Universidad del Azuay

Facultad de Ciencia y Tecnología

Escuela de Ingeniería Electrónica

“Ventajas de la utilización de MultiProtocol Label Switching (MPLS) en un esquema de arquitectura de red convencional”

Trabajo de graduación previo a la obtención del Título de Ingeniera Electrónica

AUTOR:

Alexandra Elizabeth Bermeo Arpi

DIRECTOR:

Hugo Marcelo Torres Salamea

Cuenca – Ecuador

2012

DEDICATORIA

La presente monografía está dedicada a:

Mis padres, Iván y Nancy, quienes me han dado su amor y confianza siempre, son mi fuerza, corazón y el mejor ejemplo de vida.

A mis hermanas, Benny y Anita, quienes han estado conmigo en todo momento; apoyándome, cuidándome y dándome su cariño incondicional. A seguir soñando, riendo y viviendo!

AGRADECIMIENTOS

Primero quiero agradecer a Dios, por la vida.

A mis abuelos, tíos y primos; lo más importante en la vida es la familia, y agradezco por tenerles a cada uno de ustedes, son mi motivación, mi alegría y mi más grande tesoro.

A mis queridos amigos Marcela Gómez, Verónica Bustamante, Jezabel Huanca, Patricio González, Esteban Mora, Mateo Encalada, Sebastián Fernández y Omar Alvarado; por su amistad y cariño de siempre, son lo más preciado que he conseguido en mis años universitarios, gracias por haber compartido momentos inolvidables que estarán conmigo por siempre.

Al Ing. Marcelo García, gracias por su apoyo, asistencia y consejos.

Al Banco del Austro S.A. y a Sergio Bermeo Calle, por su apertura y colaboración para la realización de la parte práctica de este documento.

A los profesores y personal de la Facultad de Ciencia y Tecnología, mi hogar los pasados seis años, gracias por su confianza y enseñanzas.

VENTAJAS DE LA UTILIZACION DE MULTIPROTOCOL LABEL SWITCHING (MPLS) EN UN ESQUEMA DE ARQUITECTURA DE RED CONVENCIONAL

RESUMEN

Para determinar las ventajas de aplicar la tecnología Multi Protocol Label Switching (MPLS) sobre un esquema de arquitectura de red convencional, como una red Frame Relay, ATM o Ethernet se realizó un estudio de tráfico, utilizando el analizador de protocolos Wireshark, en una red existente para deducir los servicios que presta y posteriormente determinar conceptos de Ingeniería de Tráfico. Finalmente, al realizar una comparación entre las arquitecturas convencionales con MPLS se determinó que la segunda tecnología es la más conveniente para una red, debido a las ventajas que presenta, tanto para el proveedor como para el cliente.

Palabras Clave: MPLS, Wireshark, Ingeniería de tráfico, Ethernet, ventajas, Frame Relay, ATM.

Alexandra Berrneo A.
Estudiante

Ing. Hugo Torres Salamea
Director

ADVANTAGES OF THE USE OF MULTIPROTOCOL LABEL SWITCHING (MPLS) IN A CONVENTIONAL SCHEME OF NETWORK ARCHITECTURE

ABSTRACT

In order to determine the advantages of applying Multi Protocol Label Switching (MPLS) into a conventional scheme of telecommunications architecture network, such as Frame Relay, ATM or Ethernet was performed a traffic study, using the protocol analyzer Wireshark in a existing network to deduce what type of services are used and then establish Traffic Engineering concepts. At last, after making a comparison between the conventional architecture and MPLS it was determined that the second technology is the most convenient for a network, due to the advantages that has shown, it will present the best performance for the carrier and the client.

Key Words: MPLS, Wireshark, Traffic Engineering, Ethernet, advantages, Frame Relay, ATM.

Alexandra Bermeo A.
Estudiante

Ing. Hugo Torres Salamea
Director

RESUMEN

Para determinar las ventajas de aplicar la tecnología Multi Protocol Label Switching (MPLS) sobre un esquema de arquitectura de red convencional, como una red Frame Relay, ATM o Ethernet se realizó un estudio de tráfico, utilizando el analizador de protocolos Wireshark, en una red existente para deducir los servicios que presta y posteriormente determinar conceptos de Ingeniería de Tráfico. Finalmente, al realizar una comparación entre las arquitecturas convencionales con MPLS se determinó que la segunda tecnología es la más conveniente para una red, debido a las ventajas que presenta, tanto para el proveedor como para el cliente.

Palabras Clave: MPLS, Wireshark, Ingeniería de tráfico, Ethernet, ventajas, Frame Relay, ATM.

ABSTRACT

In order to determine the advantages of applying Multi Protocol Label Switching (MPLS) into a conventional scheme of telecommunications architecture network, such as Frame Relay, ATM or Ethernet was performed a traffic study, using the protocol analyzer Wireshark in an existing network to deduce what type of services are used and then establish Traffic Engineering concepts. At last, after making a comparison between the conventional architecture and MPLS it was determined that the second technology is the most convenient for a network, due to the advantages that has shown, it will present the best performance for the carrier and the client.

Key Words: MPLS, Wireshark, Traffic Engineering, Ethernet, advantages, Frame Relay, ATM.

INDICE DE CONTENIDOS

CAPITULO 3 ESTUDIO DE TRAFICO

CAPITULO 4: VENTAJAS DE MPLS SOBRE UN ESQUEMA DE ARQUITECTURA DE RED CONVENCIONAL

INDICE DE FIGURAS

INDICE DE TABLAS

Bermeo Arpi Alexandra Elizabeth

Trabajo de graduación

Torres Salamea, Hugo Marcelo, Ing.

Enero del 2012

Ventajas de la utilización de MultiProtocol Label Switching (MPLS) en un esquema de arquitectura de red convencional

Introducción

El objetivo del presente trabajo de grado es mostrar las ventajas que cualquier red obtendrían al introducir la técnica MPLS en su entorno. Las técnicas de encaminamiento y transmisión usadas hasta el momento, tales como Frame Relay, ATM y Ethernet tienen todas ellas grandes ventajas, pero al mismo tiempo falencias que han sido descritas en este documento. La mayoría de estos problemas, principalmente en las dos primeras técnicas nombradas, se deben a que las rutas de transmisión de datos han estado siendo elegidas basándose en el "mejor camino", es decir, mediante parámetros que no son los adecuados para esta elección, tales como métrica o número de saltos.

Éste es un problema que se resolvería gracias a la técnica MPLS y su sistema de etiquetado de paquetes. Además esta técnica ofrece gran escalabilidad, altos niveles de seguridad, tanto para la red como para las aplicaciones que se ejecuten en la misma. Esto se debe a la capacidad de esta tecnología para transportar grandes volúmenes de datos con tiempos de retraso mínimos y la habilidad para transmitir diferentes protocolos.

