos, o degradará su calidad.

Requerimientos de QoS del Proveedor de Servicio

De un extremo al otro, la QoS es como una cadena, que es sólo tan fuerte como en el segmento más débil en ella. Por consiguiente es esencial para las empresas utilizar Proveedores de Servicio que puedan proveer los acuerdos requeridos de nivel de servicio por las aplicaciones.

Por ejemplo, consideraremos los requerimientos "extremo a extremo" (*end-to-end*) de aplicaciones demandantes de Qos (como Voz y Video Conferencia):

- No más de 1% de Pérdida
- No más de 150 [ms] de Retardo en un sentido (*one-way*)
- No mas de 30 [ms] de Variación de Retardos.

Entonces los componentes del Proveedor de Servicios (subconjunto del recorrido) deben ser considerablemente más exigentes que los requerimientos generales de la red, por ejemplo:

- No más de 0.5% de Pérdidas
- No más de 60 [ms] de Retardo en un sentido (*one-way*).
- No más de 20 [ms] de variación de Retardos.

La relación se muestra en la figura:

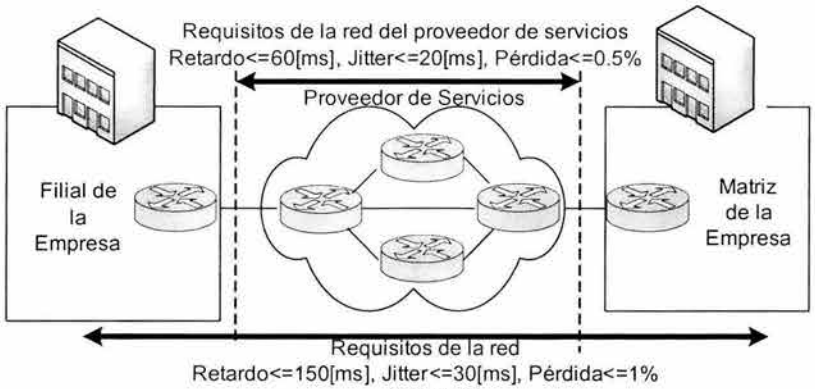


Figura 1.2.2

Para lograr dichos valores, las empresas y Proveedores de Servicio deben cooperar para ser consistentes en clasificar, proveer e integrar sus soluciones de QoS respectivas.

1.2.2 QoS POR SERVICIO OFRECIDO

Con el fin de garantizar los parámetros requeridos por cada clase de tráfico que la red a diseñar soportará, efectuaremos consideraciones de Administración de Tráfico y Clases de Tráfico, las cuales asegurarán que los requerimientos de QoS serán cubiertos, logrando transportar satisfactoriamente el tráfico en la red.

Típicamente el Gateway de Voz / Video o el Servidor de aplicaciones de Voz o Datos del cliente marcaran su RTP o control de tráfico con el DSCP apropiado y marcas de CoS. Sin embargo, algunos dispositivos finales pueden no tener la capacidad de clasificar correctamente su propio tráfico. Es también posible que por razones de control y seguridad no se quiera confiar en las marcas de CoS y ToS asignadas por el cliente, y se podría preferir rescribirlas en el ingreso de la red.

Implementar QoS en la red como Proveedor de Servicios facilitará el tráfico de datos a través de la misma, además de ofrecer la ventaja de poder controlar el tráfico circulante en condiciones extremas como congestiones de los enlaces.

Perfil de las aplicaciones

Debemos definir el perfil de las aplicaciones con el fin de proporcionar un entendimiento básico de los requerimientos de la red y patrones probables de tráfico. Asignaremos clasificaciones en cuanto a la prioridad de transmisión de datos, y dentro de dichas propuestas, se ubicarán las correspondientes aplicaciones a transitar por la red, en función de la necesidad de recursos de éstas o el nivel de servicio ofrecido al cliente por las facilidades contratadas.

Administración del tráfico

Como primer elemento participante en la QoS, el administrar la capacidad de los enlaces de la red en función de la prioridad del servicio que transite por él es una medida necesaria y de gran ayuda para asegurar que las aplicaciones prioritarias siempre cuenten con un espacio asegurado del Ancho de Banda disponible, y por otro lado, éstas no consuman la totalidad del enlace ocasionando la pérdida de la información restante, en el caso de la saturación de tráfico prioritario.

Figura 1.2.3

Clases de Tráfico

El segundo elemento es definir las Clases de Tráfico para datos en la red, la cuales se aplicarán al tráfico que ingresa a la red proveniente del usuario, para poder ser administrado por el Operador. Es recomendable no proponer más de cuatro, ya

que es contraproducente el uso de muchas clases discretas de tráfico de datos, debido a que mientras más clases son definidas existe menor distinción entre niveles de servicio. Se sugieren:

Dorado (*gold*):

Aplicable a tráfico prioritario para el Proveedor de Servicios, el cual es clasificado de ésta manera por su naturaleza sensible al mal funcionamiento de la red (Voz y Video), o por la importancia que el cliente asigna al correcto y eficiente envío de datos.

→ Recomendación General: DSCP EF, IP Precedence 5, CoS 5.

Los servicios típicos se describen a continuación:

- *Voz:* Cuando se hace referencia a la QoS necesaria para el tráfico de voz, debe tenerse lo siguiente en mente:
  - Perdidas deben ser no mayores a 1%.
  - Retardo en un sentido no debe ser mayor a 150 [ms] según el estándar de la ITU para VoIP (G.114) o 200 [ms] según criterios de algunas compañías (Cisco), ya que en la práctica existe una despreciable diferencia en los niveles de calidad.
  - El promedio de *jitter* (variaciones de retardo) debe ser no mayor a 30 [ms].
  - El Ancho de Banda garantizado como prioridad de 21-106 [kbps] es requerido por cada llamada (dependiente también de la taza de muestreo, codec empleado, etc.)
  - El Ancho de Banda garantizado de 150 [kbps] por teléfono es requerido para el tráfico de Control de Voz.

→Recomendación de Tráfico portador de Voz (Voice Bearer Traffic): DSCP EF, IP Precedence 5, CoS 5.

→Recomendación de Tráfico de Control de Voz (*Voice Control Traffic*): DSCP AF31, IP Precedence 3, CoS 3.

- *Video:* Cuando hacemos referencia a la QoS necesaria para tráfico de Video, debe tenerse lo siguiente en cuenta:

  - Perdidas no debe ser mayor a 2%.
  - Retardo no debe ser mayor a 4 o 5 [s] (dependiendo de las capacidades del buffer de la aplicación).
  - No hay requerimientos significativos de Variación de Retardos.
  - Requerimientos de Ancho de Banda dependen de la codificación y taza del flujo de video (*encoding and rate of video stream*).

Existen dos tipos principales de aplicaciones de video:

  - Flujos de video (*streaming video*): Perteneciente a la clase *Silver*
  - Video interactivo (*interactive video*): Con necesidades de QoS como tráfico de Video Conferencia:
    - Perdidas deben ser no mayores a 1%
    - Retardo en una vía debe ser no mayor a 150-200 [ms]
    - Promedio de Variación de Retardo debe ser no mayor a 30 [ms]

El Ancho de Banda mínimo garantizado se sugiere de un 20% más del tamaño de la sesión de Videoconferencia (significando que a una taza de transferencia de 384 [kbps], la sesión de videoconferencia requiere 460 [kbps] de Ancho de Banda garantizado)

Debemos considerar que el tráfico de Videoconferencia tiene naturaleza expansiva, por lo que el limitar su Ancho de Banda es una buena costumbre.

→Recomendación de Video Conferencia (Video Conferencing): DSCP AF41, IP Precedence 4, CoS 4

- *Datos Prioritarios (Misión-Critical Data):* Usualmente el tráfico *mission-critical* es asignado a las aplicaciones de datos de las clases mas altas, y son aquellas que directamente contribuyen a la operación de la empresa. Son altamente interactivas y son por consiguiente sensibles a la Pérdida y Retardo. (Aplicaciones ERP, como SAP, Oracle, PeopleSoft, transacciones y *Software in-house*).

→ Recomendación *Misión-Critical Data*: DSCP AF21-23, IP Precedence 2, CoS 2.

Plateado (*silver*):

Estas aplicaciones requieren de un nivel de Ancho de Banda garantizado, a diferencia con la clasificación anterior, de no representar un gran impacto la pérdida de paquetes, retardo, *jitter*, etc.

→ Recomendación General: DSCP AF11-AF13, IP Precedence 1, CoS 1.

Aplicaciones comunes:

- Video: En los tipos de información pertenecientes a las aplicaciones de video, se requiere una clasificación segura, más no demandante a la red para tráficos de:
  - Flujos de Video (*Streaming Video*): Las aplicaciones de flujos de video son más indulgentes en los requerimientos de QoS, así como insensibles al retardo. Streaming video puede tener contenido valioso y por consiguiente puede requerir garantías de servicio vía QoS. La distribución del tráfico debe de administrarse para evitar impactos en la red. Se incluyen aplicaciones de Flujo de Video, como IPTV o programas de Video sobre Demanda (VoD), donde herramientas significativas para QoS no son requeridas para cubrir las necesidades de estas aplicaciones.

    →Recomendación de Flujos de Video (*Streaming Video*): DSCP AF13, IP Precedence 1, CoS 1
  - Video interactivo (*interactive video*): Perteneciente a la clase *gold*
- Datos con Ancho de Banda Garantizado: Estas aplicaciones son generalmente vistas como secundarias en importancia para operaciones de negocios o son de naturaleza altamente asíncrona. (*Netmeeting, streaming video, intranet, messenging, calendarización, groupware y navegación en Internet*). Se les asigna una alta importancia en su transmisión por al red, sin embargo, es menor que el tráfico clasificado como prioritario, por lo cual, poseen riesgo de pérdida de paquetes en caso de congestión del enlace.

→ Recomendación: DSCP AF11-AF13, IP Precedence 1, CoS 1.

Best-Effort (Default Class):

Es la categoría default de las aplicaciones de datos. Estas aplicaciones juegan un rol indirecto en las operaciones normales de la empresa. Mientras algunas de estas

aplicaciones pueden ser interactivas, ningún ancho de banda garantizado es requerido. (E-mail y navegación en Internet genérica).

→ Recomendación: DSCP 2-6, IP Precedence 0, CoS 0.

Less-than-best-effort (preferencias *higer-drop*):

Clase de tráfico opcional. Es la categoría para las aplicaciones que tienen un uso de Ancho de Banda intensivo y que no tienen relación directa con los negocios de la empresa. Estas aplicaciones son típicamente altas en Retardo y de desecho de paquetes intensivo; a menudo las ejecuciones de esas aplicaciones tardan horas. Por consiguiente, esas aplicaciones pueden ser dadas con alta preferencia a tirar paquetes para prevenir que estas roben ancho de banda disponible para aplicaciones *best-effort* (transferencias de archivos muy grandes como FTP, operaciones de respaldo y aplicaciones de intercambio de entretenimiento de multimedia Peer-to-Peer como Napster, KaZaa o Gnutella).

→ Recomendación: DSCP BE, IP Precedence 0, CoS 0.

Aplicaciones Típicas	Clases de Tráfico correspondientes
Voz	*Gold*
Video Interactivo	
Señalización de llamadas	
Datos *Mission-critical*	
Enrutamiento	*Silver*
Datos transaccionales	
Streaming Video	
Administración de la red	
Best-effort	*Best-effort*
Less-than-best-effort	*Less-than-best-effort*

Tabla 1.2.4

Recomendaciones

No debemos asignar más de 3 aplicaciones a cada clase de tráfico de datos, debido a que si muchas aplicaciones son asignadas a las clases más altas, entonces la efectividad de QoS del conjunto se verá afectada, teniendo como resultado el mismo que si no se hubiera provisto con QoS a ninguna aplicación. Por esta razón, las aplicaciones provistas con QoS deben estar imitadas a solo un selecto grupo de ellas.

Políticas

Se recomienda el uso de políticas preventivas en vez de políticas correctivas, considerando los siguientes casos:

• No preferir el tráfico *less-than-best-effort* e implementar políticas restrictivas con la esperanza de mejorar indirectamente la disponibilidad de Ancho de Banda de otras aplicaciones, ya que la implicación es que el Ancho de Banda es monopolizado por aplicaciones sin importancia ocasionando que los usuarios con aplicaciones importantes tengan problemas.

• Tener en cuenta que la aplicación de políticas limitantes del Ancho de Banda incrementarán la complejidad de administración y requerirán más esfuerzo de procesamiento conforme la complejidad aumente.

• Una práctica recomendada es proveer garantías de Ancho de Banda para las aplicaciones de datos importantes, y proveer una clase default *best-effort*. Después de que estas políticas de protección están implementadas, pueden ser sobrepuestas políticas opcionales de vigilancia para tráfico *less-than-best-effort*. Sin embargo, la implementación de políticas de vigilancia crea un límite estático que no siempre es deseable.

• Obtener un visto bueno a nivel ejecutivo o de un nivel relacionado con la prioridad de la aplicación es recomendado antes de realizar la implementación de la política real con el fin de evitar un descarrilamiento potencial del proyecto. Lo anterior debido a que el proceso es usualmente muy vigilado y organizacionalmente costoso, además de que la mayoría de las veces toma más tiempo en obtenerse, comparando con la parte técnica real de la implementación de QoS.

1.2.3 SLA –SERVICE LEVEL AGREEMENT- (ACUERDO EN EL NIVEL DE SERVICIO)

Para garantizar a los usuarios de la red, y a la misma red WAN características de escalabilidad y confiabilidad, el Proveedor de Servicio, debe ofrecer al cliente un Acuerdo de Nivel de Servicio competitivo (Service Level Agreement "SLA"). El SLA debe garantizar que las necesidades son cubiertas de acuerdo a las características de cada cliente, lo cual va ligado al costo del servicio, mientras más exigencias de éste, mayor será el costo del servicio; por ejemplo, deberá especificar claramente el máximo Retardo que un paquete podría experimentar cuando viaje por el Backbone del Proveedor y la mejor disponibilidad que el éste pueda prometer. Se debe obtener

un fidedigno SLA para todos los enlaces WAN y, si como Proveedor no se cuenta con uno, debe estimarse a la brevedad para ofrecer confianza y seguridad a los clientes. Para agregar SLAs competitivos, se debe estar seguro que la red es capaz de soportar las aplicaciones del cliente.

Las estimaciones de SLA deben ser realistas y soportadas por un diseño previo que cumpla con las expectativas ofrecidas. En este punto, el diseño físico y lógico de la red WAN es fundamental para la exitosa culminación de los resultados esperados, debido entre otras consideraciones, a que las redes de empresas pueden ser implementadas con diferentes tecnologías WAN y que la disposición de los enrutadores es crítica para controlar los patrones de tráfico a través de la red del Proveedor.

1.2.4 CRITERIOS PARA LA OBTENCIÓN DEL SLA DESEADO

Las Redes de área amplia, y en consecuencia la nuestra, deben considerar para su diseño aspectos como los siguientes para asegurar que su desempeño sea óptimo, y los compromisos acordados con el cliente puedan cumplirse:

- **Optimización del funcionamiento de la red**: El funcionamiento de la red deberá ser óptimo, considerando el nivel de servicio ofrecido y la rentabilidad que esto represente.
- **Minimizar costos de operación e implementación**: El objetivo de la red debe ser alcanzado sin utilizar recursos que puedan ser ahorrados.
- **Proveer servicios de manera adecuada**: Proveer los servicios que hayan sido ofrecidos al cliente de la manera acordada y sin atentar contra alguna ley o disposición oficial.
- **Permitir redundancia para tolerancia a fallos**: Agregar redundancia para asegurar que pese a la aparición de alguna falla, el SLA ofrecido no cambiará dramáticamente.
- **Utilización al máximo de los componentes de red**: Utilizar óptimamente los componentes de la red para evitar la presencia de equipo subutilizado, sin perder de vista el limite en capacidad del equipo, el cual no deberá sobrepasar en condicionas normales el 70 u 80% de su capacidad.

- **Tener una clara orientación del servicio**: Definir exactamente los servicios que la red (o cada una de sus secciones) ofrecerá.
- **Realizar un balance entre costo y retardo en la red**: Evaluar y definir el retardo a ofrecer en el SLA, en función de las aplicaciones que transitarán y el costo de dicho ofrecimiento. Considerar 70 u 80% de utilización de los enlaces máximo.
- **Tener tan pocos enlaces como sea posible**: Con el fin de evitar fallas innecesarias. Este caso excluye la redundancia.
- **Propuesta de varias soluciones al proyecto**: Se deberán considerar la mayor cantidad de opciones de solución a la red ya que la mayoría de los algoritmos y procesos de diseño requieren aplicaciones repetitivas para dar los mejores resultados y considerar todas las posibilidades.
- **Establecimiento de criterios de Métrica**: Asignación de un valor específico a cada interfase en función de velocidad del enlace, costo, tráfico, políticas, etc.
- **Optimizar las rutas**: Buscar la interfase con menor métrica para efectuar el tránsito de datos.
- **Desempeño**: Buscar la mejor opción de diseño de red para lograr el mejor desempeño, el cual normalmente esta ligado al tiempo de respuesta.
- **Escalabilidad**: Considerar las opciones de crecimiento de la red a futuro para las decisiones de diseño de la red desde un primer momento.
- **Adaptabilidad**: Diseñar la red otorgándole la capacidad de adecuarse a la implementación de futuras aplicaciones y capacidades que sean requeridas.
- **Fiabilidad y disponibilidad**: Debe asegurarse la continuidad del servicio, donde la solución más sencilla es agregar respaldos a los enlaces WAN principales y configurar los enrutadores para ello, lo cual garantiza la disponibilidad para todos los servicios WAN, incluso si el enlace primario se viene abajo, sin embargo esta solución no es posible si la compañía no tiene el presupuesto para mantener circuitos de respaldo; otro posible punto débil de esta solución es que la capacidad de transporte de los proveedores de servicio varía en relación a los otros con los que se interconecta, por lo que la capacidad de los circuitos es muy diversa entre ellos, y como en

algún lugar intermedio se tienen que compartir enlaces en común, se destruye el mecanismo de respaldo.

- **Seguridad**: Es deseable que el diseño de red que se propone, pueda proveer opciones de autenticación y privacidad de usuarios e información.
- **Costo**: Debe intentarse el balance exacto entre características técnicas ofrecidas por la red (SLA) y el costo que esto representa para el proveedor.

Finalmente, basados en los aspectos repasados en este capitulo, seremos capaces de identificar las necesidades y aspectos como QoS y nivel de servicio a que se compromete el Proveedor, los cuales se deberán contemplar en el proceso de diseño de la red, proveyendo una visión más amplia, objetiva y real para la implementación de la red.

II CONCEPTOS BÁSICOS SOBRE REDES WAN (PUNTO DE PARTIDA)

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas, las cuales se mejoraron como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía. Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo de el grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Utilizando procedimientos y protocolos ya existentes para establecer la comunicación e incorporando moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por el medio físico.

Las necesidades de la comunicación a distancia dieron dos enfoques a las redes, el primero llamado redes privadas compuesto de líneas de dedicadas (*leased lines*) y concentradores usando una topología de estrella. El segundo concepto, llamado redes de datos públicas emergió simultáneamente.

En tiempos recientes se ha dado una rápida convergencia en áreas como redes telefónicas fijas y móviles, Internet y redes privadas, que a la par con la evolución de las equipos de comunicaciones, y la unión de la captura, transporte, almacenamiento y procesamiento de la información se están integrando con mayor fuerza y rapidez.

Sin embargo, a medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados medios de transmisión crece todavía con mayor premura.

Se propone como solución favorecer el desarrollo de redes de datos públicas ya que el enfoque de redes privadas es muchas veces insuficiente para satisfacer las necesidades de comunicación de un usuario dado o demasiado caro. La falta de interconectabilidad o la dificultad de conectar redes privadas y la demanda potencial

de información entre ellas en un futuro cercano favorecen el desarrollo de las redes públicas.

Todas las consideraciones en la facilidad y optimización de la interconexión de redes, no deben olvidar proporcionar una alta fiabilidad en la comunicación, por ejemplo al contar con trayectorias alternativas de suministro, además de tomar en cuenta su capacidad para aumentar su rendimiento.

Lo anterior nos conduce a que el concepto de redes puede aplicarse desde a un edificio, hasta a una región tan extensa como una red de área amplia.

II.1 CONCEPTO DE REDES

Concepto

Las redes constan de dos o más computadoras y/o dispositivos conectados entre sí y permiten compartir recursos e información. Los recursos son los dispositivos o las áreas de almacenamiento de datos de una computadora, compartida por otra computadora mediante la red. La más simple de las redes conecta dos computadoras, y una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo. Si se desea compartir eficientemente archivos y ejecutar aplicaciones de red, hace falta tarjetas de interfaz de red y un medio físico para conectar los sistemas. Aunque se puede utilizar diversos sistemas de interconexión, estos deben ofrecer velocidad e integridad necesaria para un sistema de red seguro y con altas prestaciones que permita manejar muchos usuarios y recursos.

Necesidades de las redes

El crecimiento y el cambio constante en diversas áreas obligan al desarrollo de nuevas tecnologías como:

- Nodos con mayor procesamiento de transmisión.
- Poder y complejidad de aplicaciones.
    - Proceso distribuido de datos.
    - Multimedia.
    - Videoconferencia.
    - Visualización / Realidad virtual.

  - Conectividad de usuarios móviles.
- Soporte de mayor tamaño de archivos.
- Soporte de incremento en el número de usuarios de red.
- En aplicaciones con voz, multimedia, video son sensibles al retardo, hay que cuidar:
  - Acceso garantizado.
  - Tasa de transmisión sin que exista error.
  - Retardo.

II.2 CONCEPTO DE REDES MPLS

Cuando el único servicio era el Protocolo de Internet (Internet Protocol - IP) para acceso a Internet, las redes IP tuvieron gran aceptación. Esto se debe a que las redes IP no eran orientadas a conexión, lo cual proveía la ventaja de hacerlas relativamente fáciles de configurar, pero las hizo también menos previsibles, relegando así su uso como un acceso barato a Internet.

En el mercado ultra-competitivo de hoy, los servicios de próxima generación de IP, tales como presencia virtual, redes privadas virtuales, video, y voz, llevan la demanda a niveles mucho más altos de previsibilidad de la red, lo cual puede ser garantizado solamente con las redes orientadas a conexión. Las garantías de servicio son necesarias para ofrecer servicios confiables y utilizables para los clientes, los cuales se traducen directamente en productos generadores de ingresos para los proveedores. El Multiprotocolo de Conmutación de Etiquetas (Multi- Protocol Label Switching -MPLS) parece ser la tecnología que lo permite, la cual agregará en última instancia la orientación a conexión a las redes IP, y la previsibilidad a los servicios IP.

La tecnología MPLS permite construir en una red una ruta disponible entre un punto de salida y un destino, o entre un grupo de salida y un grupo de destino. Esta tecnología está basada en la colocación de "etiquetas" en los paquetes que entran en una red y que van a avanzar a lo largo de un trayecto, mediante la conmutación de etiquetas. Éstas contienen información de enrutamiento específica que puede indicar varios parámetros:

- Un trayecto predefinido.
- La identidad del emisor (una fuente).
- La identidad del destinatario (un destino).
- Una aplicación.
- Una calidad de servicio, etc.

Los equipos intermedios están configurados para que a partir de esa información, se pueda deducir un tratamiento muy simple, ya que se trata esencialmente de enviar el paquete hacia el enrutador siguiente tomando un trayecto específico y predefinido.

En primer lugar, la creación de trayectos disponibles de extremo a extremo mejora mucho la rapidez de conmutación de los equipos transporte, ya que sus listas de rutas se limitan a una colección restringida de instrucciones simplificadas. Sobre todo, MPLS permite ofrecer a IP un modo circuito similar al de las tecnologías de red como X.25 o ATM y, como segunda parte, poner en práctica políticas de encaminamiento específicas a ciertos flujos. De esta forma hace posible la implantación de niveles de servicio y de calidad de servicio (QoS), así como de una Ingeniería de Tráfico evolucionada. Por último, MPLS facilita también la implementación de los servicios de las Redes Privadas Virtuales.

II.3 MODELO DE REFERENCIA OSI
-Open Systems Interconection-
(Modelo de Interconexión de Sistemas Abiertos)

Historia

A mediados de los 70 diversos fabricantes desarrollaron sus propios sistemas de red. En este desarrollo surgen como inconveniente las limitaciones ocasionadas por la existencia de un sistema propietario, como son los dispositivos especiales y la no interconectividad con otros sistemas.

OSI surge basado en una propuesta desarrollada por la International Organization for Standarization (ISO) u Organización Internacional para la Normalización por la necesidad de crear un modelo que pudiera ayudar a los diseñadores a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad).

Este modelo de referencia surge en el año de 1983 y es descrito por la norma ISO 7498 y estandarizado por el ITU-T, como recomendación X.200.

El modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial. Definió la forma en que se comunican los sistemas abiertos de telecomunicaciones, los servicios y los protocolos que posibilitan la comunicación (sistemas que se comunican con otros sistemas).

Aplicando este modelo se obtiene la interconexión de terminales procedentes de diferentes fabricantes dentro de una red. Tiene como ventaja la flexibilidad en la utilización de sus capas. El desarrollo del modelo fue orientado hacia las comunicaciones y no a la informática.

Definición

El Modelo de Referencia OSI proporciona una base estratificada orientada al funcionamiento para la interconexión de redes abiertas. Es importante destacar que no se trata de una Arquitectura, dado que no define los servicios y protocolos exactos para cada nivel, sino sólo aquello de lo que cada nivel debe ocuparse. La ISO ha producido estándares para cada nivel del modelo OSI con el fin de regular el grado y aspecto en que cada nivel del modelo será regulado.

Funcionamiento

El modelo de referencia **consiste en 7 capas o niveles** donde cada uno se encarga de problemas de distinta naturaleza, interrelacionándose con los niveles contiguos. Debido a que estos niveles se visualizan generalmente como bloques apilados o *stack of blocks*, también conocido como *OSI Protocol Stack*.

En este modelo, solo las capas que tengan otra capa equivalente en el nodo remoto podrán comunicarse, es decir, solo **las capas que son iguales se comunican entre si**. Debido a la construcción del modelo, y a la independencia entre niveles, **el protocolo de cada capa solo se interesa por la información de su capa** y no por la de las demás.

La información se pasa a las capas "de abajo" hasta que la información llega a la red. En el nodo remoto, la información es entonces pasada "hacia arriba" hasta que llega a la capa correspondiente. **Cada capa confía en que las demás harán su trabajo**, así una capa no se interesa por el funcionamiento de las demás, el único interés de ésta es la forma en como los datos serán pasados hacia arriba o hacia abajo. Por si solas, las capas no hacen nada más que mantener en buen estado el camino para que fluyan los datos.

La forma de lograr este proceso es **encapsulando y desencapsulando información** en los mensajes que se van a enviar. Todas las capas en este modelo sirven netamente de infraestructura a las telecomunicaciones.

Capas

Son **entidades que realizan por sí mismas una función específica**. Cada nivel se abstrae de los problemas que los niveles inferiores resuelven, a fin de dar solución a un nuevo problema del que se abstraerán, a su vez, los niveles superiores.

Cada capa **define los procedimientos y las reglas que los subsistemas de comunicaciones deben seguir** para poder comunicarse con sus procesos correspondientes de los otros sistemas.

Arquitectura de red basada en el Modelo OSI

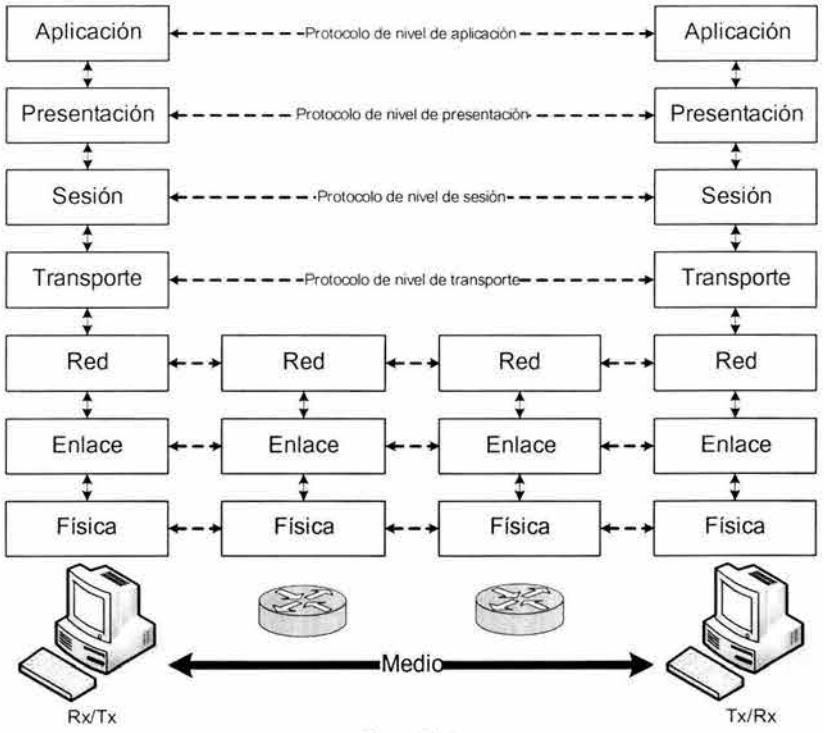


Figura 2.3.1

Criterios para definir una capa

Deberá crearse una **nueva capa siempre que se precise un nuevo grado de abstracción** y a la cual deberá asignarse un número bien definido de **funciones propias**. La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz entre ambas.

La funcionalidad de cada capa deberá tener en cuenta la posibilidad de definir **protocolos normalizados** a nivel internacional. El número de capas debe ser lo suficientemente grande como para no reunir en un nivel funcionalidades distintas y lo suficientemente pequeño para que el resultado final sea manejable en la práctica.

Características generales de las capas y comunicación

Las funciones implementadas en cada capa deben seleccionarse de tal forma que permitan la **definición de protocolos** normalizados para su materialización, sin perder de vista que el paso de información entre capas debe ser mínimo.

Es importante tener presente que el número de capas del modelo debe estar equilibrado, de forma que sea el suficiente para que funciones diferentes estén implementadas en capas diferentes. La comunicación física se lleva a cabo únicamente entre las capas de nivel 1.

Entre las ventajas más significativas de la utilización de capas está la **división de la comunicación** de red en partes más pequeñas, sencillas de manejar y fáciles de aprender; la **normalización** de los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.

Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez con relativa **independencia entre cada una** de ellas.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen **debe comunicarse con su capa igual en el lugar destino**; a ésta forma de comunicación se conoce como comunicaciones de par-a-par (*peer to peer*).

Las reglas y convenciones que controlan esta conversación se denominan **protocolo de la capa n**, y se ocupan del formato y significado de las unidades de datos intercambiadas. Durante este proceso, cada protocolo de capa intercambia unidades de información entre capas iguales de las máquinas que se están comunicando, conocidas con el nombre de Unidades de Datos de Protocolo (PDU).

Cada capa de comunicación, en el nodo origen, se comunica con un PDU específico de capa y con su capa igual en el nodo destino. Cada capa de un modelo o arquitectura de red recibe servicios a la capa que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario.

Descripción de las Capas

Capa 1 (Capa Física):

Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

Esta capa es la encargada de realizar el **transporte del flujo de bits a través del medio de transmisión**. Define la conexión física de la red abarcando:

Las **características materiales** (componentes mecánicos, conectores, conexiones, cables, componentes de interfaz con el medio de transmisión, polaridades, etc.), **características eléctricas y ópticas** (niveles de tensión, corriente, velocidad de las señales, la trama de bits, etc.) y **características funcionales** de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

Su meta es que cuanto envíe el emisor llegue sin alteración al receptor. **Garantiza la conexión** (aunque no la fiabilidad de ésta). Proporciona sus servicios a la Capa de Enlace de datos.

Capa 2 (Capa de Enlace):

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Suministra un tránsito de datos (transmisión y recepción) **confiable** a través de un enlace físico establecido entre un nodo y otro colindante en un enlace de red.

Tiene la capacidad de corregir y mantener **libre de errores** la transmisión entre secciones o tramos, para lo cual se apoya en:

Reconocimiento y retransmisión de tramas, control de las secuencias de transmisión y los acuses de recibo de los mensajes, retransmisión de los paquetes que no han sido acusados por el otro extremo, sincronización del envío de las tramas, adición de bits de paridad, uso de Códigos Cíclicos Redundantes CRC's, numeración de secuencias de tramas para evitar tramas repetidas, etc.

Provee el **control de flujo** de información entre dos nodos de la red mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción. Controla la **congestión de la red**. Regula la **velocidad** de tráfico de datos.

Utiliza como estructura para el flujo de bits un **formato predefinido** llamado trama o *frame*, que para formarla, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.

Capa 3 (Capa de Red):

Define la señalización, el establecimiento y la desconexión, incluido el encaminamiento de un enlace. Se encarga del direccionamiento lógico.

Efectúa el **enrutamiento de paquetes**, es decir, envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.

Maneja destinos, rutas, congestión en rutas, alternativas de enrutamiento, etc. Proporciona conectividad y **selección de la mejor ruta** para la comunicación entre nodos.

Es responsable de funciones de conmutación y enrutamiento de la información (**direccionamiento lógico**), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la **topología de la red**, con objeto de determinar la ruta más adecuada.

Maneja el caso en que la nodo origen y la nodo destino estén en redes distintas. Las funciones de esta capa también pueden ser capaces de reconfigurar la red para que los datos fluyan por un camino u otro si es que un enlace se cae.

Encamina la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento **a través de dispositivos intermedios (enrutadores)**. Reensambla los paquetes en el host destino.

Divide los mensajes de la capa de transporte en unidades más complejas, denominadas paquetes, a los que asigna las direcciones lógicas de los host que se están comunicando. Divide los mensajes de la capa de transporte en paquetes y los ensambla al final. Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.

Capa 4 (Capa de Transporte):

Establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Ofrece un servicio de transporte independiente de la red utilizada con carácter de comunicación extremo a extremo (conocidas como **conexiones punto a punto**) sin errores para el envío de mensajes de una sesión. Transfiere datos segura, económica y **confiablemente**, incluyendo controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.

Establece **circuitos virtuales** que son las conexiones que se establecen dentro de una red. donde no hay la necesidad de elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.

Controla la interacción entre procesos de usuarios en las máquinas que se comunican, así como el flujo de transacciones y el direccionamiento de procesos de maquina a procesos de usuario.

Permite **multiplexar** una conexión punto a punto entre diferentes procesos del usuario y provee la función de difusión de mensajes (***broadcast***) a múltiples destinos.

Efectúa la **división de archivos** originados en el host emisor en unidades apropiadas, denominadas segmentos para ser transmitidos por la red, los cuales después de viajar y llegar al destino en la red, deben de ser acomodados de la manera en que fueron enviados en el sistema del host receptor. Define tiempos y esperas de datos.

Asegura la recepción de todos los datos y en el orden adecuado, realizando un control de extremo a extremo. Realiza funciones de **control y numeración** de las unidades de información.

Proporciona sus servicios a la Capa de Sesión, efectuando la transferencia de datos entre dos entidades de sesión.

Capa 5 (Capa de Sesión):

Sincroniza el diálogo entre las capas de presentación y administra su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre máquinas, regulando quien habla y por cuanto tiempo.

Incluye los **convenios sobre el transcurso de la comunicación** (entre personas, procesos, persona/procesos).

Controla el comienzo, realización y finalización de una comunicación. Se encarga del **diálogo** (quién habla, cuándo, cuánto tiempo, *half duplex, full duplex*, funciones de sincronización). Establece, administra y finaliza las **sesiones** entre dos máquinas en red que se están comunicando.

Establece conexiones lógicas entre puntos de la red. Ordena o decide a dónde deben de ir los datos y cuántos se habrán de enviar o recibir en cierto destino de la red.

Permite a usuarios en diferentes máquinas **establecer una sesión**, donde una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.

Si por algún motivo una sesión falla por cualquier causa ajena al usuario, **restaura la sesión** a partir de un punto seguro y sin perdida de datos o, si esto no es posible, termina la sesión de una manera ordenada, verificando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.

Consigue una **transferencia de datos eficiente y un registro de excepciones** acerca de los problemas de la capa de sesión, presentación y aplicación. Realiza *checkpoints*, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

Proporciona sus servicios a la Capa de Presentación y hace que las entidades de presentación que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

Capa 6 (Capa de Presentación):

Es responsable de la **obtención y de la liberación** de la conexión de sesión cuando existan varias alternativas disponibles. **Traduce entre varios formatos** de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. **Convierte los datos** desde el formato local al estándar de red y viceversa. Da formato a la información para visualizarla o imprimirla. (**Comprime los datos** si es necesario). Aplica a los datos **procesos criptográficos** cuando sea necesario.

Dado que un protocolo de telecomunicaciones debe de ser diseñado para que diferentes versiones y sistemas lo puedan usar, los datos se deben de tener en un **formato definido y documentado**. La capa de presentación, recibe bits de las aplicaciones y las formatea de modo que sean octetos entendibles en una red. Así, recibe un mensaje con octetos de una red y los decodifica para que se conviertan en Bits de una aplicación.

Aisla a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares en un formato común de red entendible por todos los sistemas y apto para ser enviado por red.

Proporciona sus servicios a la Capa de Aplicación, garantizando que la información que envía a un sistema pueda ser entendida y utilizada por la Capa de Aplicación del otro, estableciendo el contexto sintáctico del diálogo.

Capa 7 (Capa de Aplicación):

Es el último nivel del modelo, el que aloja el programa de red que interactúa con el usuario. Soporta aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el nivel de usuario con datos de aplicación; la red es transparente a este nivel.

Relacionada con las funciones de mas alto nivel, es el **medio por el cual los procesos las aplicaciones de usuario acceden a la comunicación por red** mediante

el entorno OSI, proporcionando los procedimientos precisos para ello. Establece la **disponibilidad** de los diversos elementos que deben participar en la comunicación. Sincroniza las aplicaciones que cooperan entre sí. Establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

En esta capa se define cómo dos participantes de una comunicación colaboran en la solución de una tarea.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores WEB, etc.). Se efectúa, por ejemplo, transferencia de archivos (FTP), Login remoto (rlogin, TelNet), Correo electrónico (mail), Acceso a bases de datos, WEB Browsers.

Encapsulamiento

En el proceso en el que un enrutador envía datos a otro, éstos deben ser colocados en paquetes que se puedan administrar y rastrear, a través de un proceso denominado encapsulamiento.

Cuando las aplicaciones de usuario envían los datos desde el origen, estos viajan a través de las diferentes capas. Las tres capas superiores (Aplicación, Presentación y Sesión) preparan los datos para su transmisión, creando un formato común para la transmisión. Una vez pasados a este formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tráfico de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

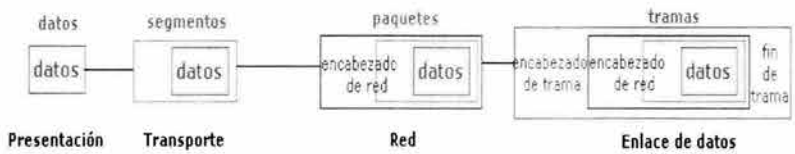


Figura 2.3.2

Pasos:

1. Crear los datos (Capa de Presentación).
2. Empaquetar los datos para ser transportados de extremo a extremo (Capa Transporte). Se dividen los datos en unidades de un tamaño que se pueda administrar (los segmentos), y se les asignan números de secuencia para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts envíen el mensaje de forma confiable para ambos extremos del sistema de comunicación.
3. Agregar la dirección de red al encabezado (Capa de Red). El siguiente proceso se produce en la Capa de Red, que encapsula el segmento creando un paquete o datagrama, agregándole las direcciones lógicas de red de la máquina origen y de la máquina destino. Estas direcciones ayudan a los enrutadores a enviar los paquetes a través de la red por una ruta seleccionada.
4. Agregar la dirección local al encabezado de enlace de datos (capa enlace de datos). En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama las direcciones MAC (número de la tarjeta de red, único para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.
5. Transmitir el tren de bits creado (Capa Física). Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, ondas, etc.). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio, que puede variar a lo largo de la ruta utilizada.

De lo anterior, concluimos y recalcamos los siguientes puntos:

- Cuando los datos se transmiten en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino.
- Si se deben enviar los datos a un host de otra red interna o a través de Internet es necesario el uso de paquetes de datos que contengan las direcciones lógicas de las máquinas que se deben comunicar.
- Las tres capas inferiores (Red, Enlace de datos y Física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet.

II.4 CAPAS DE INTERÉS SOBRE OSI

Con base en el tema anterior, es decir, el funcionamiento del modelo de referencia OSI, ubicaremos las capas de interés sobre dicho modelo de referencia para la tecnología MPLS.

Para poder deducir las capas del MROSI que utiliza MPLS mencionamos algunas de las características que esta ultima tecnología ofrece, tales como conmutación y marcado de paquetes, y uso de un identificador local del paquete (funciones de Capa 2-OSI como se recordará), además de efectuar funciones como establecimiento de circuitos, conocimiento del camino lógico, enrutamiento de un enlace y uso del campo TTL propio, el cual se decrementa únicamente dentro de la red MPLS con el fin de controlar la permanencia de un paquete en la red (funciones de Capa 3-OSI).

Por otro lado, existen funciones de Capa 2 que MPLS no efectúa, como lo son el control de flujo, multiplexaje, detección de errores y direccionamiento físico; esto es evidente si consideramos que el identificador no es una MAC-address (como en Capa 2-OSI), sino una etiqueta, que es solo un identificador que el enrutador lee para saber por qué puerto enviar el paquete. La deducción importante a todo esto (y a otras consideraciones) es que **MPLS no se ubica como un protocolo de Capa 2** exactamente.

Ahora, considerando la capa 3 del MROSI, y como diferencia con MPLS, el direccionamiento lógico no se da por medio de algún protocolo (típicamente IP), el cual funciona gracias a protocolos de enrutamiento, lo anterior debido a que el

encabezado MPLS contiene una etiqueta no una dirección IP, este identificador (etiqueta) no se propaga por medio de anuncios en toda la red como lo haría una red basaba en IP. Estas características hacen evidente su **no pertenencia a Capa 3**.

La no pertenencia exacta a alguna de las capas OSI definidas se hace aun más evidente al considerar el encabezado MPLS, el cual consta básicamente de los campos de: etiqueta, TTL, calidad de servicio, y un bit para la pila de etiquetas, lo cual no tiene parecido alguno con protocolos de Capa de Enlace o Red.

A continuación se muestran las coincidencias entre las funciones de los campos de los encabezados de: MPLS, tecnologías de Capa 2 (Frame Relay y ATM) y Capa 3 (IP):

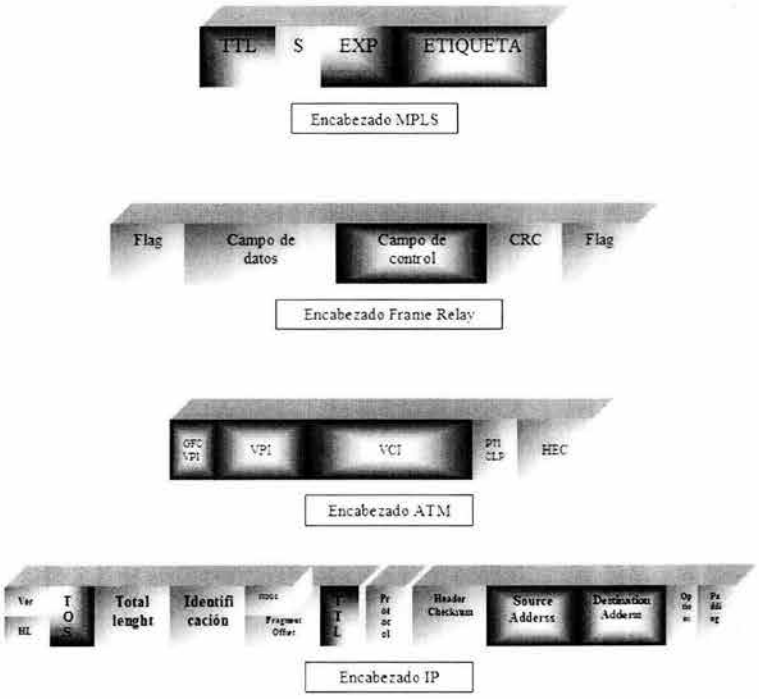


Figura 2.4.1

Otra diferencia estriba en aspectos como la realización de la conmutación por medio de etiquetas, ya que para MPLS los enrutadores actúan como Switches. Además, MPLS utiliza indirectamente la tabla de enrutamiento como base para generar una tabla de envío por etiquetas, es decir, MPLS depende indirectamente de

que un protocolo IGP, el cual proporciona una tabla de enrutamiento de la cual parte MPLS para asignar etiquetas identificando puerto e interfaces de entrada y salida.

Así se origina un gran debate al no poder ubicar a MPLS en ninguna de estas dos capas OSI, por lo tanto se crea el concepto de **"Capa 2.5"**, y aunque esta capa no existe como tal en el modelo referencia OSI se justifica al no ver a la nueva capa dentro de un "stack" de protocolos, sino como las funciones que realiza conceptualmente MPLS, proporcionando la ventaja de poder unificar la rapidez de la conmutación (característica de tecnologías de Capa 2) y la flexibilidad del enrutamiento (propia de tecnologías de Capa 3).

III PROTOCOLOS IP, TCP y UDP

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, y no uno de los estándares definidos por la ISO, IICC, u otra similar. Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la Internet se ha convertido en una de las arquitecturas de redes más difundida.

Antes de continuar, veamos la relación de esta arquitectura con respecto al Modelo de Referencia OSI de la ISO. Así como el Modelo de Referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP es definida por 4 niveles : **Capa de Enlace** [enlace y físico], **Capa de Red** [red], **Capa de Transporte** [transporte] , y **Capa de Aplicación** [sesión, presentación y aplicación]. Como se muestra en la figura 3.1:

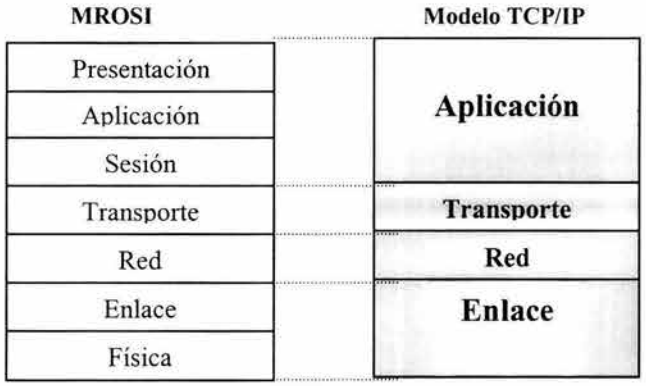


Figura 3.1

III.1 PROTOCOLO IP (INTERNET PROTOCOL)

El protocolo IP forma parte integral del modelo TCP/IP. Las tareas principales de IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que IP utiliza. Las características de este protocolo son :

- No orientado a conexión.
- Transmisión en unidades denominadas datagramas.
- Sin corrección de errores ni control de congestión.
- No garantiza la entrega en secuencia.

Formato del Datagrama

En el caso de IP se envían *Datagramas* que incluyen Datos y un Encabezado cuyo tamaño es de 20 bytes (Figura 3.1.1), en donde se insertan las *Direcciones IP o direcciones lógicas,* tanto del origen y como del destino.

Figura 3.1.1

Formato del Encabezado

El encabezado IP contiene los siguientes campos (Figura 3.1.2):

Figura 3.1.2

1. **Ver:** Versión de IP que se emplea para construir el Datagrama. (IPv4 e Ipv6).
2. **Hlen (Longitud del encabezado):** Tamaño del encabezado.
3. **TOS:** Tipo de servicio. Son 3 bits de precedencia y 5 para prioridad de los datos. La gran mayoría de los Host y enrutadores ignoran este campo.
4. **Longitud Total:** Mide en bytes la longitud de todo el Datagrama.
5. **Identificación:** Identificador único por paquete en caso de fragmentar la información.

6. **Flags:** Indica si esta fragmentada la información y si es el ultimo en haber sido fragmentado.
7. **TTL:** Tiempo de Vida del Datagrama, especifica el numero de saltos que se permite al Datagrama circular por la red antes de ser descartado.
8. **Protocolo:** Especifica el protocolo de alto nivel que se emplea para construir el mensaje transportado en el campo datos de Datagrama IP. Como TCP, UDP , etc.
9. **Checksum:** Es un campo para verificar que el paquete no este dañado. Hay que generar este campo en cada nodo intermedio debido a cambios en el TTL o por fragmentación.
10. **Dirección IP de la Fuente:** Dirección IP del equipo que envía información, 32 bits
11. **Direción IP del Destino:** Dirección IP del equipo que recibirá la información, 32 bits.
12. **Opciones IP:** Es parte del encabezado IP que puede llevar una o más opciones. Su uso es bastante raro. Entre estas opciones encontramos:
    - Uso de Ruta Estricta
    - Ruta de Origen Desconectada
    - Crear registro de Ruta
    - Marcas de Tiempo
    - Seguridad Básica del Departamento de Defensa
    - Seguridad Extendida del Departamento de Defensa
13. **Datos:** Datos

La entrega del datagrama en IP no está garantizada (no orientado a conexión) porque ésta se puede retrasar o enrutar de manera incorrecta. Por otra parte IP no contiene verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

El protocolo IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, se puede determinar su propio sistema de direccionamiento.

Conceptualmente cada dirección está compuesta por un par (RED (NetID), y Dir. Local (HostID)) en donde se identifica la red y el host dentro de la red.

Anteriormente se tenían clases (Tabla 3.1.3) A, B, C, D y E dependiendo del número de Host que tuvieran.