CAPITULO I

CONCEPTOS PRINCIPALES

El presente capítulo presenta conceptos teóricos necesarios para el desarrollo de los capítulos posteriores del presente trabajo. Trata sobre el modelo de referencia de siete capas OSI, presentando una descripción de cada una de ellas. Luego se hace una introducción a la técnica Multi Protocol Label Switching (MPLS), sus elementos, componentes y funcionamiento, además las aplicaciones y servicios que ofrece la misma.

1.1 Modelo OSI

El modelo OSI es el modelo principal de referencia para las comunicaciones hoy en día. Una de las principales ventajas que presenta este modelo es la facilidad para comunicarse entre cualquier dispositivo, sin depender de marcas o modelos. Al presentar una estructura de capas, permite visualizar sin dificultad el proceso de comunicación de red y facilita el aprendizaje de este proceso.

El modelo OSI está dividido en siete capas, de manera que “el problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo” (Cisco Networking Academy, 2003).

Figura 1.1. Modelo OSI
Fuente: Grafico Capas Modelo OSI: http://www.pchardware.org/redes/redes_osi.php

Las capas del modelo OSI están numeradas de abajo hacia arriba, de manera que la parte física de la comunicación (cables, dispositivos, etc) corresponde a la capa 1; y asi el proceso se detalla paso a paso hasta llegar a la capa 7, que es la capa donde se tienen los programas y aplicaciones.

1. Capa Física: Los datos a transmitirse en una comunicación dentro de una red, sean estos voz, audio, video, gráficos, textos, etc., viajan a través de un cable, en forma de pulsos eléctricos si se trata de un cable, o como pulsos de luz si se trata de fibra óptica. La función de esta primera capa del modelo OSI es transmitir estos pulsos, definiendo las especificaciones eléctricas necesarias para mantener o desactivar el enlace entre dos usuarios finales. Se refiere a la parte física de una comunicación.

2. Capa de Enlace: Es la capa del modelo OSI que facilita el acceso a los medios de la red permitiendo que la información transmitida encuentre su destino. Esta capa se encarga del direccionamiento físico, mediante la dirección única MAC, misma que es propia de cada dispositivo y que permite que varios dispositivos compartan el mismo medio y aun así, puedan ser identificados entre sí. Otra función de esta capa es la administración de la notificación de errores encontrados en la transmisión de datos, la topología de red y el control de flujo.

3. Capa de Red: El objetivo de funcionamiento de la capa 3 es encontrar el mejor camino para direccionar los datos dentro de la red. Los dispositivos a través de los cuales están viajando los datos utilizan el esquema de direccionamiento de esta capa para determinar el destino, a medida que estos se desplazan por la red. La red identifica los paquetes por medio de la dirección IP.

4. Capa de Transporte: Entre otras funciones, la capa número 4, regula y mantiene el flujo de datos desde el origen hasta el destino en una forma confiable y económica, aun si estos dos extremos no están conectados de manera directa o física. Es la capa encargada del transporte de datos sin errores.

5. Capa de Sesión: Esta capa del modelo OSI está encargada de controlar el dialogo entre las aplicaciones de origen y destino, es decir, determina quien “habla” (o transmite) y en qué momento lo hace; también puede agrupar los datos de manera que define grupos y sirve como punto de comprobación en caso de que se de algún error en la comunicación. Además administra las peticiones y respuestas de servicio que se puedan dar en la comunicación entre varios dispositivos.

6. Capa de Presentación: Generalmente, esta capa es un protocolo de transferencia de información, que se encarga de la representación de la información, y permite la comunicación entre aplicaciones de diferentes sistemas informáticos. Los datos transmitidos pueden tener diversas representaciones de caracteres, números, sonidos o imágenes, el objetivo de esta capa es que estos datos puedan ser reconocidos por el dispositivo de destino.

7. Capa de Aplicación: Es la última capa dentro del modelo de referencia OSI. Es la capa más cercana al usuario final, contiene los programas que éste ocupa, tales como correo electrónico, Internet y Multimedia. En esta capa se transportan los paquetes de datos antes de llegar al destino.

1.2 MPLS (Multi Protocol Label Swtiching)

1.2.1 Conceptos Generales

Multiprotocol Label Switching (MPLS, Multiprotocolo de Conmutación de Etiquetas) es un nuevo protocolo de red, muy popular en las grandes empresas de los países desarrollados; pero que poco a poco está ingresando en los ambientes de medianas y grandes empresas en todos los países del mundo, ya que cada vez se necesita de un ancho de banda más grande y la convergencia de voz, datos y video. Esto se debe a que esta popular tecnología de red presenta muchas más ventajas que sus predecesores; se le considera la tecnología que está desplazando a IP sobre ATM, hasta ahora, una de las arquitecturas preferidas por las empresas proveedoras de servicios.

Uno de los mayores problemas que se tenía con IP sobre ATM era las limitaciones al momento de gestionar dos redes totalmente diferentes; este es un problema ya solucionado en MPLS, ya que integra, sin discontinuidades o errores las capas de transporte y red, las funciones de control de ruteo con las funciones de la capa 2, que se encarga de la conmutación de los datos con rapidez y sencillez; esta combinación se logra debido a que MPLS utiliza etiquetas que se les adhiere a los paquetes que se van transmitir a través de la red.

1.2.2 Arquitectura

Para entender en su totalidad el concepto y funcionamiento de MPLS, se debe empezar por entender dos ideas básicas derivadas de su nombre:

- Tal como lo indica “Multiprotocol” o Multiprotocolo en español, esta tecnología está diseñada para trabajar con varios protocolos. Aunque en sus inicios fue diseñada únicamente para IPv4, ahora se puede transportar tanto tráfico IPv6 o cualquier flujo proveniente de la capa 2 del modelo OSI.

- La segunda parte “Label Switching” se refiere a que los paquetes que se van a transmitir ya no son paquetes ni IPv4, IPv6 o flujo de datos de capa 2 cuando están siendo transmitidos, únicamente son paquetes con una etiqueta que los identifica, esta es la parte crucial para MPLS, ya que realiza la conmutación de los paquetes basándose en la información que tiene en esta etiqueta.

1.2.3 Etiquetas

Las etiquetas MPLS se estructuran de tal manera que se ubica en el medio de las capas 2 y 3, entre las cabeceras de las capas de red y de enlace de datos, como se muestra a continuación.

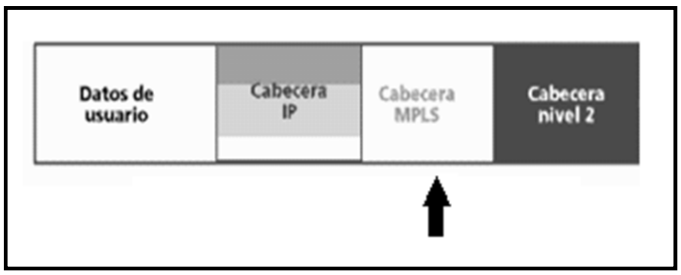

Figura 1.2 Ubicación de la etiqueta MPLS
Fuente: MPLS-FDDI, Patiño, Camilo, http://sx-de-tx.wikispaces.com/MPLS-FDDI

Una etiqueta MPLS tiene un campo de 32 bits, divididos en 4 partes:

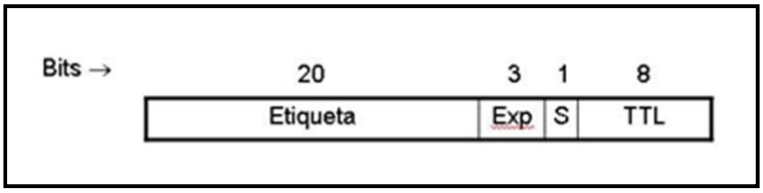

Figura 1.3 Etiqueta MPLS
Fuente: Vidal, Omar; Administración de redes http://omar1985.wordpress.com/2008/10/18/mpls/

- Etiqueta: tiene una longitud de 20 bits, es la etiqueta propiamente dicha, su objetvivo es identificar una FEC (Clase Equivalente de Enrutamiento)

- Exp: estos 3 bits son los llamados “bits para uso experimental”, se utilizan exclusivamente para QoS (calidad del servicio)
- S: Stack, es la primera etiqueta introducida, este bit sirve para jerarquizar las etiquetas el momento de ponerlas en la pila.

- TTL: con una longitud de 8 bits, es un contador, y sirve para evitar que un paquete se quede en un loop. Con cada salto que da el paquete el TTL disminuye en 1, al momento de llegar a 0, el paquete es descartado. Representa el tiempo de vida del paquete.

1.2.4 Elementos de MPLS

1.2.4.1 Router de conmutación de etiquetas (LSR)

Un LSR (Label Switching Router) es un router ubicado en el núcleo de la red MPLS que es capaz de entender las etiquetas de MPLS, de transmitir y recibir paquetes de datos etiquetados, establecer los circuitos entre los extremos de la red y conmutar el tráfico en el circuito establecido. Existen tres clases de LSR:

- LSR de Ingreso: recibe los paquetes que todavía no están etiquetados, pone la etiqueta y los transmite a un enlace de datos.

- LSR de Salida: recibe los paquetes etiquetados, retira la etiqueta y los envía al enlace de datos. Estos dos tipos de LSR son los LSR de borde, también conocidos como LER (Label Edge Router).

- LSR Intermedio: reciben los paquetes etiquetados, conmutan el paquete y lo envían al enlace de datos correcto.

1.2.4.2 Clase equivalente de enrutamiento (FEC)

Una FEC (Forwarding Equivalent Class) es un grupo o flujo de paquetes de capa 3 que comparten ciertas características de manera que son transmitidos dentro de un mismo camino y son tratados de la misma manera al momento de la transmisión. Todos los paquetes pertenecientes a una misma FEC tiene la misma etiqueta, no así a la inversa, debido a que los valores de EXP pueden variar. El router que decide a donde pertenece cada paquete es el LSR de Ingreso.

1.2.4.3 Rutas conmutadas mediante etiquetas (LSP)

Un LSP (Label Switched Path) es una secuencia de LSR que forman el trayecto donde se va a transportar los paquetes etiquetados dentro de una red MPLS. Estos trayectos pueden ser determinados manualmente o mediante protocolos de enrutamiento. El primer LSR de este camino es el LSR de ingreso asignado para ese LSP, y el último LSR a considerarse en el trayecto, se lo tomará como el LSR de salida. Todos los routers en el medio, que forman el trayecto que tomarán los paquetes, se los considera LSR intermedios. Un trayecto LSP siempre es unidireccional, esto quiere decir que el camino de regreso se lo considera como otro LSP.

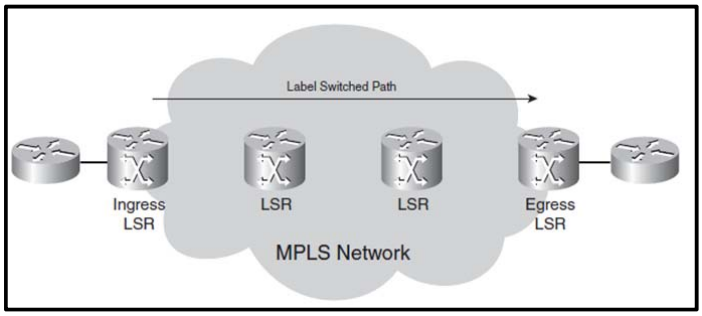

Figura 1.4 Label Switched Path
Fuente: MPLS_fundamentals_(Cisco 2008).pdf

1.2.5 Funcionamiento de MPLS

1.2.5.1 Componente de control y componente de envío

Antes de la aparición y posterior popularidad de MPLS existían diferentes técnicas que trataban de realizar la conmutación multinivel, pero presentaban problemas en cuanto a la convergencia y comunicación entre la capa de red y de enlace. Lo que tienen en común todas estas técnicas, incluso MPLS, son los parámetros en los cuales se basan, siendo estos: la separación entre las funciones de control o routing y de envío, y el intercambio de etiquetas para permitir el transporte de la información.

En MPLS, esta separación se ha dado en la utilización de dos componentes, una de control y otra de envío, al separar estas dos componentes su puede realizar cambios en ellas independientemente.

La componente de control mantiene las tablas de encaminamiento necesarias para el transporte de la información mediante la utilización de los protocolos de ruteo IGP (Protocolo de Gateway Interior), como OSPF, IS-IS Y BGP-4. También, su función es enviar la información sobre las etiquetas que van a necesitar los LSRs para continuar con el reenvío de los paquetes.

Al mismo tiempo, la componente de envío busca en la tabla de encaminamiento la ruta que debe seguir cada paquete. Esto lo hace al examinar la información que está en la cabecera del paquete, buscar en la tabla de encaminamiento y finalmente dirigir el paquete a su destino a través de los switches y routers de la red.

Para que se realice con éxito la transmisión en MPLS es absolutamente necesario que la componente de control esté en comunicación con la de envío todo el tiempo, esto se da mediante la tabla de encaminamiento con su información actualizada. Como ya es conocido, en MPLS el envío de

paquetes de da mediante el intercambio de etiquetas, es así como se está integrando las dos componentes.

1.2.5.2 Distribución de etiquetas

La distribución de las etiquetas en una red MPLS empieza en el LSR de ingreso, aquí es donde se pone la primera etiqueta al paquete, ésta indica que camino (LSP) va a seguir a lo largo de la red. El único cambio que se realiza es que la etiqueta va a ser cambiada por otra en cada uno de los saltos que dé el paquete entre los LSRs; así al llegar a un LSR intermedio éste cambia la etiqueta de entrada con otra etiqueta que será la de salida con respecto a ese router, y envía el paquete al siguiente enlace, este proceso se repite en cada uno de los routers intermedios por los que pase el paquete etiquetado. Al llegar al final, al LSR de salida del LSP determinado, éste retira la etiqueta y reenvía al enlace.