Clase	Rango de Direcciones
A	0.0.0.0-127.0.0.0
B	128.0.0.0-191.255.0.0
C	192.0.0.0-223.25.255.0
D	224.0.0.0.239.255.255.255
E	240.0.0.0-255.255.255.254

Tabla 3.1.3

Las direcciones de Clase D se usan con fines de multicast. La clase E su utilización es experimental. Actualmente debido a la gran demanda de IP's ya no existen clases, únicamente se utiliza un segmento de red, determinado por la mascara.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, formando un total de 32 bits. Por comodidad estos bits se representan en conjuntos de 8, como si estuviesen separados por un punto, el formato de dirección IP puede ser red.host. host. host con mascara de 8 bits o red.red.red. host con máscara de 24 bits.

Ejemplos de direccionamiento Consideremos la siguiente dirección IP en binario:

11001100.00001000.00000000.10101010 (204.8.0.170) (Dirección IP)

11111111.11111111.11100000.00000000 (255.255.224.0) (La máscara en binario)

11001100.00001000.00000000.00000000 (204.8.0.0) (La subred)

Según lo visto anteriormente, para hallar la SubRED (SubNet) tomamos la IP y considerando que todo lo que tenga 1s en la máscara se queda como esta en la IP, y todo lo que tenga 0s en la mascara se pone a 0 en la IP. Otra forma de verlo, es haciendo la operación AND lógica de la dirección IP con la máscara.

Finalmente se dice que por medio de protocolo de enrutamiento se pueden anunciar las redes IP automáticamente en los enrutadores, con el objetivo de hacer alcanzables las redes, desde otras distintas.

III.2 PROTOCOLO TCP (TRANSPORT CONTROL PROTOCOL)

Ahora veremos el segundo servicio más importante y mejor conocido como el Protocolo de Control de Transmisión (TCP) *que es la entrega confiable de información*.

TCP implementa sus servicios sobre IP. Esto significa que las tareas de control de flujo, corrección de errores, eliminación y secuenciamiento de datagramas IP, se hacen en este nivel con el fin de poder ofrecer un canal de flujo continuo a los procesos comunicantes.

Los servicios básicos de TCP son:

- Petición de apertura de una conexión
- El envío con posibilidad de colocar mensajes urgentes o de forzar el envío de un mensaje solo.
- La recepción con posibilidad de acceder a los mensajes urgentes directamente.
- El cierre de una conexión (close).

TCP debe instaurar un canal de comunicación altamente confiable, sobre una plataforma que puede no ser confiable, como ocurre en el caso de IP. Por eso, TCP está dotado de una variedad de mecanismos para manipular todos los elementos que soportan la confiabilidad en las comunicaciones. Esos mecanismos son:

- El acuse de recibo o reconocimiento (positive acknowledgment with retransmision). El módulo TCP espera un reconocimiento por cada paquete enviado. Si dicho reconocimiento no llega en un tiempo establecido, el paquete original es reenviado.
- Las ventanas deslizantes (sliding windows): Sirve para poder manipular el control de flujo de los paquetes.

Puertos, conexiones y puntos extremos.

TCP reside sobre el IP en el esquema de estratificación por capas de protocolos. TCP permite identificar el destino (Aplicación) final dentro de una máquina. Cada

puerto tiene asignado un número entero pequeño utilizado para identificarlo. Cada puerto esta orientado hacia una aplicación especifica, por ejemplo:

Puerto	Protocolo	Descripción
15	netstat	Estado de red
21	ftp	Protocolo de Transferencia de Archivos
23	telnet	Conexión por Terminal
25	smtp	Protocolo de Transporte de Correo Sencillo
80	http	Protocolo de Transferencia de Hipertexto
646	ldp	Protocolo de Distribución de Etiquetas
711	tdp	Protocolo de Distribución de Etiquetas (propietario)

Tabla 3.2.1

Encabezado TCP

A continuación se presenta el encabezado TCP (Figura 3.2.2) con sus diferentes campos:

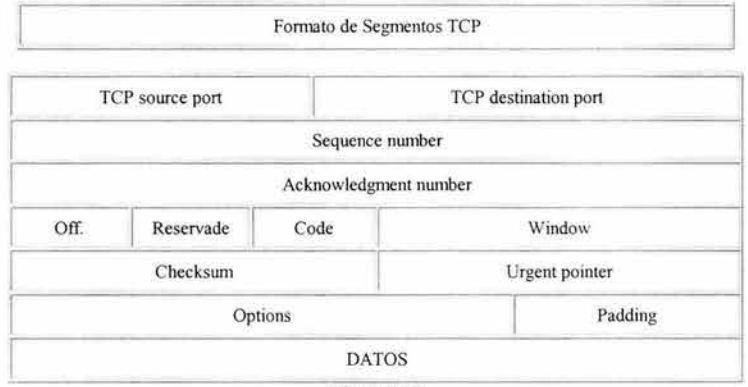


Figura 3.2.2

1. **Puerto origen y puerto destino (source port and destination port):** Son números enteros (16 bits) que designan el punto donde los procesos tienen acceso al servicio de comunicación TCP. La asignación del puerto origen de la comunicación es generalmente aleatoria, no así el puerto destino que tiene una aplicación específica.
2. **Número de secuencia (sequence number):** El número de secuencia indica la posición en el envío de datos. El número no identifica al segmento, sino a una porción de aquel envío ininterrumpido de bytes (stream), que fluye a través de una conexión TCP.

3. **Número de reconocimiento (acknowledgment number):** Se trata de un reconocimiento acumulativo de envío y recepción de segmentos.
4. **Offset**: Indica dónde termina el encabezado TCP y dónde comienzan los datos.
5. **Control o Code:** Es un campo con 6 bits, utilizados como banderas, que permiten establecer el propósito y contenido del segmento y el cómo interpretar los otros campos del encabezado. Cada bit o bandera se puede interpretar con la siguiente tabla:

SYN Sincronizar números de secuencia	**URG** El campo apuntador urgente es válido.
ACK El campo reconocimiento es válido	**PSH** Este segmento debe enviarse solo.
RST Reinicie conexión.	**SYN** Sincronizar números de secuencia.
FIN El enviar segmentos finalizó	

Tabla 3.2.3

6. **Ventana (Window):** TCP aprovecha el concepto de ventana deslizante (control de flujo), no solamente para aumentar el aprovechamiento del medio, sino también para permitir al receptor informar al emisor sobre su capacidad de almacenamiento y procesamiento. El emisor usa este valor para establecer el tamaño de su ventana de envío, el cual puede ser variable.
7. **Checksum:** Es un valor empleado para confirmar la integridad de los datos. El emisor calcula el checksum sobre los datos que enviará y lo incluye dentro del paquete. El receptor lo calcula nuevamente al recibir los datos y lo compara con el valor del emisor. Si son distintos, es altamente probable que los datos hayan sido alterados durante la transmisión.
8. **Apuntador a los datos urgentes (urgent pointer):** El emisor indica que ese segmento contiene datos urgentes.
9. **Opciones (options):** Este campo es utilizado para el diálogo entre los dos módulos TCP. Se usa, por ejemplo, para establecer el tamaño máximo de segmento a intercambiar (maximum segment size).
10. **Padding:** Relleno
11. **Datos:** Datos

III.3 PROTOCOLO UDP (USER DATA PROTOCOL)

El protocolo UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable como en IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. Este protocolo es usado para aplicaciones en tiempo real ya que en estos caso no es necesaria la retrasmisión como en TCP y se aplica en el caso de voz y video.

Encabezado UDP

A continuación se presenta el encabezado UDP Figura 3.3.1:

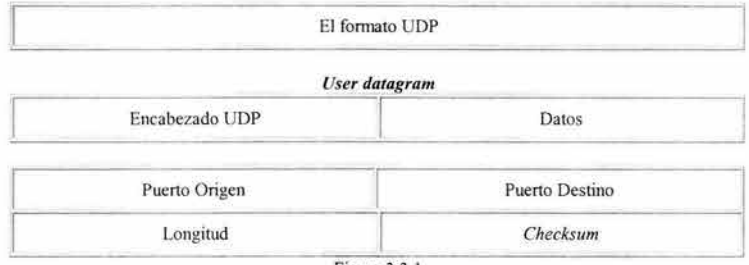


Figura 3.3.1

1. **Puerto origen y puerto destino (source port and destination port):** Son números enteros (16 bits) que designan el punto donde los procesos tienen acceso al servicio de comunicación UDP.
2. **Checksum:** Algoritmo polinomial aplicado únicamente al encabezado.
3. **Longitud:** Cantidad de bytes que hay en los datos.

La importancia de comprender este capítulo radica en conocer los aspectos relevantes del protocolo IP, ya que MPLS se basa en éste, adicionalmente entender las bases de los protocolos TCP y UDP por que son utilizados por algunos protocolos de enrutamiento y protocolos de distribución de etiquetas.

IV DESCRIPCION Y COMPARACIÓN DE TECNOLOGÍAS WAN EXISTENTES

En este capitulo nos basaremos en los conceptos del Modelo de Referencia OSI y la familia de protocolos TCP / IP para comprender el funcionamiento y características de las tecnologías.

Los aspectos de las tecnologías que se revisan son con el ánimo de entenderlas y compararlas lo mejor posible. Lo anterior con el propósito de elegir la que convenga más a nuestra red y considerar antes del diseño e implementación las necesidades inherentes a la tecnología.

A manera de introducción mencionaremos que los circuitos virtuales (VC, Virtual Circuit) son una especie de enlaces dedicados "simulados". NO existen físicamente, sino sólo desde un punto de vista lógico, pero igual que los cables reales, conectan el dispositivo del usuario con otros de su especie. Para un Proveedor de Servicio sería impensable desde un punto de vista técnico y económico tener todos lo enlaces físicos necesarios. Esto significa un ahorro económico y mayor eficiencia.

Actualmente para proporcionar el servicio de circuitos virtuales existen dos esquemas: PVC (Permanent Virtual Circuit), que se establecen en forma permanente cuando se contratan, y tienen un costo mayor debido a su alta disponibilidad.

El segundo esquema es SVC (Switched Virtual Circuit), que son circuitos que se establecen cuando el medio es requerido por el usuario mediante una negociación previa, teniendo un costo menor debido a que cuando el usuario deja de utilizar el circuito se deshabilita. Este servicio no es popular en México

IV.1 FRAME RELAY

Definición

Frame Relay fue concebido originalmente como un protocolo para uso sobre interfases ISDN (Interfases para la Red Digital de Servicios Integrados). Las propuestas iniciales a este efecto fueron presentadas a la Internacional Telecommunication Union (ITU - T) en 1984. En esta época los trabajos sobre Frame Relay también fueron emprendidos por el American National Standards Institute (ANSI).

Frame Relay es una tecnología de conmutación rápida de paquetes basada en estándares internacionales que puede utilizarse como un protocolo de transporte y/o como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones, ofrecido generalmente por las compañías telefónicas.

En este tipo de protocolo de transmisión de paquetes, los paquetes son transmitidos en ráfagas de alta velocidad a través de una red digital, y son fragmentados en unidades de transmisión llamadas frames. Inicialmente ocupaba una banda estrecha en modo de paquetes, y actualmente proporciona Anchos de Banda de 2 Mbps a 45 Mbps. Para ocupar Frame Relay se requiere una conexión exclusiva durante el periodo de transmisión.

En un inicio no se podía trasmitir señales de Video y audio, ya que estos requieren de un flujo constante de transmisión de datos, mas adelante se mencionara la razón de esta limitante.

IV.1.1 TOPOLOGIA BÁSICA

Se puede observar en la Figura 4.1.1 los elementos básicos que conforman la topología física básica de Frame Relay, en donde la nube de Frame Relay, consta de Switches FR básicamente, aunque también pueden existir enrutadores que ocupen la tecnología de Frame Relay, estos generalmente se ocupan para tener interacción con la red IP pública, es decir en la frontera de la red.

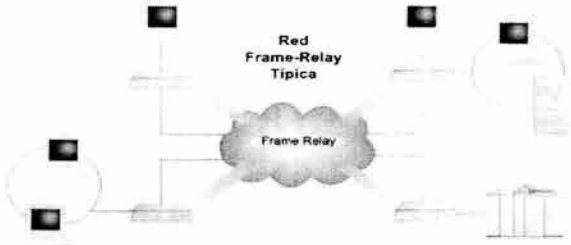


Figura 4.1.1

Por otro lado tenemos los elementos de aplicación como pueden ser servidores y redes LAN. Como se observa en la figura 4.1.1 este caso una serie de equipos pueden estar comunicándose mediante la red Frame Relay.

IV.1.2 CARACTERÍSTICAS DE FRAME RELAY

Frame *Relay trabaja en Capa 2 (Enlace)* del MROSI, por lo que no son necesarios enrutadores que procesen la información. Es una tecnología que puede proporcionar un método más rápido y de costo menor para acoplar los equipos de red. Frame Relay trabaja con Switches primordialmente.

En Frame Relay los datos son divididos en paquetes de tamaño variable los cuales incluyen información de direccionamiento. Los paquetes son entregados a la Red Frame Relay, la cual los transporta hasta su destino específico sobre una conexión virtual asignada (Circuito Virtual).

Frame Relay es usado mayoritariamente para conmutar protocolos de Redes de Area Local (LAN) tales como IPX o TCP/IP, es decir la interconexión de redes LAN, pero también puede ser usado para transportar tráfico asíncrono, SNA o incluso Voz. Su característica primaria más competitiva es el bajo costo. Frame Relay ha evolucionado, proporcionando la integración en una única línea de los distintos tipos de tráfico de datos y Voz y su transporte por una única red que responde a las siguientes necesidades:

- Alta velocidad y bajo retardo
- Eficiencia
- Transporte integrado de distintos protocolos de Voz y datos

- Conectividad "todos con todos"
- Simplicidad en la gestión

Frame Relay está orientado a conexión, lo que significa que, para poder tener comunicación entre dos puntos primero es necesario realizar una negociación entre los dos puntos, para establecer un Circuito Virtual; por otro lado Frame Relay permite compartir *varias conexiones virtuales a través de una misma interfaz física con lo cual es posible conectar múltiples localidades remotas entre sí*, sin necesidad de equipo adicional, ni costosos enlaces dedicados punto a punto. Solamente es necesaria una conexión física entre cada localidad remota y la Red Frame Relay.

Frame Relay *multiplexa estadísticamente paquetes o tramas* hacia destinos diferentes por una sola interfaz física, de esta forma hace uso eficiente del Ancho de Banda. Esta es la razón por la cual inicialmente Frame Relay se ocupaba únicamente para datos, ya que enviaba información de forma estadística y no en tiempo real como lo requieren Voz y Video, actualmente ya es posible enviar Voz y Video, porque se tienen mayores Anchos de Banda pudiendo ofrecer Calidad de Servicio (QoS), aunque es de forma muy rudimentaria.

Frame Relay puede entenderse mejor cuando se compara con el protocolo IP. En la figura 4.1.2 se ilustran los siete niveles OSI, indicando los niveles utilizados por IP y Frame Relay.

Figura 4.1.2
Niveles utilizados por Frame Relay e IP

Las funciones de capa 2 que tiene Frame Relay son las siguientes:

- Direccionamiento
- Creación de Tramas
- Control de errores
- Gestión de trafico
- Gestión de congestión

IV.1.3 FORMATO DE TRAMA

En esta tecnología **no se establece una longitud máxima de trama**, pero debe ser un *múltiplo entero de octetos* (la trama está alineada a 8 bits), lo cual se puede observar en la Figura 4.1.3 Conviene destacar que el protocolo define también el orden de transmisión de los bits de la trama por línea. Un sistema final o intermedio que reciba una trama debe saber el significado de cada bit que le llega, y este significado depende del orden de ese bit dentro de su trama.

Trama Basica de Frame Relay

Figura 4.1.3

- **CRC** (también llamado FCS): **Código de detección de errores**. Es un código cíclico. Necesario para detectar una *trama con error, y descartarla.*
- **DATOS:** En este campo es donde van los datos de la capa superior, es decir, esta información se agrega en la trama y, en recepción, se pasa directamente a la capa superior. Su longitud máxima no está definida en el estándar de facto (no está normalizada), pues no se pudo llegar a un acuerdo. Normalmente los operadores de redes FR la sitúan alrededor de 1600 bytes. Esta gran diferencia con X.25 (128 octetos) es debida a la escasa probabilidad de error (P_e).
- **FLAG:** Tiene el mismo formato que en LAB-B (01111110), y también se utiliza para separar tramas consecutivas. Cuando no hay tramas que transmitir, se generan tramas como estas continuamente.
- **CAMPO DE CONTROL:** Llamamos campo de control (Figura 4.1.4) a los bytes que siguen al Flag y que están por delante de los Datos de usuario.

Puede tener varios formatos, pero normalmente suele tener 16 bits de longitud (2 octetos):

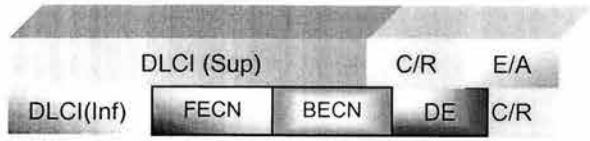


Figura. 4.1.4 Campo de control

- **DLCI:** Data Link Circuit Identifier. Estos diez bits son el identificador de conexión de enlace de datos. **Permite definir hasta 1024 circuitos virtuales.** Como ya se había dicho la función de multiplexación se realiza en el nivel 2, y gracias al **DLCI se identifica al canal lógico al que pertenece cada trama.**
- **E/A:** Extended Address. Campo de extensión de dirección. Puesto que se permiten más de dos octetos en el campo de control, este primer bit de cada octeto indica (cuando está marcado con un '0') si detrás siguen más octetos o bien (cuando está marcado con un '1') si se trata del último del campo de control. Emplear más de dos bytes resulta bastante infrecuente y se utiliza en el caso de que la dirección de multiplexación (en el campo DLCI) supere los 10 bits.
- **C/R:** Bit de Comando / Respuesta. No es un bit utilizado por la red. **Se introduce por compatibilidad con protocolos anteriores**, como los del tipo HDLC. Cuando el protocolo de enlace es fiable, utilizan este bit.
- **FECN, BECN** y **DE:** Bits para control de congestión

IV.1.4 DISPOSITIVOS

Los dispositivos conectados a una WAN Frame Relay se dividen en dos categorías principales: Equipo terminal de datos (DTE) y Equipo de transmisión de datos (DCE). Los DTE se encuentran generalmente ubicados en las instalaciones de

propiedad de un cliente. Ejemplos de dispositivos DTE son las terminales, computadoras personales, enrutadores y puentes. Los DCE son generalmente dispositivos de conmutación que pertenecen a las compañías telefónicas, pero también pueden ser propiedad de un cliente. El propósito del equipo DCE es proporcionar servicios de temporización y conmutación en una red, dispositivos que generalmente transmiten datos a través de la nube de la WAN. En la mayoría de los casos, ellos mismos son switches de paquetes Frame Relay.

IV.1.5 ESQUEMA DE FUNCIONAMIENTO

Es de nuestro interés, con ayuda de lo definido anteriormente, saber cómo la información es enrutada para poderla llevar de un punto a otro y que ésta llegue correctamente.

Supongamos que se tiene la siguiente red (Figura 4.1.5) Frame Relay:

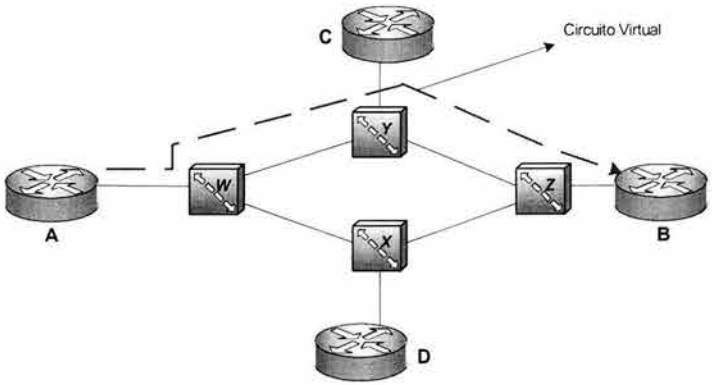


Figura 4.1.5

Inicialmente se tiene que tener una conexión o Circuito Virtual para que pueda haber intercambio de información, como se establece en la Figura 4.1.5con la línea punteada que une al enrutador "A" con el enrutador "B", esta conexión puede ser de tipo conmutada, aunque generalmente se ocupa los Circuitos Permanentes. Se puede

ver que cada uno de los Switches son los encargados de conmutar la información dentro de la red.

Cuando el enrutador "A" desea enviar información (Figura 4.1.6) a algún otro enrutador como al "B", "C" o "D". Por ejemplo el enrutador "A" se quiere comunicar con "B", inicialmente "A" debe introducir dentro del campo DLCI el identificador que lo une con el Switch "W", que se observa en la Figura 4.1.6, básicamente el DLCI esta asociado con un segmento del Circuito Virtual inicial, en este caso el que une a "A" con "W", es DLCI=400, este identificador esta asociado a un puerto de "W", en este Switch es el puerto 25, el cual esta conectado con A; el Switch "W" aplica el CRC al campo de control y si es correcta acepta el frame, luego verifica el campo DLCI y como sabe por que puerto lo recibió el frame, entonces hace su consulta con su tabla y como se observa el Switch sabe que lo tiene que enviar por el puerto 30 con el DLCI=500 que es el que identifica al segmento de circuito que une a "W" con "Y".

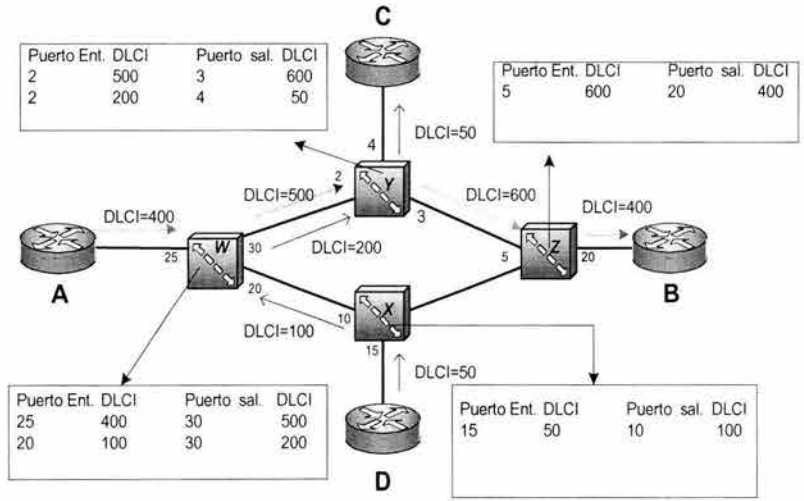


Figura 4.1.6

El switch "Y" recibe al frame por el puerto 2 y aplica CRC al Frame, si es correcto lee el campo DLCI y lo asocia por el puerto que lo recibió, lo compara en su tabla, (Figura 4.1.6) le introduce el nuevo DLCI=600 y lo envía por el puerto indicado en la tabla, en este caso el puerto 3. A su vez el Switch "Z" realiza el mismo procedimiento con el frame, identifica el puerto por el que recibió el frame que es el

5, aplica CRC, revisa en su tabla y observa que lo tiene que enviar por el puerto 20 con el DLCI=400. Y finalmente se completa la transmisión de la información.

Cabe destacar que por lo regular los dos equipos terminales (extremos del PVC) generalmente están identificados con el mismo DLCI, esto para su mejor administración, para este ejemplo el DLCI=400 identifica la comunicación de "A" con "W" y de "Z" con "B", sin embargo todos los DLCI pueden ser iguales en el PVC; en caso de que esto suceda, se le conoce como *direccionamiento global* esto quiere decir que todo el Circuito Virtual estará identificado por el mismo DLCI.

Lo mismo sucede con cualquier Circuito Virtual que conecte a dos enrutadores, por ejemplo en el caso de "D" con "C" (Figura 4.1.6), supongamos que ya se estableció el Circuito Virtual entre "D" y "C", si "D" desea enviar información a "C", se realiza el mismo procedimiento, que el anterior; X recibe por el puerto 15 con DLCI=50, éste lo envía por el puerto 10 con DLCI=100, a su vez W recibe por el puerto 20 con DLCI=100 y consultando su tabla envía por el puerto 30 con DLCI= 200. Como se puede observar en este momento, el enlace que existe W con Y contiene dos conexiones virtuales DLCI=500 y DLCI=200, esto quiere decir que por una conexión física puede haber varias conexiones virtuales. Ya por ultimo el Switch "Y" envía su paquete a "C".

Finalmente con lo anterior decimos que Frame Relay entre sus funciones mas importantes tiene las siguientes características.

- Hay múltiples Circuitos Virtuales, asignando un DLCI a cada par de DTE/DCE, estos Circuitos Virtuales son identificados por el DLCI sirven para la administración de la red.
- Los DLCI tienen un significado local o global dependiendo de la configuración del PVC.
- Los equipos de conmutación relacionan valores de DLCI a puertos de salida del equipo y fungen como una tabla de enrutamiento.
- Se establece el camino completo antes de enviar el frame.
- Frame Relay no implementa todas las funciones de la capa de enlace de OSI.

- Realiza detección de errores y descarta los paquetes dañados, por lo tanto no puede realizar retrasmisiones.

IV.1.6 VENTAJAS

- Frame Relay permite una mayor velocidad
- Permite que un mismo circuito sirva a varias conexiones (reduciendo, el número de enlaces, y por tanto el costo total.
- Se limita a eliminar parte de la carga de protocolo y funciones de IP.
- Está orientado a conexión, ya que todas las tramas siguen la misma ruta a través de la red, basadas en un identificador de conexión, lo cual proporciona control estático sobre el tráfico.

IV.1.7 DESVENTAJAS

- Debido a que no hay corrección de errores en la conmutación, los medios de transmisión deben ser lo mas confiables posible para que no haya errores en el medio (no informa sobre tramas perdidas ni trata de recuperar tramas erróneas), de esto se encarga el protocolo de capa 4 TCP como ya habíamos mencionado.
- Los nodos conectados a Frame Relay no deben ser terminales tontos, sino que emplearán sus propios protocolos para control de flujo, recuperación de errores y envío de ack's.
- Sigue siendo una tecnología antigua, ya que no inventa nuevos protocolos ni mejora los dispositivos de la red.
- Las redes orientadas a conexión son susceptibles de perder la información si el enlace entre el nodo conmutador de dos redes falla. Aún cuando la red intente recuperar la conexión, deberá de ser a través de una ruta diferente, lo que cambia el retraso extremo a extremo y puede no ser lo suficientemente rápido como para ser transparente a las aplicaciones.

- Su administración se vuelve compleja ya que solo existen dos tipos de topología: conexión estrella o full mesh (todos contra todos), lo que resulta complicado cuando se agregan nuevos nodos de clientes de la red. Con esto podemos decir que la red Frame Relay es difícilmente escalable y flexible.

IV.2 ATM –ASYNCHRONOUS TRANSFER MODE- (MODO DE TRANSFERENCIA ASÍNCRONA)

Definición

En un principio ATM fue pensado como el corazón de las redes digitales de servicios integrados de Banda Ancha (B-ISDN), y debido a su versatilidad en la conmutación de paquetes de longitud fija (denominadas celdas ATM), posibilitadas para soportar la demanda de un gran Ancho de Banda, su uso se ha extendido en gran medida; necesidad originada por la demanda de Ancho de Banda en conexiones a Internet principalmente.

Ésta es una tecnología de transporte orientada a conexión, puede soportar Circuitos Permanentes o Conmutados. Surge como respuesta a la necesidad de transportar un universo diferente de servicio de Voz, Vídeo por un lado y datos por otro de manera eficiente usando una simple tecnología de conmutación y multiplexación.

ATM se adecua a las diferentes necesidades de transporte de información en aspectos importantes como son su capacidad de manejo de volúmenes de datos, flexibilidad de conmutación y facilidades para el operador. Además propone una solución combinando la simplicidad de la multiplexación por división en el tiempo encontrada en la conmutación de circuitos, con la eficiencia de las redes de conmutación de paquetes con multiplexación estadística orientada a conexión.

Los equipos especializados (conmutadores ATM), aseguran que el tráfico de grandes volúmenes sea conmutado al destino correcto.

Las aplicaciones que pueden utilizar ATM como base de transporte de información van desde servicios públicos de salud (Videoconferencias médicas), redes financieras interconectadas con los entes de intermediación y validación, vídeo en demanda para hogares con alta definición de imágenes y calidad del audio de un CD, etc.

Un beneficio importante de mencionar es que en ATM es posible pagar solamente por la carga de celdas que es efectivamente transportada y conmutada para el usuario.

La forma en que transfiere la información es a través de celdas de 53 bytes de longitud y su funcionamiento de describe más adelante.

IV.2.1 TOPOLOGÍA BÁSICA

En la figura 4.2.1 se muestra la topología básica de la red de switches ATM junto con las redes del cliente

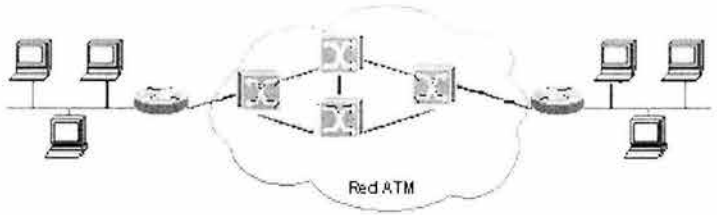


Figura 4.2.1

IV2.2 CELDAS Y ENVÍO

Jerarquías de conexión:

Existen dos niveles jerárquicos en los que ATM basa su funcionamiento; estos son:

- Virtual Paths (VP): Traducidos como trayectos virtuales, hacen referencia al camino (orden de conmutaciones) entre equipos ATM por donde transitan los datos.
- Virtual Channels (VC): Contenidos en los Virtual Paths, los canales virtuales son la conceptualización lógica de un flujo de información específico entre equipos ATM.

Figura 4.2.2

Una conexión ATM, consiste de "celdas" de información contenidas en un Circuito Virtual (VC). Estas celdas provienen de diferentes fuentes representadas

como generadores de bits a tasas de transferencia constantes como la Voz y/o a tasas variables tipo ráfagas (*bursty trafic*) como los datos.

Cada celda está compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para transporte de información y los restantes para uso de campos de control (encabezado) con información de identidad y destino. La celda es identificada por dos identificadores dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión:

- Virtual Circuit Identifier (VCI): Es el identificador del Virtual Circuit al que pertenece la celda.
- Virtual Path Identifier (VPI): Identifica el Virtual Path al que pertenece la celda

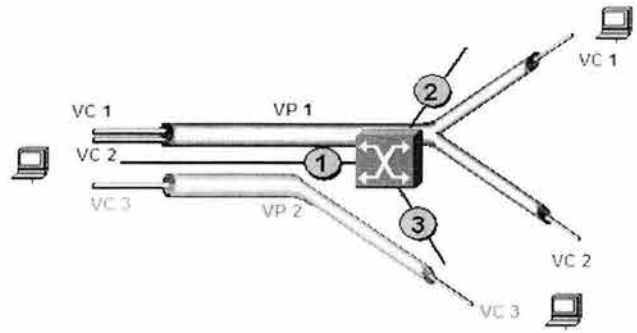


Figura 4.2.3

Interfases

Para la comunicación en la red, se diferencian dos tipos de interfases:

- User to Network Interfase (UNI): La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente (Customer Premises Equipment), tal como hubs o enrutadores ATM y la red de área amplia ATM (ATM WAN). Existe entre el usuario y la Red
- Network to Network Interfase (NNI): La NNI define la interfase entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfase entre una red ATM de un usuario privado y la red ATM de un proveedor público (carrier).

Específicamente, la función principal de ambos tipos de encabezados de UNI y la NNI, es contener los *Virtual Path Identifiers* y a los *Virtual Circuit Identifiers* como

identificadores para el enrutamiento y la conmutación de las celdas ATM. Su utilización se observa entre red y red.

Dependiendo si el switch pertenece o esta localizado en las instalaciones de un cliente o pertenece y esta operado por una institución pública, UNI y NNI pueden subdividirse en:

	PUBLICA	PRIVADA
UNI	Conecta un dispositivo final o switch ATM privado con un switch ATM público.	Conecta un dispositivo final con un switch ATM privado
NNI	Conecta dos switches ATM dentro de la misma organización pública	Conecta dos switches ATM dentro de la misma organización privada

Tabla 4.2.4

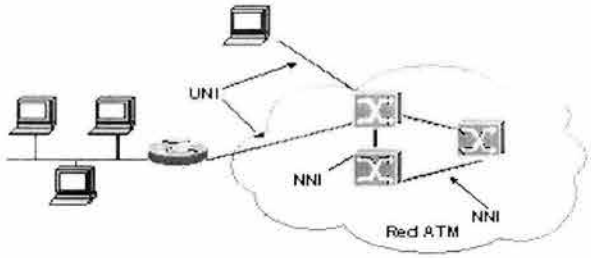


Figura 4.2.5

Formato de celda y encabezado

Los campos en las celdas ATM UNI y NNI varían ligeramente. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local (ya que pueden ser cambiados de interfase a interfase), pero su estructura general es:

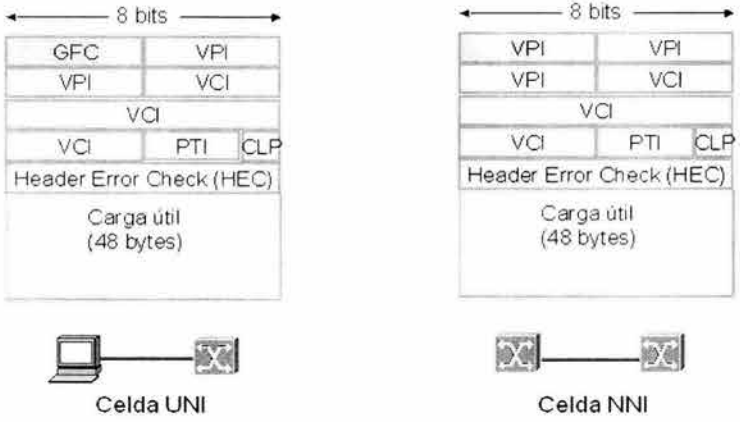


Figura 4.2.6

donde:

Campo	Características
GFC *(Generic Flow Control)*	No usado
VPI *(Virtual Path Identifier)*	Hasta 256 (UNI) o 4096 (NNI)
VCI *(Virtual Channel Identifier)*	Hasta 65536
PTI *(Payload Type Identifier)*	3 bits. Puede ser de usuario o gestión
CLP *(Cell Loss Priority)*	1 bit
HEC *(Header Error Check)*	Es un CRC de todo el encabezado, de 8 bits

Tabla 4.2.7

Dispositivos

Consisten en:

- Switches ATM: Responsables del tránsito de las celdas a través de la red ATM; acepta celdas de entrada de un dispositivo final u otro switch, entonces lee y actualiza la información en el encabezado de la celda e inmediatamente la conmuta a una interfase de salida hacia su destino.
- Dispositivos finales ATM: Contienen una interfase ATM. (enrutadores, estaciones de trabajo, LAN switches, etc.)

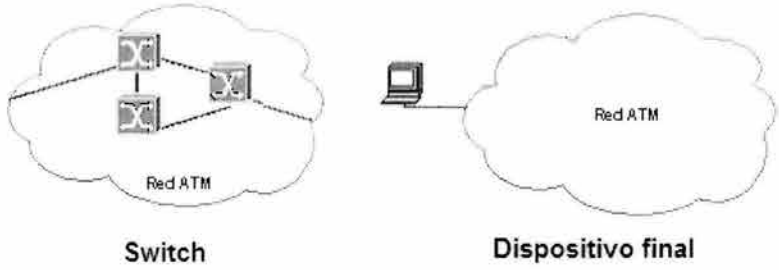


Figura 4.2.8

IV.2.3 FUNCIONAMIENTO

La conmutación se realiza atendiendo a las relaciones entre los identificadores VPI/VCI y los puertos de Entrada/Salida correspondientes. Los identificadores VPI/VCI se crean al generar el Circuito Virtual en el momento de la conexión o el Circuito Permanente en la configuración del conmutador, bajo la filosofía "Primero que entra es el primero que sale" (FIFO por sus siglas en inglés).

Los identificadores VPI/VCI, al ser asignados por cada conmutador son modificados en cada salto de conmutación realizado en el trayecto. Un identificador puede utilizarse sólo una vez en cada puerto para evitar confusión en las trayectorias.

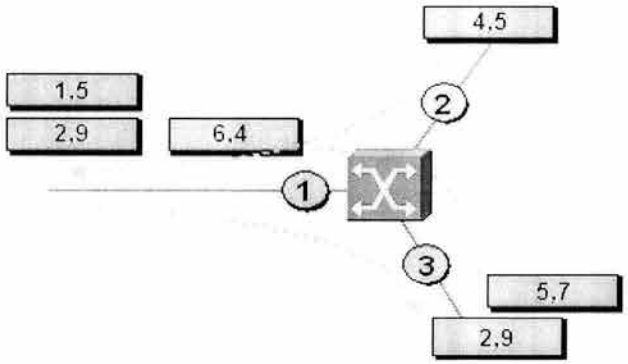


Figura 4.2.9

Entrada		Salida	
Puerto	VPI - VCI	Puerto	VPI - VCI
1	2,9	2	4,5
2	4,5	1	2,9
1	1,5	3	5,7
3	5,7	1	1,5
1	6,4	3	2,9
3	2,9	1	6,4

Tabla 4.2.10

En los conmutadores se crean tablas que contienen Circuitos Virtuales por los que viajan las celdas.

La técnica ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), similar a la técnica TDM. Sin embargo, ATM llena cada slot con celdas de un Circuito Virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes.

El proceso puede ser ejemplificado con la figura siguiente:

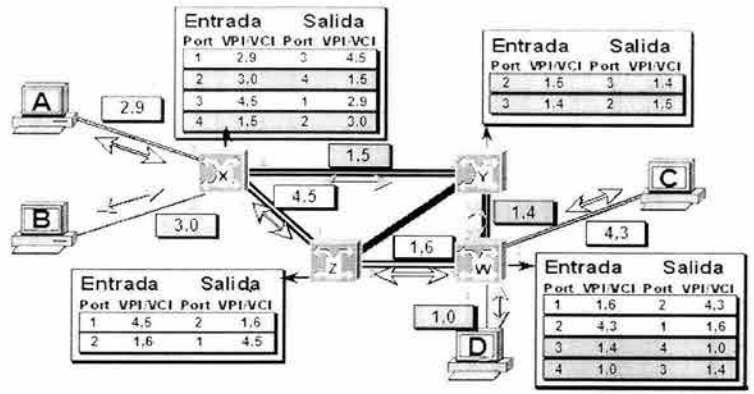


Figura 4.2.11

Se observa que el Circuito Virtual representado en color blanco se extiende entre las terminales "A" y "C", mientras que el trayecto gris va de "B" a "D". En ambos casos se observa que en cada elemento ATM de conmutación de la red se tiene una tabla con la combinación de VPI y VCI especifico como un identificador relacionado con el puerto de entrada o salida del dispositivo.

Dado que un VC representa el Circuito Virtual generado entre hosts y un VP el trayecto que las celdas seguirán entre conmutadores, podemos representarlo como:

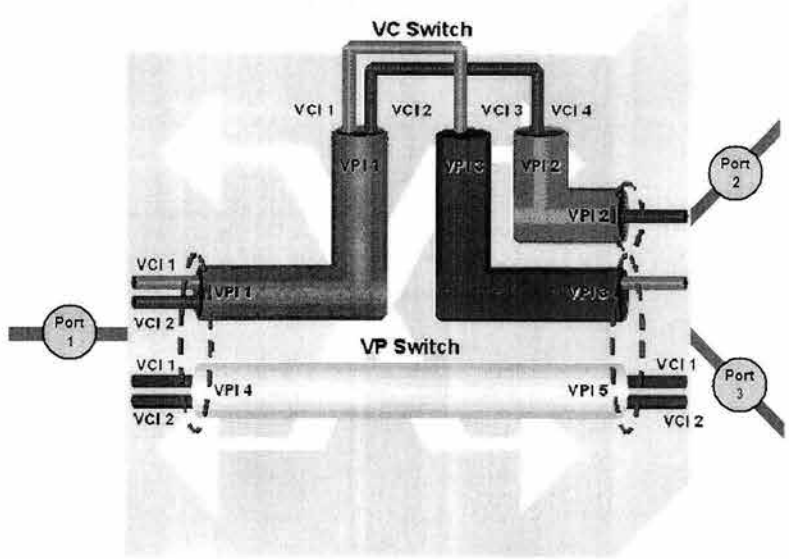


Figura 4.2.12

Como se observa, en un conmutador ATM puede realizarse el proceso de conmutar VPs y VCs con el fin de redirigir el flujo de celdas que ingresan en los puertos de entrada hacia el puerto de salida correspondiente en función del destino especificado para cada celda, pudiendo formar así nuevos VPs o VCs.

Realización de Circuitos Virtuales:

Punto a punto:

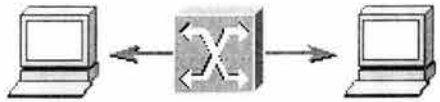


Figura 4.2.13

Punto a Multipunto (*Broadcast*):

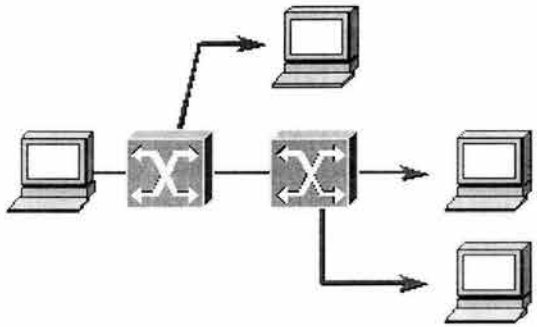


Figura 4.2.14

Parámetros

El servicio de la red puede estar restringido por parámetros de:

- Tráfico: Compromiso del usuario de no exceder el límite de datos de transmisión convenido con el operador
- Servicio: Compromiso del operador de garantizar una tasa mínima de disponibilidad de transferencia de información.

Los parámetros anteriores son configurables a razón de las especificaciones del servicio contratado, por lo que para cada conexión y sentido del flujo de datos se establecen parámetros diferentes.

Categorías de Tráfico

Categoría	Características
Constant Bit Rate (CBR)	Simula línea punto a punto. Reserva estricta de capacidad. Flujo constante con mínima tolerancia a ráfagas.
Variable Bit Rate real time (VBR-rt)	Asegura un flujo medio y un retardo. Permite ráfagas
Variable Bit Rate no real time (VBR-nrt)	Asegura un flujo medio pero no retardo. Permite ráfagas.
Available Bit Rate (ABR)	Asegura un flujo mínimo, permite usar capacidad sobrante de la red. Incorpora control de congestión
Unspecified Bit Rate + (UBR+)	Intenta conseguir un flujo mínimo. Usa el sobrante.
Unspecified Bit Rate (UBR)	No asegura nada. Usa flujo sobrante.

Figura 4.2.15

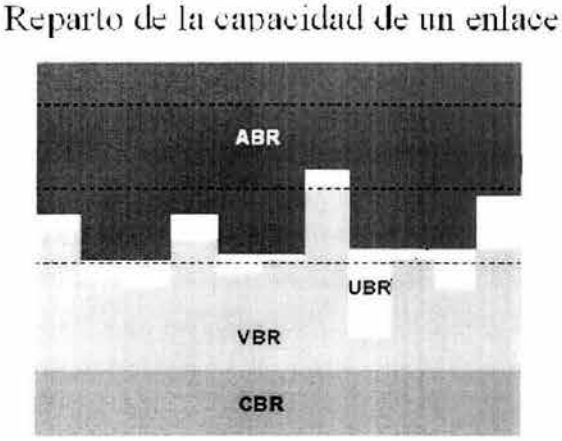


Figura 4.2.16

IV.2.4 CONMUTACIÓN

Al aplicar el esquema de conmutación básica utilizando los identificadores VPI y VCI, aunado a criterios de tráfico tales como consideraciones de capacidad o velocidad del enlace se tiene el criterio básico de enrutamiento en cada dispositivo de conmutación ATM, el cual dirigirá el flujo de datos de sus puertos de entrada hacia alguno de sus puertos de salida en función de los identificadores antes citados.

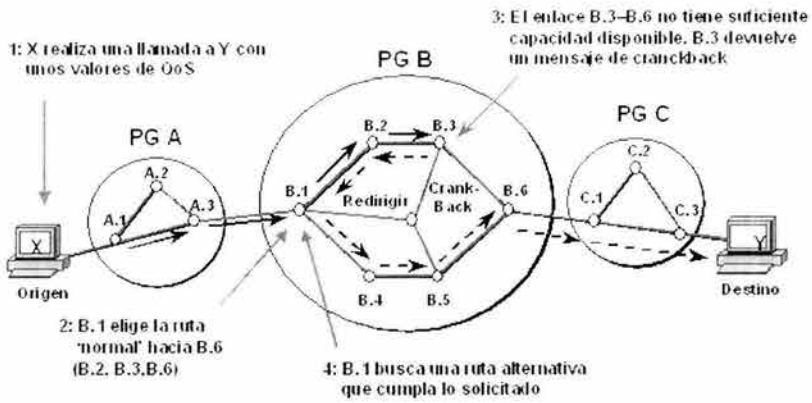


Figura 4.2.17

De la figura anterior se observa la ruta que tomarán los datos, la cual es formada en cada dispositivo de conmutación y depende de especificaciones de tráfico del administrador de la red si se trabaja con Calidad de Servicio.

Se utiliza el protocolo de enrutamiento Privete Network – Network Interfase (PNNI), el cual permite mayor fiabilidad, pero no reparto de tráfico (orientado a conexión). Normalmente empleado en conmutadores, pero puede utilizarse también en hosts dual-homed (redundancia).

Utiliza direcciones formato NSAP. Puede contener hasta 105 niveles jerárquicos. Abarca el enrutamiento intra e inter-Sistemas Autónomos.

Su utilización solo tiene sentido si existe más de un camino posible (red mallada) o se pueden crear SVC's (señalización)

Modelo lógico

El funcionamiento de ATM se basa en un modelo lógico, el cual abarca la Capa Física y parte de la Capa de Enlace del MROSI.

Planos:

El modelo ATM está compuesto por tres planos que abarcan todas las capas:

- Control: Responsable de generar y administrar solicitudes de señalización.
- Usuario: Responsable de administrar la transferencia de información
- Administración: Se divide en dos planos más:

- Administración de capas (Layer Management): Administra funciones específicas de cada capa como la detección de fallas y problemas con los protocolos.
- Administración de planos (Plane Management): Administra y coordina funciones relativas o el sistema completo; cumple un papel de administrador global del sistema.

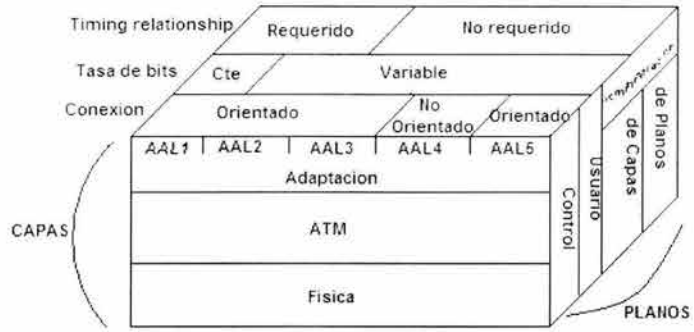


Figura 4.2.18

Capas:

Capa Física (Physical Layer) (PHY)

Define las interfases físicas con los medios de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. Provee transmisión de celdas ATM sobre un medio físico que conecta dispositivos ATM.

Tiene cuatro funciones:

- Convertir bits en celdas.
- Controlar la transmisión y recepción de bits sobre el medio físico.
- Rastrear los límites de las celdas ATM.
- Empaquetar las celdas en el tipo apropiado de frame de acuerdo al medio físico.

A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente del transporte físico.

Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), T3/E3, TI/EI o aún en modems de 9600 bps.

Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos:

- Subcapa física dependiente del medio (PMD):
- Subcapa de convergencia de transmisión (TC).

Capa ATM

La capa ATM (ATM Layer) combinada con la capa de Adaptación ATM (AAL), es análoga a la Capa de Enlace del MROSI.

La capa ATM es responsable de establecer conexiones y pasar las celdas por la red ATM. (Todo esto lo hace con la información del encabezado de cada celda ATM).

Define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM. Esta capa es independiente del servicio.

El formato de una celda ATM es muy simple. Consiste de 5 bytes de encabezado y 48 bytes para información.

Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red.

Capa de Adaptación ATM (AAL)

La capa de Adaptación de ATM yace entre la capa ATM y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles de la capa ATM.

Su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos, (circuit emulation), Vídeo, Audio,etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes.

La capa de Adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. Juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Su función principal es convertir flujos de celdas en formatos que pueden ser usados por un amplio rango de aplicaciones.

La información transportada por la capa de Adaptación se divide en cuatro tipos de servicio AAL **(Protocolos de transporte AAL)** según las propiedades siguientes:

- Que la información que esta siendo transportada dependa o no del tiempo.
- Si la tasa de bits es constante o variable.
- Modo de conexión.

Dichos servicios son:

- AAL-1: Se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. Provee recuperación de errores e indica la información con errores que no podrá ser recuperada.
- AAL-2: Se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que ésta puede recuperarse en el destino. Provee recuperación de errores e indica la información que no puede recuperarse.
- AAL-3: Se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. Puede ser dividido en dos modos de operación: Fiable y No Fiable.
- AAL-4: Se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar a AAL3 y también puede operar en transmisión fiable y o fiable. Provee la capacidad de transferir datos fuera de una conexión explícita.