1.2.5.2.1 Protocolo de distribución de etiquetas (LDP)

Para transportar las etiquetas a lo largo de la red MPLS el protocolo más usado es LDP (Label Distribution Protocol). La función de este protocolo es distribuir la información de las etiquetas en todos los dispositivos que son parte de la red, ya que para transportar un paquete entre dos routers LSR es necesario que los dos conozcan el significado de las etiquetas utilizadas para mover el tráfico en esa red. Lo que hace LDP es determinar una serie de procedimientos mediante los cuales un LSR informa a otro sobre los enlaces de etiquetas que ha realizado. El LSR utiliza este protocolo para establecer rutas de encaminamiento a lo largo de la red.

1.2.5.3 Funcionamiento general de MPLS

Luego de conocer los elementos indispensables de MPLS, el funcionamiento se lo define en tres pasos:

1. Al llegar cada paquete al LER de ingreso, se construyen las tablas de encaminamiento, después se crean los LSPs que seguirán estos paquetes: estos LSP dan la idea de que cada router está únicamente a un salto de distancia, es decir, la topología MPLS funciona como si todos los routers estuvieran unidos entre sí (topología de malla), de manera directa o con PVCs. Los LSP se crean usando las tablas de intercambio de etiquetas proporcionadas por los LSR vecinos.

2. A continuación, el LER de ingreso revisa, procesa, etiqueta y envía el paquete hacia los LSRs intermedios para su conmutación. Hay que recordar que en cada LSR se realiza un cambio de etiqueta, pero que el paquete nunca cambia de LSP.

3. Finalmente, al llegar el paquete al LER de salida, éste le retira la etiqueta y envía el paquete al destino, o a la red convencional de routers que está presente en las dos fronteras de la red MPLS. Mientras el paquete está dentro de la red MPLS, las cabeceras IP son ignoradas por los LSR. Lo único que revisan los routers intermedios con las etiquetas, que luego de ser consultadas en la tabla de encaminamiento, son reemplazadas.

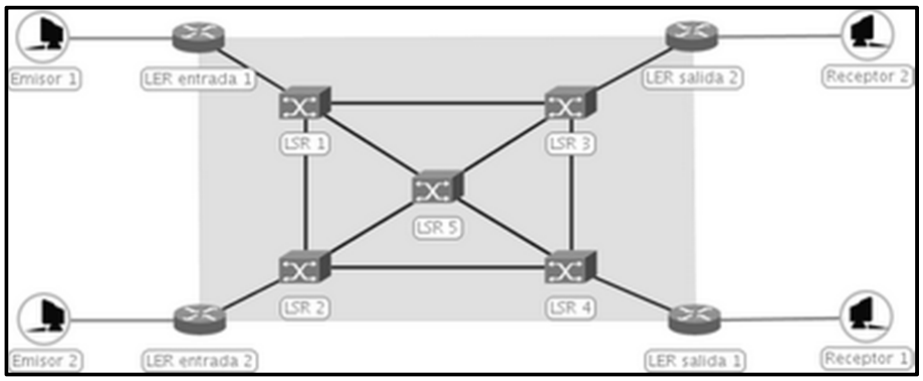

Figura 1.5 Arquitectura MPLS
Fuente: http://jedicerocool.blogspot.com/2009/08/mpls.html

1.3 Aplicaciones de MPLS

1.3.1 Ingeniería de Trafico

La ingeniería de tráfico es un proceso cuyo objetivo es mejorar la utilización de las redes, distribuyendo el tráfico existente en ellas de acuerdo a la disponibilidad que presenten los dispositivos de la red. Su objetivo es equilibrar la utilización de los recursos, de manera que no existan puntos congestionados cuando otros están sin utilizar y reservar enlaces para servicios o clientes especiales. El concepto de ingeniería de tráfico consiste en seleccionar flujos que, de acuerdo a los protocolos IGP, están siendo transmitidos en enlaces congestionados y trasladarlos a enlaces que están con poco tráfico o libres, pese a que no estén dentro de la ruta más corta o con menos saltos.

MPLS presenta las siguientes características de Ingeniería de Tráfico:

- Puede establecer rutas forzadas, se establece desde el router LER de ingreso que parámetros debe cumplir el LSP. Estas condiciones a cumplir pueden ser ancho de banda, retardo, prioridad del enlace, etc., que se requiere que tenga el flujo

- Se puede obtener datos estadísticos del uso de cada LSP. Esta información posteriormente se puede usar para hacer mejoras en la planificación de la red, como la manera de evitar cuellos de botella o enlaces recargados. También para futuras expansiones de la red.

- Seleccionar rutas para servicios o clientes especiales, mediante el CBR (Constraint Based Routing), que es un encaminamiento restringido. A partir de esto se tiene niveles de QoS, garantías de retardo, de ancho de banda, de pérdida de paquetes.

1.3.2 Calidad de Servicio

La calidad de servicio de una red de telecomunicaciones, QoS, es un mecanismo creado con el objetivo de mejorar el rendimiento de la red mediante la eliminación de aspectos como latencia, retardo, jitter, etc., y de esta manera satisfacer los requerimientos que tengan las aplicaciones. En una red con QoS los enlaces son controlados y el tráfico generado por aplicaciones críticas priorizado.

Para aplicar este concepto en MPLS, tiene que ser definido en cada LSP, asignando mayor ancho de banda al servicio que así lo necesite, además la ruta establecida será la más corta, para de esta manera garantizar la entrega de los paquetes con un retardo mínimo.

1.3.3 Clases de Servicio

La manera en que está diseñado MPLS permite manejar servicios diferenciados, esto se lo hace mediante el modelo del IETF llamado DiffServ (Servicios Diferenciados). Este modelo “permite diferenciar servicios como la transferencia de archivos, correo electrónico, considerando que para éstos el retardo no es crítico, en comparación con aplicaciones como el video y la voz en tiempo real, los mismos que si son dependientes del retardo” (Cisco Company, 2006)

1.3.4 Redes Privadas Virtuales (VPNs)

Una VPN (Red Privada Virtual) es una red con funcionalidad y seguridad para el transporte de datos equivalente a una red privada física, pero que tiene sus conexiones en una infraestructura pública y compartida con otros usuarios. En una VPN la información se envía a través de un túnel privado y seguro, que está sobre una red compartida, en el caso de MPLS sobre la red de un proveedor de servicios. Las VPNs brindan soporte a aplicaciones dentro o fuera de la red, soportan tráfico de voz, video y datos.

En MPLS las VPNs se establecen en los LSP, de manera que en estos LSP únicamente puede entrar el tráfico definido en la VPN respectiva, este proceso se lo realiza mediante el intercambio de etiquetas. Los beneficios que las VPNs traen a una red son las siguientes:

- Flexibilidad para elegir la tecnología o proveedor de servicio que se desee.

- Tiene un alto índice de escalabilidad, lo que permite un crecimiento sin problemas de la red.

- Implementar VPNs no representa grandes inversiones, ya que se la implementa sobre una estructura ya existente, no es necesario añadir dispositivos nuevos a la red.

- Y la mayor ventaja que se obtiene al utilizar estas redes privadas es la seguridad, ya que el tráfico viaja a través de túneles, de manera que no es posible que otras redes tengan acceso a esta información.