AAL 2, AAL 3/4 y AAL 5 manejan varios tipos de servicios de datos sobre la base de tasas de bits variables tales como Switched Multimegabit Data Service (SMDS), Frame Relay o tráfico de redes de área local (LAN). AAL 2 y AAL 3 soportan paquetes orientados a conexión.

Los tipos de servicio AAL constan de dos subcapas:

- Capa de Segmentación y Reensamblaje (Segmentation And Reassembly 'SAR'): Esta capa recibe los datos de la capa de Convergencia y los divide en trozos formando los paquetes de ATM. Agrega el encabezado que llevará la información necesaria para el reensamblaje en el destino. Se encarga de obtener y extraer los datos de las aplicaciones.

• Capa de convergencia (Convergence Sublayer 'CS'): En esta capa se calculan los valores que debe llevar el encabezado y los payloads del mensaje. La información en el encabezado y en los datos depende de la clase de información que va a ser transportada. Se encarga de fragmentar los datos para generar las celdas de longitud variable, o de reensamblar celdas para recuperar la información proveniente de varias aplicaciones; Es dependiente del servicio.

Puede utilizarse un protocolo AAL diferente para cada VCC, pero el mismo en sus extremos. No se define en los conmutadores, sino en los hosts. Una de sus utilidades es que se tiene lo posibilidad, basado en conmutadores AAL, de implementar un descarte inteligente de celdas.

IV.2.5 VENTAJAS

• En comparación con una red IP tradicional, la velocidad de tránsito de los datos se ve incrementada.

• Mayor seguridad en el establecimiento de circuitos y transmisión de datos a través de ellos, por su carácter orientado a conexión.

IV.2.6 DESVENTAJAS

• Mayor costo que una red IP tradicional.

• Necesidad de dispositivos específicos para esta tecnología.

• Flexibilidad reducida al ser una tecnología orientada a conexión.

• No existen mecanismos de corrección de errores en esta tecnología, lo cual hace necesario un medio altamente confiable (caro).

IV.3 MPLS -MULTI PROTOCOL LABEL SWITCHING- (MULTIPROTOCOLO DE CONMUTACIÓN DE ETIQUETAS)

Definición

Del inglés Multi Protocol Label Switching o Multiprotocolo de conmutación de Etiquetas. MPLS es un estándar emergente del IETF que surgió para unificar diferentes soluciones de conmutación multicapa, propuestas por distintos fabricantes como lo son técnicas de "conmutación IP" (IP switching) o "conmutación multicapa" (multilayer switching).

También sustituye a una serie de tecnologías propietarias entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Enrutador (CSR) de Toshiba, creados en los 90´s.

La tecnología MPLS permite construir una ruta, entre un punto de salida y un destino, o entre un grupo de salida y un grupo de destino (multicast), a través de un camino o Circuito Virtual. Esta tecnología está basada en la colocación de "etiquetas" en los paquetes que entran a la red MPLS y que van a avanzar de enrutador a enrutador a lo largo de un trayecto específico y predefinido, llamado "LSP" (Label Switched Path: Trayecto Conmutado por Etiquetas o Circuito Virtual). Las etiquetas pueden indicar varios parámetros:

• Un trayecto predefinido

• La identidad del emisor (una fuente)

• La identidad del destinatario (un destino)

• Una aplicación

• Una Calidad de Servicio, funciones de Ingeniería de Tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente), Policy Routing, Servicios de VPN.

La creación de trayectos de extremo a extremo mejora mucho la rapidez de conmutación de los equipos del núcleo, ya que sus listas de rutas, se limitan a una serie de instrucciones simplificadas. Sobre todo, MPLS permite ofrecer a IP, un modo circuito similar al de las tecnologías de red más antiguas, como Frame Relay o ATM

pero sin los inconvenientes de estos mismos, como, poner en práctica políticas de enrutamiento específicas a ciertos flujos. De esta forma, hace posible la implantación de niveles de servicio y de Calidad de Servicio (QoS), así como de una Ingeniería de Tráfico evolucionada. MPLS facilita la implementación de Redes Privadas Virtuales VPN´s.

Debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de "*routing y forwarding*" en las redes IP, lo que implica una evolución en la forma de construir y gestionar estas redes. Su principal objetivo es construir redes flexibles y escalables con un incremento en el desempeño y estabilidad. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF, es decir la rapidez no era la principal causa de la implementación de MPLS.

Los objetivos establecidos por ese grupo en la elaboración del estándar fueron que MPLS debia:

- Funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- Soportar el envío de paquetes tanto unicast como multicast.
- Ser compatible con el Modelo de Servicios Integrados del IETF.
- Permitir el crecimiento constante de la Internet.
- Ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

IV.3.1 CONCEPTO Y CARACTERÍSTICAS DE MPLS

En el plano conceptual, MPLS es una tecnología de enrutamiento intermedio entre la Capa de Enlace (Capa 2 OSI) y la Capa de Red (Capa 3 OSI) capaz de asociar la potencia de la conmutación, con la flexibilidad del enrutamiento logrando la integración de las Capas 2 y 3. Asigna a los frames de cada flujo una etiqueta única que permite una conmutación rápida en los enrutadores intermedios (solo se mira la etiqueta, "no" la dirección de destino IP), estas etiquetas definen el Circuito Virtual por toda la red.

Las etiquetas, que son la base de identificadores específicos, son distribuidas usando protocolos de distribución de etiquetas LDP (Label Distribution Protocol), en el caso de enrutamiento se ocupan protocolos como BGP, IS-IS y OSPF. Cada

paquete de datos es encapsulado llevando un encabezado en el cual esta la etiqueta y que define su trayecto durante su trayecto del origen al destino. La conmutación de alta velocidad de datos es posible porque las etiquetas son de longitud fija y son insertadas al principio mismo del paquete y pueden ser usadas por el hardware para cambiar paquetes rápidamente entre enrutadores.

Cabe destacar que MPLS tiene dos modos de operación, uno de ellos es **Cell-Mode** que esta orientado hacia una ambiente con tecnología ATM (los paquetes son transportados en celdas ATM), y por otro lado, el modo que es de nuestro interés denominado **Frame-Mode**, que actúa en un ambiente puramente de enrutadores IP, se llama de esta forma debido a que los paquetes son etiquetados en frames sobre la Capa 2 de OSI.

IV.3.2 TOPOLOGÍA BÁSICA

En la topología se muestran los enrutadores que pertenecen a la red MPLS como lo son A, B, C y D que son los que utiliza MPLS, mientras que los enrutadores de frontera son los que hacen la traducción de IP a etiquetas MPLS y viceversa.

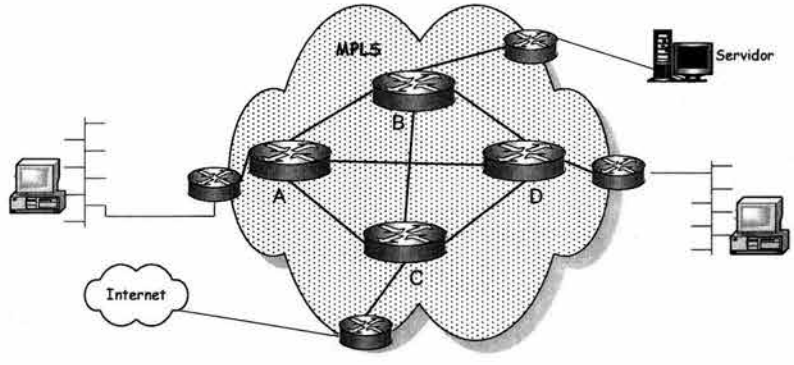


Figura 4.3.1

IV.3.3 ETIQUETA Y FRAME

Etiqueta

Una etiqueta, en su forma más simple, es un identificador que sirve para que cada enrutador reconozca el camino que cada paquete debe seguir. Una etiqueta es encapsulada en un encabezado de Capa 2 con el paquete. El enrutador de recepción

examina la etiqueta para determinar el siguiente salto. Una vez que han etiquetado un paquete, el resto del viaje está basado en la conmutación de etiqueta.

Para poder enviar los paquetes en MPLS hay que tener bien claro cuales son las funciones de las etiquetas y como se forman por lo que hay que aclarar lo siguiente:

- Las etiquetas solo tienen significado local, son relevantes únicamente para el enlace entre dos enrutadores y definen el camino a través de la red MPLS
- Las decisiones de enrutamiento se basan en la última etiqueta del "label stack".
- Los paquetes se guían mediante esas etiquetas.
- Las etiquetas por tanto permiten: establecer un VC o LSP (Virtual Circuit o Label Switched Path), y conmutar rápidamente en función de la etiqueta sin ningún proceso adicional.

Formato de etiqueta

En la Figura 4.3.2 se representa el esquema de los campos del encabezado genérico MPLS y su relación con los encabezados de los otros niveles. Según se muestra en la figura, los 32 bits del encabezado MPLS:

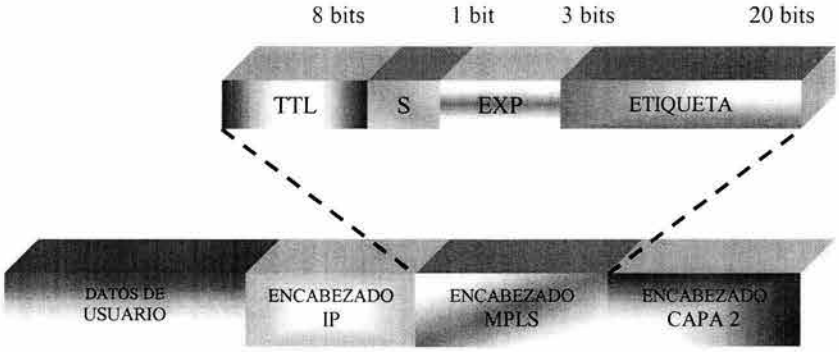


Figura 4.3.2

- ETIQUETA: 20 bits para el identificador.
- EXP: 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS)
- S: 1 bit de stack para poder apilar etiquetas de forma jerárquica.

- TTL: 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, los encabezados MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red. El funcionamiento de TTL es:
  - Al entrar un paquete en la red MPLS el enrutador de ingreso inicializa el TTL de la etiqueta al mismo valor que tiene en ese momento el encabezado IP
  - Durante el viaje del paquete por la red MPLS el campo TTL de la etiqueta disminuye en uno por cada salto. El encabezado IP no se modifica.
  - A la salida de la red MPLS el enrutador de egreso coloca en el encabezado IP el valor del TLL que tenía la etiqueta, menos uno
  - Si en algún momento el TTL de MPLS vale 0 el paquete es descartado

Frame

Una vez que un paquete ha sido clasificado, una etiqueta es asignada al paquete. Para los distintos protocolos de Capa 2, los identificadores de Capa 2, su espacio puede ser utilizado directamente para las etiquetas. Los paquetes entonces son expedidos basados en su valor de etiqueta.

Inserción de la etiqueta MPLS en tecnologías de capa de enlace:

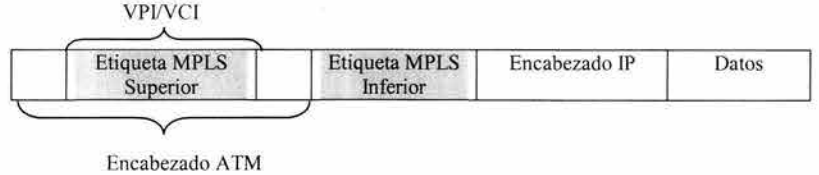
PPP (líneas dedicadas)

Encabezado PPP	Pila de etiquetas MPLS	Encabezado IP	Datos	Cola PPP

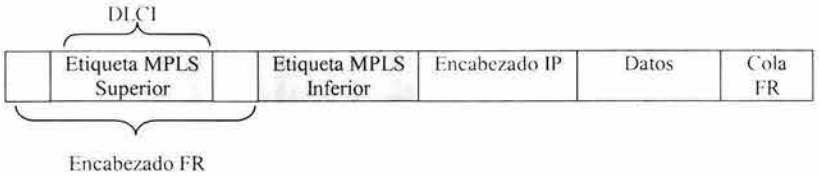
LAN (802.2)

Encabezado MAC	Encabezado LLC	Pila de etiquetas MPLS	Encabezado IP	Datos	Cola MAC

ATM



Frame Relay



Pila de Etiquetas (Label Stack)

Las decisiones de asignación de etiqueta pueden estar basadas en la expedición de criterios, en una red MPLS típica solamente es asignada una etiqueta única a los paquetes, existen ciertas aplicaciones en la cuales se requieren de más etiquetas para poder identificar cierto tipo de servicios como lo puede ser:

- MPLS VPN´s: en este caso se ocupan dos etiquetas, la primera es asignada en el ingreso para identificar la VPN y la segunda de MPLS la cual se ocupará para realizar la conmutación en la red.
- MPLS TE (Ingeniería de Tráfico): En este caso dos o mas etiquetas son asignadas. La primera es asignada para el túnel de Ingeniería de Tráfico del punto de ingreso al punto de egreso y la segunda etiqueta de MPLS para llegar a la red destino.
- MPLS VPN combinado con TE: En este caso tres o mas etiquetas son usadas

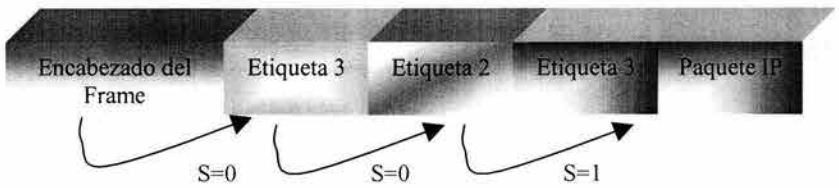


Figura 4.3.3

IV.3.4 ARQUITECTURA BÁSICA

MPLS lo podemos dividir en dos partes: la de conmutación (Capa 2), que es envío de datos (plano de datos) y el plano de control (Capa 3) que es la de enrutamiento, sin embargo estas dos partes no interactúan directamente pero la conmutación depende del correcto funcionamiento de capa 3, como se muestra en la figura:

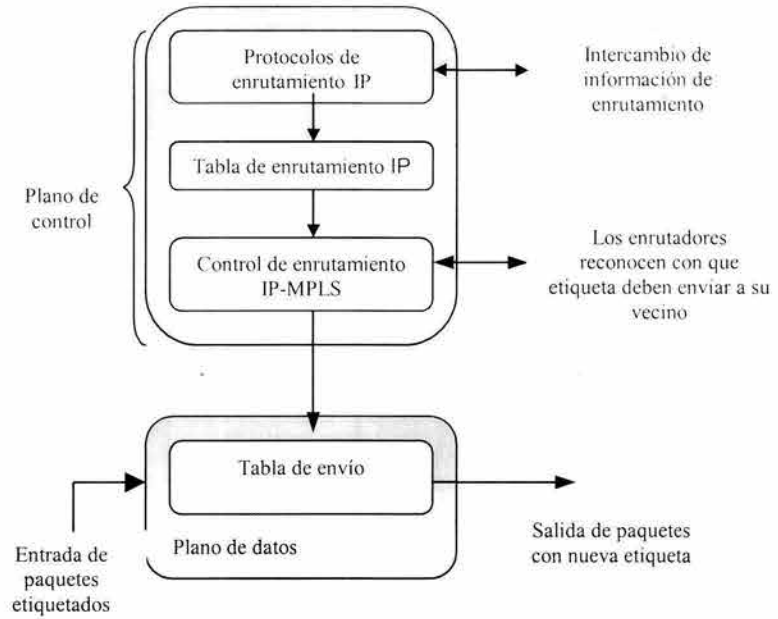


Figura 4.3.4

En el plano de envío únicamente se basa en la lectura y asignación de las etiquetas dependiendo del puerto por donde lleguen, es decir, al entrar un paquete se lee la etiqueta, se verifica en la tabla de envío, se asigna la nueva etiqueta y se envía por el puerto. En complemento, el plano de control genera, distribuye y actualiza las etiquetas para el envío de paquetes y la creación de una tabla de etiquetas. También relaciona la tabla de enrutamiento IP con la tabla de envío de etiquetas.

El plano de control utiliza adicionalmente la tabla de enrutamiento para determinar el intercambio de etiquetas (binding) con otros enrutadores MPLS, con el fin de conocer subredes existentes, este intercambio se ejecuta por medio del protocolo Label Distribution Protocol (LDP).

FEC (Forwarding Equivalence Class):

Es una representación de un conjunto de paquetes que entran en la red, que reciben la misma etiqueta y por tanto circulan por un mismo trayecto y que comparten las mismas exigencias para su transporte. Normalmente se trata de datagramas que

pertenecen a un mismo flujo. Todos los paquetes pertenecientes a una FEC tienen el mismo tratamiento en la ruta hasta el destino.

Una FEC puede agrupar varios flujos, pero un mismo flujo no puede pertenecer a más de una FEC al mismo tiempo.

Las etiquetas están destinadas a un FEC como consecuencia de algún acontecimiento o política que indica una necesidad de agrupamiento, bajo criterios de datos o control. El último criterio es preferible debido a sus propiedades de escalamiento avanzadas que pueden ser usadas en MPLS.

LSP (Label Switched Path):

Es el camino que siguen por la red MPLS los paquetes que pertenecen a la misma FEC. Es equivalente a un Circuito Virtual.

Se forman desde el destino hacia el origen de la siguiente manera:

- El origen (LSR entrada o interno) inicia una cadena de mensajes de petición de etiquetas para crear un LSP
- El destino (LSR interno o LSR salida) responde con mensajes de asociación de etiquetas creando el LSP
- Se va formando el LSP hasta el origen

El proceso para la creación de una ruta de los paquetes IP, desde su origen hasta su red destino es, como se muestra en la Figura 4.3.5, el siguiente:

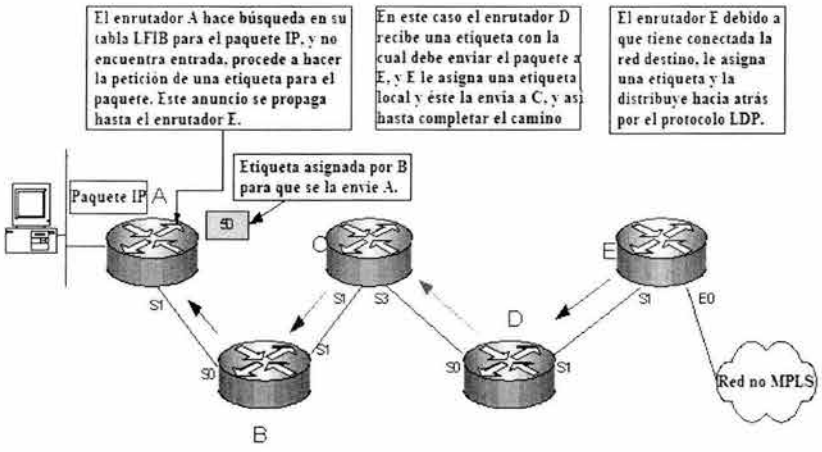


Figura 4.3.5

El último enrutador MPLS (en este caso E) antes del destino asigna una etiqueta; éste la distribuye en dirección al origen, llegando así al enrutador D, el cual se entera de la etiqueta con la cual deberá mandar el paquete IP a E, cuando sea el caso. Dicho enrutador D asigna una etiqueta local a la ruta recibida, repitiendo el mismo proceso con el enrutador C, y de la misma manera hasta llegar al origen de la transmisión.

Ya establecido el camino, el enrutador origen sabrá qué camino asignar al paquete para que llegue a la red destino. A este proceso se le conoce como creación del Label Switched Path (LSP).

IV.3.5 ESQUEMA DE ENRUTAMIENTO

Para poder comprender claramente MPLS es necesario tener una idea correcta sobre enrutamiento, es decir, la función de los protocolos de enrutamiento.

Enrutamiento es una función de la Capa de Red con respecto al Modelo de Referencia OSI, tiene como objetivo elegir el camino óptimo entre dos puntos, entre varias posibles rutas, y transmitir la información por el camino elegido. Para poder enrutar es necesario tener tanto la dirección origen como la dirección destino, y con esta última el enrutador verifica en su tabla de enrutamiento la mejor ruta por la cual se puede alcanzar la red de esa dirección IP.

Enrutadores MPLS:

Un enrutador MPLS puede conmutar paquetes en función del valor de la etiqueta MPLS, además de ocupar un protocolo de distribución de etiquetas.

Los dispositivos que participan en los mecanismos de protocolo MPLS pueden ser clasificados en enrutadores de etiqueta de borde (Edge-LSR: Edge Label Switch Router) y enrutadores de conmutación de etiqueta (LSR: Label Switch Router).

Se clasifican de la siguiente manera:

- LSR: Enruta paquetes dentro de la red MPLS. Su misión es únicamente cambiar las etiquetas para cada FEC según le indica su tabla de etiquetas (LIB). Un LSR es un dispositivo de alta velocidad en el corazón de una red de MPLS que participa en el establecimiento de LSP's utilizando la etiqueta

apropiada, señalando el protocolo y la conmutación de alta velocidad para los datos de tráfico basado en los caminos establecidos

- Edge LSR: es un dispositivo que funciona en el borde de la red de acceso y la red de MPLS. El Edge LSR juega un papel muy importante en la asignación y el retiro de etiquetas, y cómo el tráfico entra o sale de una red MPLS.
    - o Edge LSR de ingreso: Los que se encuentran en la entrada del flujo a la red MPLS (al principio del LSP). Se encargan de clasificar los paquetes en FEC's y poner las etiquetas correspondientes.
    - o Edge LSR de egreso: Los que se encuentran a la salida del flujo de la red MPLS (al final del LSP). Se encargan de eliminar del paquete la etiqueta MPLS, dejándolo tal como estaba al principio.

En la figura se muestra la arquitectura de un enrutador Edge-LSR:

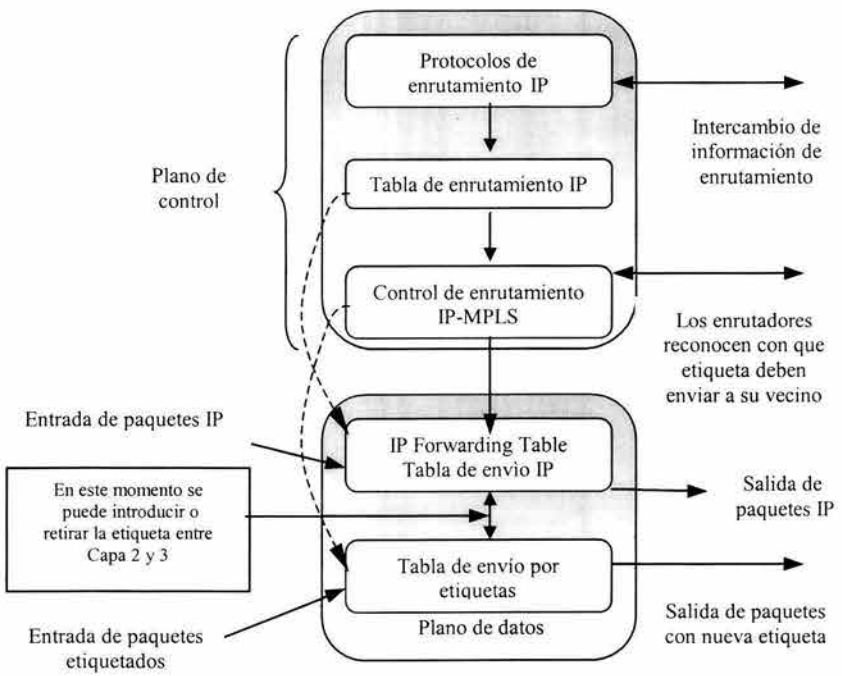


Figura 4.3.6

En la figura 4.3.6 tenemos dos tipos de entradas, una son paquetes MPLS (que ya tienen etiqueta), en este caso únicamente lee la etiqueta, le asigna una nueva y lo reenvía, o bien paquetes IP, la importancia de este enrutador, radica en que maneja tanto información de la tabla de enrutamiento, como de la tabla de control de enrutamiento de etiquetas, es decir, si es un paquete puramente IP, únicamente consultara su tabla de enrutamiento y envía el paquete, pero si el paquete IP esta contemplado para que sea encapsulado por MPLS, se le asigna la etiqueta y es enviado, o en caso contrario se le retira la etiqueta y es enviado en el protocolo de Capa 3 IP.

Construcción de tablas de etiquetas

Consideraremos las siguientes etapas para la construcción de las tablas de etiquetas:

1.-Enrutamiento "convencional" (IP)

Se tiene una tabla de enrutamiento por cada enrutador con el siguiente formato básico:

- Source Adress (Dirección Origen)
- Destination Adress (Dirección Destino)
- Next Hop (Siguiente Salto)

Se considera una búsqueda en la Tabla Global de Enrutamiento buscando una ruta por la cual alcanzar el siguiente salto de la trayectoria, con la dirección destino y el siguiente salto

Source Adress	Destination Adress	Next Hop	Output Interfase	# Hops	.....
Direccion IP	Direccion IP	Direccion IP	Puerto	Numero de saltos	

2.-Tabla base de MPLS (FIB)

Se crea la tabla Forwarding Information Base (FIB), la cual se muestra a continuación:

Destination Adress	Next Hop	Output Interfase
Direccion IP	Direccion IP	Puerto

3.- Tabla LIB

Con la tabla FIB el enrutador MPLS de borde (Edge LSR) genera etiquetas con un valor numérico aleatorio en un rango entre 24 y 220 combinaciones, o bien asignado manualmente por el administrador, resultando una asociación de la dirección IP destino con las etiquetas de la tabla FIB denominada Label Information Base (LIB), la cual básicamente representa a la tabla global de enrutamiento traducida en entradas por identificador de etiquetas.

Su forma es la siguiente:

Destination Adress	Local Label	Next hop label
Direccion IP	Etiqueta	etiqueta

- Dirección destino: la misma IP destino de la tabla global de enrutamiento.
- Etiqueta de entrada (Ingoing Tag): Etiqueta local asignada según la IP destino y es retirada al arribar el paquete.
- Etiqueta de salida o de siguiente salto (Local tag): Es la etiqueta con que se marcará para su envío el paquete por la interfaz correspondiente.

Todas las etiquetas son de significado local únicamente. Para hacer distinción de tráfico puede considerarse la dirección IP origen en el proceso de asignación de etiquetas, permitiendo administrar prioridades de tráfico y marcado de paquetes; es decir, permitiendo asignar etiquetas diferentes a paquetes provenientes de distintos orígenes con el mismo destino. (Figura 4.3.7)

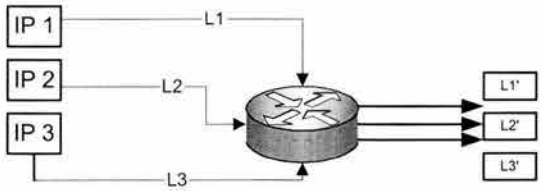


Figura 4.3.7

4-Tabla LFIB

Basados en la información de la tabla LIB, se forma la Label Forwarding Information Base (LFIB). Como podemos imaginarlo, y dada la orientación de MPLS al manejo de etiquetas para establecer las trayectorias, esta tabla es equivalente a la

tabla FIB con la diferencia de manejar las entradas y salidas a base de identificadores de etiqueta asociados a la interfase de salida correspondiente.

Local label	Next hop label	Output interfase
Etiqueta	Etiqueta	Puerto

Estas son las tablas que se intercambian entre enrutadores MPLS, con la ventaja adicional de proporcionar seguridad a la red, ya que los flujos de información (direcciones IP) no pueden se vistos en el exterior, dado que solo se manejan etiquetas con significado local.

Proceso de etiquetado

Al llegar un paquete IP al enrutador de frontera, se realiza una búsqueda en la tabla LIB, si no existe una entrada se realiza el proceso descrito anteriormente; si existe una entrada al paquete correspondiente se hace la asignación de la etiqueta por medio de la tabla LFIB, este proceso se muestra en la Figura 4.3.8:

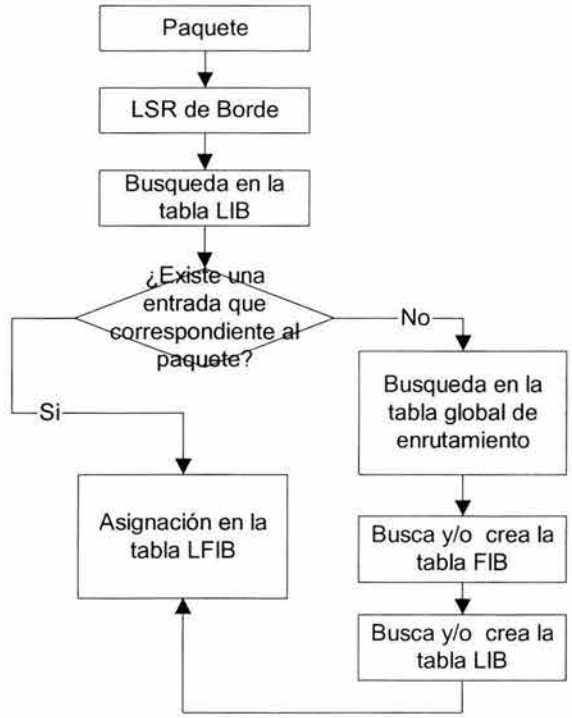


Figura 4.3.8

Control MPLS

En el caso de control, se puede observar que está basado en los protocolos de enrutamiento así como los protocolos de distribución de etiquetas. Se pueden resaltar los protocolos de enrutamiento que crean las tablas de enrutamiento y donde el protocolo IP juega un papel muy importante. Por otro lado en el caso de los protocolos de distribución de etiquetas estos están implementados sobre el protocolo TCP (como se verá en los siguientes apartados), este protocolo a su vez esta implementado sobre la Capa 3, la cual da servicio la parte de enrutamiento. Es preciso señalar que estas dos partes dan servicio a la parte de envío de datos en la arquitectura de MPLS, es decir construyendo tablas de etiquetas, así como propagando esta información de etiquetas.

Los protocolos de enrutamiento (operando en Capa 3 OSI), son de utilidad para que los enrutadores de la red MPLS, (LSR) conozcan información de sus vecinos, su objetivo principal es que todos y cada uno de los LSR se conozcan y elijan la mejor ruta entre ambos, es decir con la menor métrica, esta parte del diseño debe estar bien realizado para evitar problemas de enrutamiento. En MPLS, como ya se había mencionado, se requieren protocolos de estado de enlace (OSPF o IS-IS) y de tiempos de convergencia pequeños, así como gran flexibilidad. Debemos garantizar que la información de enrutamiento sea correcta, para no tener problemas cuando comience a funcionar MPLS.

Penultimate Hop-Popping

Penultimate Hop-Popping consiste en retirar la etiqueta en el penúltimo enrutador, y enviar únicamente el paquete encapsulado en IP al ultimo enrutador, el objetivo principal, es evitar que el ultimo enrutador (Edge-LSR) de la red MPLS, realice una doble búsqueda es decir, revisar su tabla LFIB y retirar la etiqueta, para posteriormente revisar su Tabla de enrutamiento IP para saber el next-hop. En la Figura 4.3.9 se muestra como el enrutador D retira la etiqueta y envía sólo el Paquete IP hacia el enrutador E, éste únicamente realiza una búsqueda en su tabla de enrutamiento IP y lo envía a su destino fuera de la red MPLS.

IV.3.6 CONMUTANDO EN MPLS

El siguiente ejemplo de la figura nos servirá para ejemplificar la conmutación en MPLS:

Se cuenta con 5 enrutadores y se mostrará la función de cada uno por separado, el objetivo es enviar información desde la red 10.0.0.0 a la dirección 192.168.20.3; para lograr lo anterior se utilizara MPLS.

Enrutador A: Es un enrutador de ingreso el cual tiene la función de asignar una etiqueta al paquete IP, a partir de su tabla LFIB, en este caso le asigna la etiqueta 50 la cual se asignó de manera local en el enrutador B y fue informada al enrutador A via LDP, posteriormente lo envía con puerto de salida serial 1.

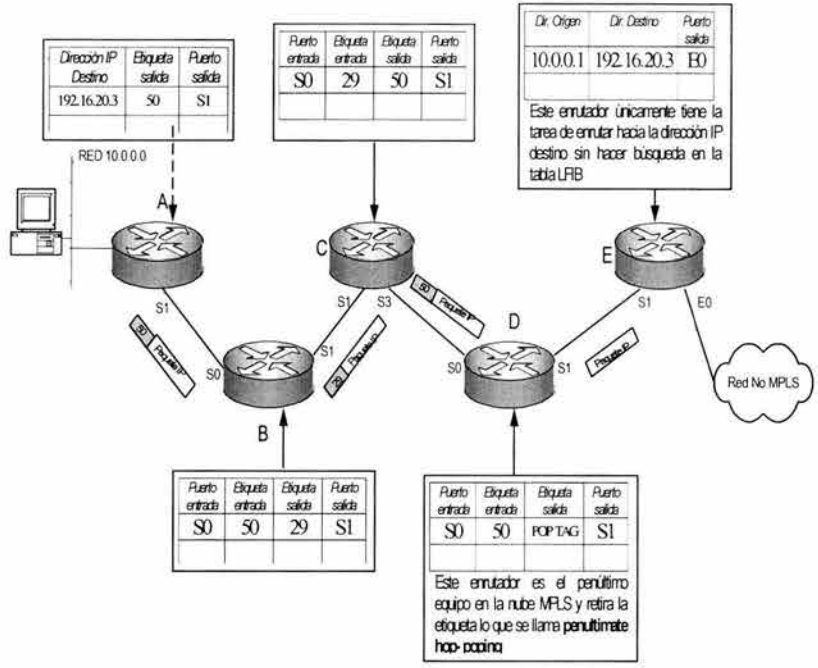


Figura 4.3.9

Enrutador B: Este enrutador es interno, por lo cual solo tiene la función de intercambiar etiquetas, le llega un paquete por el puerto S0 con etiqueta de entrada 50 (que localmente asignó y distribuyó al enrutador A), al consultar su tabla LFIB asigna la etiqueta 29, asignada localmente por el enrutador C y difundida a B vía LDP, para finalmente enviar con puerto de salida S1.

Enrutador C: Se realiza el mismo procedimiento al enrutador B, en este caso el puerto de entrada es S1 con etiqueta de entrada 29 y se asigna etiqueta 50 asignada localmente por D y distribuido vía LDP y con puerto de salida S3.

Enrutador D: Este enrutador también es interno, tiene la cualidad de ser el penúltimo enrutador en la red MPLS, por lo que implementa el Penultimate Hop-Popping, recibe el paquete con la etiqueta 50 y lo reenvía en IP puro por el S1, es decir, retira la etiqueta MPLS enviando únicamente un paquete encapsulado en IP.

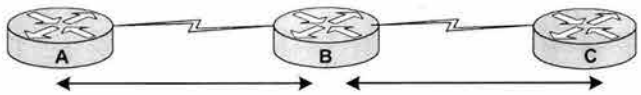
Enrutador E: Este es enrutador de egreso, el cual consulta su tabla de enrutamiento IP, y envía el paquete a su dirección destino que es la 192.168.20.3

IV.3.7 LDP (LABEL DISTRIBUTION PROTOCOL)

El protocolo de distribución de etiquetas LDP se ejecuta sobre TCP éste le proveerá de fiabilidad en el envío de mensajes.

El protocolo de distribución de etiquetas es el conjunto de procedimientos mediante los cuales un LSR se comunica con otro para notificarle el significado de las etiquetas para reenviar el tráfico entre ellos.

El uso más sencillo de LDP consiste en establecer enlaces unitarios de LSPs.



Intercambio de Etiquetas entre LSR's adyacentes

Figura 4.3.10

El protocolo de distribución de etiquetas asocia una FEC con cada LSP que crea. Dos LDPs serán LDP peers cuando ambos LSRs intercambien información de asociaciones de etiquetas y FECs. Para intercambiar dicha información establecerán una sesión LDP.

Clasificación de los mensajes LDP

Los pares LDP podrán intercambiar cuatro clases de mensajes:

1. Mensajes de descubrimiento (discovery messages): Se usan para anunciar y mantener la presencia de un LSR en la red. Un LSR mandará

periódicamente por la red mensajes HELLO con la dirección multicast "todos los enrutadores de esta subred".

2. Mensajes de sesión: Se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Cuando un LSR descubre a otro por medio de mensajes HELLO utilizará un procedimiento de iniciación LDP.
3. Mensajes de anuncio (advertisement messages): Se usan para crear, modificar y eliminar asociaciones de etiquetas a FECs. Cuando se haya establecido la asociación los pares LDP podrán intercambiarse este tipo de mensajes.
4. Mensajes de notificación: Hay dos tipos de mensajes de notificación: notificaciones de error y notificaciones de aviso. El primer tipo se utiliza para notificar errores fatales, en cuyo caso terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión. El segundo tipo se utiliza para pasarle a un LSR información de la sesión LDP o el estado de algún mensaje anterior.

Identificadores LDP

Un identificador LDP se utiliza para identificar el espacio de etiquetas de un LSR. Se compone de seis octetos, de los cuales los cuatro primeros identifican al LSR y los dos últimos identifican el espacio de etiquetas de dicho LSR. El espacio de etiquetas puede ser por interfaz o por plataforma. Si los dos últimos octetos tienen un valor de cero el espacio de etiquetas será por plataforma.

LDP utiliza el siguiente formato para representar su identificador:

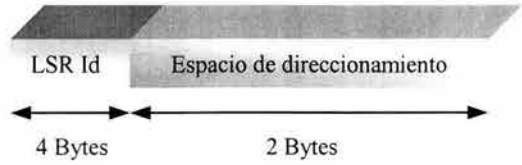


Figura 4.3.11

Sesión LDP

Cuando un LSR utiliza LDP para anunciar más de una etiqueta a otro LSR, utilizará diferentes sesiones LDP para cada espacio de etiquetas. Como se comentó anteriormente, LDP utiliza TCP. Cuando dos LSRs requieren múltiples sesiones LDP, se establecerán sesiones TCP distintas para cada sesión LDP.

En la especificación del protocolo se definen dos fases para el establecimiento de la sesión:

- Descubrimiento
- Establecimiento y mantenimiento de sesiones LDP

Descubrimiento

Existen dos modalidades de descubrimiento: básica y extendida.

En la modalidad básica el LSR envía periódicamente mensajes HELLO a un puerto bien conocido con la dirección multicast "todos los enrutadores de esta red". Los enrutadores están escuchando continuamente en este puerto a la espera de recibir mensajes HELLO. Por tanto, llegará un momento en el que el LSR conocerá todos los LSRs con los que tiene una conexión directa. Por tanto este mecanismo se utiliza si los LSRs están conectados directamente por medio de un enlace.

Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar en esa interfaz, además de otro tipo de información.

Con la modalidad extendida se permite que dos LSRs que no están conectados directamente establezcan una sesión LDP. Con esta modalidad, un LSR emite periódicamente mensajes HELLO a un puerto bien conocido y con una dirección específica, que habrá aprendido de algún modo (por ejemplo, por configuración). Los mensajes HELLO transportarán el identificador LDP con el espacio de etiquetas que LSR pretende usar, además de otro tipo de información. El LSR al que se le están enviando los mensajes HELLO podrá responder o ignorar dicho mensaje. Si decide responder a dicho mensaje deberá mandar periódicamente mensajes HELLO al LSR que inició el proceso.

La modalidad extendida es útil cuando se ha configurado un LSP entre dos LSRs por Ingeniería de Tráfico, deseando mandar paquetes ya etiquetados a través de ese LSP. El LSR situado al principio del LSP necesitará saber como etiquetar los paquetes que le enviará la LSR situado al final del LSP.

Establecimiento y mantenimiento de sesiones LDP

Una vez conocidos los vecinos se podrá establecer la sesión. Cada uno de los LSRs implicados puede jugar un papel activo o pasivo. El establecimiento de una sesión consta de dos fases:

- *Establecimiento de la conexión de transporte*

  Esta fase consiste en el establecimiento de una conexión TCP entre los LSRs implicados, para una nueva sesión LDP.
- *Inicio de la sesión*

Una vez establecida la conexión TCP los LSRs deben negociar los parámetros de la sesión. Esto se hace intercambiando mensajes de iniciación. Estos parámetros incluyen la versión del protocolo LDP, el método de distribución de etiquetas, valor de los temporizadores, etc.

Si un LSR juega el papel activo, éste iniciará la negociación de los parámetros de la sesión enviando un mensaje de iniciación a un segundo LSR. Este mensaje contendrá tanto el identificador LDP del primer LSR así como el identificador del segundo.

Cuando un LSR recibe un mensaje de iniciación, mirará dicho mensaje para determinar si los parámetros son aceptables. Si lo son, responderá con su propio mensaje de iniciación proponiendo los parámetros que desea usar y un mensaje de mantenimiento (KeepAlive) para notificar al otro LSR que acepta los parámetros. Si los parámetros no son aceptables, responderá con un mensaje de notificación de error de parámetros rechazados.

Formato de los mensajes

PDUs LDP

El intercambio de mensajes entre LSRs pares se realiza mediante el envío de PDUs (PDU: Protocol Data Unit: Unidad de datos del protocolo) LDP. Cada PDU LDP puede transportar más de un mensaje.

Cada PDU LDP está compuesto por un encabezado seguida de uno o más mensajes LDP. El formato del encabezado es el siguiente:

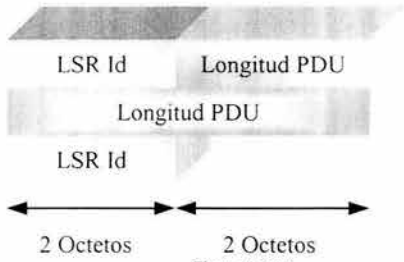


Figura 4.3.12

- Versión: dos octetos que identifican la versión del protocolo. Actualmente la 1
- Longitud PDU: dos octetos que especifican la longitud total en octetos de la PDU excluyendo los campos de la Versión y la Longitud de la PDU. La longitud de la PDU es negociable cuando se inicia la sesión LDP. Antes de la negociación, el tamaño máximo admitido es de 4096 octetos.
- Identificador LDP: campo de 6 octetos definido anteriormente.

Mensajes

Todos los mensajes LDP tienen el siguiente formato:

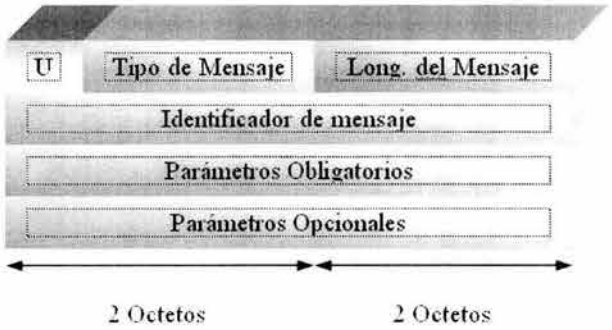


Figura 4.3.13

- U: bit de mensaje desconocido. Cuando se reciba un mensaje desconocido, si U = 0 se enviará una notificación al origen del mensaje. Si U = 1 simplemente se ignorará.

- Tipo de mensaje: identifica el tipo del mensaje.
- Longitud del mensaje: longitud del identificador del mensaje, de los parámetros obligatorios y de los parámetros opcionales
- Identificador del mensaje: identificador del mensaje.
- Parámetros obligatorios: conjunto de todos los parámetros obligatorios de los mensajes. Este campo tiene una longitud variable. Algunos mensajes no tienen parámetros obligatorios.
- Parámetros opcionales: conjunto de los parámetros opcionales de los mensajes. Este campo también es de longitud variable.

Los tipos de mensajes que define la especificación son los siguientes:

Mensaje de notificación

Este tipo de mensajes es utilizado por un LSR para notificarle a su par LSR de una condición de error o para suministrarle información de aviso.

Mensaje HELLO

Este tipo de mensajes son intercambiados entre pares LDPs durante la fase de descubrimiento.

Mensaje de iniciación

Este mensaje se utiliza cuando dos pares LDP desean establecer una sesión LDP.

Mensaje de mantenimiento (KeepAlive)

Estos mensajes los intercambian pares LSRs para monitorizar la integridad de la conexión de transporte de la sesión LDP.

Mensaje de dirección

Este mensaje se lo manda un LSR a su par LSR para notificarle las direcciones de sus interfases. El LSR que reciba este mensaje utilizará las direcciones aprendidas para actualizar una base de datos para las correlaciones entre los identificadores LDP de los pares y las direcciones de los siguientes saltos.

Mensaje de retiro de direcciones

Este mensaje se utiliza para retirar las direcciones de interfases notificadas anteriormente.

Mensaje de asociación de etiquetas

Este mensaje lo utiliza un LSR para notificarle a su par LSR una asociación de etiquetas.

Mensaje de petición de etiquetas

Este mensaje se lo manda un LSR a su par LSR cuando quiere solicitarle una asociación de etiquetas.

Mensaje de petición de abandono de etiqueta

Este mensaje abandona una petición de etiquetas pendiente.

Mensaje de retiro de etiquetas

Este mensaje se utiliza para retirar una asociación de etiquetas que está siendo usada. Un LSR le enviará este tipo de mensaje a su par LSR para indicarle que no puede continuar usando la asociación que previamente anunció. De esta forma se rompen las asociaciones entre etiquetas y FECs.

Mensaje de liberación de etiquetas

Este mensaje se utiliza cuando un LSR quiere informar a su par LSR que ya no necesita una asociación pedida o advertida anteriormente por su par LSR.

IV.3.8 APLICACIONES DE MPLS

Las aplicaciones principales de MPLS son:

- Facilidad de administración, con aplicaciones como: QoS, TE y CoS.
- Servicio de Redes Privadas Virtuales (VPN: Virtual Private Network).
- Integración de IP con todo tipo de redes subyacentes como Frame Relay, ATM, SDH por medio de AToM

A continuación se explicarán algunas de las aplicaciones:

Ingeniería de Tráfico

La Ingeniería de Tráfico persigue adaptar flujos de tráfico a recursos físicos de la red, de tal forma que exista un equilibrio entre dichos recursos. De esta forma se conseguirá que no haya recursos excesivamente utilizados, con cuellos de botella, mientras existan recursos poco utilizados.

Uno de los mayores problemas de las redes IP actuales es la dificultad de ajustar el tráfico IP para hacer un mejor uso del Ancho de Banda, así como mandar

flujos específicos por caminos específicos. En las redes IP convencionales los paquetes suelen seguir el camino más corto. Por ejemplo, los protocolos IGP siguen este criterio. Esto suele provocar que algunos enlaces se saturen mientras otros están subutilizados. Este problema se ha resueto añadiendo más capacidad a los enlaces. Veamos un ejemplo:

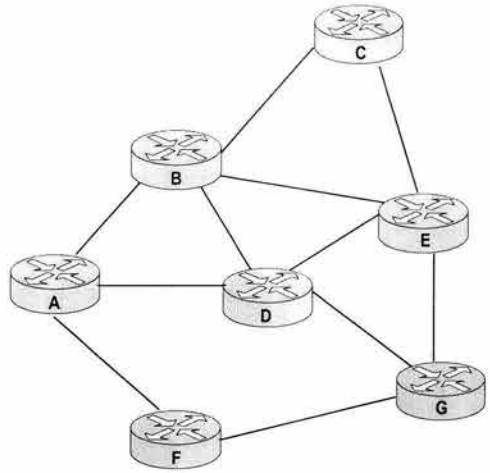


Figura 4.3.14

En la figura 4.3.14, el camino más corto entre A y C según la métrica normal IGP es el que tiene dos saltos (A-B-C), pero puede que el exceso de tráfico sobre estos enlaces o la carga de los encaminadores hagan aconsejable la utilización de un camino que requiera saltos adicionales, como por ejemplo A-D-E-C.

MPLS es una herramienta efectiva para la Ingeniería de Tráfico:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP.
- Permite usar el enrutamiento basado en restricciones de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales con distintos niveles de calidad (por ejemplo, con garantías de Ancho de Banda, etc.).

Soporte a las clases de servicio

MPLS soporta diferentes clases de servicio para cada LSP. Como caso particular, puede soportar servicios diferenciados en el mismo LSP.

La capacidad de poder asegurar que un paquete en concreto recibirá, a lo largo de todo el dominio, el tratamiento requerido, se apoya en dos posibilidades, la primera es IntServ (Integrated Services): apoyándose en RSVP, se reservan los recursos necesarios asociándose a LSP's concretos.

La segunda DiffServ (Differenciated Services): orientado al tráfico IP, basa su funcionamiento en la clasificación del tráfico a la entrada de la red y en la asignación de prioridades a estos tipos de tráfico mediante el Campo de 8 bits DSCP (DiffServ Code Point) (campo ToS (Type of Service) en IPv4 y Clase de Tráfico en IPv6). En función de este campo, cada nodo intermedio tratará el paquete de la forma adecuada. Históricamente, Internet ha ofrecido un solo nivel de servicio: "Best effort". Con la aparición de aplicaciones multimedia y aplicaciones en tiempo real, surgió la necesidad de la diferenciación de servicios en Internet. De esta forma se podrán diferenciar servicios como el correo electrónico de otros que dependen mucho más del retardo y de la variación del mismo como el Video y la Voz interactiva.

El modelo de los servicios diferenciados define los mecanismos para poder clasificar el tráfico en clases de servicio con diferentes prioridades. Para clasificar el tráfico se emplea el campo ToS (Type of Service: Tipo de Servicio). A este campo se le llama DS en DiffServ. Una vez clasificados los paquetes en la frontera de la red, los paquetes se reenvían basándose en el campo DS. El reenvío se realiza por salto, es decir, el nodo decide por sí solo como se deberá realizar el reenvío. A este concepto se le denomina comportamiento por salto (PHB: Per-Hop Behavior).

MPLS se adapta bien a este modelo, ya que las etiquetas MPLS tienen el campo Exp para poder propagar la clase de servicio CoS en el correspondiente LSP. Por tanto, una red MPLS puede transportar distintas clases de tráfico. Entre cada par de LSRs exteriores se pueden tener distintos LSPs con distintas prestaciones y distintos Anchos de Banda.

Redes privadas virtuales

Una de las principales razones del despliegue de MPLS en proveedores de servicios y redes empresariales son los servicios de VPNs (VPN: Virtual Private Network).

Una red privada virtual se puede definir como una red en la que la conectividad entre múltiples lugares se realiza a través de una infraestructura compartida con las mismas políticas de acceso y seguridad que en una red privada.

Una compañía en la que su intranet funcione sobre de un servicio de VPN tendrá la misma seguridad, fiabilidad, etc, que el resto de sus redes privadas. Por tanto, el objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de Voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables.

Las dos características más importantes de una VPN desde el punto de vista del usuario son la seguridad y la privacidad.

Las principales características de una VPN son:

- Escalabilidad: debe ser capaz de asumir cambios de conectividad y capacidad de forma muy ágil. MPLS ofrece conectividad «todos-con-todos», lo que la convierte en una red realmente flexible con unos requerimientos de configuración mínimos a la hora de añadir un nuevo extremo a la VPN, pues sólo hay que configurar el nuevo extremo, sin tener que tocar la configuración del resto de extremos. MPLS evita la complejidad de los túneles y PVCs.
- Seguridad: debe asegurar que el tráfico de cada cliente es confidencial; ningún usuario ajeno a la VPN debe ser capaz de acceder a la información que viaja por ésta. La seguridad de una VPN MLPS es comparable a la de FR o ATM.
- QoS: Debe asegurar la priorización del tráfico crítico o sensible al retardo sin despreciar tampoco el resto del tráfico gestionando el Ancho de Banda asignado a cada tipo de tráfico. MPLS soporta la diferenciación de tráfico de una forma estandarizada y permite garantizar SLAs para dichos tipos de tráfico, pudiéndose implementar herramientas, incluso vía web, que

permitan a los usuarios controlar el funcionamiento de su red en todo momento.

- Gestión: una VPN con una gestión ágil y eficiente resulta imprescindible para poder cumplir con los objetivos anteriores y alcanzar unos SLAs competitivos. La posibilidad de aplicar técnicas de Ingeniería de Tráfico es la herramienta básica para la gestión en una red MPLS.
- Fiabilidad: es indispensable para poder prever y garantizar una gran disponibilidad del servicio. La red MPLS «sabe» de la existencia de una VPN, ya que se trata de un modelo acoplado y no superpuesto.

El avance que supone MPLS en cuanto a IP VPNs respecto a las actuales soluciones existentes reside en un cambio de concepto.

Las soluciones actuales, basadas en túneles extremo a extremo, emplean un modelo topológico superpuesto al modelo físico existente, con los consiguientes inconvenientes en cuanto a escalabilidad y gestión del servicio.

MPLS se basa en un modelo acoplado, donde en lugar de conexiones extremo a extremo entre cada emplazamiento, lo que hay son conexiones IP a una «nube» exclusiva de los miembros de la VPN. Esta «nube» se implementa mediante LSPs que transportan los paquetes de usuario sin consultar su contenido, a base de encapsularlos sobre otro protocolo. La diferencia entre ambas soluciones es que en los túneles se utiliza el enrutamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de enrutamiento IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Intranet entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen del encabezado IP, que la red MPLS podrá propagar hasta el destino así como técnicas de Ingeniería de Tráfico.

Ventajas de las aplicaciones

MPLS aparece como una posible solución para proporcionar QoS e Ingeniería de tráfico a una red global que soporte con grandes posibilidades de éxito debido a la a las ventajas que MPLS ofrece.

Una importante ventaja de una red única es la simplificación en cuanto a administración de una sola de red, sobre la se pueden crear tantas redes virtuales como sea necesario. Esto facilitará enormemente la labor a los Proveedores de Servicio al tiempo que les permitirá ofrecer servicios de valor agregado, pues es lo que en definitiva acabará marcando la diferencia entre ellos. Ya hay operadores migrando a esta solución como es el caso de, por ejemplo, Cable & Wireless, Equant, Genuity y MCI World- Com. Los fabricantes también se han volcado de lleno en el desarrollo del software necesario para la migración y del equipamiento propio de MPLS. Tanto CISCO como Nortel Networks, Juniper Networks o Nokia (entre otros) disponen de grupos de trabajo especializados desarrollando este nuevo estándar. Éste es el punto clave para que los Proveedores de Servicio puedan comprobar la aceptación de MPLS en el mercado, dando así el primer paso hacia una nueva etapa para las redes de comunicaciones. Una etapa, si todo evoluciona siguiendo la trayectoria actual, muy prometedora.

IV.4 JUSTIFICACIÓN DE ELECCIÓN DE MPLS

En este punto suponemos que al elegir cualquiera de las opciones de tecnología de transporte de Capa 2 antes mencionadas, se aseguraría una transmisión de datos en la red con ventajas sobre una red IP tradicional, tales como capacidad, velocidad y/o administración con diferente grado en cada una de las opciones.

De la misma forma, se presentarán desventajas, inconvenientes o dificultades específicas a cada tecnología, las cuales también deberán ser comparadas para asegurar que su implementación proporcionará la mayor cantidad de ventajas disponibles, así como la menor cantidad de complicaciones.

En la siguiente tabla comparativa se mencionan algunas de las características más importantes, representativas y en que diferencian las tecnologías WAN explicadas anteriormente.

Característica	Frame Relay	ATM	MPLS
Capa del modelo de referencia OSI en la que opera	Capa 2	Capa 2	Capa 2.5. tiene ventajas de Capa 2, así como el control de Capa 3
Integración de capas 2 y 3 sin discontinuidades	No	No	Si
Orientado a Conexión	Si	Si	Si
Asignación de los PVC (LSP), por medio de identificadores	Manual	Manual	Automática y Manual. Adicionalmente maneja un protocolo de distribución de etiquetas
Requiere de enlaces confiables (debido a la falta de mecanismo de corrección de errores)	Requisito	Recomendable, más no indispensable	Recomendable, más no indispensable
Susceptibilidad a perder la conectividad si el enlace físico se pierde	Si	Si	No, mediante el protocolo de enrutamiento genera una ruta alterna.
Capacidad de transporte	Ancho de Banda reducido	Soporta anchos de banda grandes	Soporta anchos de banda muy grandes (tanto como la red IP tenga disponibles)
Aumento de la complejidad administrativa al escalar la red.	Si	Si, IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP	Manejable al descansar en una topología escalable; estable por el protocolo de enrutamiento.
Flexibilidad en la implantación de aplicaciones y escalabilidad	Escasa	Regular	Alta
Calidad de Servicio	No lo maneja	Implementación con aplicaciones adicionales.	Maneja de buena forma Calidad de Servicio basado en IP.
Facilidad de implementación de Ingeniería de Tráfico	No disponible	Configuraciones complicadas	Relativamente sencilla
Soporte de VPN's	Si	Si	Si, con un mejor control y administración sobre ellas.
Dispositivos de Conmutación	Se requieren conmutadores específicos, para generar la red	Se requieren conmutadores específicos, para generar la red	En MPLS pueden aprovecharse los enrutadores de la red IP.
Costo de implementación	Costo de equipos más interfases	Costo de equipos más interfases	Ninguno si se cuenta con infraestructura adecuada IP
Soporte de servicios multimedia (Voz, datos, Video)	Si	Si	Si
Posibilidad de transporte de otras tecnologías.	No	No	Si, con funcionalidades adicionales
Facilidades de Administración de la red	Si	Si	Mayor

Basados en el cuadro comparativo anterior, y en base a características reales (técnicas y administrativas), la elección de MPLS como tecnología alterna de capa 2.5 en la red a diseñar es una excelente opción, ya que ofrece ventajas sobre tecnologías

similares utilizadas en las redes que se han implementado en el pasado, con la propiedad de ser compatible desde su esencia con la Capa 3, otorgándole un entendimiento natural con la red IP sobre la que descansa.

Aún después de elegir MPLS como la mejor opción, no hay que perder de vista sus limitaciones, así como sus indiscutibles ventajas, sobre todo en el área administrativa de la red y la facilidad de implementación de aplicaciones sumamente útiles en el amplio mercado requirente de accesos de Ancho de Banda óptimos. Así también, el haber comprendido el funcionamiento de la tecnología nos posibilita para deducir los aspectos básicos con que la infraestructura de red deberá contar, logrando un proceso de diseño satisfactorio.

V PROTOCOLOS DE ENRUTAMIENTO

En las redes de datos IP es indispensable hacer llegar la información a su destino, para ello son necesarios los protocolos de enrutamiento, que son los encargados de implementar algoritmos y procedimientos para lograrlo óptimamente. En el caso de MPLS son necesarios para conocer los caminos y destinos que se utilizarán en el envio de paqutes por medio de etiquetas.

Enrutamiento

Enrutamiento es una función de la capa de red con respecto al modelo de referencia OSI, tiene como objetivo elegir el camino óptimo entre dos puntos de entre varias posibles rutas, y transmitir la información por el camino elegido. Para poder enrutar es necesario tener tanto la dirección origen como la dirección destino, y con esta última el enrutador verifica en su tabla de enrutamiento la mejor ruta por la cual se puede alcanzar la red de esa dirección IP.

El proceso que se sigue es el siguiente:

1. El enrutador analiza la dirección destino.
2. Busca una entrada en la tabla de enrutamiento
    - Si la encuentra envía el paquete por la interfase de salida y decrementa el tiempo de vida del paquete (TTL).
    - Si no encuentra una ruta
        - Verifica si tiene configurada una ruta por default y envía el paquete.
        - Si no tiene configurada una ruta por default desecha el paquete.

Para el proceso de enrutamiento se realiza mediante dos procesos básicamente, enrutamiento estático y enrutamiento dinámico.

Enrutamiento estático:

- Se configura una ruta manualmente en el enrutador,
- No responde a los cambios en la topología.
- Adecuado para redes pequeñas.
- Consume pocos recursos del enrutador.

- Éstas tienen la menor distancia administrativa.

Enrutamiento dinámico:

- Responde a cambios en la topología.
- Adecuado para redes grandes a muy grandes.
- Consume mas recursos del enrutador.
- Ocupa los protocolos de enrutamiento que pueden ser distance-vector o link-state.

Protocolos de Enrutamiento

La idea fundamental de los protocolos de enrutamiento es la notificación de rutas entre los enrutadores presentes en la topología. Para lograrlo, el protocolo de enrutamiento informa automáticamente, y a intervalos regulares, a los demás enrutadores de todas las rutas que conoce. Estos paquetes de información se llaman anuncios o actualizaciones de enrutamiento, según el protocolo especifico en cuestión. Estas actualizaciones permiten a todos los enrutadores aprender automáticamente sobre todas las rutas.

Estos protocolos tienen como objetivo:

- Reducir el esfuerzo administrativo que supone generar dinámicamente las tablas de enrutamiento.
- Cuando se dispone de más de una ruta para una red dada:
    - Colocar la mejor ruta de la tabla,
    - Colocar múltiples rutas de la tabla y efectuar un balance de carga entre las rutas.
    - Eliminar automáticamente las rutas no válidas de la tabla cuando se produzca fallo.
    - Si se dispone de una ruta mejor, hay que añadirla a la tabla.
    - Eliminar loops de enrutamiento tan rápido como sea posible.

Los protocolos de enrutamiento se clasifican según el principio de funcionamiento que emplean. Existen dos clasificaciones importantes que son:

- Distance Vector: Suele denominarse "enrutamiento por rumor". Este tipo de algoritmo anuncia sus rutas a todos sus vecinos conectados directamente, mientras ellos hacen lo mismo añadiendo a su tabla lo que aprenden.
- Link State: Básicamente, los protocolos de estado de enlace trazan un "mapa" de la red, de manera que tienen intrínsecamente una idea más precisa de dónde está situado cada enrutador, que la que tienen los Distance Vector. Esta ventaja vuelve a estos protocolos más atractivos y sofisticados, pero resultan más difíciles de entender, pero su implementación es mas sencilla.

Por lo discutido en el capitulo IV, en cuanto a las características de funcionamiento de MPLS, éste debe crear LSPs, para ello requiere de protocolos de enrutamiento de estado de enlace (link-state) entre los que encontramos a OSPF, IS-IS y BGP, con la ventaja de ser protocolos más robustos y con mayor estabilidad explicados a continuación. En los protocolos que no profundizaremos son los distance-vector como RIP e IGRP.

V.1 OSPF (OPEN SHORTEST PATH FIRST)

El grupo Fuerza de Trabajo de Ingenieros de Internet (IETF) empezó a desarrollar un nuevo protocolo de enrutamiento que reemplazaría al protocolo RIP. Se desarrolló entonces el protocolo de enrutamiento OSPF - *Open Shortest Path First.- (Abrir la ruta más corta primero)* . OSPF es un protocolo de enrutamiento para redes IP.

El protocolo OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de tablas de enrutamiento con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de enrutamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de costo, en el caso de RIP se calcula sólo la métrica y no el trafico del enlace, por esta causa OSPF es un protocolo de enrutamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de enrutamiento distribuida y de rápida propagación, entre las características más resaltantes de OSPF están:

- Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas sin loops.
- Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- División de tráfico por varias rutas equivalentes.
- Enrutamiento según el tipo de servicio.
- Uso de multicast en las redes de área local.
- Maneja VLSM.
- Autentificación.

OSPF es un protocolo link-state "no propietario", esto quiere decir principalmente dos cosas: Primero que es de libre uso y suele estar soportados por la mayoría de los equipos destinados a ofrecer servicios a la red y segundo el ser un link-state quiere decir que a diferencia de RIP o IGRP que son Distance-vector, no mandan continuamente la tabla de rutas a sus vecinos sino que solo lo hacen cuando hay cambios en la topología de red, de esta forma se evita el consumo de Ancho de Banda innecesario. En un cambio de topología, OSPF envía el cambio inmediatamente de

forma que la convergencia de la red es mas rápida que en los distance-vector, donde depende de timers asignados, de forma que en un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red y en RIP puede ser de 180 segundos.

V.1.1 FUNCIONAMIENTO DE OSPF.

Todos los enrutadores de OSPF tiene una base de datos detallada con la información necesaria para construir un árbol de enrutamiento del área, con la descripción de:

- Todas las interfaces, conexiones y métricas de los enrutadores.
- Todas las redes de multiacceso y una lista de todos los enrutadores de la red.

Para conseguir esta información empieza descubriendo quienes son sus vecinos mediante un mensaje de saludo (Hello).

Sistemas autónomos de área (AS).

En el ámbito de OSPF, el término red significa una red IP. De la misma forma, una máscara de red identifica una red o una subred. Un área es un conjunto de redes y host contiguos, incluyendo los de frontera. Un Sistema Autónomo que use OSPF está construido por una o más áreas. Cada área tiene asignado un número que la identifica. El área 0 es el Backbone que enlaza con el resto de áreas y agrupa al resto de sistemas autónomos.

La topología de OSPF esta basada en áreas conectadas de forma jerárquica.

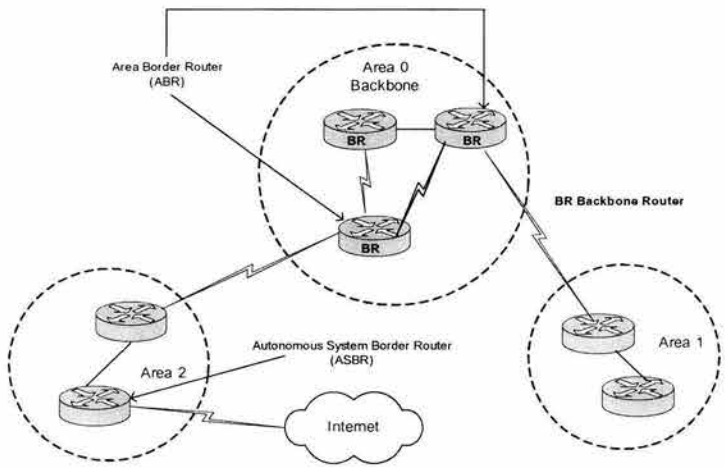


Figura 5.1.1

Enrutamiento de área en OSPF.

El enrutamiento dentro de un área se basa en un mapa completo de estado de enlace del área. OSPF se diseñó para que admitiera el crecimiento de la red porque un enrutador necesita conocer la topología detallada e información de métricas sólo del área a la que pertenece.

Todos los enrutadores con OSPF implementado en un área mantienen una base de datos de enrutamiento idéntica que describe la topología y estado de todos los nodos de esa área. La tabla de enrutamiento se usa para construir el mapa de esa área. Esta tabla de enrutamiento incluye el estado de todos los enrutadores, interfaces útiles de los enrutadores, las redes conectadas y sus enrutadores adyacentes. Siempre que ocurre un cambio, la información se propaga por toda el área. De esta forma siempre los enrutadores estarán en un estado óptimo para cualquier petición. De esta manera si tenemos un área bastante densa y falla un enlace con un enrutador, en ese momento el enrutador vecino de ese enlace perdido informará a todos los demás que esa ruta será inaccesible, en cuanto se recupere el enlace informará de nuevo que se recuperó la comunicación con ese enrutador.

Un enrutador que esté arrancando obtendrá una copia de la tabla de enrutamiento actual de enrutamiento de su vecino más cercano, tras esto, solo se comunicaran los cambios (esto hace más óptimo a OSPF, ya que no replica toda la tabla de enrutamiento de nuevo). Los cambios se difunden rápidamente, ya que OSPF utiliza un algoritmo de distribución eficiente para extender la información de actualización por un área.

Caminos más cortos de un área OSPF

Un enrutador usa su tabla de enrutamiento para construir un árbol de caminos más cortos poniéndose a sí mismo en la raíz. Este árbol se usa para construir la tabla de enrutamiento. Si se dispone de enrutamiento por tipo de servicio en el área, se construye un árbol separado y un conjunto de rutas para cada tipo de servicio.

Backbone y fronteras de OSPF.

La red agrupa las áreas. El Backbone contiene todos los enrutadores que pertenecen a múltiples áreas, así como las redes y enrutadores no asignados a ninguna área. Hay que recordar que las áreas están numeradas y que el Backbone es el Área 0.

El enrutador frontera pertenece a una o más áreas y al Backbone. Si el Sistema Autónomo está conectado el mundo exterior, los enrutadores de frontera pueden conocer rutas a redes que son externas al Sistema Autónomo.

Enrutamiento por una frontera de área de OSPF.

El enrutador de frontera conoce la topología completa de las áreas a las que esta conectado. Es conveniente recordar que todos los enrutadores frontera pertenecen al Backbone, por lo que también conocen la topología del Backbone.

Sumarización dentro de un área OSPF.

Los enrutadores frontera resumen la información de área e indican a otros enrutadores del Backbone lo lejos que están de las redes dentro de su propia área. De esta forma todos los enrutadores frontera pueden calcular las distancias a destinos fuera de sus propias áreas y transmitir esta información dentro de sus áreas. La sumarización incluye un identificador de red, subred o superred, una máscara de red y la distancia desde el enrutador a la red externa.

Destino fuera de los AS de OSPF.

Muchos Sistemas Autónomos están conectados a otros o a Internet. Los enrutadores límite de OSPF ofrecen información sobre distancias a las redes externas al Sistema Autónomo. Existen dos tipos de métrica, la que es dentro del área (local) y la que es fuera del área.

Tipos de mensajes OSPF.

Los cinco tipos de mensajes del protocolo OSPF son:

- Saludo: Se usa para identificar a los vecinos, es decir, enrutadores adyacentes en un área para elegir un enrutador designado para una red multicast, para encontrar un enrutador designado existente y para enviar señales de "Estoy aquí".
- Descripción de la tabla de enrutamiento: Durante la inicialización, se usa para intercambiar información de manera que un enrutador puede descubrir los datos que le faltan en la tabla de enrutamiento.
- Petición del estado del enlace: Se usa para pedir datos que un enrutador se ha dado cuenta que le faltan en su tabla de enrutamiento o que están obsoletos.

- Actualización del estado del enlace: Se usa como respuesta a los mensajes de Petición del estado del enlace y también para informar dinámicamente de los cambios en la topología de la red.
- ACK de estado del enlace: Se usa para confirmar la recepción de una Actualización del estado del enlace. El emisor retransmitirá hasta que se confirme.

Tipos de enrutadores

Enrutador designado.

En una red multiacceso, los mensajes de saludo también se usan para identificar a un Enrutador designado. El enrutador designado cumple dos funciones:

- Es responsable de la actualización fiable de sus vecinos adyacentes con la información más reciente de la topología de la red.
- Crea avisos de enlaces de red con la lista de todos los enrutadores conectados a la red multiacceso.

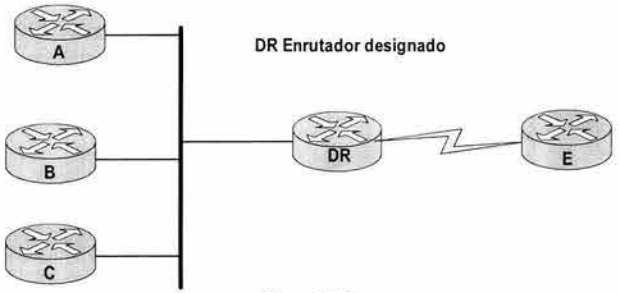


Figura 5.1.2

El DR intercambia información con los enrutadores A,B, C de su LAN, así con el enrutador E conectado con su enlace punto a punto, como se muestra en la figura 5.1.2

Area Border Enrutador (ABR): enrutador de borde del área.

Enrutador OSPF con una interfaz en un área y al menos otra interfaz en una área distinta. Este enrutador pertenece a dos áreas (por lo menos).

Autonomous System Boundary Enrutador (ASBR -Enrutador de área límite de Sistema Autónomo-)

Enrutador OSPF con una interfaz conectada a una red externa con un protocolo de enrutamiento distinto. Son los responsables de "inyectar" rutas aprendidas por otros

protocolos. Las rutas se ingresan en los enrutadores junto con dos parámetros más, la distancia administrativa (Admininstrative Distance) y la métrica o costo. La distancia administrativa es un indicador de confianza asignado a la ruta aprendida por un protocolo de enrutamiento.

PROTOCOLO	DISTANCIA ADMINISTARTIVA
DIRECTAMENTE CONECTADAS	0
ESTÁTICAS	1
OSPF	110
RIP	120

Tabla 5.1.3

Adyacencias

El enrutador DR de la figura 5.1.2 actúa como el experto local y mantiene actualizada la topología local completa. Después comunica a los enrutadores adyacentes la información. A, B y C mantienen sus propias tablas de enrutamiento sincronizadas hablando con DR. No tienen que intercambiar información con los otros, así se reduce drásticamente el tráfico de información. Dos enrutadores que sincronizan sus tablas de enrutamiento uno con otro se llaman adyacentes. B y C son vecinos, pero no son adyacentes el uno del otro debido a que consultan con DR.

Claramente es un método eficiente de mantener sincronizadas las tablas de enrutamiento de los enrutadores de la LAN. Los enrutadores pueden intercambiar mensajes de saludo por circuitos virtuales, elegir un enrutador designado y sincronizan sus tablas de enrutamiento con el enrutador designado. De esta forma se acelera la sincronización y se reduce el tráfico de la red. La perdida de un enrutador designado podría ser muy perjudicial. Por eso, siempre se elige un enrutador designado de respaldo y siempre está listo para reemplazarle inmediatamente.

Tipos de LSA (Link State Acknowledge):

- Tipo 1: Enrutador LSA: Lo genera el enrutador correspondiente a cada área de la que forma parte dicho enrutador. Estos LSA contienen el estado de todos los enlaces del enrutador de un área dada e inundan a todos los enlaces de la misma área.

- Tipo 2: Network LSA: Los genera un DR que están en todas las redes que no sean punto a punto (es decir, multiacceso). Los LSA tipo 2 incluyen a todos los enrutadores vinculados a la red en la que el enrutador actúa como DR.
- Tipo 3: Summary Links. Los genera los ABR y anuncian redes internas procedentes de un área especifica a otros ABR
- Tipo 4: ASBR. Los utilizan los ABR para anunciar los mejores caminos que conducen a los ASBR.
- Tipo 5: External LSA: Los envian los ASBR y anuncian los destinos externos a los AS (destinos redistribuidos desde otro AS OSPF u otro protocolo de enrutamiento).
- Tipo 7 NSSA: Solo los generan los ASBR en las NSSA. Los LSA tipo 7 solo inundan los NSSA. Los ABR convierten los tipo 7 en tipo 5 para redistribuirlos al resto del AS
- Tipo 8 Atributos de BGP
- Tipo 9,10, 11 Ingeniería de Tráfico y MPLS

Tipos de área

- Área estándar: Es el tipo más común. Todas aquellas áreas que no sean Backbone o alguna clase de área modular son área estándar. Dichas áreas admiten los LSA que van del tipo 1 al 5.
- Área de Backbone (área 0): Es el concentrador presente en el AS OSPF. El área de Backbone tiene la responsabilidad de garantizar el tráfico entre distintas áreas. Todas las áreas situadas en una solución OSPF multiárea deben tener una conexión con el Área 0.
- Área de tránsito: Es el área donde el tráfico procede de otras áreas, puede viajar a través de una ruta hasta su destino final. Un área troncal se considera un área de tránsito.
- Área modular: Es el área donde solo hay una forma de alcanzar destinos externos (otros AS). Por esta razón, un área modular no requiere el uso de LSA tipo 4 o 5. En su lugar, se inserta su único LSA tipo 3 para una ruta por omisión en el área modular con el fin de proporcionar el camino a destinos externos. Las áreas modulares requieren menos recursos de red,

CPU y memoria, ya que no existe la necesidad de mantener los LSA externos en la tabla topológica, Las áreas modulares sólo permiten el uso de LSA de tipo 1 a tipo 3.

- Área totalmente modular: Es el área en la que sólo hay forma de alcanzar destinos externos (otros AS) y destinos entre áreas. En otras palabras, en un área totalmente modular hay una única forma de alcanzar destinos externos que conducen al área. Permite el uso de LSA tipo 1 y 2.
- Área no tan modular NSSA (No So Stubby Área): Es un área que requiere la transmisión de LSA externos desde un ASBR dentro del área, pero que solo tiene un camino que conduce a los ASBR presentes en otras áreas. Puesto que el área NSSA solo dispone de un camino que conduce a destinos externos a los que acceden otros ASBR de otras áreas, puede convertirse en un área modular.

Inicialización de una tabla de enrutamiento (Base de Datos)

En la figura 5.1.2 suponga que el enrutador B acaba de arrancar tras un período de mantenimiento. En primer lugar B escucha los mensajes de saludo, descubre quienes son sus vecinos y descubre que el enrutador DR que es el enrutador designado. A continuación, B se pone al dialogar con DR.

Más concretamente, DR y B intercambian mensajes de descripción de información de enrutamiento. Estos mensajes contienen una lista de lo que tiene cada uno en su tabla de enrutamiento. Cada elemento tiene un número de secuencia que se usa para establecer qué enrutador tiene la información más reciente sobre dicho elemento. El número de secuencia de una entrada de enrutamiento se incrementa siempre que se actualiza.

Tras terminar esta intercambio de información, ambos conocen:

- Qué elementos no están todavía en su tabla de enrutamiento.
- Qué elementos si están presentes pero obsoletos.

Se usan mensajes de petición de estado del enlace (Link State Request) para solicitar todas las entradas que necesiten una actualización. Los mensajes de actualización del estado del enlace (Links State Update) son las respuestas a las peticiones. Tras un intercambio de información, con confirmaciones del estado del enlace, también se usan para informar de los cambios en la topología del área. La

actualización de la topología se expande por el área de manera que todas las Tablas de enrutamiento se mantengan sincronizadas.

Estados OSPF

Para una comprensión más profunda de OSPF es necesario comprender las relaciones o estados que tienen entre si los enrutadores que utilizan OSPF.

1. **Estado Down**: En el estado Down, el proceso OSPF no ha empezado a intercambiar información con ningún vecino. OSPF está esperando a entrar en el siguiente estado.
2. **Estado Init:** Los enrutadores que utilizan OSPF envían LSAs de tipo 1 (Hello) en intervalos regulares (por defecto 10 segundos en Cisco) para establecer relación con sus enrutadores vecinos, cuando un interfaz recibe su primer LSA Hello entonces decimos que el enrutadores ha entrado en estado Init y está preparado para entrar en el siguiente estado.
3. **Estado Two-Way**: Utilizando LSAs Hello, cada enrutador OSPF intenta establecer una comunicación bidireccional con cada enrutador vecino que está ubicado en la misma red IP. Un enrutador entra en estado two-way en el momento que se ve en una de las actualizaciones de uno de sus vecinos.: El estado two-way es la relación más básica que pueden tener los enrutadores OSPF, pero la información de enrutamiento no se intercambia en este estado. Para aprender sobre enlaces de otros enrutadores, el enrutador tiene que tener al menos una adyacencia completa.
4. **Estado ExStart:** Técnicamente, cuando un enrutador y su vecino entran en estado ExStart, su conversación se caracteriza por una adyacencia, pero los enrutadores todavía no tienen una adyacencia completa. El estado ExStart se establece utilizando LSAs de tipo 2. Entre los dos enrutadores se utilizan LSAs Hello para determinar cual de los dos es el maestro y cual es el esclavo en su relación y se intercambian LSAs de tipo 2.
5. **Estado.Exchange**: En el estado exchange se utilizan LSAs de tipo 2 para enviar al otro enrutador su información de estado del enlace. En

otras palabras, los enrutadores describen sus tablas de enrutamiento de estado del enlace al otro enrutador. Si alguna de las rutas no está en la tabla de enrutamiento del enlace del enrutador receptor de la información, este solicita una actualización completa, la cual se realiza en el estado Loading.

6. **Estado Loading**: Después de que todas las tablas de enrutamiento han sido descritas a cada enrutador, se tiene que solicitar una información que es más completa utilizando LSAs de tipo 3. Cuando un enrutador recibe un LSA de tipo 3, este responde con una actualización mediante un LSA de tipo 4. Los LSAs de tipo 4 describen la información de estado del enlace que es el corazón de los protocolos de enrutamiento de estado del enlace. Los LSAs de tipo 4 son respondidos con LSAs de tipo 5.
7. **Adyacencia Completa**: Cuando termina el estado Loading, los enrutadores están en una adyacencia completa. Cada enrutador mantiene una lista de sus vecinos adyacentes.

Ya que la adyacencia es necesaria para que los enrutadores que utilizan OSPF puedan compartir su información de enrutamiento, un enrutador tiene que estar adyacente con al menos otro enrutador en la red IP a la que esté conectado. Si hay o no adyacencia depende del tipo de red que se esté utilizando, es decir, de qué tipo de red esté conectado los enrutadores.

V.2 IS-IS (Intermediate System - Intermediate System)

El protocolo de enrutamiento IS-IS está basado en el algoritmo de estado de enlace. Además IS-IS permite hacer enrutamiento integrado, es decir, calcular las rutas una vez y aplicarlas para todos los protocolos utilizados, permitiendo así auténtico enrutamiento multiprotocolo. Admite además, hasta ocho niveles de jerarquía para reducir la cantidad de información de enrutamiento intercambiada. IS-IS es un es un protocolo de la enrutamiento desarrollado por la ISO.

La ocupación primordial es el intercambio de información de enrutamiento y la construcción de las tablas a partir de las que indica cuáles son las mejores rutas a través de la red. Es posible designar a un único enrutador para que difunda la información de enrutamiento. IS-IS se comporta como OSPF pero los dos protocolos tienen algunas diferencias significativas.

Utiliza protocolos del MROSI para entregar sus paquetes y para establecer sus adyacencias. Los enrutadores necesitan ser asignados con las direcciones IP, que utilizan como identificación del enrutador para crear la estructura de la red.

El protocolo IS-IS define un área, que es un conjunto de redes físicas y los dispositivos conectados a ellas. Los enrutadores que interconectan redes dentro de un área se denominan enrutadores de nivel 1. Los que interconectan un área con otra son los enrutadores de nivel 2 que trabajan como si formaran una sola unidad administrativa. El enrutamiento tiene lugar como sigue:

- Un sistema final (ES) envía un paquete a cualquiera de los enrutadores de nivel 1 de su área, de entre los que estén directamente conectados a él.
- El enrutador determina dónde está situada la dirección de destino y reenvía el paquete a través de la mejor ruta.
- Si la dirección de destino está en otra área, en enrutador de nivel 1 envía el paquete al enrutador de nivel 2 más cercano.
- El enrutador de nivel 2 podría a su vez enviar el paquete a otro enrutador de nivel 2, y así sucesivamente, hasta que el paquete alcance su área de destino.

- Finalmente, un enrutador de nivel 1 del área de destino se ocupará de que el paquete llegue al sistema final.

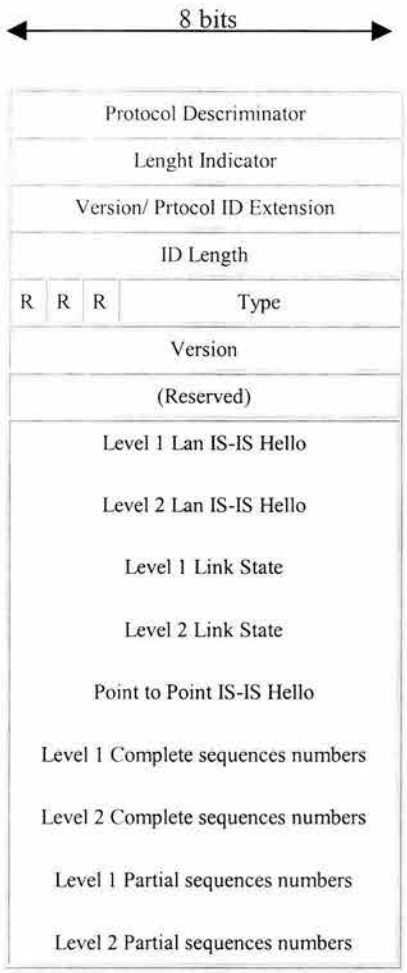


Figura 5.2.1

Tiene cuatro tipo de paquetes :

- **Hellos:** Establece y mantiene las adyacencias.
- **LSP ((Link State PDU): A**nuncia la información del link state.

- **CSNP (Complete Sequence Number PDU**): Que contiene la lista completa de LSP's aprendida por el enrutador.
- **PSNP (Partial Sequence Number PDU):** Reconoce una actualización de enrutamiento (LSP) en enlaces punto a punto para señalar y para solicitar la información que falta sobre una ruta después de recibir un CSNP.

Áreas de IS-IS:

ISIS: Se compone de 2 grandes niveles de áreas :

- Área Nivel 2: Es el área de Backbone, solo los componentes de esta área contienen vecinos en otras áreas.
- Área Nivel 1: Son las áreas secundarias , solo conocen su propia topología de red-área.

IS-IS agrupa las redes en dominios de modo análogo a OSPF. Un dominio de enrutamiento es análogo a un AS, y se subdivide en áreas, exactamente como OSPF. Aquí hay una descripción de los aspectos más importantes del enrutamiento IS-IS. Cuando es posible, se hacen comparaciones con conceptos equivalentes de OSPF.

- Los enrutadores se dividen en enrutadores de nivel 1, que no saben nada de la topología fuera de sus áreas, y de nivel 2, que conocen la topología de nivel superior, pero no saben nada de la topología de dentro de las áreas, a menos que sean también "enrutadores" de nivel 1.
- Un enrutador de nivel 1 puede pertenecer a más de un área, pero a diferencia de OSPF esto no se hace con propósitos de enrutamiento sino para facilitar la gestión del dominio, y normalmente por poco tiempo. Un "enrutador" de nivel 1 reconoce a otro como un vecino si están en la misma área.
- Un enrutador de nivel 2 reconoce a todos los demás enrutadores de nivel 2 como vecinos. Un "enrutador" de nivel 2 puede ser también un "enrutador" de nivel 1 en un área, pero no en más.
- Un enrutador de nivel 1 en IS-IS no puede tener un enlace con un enrutador externo (en OSPF un "enrutador" interno puede ser una ASBR).
- Hay una troncal de nivel 2 que contiene todos los enrutadores de nivel 2, pero a diferencia de OSPF, debe estar conectada físicamente.

- El esquema de dirección OSI identifica explícitamente el área objetivo de un paquete, permitiendo una selección sencilla de las rutas del modo siguiente:
    - Los enrutadores de nivel 2 enrutan hacia el área sin importarles su estructura interna.
    - Los enrutadores de nivel 1 enrutan hacia el destino si está en su área, o al enrutador de nivel 2 más cercano si no es así.
- Las redes multicast usan el concepto de DR ("Designated Enrutador"). Para evitar el problema "n(n-1)/2" en OSPF, IS-IS implementa un pseudo-nodo para la WAN. Se considera que cada enrutador conectado a la WAN tiene un enlace con el pseudo-nodo, pero ninguno con los demás enrutadores de la WAN. El DR actúa representando al pseudos-nodo.
- IS-IS integrado permite una mezcla considerable de las dos pilas de protocolo, sujeto a ciertas restricciones sobre la topología. Se definen tres tipos de rutas:
    - **IP-only:** Un enrutador que usa IS-IS como protocolo de enrutamiento y para IP, y no soporta protocolos OSI (por ejemplo, tales enrutadores no serían capaces de transmitir paquetes CLNP).
    - **OSI-only:** Un enrutador que usa IS-IS como protocolo de enrutamiento para OSI pero no usa IP.
    - **Dual:** Un enrutador que usa IS-IS como un único protocolo de enrutamiento integrado tanto para IP como para OSI.

Es posible tener un dominio mixto que contenga enrutadores IS-IS, algunos de los cuales son "IP-only", algunos "OSI-only" y algunos del tipo "dual". Cada área dentro de un dominio se configura como OSI, IP o "dual". Las áreas que han de soportar tráfico mixto deben tener todos los enrutadores de capa 1 del tipo "dual". Similarmente, los "enrutadores" de nivel 2 en un dominio mixto deben ser "dual" si el tráfico mixto se tiene que encaminar entre áreas.

V.3 BGP (BORDER GATEWAY PROTOCOL)

El Border Gateway Protocol (BGP) es un protocolo de enrutamiento entre Sistemas Autónomos (SA), sin este protocolo se tendrían graves problemas para el enrutamiento de la información en Internet y fue diseñado para solucionarlos. Es por ello que para un ISP es indispensable implementar este protocolo de enrutamiento, con el objetivo de poder interactuar con diferentes SA´s.

BGP no tiene ninguna restricción sobre la topología de la red, este sólo asume que el enrutamiento dentro de los Sistemas Autónomos esta funcionando correctamente, vía el IGP (OSPF, IS-IS, Enrutamiento estático etc). BGP genera una topología lógica de los SA´s en base a la información de enrutamiento. Generalmente esta topología lógica la podemos plantear como un *árbol*. Cada SA esta identificado por un número de Sistema, para poder adquirir un número de SA, es necesario hacer trámites con los organismos correspondientes.

V.3.1 FUNCIONAMIENTO DE BGP

BGP ocupa el protocolo TCP (puerto 179); esto asegura que todo el envío de información de enrutamiento llegará de forma segura a todos los enrutadores (Capítulo 3). Cuando se ocupa el protocolo TCP permite que las sesiones de BGP puedan darse entre enrutadores que no estén directamente conectados, como se muestra en la figura 5.3.1:

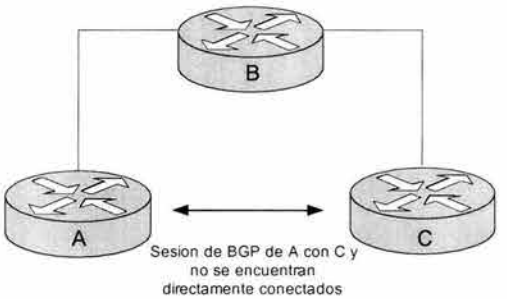


figura 5.3.1

Dos enrutadores que tengan activa una sesión BGP con el objetivo de intercambiar información de enrutamiento, serán referidos como **enrutadores vecinos;** estas sesiones son declaradas manualmente. Inicialmente cuando una sesión de BGP es establecida entre dos vecinos, todas la rutas de BGP son candidatas a ser intercambiadas, por otro lado cuando existe un cambio en la topología de la red solo se envía la información que cambió y no toda la tabla de enrutamiento. Lo anterior se muestra como una enorme ventaja para el procesamiento en los enrutadores.

Como ya se había mencionado, para que BGP opere correctamente requiere de un IGP o enrutamiento estático, una forma de explicarlo es que BGP conoce la red destino, pero BGP dentro del SA no sabe como alcanzarla, aquí es donde entra el protocolo IGP, el IGP sabe internamente como alcanzar esa red. Por lo tanto podemos decir que BGP opera en dos modos como: EBGP (BGP externo) intercambia rutas entre diferentes sistemas autónomos, y por otro lado encontramos IBGP (BGP interno). quien porta las rutas internas de direccionamiento de clientes, y dejar al IGP el soporte de la infraestructura para saber comó llegar al siguiente salto.

Formato del encabezado de los mensajes de BGP

Todos los mensajes de BGP tienen una encabezado de 19 Bytes, que constan de tres campos:

1. **Marcador:** Campo de 16 Bytes, y es usado para que el receptor pueda verificar la autenticidad del emisor, también sirve para detectar perdida de sincronización entre dos vecinos. El campo de marcador tiene alguno de los dos siguientes mensajes.
   - Un tipo de mensaje es el OPEN, este mensaje no requiere de autenticación, en este caso todo el campos se encuentra en 1´s
   - El segundo de ellos, es cuando el campo de marcador es analizado y forma parte del mecanismo de autenticación.
2. **Longitud:** Campo de 2 Bytes, y es usado para indicar el tamaño total del mensaje BGP, incluyendo el encabezado. El mensaje más pequeño es de 19 Bytes y el mas grande es de 4096 bytes.

3. **Tipo:** Su tamaño es de 1 byte e indica el tipo de mensaje que se puede enviar entre los que encontramos: OPEN, UPDATE, NOTIFICATION y KEEPALIVE.

Mensajes BGP

- **OPEN:** Es el primer mensaje que se envía para entablar una sesión de BGP. En adición al encabezado común del paquete, el mensaje OPEN tiene varios campos. El campo *versión* que provee un número de versión BGP (ej. Versión 4), y permite que el receptor verifique que esta ocupado la misma versión que el emisor. El campo *autonomous system* provee el número del SA del emisor. El campo *hold-time* indica el número máximo de segundos que pueden transcurrir sin recepción de un mensaje antes de que el transmisor asuma que la conexión finalizo. El campo *authentication code* indica que tipo de autentificación está siendo usado. El campo *authentocation data* contiene datos de autentificación actual.
- **KEEPALIVE:** Consta solamente del encabezado. Son mensajes enviados periódicamente entre enrutadores vecinos para mantener "viva" la sesión entre estos. Estos mensajes tienen que ser enviados antes de que el tiempo de envío expire.
- **UPDATE:** Facilita dos tipos de información; la de una ruta particular a través de un conjunto de redes, y la de una lista de rutas previamente anunciadas por este dispositivo para que sean anuladas Estas actualizaciones contienen toda la información necesaria para construir una tabla topológica de la red.
  1. **Network Layer Reachability Information (NLRI):** Indica cómo la ruta y el prefijo IP son anunciados.
  2. **Trayectoria de Atributos:** Habilita a BGP para detectar loops de enrutamiento y da flexibilidad para implementar políticas de enrutamiento local y global.
  3. **Rutas no Factibles:** Son mensajes para retirar rutas de las tablas de enrutamiento debido a que no son alcanzables.

- **NOTIFICATION:** Se envía cuando se detecta una condición de error, como por ejemplo, error en el encabezado del mensaje, error en el mensaje de OPEN y UPDATE, tiempo de mantenimiento expirado, error en la maquina de estados finitos entre otras.

Máquina de Estados Finitos

Para la negociación para la adquisición de un vecino es necesario que se genere una secuencia de estados antes de que la conexión quede establecida, en la Figura 5.3.2 se muestra de forma simplificada de como se da esta negociación entre dos enrutadores que desean establecer una sesión de BGP.

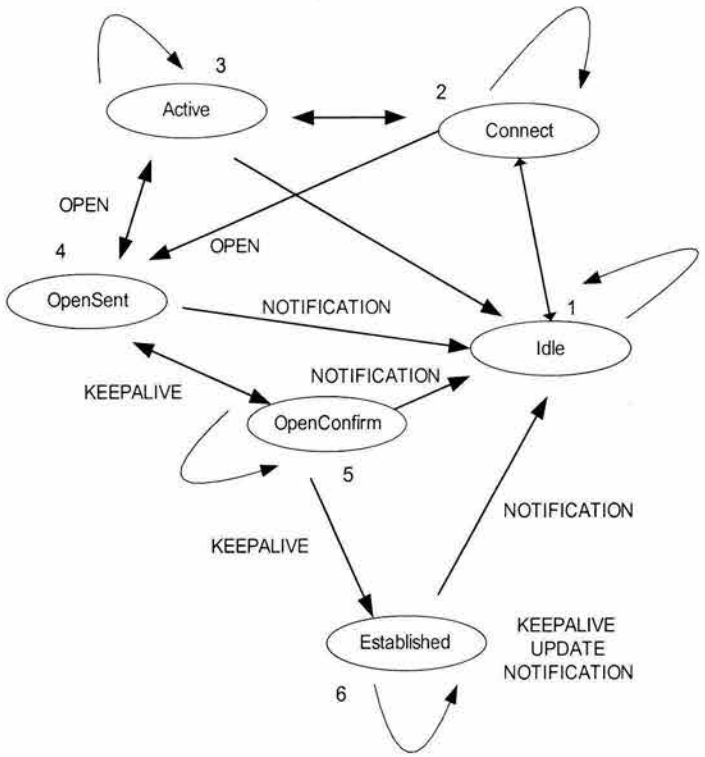


Figura 5.3.2

1. **Idle**: Es el primer estado de conexión. BGP esta esperando un evento de inicio. Inicializa la conexión de TCP para escuchar la respuesta del otro

enrutador. Una vez establecida esta negociación pasa al estado de Connect, si esta falla permanece en IDLE.

2. **Connect:** BGP esta esperando que la conexión del protocolo TCP sea concretada, si la conexión es exitosa, la transición se hace al estado de OpenSent (éste es el momento donde el mensaje de OPEN es enviado). Si la conexión no es exitosa se transita a una estado de Active; si el tiempo de ConnectRetry espira, se vuelve a reiniciar el estado de conexión, si no prospera este estado regresa a estado IDLE.

3. **Active:** BGP trata de que se inicialice la conexión TCP. Si ésta es establecida envía un mensaje de OPEN y pasa a estado de OpenSent. Si el tiempo para establecer la conexión expira se vuelve a iniciar el proceso anterior, o bien pasa a estado Connect. Esto sucede generalmente debido a que hay muchas retransmisiones de TCP.

4. **OpenSent**: BGP es esperando por el mensaje de OPEN de su vecino, al recibirlo es revisado para establecer la conexión. En caso de errores el sistema envía un mensaje de NOTIFICATION y regresa al estado IDLE. Si no hay errores, BGP comienza a enviar mensajes de KEEPALIVE. En este estado BGP reconoce, si la conexión es con un enrutador que pertenece al mismo SA o no, esto por medio del numero de SA que se envía en el mensaje de OPEN, si esta en el mismo SA, se implementa IBGP o bien si el numero de SA es distinto se establece en un modo de EBGP.

5. **OpenConfirm**: BGP espera un mensaje de KEEPALIVE, si es recibido pasa a estado de Established, en caso de no recibirlo se envían mensajes de NOTIFICATION, si la negociación no es completada pasa a estado IDLE.

6. **Established**: Es cuando la negociación entre los vecinos pasa a un estado donde pueden empezar a intercambiar mensajes de UPDATE. Aunque en este estado se siguen enviando mensajes de KEPPALIVE y de NOTIFICATION.

Atributos BGP

Los atributos en BGP son una serie de parámetros que son usados para mantener información especifica de una trayectoria, dar un grado de preferencia a una ruta, tener el siguiente salto de una ruta o información que puede ser agregada. Estos parámetros son usados en BGP para realizar funciones de filtrado y un generar procesos de decisión para una ruta. Un atributo esta formado de tres partes principalmente: <tipo de atributo , tamaño del atributo , valor del atributo>.

A continuación se presentan las cuatro categorías de atributos que se tienen en BGP:

1. **Well-known mandatory:** Es un atributo que debe de existir en el mensaje de UPDATE. Debe ser reconocido por todas las implementaciones de BGP. Por ejemplo si un atributo Well-known mandatory nos es incluido en el mensaje de UPDATE se genera un mensaje de NOTIFICATION de error, y la sesión se cierra. Esto es para asegurarse que todas las implementaciones con BGP coincidan, ejemplos de los Well-known mandatory son:
    - AS_PATH: Es un registro que contiene los SA por los que pasa la información para llegar a la red destino
    - NEXT HOP: Siguiente salto al enrutador para alcanzar la red destino.
2. **Well-known discretionary:** Es un atributo que es reconocido por todas las implementaciones de BGP, pero puede aparecer o no en el mensaje de UPDATE. Un ejemplo es:
    - Local Preference: Es una forma de anunciar cierta preferencia cuando se tienen dos opciones para enviar la información
3. **Optional transitive:** Este atributo opcional no es reconocido por todas las implementaciones de BGP, es decir, la implementación únicamente propaga el atributo aunque no sea soportado por esta. Un ejemplo es:
    - Comunity: Se le inserta una etiqueta para identificar de una forma mas sencilla las rutas.