CAPITULO II

ESQUEMAS DE ARQUITECTURA DE RED CONVENCIONAL

Existen actualmente varias tecnologías de transporte, tales como SDH, Frame Relay, ATM, mismas que son utilizadas principalmente en las redes de los proveedores de servicios. En cuanto a las redes de área local (redes LAN), el estándar más utilizado para el transporte de los datos es Ethernet. A continuación se presenta una descripción del funcionamiento de cada una de estas técnicas, sus ventajas y desventajas.

2.1. Tecnologías de Transporte

2.1.1. SDH

SDH corresponde a las siglas en inglés de Synchronus Digital Hierarchy (Jerarquía Digital Síncrona), que es un estándar internacional usado en las redes ópticas de telecomunicaciones que tienen una alta capacidad. La principal característica es que los relojes que son usados para procesar las señales recibidas y generar las señales a transmitir a cualquier nodo dentro de esta configuración están sincronizados. Esto permite que la multiplexación se realice byte por byte, con una trama idéntica, usando diferentes tipos de justificación.

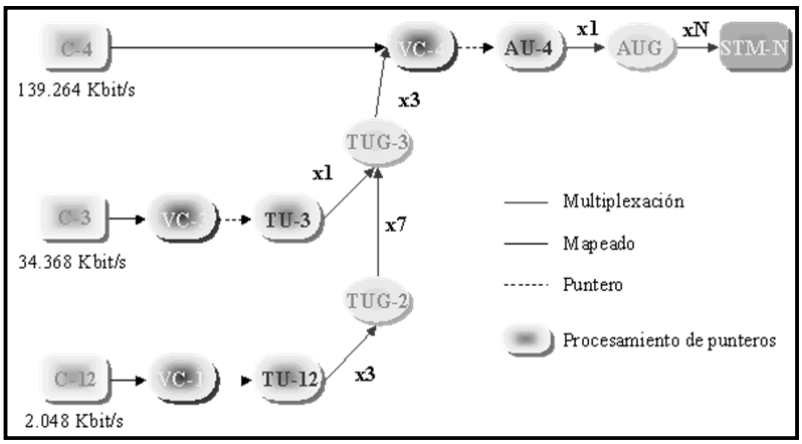

Figura 2.1 Estructura de multiplexación de SDH
Fuente: http://www.ramonmillan.com/tutoriales/sdh.php

2.1.1.1. Ventajas y desventajas de SDH

Entre las ventajas que presenta SDH se encuentran el hecho que presenta una infraestructura sencilla, que permite la administración y control de la red de una manera centralizada; además es una red flexible para ser aplicada en las telecomunicaciones, permite transportar diferentes tipos de señales (digitales o análogicas) y admite el uso de una sola infraestructura, es decir, puede interconectar equipos de diferentes marcas y modelos.

Al buscar las desventajas que tiene SDH se tiene principalmente que la cabecera de los paquetes a transmitir es muy grande, esto conlleva pérdida de eficiencia. Otra desventaja es la necesidad de sincronización entre todos los nodos de una red SDH, esto quiere decir que todos los servicios y dispositivos que funcionen en esta red deben trabajar bajo una misma frecuencia. Una red SDH implica una inversión alta y necesidad de personal constante, ya que es necesario tener un Centro de Gestión de Red.

2.1.2. Frame Relay

Es otro tipo de estándar de transmisión, se le define como un “protocolo de capa de enlace de datos con conmutación que maneja múltiples circuitos virtuales mediante una forma de encapsulamiento HDLC (HDLC: High-Level Data Link Control, 2003) entre dispositivos conectados” (Cisco Network Academy, 2003)

Frame Relay es un servicio de telecomunicaciones diseñado para la transmisión de datos con gran eficiencia y costo razonable entre redes LAN, entre conexiones de usuarios finales en redes WAN, con backbones, o en redes privadas mediante líneas T-1 alquiladas a los proveedores de servicios. Este servicio funciona mediante una línea dedicada durante toda la transmisión.

La transmisión de datos se realiza mediante el envío de”*frames”* o paquetes, estos son una unidad de tamaño variable de datos; a cada uno de estos paquetes se les asigna un identificador, mismo que mantiene a lo largo de la trasmisión. Frame Relay encarga la corrección de errores y retransmisión de datos a los puntos de destino, para de esta manera obtener más velocidad en la transmisión. Los circuitos están conectados a un switch que se encarga de enviar los paquetes a los respectivos usuarios finales.

Para la mayoría de servicios se utiliza un PVC (Circuito permanente virtual), de esta manera el usuario dispone de una línea dedicada de conexión sin tener que pagar por el alquiler de una línea física, ya que el proveedor del servicio es quien determina la ruta por la que cada uno de los paquetes va a viajar, y en base a esto se determina el costo final.

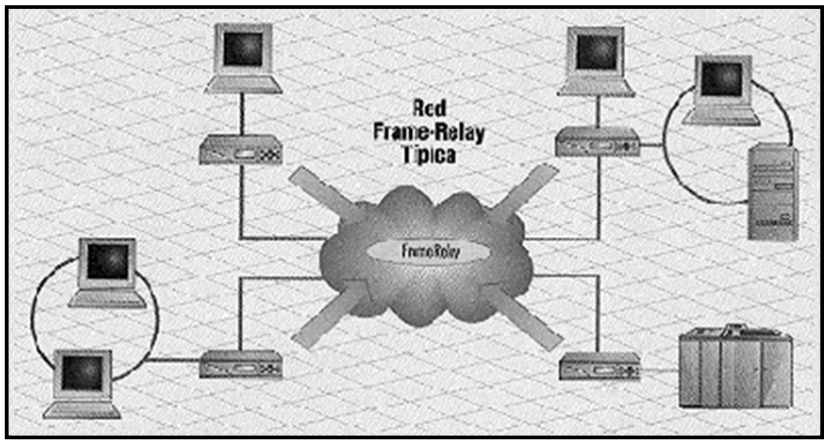

Figura 2.2 Esquema de red Frame Relay típica
Fuente: http://fmc.axarnet.es/redes/tema_07.htm

2.1.2.1 Ventajas y desventajas de Frame Relay

La mayor ventaja que presenta Frame Relay es que provee todas las características y beneficios de un servicio de red mediante una línea dedicada, pero sin los altos costos que representa tener varios de estos circuitos. Las desventajas que se encuentra son que es mucho más difícil de configurar que las otras técnicas, el manejo de la red es complejo y no es una técnica adecuada para transmisiones de voz o datos, ya que éstas requieren de un flujo constante en la transmisión.

2.1.3 ATM

El Modo de Transferencia Asíncrono – ATM (*Asynchronous Transfer Mode*) es una tecnología de transferencia de paquetes con conexión dedicada que funciona tanto en redes LAN como WAN. Esta tecnología soporta comunicaciones de voz y video en tiempo real. ATM ha sido “concebida como una tecnología multiservicio basada en celdas, ideal para soportar una amplia variedad de tipos de tráfico y métodos de acceso, suministrando un protocolo de transmisión capaz

de aplacar las demandas de los usuarios de las redes empresariales" (Lusa, 1999). Es un servicio orientado a la conexión, funciona en la capa 2 del modelo OSI y usualmente usa SONET para la corrección de errores.

Esta topología utiliza switches, mismos que forman un circuito lógico de extremo a extremo, esto garantiza la calidad de servicio (QoS) de la comunicación. Para la transmisión de la información, ésta es organizada en celdas de 53 bytes, y transmitidas a lo largo de un medio físico; se utiliza celdas de este tamaño ya que son más rápidas de procesar, y además al tener celdas pequeñas aseguran que paquetes que contienen voz o video pueden ser insertadas en el flujo de transporte tan a menudo para que la transmisión sea en tiempo real.

Para enrutar las celdas a su destinatario se toman en cuenta las direcciones como identificadores. De ser necesaria una conexión virtual, este se establece antes de empezar con la transferencia de datos. Los parámetros de calidad de servicio se determinan o negocian al momento que se realiza la conexión.

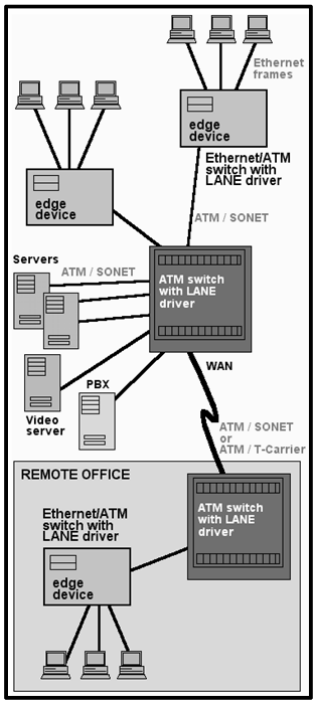

Figura 2.3 Esquema ATM
Fuente: Computer Desktop Encyclopedia, The Computer Language Inc., 2000, PC Magazine

2.1.3.1 Ventajas y desventajas de ATM

ATM presenta ventajas tales como la garantía de fiablidad en el transporte de los datos, ofrece altas velocidades de transmisión, y finalmente presenta una alta compatibilidad con aplicaciones que transportan voz, video y datos, y al transporte de grandes volúmenes de datos. Las falencias de ATM son que no presenta facilidades en la migración a LAN, requiere el cambio de varios de sus componentes, lo que implica altos costos y una gran cantidad de tiempo. También que esta tecnología es únicamente aplicable a backbones de alta velocidad o redes WAN, no así a empresas pequeñas o computadores personales. Y, finalmente, ATM no se puede adaptar totalmente al transporte de voz, ya que se requiere de una actualización de SONET para tener el ancho de banda necesario, y al tener ya esta actualización lo más probable es que ATM ya no sea necesario.

2.1.4 TCP/IP

La arquitectura TCP/IP es un protocolo de comunicaciones más usado y fundamental en el Internet, aunque también es usado por algunas redes Intranet y Extranet. De hecho, TCP/IP no es un solo protocolo, sino está formado por dos protocolos:

- **TCP** (Transmission Control Protocol; Protocolo de Control de Transmisión), es responsable de verificar la entrega correcta de los datos desde el cliente hasta el servidor, ya que muchas veces la información que se está transportando puede perderse en el camino. Además brinda soporte para la detección de errores y maneja la retransmisión de datos hasta que la información sea recibida completa y correcta.

- **IP** (Internet Protocol; Protocolo de Internet), es responsable del transporte de los paquetes de nodo a nodo. IP envía los paquetes basándose en la dirección IP, que está formada por 4 bytes. Las

autoridades de control del Internet asignan diferentes rangos de direcciones IP a diferentes organizaciones; estas organizaciones asignan grupos de direcciones a sus departamentos. El trabajo de IP es transportar los paquetes de datos desde los departamentos, a las organizaciones, y finalmente, al mundo.

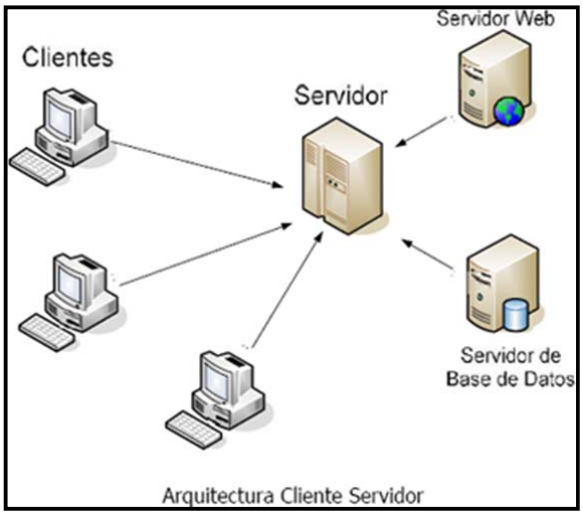

Figura 2.4 Esquema funcionamiento TCP/IP

Fuente: http://www.mailxmail.com/curso-php-mysql-aplicaciones-web-1/web-site funcionamiento-tipos-programacion

2.1.4.1 Ventajas de TCP/IP

- Es un protocolo de alto nivel, que prestan sincronización con varios servicios y aplicaciones. Además el direccionamiento de paquetes es único, mediante las direcciones IP

- La posibilidad de transportar paquetes de datos mediante Circuitos Virtuales (con un alto grado de confiabilidad), y Datagramas, que no presentan confiabilidad.

- Tiene independencia total del medio físico al no necesitar un interfaz físico en particular.

- Es el protocolo fundamental de la red más grande conocida, el Internet.

2.1.4.2 Comparación entre el Modelo OSI y el modelo TCP/IP

Actualmente, las funciones de una red están divididas en siete capas, mismas que están representadas en el Modelo de Referencia OSI, aunque hasta el momento no se ha logrado implementar ninguna red que cumpla con esta estructura. Es por esto que apareció el modelo TCP/IP, que está basado en protocolos ya existentes, y por lo tanto, su implementación resulta sencilla.

El protocolo TCP/IP está formado por cuatro capas, cada una de las cuales presenta una funcionalidad cuyo objetivo es resolver un grupo de problemas. Este protocolo usa la encapsulación para proporcionar independencia de protocolos y servicios a cada una de las capas. Generalmente, el modelo empieza su funcionamiento desde la capa más alta, en este caso la capa de aplicación, donde mediante un conjunto de protocolos transmite la información hacia las otras capas, siendo esta encapsulada en cada una de ellas.

De acuerdo a la recomendación RFC 1122, los protocolos y servicios utilizados en el modelo TCP/IP están divididos en cuatro capas, siendo estas: Capa de Aplicación, Capa de Transporte, Capa de Internet y Capa de Acceso a la Red. Se puede definir la manera en que estas capas tienen similitud y correspondencia con las del Modelo de Referencia OSI de la siguiente manera:

- Capa 4 o Capa de Aplicación: en esta capa están incluidas las capas de sesión (capa 5), de presentación (capa 6) y de aplicación (capa 7) del modelo OSI. Aquí se maneja la representación, codificación

y control de la comunicación. Funcionan protocolos como SMTP, FTP, SSH o HTTP.