4. **Optional nontransitive:** No se requiere que sean soportado por todas las implementaciones de BGP, por lo que si la implementación no lo soporta únicamente no lo propaga a otras redes de utilicen BGP.

Topología de los Vecinos en el IBGP

En el Protocolo IBGP se pueden presentar varias topologías con las cuales se puede implementar el protocolo, las más importantes son las siguientes:

IBGP Mesh

En este caso se establecen sesiones de IBGP con todos los enrutadores dentro del SA, es decir, siempre se declararan manualmente todos lo vecinos de BGP. Esto complica la configuración de los enrutadores, y no es escalable, permite trabajar sin sincronización. A continuación se presenta una figura donde se presenta esta topología:

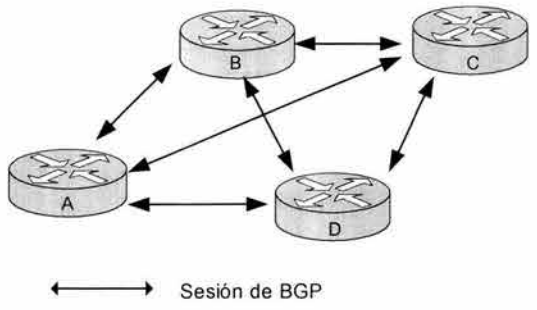


Figura 5.3.4

Route Reflector (RR)

Permite al Backbone denominar a un enrutador como el que realizara las actualizaciones a todos los enrutadores y a su vez todos lo enrutadores enviara sus actualizaciones a este enrutador, para que éste las propague, esto genera una topología lógica de estrella entre los enrutadores, se recomienda que en una red se tengan varios RR para una mejor administración y disminuir los puntos de falla. Algunos beneficios de esta configuración encontramos:

- No altera el envío de paquetes de información
- Puede coexistir con sesiones de EBGP
- Se pueden configurar múltiples RR para redundancia.
- Puede haber una jerarquía de RR.
- Es fácil escalar la red.

A continuación se presenta la figura 5.3.5 donde se muestra el funcionamiento de una topología con la incorporación de Route Reflector:

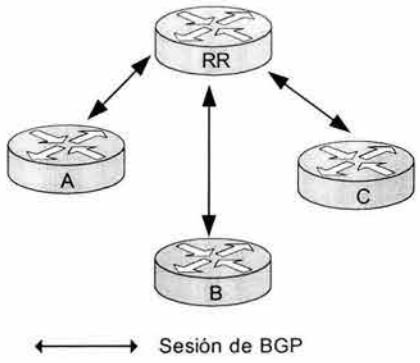


Figura 5.3.5

Se realizan actualizaciones de las rutas entre el Route Reflector y los enrutadores A, B y C. La forma de habilitar una ruta en la tabla de enrutamiento utilizando BGP sin implementar Route Reflector es la siguiente: Si un enrutador recibe una ruta de un vecino que pertenezca al mismo AS, no propagará la ruta.

A continuación se muestra el algoritmo para elegir la mejor ruta:

1. Local Preference
2. Local Route
3. Shortest AS-PATH
4. Lowest Origin
5. Lowest MED
6. EBGP path over IBGP path
7. Oldest Route from BGP path

8. Path with de lowest BGP ID
9. Path with de lowest IP address

V.3.1 MBGP (MULTIPROTOCOL BGP)

MBGP (Multiprotocol BGP) es un protocolo de distribución de información de enrutamiento empleando extensiones multiprotocolo y atributos de comunidades, define "quien" puede intercambiar información de enrutamiento con "quien". Este protocolo es ocupado principalmente para la distribución de información de enrutamiento de las VPN´s, es decir, una VPN depende de que MBGP le asigne un valor de Route Distinguisher (RD) –identificador básico de MBGP-.

Los RD son desconocidos para los usuarios finales, ésto les imposibilita tener acceso a la red. En MPLS-VPN, MBGP distribuye la información de envio de la tabla LFIB, acerca de cuales con los miembros que pertenecen a la misma VPN, proveyendo a la red de seguridad lógica. El proveedor de servicio es el que asocia una VPN especifica con cada interfase cuando se realiza la asignación de la VPN. Los usuario solo pueden participar en una Intranet o Extranet si y sólo si configuran de manera correcta un puerto lógico o físico con su respectivo RD. Lo anterior hace casi imposible que un usuario no autorizado entre una VPN.

Por lo tanto en el Backbone funcionará de la siguiente manera: El IGP distribuye la información de enrutamiento. Los enrutadores del Backbone configuran los LSP ocupando el protocolo LDP generando la tabal LIB. Esta información es distribuida a través de los enrutadores mapeando las tablas LIB ocupando MBGP, ya que a este protocolo le es más sencillo introducir la información de VPN.

Finalmente surge el termino VRF que es una extensión de enrutamiento IP que provee múltiples instancias de enrutamiento y separa el enrutamiento y el envío de cada VPN. VRF es ocupando en conjunto con MBGP ya este e distribuye la información de los VRF´s entre los enrutadores MPLS.

Los protocolos de enrutamiento son indispensables para el diseño de la red y son los de mayor impacto en la arquitectura de la red, de ahí la importancia de comprenderlos a fondo y elegir al que más convenga a las necesidades y metas de la red.

VI PASOS DE DISEÑO DE RED

En el presente capítulo presentaremos los conceptos y consideraciones básicas del proceso de diseño de red. Los temas en adelante expuestos se enfocan en lograr una red que presente un desempeño adecuado al ajustarse a las especificaciones, así como la manera más recomendable de implementar la red para mejorar su administración, facilidad de escalamiento, tolerancia a fallos y eficiencia.

Cabe mencionar en este punto, que la definición de los servicios a proporcionar en la red y su clasificación ya deberán haber sido resueltos. De la misma manera, se deberá contar con una aproximación de la cantidad y ubicación del tráfico y usuarios a recibir.

Comenzaremos proponiendo un modelo funcional de la red, donde conceptualizaremos las funciones y organización de los elementos de la misma. Nos apoyaremos en la descripción de topologías de servicio existentes, mencionando las características que buscamos en ellas, ventajas, desventajas y la descripción de sus componentes en función de la relevancia que consideremos tenga el modelo. Mencionaremos algunas implicaciones técnicas-administrativas de la construcción de una red orientada al Proveedor de Servicio.

Explicaremos las formas de interconexión física más utilizadas, sus características y ventajas. Las funcionalidades que corresponden a cada elemento de la red desde el punto de vista físico y la integración de topologías para conformar un diseño completo. Se tratarán aspectos relacionados con los nodos, interfases, redundancia, escalamiento y políticas de diseño.

Propondremos aspectos de la interconexión lógica de los nodos, para formar una red con un esquema de enrutamiento bien definido, sólido y escalable. Propondremos una topología lógica congruente con las necesidades de un Proveedor de Servicio, revisaremos parámetros y complementos del diseño lógico, así como la elección de protocolos de enrutamiento interno y externo, explicando y justificando las proposiciones en cada uno de ellos.

Finalmente, mencionaremos consideraciones que el Proveedor de Servicio debe tomar en cuenta en la forma de sus conexiones, así como la implementación de MPLS en el diseño como aplicación para maximizar el desempeño de la red.

VI.1 PASO 1 de 3 ESTRUCTURA FUNCIONAL

Diseñar y construir una infraestructura de red WAN escalable, fiable, tolerante a fallas y altamente disponible es difícil, ya que se debe tener un control administrativo total en todos los enlaces y equipos. Sin embargo, éste será el objetivo de nuestra red, ya que asegurando un diseño satisfactorio IP, los servicios que se brindarán así como aplicaciones adicionales (como es el caso de MPLS) no encontrarán dificultades en su implementación.

Para poder visualizar el sistema de comunicación en una red como un todo es conveniente utilizar el concepto de topología (o estructura de la red), debido a que éstas describen el funcionamiento y organización de la red. En esta etapa utilizaremos un enfoque administrativo y funcional el diseño de la red, y llegaremos a una propuesta fundamentada en las expectativas de un buen diseño que cumplan con las expectativas del Proveedor de Servicio, con capacidades de expansión y total capacidad para cubrir los requerimientos del cliente.

VI.1.1 DEFINICIÓN DE COBERTURA

Se debe definir perfectamente el área de cobertura a la que la red dará servicio, identificando dichas regiones por el tráfico que se espera concentrar de cada una de ellas, los usuarios que seguramente contratarán los servicios, el tipo de servicios que utilizarán, tráfico que se espera manejar en el futuro, políticas de crecimiento de la red, etc.

Este es el paso inicial para comenzar a proponer alguna topología de red, ya que al identificar los orígenes del tráfico que se manejará tendremos la capacidad de localizar los puntos de mayor interés, organizarlos, agruparlos, o simplemente definir la forma de proceder con el flujo de los datos al proyectar la forma de utilización de la

red de manera óptima para la transmisión de información y administración de tráfico y usuarios.

VI.1.2 TOPOLOGÍAS DE SERVICIO

Con miras a obtener un diseño de red satisfactorio, como primer paso de diseño consideremos la Topología de Servicio en que nos basaremos para la conceptualización de la red en diseño.

Características Buscadas

Estructura

Se sugiere que la Topología de Servicio cuente con una estructura bien definida, ofreciendo la ventaja de crear límites en caso de ocurrencia de fallas, así como facilitar la administración y conceptualización de la red.

Jerarquía

Esta característica brinda a la red una estructura funcional dado que divide la red en entidades con funciones específicas y únicas; logrando con esto asignar tareas y funcionalidades específicas a cada parte de la red.

Modularidad

La modularidad simplifica cualquier tarea de diseño, implementación o actualización de la red al crear bloques de construcción manejables. Un modulo es un bloque constructivo funcional definido por las funciones que realiza, no por los dispositivos que utiliza. Esta característica proporciona:

- Facilidad de crecimiento
- Administración distribuida
- Aislamiento de fallas y su reparación
- Impacto de fallas fácilmente reconocible

Al realizar el diseño con estas tres características se aseguran los siguientes beneficios para la red:

- Tener óptimo desempeño en el envío de paquetes
- Enrutamiento y crecimiento escalable
- Fiabilidad y disponibilidad de la red
- Mejora del desempeño de red
- Proveer una base firme para la implementación de servicios

- Facilidad de administrar cambios
- Balance costo – eficiencia
- Reducir costos del operador

A continuación, mencionamos algunas topologías probadas y documentadas haciendo notar sus beneficios y problemas inherentes.

Topología de Una Capa (Diseño Distribuido o Simpler)

Un diseño de una sola capa se implementa normalmente en redes pequeñas, cuando el acceso remoto es limitado y la mayoría de las aplicaciones y/o usuarios pertenecen al área de la red. La clave para decidir el diseño específico la da la localización de los orígenes de tráfico de datos; éstos pueden estar distribuidos a través de diversas localizaciones, o concentrados en una localización central. El diseño de una capa es típicamente implementado donde existen pocas locaciones remotas en la red y el acceso a las aplicaciones se hace principalmente en el área de la red o el origen de datos es local. La principal desventaja de esta topología es su difícil interconexión con redes externas y su dificultad de ser escalable en equipos o dominios. Funciona bien si únicamente se quieren conectar los equipos de una red sin prioridad de unos sobre otros, o diferencia en sus funciones.

Topología de Dos Capas

Esta topología se aplica cuando una interfase es utilizada para interconectar varias redes separadas. Un enrutador se convierte en un punto de concentración de interfases, ocasionando la presencia de una capa encargada del transporte de datos en el área, y una capa encargada de la interconexión con redes externas. Este diseño funciona bien con redes bien definidas en su interconexión, ya que ofrece poca flexibilidad al cambio. Los nodos de la red funcionan recibiendo el tráfico de datos o conmutándolo para alcanzar otras redes.

Topología de Tres Capas (Modelo Jerárquico)

El diseño más escalable para implementación de redes WAN es el Modelo Jerárquico donde cada capa desempeña una función particular y requiere un diseño también particular, dado que se aplican diferentes reglas y criterios para cada una.

Cada nodo en la red pertenecerá a una capa en específico dependiendo de la función que realice en la red en el tránsito de información. Se considera a los enrutadores como puntos de decisión de caminos de los datos. En este modelo, el

tráfico de datos fluirá fuera del nivel de jerarquía al que pertenece, únicamente tan lejos como lo necesite para encontrar el destino de la información. Se enfoca a decidir la ubicación de los enrutadores, pudiendo asignarlos de acuerdo a los usuarios, tráfico o Ancho de Banda WAN disponible.

Componentes

- Backbone (Core layer)
- Capa de Distribución (Distribution layer)
- Capa de Acceso (Access layer)

La conceptualización de la topología de tres capas se muestra en la figura siguiente, observando que los servicios de ciertas capas son requeridas por otras.

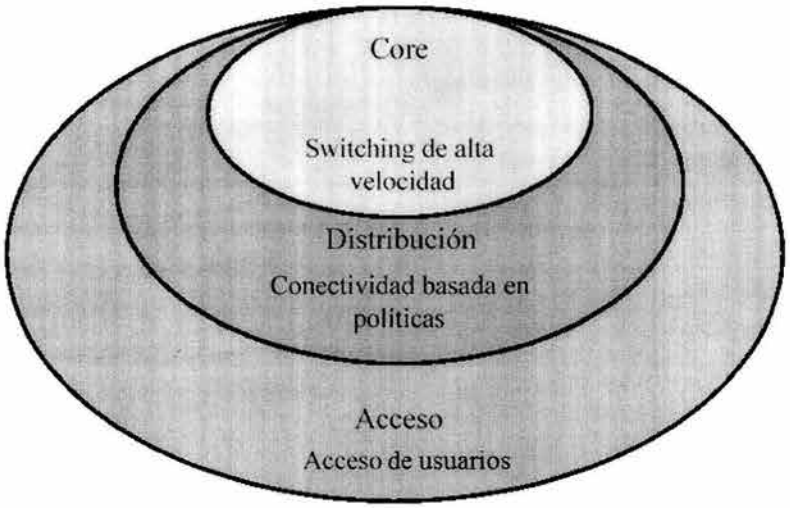


Figura 6.1.1

La implementación del modelo Jerárquico con equipos de conmutación se ejemplifica a continuación, observando la separación entre las capas, y el flujo de información entre ellas.

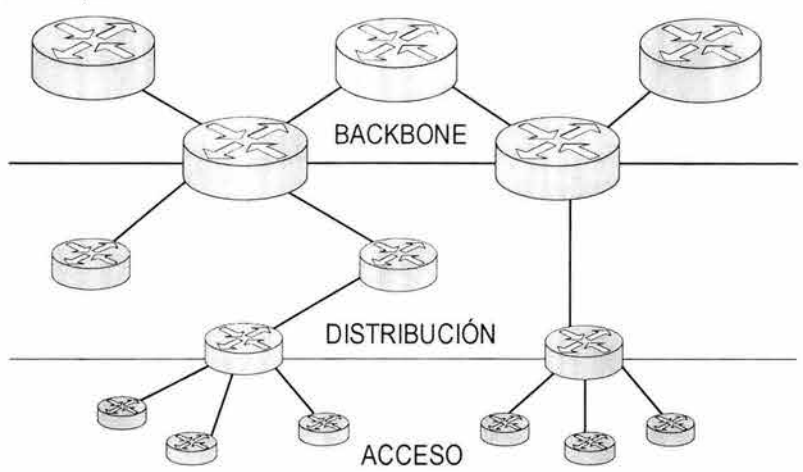


Figura 6.1.2

Backbone (Core layer)

Provee conexiones WAN rápidas entre sitios geográficamente remotos, ya sea que se trate de unir redes más pequeñas, corporaciones o ISPs.

Las interfases del Backbone son usualmente punto a punto. Los servicios del backbone son típicamente los más requeridos a un proveedor de servicios de telecomunicaciones (con diferentes tecnologías desde E1/E3 hasta SONET/SDH).

No manipula los datos, sólo los enruta a su destino. Concentra nodos de Distribución, nunca clientes directamente. Posee redundancia lógica en interfases y equipos. En esta capa es donde se asigna el mayor Ancho de Banda.

Funciones y Objetivos:

- Minimizar interfases conectadas a los nodos.
- Definir y minimizar el número de saltos entre los nodos.
- Balancear la carga de tráfico para generar un diseño óptimo.
- Optimizar el transporte entre sitios remotos y trayectorias.
- Proporcionar trayectos redundantes.
- Lograr rapidez de convergencia.
- Usar eficientemente el Ancho de Banda.
- Proveer tolerancia a fallas.
- Proporcionar rápida adaptación de cambios.

- Ofrecer baja latencia y buena administración.
- Poseer una tasa consistente de Ancho de Banda.
- Evitar Particionamiento de la Topología (significa que con la caída de ciertos enlaces la red quede aislada).

Capa de Distribución (Distribution Layer)

Se encarga de proporcionar los servicios de la red a múltiples subredes dentro de secciones de red determinadas. Esta capa es implementada en lugares grandes y se utiliza para interconectar regiones o ciudades y distribuir tráfico. En esta capa se manipulan los paquetes. Administra indirectamente el Ancho de Banda del Backbone y constituye límites entre protocolos de enrutamiento. Está demarcada entre Backbone y Capa de Acceso, concentra nodos de Acceso y es camino obligado de tránsito hacia el Backbone. Puede contar con redundancia en sus enlaces hacia el Backbone para garantizar su conexión.

Funciones y Objetivos:

- Conectividad basada en políticas del ISP.
- Control de protocolos de acceso a los servicios.
- Definición de métricas de los trayectos.
- Anuncios de control de la red.
- No existen nodos finales (Acceso) ni nodos de direccionamiento (Backbone).
- Crea un camino de transito para el trafico entre usuarios pertenecientes a una misma área de servicio.
- Implementa políticas de red.
- Administra y proporciona seguridad.
- Sumariza y agrega direcciones.
- Define bordes de dominios para evitar fallas.
- Efectúa translación de medios de transmisión.
- Realiza redistribución entre dominios de enrutamiento.
- Demarca dominios de protocolos de enrutamiento estáticos y dinámicos.
- Posee capacidad de filtrado.

Capa de Acceso (Access Layer)

No concentra nodos de la misma Capa o superiores. Provee a los usuarios, grupos de usuarios (usuarios con características en común) o empresas, de acceso a los servicios de la red. La Capa de Acceso es donde todos los equipos del usuario son incluidos en la red.

Recibe los paquetes de las aplicaciones del cliente (Voz, Datos, Video), efectúa la marcación del los paquetes con QoS y los encripta si es necesario. Los nodos de Acceso enrutan todo el trafico al nodo local de Distribución en su camino al Backbone. Se caracteriza por ser conmutada y compartir el Ancho de Banda. Se diseña con redundancia en sus interfases hacia Distribución, con capacidades relacionadas con el tipo de tráfico que será recibido por el nodo.

Funciones y Objetivos:

- Conecta redes de clientes a la red.
- Provee segmentación lógica a la red.
- Agrupa usuarios con intereses en común.
- Realiza manipulación alta y exhaustiva del tráfico.
- Asigna características de: Vigilancia, Seguridad, Servicios, Direccionamiento y Marcado de QoS.
- Efectúa filtrado intensivo de paquetes e incluso aplicaciones.

Beneficios del Modelo Jerárquico

- *Escalabilidad: Las redes que siguen el Modelo Jerárquico pueden crecer* mucho más sin sacrificar control o facilidad de administración porque la funcionalidad es local y los problemas potenciales pueden ser reconocidos más fácilmente, ya que éste concepto hace referencia a la capacidad del sistema para mantener y mejorar su rendimiento medio conforme aumenta el número de clientes.

  El nivel de escalabilidad intrínseco de un sistema distribuido no puede detectarse fácilmente con una herramienta de control o análisis. Por otro lado, existe una serie de aspectos de implementación (abundancia de recursos críticos, cuellos de botella en el diseño, etc) que constituye una clase de prueba circunstancial del nivel de escalabilidad.

- *Facilidad de Implementación*: El diseño jerárquico asigna una clara funcionalidad específica a cada capa, es por eso que hace la implementación de la red más fácil.
- *Segmentación del impacto de fallas*: Dado que las funciones de las capas individualmente están bien definidas, el aislamiento de los problemas en la red es menos complicado. Segmentar temporalmente la red reducirá el alcance del problema, lo cual es sencillo.
- *Predictibilidad*: El comportamiento de una red usando capas funcionales es mucho más predecible, lo cual hace la capacidad de planeación del crecimiento mucho más fácil; este diseño suministra también facilidades de modelar el desempeño de la red para propósitos analíticos.
- *Soporte de protocolos*: La mezcla de aplicaciones y protocolos actuales y futuros será mucho más fácil en las redes que sigan los principios jerárquicos en su diseño dado que la infraestructura existente ya se encuentra organizada lógicamente.
- *Disponibilidad*: Los sistemas Jerárquicos ofrecen elevada disponibilidad y un nivel de servicio aceptable con tiempos de inactividad despreciables. Los tiempos de inactividad perjudican a las empresas porque reducen su productividad y aumentan las pérdidas de ventas y la desconfianza de los clientes y socios.
- *Seguridad*: La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las terminales distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder furtivamente a datos de carácter confidencial. En este punto, un diseño Jerárquico bien desarrollado posibilita la implantación de políticas para resguardar la información de la red.
- *Gestión*: La labor de mantenimiento y operación de una WAN exige dedicación completa al considerar que la red está geográficamente dispersa. El modelo Jerárquico ofrece ventajas en los principios básicos de la gestión de redes distribuidas y heterogéneas.

- Administración: Todos los beneficios listados contribuyen a ampliar la facilidad de administración de la red, los cuales son originados a partir de un buen diseño de la misma.
- *Modelo de tráfico (método para controlar datos)*: Al colocar puntos de enrutamiento a través de la red, donde los nodos son puntos de decisión de caminos de los datos, el tráfico de datos fluirá fuera del nivel de jerarquía propio, únicamente tan lejos como lo necesite para encontrar su destino, evitando recurrir al uso de Backbone e incluso Distribución cuando sea posible.

VI.2.3 CONSIDERACIONES DE ADMINISTRACIÓN

Límite de Responsabilidad

El Proveedor de Servicio, en su ofrecimiento de SLA, debe ser muy preciso en el ofrecimiento de nivel de servicios hacia el cliente, pero también en el punto en que empieza y termina dicho acuerdo.

Lo anterior se hace evidente si consideramos las complicaciones en los enlaces WAN, ya que en el tránsito de los datos hacia una red externa al proveedor, se utilizarán los enlaces de varios Proveedores de Servicio, los cuales podrían no cumplir con las condiciones básicas necesarias para sostener el acuerdo del SLA. Por lo tanto, propondremos que desde el punto de acceso a la red del Proveedor hasta el puerto de salida de su enrutador más lejano en la trayectoria, el contrato de SLA será cumplido, más allá será el mejor esfuerzo por parte del Proveedor, y entera responsabilidad del Proveedor por el que transite la información.

Dentro de los servicios adicionales ofrecidos al cliente se podrá aceptar que el enrutador del cliente sea administrado por el proveedor de servicio, sin embargo ésta es solo una opción extra al contrato, ya que el proveedor en operación normal se encargará de recibir el tráfico del enrutador del cliente, sin administrarlo.

Conexión con otros ISPs (Peering y Multi-Homming)

Se propondrá un punto en la topología de la red para la conexión con otros ISPs (Peering). Deberán establecerse políticas de conexión con los otros proveedores, así como propias para evitar la interferencia de los esquemas de enrutamiento ajenos en los propios, y viceversa.

Los puntos físicos específicos de interconexión serán elegidos en función de nuestras políticas como Proveedor de Servicio, las cuales podrán incluir entre los criterios decisivos, la cantidad de tráfico que transita por al zona o la cercanía geográfica al Proveedor con el que se efectuará al conexión.

Al diseñar una red WAN confiable y consiste, una alternativa es que la red del usuario cuente con más de un punto de entrada a Internet (Multi-Homming). Esto provee tolerancia a fallas para aplicaciones que requieran acceso a Internet y alta disponibilidad para empresas con servidores de acceso publico; sin embargo, desde la óptica del Proveedor de Servicios, debe considerarse desde la fase de diseño de la red para evitar repercusiones de las configuraciones y tráfico del usuario así como de los otros proveedores a los que se conecta la red propia.

VI.2 PASO 2 de 3 TOPOLOGÍA FÍSICA

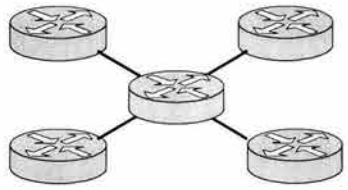
Como segundo paso en el diseño de la red, y conociendo las opciones de Estructura Funcional con que pudiera plantear la solución de red, tenemos que considerar la forma en que físicamente los nodos de la red se conectarán entre ellos. En este sentido existen diversas formas preestablecidas y probadas de interconectar los nodos, y mientras unas tienen ventajas y desventajas sobre otras, trataremos de aprovechar las bondades en el nivel de servicio que ofrece cada una par elegir la más conveniente.

También mencionaremos aspectos que los enrutadores e interfases deberán considerar y cumplir para el correcto funcionamiento de la red. Además, basados en las consideraciones de la Estructura Funcional de la Red, propondremos la conexión de equipos en función de las diferentes etapas de la red, y servicios ofrecidos.

A continuación se explican algunas posibilidades sin olvidar que típicamente las redes WAN tienen topologías combinadas, no estrictamente apegadas a una topología física única, o simplemente irregulares.

VI.2.1 TOPOLOGÍAS FÍSICAS

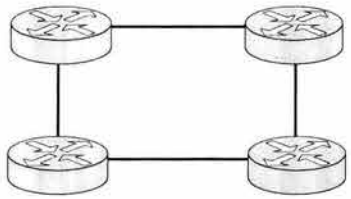
Estrella



En este esquema, todos los nodos están conectados a un nodo central, y como es una conexión de punto a punto se necesita una interfase desde cada estación al nodo central. Una ventaja de usar una red de estrella es que ningún punto de falla inhabilita a ninguna parte de la red, sólo a la

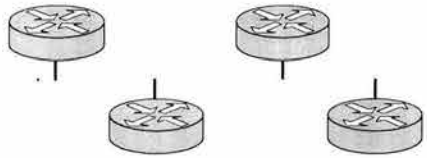
porción en donde ocurre la falla, y la red se puede seguir operando de manera eficiente. Un problema que puede surgir es cuando al nodo central le ocurra un error se verán afectados todos los nodos, dado que dependen directamente de él.

Anillo



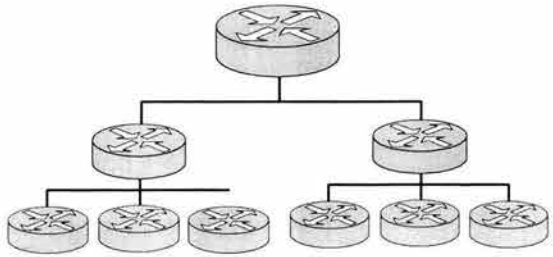
En esta configuración, todos los nodos reenrutan la señal mandada por el nodo transmisor hasta llegar a su destino. El mensaje se transmite de nodo en nodo por cada uno de ellos hasta que se alcanza el destino de la transmisión. Una desventaja con esta topología es que si algún nodo falla, podría afectar severamente el funcionamiento general de la red, aunque el administrador puede sacar el nodo defectuoso de la red, así evitando algún desastre.

Bus



También conocida como topología lineal de bus, es un diseño simple que utiliza una interfase, a la cual todos los nodos se conectan. La topología usa un medio de transmisión compartido por todos los nodos colocados típicamente en la misma localización geográfica, ya que todos los nodos pueden recibir las transmisiones emitidas por cualquier otro nodo. Como es bastante simple la configuración, se puede implementar de manera barata. El problema inherente de este esquema es que si la interfase se daña en cualquier punto, ningún nodo podrá transmitir.

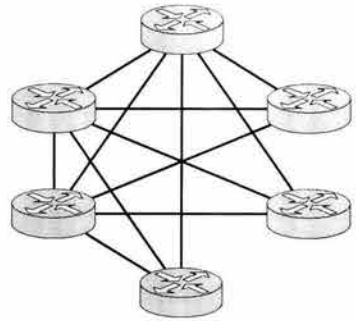
Árbol



Esta topología es un ejemplo generalizado del esquema de bus. El árbol

tiene su primer nodo en la raíz, y se expande hacia afuera utilizando ramas, en donde se encuentran conectados los demás nodos. Ésta topología permite que la red se expanda, y al mismo tiempo asegura que solo existe una ruta de datos (data path) entre 2 nodos cualesquiera.

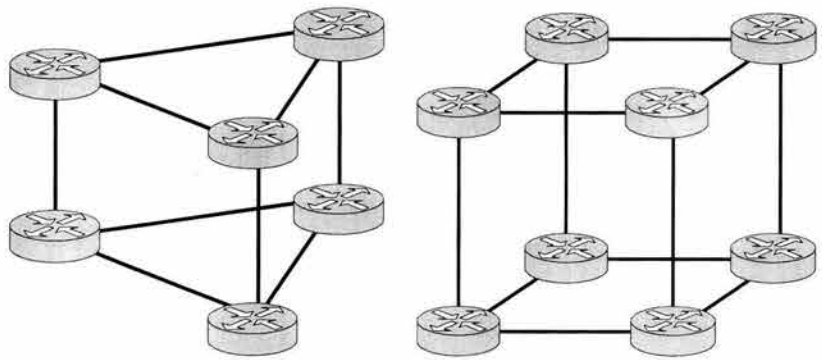
Full Mesh / Partial Mesh



En esta topología, cada nodo se encuentra conectado directamente con todos y cada uno de los demás nodos de la red (Full Mesh) o con la mayoría (Partial Mesh), implica una alta redundancia y confiabilidad, pero mayor costo, dificultad de configuración y resolución de problemas, sobre todo de enrutamiento y administración.

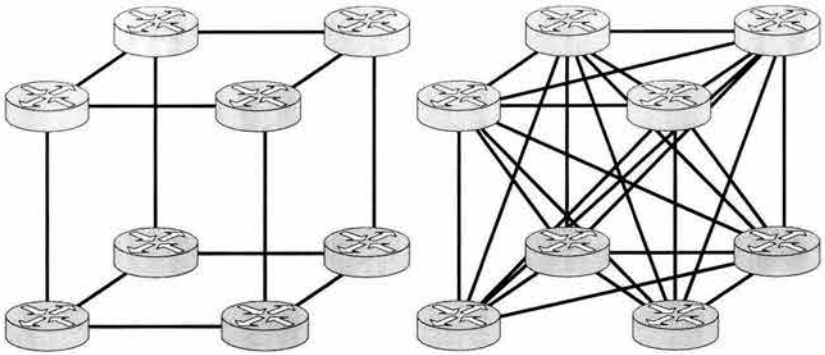
HiperCubo

En esta topología, los nodos se colocan en los vértices de un cubo imaginario (o prisma en general), conectando a todos ellos por medo de interfases que siguen las aristas de dicho prisma. Este diseño optimiza la conexión entre los nodos, proveyendo la redundancia suficiente para evitar una Fragmentación del Backbone sin desperdiciar recursos como el caso de Full Mesh.



Comparando el caso de contar con 8 nodos, observamos las diferencias comparativas en la tabla; además, deducimos que es más difícil de escalar y actualizar por que se en cada modificación de la topología de la red, se requiere también un cambio en cada enrutador, lo que resulta lento y caro (enrutadores más n-1 interfases)

	HiperCubo	Full mesh
Número de nodos	8	8
Interfases	24	56
Circuitos	12	28



VI.2.2 PROPIEDADES DE LOS ENRUTADORES EN FUNCIÓN DE LA CAPA A LA QUE PERTENECEN

Enrutadores de Capa de Acceso -PE (Provider Edge Router)-

Es el enrutador de último salto (last hop) en la red del Proveedor. Este enrutador provee conectividad con la red del Proveedor de Servicios al conectarse con el enrutador de frontera del usuario (CPE). El enrutador PE puede o no ser conciente de cualquier funcionalidad MPLS en función de las aplicaciones que maneje hacia el usuario.

El enrutador PE puede ser responsable de la clasificación y marcado de paquetes para asegurar que el tráfico será tratado apropiadamente por la red conforme a los acuerdos con el Proveedor; adicionalmente podrá ser requerido para realizar manejo de tráfico y asegurar que ningún paquete sea marcado como descartable y así para ajustarse a la taza acordada en la contratación del servicio.

El enrutador PE es requerido para proveer QoS para paquetes originales de IP (en el enlace PE a CPE), así como paquetes etiquetados de MPLS (en los enlaces PE a P). El enrutador PE también provee manejo de tráfico, pero no reclasificación de paquetes.

Enrutadores de Distribución y de Backbone -P (Router Provider)-

Son dispositivos del Backbone o Distribución del proveedor (configurados para soportar MPLS). Ninguna definición de las aplicaciones que transitarán es necesaria en esos dispositivos. Básicamente su función es formar la capa en la jerarquía que se encarga de la conmutación rápida de datos.

Todas las funciones modulares de QoS están disponibles para vigilar y encolar el tráfico basados en los bits EXP.

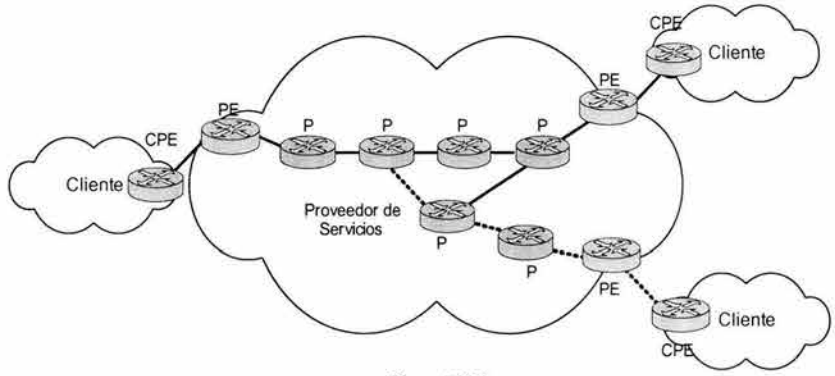


Figura 6.2.10

VI.2.3 INTEGRACIÓN DE TOPOLOGÍAS

En base a la estructura funcional analizada en el capítulo anterior, y con la aplicación de las topologías mencionadas en el principio de este capítulo, proponemos un diseño físico de red, el cual aprovechará las ventajas de una estructura Jerárquica en Tres Capas, implementada por medio de las siguientes topologías físicas:

- Backbone: Se implementará con topología HiperCubo para lograr máxima conectividad, así como minimizar los recursos para lograrla.
- Distribución: Implementaremos una estructura en estrella o en su defecto, un solo nodo; con el objeto de lograr la cobertura que se asigne conservando una topología fácilmente administrable en la red.

- Acceso: En esta capa se usará una topología en árbol, con el fin de lograr que la capa superior recopile todo el tráfico sin esfuerzo, y a la vez, poder ofrecer acceso a la red a cualquier usuario.

Basándonos en la descripción anterior, el Módulo de Construcción Básico que al replicarse en torno a los nodos de Backbone conformará la estructura de la red, puede conceptualizarse como lo muestra la figura:

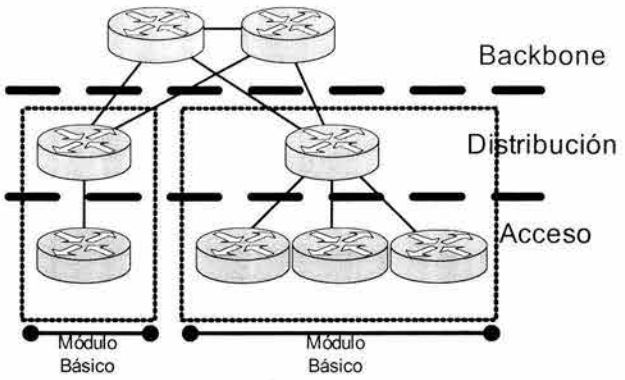


Figura 6.2.11

Como podemos observar en las siguientes posibilidades de expansión de cualquier Módulo Básico de la topología física sugerida, las posibilidades de escalamiento que posee dicha elección aseguran un fácil y seguro crecimiento de la red según las políticas de diseño, ya que podrán resolverse los requerimientos mínimos de transporte de tráfico con un mínimo de infraestructura sin perder la organización jerárquica, así como ajustarse a las diversas posibilidades de crecimiento de la red, basándonos en modificaciones simples del modelo original.

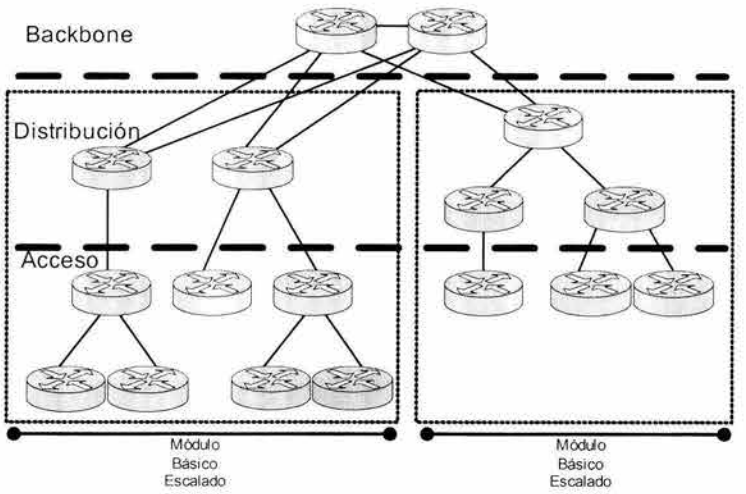


Figura 6.2.12

La implementación física de una topología de esta naturaleza facilita la implementación de módulos del mismo tipo en la red, asegurando que por sus características funcionarán óptimamente, que cada módulo podrá ser situado en cualquier parte de la red sin problemas de compatibilidad y las capacidades de escalamiento de la red en su totalidad serán satisfactorias.

VI.2.4 NODOS E INTERFASES

Ancho de Banda de Interfases

La capacidad del enlace será medida por el Ancho de Banda, que es un indicador de la cantidad de datos que pueden transmitirse en determinado periodo de tiempo por un canal de transmisión, en nuestro caso en bits por segundo (bps), y deberá ser lo bastante grande para poder pasar toda la información.

En lo respectivo al diseño físico, debe considerarse cuál es la necesidad real de Ancho de Banda a utilizar, tanto para soportar el tráfico de las aplicaciones de los usuarios que utilizarán la red, como la expectativa de crecimiento a futuro.

Las interfases con que los nodos se conectarán serán definidas en función de la capa a la que cada nodo pertenezca, considerando un nivel de utilización del 70 u 80% en el enlace principal, y un segundo enlace sugiriendo la misma capacidad en

caso de ser requerido para asegurar la conectividad entre los nodos y redundancia (backup).

Los valores sugeridos para los enlaces están en función del tamaño y funcionalidad del nodo, se sugiere aplicar enlaces STM1 a STM16 en Backbone, para Distribución de **E3** a STM1, y en Acceso típicamente E0, E1 o E3, todos ellos dependientes de la cantidad de tráfico que pase por ellos, sobre todo en Acceso, donde su tráfico se afecta directamente del tipo de aplicaciones que el nodo en específico provea.

Redundancia y Conexiones

En este punto se deben considerar los nodos más recomendables para interconectar la red del ISP a uno mayor en la mayoría de los casos, para asegurar la salida a Internet, por lo que se propondrán los nodos de conexión, interfases y acuerdos con la compañía con la que se conecte.

Se aplicará el concepto de redundancia de la siguiente manera en función de la capa en que se localice el nodo:

- Backbone: Proponemos redundancia de equipos, un enlace principal y uno redundante sugiriendo la misma capacidad.
- Distribución: Se sugiere redundancia en enlaces a dos nodos Backbone diferentes. Puede efectuarse distribución de carga en dichos enlaces.
- Acceso: Opcionalmente podrán agregarse enlaces redundantes al nodo de Distribución correspondiente

Elección de los Nodos:

Deben de considerarse las características de los equipos que integrarán la red, Primordialmente en función al tipo de servicio que prestará en la red, y en general, basándose en capacidades como:

- Ancho de Banda: Es un aspecto importante, dado que este aspecto limitará la capacidad de transmisión de información por los elementos de la red.
- CPU: Como norma general, se intentan proporcionar las prestaciones de procesamiento suficientes para que el uso de la CPU se mantenga por debajo del 80%.
- Memoria: El principal objetivo consiste en proporcionar la memoria suficiente para soportar los protocolos, tablas y aplicaciones en el equipo.

- Chasis: El chasis del equipo debe proveer las funciones que el proveedor de servicios demanda en su diseño como las siguientes:
  - Tamaño y facilidad de instalación (normalmente en racks)
  - Suficientes *line-card slots* e *interface slots* para recibir las tarjetas de interfases
  - Sistema de ventilación
  - Facilidades de administrar conexiones de cables de fibra y coaxiales densas
  - Conectores de interfases y energía seguros
  - Flujo de aire del frente a atrás
  - Fuente de poder redundante y de suficiente capacidad
- Puertos: Dependiendo de la función y Capa de pertenencia del enrutador, deberá especificarse un número mínimo de ellos, así como especificar su tipo y características
  - Puertos Gigabit Ethernet WAN
  - Puertos Fast Ethernet
  - Puertos Seriales
  - Puertos con soporte de tráfico simple o multiplexado en rangos: DS0, E1 - E3, OC1 – OC12, STM1 – STM16 en función del tipo de enrutador
  - Facilidades de encolamiento en los puertos WAN
  - Soporte para protocolos y aplicaciones específicas (MPLS, VPNs, AToM, QoS, manejo de tráfico, etc.)
  - Soporte para diversos protocolos aplicados en la red (PPP, HDLC, etc.)
  - Se sugiere contar con un MODEM conectado y habilitado en el puerto auxiliar del enrutador para facilitar la resolución de problemas, sobre todo de manera remota.
- Software: Debe ser congruente con las características físicas del equipo, así como con el tipo de tráfico que transitará por éste, algunos puntos importantes a considerar:
  - Versión del Sistema Operativo y Actualizaciones

- Facilidades de Análisis de la Red (*Network análisis*), con capacidades como: Análisis de Tráfico, Monitoreo Remoto, y facilidades de resolución de fallas en forma remota.
- Módulos aceleradores (de VPNs por ejemplo)
- Soporte de tecnologías y protocolos necesarios (MPLS por ejemplo)
- Funcionalidades administrativas como Balanceo de carga y Encriptación

- Parámetros: Debemos considerar características como:
  - Baja Latencia
  - Alta Disponibilidad
  - Soporte de los Protocolos de red utilizados
  - Soporte de los Protocolos de enrutamiento utilizados
  - Facilidad de implementar filtrado de paquetes
- Propiedades del equipo
  - Facilidad de configuración
  - Protocolos de administración
- Proveedor del Equipo:
  - Disponibilidad y calidad soporte técnico
  - Disponibilidad y calidad de documentación
  - Disponibilidad y calidad de entrenamiento
  - Reputación y viabilidad del enrutador
- Análisis de Costo/beneficio

Criterios para posicionar los Nodos

Para decidir la ubicación física de los nodos, nos ayudará una estimación de los usuarios que puedan requerir el servicio, lo cual permitirá dimensionar los recursos. Para realizar dicha estimación podemos referirnos a la propuesta de Estructura Funcional realizada en el capítulo anterior.

Se buscará asegurar al posicionar un nodo, un lugar seguro y específicamente dedicado para alojar el nodo correspondiente, que cuente con un suministro de electricidad constante así como facilidades adicionales como implementación de aire

acondicionado en caso de ser necesario, y que tenga una ubicación conveniente respecto a los nodos restantes de la red.

VI.2.5 POLÍTICAS DE DISEÑO

Escalando la red (tráfico)

Conforme la red crece y el número de usuarios aumenta, el requerimiento de flujo de tráfico por los nodos se ve incrementado rápidamente. Ante esta situación, diversas soluciones son sugeridas, entre ellas:

Migración de capa del nodo

Puede sugerirse migrar el nodo a una capa superior debido a la cantidad de trafico que es necesario conmute y las funciones que debe realizar; ya que la pertenencia de un nodo a la capa en que fue instalado por primera vez depende solamente de políticas del administrador de la red, un nodo en específico podrá cambiar de capa para facilitar la administración o conservar la congruencia con los criterios especificados en el diseño (ya sea por el área a la que sirve, tipo de tráfico o tipo de nodos que se conectan a él).

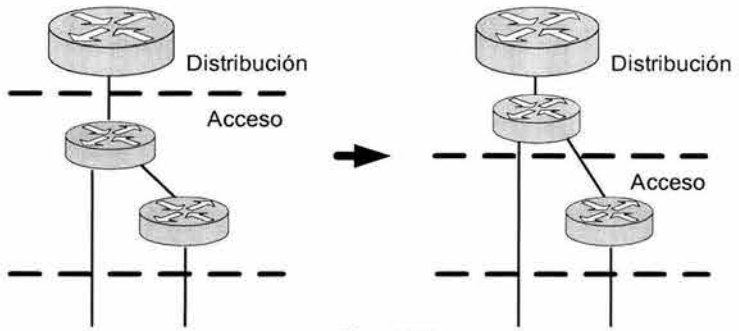


Figura 6.2.13

Esta solución, aunque útil en algunos casos, implica la transformación de la topología de la red, ocasionando cambios que pueden afectar notablemente la facilidad de interconectar los equipos para cumplir con las especificaciones físicas propuestas por el diseñador, o impedir agrupar los nodos lógicamente como se tenía previsto.

Aumento de capacidad del nodo

Como segunda opción se propone escalar la capacidad de transmisión y/o procesamiento del equipo, así como el Ancho de Banda de sus enlaces; esta situación

es originada nuevamente por el aumento en el tráfico o servicios a transmitir por este nodo en específico.

Regularmente, la capa a la que se solicita aumento en su capacidad de transmisión de tráfico en un primer momento es el Acceso, pudiendo agregar equipos o aumentar la capacidad de los existentes para solucionarlo.

Figura 6.2.14

Respecto a la Capa de Distribución, el aumento en el tráfico o área de servicio, ocasionará mayor demanda de recursos y procesamiento, los cuales solucionaremos aumentando la capacidad de los equipos y/o agregando un nivel más dentro de la misma capa.

Figura 6.2.15

Finalmente, el Backbone será escalado únicamente en sus equipos, pudiendo aumentar su capacidad o colocar enrutadores en paralelo con el original.

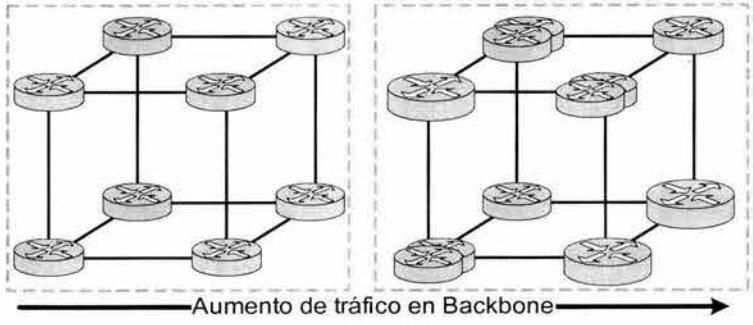


Figura 6.2.16

Escalando la red servicios

El aspecto de cantidad o crecimiento de los servicios ofrecidos por un nodo en la red impactará directamente a la Capa de Acceso, ya que es ella la encargada de ofrecer los servicios directamente al usuario.

Al aumentar los servicios ofrecidos, o bien, el tipo de acceso a ellos, pueden proponerse diferentes topologías a partir del siguiente esquema básico:

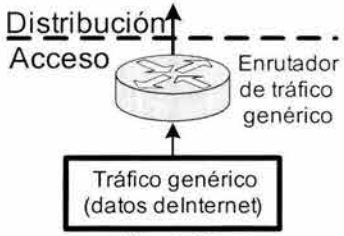


Figura 6.2.17

Tráfico de Datos (Internet)

Todos los enrutadores de acceso tendrán la capacidad de conmutar tráfico de datos (Internet principalmente), pueden agregarse enrutadores con jerarquías menores para facilitar la administración y recepción del tráfico de los usuarios

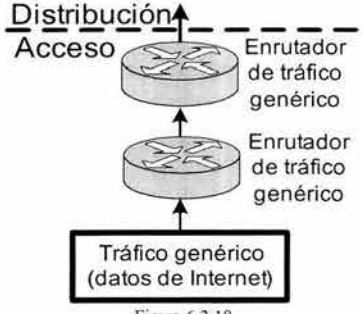


Figura 6.2.18

Tráfico MPLS (VPNs)

Se sugiere el uso de un enrutador encargado del manejo y administración de las redes que requieren MPLS, tal como VPN's. La proposición anterior es con la intención de simplificar las configuraciones en los equipos, así como reducir la complejidad inherente a cualquier cambio.

En el caso de VPN's, la interfase de entrada en el enrutador CE es configurada para definir la VPN especifica a la cual el cliente esta conectado. El enrutador CE es

responsable de asignar una etiqueta a cada VPN y redistribuir las rutas entre el cliente y BGP dentro del Backbone del Proveedor.

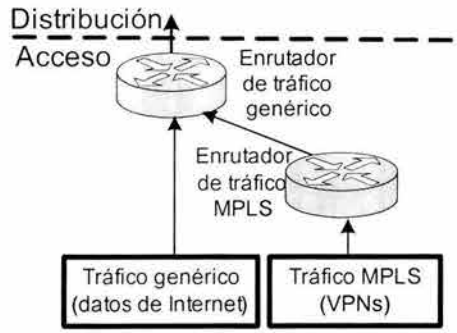


Figura 6.2.19

DSL

El tráfico de usuarios DSL se concentrará por medio de un enrutador destinado para éste fin, y será el encargado de ingresarlo en el enrutador de Acceso inmediato superior a él. Este tipo de tráfico podrá ser el resultado de una reventa de servicios a una compañía intermediaria, con la ventaja que al usuario DSL podrá ocultársele el Backbone del ISP mediante la implementación de MPLS.

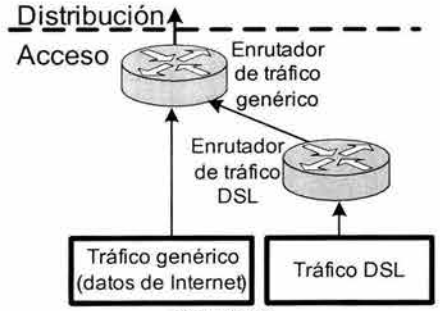


Figura 6.2.20

Dial Up

El tráfico de usuarios Dial Up se concentrará por medio de un Servidor de Acceso (Remote Access Server –RAS-) destinado para éste fin, y será el encargado de ingresarlo en el enrutador de Acceso inmediato superior a él. En este caso, también el tráfico Dial Up podrá ser el resultado de revender el servicio de uso de infraestructura

de red a una compañía intermediaria, con la ventaja que al usuario DialUp podrá ocultársele el Backbone del ISP mediante la implementación de MPLS.

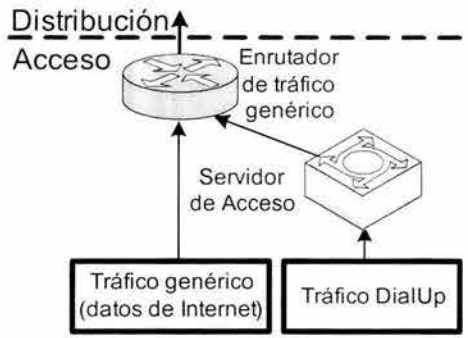


Figura 6.2.21

La forma de interconexión de los enrutadores específicos de cada servicio, con un enrutador en la misma Capa de Acceso actuando como distribuidor es con el fin de facilitar la escalabilidad y actualización de los servicios y tráfico de la red, pudiendo asegurar el tráfico de datos y una fácil configuración, administración, detección y corrección de fallas en cada uno de los equipos especializados.

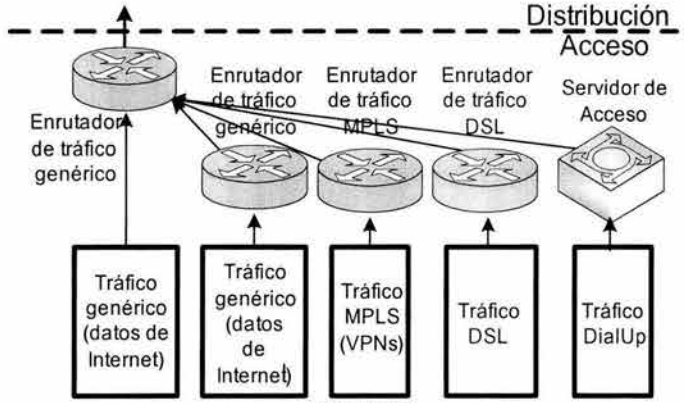


Figura 6.2.22

Optimización futura de la red (capacidad-costo)

La implementación física de la red se realizará con la filosofía de cubrir los requisitos técnicos y de servicio solicitados de la manera más sencilla, económica, administrable y fácil de implementar.

Deberá considerarse paralelamente el posible crecimiento de la red y opciones para optimizar su funcionamiento en función de la rentabilidad que presente en el futuro, además de prever y proponer nuevos servicios, aplicaciones y trafico que pudiera cursar por la red.

Ubicar el cuello de botella

Ubicar el punto en el que el Ancho de Banda se reduce (conocido como cuello de botella), tanto en el Backbone, como en los demás elementos de la red es muy importante para el funcionamiento de la red. En algún punto, la infraestructura deberá converger en una interfase compartida por más de dos flujos, punto que podrá ocasionar complicaciones si el nivel de tráfico aumenta más de lo previsto.

La solución al problema anterior es aumentar el Ancho de Banda del enlace, sin embargo, debido a la eventual imposibilidad de invertir más en Ancho de Banda, o poder escalar todos los enlaces, surge como punto básico y requerimiento mínimo, tener la conciencia de la ubicación de los posibles fallos en Ancho de Banda, para poder solucionar la situación a la primera señal.

Siguiendo las consideraciones anteriores, podemos asegurar que el diseño físico de la red será satisfactorio, y cumplirá con los criterios básicos exigidos a una red, tales como escalabilidad, fiabilidad y tolerancia a fallos; además de ofrecer una base sólida para el crecimiento propio de cualquier red, y facilidad de adecuarla a las necesidades que se presenten.

VI.3 PASO 3 de 3 TOPOLOGÍA LÓGICA (ENRUTAMIENTO)

VI.3.1 TOPOLOGÍA DE RED

La topología física de una red es descrita por el conjunto completo de enrutadores y redes que se conectan a ellos. Así también existe la topología lógica, que en principio se tiene que adecuar lo mejor posible a la topología física. Sin embargo los que dictan la pauta para generar la topología lógica serán principalmente los protocolos de enrutamiento.

Para generar la topología lógica, se necesita que esta también se ajuste al modelo

jerárquico, sin embargo lógicamente podemos conceptualizar dos tipos de áreas cada una con su nivel de importancia:

- Backbone (Área 0)
- Área de Distribución - Acceso (DA)

Área 0 o Backbone

Es el área mas importante de nuestro diseño, en esta área únicamente se realiza conmutación, esta depende del protocolo de enrutamiento IGP como OSPF o IS-IS, que tiene como objetivo saber el siguiente salto de manera interna, mientras que BGP (internal BGP) tiene el objetivo principal de propagar las rutas de redes de clientes y EBGP (external BGP) tiene el objetivo principal de propagar las rutas de redes no pertenecientes al ISP. Como BGP es un protocolo robusto se hace cargo del enrutamiento externo aunque también tiene soporte dentro del ISP, se recomienda que se tengan tan solo uno o dos enrutadores las tablas globales de Internet en BGP, mientras que el resto puede funcionar con rutas por default. El IGP por lo regular, al tener muchas rutas puede tornarse inestable, por lo que BGP puede brindar este apoyo al IGP.

En esta área no se corre ningún tipo de aplicación, es puramente de conmutación y justamente en este momento es donde MPLS tiene gran impacto sobre el desempeño de la red, esto debido a que no se consumen recursos de los enrutadores (como es en el caso de protocolos de enrutamiento al consultar sus tablas de enrutamiento), por lo que la conmutación se vuelve sencilla y efectiva. Son áreas generalmente pequeñas en cuanto al número de enrutadores, y estos pueden estar dispuestos en diferentes lugares.

Distribución - Acceso

En esta área debemos tener perfectamente delimitado la pertenencia de un enrutador a esta capa, ya que físicamente colinda con dos capas (Acceso y Backbone), y lógicamente engloba Distribución y Acceso. Son enrutadores que tienen activos los mismos procesos de protocolos de enrutamiento que en el Backbone, sin embargo no es necesario que conozcan a los enrutadores de otras áreas, porque pueden existir rutas por default hacia el Backbone o bien rutas sumarizadas a otras áreas. Es aquí donde podemos observar un mejor desempeño cuando se tienen áreas pequeñas, ya que se puede reducir la tabla de enrutamiento por un lado y por otro los LSP creados

en MPLS, ya que su creación es directamente proporcional al numero de rutas en la tabla.

También en esta área tenemos los enrutadores que colindan con los clientes, es en esta parte donde se tiene una gran cantidad de enrutadores, y anchos de banda "pequeños" (solo en la capa de acceso). En esta capa hay que tener un especial cuidado que al incluir a un cliente nos afecte lo menos posible en el desempeño y escalabilidad, y por otro lado buscar que los clientes no tengan inferencia en los protocolos de enrutamiento que maneja el ISP, por lo que generalmente se tienen rutas estáticas o rutas por default, probablemente pueden entablar una sesión de EBGP si se quieren tener enlaces redundantes o balanceo de carga (no simétrica), y es recomendable que no entable un protocolo IGP con el ISP.

Por otro lado podemos decir que MPLS, sigue respetando el modelo jerárquico, ya que depende directamente de un protocolo de enrutamiento (OSPF, IS-IS o BGP) que también lo es.

A continuación presentamos una figura 6.3.1 que genera una idea más concreta de lo señalado anteriormente. Partiremos de la topología física mencionada en el capítulo anterior:

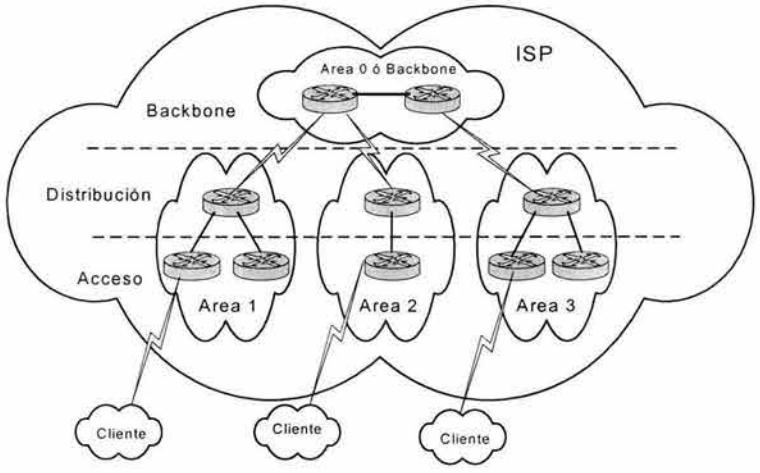


Figura 6.3.1

Como se observa en la figura, un área DA esta destinada a cubrir un nodo de distribución incluyendo también los enrutadores de acceso que tenga conectados.

VI.3.2 REQUERIMIENTOS PARA EL DISEÑO LÓGICO.

Direccionamiento

Un enrutador puede tener múltiples interfases, teniendo una dirección IP por cada una de ellas, las interfases son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz. El optimizar al máximo el direccionamiento para no desperdiciar las direcciones IP disponibles haciendo más sencilla la administración.

Para poder diseñar correctamente, el direccionamiento debe ser ordenado, como se muestra en la Figura 6.3.3, evitando redes separadas lógicamente. Es indispensable que cada área sea una red separada, asignándole un rango de direcciones. Existen métodos que facilitan la división de las redes como VLSM en el caso de los IGP y CIDR en el caso de BGP.

Sumarización de rutas

Los procedimientos de sumarización de rutas condensa información de enrutamiento. Sin sumarización cada enrutador en una red necesitaría retener una ruta específica para cada subred. Con la sumarización, los enrutadores pueden reducir conjuntos de rutas a un simple anuncio (Figura 6.3.3), reduciendo la carga del enrutador y la complejidad percibida en la red. La importancia de la sumarización de rutas se incrementa con el tamaño de la red.

La reducción en la propagación de información de enrutamiento puede ser muy significativa. La figura 6.3.2 ilustra los ahorros potenciales. El eje vertical de la figura muestra el número de entradas en la tabla de enrutamiento. El eje horizontal mide el número de subredes.

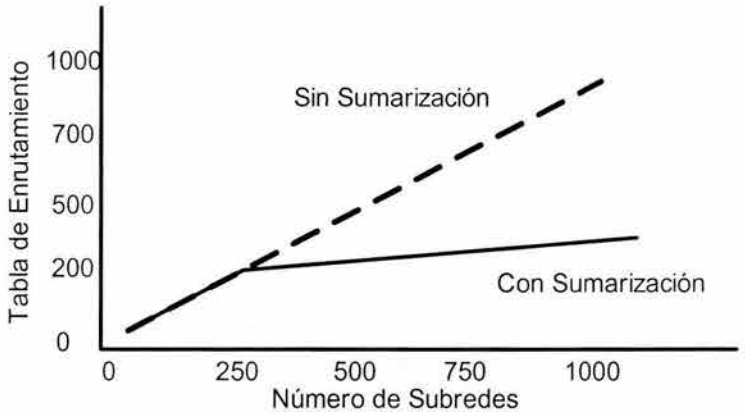


Figura 6.3.2

A continuación se muestran en la figura 6.2.3 las ventajas de la sumarización en cuanto a las redes que se anuncian en la tabla de enrutamiento esto es aplicable tanto al IGP como a BGP.

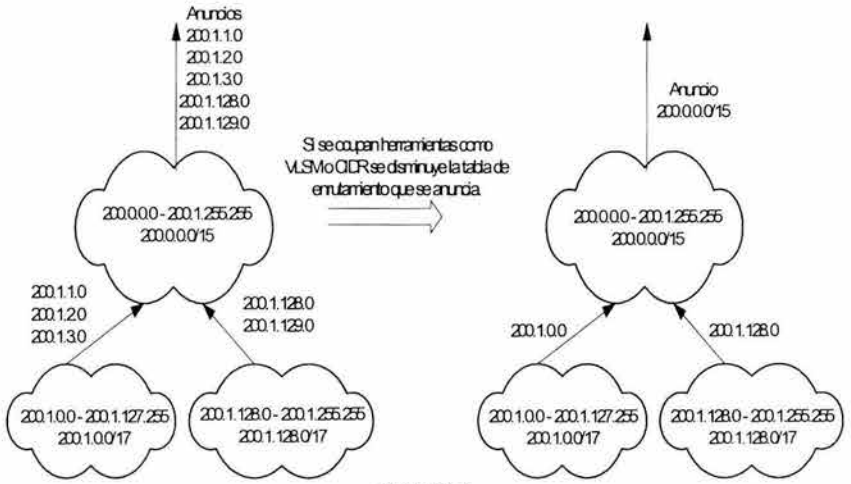


Figura 6.3.3

Un protocolo de enrutamiento puede sumarizar con un límite de hasta un bit solo si soporta VLSM (Variable Length Subnet Mask). Algunos protocolos de

enrutamiento sumarizan automáticamente mientras que otros requieren una configuración manual para soportar sumarización de rutas.

Selección de rutas

La selección de rutas es trivial cuando existe sólo una ruta para llegar al destino. Si alguna parte de esta ruta llegara a fallar, no hay forma de recuperarla. Por consiguiente, la mayoría de las redes son diseñadas con rutas múltiples para que existan alternativas en caso de que una falla ocurra.

Los protocolos de enrutamiento comparan ciertos aspectos como la métrica (numero de saltos, Ancho de Banda de los enlaces, costo, etc), distancia administrativa del protocolo de enrutamiento y atributos (únicamente BGP), para seleccionar la mejor de un grupo de posibles rutas.

La mayoría de los protocolos de enrutamiento pueden usar múltiples rutas si éstas tienen un costo igual. Otros protocolos de enrutamiento pueden aún usar múltiples rutas cuando tienen un costo diferente. En cualquier caso, el balanceo de carga puede mejorar las condiciones en el Ancho de Banda de la red.

Convergencia

Cuando la topología de la red cambia, el tráfico de la red debe re-enrutarse rápidamente. El término "Tiempo de Convergencia" describe el tiempo que le toma al enrutador empezar a usar una nueva ruta después del cambio en la topología. Los enrutadores deben seguir cuatro pasos después de que la topología cambia:

- Detectar el cambio.
- Seleccionar una nueva ruta.
- Propagar la información de la ruta cambiada.
- Generación o actualización de un LSP de MPLS.

Algunos cambios son detectables inmediatamente, por ejemplo fallas en la línea que involucran la pérdida de la portadora. Otras fallas son difíciles de detectar, por ejemplo si una línea se convierte en inutilizable pero la portadora no esta perdida, el enlace inservible no es detectable inmediatamente, lo cual retarda el tiempo de convergencia de la red y por lo tanto su disponibilidad. En general la detección de fallas depende del medio involucrado y el protocolo de enrutamiento utilizado. En este caso OSPF tiene un tiempo de convergencia aproximado de 5 [s].

Una vez que la falla ha sido detectada el protocolo de enrutamiento debe seleccionar una nueva ruta. El mecanismo usado para realizar esto es dependiente del protocolo. Todos los protocolos de enrutamiento deben propagar la ruta cambiada.

Escalabilidad.

La escalabilidad la podemos ver como la capacidad de la red para extender tanto el número de clientes como de enrutadores en cualquiera de las capas, sin impactar a la red, esto depende directamente del protocolo de enrutamiento usado, y la calidad del diseño de la red, también aplicable a MPLS ya que los LSP's crecerán a la par del protocolo de enrutamiento pero sin impactar severamente a la red.

La escalabilidad de una red es limitada por dos factores principalmente:

Problemas operacionales

Sugieren el uso de áreas grandes o protocolos que no requieran las estructuras jerárquicas. Cuando son requeridos protocolos jerárquicos que sugieren el uso de áreas pequeñas. Buscar el balance correcto es el objetivo principal en el diseño de redes. Típicamente son más significativos que los problemas técnicos.

Problemas técnicos

Repercuten en que los protocolos como IS-IS y OSPF tengan un buen balance, es decir, que el consumo de recursos en los enrutadores crezca menos en comparación con el crecimiento de la red. Tres recursos críticos son usados por los protocolos de enrutamiento:

- Memoria
- Unidad Central de Procesos
- Ancho de Banda

Seguridad.

En redes WAN, se tiene que hablar de evitar que los enrutadores sean accesados por personas ajenas al ISP, es decir, controlar el acceso a los recursos de la red es de primera importancia. Inicialmente de forma obligatoria hay que introducir passwords a los enrutadores para que no se pueda entrar de forma remota, también se pueden crear listas de acceso por determinadas IP's. Algunos protocolos de enrutamiento proveen técnicas que pueden ser usadas como parte de una estrategia de seguridad y

se pueden insertar filtros en los enrutadores para filtrar las rutas que son anunciadas y así mantener segura la información de la red.

Hay que prevenir que equipos no autorizados participen en el protocolo de enrutamiento, por lo que se recomienda usar autenticación para establecer vecindades y evitar que los enrutadores de los clientes y los del operador entablen algún protocolo de enrutamiento con el ISP.

Por otro lado en la arquitectura de MPLS la parte que más debe estar protegida es la de VPN-MPLS debido a que esto repercute directamente en el usuario. Por lo tanto existen dos formas básicas para proteger la red, primero, como ya se había mencionado, evitar accesos remotos no autorizados, y segundo, hacer a la red lo mas inaccesible posible.

Otro tema que hay que tomar en cuenta, es que en una red IP pura es fácil hacer Spoofing; MPLS finalmente trabaja con direcciones IP. La forma de atacar es que traten de entrar insertando paquetes con una etiqueta que no le pertenece a la red.

VI.3.3 ELECCIÓN DEL PROTOCOLO DE ENRUTAMIENTO INTERNO (IGP)

Uno de las decisiones más importantes que se deben tomar en el diseño de la red IP WAN es seleccionar el mejor protocolo de enrutamiento. Aun cuando todos ellos tienen la misma meta en general, que es compartir la información de enrutamiento de la red entre todos los enrutadores, cada protocolo de enrutamiento posee diferentes características como escalabilidad y desempeño. Por consiguiente, un protocolo de enrutamiento en específico no es la solución universal. Sin embargo, como diseñador de la red, se debe ser capaz de hacer la elección correcta. Los protocolos de enrutamiento dinámico interno usados ampliamente hoy en día son RIP, IGRP, EIGRP, IS-IS y OSPF. Cada protocolo tiene sus ventajas y desventajas. Así, el usarlos o no depende de los requerimientos específicos de enrutamiento y el escenario particular; por ejemplo, si se desea que servidores UNIX participen en el dominio de enrutamiento, entonces RIP es la única opción dado que los servidores UNIX manejan únicamente RIP pese a sus limitaciones. Si se tienen enrutadores de diferentes vendedores en el mismo dominio de enrutamiento, entonces EIGRP no funcionara dado que es propietario de Cisco. Por otro lado OSPF y IS-IS anuncian las

rutas IP con máscaras de subred, es decir, pueden manejar VSLM, por lo que pueden manejar redes discontinuas, y ambos pueden ser usados como protocolo de enrutamiento interno. Finalmente cabe destacar que OSPF tiene, como ya se había mencionado, LSA´s que están dirigidos al uso de MPLS.

Para elegir un protocolo que enrutamiento sugerimos se cuente con los siguientes aspectos:

- Algún límite dispuesto en la métrica.
- Soportar VSLM.
- Rapidez de convergencia del protocolo de enrutamiento cuando ocurre una actualización o cambio.
- Que tan a menudo son transmitidas las actualizaciones de enrutamiento o los anuncios link-state.
- Ancho de Banda que es usado para transmitir actualizaciones de enrutamiento.
- Cuán ampliamente son distribuidas las actualizaciones de enrutamiento.
- Cuánta utilización de CPU es requerida para procesar las actualizaciones de rutas o mensajes link-state.

Considerando los puntos anteriores, se deber ser capaz de determinar el mejor protocolo de enrutamiento disponible bajo ciertas circunstancias. El protocolo IS-IS es un protocolo muy completo, robusto y tiene muy buen desempeño, sin embargo el mercado de redes está optando por protocolos más sencillos y con mayor acceso a la información, como lo es OSPF. Por otro lado, seleccionar el protocolo de enrutamiento es simplemente una preferencia personal de los diseñadores de red y los que cuentan con mas experiencia diseñan y configuran OSPF, debido a su flexibilidad y a que está normalizado. Por estas razones podemos elegir un protocolo de enrutamiento ***de estado de enlace*** como lo es ***OSPF***.

XI.3.4 DISEÑO DE LA RED CON OSPF

Para poder diseñar la red, hay que tomar en cuenta las características del protocolo de enrutamiento elegido, en nuestro caso es OSPF.
En el diseño de redes con OSPF dos situaciones son críticas:

1. Definir correctamente las Áreas y su tamaño.
2. Realizar correctamente el Direccionamiento.

Los puntos a tomar en cuenta en el diseño con OSPF son:

- Topología de la red.
- Direccionamiento y Sumarización.
- Selección de Rutas.
- Convergencia.
- Escalabilidad de la Red.
- Seguridad.

OSPF trabaja mejor en un ambiente de topología Jerárquica, lo cual coincide perfectamente con nuestro diseño físico. La primera decisión, y más importante cuando se esta diseñando la red OSPF es determinar qué enrutadores y enlaces están incluidos en el Backbone, cuáles estarán incluidos en algún Área DA, y finalmente cuáles interactúan con dos áreas (Distribución-Acceso y Backbone).

Generalmente se recomienda que las áreas no tengan más de 50 enrutadores por área, ya que disminuye la capacidad del CPU como ya se había mencionado. Así como también las siguientes consideraciones:

1. *El número de vecinos de cada enrutador:* Los enrutadores con mayor número de vecinos tiene más trabajo. Se recomienda que cada enrutador no tenga más de 60 vecinos.
2. *El numero de áreas soportadas por los enrutadores:* Generalmente se ocupa que un enrutador tenga en común dos áreas (ejemplo Backbone y Distribución - Acceso), se recomienda que sus puertos no estén en mas de tres Áreas, esto también se refleja en que los enrutadores de distribución no estén directamente conectados y siempre el trafico pase por el Backbone.
3. *Selección del DR (Designated Router):* Se sabe que el *DR* y el *DR backup* en un nodo dentro de un Área, son lo que más trabajo tienen por lo que es recomendable que estos enrutadores no tengan otros procesos de CPU intensos, también se recomienda que un DR no sea el DR de varias Áreas.

Consideraciones en el Backbone

La Estabilidad y Redundancia son los dos principales criterios en el Backbone. La Estabilidad se incrementa manteniendo el tamaño del Backbone pequeño, esto se debe

a que cada enrutador requiere procesar sus rutas por cada cambio en el estado de los enlace, si son pocos enrutadores (no mas de 50), se reduce la carga al CPU. En el caso de la Redundancia es importante que si uno de los enrutadores o enlaces falla se tengan rutas de respaldo.

Consideraciones de las Áreas

Las áreas de forma individual deben ser contiguas, esto quiere decir que debe existir un camino que pueda ser trazado de cualquier enrutador en un Área a cualquier otro en la misma Área. Esto no quiere decir que todos los enrutadores compartan el mismo medio de red. Los dos aspectos más importantes del diseño dentro de un Área son:

1. Determinar cómo se otorga el direccionamiento del Área.
2. Determinar cómo el área será conectada al Backbone.

Las Áreas deben tener el mismo espacio de direccionamiento, de lo contrario no será posible implementar la sumarización. No es recomendable tener varios enrutadores conectados a Áreas distintas. En nuestro caso todas las Áreas DA estarán conectadas directamente al Área 0. A continuación se presentan algunas reglas que ayudan a asegurar que la red será flexible y proveerá de los recursos necesarios a los usuarios.

- Considerar la proximidad física de los nodos cuando se definen las Áreas.
- Reducir el tamaño de las Áreas si los enlaces son inestables.

La sumarización en OSPF se realiza tomando los siguientes puntos en cuenta:

- Separar las redes de cada Área
- Manejar VLSM.

Convergencia de OSPF

Una de las ventajas que ofrece OSPF es la de su rapidez en el tiempo de convergencia a cambios en la topología de la red, existen dos componentes en la convergencia:

- Detección en cambios de la topología: se ocupan dos métodos para detectar los cambios en la topología, uno es detectar cambios en el Status de la Interfase, y el segundo es no recibir paquetes de *Hello* de su vecino, suponiendo a su vecino desconectado después de cierto tiempo de no recibir

este paquete. Éste tiempo puede ser configurado.

- Recálculo de rutas: Una vez que detecto la falla, envía información con el nuevo estado, los demás enrutadores reciben este paquete y recalculan su ruta aplicando el algoritmo correspondiente.

Escalabilidad de OSPF

La red OSPF puede ser escalable dependiendo de su estructura y del esquema de direccionamiento. Es por ello que se comentó anteriormente la importancia del direccionamiento y la sumarización, con ello podemos optar por un ambiente de direccionamiento jerarquizado y una asignación de direccionamiento estructurada, que serán lo factores que determinaran la escalabilidad de nuestra red, por lo que hay que tomar en cuenta las siguiente consideraciones.

- Operativamente, las redes OSPF deben ser diseñadas de forma que las Áreas no necesiten ser modificadas para poder crecer. El rango de direcciones debe ser reservado para permitir la adición nuevos enlaces o Áreas.
- Técnicamente, la escalabilidad de OSPF está determinada por la utilización de tres recursos principalmente: CPU, memoria y Ancho de Banda.

Seguridad de OSPF

Hay dos tipos de seguridad que son aplicables a los protocolos de enrutamiento:

- Control de Enrutadores que participan al la red OSPF: OSPF contiene un campo opcional para la autenticación para que ningún otro equipo pueda intervenir en el proceso de OSPF.
- Controlando la información de enrutamiento que intercambian: Todos los enrutadores deben tener la misma información del Área OSPF, como resultado de ésto no es posible ocupar filtros en la red OSPF.

La elección de un protocolo de enrutamiento es básicamente considerar qué servicios se piensan prestar en la red y el valorar la potencialidad del protocolo para que la red sea fácilmente escalable. Pero el que finalmente tendrá la decisión es el diseñador para elegir con qué protocolo de enrutamiento se sienta más familiarizado, siempre y cuando cumpla con los puntos antes mencionados.

VI.3.5 DISEÑO DE LA RED CON BGP

En la actualidad únicamente existe un solo protocolo de enrutamiento EGP, que es BGPv.4 (Border Gateway Protocol v.4). En este tema se evaluarán los criterios que hay que tomar en cuenta para poder implementar el protocolo BGP, cabe destacar que es uno de los temas de mayor trascendencia ya que este protocolo será el que interactué con otros SA´s, ya que una mala configuración en este protocolo puede causar inconsistencias de enrutamiento en redes ajenas.

Como ya se había mencionado existen dos modos de operación de BGP, dependiendo con que enrutadores interactúe, estos dos modos son EBGP e IBGP (Figura 6.3.4). Básicamente las principales diferencias son: Si hay una sesión de dos enrutadores que se encuentran en el mismo SA, se le denomina IBGP, pero si la conexión es con enrutadores de distintos SA´s de le denomina EBGP.

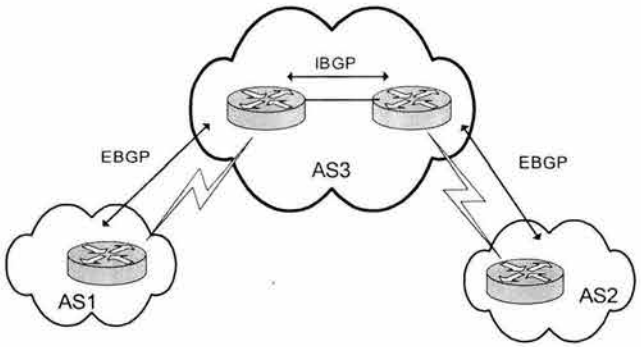


Figura 6.3.4

Sincronización en un SA

Ésta es una parte muy importante en el diseño y configuración de la red del ISP por la siguiente razón:. Las sesiones de BGP requieren estar sincronizadas con el protocolo IGP antes de que BGP anuncie rutas es otro SA. La importancia radica en que las rutas que se aprendieron por BGP estén totalmente redistribuidas en el IGP, si no es así, otros SA´s enviaran el tráfico a nuestro SA y este no sabrá como llegar al siguiente salto. Esto tiene gran importancia, ya que las tablas de enrutamiento dentro del IGP crecerán considerablemente lo cual provocará que los enrutadores incrementen el procesamiento del CPU. El ocupar la sincronización provoca que

existan inconsistencias en el enrutamiento de la red, siendo siempre recomendable no utilizar la sincronización y buscar métodos alternativos para que siempre existan rutas activas.

Así como en OSPF, también en BGP el direccionamiento es muy importante, ya que tenemos que tomar en cuenta criterios como el de sumarización, así como los diferentes escenarios de direccionamiento que se pueden presentar a un ISP. Como ya habíamos mencionado, para anunciar rutas en BGP, hay que tener mucho cuidado con su configuración, ya que alguna inconsistencia que se genere afectará a todas sus vecindades externas.

Escenarios de direccionamiento con proveedores externos o clientes

- *Esquema de single-home, donde el ISP asigna el direccionamiento:* Es el escenario mas común y el mas sencillo, ya que el ISP anunciara las redes del cliente y únicamente se configurara una ruta estática (Figura 6.3.5) del cliente al ISP.

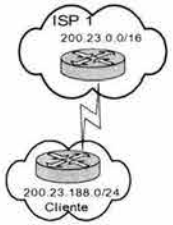


Figura 6.3.5

- *Esquema donde se tiene single-home pero el cliente tiene su propio espacio de direcciones:* En este caso el cliente esta conectado a un solo Carrier y el cliente su propio espacio de direcciones totalmente diferente al del proveedor del servicio. En este momento el proveedor debe enviar el anuncio específico por medio de BGP (figura 6.3.6).

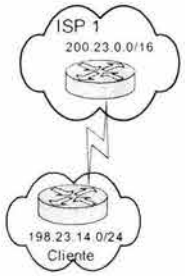


Figura 6.3.6

- Donde un cliente tiene servicio con dos ISP y ocupa el direccionamiento de uno de los ISP: Este escenario prevé que un cliente esta conectado a múltiples ISP y él debe tomar direcciones de alguno de los ISP, esta agregación de rutas debe hacerse con mucho cuidado debido a que puede ocasionar problemas de enrutamiento entre Carriers. En la figura 6.3.7 se muestra que el ISP 2 tiene que anunciar la red del cliente pero esa red también pertenece al ISP 1, por lo que hay que tener mucho cuidado con sumarizar las rutas.

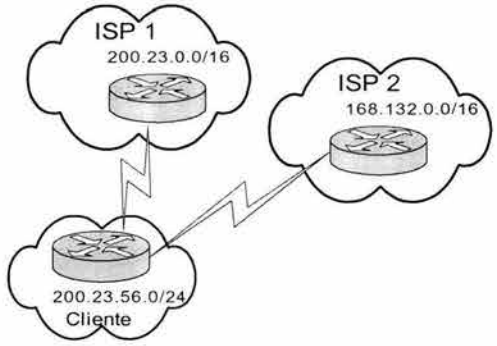


Figura 6.3.7

Topología de Route Reflector

En algunas redes de los ISP, el IBGP puede tener sesiones de tipo full-*mesh o partial-mesh*, una red de gran escala se considera como tal cuando se tienen más de 100 sesiones de IBGP. Es en este momento, debido a la complicación de la administración, que se sugiere el uso del Route Reflector (RR). Como ya sabemos el RR es como un servidor de rutas del IBGP que actualiza a todos los demás

enrutadores, esto minimiza la cantidad de sesiones IBGP entre los enrutadores, sin embargo esto introduce un procesamiento extra en el enrutador RR, y si este no es configurado correctamente puede introducir *loops* de enrutamiento e inestabilidad. Es importante destacar que los RR nos son recomendados para cualquier topología.

Se tienen básicamente dos convenciones en el RR: enrutadores que son clientes y enrutadores que no son clientes como se muestra en la figura 6.3.8 Los enrutadores clientes y el RR forman un cluster.

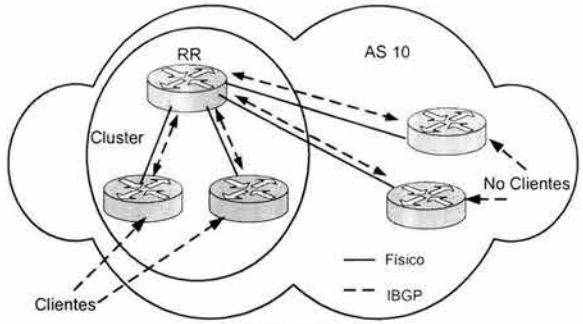


Figura 6.3.8

El RR recibe múltiples rutas para un mismo destino y tiene que implementar un proceso de decisión, sobre las cuales elegirá la mejor ruta y a su vez la anunciara.

1. Si la ruta es recibida por un no-cliente, solo lo anuncia la red a sus clientes.
2. Si la ruta es recibida por un cliente la anuncia a todos clientes y no clientes.
3. Si la ruta es recibida por un EBGP, la anuncia los clientes y los no-clientes

De las mejores prácticas es tener RR de backup, lo cual proveerá de redundancia lógica al diseño de la red.

Por lo tanto la topología que se recomienda para las redes de gran escala como las de los ISPs sea la mostrada en la figura 6.3.9:

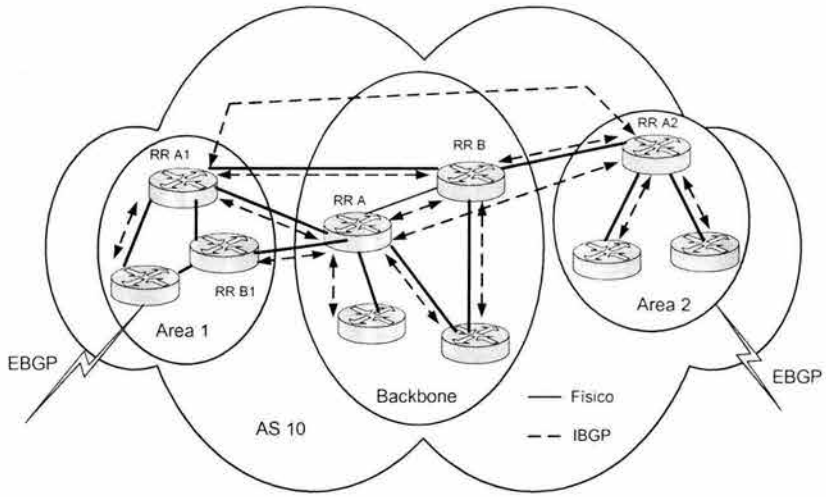


Figura 6.3.9

Como se puede observar (Figura 6.3.9) se tienen las áreas de OSPF, Área de Backbone, y Área 1 y 2 de Distribución - Acceso. En el Área de Backbone encontramos a los "RR A" y al "RR B", los cuales son redundantes para el Backbone y por lo tanto para toda la red, ya que tienen enlaces a los RR A1 y RR A2, también se ve que en el caso del RR A1 se tiene tanto redundancia lógica como redundancia física con los RR A y RR B, mientras que el RR A2 tiene únicamente redundancia lógica. Dependiendo del grado de importancia de nuestro nodo de distribución se pueden tener dos enrutadores para redundancia RR A1 y RR B1, esto puede proveer tanto redundancia física como lógica, así como de equipos, lo cual puede ser de bastante utilidad para la red.

Topología de Confederaciones

Es otra forma de poder evitar la topología IBGP *full-mesh o partial-mesh*. Las confederaciones son recomendadas únicamente en el caso donde el IBGP involucra muchas sesiones de IBGP. Las confederaciones de IBGP están basadas en el concepto de que un SA puede ser dividido de Sub-SA´s (Figura 6.3.10), es decir, un SA se divide en Sub-SA´s con diferente número de SA, esto provoca que existan sesiones de EBGP internamente en el SA del ISP. En la siguiente se Figura 6.3.10 se muestra esta topología.

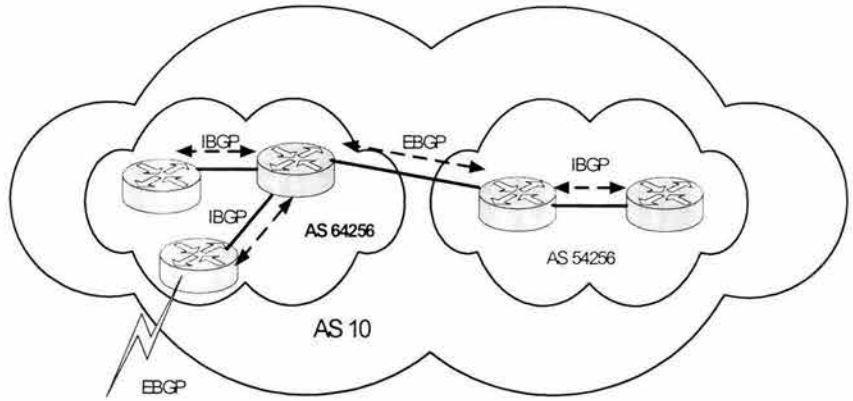


Figura 6.3.10

Los diseñadores con más experiencia prefieren trabajar con la topología del Route Reflector, ya que es más estable, flexible para escalar y su administración es más sencilla. Por otro lado las confederaciones pueden ser usadas ocupando el protocolo OSPF en cada uno de los Sub-SA´s de forma independiente, lo cual nos ayuda a reducir las áreas de OSPF, sin embargo con confederaciones sería más complicado delimitar nuestras tres regiones del modelo jerárquico (Backbone, Distribución y Acceso). Finalmente en algunas implementaciones pueden ser combinadas ambas topologías.

VI.3.6 FORMAS DE CONEXIÓN DEL CLIENTE AL ISP

Para poder implementar el esquema de enrutamiento del cliente es necesario verificar el esquema de conexión física y asignación del direccionamiento del cliente al ISP o a sus ISP´s. Para poder implementar el enrutamiento se presentan tres propuestas básicamente:

Ruta Estática

Este esquema es el más sencillo de implementar y de funcionamiento más simple, dado que no tiene implicaciones de enrutamiento para el ISP, éste únicamente anuncia

las rutas del cliente a Internet (Figura 6.3.11). Para poder implementar este esquema hay que tener en cuenta los siguientes puntos:

- El cliente únicamente debe tener un proveedor, por lo tanto no permite la redundancia con distintos ISP´s.
- Es eficiente, si se tienen dos enlaces y se hace balanceo de carga simétrico, con el mismo proveedor.

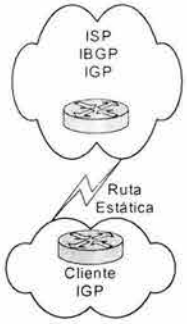


Figura 6.3.11

Entre las ventajas que encontramos es que la administración y configuración de la red se vuelve sencilla en la Capa de Acceso, por otro lado si el cliente presenta una falla en su red no tiene repercusiones dentro del ISP ni en Internet, únicamente la red se vuelve inalcanzable.

Establecimiento de una Sesión de BGP

Este esquema se da cuando el cliente requiere implementar enrutamiento en Internet, o bien la red del cliente es un Sistema Autónomo (Figura 6.3.12). Este esquema es un poco complejo de implementar, ya que el cliente debe tener la suficiente infraestructura en equipos para poder soportar las tablas de BGP; si se va a implementar este esquema comúnmente es por las siguientes necesidades:

- Que el cliente requiera de la tabla de BGP, para su red.
- El cliente tenga dos o más proveedores de Internet, con el fin de plantear un esquema de redundancia.

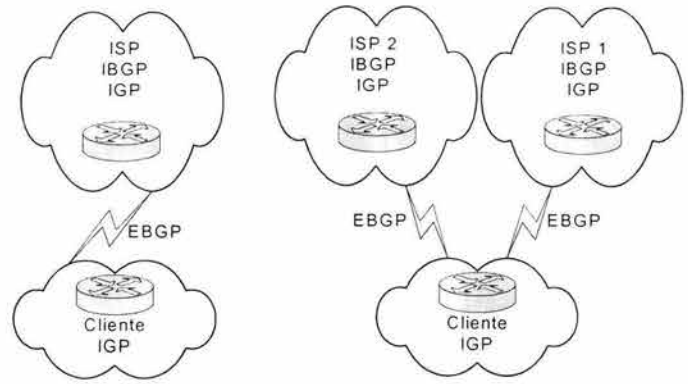


Figura 6.3.12

Este esquema tiene una desventaja, ya que si el cliente tiene una falla en su red, ésta repercute en toda la tabla de BGP en Internet, y puede crear conflictos de enrutamiento si el cliente realiza una mala configuración de las redes que anuncia a Internet, siendo que los tiempos de convergencia en Internet son mayores.

Establecimiento de un protocolo de enrutamiento Interno entre el ISP y el cliente.

Este esquema no es recomendable ya que el cliente participa en el protocolo de enrutamiento del ISP (Figura 6.3.13), y si el cliente hace una mala configuración en el protocolo de enrutamiento interno, se pueden generar problemas internos y repercutir en el ISP hasta en la suspensión del servicio.

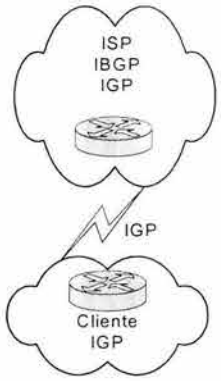


Figura 6.3.13

Nivel de los ISP

Como ya sabemos hay distintos niveles de proveedores de Internet, por lo que en México únicamente tenemos proveedores de nivel "dos". Si se quiere tener conectividad con cualquier parte del mundo es necesario conectarse a ISP de nivel "uno" (Figura 6.3.14), y estos en nuestro caso los mas cercanos se encuentran en E.E.U.U., entre los mas importantes encontramos a ATT, MCI, Teleglobo, entre otros. Y estos son los que nos darán el servicio de Internet o bien la conectividad con todo el mundo. Es por ello que debemos tener enlaces Internacionales y ubicarlos de la mejor forma en nuestro Backbone. Por otro lado tenemos proveedores de Nivel "tres", estos son ISP´s con menor infraestructura y que requiere de un proveedor de Internet de nivel "dos".

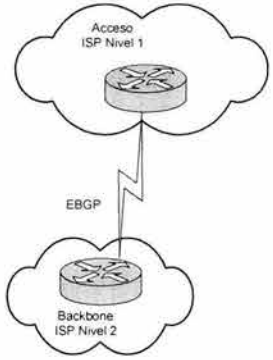


Figura 6.3.14

Es recomendable no tener sólo un proveedor de Internet nivel "uno", es mejor tener dos enlaces con distintos ISP´s, para efectos de un mejor servicio y eliminar puntos de falla.

VI.3.7 IMPLEMENTACIÓN DE MPLS EN EL DISEÑO.

En el caso de la conmutación, MPLS ofrece grandes ventajas; como ya sabemos MPLS creará un LSP a través de los enrutadores internos del ISP, por lo que sólo los enrutadores de frontera requieren saber las rutas de BGP. Esto tiene ventajas de simplificación en la configuración y facilidad en la administración como se muestra en la siguiente Figura 6.3.15:

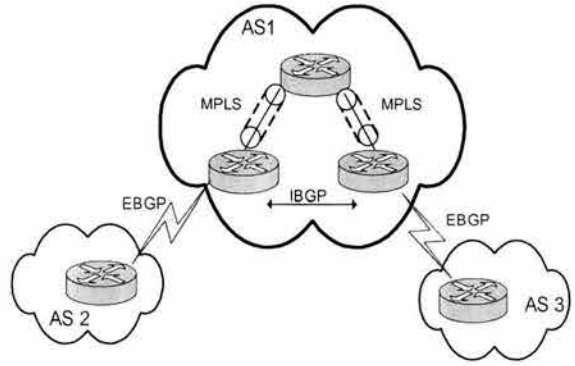


Figura 6.3.15

Por otro lado uno de los grandes beneficios de MPLS, es que el consumo de los recursos del enrutador se reduce considerablemente con respecto al del enrutamiento normal, ya que el análisis del paquete se vuelve más sencillo, y la consulta a la tabla de etiquetas es más rápida que la consulta a la tabla de enrutamiento, **repercutiendo principalmente en la disminución de la utilización del CPU del enrutador.**

Cuando se implementa MPLS en la red, se tienen que tener varias consideraciones en cuanto al trafico que se va a cursar, se debe delimitar dónde se va a implementar MPLS, ya que hay que tomar en cuenta cómo repercute la sumarización para la asignación de etiquetas.

Clasificación del Tráfico

Básicamente para definir el proceso de etiquetado hay que considerar dos casos básicos, si la aplicación es VPN se tiene que implementar MPLS desde la Capa de Acceso para poder cumplir con la función de la VPN, por lo que las rutas deben ser totalmente explícitas desde los enrutadores de Acceso, como se ve en la Figura 6.3.16, sin embargo si se va a cursar tráfico hacia Internet, por consideraciones de diseño de MPLS proponemos este implementado a partir de la Capa de Distribución para encontrar el punto de equilibrio entre la utilidad de la sumarización y las ventajas de IP-MPLS.

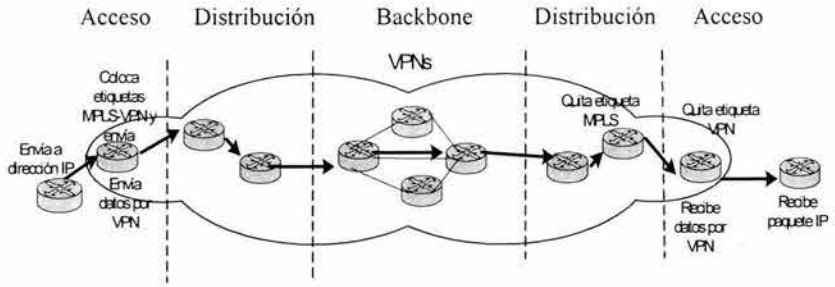


Figura 6.3.16

Políticas de Diseño Lógico para MPLS

Otro caso particular es cuando la trayectoria es relativamente corta. Esto se presenta generalmente cuando dos nodos de distribución están conectados al mismo enrutador de Backbone como se muestra en la figura 6.3.17:

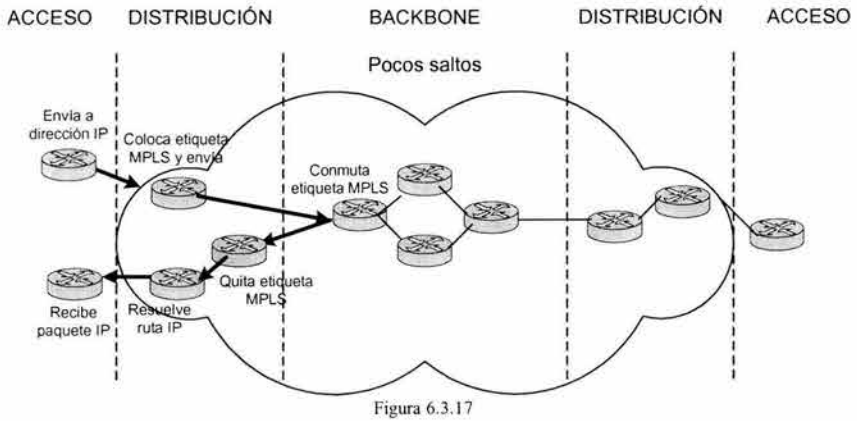


Figura 6.3.17

Este podría considerarse como el peor caso, donde se desperdicia la utilidad de las funcionalidades de la red MPLS, sin embargo, dada la poca frecuencia en que se presenta esta situación (debido a que la mayoría del tráfico se dirige a Internet) y que el consumo de los recursos de los enrutadores no es crítico, este caso particular no impactará la red.

Si se plantea un esquema donde se implemente MPLS desde la capa de Acceso (a excepción del caso de las VPNs), no se podrían sumarizar rutas, ya que MPLS requeriría saber todas las rutas y asignar una etiqueta para cada ruta, lo cual provocaría que nuestra tabla de enrutamiento creciera de forma considerable.