- Capa 3 o Capa de Transporte: es similar a la capa 4 del modelo OSI. Aquí opera el protocolo TCP (Transfer Control Protocol), mismo que establece un circuito virtual entre los dispositivos finales antes de transmitir los datos. Además funcionan en esta capa UDP (User Datagram Protocol, no está orientado a la conexión, por lo tanto no presenta garantías referentes a el transporte y control de errores. El objetivo de esta capa es permitir, entablar y mantener la comunicación; y también asegurar la transmisión y recepción de los mensajes completos.

- Capa 2 o Capa de Internet: equivale a la capa 3 (capa de red) del modelo OSI. Esta capa define la dirección IP del dispositivo y los caminos de enrutamiento para el transporte de los paquetes de datos de una dirección IP a otra. Recibe los paquetes TCP o UDP desde la capa 3 y los ubica con la dirección MAC (Media Access Control) correspondiente. En esta capa, además de las dos versiones de protocolo IP: IPv4 e IPv6, también funcionan ICMP, IGMP.

- Capa 1 o Capa de Acceso a la Red: Se le puede comparar con la capa física y de enlace de datos del modelo OSI. Esta capa define los protocolos de bajo nivel que son utilizados en la señalización y comunicación, tales como PPP, FDI, Frame Relay, ATM, GPRS, etc.; y también está en esta capa la parte física de la red, todos los dispositivos, cables, y sistemas de señalización, tales como Ethernet, SONET/SDH, ISDN, módems, routers.

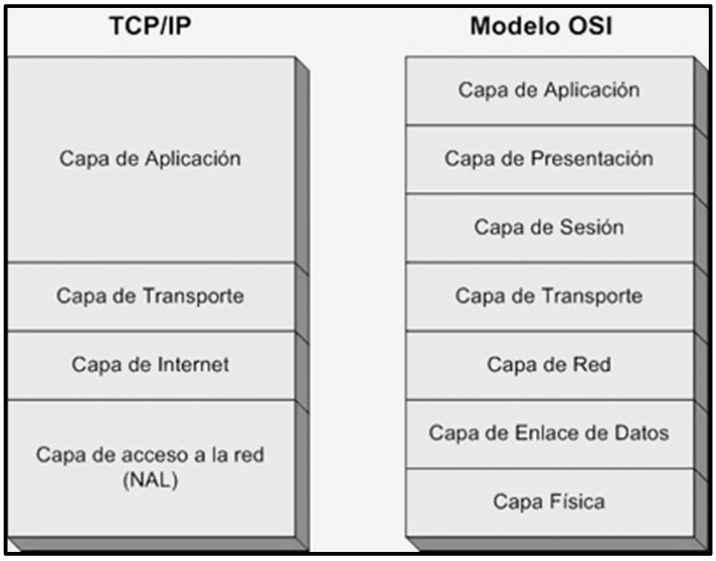

Figura 2.5 Comparación modelo TCP/IP y modelo OSI
Fuente: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

La información a ser transportada en el modelo TCP/IP, al igual que en el modelo OSI, descienden por las capas del protocolo en el caso de la parte que está enviando la información, y de manera ascendente cuando se trata del receptor. En cada una de las capas, al paquete de le añade una cabecera de datos para el control de envío, esto es lo que se conoce como encapsulación. Una vez que los datos han sido recibidos se procede a la inversa; es decir, mientras los datos suben por cada capa del modelo se le va retirando las cabeceras agregadas anteriormente.

2.2 Arquitectura IP sobre ATM

Debido al gran desarrollo del internet, y la necesidad de los proveedores de suplir la amplia demanda de ancho de banda, se buscó maneras de ampliar los circuitos que se utilizaban, y, principalmente, aprovechar de mejor manera los recursos con los que ya contaba estas empresas. Para lograr esto se determinó que una de las soluciones era combinar los switches ATM, conocidos por su gran eficacia y rentabilidad, con los routers IP, que presentan muchas ventajas para el control del tráfico; es decir,

integrar en una sola tecnología las capas 2 y tres del modelo OSI. Se puede resumir en: una red de arquitectura IP sobre ATM une las ventajas de utilizar la tecnología IP, que es no orientada a la conexión, como la red de transporte, sobre la tecnología ATM, que es orientada a la conexión.

El funcionamiento de IP sobre ATM representa el montaje de circuitos virtuales de routers IP sobre un esquema real de switches ATM. El backbone de la red ATM es el núcleo (o nube central) de los routers externos. De esta manera se tiene el ruteo en la topología virtual, donde se envía y controla los paquetes; y la conmutación en la topología física, aquí se realiza el control y señalización para el envío de las celdas.

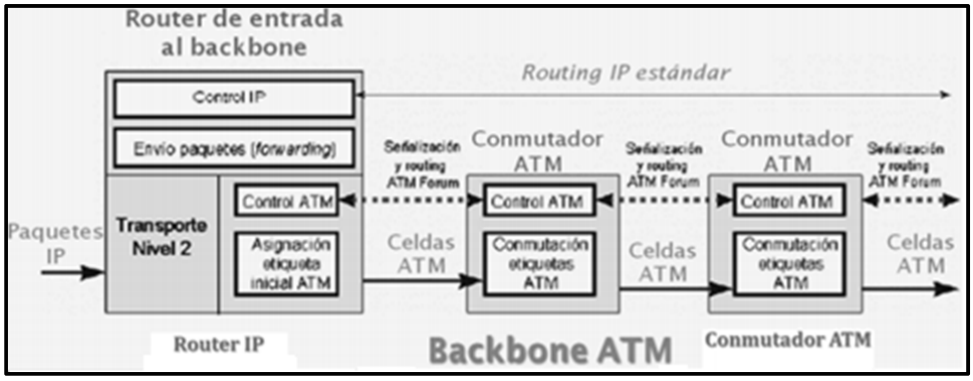

Figura 2.6. Funcionamiento de IP sobre ATM
Fuente: Funcionamiento de IP sobre ATM:
http://coimbraweb.com/documentos/telecom/9.7_ip_o_atm.pdf

2.2.1 Ventajas y desventajas de la Arquitectura IP sobre ATM

Al implementar IP sobre ATM lo que se puede ganar es una red de telecomunicaciones con ciertas ventajas, por ejemplo: se va a tener una conmutación rápida debido a las características de ATM, una alta velocidad de transmisión de los paquetes y la posibilidad de desarrollar varias aplicaciones al mismo tiempo gracias a la multiplexación de la información. El transporte de datos se realiza utilizando circuitos virtuales, estos pueden ser permanentes o conmutados, de esta manera se logra que la entrega de datos sea rápida, viajando a través de una red confiable, y con beneficios como la reserva de recursos, el tener varias clases de direccionamiento.