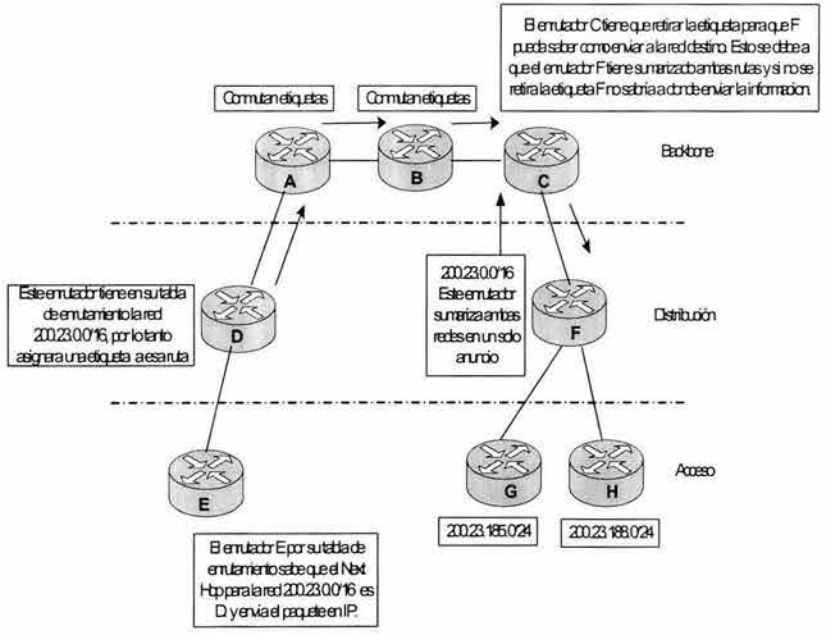


Figura 6.3.18

Como se muestra en la figura 6.3.18 cuando se tiene sumarización se tiene que retirar la etiqueta antes de que entre a la capa de Distribución debido a que no conoce la ruta IP exacta a la que correspondería a la etiqueta, por lo que es necesario que el enrutador de Backbone retire la etiqueta al enrutador de Distribución (penultimate hop-popping), para que éste pueda consultar su tabla de enrutamiento normalmente, y

enviar al Next Hop. Con la desventaja que el enrutador de Backbone tendrá que retirar la etiqueta desaprovechando infraestructura MPLS.

Sin embargo la mejor capa en el diseño para implementar MPLS es en la capa de distribución y Backbone, y donde se puede tener el mejor equilibrio, es decir que no se distribuya todas la rutas de forma explícita, como seria el caso si se insertara la etiqueta en la Capa de Acceso; tampoco es recomendable implementar únicamente MPLS en el Backbone, por que sub-utilizaríamos la capacidad MPLS de la infraestructura.

A través de este capítulo hemos destacado los tres rubros que conforman según nuestro criterio el diseño de una red: Estructura Funcional, Topología Física y Topología Lógica, las cuales proporcionan todos los enfoques necesarios para obtener una red exitosa. El desarrollo del capítulo nos da una visión integral del diseño, proporcionando todas las posibilidades y las herramientas a ser aplicadas en el diseño al conocer sus ventajas y desventajas, con el fin de ser utilizadas en un diseño específico con necesidades y metas propias.

VII PLAN DE IMPLEMENTACIÓN DE UNA RED PROPUESTA

La meta de diseñar una red MPLS antes de su instalación es producir una red que opere óptima y eficientemente. Debemos recordar que los clientes no son capaces de decir al Proveedor de Servicio exactamente qué y cuánto tráfico quieren enviar a un destino específico debido a la naturaleza no orientada a conexión inherente al tráfico IP. Por lo anterior no es posible diseñar perfectamente una red independiente del momento en que se proponga su solución.

En este capítulo presentamos una propuesta de red que satisface las consideraciones planteadas en el capítulo "Requisitos de la Red", buscando el óptimo funcionamiento de una red IP siguiendo los parámetros de diseño mencionados en "Estructura Funcional", "Topología Física" y "Topología Lógica".

Cabe destacar que la propuesta de red que se desarrolla a continuación se realiza únicamente con el carácter de posible aplicación de las directivas discutidas en los capítulos anteriores, haciendo énfasis en consideraciones prácticas y criterios que podrían ser considerados en la implementación de cualquier red independientemente de su tamaño, necesidades, usuarios, tipos de servicio, etc.

Recalcamos una vez más que la presente propuesta no es la opción única de resolución e implementación, y ésta podrá ser conveniente o no en función de las necesidades específicas a resolver por el diseñador y administrador de la red. Por el carácter básico de la propuesta de diseño se tocarán los criterios para diseño de mayor importancia explicados en los capítulos anteriores.

VII.1 PROPUESTA DE RED

Propondremos una red considerando como área de servicio el territorio nacional, ya que éste es un ambiente adecuado para desarrollar una red para un Proveedor de Servicio o compañía que ofrezca servicios similares.

Como primer paso de la red propuesta es conveniente y necesario delimitar la misma, para posteriormente sugerir soluciones y explicar los modelos utilizados además de las razones de elección de los mismos.

Las políticas que proponemos para la fase de diseño y posteriores de escalamiento son las siguientes:

- Se tiene como meta: "Generar una red IP Escalable, Fiable y Tolerante a Fallas", ya que con estos parámetros aseguramos soportará aplicaciones exigentes en el desempeño de la red, como tráfico multimedia transitando por MPLS.
- La red se implementará basándonos en un Modelo Funcional *Jerárquico*, donde la importancia de dicho nodo es la Capa de la topología a la que pertenece, en función de la cual se le asignarán funcionalidades, conexiones y configuraciones correspondientes a dicha Capa, es decir, el diseño no se efectuará pensando en un equipo en específico.
- Contar indispensablemente con soporte MPLS en los enrutadores de Backbone y Distribución, y eventualmente también en Acceso en función de los servicios ofrecidos, con el fin de asegurar el correcto funcionamiento de VPN's y otras aplicaciones basadas en conmutación de etiquetas cuando transiten por la red.

VII.1.1 PRESTACIÓN DE SERVICIOS

Usuarios

El mercado al que enfocarémos nuestros servicios se dirigirá a:

- Empresas corporativas con diferentes necesidades de servicios de transporte de datos, y con posibilidad de requerir aplicaciones altamente demandantes de Ancho de Banda de una red (Voz, Video, Datos y Aplicaciones de datos críticos)
- Usuarios con menor exigencia de Ancho de Banda.

Se podrán ofrecer diferentes planes de contratación en los cuales se incluyan distintos esquemas de servicios a ofrecer, así como diferente nivel en los parámetros descriptivos de la red. Dichos planes se diseñarán en base a los requerimientos de los clientes, agrupándolos de acuerdo a las características en común del tráfico, para crear perfiles adecuados en la cartera de servicios que se ofrecerá a la venta.

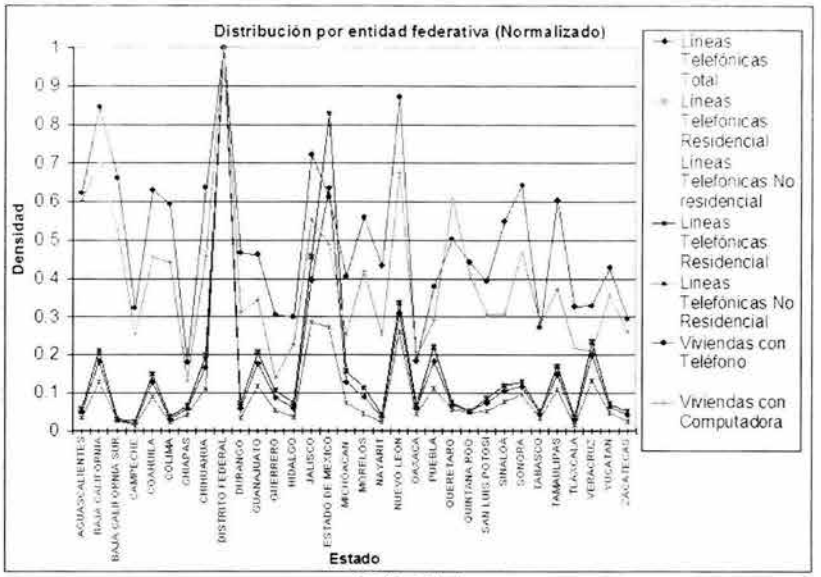
Ubicación geográfica

Una vez ubicado el espectro de usuarios a los que se proveerá servicio. debemos localizarlos geográficamente para comenzar a proponer la red como tal.

En este caso nos basaremos en la cantidad de usuarios de líneas telefónicas residenciales y no residenciales, viviendas con computadora y viviendas con teléfono conforme a los datos proporcionados por el INEGI y COFETEL por entidad federativa en el año 2003, ya que proporcionan un indicador del nivel de requerimientos y desarrollo en telecomunicaciones de cada una de las entidades, y aunque no reflejan la tendencia del tipo de tráfico exactamente al que enfocaremos la red, si proporciona un indicador de la posibilidad de recibir tráfico en dichas zonas geográficas, ya que al estar más urbanizada, con mayor población y más capacidad de comunicaciones, requerirá mayores facilidades en el servicio del tráfico de información, requerimiento que nuestra red como Proveedor de Servicios de comunicaciones solucionará.

Los datos se tabulan a continuación como primer paso de la localización de los puntos de interés.

Tomando como base las tablas 7.1.2 y 7.1.3, se grafican las distribuciones de tráfico normalizándolas respecto al máximo de cada categoría, buscando las áreas de mayor demanda de servicios:



Gráfica 7.1.1

	INEGI			COFETEL			
	Lineas Telefónicas Total [lineas]	Lineas Telefónicas Residencial [lineas]	Lineas Telefónicas No residencial [lineas]	Lineas Telefónicas Residencial [lineas]	Lineas Telefónicas No Residencial [lineas]	Viviendas con Teléfono [por cada 100 habitantes]	Viviendas con Computadora [por cada 100 habitantes]
Aguascalientes	166,138	125,905	40,233	125905	40233	41.1	13
Baja California	616,712	466,735	149,977	466735	149977	55.8	15.1
Baja California Sur	98,026	66,424	31,602	66424	31602	43.6	11.3
Campeche	68,274	52,139	16,135	52139	16135	21.3	5.5
Coahuila	434,676	330,470	104,206	330470	104206	41.5	9.8
Colima	104,789	78,365	26,424	78365	26424	39.2	9.5
Chiapas	194,659	146,724	47,935	146724	47935	11.8	2.8
Chihuahua	564,893	436,375	128,518	436375	128518	42	9.9
Distrito Federal	3,377,563	2,210,744	1,166,819	2210744	1166819	66	21.5
Durango	198,068	158,682	39,386	158682	39386	30.8	6.7
Guanajuato	594,663	458,962	135,701	458962	135701	30.5	7.4
Guerrero	293,672	232,323	61,349	232323	61349	20.1	3
Hidalgo	201,545	160,024	41,521	160024	41521	19.8	4.9
Jalisco	1,340,974	1,007,847	333,127	1007847	333127	47.7	11.9
Estado de México	2,151,466	1,833,421	318,045	1833421	318045	40.4	10.5
Michoacán	431,126	346,648	84,478	346648	84478	26.7	5.5
Morelos	301,335	249,336	51,999	249336	51999	37	9
Nayarit	122,232	94,963	27,269	94963	27269	28.6	5.4
Nuevo León	1,050,412	745,689	304,723	745689	304723	57.5	14.5
Oaxaca	201,854	150,815	51,039	150815	51039	12.1	4.2
Puebla	615,655	486,496	129,159	486496	129159	25	6.3
Queretaro	227,308	163,022	64,286	163022	64286	33.2	13.1
Quintana roo	171,788	114,583	57,205	114583	57205	29.2	8.8
San Luis Potosi	247,084	186,869	60,215	186869	60215	25.9	6.6
Sinaloa	351,911	261,935	89,976	261935	89976	36.2	6.6
Sonora	398,073	287,384	110,689	287384	110689	42.4	10.1
Tabasco	152,245	114,399	37,846	114399	37846	18	6.1
Tamaulipas	503,041	377,074	125,967	377074	125967	39.8	8
Tlaxcala	100,227	83,279	16,948	83279	16948	21.6	4.7
Veracruz	674,851	520,539	154,312	520539	154312	21.7	4.5
Yucatan	214,600	159,234	55,366	159234	55366	28.3	7.7
Zacatecas	141,270	112,886	28,384	112886	28384	19.5	5.6
Nacional	16,311,130	12,220,291	4,090,839	12220291	4090839	36.2	9.5

Tabla 7.1.2

La tabla 7.1.3 se presenta ordenada en cada una de sus columnas descendentemente en función del tráfico del servicio en cada uno de los estados:

Lineas Telefónicas Total	Lineas Telefónicas Residencial	Lineas Telefónicas No residencial	Lineas Telefónicas Residencial	Lineas Telefónicas No Residencial	Viviendas con Teléfono	Viviendas con Computadora
DISTRITO FEDERAL	DISTRITO FEDERAL	DISTRITO FEDERAL	DISTRITO FEDERAL	DISTRITO FEDERAL	DISTRITO FEDERAL	DISTRITO FEDERAL
ESTADO DE MEXICO	ESTADO DE MEXICO	JALISCO	ESTADO DE MEXICO	JALISCO	NUEVO LEON	BAJA CALIFORNIA
JALISCO	JALISCO	ESTADO DE MEXICO	JALISCO	ESTADO DE MEXICO	BAJA CALIFORNIA	NUEVO LEON
NUEVO LEON	NUEVO LEON	NUEVO LEON	NUEVO LEON	NUEVO LEON	JALISCO	QUERETARO
VERACRUZ	VERACRUZ	VERACRUZ	VERACRUZ	VERACRUZ	BAJA CALIFORNIA SUR	AGUASCALIENTES
BAJA CALIFORNIA	PUEBLA	BAJA CALIFORNIA	PUEBLA	BAJA CALIFORNIA	SONORA	JALISCO
PUEBLA	BAJA CALIFORNIA	GUANAJUATO	BAJA CALIFORNIA	GUANAJUATO	CHIHUAHUA	BAJA CALIFORNIA SUR
GUANAJUATO	GUANAJUATO	PUEBLA	GUANAJUATO	PUEBLA	COAHUILA	ESTADO DE MEXICO
CHIHUAHUA	CHIHUAHUA	CHIHUAHUA	CHIHUAHUA	CHIHUAHUA	AGUASCALIENTES	SONORA
TAMAULIPAS	TAMAULIPAS	TAMAULIPAS	TAMAULIPAS	TAMAULIPAS	ESTADO DE MEXICO	CHIHUAHUA
COAHUILA	MICHOACAN	SONORA	MICHOACAN	SONORA	TAMAULIPAS	COAHUILA
MICHOACAN	COAHUILA	COAHUILA	COAHUILA	COAHUILA	COLIMA	COLIMA
SONORA	SONORA	SINALOA	SONORA	SINALOA	MORELOS	MORELOS
SINALOA	SINALOA	MICHOACAN	SINALOA	MICHOACAN	SINALOA	QUINTANA ROO
MORELOS	MORELOS	QUERETARO	MORELOS	QUERETARO	QUERETARO	TAMAULIPAS
GUERRERO	GUERRERO	GUERRERO	GUERRERO	GUERRERO	DURANGO	YUCATAN
SAN LUIS POTOSI	SAN LUIS POTOSI	SAN LUIS POTOSI	SAN LUIS POTOSI	SAN LUIS POTOSI	GUANAJUATO	GUANAJUATO
QUERETARO	QUERETARO	QUINTANA ROO	QUERETARO	QUINTANA ROO	QUINTANA ROO	DURANGO
YUCATAN	HIDALGO	YUCATAN	HIDALGO	YUCATAN	NAYARIT	SINALOA
OAXACA	YUCATAN	MORELOS	YUCATAN	MORELOS	YUCATAN	SAN LUIS POTOSI
HIDALGO	DURANGO	OAXACA	DURANGO	OAXACA	MICHOACAN	PUEBLA
DURANGO	OAXACA	CHIAPAS	OAXACA	CHIAPAS	SAN LUIS POTOSI	TABASCO
CHIAPAS	CHIAPAS	HIDALGO	CHIAPAS	HIDALGO	PUEBLA	ZACATECAS
QUINTANA ROO	AGUASCALIENTES	AGUASCALIENTES	AGUASCALIENTES	AGUASCALIENTES	VERACRUZ	MICHOACAN
AGUASCALIENTES	QUINTANA ROO	DURANGO	QUINTANA ROO	DURANGO	TLAXCALA	CAMPECHE
TABASCO	TABASCO	TABASCO	TABASCO	TABASCO	CAMPECHE	NAYARIT
ZACATECAS	ZACATECAS	BAJA CALIFORNIA SUR	ZACATECAS	BAJA CALIFORNIA SUR	GUERRERO	HIDALGO
NAYARIT	NAYARIT	ZACATECAS	NAYARIT	ZACATECAS	HIDALGO	TLAXCALA
COLIMA	TLAXCALA	NAYARIT	TLAXCALA	NAYARIT	ZACATECAS	VERACRUZ
TLAXCALA	COLIMA	COLIMA	COLIMA	COLIMA	TABASCO	OAXACA
BAJA CALIFORNIA SUR	BAJA CALIFORNIA SUR	TLAXCALA	BAJA CALIFORNIA SUR	TLAXCALA	OAXACA	GUERRERO
CAMPECHE	CAMPECHE	CAMPECHE	CAMPECHE	CAMPECHE	CHIAPAS	CHIAPAS

Tabla 7.1.3

A partir de la tabla anterior, se encuentran las ciudades con mayor cantidad de tráfico coincidentes en las diferentes categorías graficadas, clasificándolas en tres bloques de Estimación de Tráfico (Mayor. Medio y Menor)

MAYOR	MEDIO	MENOR
BAJA CALIFORNIA	AGUASCALIENTES	CAMPECHE
DISTRITO FEDERAL	BAJA CALIFORNIA SUR	CHIAPAS
ESTADO DE MEXICO	CHIHUAHUA	DURANGO
JALISCO	COAHUILA	GUERRERO
NUEVO LEON	COLIMA	HIDALGO
PUEBLA	GUANAJUATO	NAYARIT
	MICHOACAN	OAXACA
	MORELOS	QUINTANA ROO
	QUERETARO	SAN LUIS POTOSI
	SINALOA	TABASCO
	SONORA	YUCATAN
	TAMAULIPAS	ZACATECAS
	TLAXCALA	
	VERACRUZ	

Tabla 7.1.4

VII.1.2 ESTIMACIÓN DE TRÁFICO Y REGIONES

Estimación de Tráfico

La estimación del tráfico en los enlaces se hará considerando la filosofía del peor caso, es decir, considerando que todos los usuarios de la red se conecten al mismo tiempo utilizando el máximo del Ancho de Banda contratado en el tiempo conocido como de alta utilización (busy-period), así como en el instante más ocupado del día. Así, dimensionaremos los enlaces al 50% del tráfico total encontrado, obteniendo una primera propuesta para el diseño e implementación de la red. Consideraremos también, que al monitorear el tráfico en la red y encontrar que un enlace se utiliza continuamente por arriba del 80% de su capacidad total, se deberá aumentar el Ancho de Banda para evitar congestiones y complicaciones de tráfico.

Es necesario definir el tipo (capa de pertenencia) de los nodos de la red, los cuales fueron posicionados de acuerdo a las políticas de tráfico y servicio del Proveedor para proponer la capacidad del enlace que les corresponderá. Servirá grandemente contar de antemano con estimaciones de los patrones de tráfico para cada región.

Tenemos que considerar en la probabilidad de falla de un enlace, donde el Ancho de Banda de los enlaces sobre los que se distribuirá la carga podrá ser sobrepasado, por lo que se recomienda limitar el Ancho de Banda o agregar capacidad como respaldo.

Se proponen las siguientes capacidades para los enlaces:

- Unión de nodos Backbone: Enlaces STM4 = 612 Mbps.
- Enlaces Distribución a Backbone: Enlaces STM1 = 155 Mbps.
- Enlaces Acceso a Distribución: Enlaces E3 = 34 Mbps (o mayor en función de los servicios como en el caso de ofrecer VPNs).

Se propone dimensionar los enlaces de la red, y aunque no es el propósito del diseño inicial el producir una red perfectamente dimensionada, se hará la mejor aproximación posible. Posteriormente se podrán realizar muchas aproximaciones en el proceso de optimización de la red, que es el último paso en el proceso de diseño.

Con la estimación de tráfico hecha, y para proponer paquetes de servicio que cubran con las necesidades grupos de usuarios, solo nos resta ubicar el tráfico a recibir de cada región del área total de servicio.

Regiones

Considerando la distribución esperada de tráfico y teniendo en mente el volumen de tráfico que tendrá que ser manejado por cada una de las áreas, representaremos esto gráficamente en el área elegida para el servicio en la figura 7.1.5.

La separación en regiones se hará con el criterio de recopilar la mayor cantidad de tráfico actual, así como prever las regiones donde se espera mayor crecimiento en sus requerimientos de transporte de datos en los próximos años.

A partir de la figura 7.1.5, delimitaremos las áreas en las que proporcionaremos el servicio más intensamente, así como la conveniencia de unir o separar tráfico de distintas zonas.

Proponemos la figura 7.1.6 organizando las regiones de tráfico en conjuntos manejables como primer paso para la proposición de la estructura funcional del diseño de red.

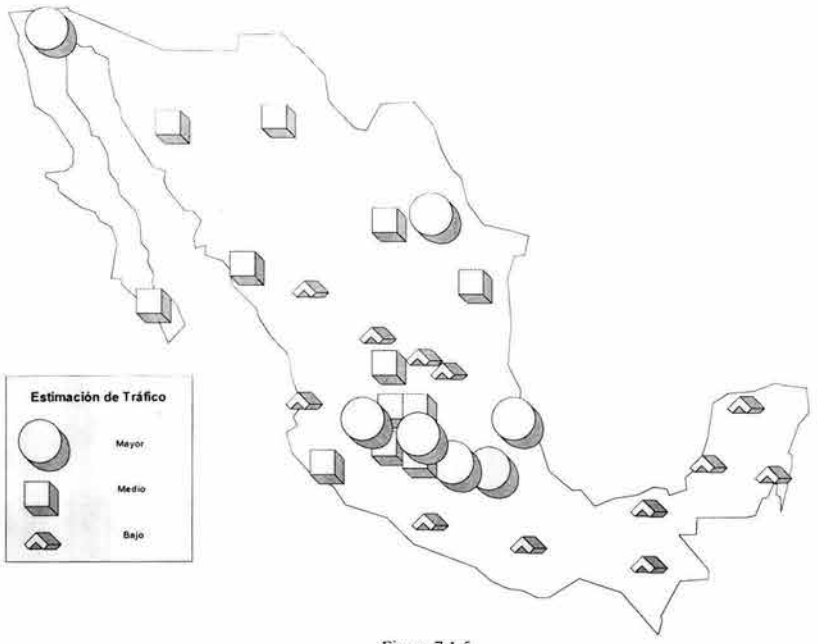


Figura 7.1.5

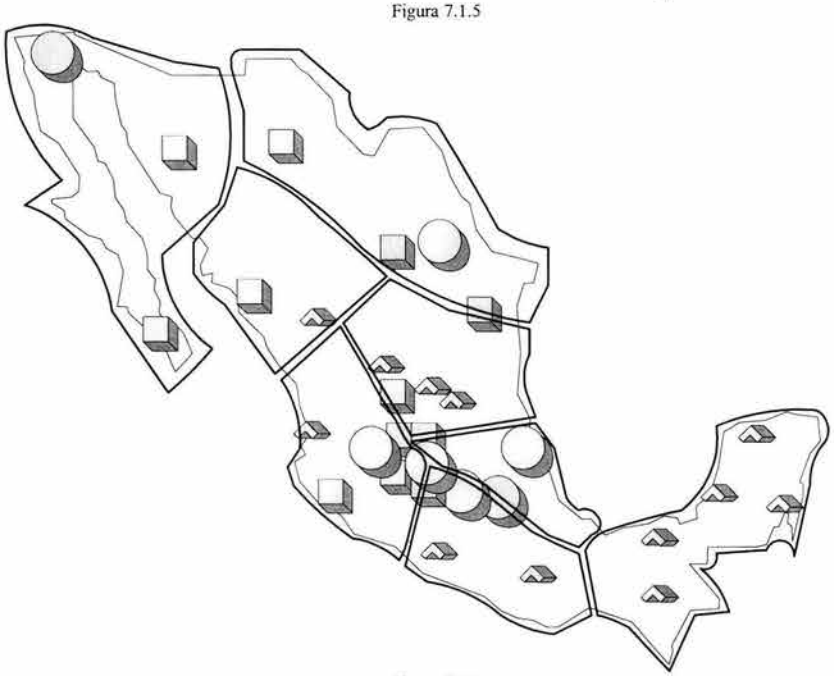


Figura 7.1.6

Una vez ubicando las áreas de servicio, asignaremos dentro de cada una de ellas, de acuerdo a la distribución esperada de tráfico, un nivel de la jerarquía del modelo de tres capas, teniendo en cuenta el sitio de mejor localización de los nodos de Backbone, ya que al transitar toda la información por ellos, debe ser accesible a todos los nodos de Distribución, que a su vez deberán posicionarse con vista a que puedan recolectar el tráfico de su área asignada fácilmente; finalmente, los nodos de Acceso se posicionarán específicamente donde se requiera recolectar el tráfico de los usuarios.

Conceptualmente, con base a la funcionalidad de los nodos, la red será propuesta de la siguiente manera:

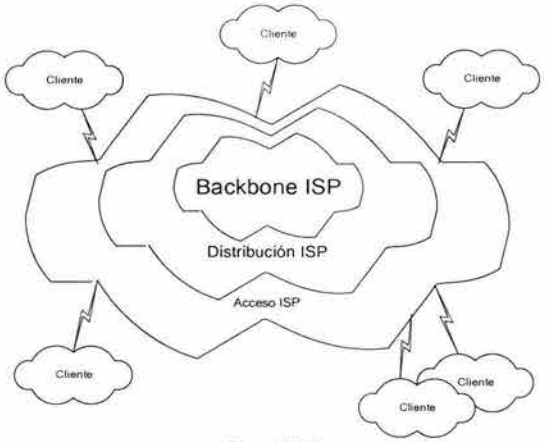


Figura 7.1.7

VII.2 PROPUESTA DE TOPOLOGÍA FÍSICA

En este punto, conocemos las posibilidades de configuración con las que contamos para implementar la red, por lo que procederemos a proponer la topología física específica, es decir, la forma de interconexión de los elementos de la red.

Teniendo presentes las consideraciones del subtema anterior, estamos en posibilidad de ubicar físicamente los nodos de la red, los cuales aseguramos tendrán

facilidades de escalamiento y administración por ser configurados con el modelo jerárquico.

Ahora propondremos la interconexión de equipos.

VII.2.1 BACKBONE

Su utilidad es innegable, ya que por ésta capa, transitará todo el tráfico de la red. La localización de sus nodos se propondrá en sitios de mucho tráfico local para que la Capa de Distribución se encuentre cercana físicamente. Se considera como localización ideal una población con una ubicación ventajosa respecto a los nodos restantes de la red, asegurando que el tránsito por dicho nodo sea accesible y conveniente a la mayoría de sus nodos vecinos (Distribución y Backbone). Lo anterior buscando la mayor confiabilidad y redundancia. Se implementará con la topología de HiperCubo revisada en el Capítulo 6.

Para la implementación específica nos guiaremos en la Tabla 7.2.1 que indica las ciudades con mayor tráfico, así como en la distribución por regiones previamente realizada, proponiendo la sustitución de algunos nodos, prefiriendo la recopilación de tráfico de lugares aledaños a el local (lo que representará un mayor tráfico colectado). Así, nuestra propuesta será la siguiente:

Localización del Nodo	Estimación de tráfico local	Región de servicio	Criterio de posicionamiento
Baja California Norte	Alto	Baja California Norte Baja California Sur Sonora	Área / Tráfico
Nuevo León	Alto	Chihuahua Coahuila Nuevo León Tamaulipas	Área / Tráfico
Sinaloa	Medio-Bajo	Sinaloa Durango Nayarit Zacatecas	Área
San Luis Potosí	Medio-Bajo	San Luis Potosí Norte de Veracruz Guanajuato Querétaro Hidalgo	Área
Jalisco	Alto	Jalisco Aguascalientes Colima Michoacán Guerrero	Trafico
Distrito Federal Norte	Alto	Cetro de Veracruz	Trafico

		Estado de México Distrito Federal Tlaxcala	
Distrito Federal Sur	Alto	Estado de México Distrito Federal Morelos Puebla Guerrero Oaxaca	Trafico
Tabasco	Bajo	Sur de Veracruz Oaxaca Yucatán Campeche Quintana Roo Tabasco Chiapas	Área

Tabla 7.2.1

Donde la estimación del tráfico local se efectuó en base a la tabla 7.1.1, y en la columna de la Región de Servicio se incluye genéricamente las entidades y regiones que serán cubiertas por el nodo. Se ha colocando un nodo más en DF dada la cantidad de tráfico que pasa por él y su cercanía al área metropolitana, así como colocar un nodo en Tabasco, ya que su localización proporcionará servicio a la zona sur.

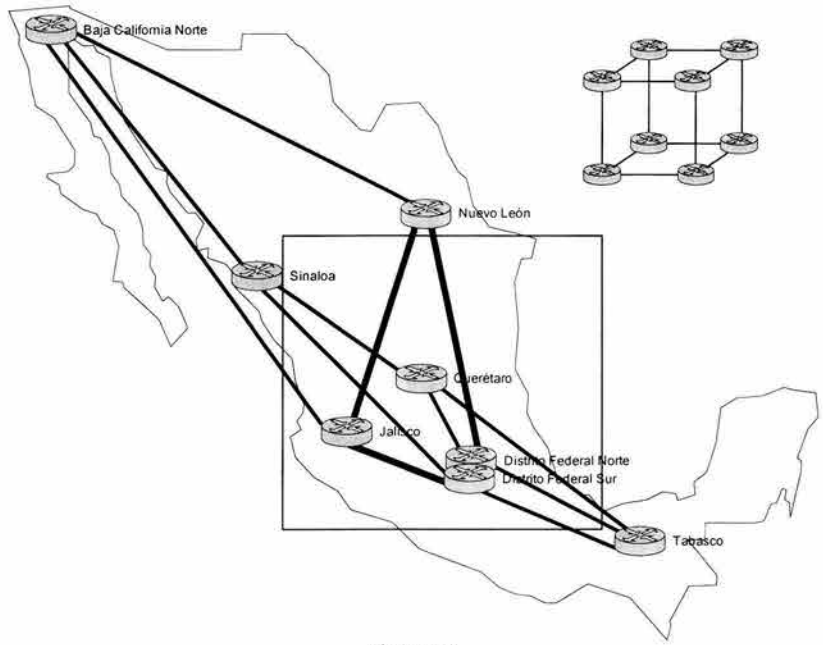


Figura 7.2.2

Cabe destacar que en las redes tradicionales orientadas a conexión, la acción de re-enrutar los VC's es el ultimo recurso a usarse solo cuando todos los otros mecanismos de redundancia han fallado. Esto es por que inevitablemente se involucra interrupción del tráfico del usuario por varios segundos o minutos, mientras todos los circuitos son re-enrutados. En las redes IP tradicionales, re-enrutar es un problema mucho menos severo, dado que cuando un paquete fluye puede ser conmutado de un enlace a otro casi instantáneamente, una vez que el protocolo de enrutamiento ha convergido.

Las redes MPLS oscilan entre esos dos extremos, ya que el re-enrutamiento en las redes MPLS es necesario que converja el protocolo de enrutamiento, para posteriormente se creen los LSPs. Sin embargo, dicha necesidad no afecta el desempeño general de la red ni su administración.

VII.2.2 DISTRIBUCIÓN

Proponemos como topología física para la conexión de los nodos de ésta capa, la conexión directa a Backbone, o en caso de requerir mayor jerarquización, utilizar una topología en estrella de un nivel para optimizar la administración y topología de la red. Su función principal es distribuir el servicio cubriendo el área en que se de servicio, asegurando una jerarquización, administración y flujo de datos sencillos

En base a las áreas propuestas (y cubiertas por los nodos Backbone posicionados), colocaremos los nodos de Distribución en las ciudades y regiones que así lo exijan en base al tráfico estimado que se recibirá de ellos.

Se presenta un acercamiento a la región centro del país, mostrando posibles localizaciones de los nodos de Distribución.

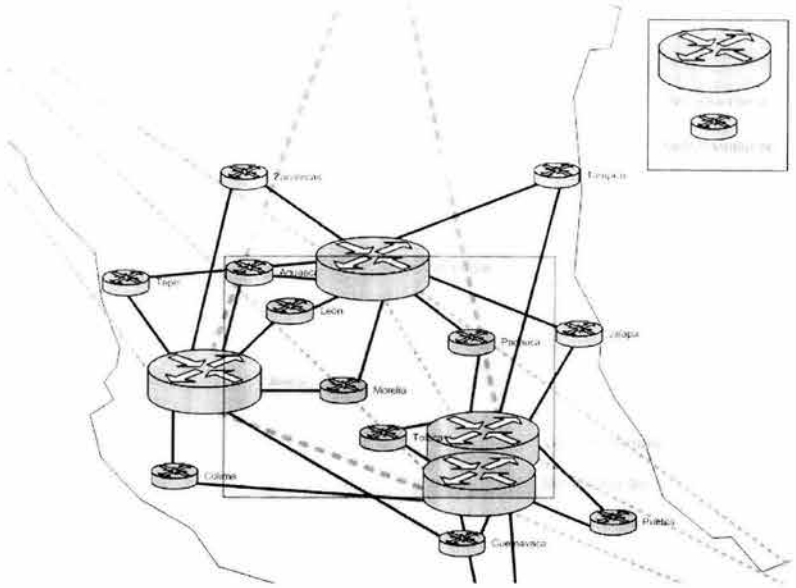


Figura 7.2.3

VII.1.3 ACCESO

Propondremos como interconexión de los nodos de esta capa, la topología en árbol explicada en el Capitulo 6. No se establece un límite en los niveles de expansión ni en los usuarios conectados. En función de los servicios y para escalabilidad y administración se agregan enrutadores especializados, debido a que buscamos recolectar el tráfico de los usuarios en un punto de acceso de la red.

El criterio para posicionar los nodos de Acceso será el volumen de tráfico recibido y la necesidad de proporcionar el servicio de red en un área particular.

Se presenta una propuesta de localización de nodos en un acercamiento a la región central del país.

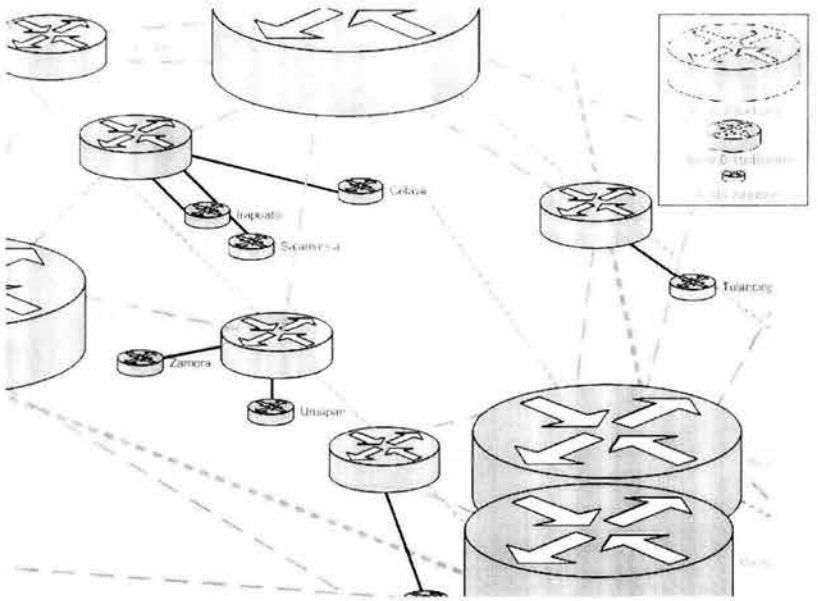


Figura 7.2.4

La implementación específica del nodo de distribución, es decir, la capacidad de los enrutadores, el tipo y número de ellos serán determinados por el volumen de tráfico estimado a captar en esa región y al tipo de acceso, y servicios ofrecidos en la misma área.

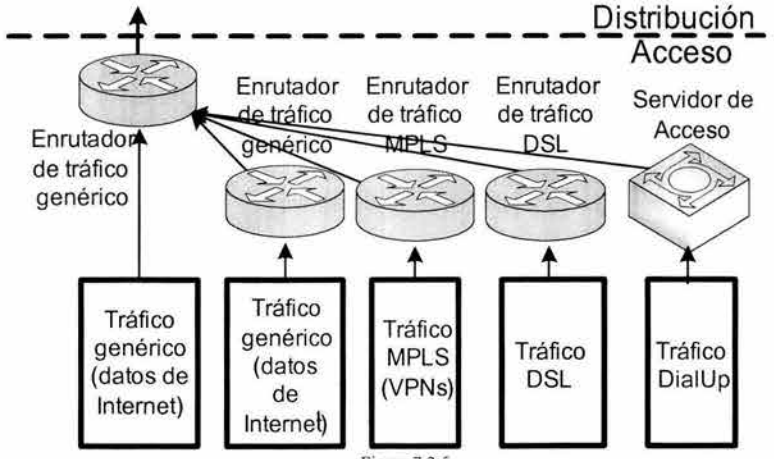


Figura 7.2.5

VII.2.4 CONEXIÓN CON OTROS ISP's

Propondremos dos puntos de interconexión con proveedores de servicio mayores, por razones de eficiencia y redundancia en el tráfico de datos. Los nodos Backbone elegidos serán: DFN debido a su ubicación céntrica, concentradora de tráfico y servicios, así como NL por su concentración de tráfico y cercanía geográfica con el proveedor de conexión.

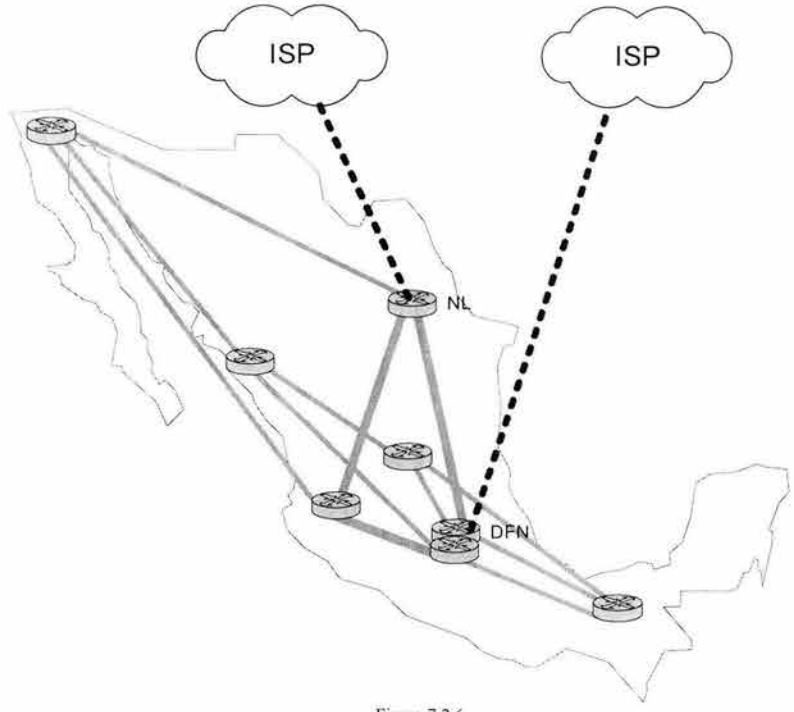


Figura 7.2.6

Proseguiremos con el proceso de diseño, asegurando que esta topología física cumple con los criterios propuestos en el principio del capítulo como directivas básicas del diseño de red, es decir, contar con escalabilidad, redundancia y tolerancia a fallas.

VII.3 PROPUESTA DE TOPOLOGÍA LÓGICA

Enunciando las mejores prácticas, que cabe resaltar únicamente son eso, mejores prácticas, y a partir del capítulo anterior donde mostramos un esquema ocupando los mejores criterios para la elección de una topología lógica, ahora tenemos las bases para realizar una propuesta de topología lógica específica.

Básicamente tenemos un objetivo principal, que la topología lógica se ajuste en la su mayor parte a la topología física, la razón es que de esta forma se tendrá una mejor administración y nuestro diseño será escalable, ya que cuando se quiera escalar la topología física también podremos escalar de forma sencilla la topología lógica o viceversa. Lo anterior nunca hay que perderlo de vista, ya que un buen diseño depende de que tan fácil sea hacer modificaciones a la red, sin tener un impacto negativo en su desempeño. Hay que partir de que entre mas sencilla sea la red más fácil será su administración, esto no quiere decir que no sea robusta.

Elección del Modelo

En principio, como ya se mencionó en la topología física, ocuparemos el *modelo jerárquico*, es decir, tendremos Capa 0 o Backbone, Distribución y la Capa de Acceso, mientras que en la topología lógica tendremos el Área 0 ó Backbone, y áreas aledañas que conocidas como Capa de Distribución y Acceso, denominadas DA´s.

Si partimos de la topología física propuesta en el subtema anterior, se tendrán enrutadores de Backbone y de Distribución conocidos como enrutadores "P", y los enrutadores de Acceso (PE). Lo anterior puede escucharse obvio pero esto es el resultado del proceso de convenciones que se siguen en el diseño de la red.

VII.3.1 CONSIDERACIONES DEL PROTOCOLO OSPF

Como nuestro IGP es OSPF, debemos respetar las consideraciones mencionadas en el diseño lógico destacando por su importancia:

1. Topología de red (Área Backbone y Áreas DA)
   Definir correctamente las Áreas y su tamaño es de primera necesidad, y está profundamente relacionada con la topología física, ya que se tiene que encontrar el balance entre el tamaño físico así como su ubicación de ambas partes.
2. Realizar correctamente el Direccionamiento, así como su dimensionamiento para el crecimiento posterior.
   El direccionamiento es muy importante, principalmente debemos tomar en cuenta:
   - El direccionamiento deberá ser totalmente aprovechado, por ejemplo para direccionar un enlace entre 2 enrutadores solo se requiere de las IP de ambas interfases (figura 7.3.1), y tomar en cuenta la red y el broadcast, es por ello que únicamente se requiere una máscara de 30 bits para la red como se muestra en la figura:

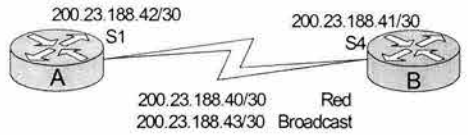


Figura 7.3.1

   - Por otro lado hay que dimensionar correctamente el direccionamiento de las áreas, esto depende del tamaño del área y del crecimiento que se pueda tener a futuro, por lo que es importante dejar el direccionamiento suficiente. Una forma de verlo es si se van a tener 12 enlaces en un área, cada enlace requiere de 4 IP´s, por lo que el direccionamiento requerido es de 48 IP´s, sería suficiente una máscara de 26 bits para esa red, pero

para esa área es recomendable asignar una mascara de 25 bits por ejemplo. En OSPF el direccionamiento puede ser privado, por lo cual se pueden dejar rangos de IP´s extras para el crecimiento, sin costo alguno. Por otro lado se puede **sumarizar** toda la subred con un solo anuncio hacia el Backbone, aunque MPLS es un elemento que hay que tomar en cuenta, ya que si existe una sumarización de muchas redes MPLS puede desaprovechar su potencial.

3. Áreas pequeñas y bien delimitadas.
   Como ya se había mencionado para el correcto funcionamiento de OSPF las áreas tienen que ser pequeñas.
4. Escalabilidad de la Red.
   Cumpliendo con los tres puntos anteriores, en el caso de OSPF, es suficiente para poder tener una red escalable.
5. Selección de Rutas.
6. Convergencia.
7. Seguridad.

VII.3.2 CONSIDERACIONES DEL PROTOCOLO BGP

A) Tipo de conexión del Cliente

Para nuestro diseño e implementación, por política, solo permitiremos que los enrutadores PE, interactúen mediante rutas estáticas, o mediante el protocolo BGP como se muestra en la figura 7.3.2.

Figura 7.3.2

B) Dimensionamiento del Direccionamiento

En este caso es muy importante, ya que este direccionamiento hay que tramitarlo ante NIC, y generalmente tiene un costo. Por lo que hay determinar las necesidades del cliente y asignar un direccionamiento justo al cliente, por otro lado hay que dejar suficientes direcciones públicas para cada área de acceso, es recomendable reservar un rango de direcciones IP para un posible centro de computo del ISP, donde se pueda prestar servicios de hosting.

C) Implementación del protocolo en el ISP

Como se vio en las características de BGP se puede manejar Route Reflector (RR), que es la mejor opción para realizar actualizaciones de rutas de BGP, esto tiene grandes ventajas en la administración y mantenimiento de la red, ya que todas la sesiones serán con el RR.

Es recomendable que en cada área de Distribución tenga un RR para actualizar la tabla del BGP de los enrutadores del Área (figura 7.3.3), y este establecerá una sesión de BGP con el RR de Backbone, éste último actualizará las tablas de BGP de todos los RR de Distribución, por lo que se recomienda que en el Backbone se tenga un RR de backup. Lo anterior decrementa el desempeño de los enrutadores, pero la ventaja es evidente en la mejor administración de la red.

D) Proveedores de servicio de Internet del ISP

Se propone que se tengan por lo menos dos proveedores de servicio internacionales (figura 7.3.3), por redundancia en el servicio de Internet y aprovechar ambas salidas funcionando simultáneamente. Generalmente esta conexión se realiza ocupando el protocolo BGP o Enrutamiento estático, solo que ahora el ISP forma parte de los clientes de un ISP de mayor capacidad.

Basándonos en el topología física propuesta, así como en la consideraciones anteriores podemos ver a nuestra red como en la figura 7.3.3:

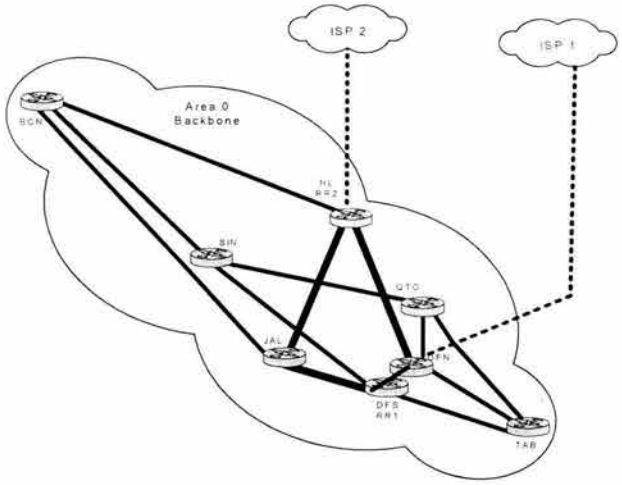


Figura 7.3.3

Con el fin de aprovechar la funcionalidad de la presencia de un RR en Backbone, designaremos al nodo DFS-RR1, sin embargo por redundancia en el diseño se pondrá al enrutador QRO-RR2 como el enrutador de respaldo (figura 7.3.3), se pueden tener enlaces físicos redundantes al Backbone, así como sesiones redundantes desde el punto de vista lógico (figura 7.3.3) como se vio en el capítulo anterior. Bajo consideraciones especiales, se podría considerar implementar una topología full-mesh en el Backbone en el caso de contar con poco equipos en esta capa.

En cuanto al área de Distribución - Acceso, la podemos ver como una nube conectada al área 0, con la característica de dar servicio a una región en específico, se debe tomar en cuenta la sumarización, así como el tamaño del nodo de distribución. Estas Áreas pueden ser de distintos tamaños dependiendo de la región geográfica en la que se encuentren, y el tráfico que se pueda recibir de cada región. Como se ve en el Área 1, se tienen dos enrutadores de distribución debido a la cobertura e importancia que se tiene en el Área, por lo que es bueno distribuir el trabajo a dos

enrutadores, sin perder de vista que pertenecen al la misma Área de OSPF y que se siga respetando el modelo jerárquico, ambos son RR (RR A1 y RR B1) del Área, esto para proveer mayor redundancia y tolerancia a fallas.

Por otra parte, cuando no se tiene la suficiente infraestructura, el diseño puede ser muy vulnerable, como es el caso del Área 3, donde se tiene un solo RR y un solo enlace al Backbone, así como una sesión de BGP con el RR1. El caso más usual en el cual la propuesta hace mayor referencia es el Área 4, donde se tienen enlaces físicos redundantes si como sesiones de BGP con ambos RR de Backbone.

A continuación se muestra (figura 7.3.4) la estructura de la propuesta lógica:

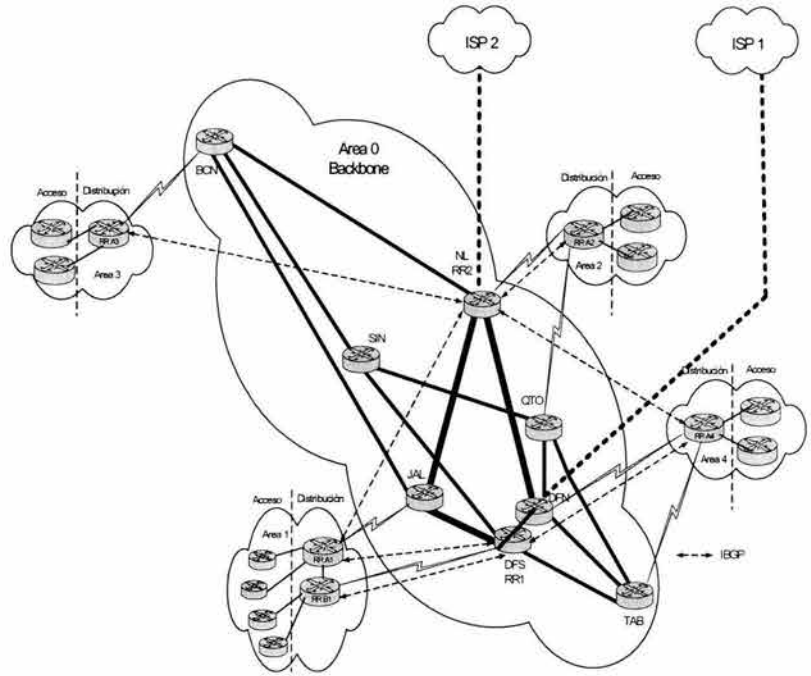


Figura 7.3.4

VII.3.3 DISEÑO LÓGICO CON MPLS

Para poder implementar MPLS en el diseño IP, se requiere que se tomen en cuenta diferentes aspectos importantes, los cuales nos darán un "*checklist*" de los pasos que deben estar ya funcionando para que MPLS opere correctamente.

- Direccionamiento asignado.
- Esquema de enrutamiento de OSPF y BGP debe estar funcionando correctamente.
- Probar la conectividad entre equipos terminales de los sitios.
- Medidas de eficiencia (Ancho de Banda).
- Revisar hardware y software de los enrutadores (P y PE) y asegurarse que soporten MPLS, VPN, LDP, RSVP. Hacer actualizaciones si es necesario.

Posteriormente habilitar:

  - MPLS en Backbone y DA.
  - LDP en Backbone y DA.
- MPLS-TE en áreas necesarias.
- Habilitar MBGP (para VPNs).
- Habilitar QoS.
  - Scheduling.
  - Encolamiento.
  - Congestión.

Nos interesa determinar en qué parte de la red se implementará MPLS, en este caso lo podemos dividir en tres partes básicamente:

1. MPLS-Internet: Tenemos que se implementará MPLS en el Backbone y en los enrutadores de Distribución esto únicamente con el objetivo de conmutar la información que va a Internet.
2. MPLS-Ingeniería de Tráfico: Se ocupará MPLS en las áreas de Backbone y distribución para elegir rutas alternativas para evitar la saturación de los enlaces.

3. MPLS-VPN: Se tiene que implementar desde la capa de Acceso es por ello que se dedicarán equipos específicos para realizar este tipo de tarea. Para realizar esta hay que tener explícitamente toda la información de enrutamiento.

Esta consideración de topología lógica es escalable, flexible, tolerante a fallas y cumple con todas las características y objetivos que nos hemos planteado en capítulos anteriores.

Aplicaciones de MPLS

Una vez diseñada la red IP, complementaremos como funcionalidad adicional MPLS, dado que en comparación con tecnologías similares que buscan optimizar el uso de la red, MPLS ofrece características deseables en nuestra red, persiguiendo:

- Ampliación de la cartera de servicios como Proveedor con la utilización de la infraestructura existente (principalmente enfocado a VPNs).
- Facilidad de administración de la red, QoS y TE.
- Reducción de carga para el protocolo IGP en la conmutación en el Backbone.
- Tráfico de distintas tecnologías por nuestra red (AToM).

En base al análisis de la tecnología, podemos encontrar varias ventajas en MPLS, por lo que visualizamos la aplicación de MPLS en la red, como una aplicación adicional, la cual incrementará el desempeño de la red, sobre todo en los siguientes ámbitos de datos:

Multimedia

MPLS es ideal para las comunicaciones multimedia cuyas exigencias de retardo de red son muy elevadas asegurando la entrega del tráfico con la velocidad y fiabilidad requerida (aplicaciones de voz y video corporativo).

Es adecuado para aquellas aplicaciones sensibles al retardo y en general para todo tipo de tráfico crítico para su negocio que se beneficiarán de un tratamiento prioritario

extremo a extremo dentro de la red (aplicaciones financieras y/o de gestión comercial).

Proporciona facilidad de la implementación de calidad de servicio.

Datos

Apropiado para aquellas aplicaciones de baja prioridad que transportan todo tipo de tráfico de datos sin requerimientos estrictos de retardo (e-mail, FTP, mensajería instantánea, chat)..

MPLS tiene la cualidad de permitir a las empresas clasificar sus aplicaciones y dar prioridad a aquellas que son de misión crítica y las sensibles al tiempo - tales como Vídeo o Voz-, sobre el tráfico que no es crítico en cuanto al tiempo, - correo electrónico o datos no prioritarios-. Así mismo, asigna a cada uno el Ancho de Banda que requiere.

Video

Un servicio de Videoconferencia administrado a través de una MPLS IP resulta útil debido al precio de tarifa fija, la facilidad de uso y la configuración de llamada rápida. Nos basamos en la muy probable convergencia de Video y Voz en la red de datos IP como próximo paso natural en los servicios de red de datos

Utilizando MPLS para distinguir la entrega de diversas calidades del tráfico del servicio (QoS), es posible combinar las redes de Vídeo y de Datos en un Proveedor de Servicio.

Otras funciones de video en MPLS:

- Alta velocidad, siempre en Ancho de Banda, adecuada para Videoconferencias.
- Contratos de nivel de servicio especialmente diseñados para cubrir los exigentes criterios de las comunicaciones internacionales de Video.
- Disponible como Video independiente o convergente con Voz y Datos.

Voz

Funcionando el tráfico deVvoz en MPLS en una red, la incertidumbre y la imprevisión del Internet es eliminada, y un nuevo nivel de la seguridad se permite.

Utilizando MPLS se puede asignar al tráfico de Voz una prioridad más alta, o la calidad del servicio (QoS) de tal modo se asegura que la Voz será entregada sin estado latente o pérdida del paquete. Se garantiza este rendimiento más alto con

acuerdos del porcentaje de disponibilidad-industria. Se mejoran los siguientes aspectos:

1. La imprevisión del Internet público
2. La carencia del control sobre pérdida del paquete y retraso
3. Establecer la seguridad para el tráfico de la Voz
4. La solución debe ser rentable justificar la puesta en práctica

VII.5 OPTIMIZACIÓN DE LA RED

Es recomendable, y necesario en la mayoría de los casos de diseño de red, refinar el diseño una vez que la red esta en operación como paso final en el proceso de optimización y puesta a punto.

La optimización más que un proceso correctivo, será una consecuencia del proceso iterativo continuo de monitoreo y administración de la red, posterior a la propuesta de dimensionamiento inicial de la red, la cual ayudará a que la red actualice sus objetivos de servicio específicos, manteniendo al día la cobertura y calidad de su servicio.

Adicionalmente debemos considerar que en la propuesta inicial de la red, la proposición de tráfico a captar de los usuarios es una estimación (lo mejor realizada con los elementos con que se cuente), sin embargo, la relación costo – beneficio que se evalúe tras cada periodo de operación, será un indicador esencial del nivel de optimización que se aplicará a la red.

VIII DOCUMENTANDO LA RED

Una vez terminado el proceso de análisis y diseño de la red, así como su implementación y pruebas, deberá contarse con registros de las características de la misma. Típicamente incluyen:

- Información geográfica detallada, como municipios, estados, ciudades e instalaciones.
- Conexiones WAN entre diferentes localizaciones geográficas.
- Indicación de la tecnología de capa de enlace de datos, así como el Ancho de Banda.
- Nombre de los proveedores de servicio WAN con que se interconecta, y de ser posible, el número del sistema autónomo deberá incluirse.
- Localización y direcciones de los dispositivos de interconexión importantes, (enrutadores).
- Localización y direcciones enrutadores con características especiales dentro de la red, tales como administración y Route Reflector.
- Documentación de configuración del software del enrutador.
- Documentación de configuración de hardware.

Aunque el procedimiento de documentación toma tiempo, dicha inversión es redituable al paso del tiempo, ya que el tener un manual de la red hará el trabajo de administrarla mucho mas sencillo. También hay que considerar que es necesario mantener la documentación actualizada.

Beneficios de documentar la red

- *Resolución de problemas más rápida*: El poseer una buena documentación reduce la necesidad de investigar soluciones para el mismo problema cada vez que éste aparezca. Un diagrama visual puede ayudar a identificar áreas potencialmente problemáticas a tiempo.
- *Reducción de pérdida de información*: Es útil para prevenir pérdida de información importante para a red cuando los empleados dejen la organización haciendo el periodo de transición menos difícil.

- *Compartición de tareas más fácil*: Con una documentación adecuada, los administradores de la red pueden exitosamente delegar responsabilidades de la red porque la información importante esta disponible en forma escrita.
- *Mejorar el diseño de la red*: Un diagrama actualizado de la red es un elemento clave en cualquier proceso de diseño, ya que se contará con una base sólida de la cual partir para proponer las mejoras.

VIII.1 INFORMACIÓN

Teóricamente: Una buena regla es incluir todo lo que sería necesario para reconstruir la red por completo cuando falle.

Realmente: La cantidad de profundidad de la documentación dependerá de la complejidad de la red y la cantidad de recursos vitales para la red.

Típicamente, una documentación de red se considerará completa si contiene como mínimo con los siguientes elementos:

- Diagrama (mapa) de la localización física.
- Diagrama lógico de la red.
- Diagrama físico de la red.
- Información del hardware.
- Información de la configuración.
- Información del protocolos.
- Información de funcionalidades adicionales.
- Información de administración de la red.
    - Información de clientes.
    - Información de otros proveedores de servicio.
- Hojas de especificaciones de los dispositivos.
- Documentación de procedimientos.
- Informes de utilización de red básicos.
- Políticas de uso.
- Políticas de seguridad.

- Plan de recuperación de desastres.

VIII.2 DIAGRAMAS

Diagrama Físico de la red

Para una rápida y efectiva resolución de problemas en la red, se debe entender la interacción física de las capas, equipos, y su interconexión; es decir, el cómo la piezas de la red encajan. La mejor manera de entender esto es a través de un diagrama físico de la red.

Se propone usar un diagrama del lugar geográfico en que la red esta instalada, y sobre él, crear un diagrama del cableado de la red en el que se incluya:

- Listado y localización física de los dispositivos de la red (enrutadores).
- Listado y localización de las interfases.
- Puntos de interconexión con otros proveedores.
- Segmentación lógica de la red.
- Dispositivos especiales.

También es recomendable incluir un diagrama con la disposición física del equipo donde se detalle:

- Puertos y direcciones correspondientes.
- Armario de alambrado (Wiring closet).
- Trayectos de los cables.

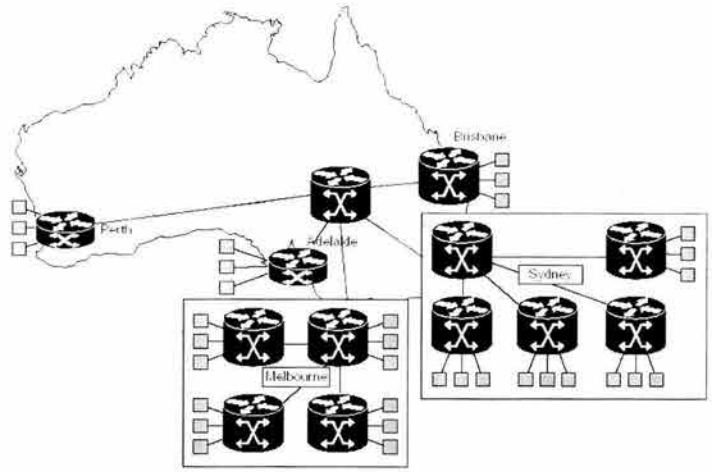


Figura 8.2.1

Punto de partida

Es recomendable, mas no necesario, empezar en el dispositivo de frontera o punto donde la red se conecte con el mundo exterior. Durante el proceso de creación del diagrama físico de la red, se puede físicamente verificar y documentar el cómo cada dispositivo de red esta conectado, así como etiquetar cada dispositivo identificado, para lo cual podemos considerar:

- Crear un esquema de etiquetado.
- No basar etiquetas en nombres propios.
- Etiquetar ambos extremos de cada cable.

Utilización de software para diagramas

La documentación puede ser tan simple como un dibujo hecho a mano del diagrama de la red, o tan complejo como una serie de diagramas de software especializado interconectados con la configuración de los equipos incluida. El factor determinante es que la información sea factible a actualizarse.

- Ventajas: Usar un software puede hacer las actualizaciones más sencillas. Solo habrá que asegurarse que se tenga clara la versión actual del diagrama de la red.
- Desventajas: Algunos paquetes son complejos y caros. La curva de aprendizaje puede ser un poco alta.

Ejemplos de Diagramas físicos de la red

No es importante cual herramienta se utilice para el diagrama de la red. Lo que es importante es que se realize.

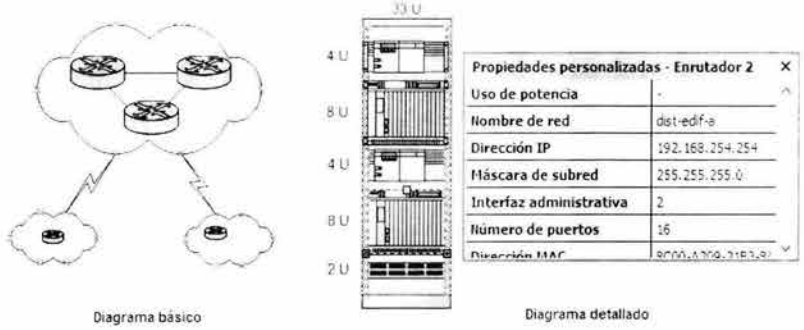


Figura 8.2.2

Diagrama lógico de la red

El diagrama lógico de la red contiene información de capas superiores (por ejemplo protocolos de enrutamiento, aplicaciones, etc). Esto provee una información detallada de cómo el tráfico toma forma de un dispositivo a otro lógicamente.

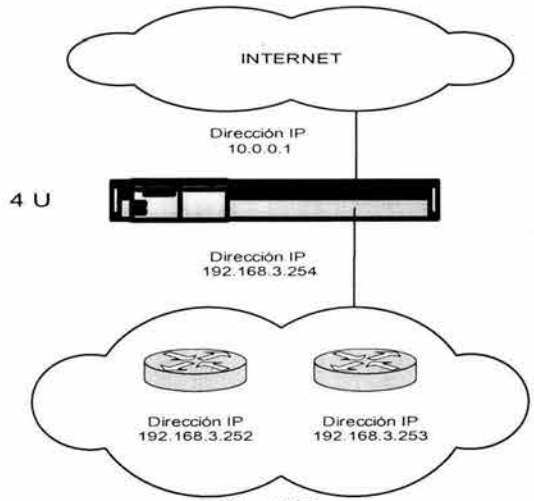


Figura 8.2.3

VIII.3 INFORMACIÓN DE LOS DISPOSITIVOS Y ADMINISTRACIÓN DE LA RED

Rastreando la información

Se puede partir en base a la red, rastreando la documentación por uno mismo o utilizando una herramienta que ayude a hacer el seguimiento de forma mas automatizada.

Hardware

Enlistar la informaron de hardware para cada dispositivo de red

- Fabricación, marca, modelo.
- Numero de serie.
- Numero de puertos.
- Hechura y modelo de la tarjeta de interfase de red.
- Dirección MAC.
- Tipo de conector(es).

Información de la configuración

Documentar la información de la configuración puede ser aun más crítico que la información de hardware. El hardware es fácilmente reemplazado, pero una configuración perdida o una configuración no estándar puede ser imposible de recrear. Se debe documentar la configuración para cada dispositivo.

- Imprimir copias de los archivos de configuración.
- Guardar copias en disco o en otro enrutador.
- Documentar configuraciones específicas de software.
- Incluir rangos usados, por ejemplo, en TCP/IP.

Recursos de administración de la red

- Listas de llamadas: A quien llamar cuando exista un problema en la red.
  - Nombres de los contactos.
  - Números telefónicos.
- Informaron del vendedor del hardware.
- Información del vendedor del software.
- Información de las licencias de software.
- Contactos de mantenimiento.

Hojas de eventos para la información actualización / parches del Hardware / Software

Información de eventos para cada dispositivo de la red

- Cambios en la configuración y la fecha en que dichos cambios fueron efectuados.
- Versiones de las actualizaciones o parches.
- Información de actualización o reemplazo de hardware (numero de las partes).

Procedimientos de Documentación

Administración de la red en general

- Como agregar usuarios.
- Plantillas usadas.

Administración del enrutador

- Configuraciones típicas de enrutadores.
- Información de configuraciones para aplicaciones específicas (VPN's por ejemplo).
- Agenda (respaldos, parches, archivos de sucesos, etc.)

Estadísticas de utilización

Para propósitos de resolución de problemas, es recomendable que se tenga una línea de partida en forma estadística de utilización de los dispositivos, comprendiendo Datos comparativos y Tendencias de uso.

Políticas aceptables de uso

Incluir una copia actualizada de las políticas de uso de la compañía, la cual delinea los términos y condiciones para el uso de la red. Define que es considerado como uso aceptable y también penaliza las violaciones de las reglas.

Información de seguridad

Debe de considerarse hacer copias de la política de seguridad activa para cada segmento de red, así como un registro de quién ha tenido acceso a la información de passwords y otra información confidencial. Es recomendable tener establecidos procedimientos para reportar un incidente de seguridad, antes que el mismo se presente.

Plan de recuperación después de desastres

Incluir en cada localización del dispositivos, una copia actualizada del plan de recuperación después de desastres de la organización, donde se contemplen las acciones generales en la red, y específicas de cada dispositivo en particular.

Facilidades para realizar la documentación

- Generada por externos.
- Herramientas de red (Software).
- Recursos Adicionales (Libros, Periódicos).

CONCLUSIONES

El tocar conceptos básicos de redes, nos permitió comprender y explicar mejor los conceptos posteriores, los cuales se fundamentan en los conceptos básicos de redes WAN, modelo de referencia OSI, la familia de protocolos TCP / IP y tecnologías de Capa 2 como Frame Relay y ATM.

Expusimos las ventajas de contar con MPLS en la red, como una administración más sencilla, posibilidad de implementar más aplicaciones con mejores funcionalidades y en general ser una solución mas barata, ya que es una tecnología que se instala sobre la infraestructura IP existente de manera sencilla, y no de manera inversa en contraste con otras tecnologías.

En cuanto a los protocolos de enrutamiento, tratamos los de mayor importancia para las redes IP-MPLS con el objetivo de encontrar los protocolos óptimos para cada caso, que faciliten la implementación de la infraestructura IP y de MPLS. Nos basamos en aspectos como la estandarización del protocolo, la facilidad de encontrar información sobre él, soporte de MPLS (extensión MBGP de BGP, por ejemplo), etc. También tomamos en cuenta la tendencia de utilización de protocolos que existe actualmente en las redes (OSPF, BGP) y mencionamos sugerencias para su mejor funcionamiento, lugar de implementación y topología recomendada. Concluimos que una parte fundamental en la implementación de cualquier red es la elección de los protocolos de enrutamiento, porque éstos definirán las políticas de diseño, y una buena elección de éstos es parte fundamental de un buen diseño que cumpla con nuestros requerimientos de red.

Revisamos las consideraciones para un diseño satisfactorio de una red IP (funcionales y conceptuales) que se recomienda sean anteriores a la construcción de la misma, pudiendo constatar que existen diversas formas de organizar y delimitar el problema, pero no importando cual de ellas elijamos, debemos de decidirnos por una forma de proceder desde el inicio.

En el análisis de la topología física se revisaron aspectos de posible interconexión de nodos, su organización, escalamiento, políticas a seguir, y una guía de dimensionamiento de enlaces y redundancia. Nos dimos cuenta, y lo transmitimos en

el capítulo, que la Topología Física involucra más que la simple interconexión de equipos.

La Topología Lógica fue planteada considerando los protocolos de enrutamiento, ya que al definir la políticas de diseño se buscó conjuntarlos y generar los mejores criterios para obtener una red que cumpliera con el objetivo de esta tesis. Vimos que es recomendable ajustar al máximo la topología física con la topología lógica, beneficiando principalmente a la escalabilidad de la red, consiguiendo una estrecha relación en el crecimiento de las topologías física y lógica, dada principalmente por la relación entre la ubicación física de los equipos y su conformación en áreas lógicas acordes con las necesidades de la red (como agregar MPLS).

Consideramos que el concluir el trabajo teórico con la propuesta de una implementación de red utilizando las directivas propuestas en el transcurso de la tesis, es una prueba para nosotros mismos, donde encontramos que los criterios descritos son válidos y utilizables, y que aunados a un criterio y necesidad específicos de un Proveedor de Servicios, podrán ser suficientes para obtener una red con las características buscadas.

El proponer el territorio nacional como área de cobertura, nos proporcionó la posibilidad de contar con un territorio extenso de servicio, y una relativa facilidad de ubicar los puntos de mayor tráfico esperado. Pudimos distinguir fácilmente los requerimientos de la red. La interconexión física y lógica se llevó a cabo considerando totalmente las directivas expuestas. Algunos aspectos fueron resaltados más que otros por la aplicabilidad que tienen por las condiciones de la red en específico, como la geografía del lugar, la relación costo-beneficio, la localización del trafico, crecimiento a futuro, conexión con otros ISP´s y el análisis de la viabilidad en el diseño.

Finalmente el diseño no es definitivo ya que forma parte de un continuo proceso de renovación y actualización para llegar a un punto óptimo en el cual la red cumpla con el mayor número de criterios antes enunciados. Es una buena práctica llevar toda la documentación y una bitácora de cambios realizados a la red así como el tener diagramas actualizados y documentar las políticas de la red, donde se puedan mostrar las características de ésta.

El trabajo en general ha proporcionado una visión diferente de las características y aspectos a considerar en el diseño de red, específicamente con el uso de MPLS en una red WAN; ha aportado multitud de conocimientos nuevos y una mejor comprensión de algunos ya conocidos; proporcionó una base para la reflexión sobre la forma de transitar datos actualmente, las propuestas de nuevas maneras de hacerlo (MPLS), así como las necesidades a cubrir en un futuro por las redes WAN de los Proveedores de Servicios

Finamente, podemos decir que el objetivo planteado de proporcionar un documento que especificara el procedimiento y aspectos a considerar para la implementación de una red IP-MPLS escalable, confiable y tolerante a fallos ha sido cubierto, y afortunadamente nos ha dejado la satisfacción de haber podido encontrar y comprender la información de las tecnologías utilizadas actualmente, proponiendo nuestra solución personal, justificada y con la plena confianza que será funcional y útil. Ahora, los criterios utilizados en el trabajo podrán ser aprovechados en cualquier red de datos basada en IP-MPLS, pudiendo ser capaz de soportar aplicaciones altamente demandantes de recursos de red.

TRABAJO FUTURO

Después de revisar los aspectos generales al proponer una guía de diseño para redes IP-MPLS, donde se presenta información valiosa para personas que se dediquen al diseño de redes WAN, podemos identificar áreas en que es factible profundizar el análisis en función de las necesidades y condiciones específicas de la red, utilizando criterios más concretos al contar con una propuesta de red específica y real. Ejemplos de estas consideraciones son:

- El cálculo de parámetros de la red a través de algoritmos matemáticos para su optimización, necesarios en la propuesta y monitoreo de sus servicios, tales como Disponibilidad, Pérdidas, Retardo, Variación del retardo, Cálculo de la mejor ruta, etc, pudiendo ser analizados con la ayuda de un simulador.
- La propuesta de configuraciones de cada uno de los equipos pertenecientes a la red en específico, así como la mención de sus posibles aplicaciones, fallas, método de puesta a punto y complicaciones más probables.
- La especificación de aspectos más concretos de administración, prioridad y control del tráfico en la red.

En cuanto a la tecnología MPLS en específico en la red, posibilita a la misma el incrementar su desempeño en gran medida, debido a que además de incrementar la velocidad de la conmutación de paquetes, posee la capacidad de soportar aplicaciones con mucho potencial, las cuales quedan como campo abierto a su posterior estudio y análisis, cada una de las aplicaciones brevemente explicadas en la sección correspondiente de la tesis, tales como:

- La implementación de Redes Privadas Virtuales (VPN's), las cuales son hoy en día la aplicación más extendida de MPLS, proporcionando un transporte de datos seguro a la información, proporcionando facilidades muy apreciadas.

- La facilidad en la administración de la red al implantar Ingeniería de Tráfico y Calidad de Servicio sobre MPLS, pudiendo controlar y optimizar el funcionamiento de la red en un rango más amplio de opciones, con gran facilidad, sin embargo habrá que evaluar las repercusiones en el desempeño y escalabilidad de la red
- La Posibilidad de transitar cualquier tecnología de transporte de datos sobre la red MPLS al utilizar la funcionalidad agregada AToM (Any Transport over MPLS), lo cual establece una ventaja enorme al no tener la necesidad de contar con infraestructura de cada tecnología para poder transitar datos de ella.
- Indagar el punto óptimo en la utilización de MPLS, en el cual el balance costo / beneficio sea el más ventajoso posible.

El profundizar en alguno de los campos antes mencionados, y algún otro en el que MPLS mejore la red, podrá ser un tema de amplio estudio y desarrollo en la intención de aprovechar al máximo la potencialidad de la red, y las facilidades agregadas con MPLS.

Finalmente, el investigar y evaluar más a fondo todas las posibilidades de protocolos de enrutamiento que podrían utilizarse ya que el tema de protocolos es muy extenso y solo se dieron las bases para un diseño con las características que se plantearon al inicio del trabajo, pero se debe considerar que existen diversas formas de implementación de los protocolos de enrutamiento. Profundizar en las topologías y formas de funcionamiento de lo protocolos BGP, IS-IS y OSPF ampliará nuestro panorama al elegir el adecuado para la red en específico que se va a administrar.

Deberá considerarse el desarrollo de un proceso cíclico de revisión y ajuste, dado que la búsqueda de la optimización del diseño de red normalmente será un proceso iterativo perfectible a través del paso del tiempo, adquisición de experiencia y nuevas perspectivas de desarrollo.

Otro punto a ampliar es el análisis del alcance de negocios, comercialización de la red, estimación de costos, viabilidad del negocio y estudio de mercado entre otros aspectos relevantes es la comercialización de la red, así como la posibilidad de profundizar en la definición del SLA dada su delicadeza, la propuesta y formas de

implementación de políticas de red y rangos permisibles a ofrecer en los parámetros de red al público en función del mercado actual de las telecomunicaciones.

Podrá considerarse el proceso de certificación de la red diseñada, así como la evaluación y reconocimiento del servicio por órganos externos cuya opinión sobre la calidad de los recursos ofrecidos por nuestra red sea irrefutable.

GLOSARIO DE TÉRMINOS

A

Ancho de banda (Bandwith): Es la máxima velocidad a la cual los datos pueden ser enviados o recibidos a través de una conexión.

ATM (*Asynchronous Transfer Mode*): Modo de Transferencia Asíncrona. Tecnología de transporte que puede soportar Circuitos Permanentes o Conmutados

B

Backbone: Capa fundamental en el modelo Jerárquico que provee de una conexión de alta velocidad a sitios geográficamente remotos dentro de una red WAN.

BGP (*Border Gateway Protocol*): Protocolo de enrutamiento entre Sistemas Autónomos.

Broadcast: Es un tipo especial de dirección IP usada para enviar un mensaje a todos los nodos de una red.

C

Calidad de Servicio: QoS (*Quality of Service*). Es la medida del desempeño de un sistema de transmisión que refleja la calidad de trasmisión y disponibilidad de servicio *Ver capítulo I.*

Cliente (usuario): Empresa o particular contratante del servicio de transporte de datos del ISP.

D

Datagrama (paquete): Es la unidad de los mensajes o datos que son transmitidos a través de una red TCP/IP.

Cada uno es una entidad independiente que contiene la dirección de origen y destino de los datos así como el método de transporte en la red.

Dirección IP: Es la dirección de Internet con formato numérico compuesto por 4 bytes, usualmente representada por cuatro números decimales separados por un punto. *Ver capítulo III.*

E

Encabezado (*header*): Porción de un paquete, precediendo los datos, que contiene las direcciones fuente y destino y campos de detección de errores.

Enrutador (*Router*): Es un dispositivo que permite la conexión de dos redes distintas transmitiendo sus paquetes por la mejor ruta.

F

Frame Relay: Tecnología de conmutación rápida de frames ubicada en la Capa 2 OSI.

FTP (*File Transfer Protocol*): Protocolo de transferencia de archivos. Es un servicio de Internet para transferir archivos entre una Terminal y otra.

***Firewall* (muro de fuego):** Programa o dispositivo físico usado para actuar como barrera protectora entre una terminal y la red a la cual ésta se conecta.

G

***Gateway* (puerta de enlace):** Es una terminal que permite la conexión de dos tipos diferentes de redes y transmite paquetes de una red a otra.

I

IETF (*Internet Engineers Task Force*): Fuerza de Trabajo de Ingenieros de Internet.

Ingeniería de Tráfico: TE (*Traffic Engineering*). Aplicación para el control del envío y transmisión de paquetes en la red y administración de sus recursos.

Internet: Red mundial que abarca miles de redes con varios miles de millones de sitios con información de diverso tipo, comprende distintos tipos de servicios y elementos, en una lista muy amplia y variada.

IS-IS (*Intermediate System - Intermediate System*): Protocolo de enrutamiento que permite calcular las rutas una vez y aplicaras para todos los protocolos utilizados.

ISO (*International Organization for Standarization*): Organización internacional que establece normalizaciones en muchos campos de la técnica. Entre otras cosas, coordina los principales estándares de redes que se usan hoy en día.

IP (*Internet Protocol*): Protocolo de Internet. Componente de la familia de protocolos TCP/IP encargado de transmitir los paquetes por la red.

L

LAN (*Local Area Network*): Red de área local. Es aquella red que está situada en un mismo espacio físico.

LSP (*Label Switched Path*): Camino Conmutado de Etiquetas. Trayecto virtual creado a partir de etiquetas.

M

MBGP (*Multiprotocol BGP*): Adición al protocolo de enrutamiento BGP que emplea extensiones multiprotocolo y atributos de comunidades.

Multimedia: Nombre dado a las aplicaciones que conjuntan en su funcionamiento Voz, Video y Datos.

Multicast: Es un grupo especial de direcciones IP que comienzan con la secuencia 255. Si la dirección de multicast es especificada en la asignación de direcciones de un paquete, todos los nodos que tienen esa dirección recibirán ese paquete.

N

Nodo: Punto de confluencia de una red, como puede ser un dispositivo de conmutación dentro de una red local o una terminal conectada a su red local.

O

OSI (*Open Systems Interconection*): Interconexión de Sistemas Abiertos. Modelo de referencia para facilitar la conectividad entre equipos *Ver capitulo II.*

OSPF (*Open Shortest Path First*): Protocolo de enrutamiento que propone el uso de rutas más cortas y accesibles.

P

PDU (*Protocol Data Unit*): Unidad de Datos de Protocolo.

Protocolo : Es un conjunto de reglas aceptadas para un particular tipo de intercambio de comunicaciones. Los dispositivos que intenten transferir datos entre sí deberán utilizar el mismo tipo de protocolo para que la comunicación sea posible y la transferencia sea realizada correctamente.

Proveedor de Servicio (*Internet Service Provider, ISP*): Compañía encargada de ofrecer diversos servicios de transporte de datos, entre ellos la conexión a Internet.

Puerto

El puerto es un dispositivo que se define por programación y que no necesariamente debe tener una asignación física en el equipo. A cada aplicación se le asigna un número de puerto según el tipo de dato que será transmitido.

R

Red: Una red se compone de dos o más dispositivos unidos a través de un medio físico y vinculados mediante programas y procedimientos adecuados, que les permite compartir datos y/o recursos entre sí.

S

Sistema Autónomo: AS (*Autonomous System*). Conjunto de redes bajo la misma administración y políticas de servicio.

SLA (*Service Level Agreeement*): Acuerdo en el Nivel de Servicio. Son los parámetros que el Proveedor se compromete a ofrecer al cliente en la contratación del servicio.

T

Tabla de Enrutamiento: Es una Base de Datos donde se encuentran todas las rutas conectadas y aprendidas por un enrutador.

TCP (*Transmission Control Protocol*): Protocolo de Control de Transmisión. El mayor protocolo de transporte de datos en red y en Internet, asegura una distribución confiable ya que retransmite los datos si fuera necesario.

U

UDP (*User Datagram Protocol*): Protocolo de Datagrama de Usuario. Es un protocolo que provee herramientas simples de bajo nivel para la transmisión y recepción de paquetes de red directamente a las aplicaciones.

V

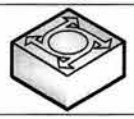
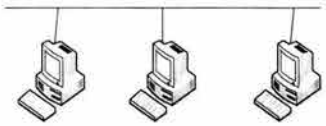
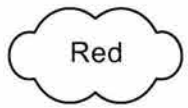
VPN (*Virtual Private Network*): Red Privada Virtual. Es una red en la que la conectividad ente múltiples lugares se realiza a través de una

infraestructura compartida, con las mismas políticas de acceso y seguridad que en la red privada.

W

WAN (*Wide Area Network*): Red de Área Amplia. Una red extendida que ofrece conectividad entre dispositivos y/o redes locales ubicada en áreas geográficas distintas y dispersas.

GLOSARIO DE FIGURAS

Terminal	
Enrutador	
Enrutador ATM	
Enrutador FrameRelay	
Servidor de Acceso	
LAN	
Enlace WAN	
Red	

BIBLIOGRAFÍA

CAPÍTULO I Requisitos de la red

Cisco AVVID Network Infrastructure Quality of Service Overview, Overview, Cisco Systems Inc., PDF, pp. 3, CISCO, www.cisco.com

Cisco AVVID Network Infrastructure Enterprise Quality of Service Design, Solutions Reference Network Design, August, 2002, PDF, pp. 208, CISCO, www.cisco.com

Introduction to Network Management, Networkers 2003, PDF, pp 89, CISCO, www.cisco.com

Introduction to Performance Management, Networkers 2003, PDF, pp 125, CISCO, www.cisco.com

Deploying Quality of Service for Converged Networks, Networkers 2003, PDF, pp 107, CISCO, www.cisco.com

Internet Service Provider Security Best practices, Networkers 2003, PDF, pp 94, CISCO, www.cisco.com

Designing Voice-Enabled IPSec VPNs, Networkers 2003, PDF, pp 133, CISCO, www.cisco.com

Designing Service Provider Core Networks to Deliver Real-Time Services, PDF, pp. 16, CISCO, www.cisco.com

Cisco IOS MPLS Quality of Service, PDF, pp. 5, CISCO, www.cisco.com

Cisco - When Is CEF Required for Quality of Service?, PDF, pp. 5, CISCO, www.cisco.com

Networking. Enterprise IP LAN/WAN Design, Ya Wen, Version 1.1, TAOS, PDF, pp 26, www.taos.com

Cisco – When Is CEF Required for Quality of Service?, PDF, pp.5, CISCO

Historia de las Redes, http://www.geocities.com/Eureka/Plaza/2131/redes.html

CAPÍTULO II Conceptos Básicos sobre red

Redes y Comunicaciones I, Interconectividad, Universidad ICESI., PDF, pp. 58, http://www.iespana.es/canalhanoi/internet/transdatos.htm

Redes Básicas, www.OCIOSO.net

Wide Area Networks (WANs)
http://www.delmar.edu/Courses/ITSC1391/Sem4/2WANs.htm

CAPÍTULO III IP, TCP y UDP

Protocolo IP, www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/**ip**.htm

Protocolo TCP-IP, www.protocols.com/pbook/tcpip.htm

Protocolo UDP, www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cnfc/cnfc_por_simw.asp

Protocolos UDP TCP-IP, compnetworking.about.com/cs/protocols**tcpudp**

CAPÍTULO IV Descripción de Tecnologías WAN

ATM, Modo de Transferencia Asíncrona, Ivan Dario Cruz Prada, http://www.monografias.com/trabajos/atm/atm.shtml

Frame Relay in Public Networks. M. Irfan Ali. IEEE - Communications Magazine - March 1992.

ATM Internetworking. Anthony Alles. Cisco Systems Inc, Marzo 1995.

Revisión y Clasificación de Protocolos para Redes de Tecnología ATM, José Luis González-Sánchez, Universidad de Extremadura, Dpto. de Informática, Área Arquitectura y Tecnología de Computadores, Jordi Domingo-Pascual, UPC, Dept. d'Arquitectura de Computadors, http://www.rediris.es/rediris/boletin/46-47/ponencia10.html

ATM, Tecnología y Aplicaciones,
http://www.reuna.cl/central_apunte/apuntes/tecno4.html

SVCs, ATM and Frame Relay,
http://cisco.com/univercd/cc/td/doc/product/wanbu/8_5/switch/sys/sysatsvc.htm

ATM , http://www.tectimes.com/cda/glosario.asp?texto=A&codpalabra=572TEMA

Tecnología de las redes, http://www.blackbox.com.mx/page.asp?cc=MX&pc=7&tc=10&bc=techoverviews

Libro tarifarlo de Miditel, Sección. Servicio Frame Relay, (Vigencia 26 de junio de 1998), http://cofetel.gob.mx/html/4_tar/mid/miditel3.html

Frame Relay: Sistema de altas prestaciones., http://www.interec.com/Frame_Relay/

Tutorial:Frame Relay, ATM, VLAn, http://www.consulintel.es/Html/Tutoriales/articulos.htm

Guías Didácticas Ethernet, http://www.consulintel.es/Html/Tutoriales/Lantronix/tutor_lantr.htm

Frame Relay - Enlaces de datos de alta capacidad., http://www.technidata.com.mx/servicios/att/framerelay/

Red ATM. Conceptos básicos, PDF, pp. 10

Frame Relay, Marta Poza Poza, PPT, Presenatcion

Redes Frame Relay y ATM , Rogelio Montañana, Departamento de Informática, Universidad de Valencia, PPT, http://www.uv.es/~montanan/, Presentcion

ATM – FR, Instituto de Investigación e Innovación Tecnológica, Carlos Usbeck Wandamberg, Complementos electronicos s.a., Ecuador, PDF, pp. 17

Advanced Topics in MPLS-TE Deployment, Withe paper, Cisco systems inc., PDF, pp. 33, CISCO, www.cisco.com

CISCO IP/MPLS Edge Routers, Networkers 2003, PDF, pp 48, CISCO, www.cisco.com

Introduction to MPLS, Networkers 2003, PDF, pp 93, CISCO, www.cisco.com

Deploying MPLS-VPN, Networkers 2003, PDF, pp 93, CISCO, www.cisco.com

Troubleshooting MPLS VPN Networks, Networkers 2003, PDF, pp 110, CISCO, www.cisco.com

Configuring Basic MPLS Using OSPF, PDF, pp. 8, CISCO, www.cisco.com

Deploying Guaranteed-Bandwidth Services with MPLS, With Paper, PDF, pp. 31, CISCO, www.cisco.com

How Virtual Private Networks Work, PDF, pp. 10, CISCO, www.cisco.com

Multiprotocol Label Switching Troubleshooting, PDF, pp.7, CISCO, www.cisco.com

Advanced Topics in MPLS-TE Deployment, White paper, PDF, pp. 33, CISCO, www.cisco.com

Cisco Express Forwarding Overview, PDF, pp. 6, CISCO, www.cisco.com

Security of the MPLS Architecture, White paper, PDF, pp. 18, CISCO, www.cisco.com

When Is CEF Required for Quality of Service?, PDF, pp. 5, CISCO, www.cisco.com

RFC3037, LDP Applicability, Network Working Group , B. Thomas, Cisco Systems, Inc., E. Gray, Zaffire, Inc., Category: Informational , January 2001

RFC3346, Applicability Statement for Traffic Engineering with MPLS, Network Working Group ,, Category: Informational, J. Boyle, PD Nets, V. Gill, AOL Time , arner, Inc., A. Hannan, RoutingLoop, D. Cooper, Global Crossing, D. Awduche, Movaz Networks, B. Christian, Worldcom, W.S. Lai, AT&T, August 2002

MPLS, , Diaz, SI Polo, Lopez, Piñeiro, Vargas, http://suma.ldc.usb.ve/~G5/mpls/index.html

MPLS: Convergencia entre el nivel de transmisión y el nivel de enrutamiento, Ana González., PDF, pp. 9, Revista Natwork

Redes Privadas Virtuales y MPLS, Tomas P. de Miguel, DIT Univ. Poltécnica Madrid

EoMPLS: ¿El despliegue definitivo de la redes MAN de Banda Ancha?, , Operadores, Revista Comunicaciones World, Nov 2001, PDF, pp. 2

MPLS: Una arquitectura de backbone para la Internet del siglo XXI (MPLS: A backbone architecture for the Internet of the 21st Century)}, José Barberá, http://www.rediris.es/rediris/boletin/index.html

Articulo de MPLS http://www.aniret.org.mx/pdf/articulos/mpls.pdf

Frame Relay http://www.udabol.edu.bo/biblioteca/ing.telecomunicaciones/BIBLIOTECA%20ing%20telecom/Electronica/tecnologia%20frame%20relay/relay-1.pdf

Restablecimiento de servicio MPLS con la calidad y fiabilidad que se exigen a una compañía operadora, http://www.ciena.com/

Multiprotocol Label Switching Overview, Cisco IOS Switching Services Configuration Guide, PDF, pp. 62, , CISCO

Cisco - MPLS FAQ For Beginners, PDF, 6, CISCO

Cisco MPLS Tunnel Builder Pro, Brochure, PDF, pp. 4, CISCO

Advanced Topics in MPLS-TE Deployment, White Paper, PDF, pp. 33, CISCO

Positioning MPLS, White Paper, PDF, pp. 4, CISCO

Security of the MPLS Architecture, white paper, PDF, pp. 18, CISCO

Configuring Basic MPLS Using OSPF, PDF, pp. 8, CISCO

Cisco - When Is CEF Required for Quality of Service?, PDF, pp.5, CISCO

LDP based VPN Traffic classification, http://www.ietf.org/internet-drafts/draft-vijay-mpls-ldp-vpn-class-00.txt, white paper

Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP), http://www.ietf.org/internet-drafts/draft-ietf-mpls-ldp-mib-13.txt, withe paper

Refecrencia de comandos MPLS de CISCO, http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_command_reference_chapter09186a008010a795.html

MPLS and VPN Architectures, Pepelnjak, Guichard,Cisco Systems, EUA, 2001

CAPÍTULO V Protocolos de enrutamiento

Multicast for MPLS-VPNs, Networkers 2003, Thomas Kramer, PDF, pp 113, CISCO, www.cisco.com

What Is Administrative Distance?, PDF, pp 5, CISCO, www.cisco.com

Configuring Basic MPLS Using OSPF, PDF, pp. 8, CISCO, www.cisco.com

White Paper: EIGRP, With paper, PDF, pp. 57, CISCO, www.cisco.com

Specifying a Next Hop IP Address for Static Routes, PDF, pp. 11, CISCO, www.cisco.com

Diez razones para migrar a MPLS

http://www.ifxnetworks.com/document/10razones_mpls.pdf

Curso de MPLS

http://www.fi.upm.es/~jgarcia/Curso_MPLS/capitulo6.html

Protocolo BGP

http://iie.fing.edu.uy/ense/asign/redes2/material/096BGP%20(parte%202).pdf

Route Selection in Cisco Routers, PDF, pp. 9, CISCO, www.cisco.com

Enrutadores BGP, http://merry.netsys.more.net/lg/index.cgi

Interior Gateway Routing Protocol (IGRP),

http://www.delmar.edu/Courses/ITSC1391/Sem3/5IGRP.htm

Configuring Basic MPLS Using OSPF, PDF, pp. 8, CISCO

MPLS y VPNs

http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdf

Tutorial de MPLS

http://www.iec.org/online/tutorials/mpls/topic03.html?Next.x=35&Next.y=24

Archivo MPLS , http://www.mpls.jp/2002/pdf/OAM_Arch.pdf

CAPÍTULO VI Pasos para el diseño de una red

Cisco AVVID Network Infrastructure Enterprise Quality of Service Design, Solutions Reference Network Design, August, 2002, PDF, pp. 208, CISCO, www.cisco.com

Deploying Metro Ethernet: Architecture and Services, Networkers 2003, PDF, pp 115, CISCO, www.cisco.com

Campus Architectures, Networkers 2003, PDF, pp 95, CISCO, www.cisco.com

Design Principles for Secure Network Edges, Networkers 2003, PDF, pp 93, CISCO, www.cisco.com

Internet Service Provider Security Best practices, Networkers 2003, PDF, pp 94, CISCO, www.cisco.com

deploying Complex and Large Scale IPsec, Networkers 2003, PDF, pp 161, CISCO, www.cisco.com

Diseño de Redes Wan

http://www.delmar.edu/Courses/ITSC1391/Sem4/3WANdesign.htm

Constitución de redes WAN

http://www.monografias.com/trabajos5/redwan/redwan.shtml#constitucion

Designing Voide-Enabled IPSec VPNs, Networkers 2003, PDF, pp 133, CISCO, www.cisco.com

Deploying Guaranteed-Bandwidth Services with MPLS, With Paper, PDF, pp. 31, CISCO, www.cisco.com

Designing Large-Scale IP Internetworks, PDF, Pp 64, CISCO, www.cisco.com

Designing Internetworks for Multimedia, PDF, pp. 48, CISCO, www.cisco.com

Designing Packet Service Internetworks, PDF, pp. 18, CISCO, www.cisco.com

Designing Service Provider Core Networks to Deliver Real-Time Services, PDF, pp. 16, CISCO, www.cisco.com

Designing Switched LAN Internetworks, PDF, pp. 30, CISCO, www.cisco.com

Multi-homing—Connecting to Two ISPs, White paper, Vincent. C. Jones, PDF, pp. 4, CISCO, www.cisco.com

Internetworking Design Basics, PDF, pp. 42, CISCO, www.cisco.com

Security of the MPLS Architecture, White paper, PDF, pp. 18, CISCO, www.cisco.com

Cisco Networking Essentials for Educational Institutions, Educational guide, PDF, pp. 36, CISCO, www.cisco.com

Designing Packet Service Internetworks, PDF, pp. 18, CISCO, www.cisco.com

Internetworking Design Basics, PDF, pp. 42, CISCO, www.cisco.com

TDC 562: Computer Network Design & Analysis (Internet Engineering), Network Design Tutirual, Ehab S. Al-Shaer, School of Computer Sciences & Telecommunication, DePaul University, Chicago IL, pdF, pp 30, www.com

Hierarchical Cache Consistency in WAN Estended Abstract, Jian Yin, Lorenzo Alvisi, Mike Dahlin, Calvin Lin, Department of Computer Sciences, University of Texas at Austin, PDF, pp-12, www.com

Hierarchical Network Management, Manfred R. Singl, Georg Trausmuth, PDF, pp. 10, www.com

Building Cabling, Wide Area Networking Options for REAL Wide Area Networking Considerations for Library Automation Systems, Research and Innovation, Quality of Service Customer Edge Devices, Documenting Your Network, http://www.more.net/technical/netserv/

WAN Design, http://www.delmar.edu/Courses/ITSC1391/Sem4/3WANdesign.htm

Diseño De Redes De Distribucion Empleando Heuristica Constructiva, Miguel Arias A., Víctor Parada, PDF, pp. 4, Articulo

Metodología de Diseño de Redes, Instituto de Investigación e Innovación Tecnológica, PDF, pp. 53

Estructura y Diseño de redes, Sr. Moumoulidis, OTE, ITU, PDF, pp.14, Articulo http://www.iespana.es/canalhanoi/internet/transdatos.htm

CAPÍTULO VII Diseño de Estudio Propuesto

Cisco AVVID Network Infrastructure Enterprise Quality of Service Design, Solutions Reference Network Design, August, 2002, PDF, pp. 208, CISCO, www.cisco.com

Introduction to Network Management, Networkers 2003, PDF, pp 89, CISCO, www.cisco.com

Introduction to Performance Management, Networkers 2003, PDF, pp 125, CISCO, www.cisco.com

Deploying Metro Ethernet: Architecture and Services, Networkers 2003, PDF, pp 115, CISCO, www.cisco.com

Deploying MPLS-VPN, Networkers 2003, PDF, pp 93, CISCO, www.cisco.com

Design Principles for Secure Network Edges, Networkers 2003, PDF, pp 93, CISCO, www.cisco.com

Internet Service Provider Security Best practices, Networkers 2003, PDF, pp 94, CISCO, www.cisco.com

Deploying Guaranteed-Bandwidth Services with MPLS, With Paper, PDF, pp. 31, CISCO, www.cisco.com

Designing Large-Scale IP Internetworks, PDF, Pp 64, CISCO, www.cisco.com

Designing Internetworks for Multimedia, PDF, pp. 48, CISCO, www.cisco.com

Designing Packet Service Internetworks, PDF, pp. 18, CISCO, www.cisco.com

How Virtual Private Networks Work, PDF, pp. 10, CISCO, www.cisco.com

Multi-homing—Connecting to Two ISPs, White paper, Vincent. C. Jones, PDF, pp. 4, CISCO, www.cisco.com

Advanced Topics in MPLS-TE Deployment, White paper, PDF, pp. 33, CISCO

Internetworking Design Basics, PDF, pp. 42, CISCO, www.cisco.com

Cisco Networking Essentials for Educational Institutions, Educational guide, PDF, pp. 36, CISCO, www.cisco.com

Designing Packet Service Internetworks, PDF, pp. 18, CISCO, www.cisco.com

Internetworking Design Basics, PDF, pp. 42, CISCO, www.cisco.com

Metodología de Diseño de Redes, Instituto de Investigación e Innovación Tecnológica, PDF, pp. 53

Release Notes for Cisco IOS Release 12.0(14)ST2, , PDF, July 2 2001, PDF, pp. 56, CISCO, www.cisco.com

CAPÍTULO VIII Documentación de la Red

Building Cabling, Wide Area Networking Options for REAL Wide Area Networking Considerations for Library Automation Systems, Research and Innovation, Quality of Service Customer Edge Devices, Documenting Your Network, http://www.more.net/technical/netserv/

Diseño Físico de Redes, http://cursos.itam.mx/jincera/DisRed/disfis.pdf

Diseño y documentación, http://www.cec.uchile.cl/~jsandova/el64e/clases/clase23-24.pdf

Datos, Voz y Multimedia,
http://www.microsoft.com/spanish/msdn/articulos/archivo/180501/voices/data03082001.asp

Red MPLS , http://red-mpls.udg.es/presentaciones/rpv_mpls.pdf