Finalmente, entre las limitaciones que presenta este modelo se tiene la dificultad que presenta el operar e integrar al mismo tiempo dos tecnologías que son muy distintas y que funcionan incluso en diferentes capas del modelo OSI; la aparición de nuevos dispositivos de alto rendimiento, tales como switches ATM e IP que están siendo instalados en las redes troncales, y por último, los beneficios, como mayor velocidad y confiabilidad que ofrecen SDH/SONET y DWDM (Dense Wavelength Division Multiplexing) respecto a las redes ATM.

2.3 Ethernet

Actualmente es la componente de la capa física más usada y popular para redes LAN. Su popularidad se debe a que proporciona balance entre velocidad, costo y facilidad de instalación, también soporta prácticamente todos los protocolos de red. Se le puede definir como una LAN de medios compartidos. Puede conectar hasta 1024 dispositivos a 10 Mbps sobre un cable trenzado, cable coaxial o fibra óptica. Ethernet fue definido por la IEEE mediante el estándar 802.3. Ethernet tiene la capacidad de transmitir paquetes de distinto tamaño, cada uno contiene una cabecera con la dirección de origen y destino, también tiene corrección de errores.

Una característica típica de Ethernet es su propensión a colisiones. Ya que es un medio compartido, se necesita seguir ciertas reglas al momento de enviar los paquetes, para de esta manera evitar conflictos con otros nodos o dispositivos, y al mismo tiempo proteger los datos.

Las colisiones se dan cuando dos equipos intentan enviar datos al mismo tiempo, ya que consideran que la red no está en uso. Una de las causas de las colisiones es la mala planificación de la red, por ejemplo existen demasiados usuarios en la red, y esto se deriva en una disputa constante por el ancho de banda de la red. Una solución para evitar estas colisiones es la segmentación lógica de la red, uniéndola únicamente mediante un hub o switch, para de esta manera reducir la saturación presente en la red.

Para detectar las colisiones, Ethernet utiliza CSMA/CD para enviar un mensaje de broadcast al medio físico. De esta manera todos los dispositivos conectados a esta red “escuchan” la solicitud, y solamente el equipo con la dirección de destino acepta el paquete y lo revisa por errores. Ethernet funciona en las capas 1 y 2 del modelo OSI.

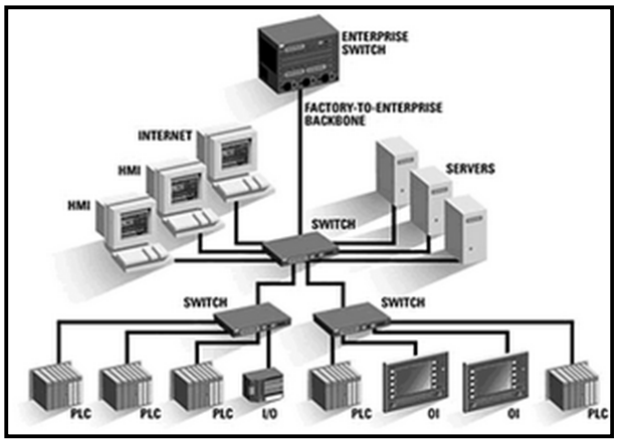

Figura 2.7 Esquema de red Ethernet

Fuente: http://4esoies.blogspot.com/2011/10/redes-locales.html

2.3.1 Ventajas y desventajas de la red Ethernet

El estándar para transmisión de datos Ethernet es la solución más adoptada al momento de elegir un estándar de transporte para una red LAN. Esta alta tasa de aceptación se ha dado debido a las ventajas que presenta, como la gran capacidad de velocidad que permite para las redes que así lo necesitan, tiene un costo bajo de implementación y mantenimiento, es sencilla de manejar y su mantenimiento no es complicado, es muy flexible al momento de incorporar tecnologías nuevas y tiene un alto nivel de confiablidad.

Su principal desventaja es que, al ser un medio compartido por todos los dispositivos parte de la red, tiene a presentar colisiones de datos, lo que puede caer en pérdida de información y altos niveles de retardo en la transmisión de los flujos de tráfico. También que el servicio de la red está en función del número de

dispositivos conectados a la misma, y además, el tráfico total no debe ser mayor al 40% del ancho de banda disponible

2.4 Resumen de arquitecturas convencionales

	Ventajas	Desventajas
SDH	- Está basado en la multiplexación síncrona directa, esto gracias a la utilización de punteros - Señales más lentas pueden ser multiplexadas en señales SDH rápidas, sin multiplexaciones intermedias - Infraestructura sencilla. Admite interconexión entre diferentes marcas. - Transporta señales analógicas y digitales - Puede ser utilizada en: redes de larga distancia, LAN y bucles de portadores.	- Cabecera grande de los paquetes. - Se necesita sincronización entre todos los nodos. - Inversión alta. - Necesidad de personal constante - La velocidad de los canales es fija. - No admite multiplexación estadística, misma que provee un mejoramiento en la utilización del enlace - Cuando es utilizado en enlaces punto a punto, a cada circuito se le asigna una cantidad de terminada de ancho de banda, misma que es desperdiciada cuando el circuito no está en uso.
Frame Relay	- Beneficios de una línea dedicada, sin los altos costos de ésta.	- Configuración complicada - No es adecuada para transporte de voz y video.

	- Los circuitos virtuales únicamente consumen ancho de banda cuando están en uso, por lo tanto se puede tener varios de estos circuitos en una misma línea. - Los dispositivos pueden usar más ancho de banda del necesario y así operar a velocidades más altas. - Permite aplicar QoS - Mejor desempeño y tiempo de respuesta de la red.	- No garantiza entrega de datos, y por lo tanto no es el protocolo adecuado para realizar el envío de información susceptible. - Al permitir tramas de tamaños variables se pueden crear retrasos para algunos usuarios. - Ya que utiliza una red común para transportar los circuitos virtuales puede haber momentos en que la cantidad de datos a transmitirse excede la capacidad de la red y provoca congestionamientos en la misma.
ATM	- Garantía de fiablidad - Flexibilidad y alta velocidad de transmisión. - Compatibilidad para transportar voz, video y datos. - Permite multiplexación estadística. - Es escalable y flexible, ya que no está ligada a un medio físico específico. - El ancho de banda puede ser asignado de acuerdo a las necesidades, para que de esta manera reduciendo el impacto de usuarios con alto nivel de uso.	- Altos costos para la migracion a ATM; y para el mantenimiento de la red. - Principalmente aplicable a backbones o redes WAN. - Complejidad de funcionamiento e implementación - Pese a que puede presentar ciertos mecanismos de QoS, estos son muy complejos. Además se refieren únicamente a las capas más altas.

TCP/IP	- Protocolo de alto nivel. - Direccionamiento único: direcciones IP - Diseñado para enrutamiento, con alto grado de confiabilidad. - Independencia del medio físico. - Protocolo fundamental del Internet	- Difícil de configurar y mantener. - Presenta lentitud en redes con tráfico bajo.
IP sobre ATM	- Conmutación rápida - Alta velocidad - Multiplexación de la información - Tiene la capacidad para permitir calidad de servicio. - No tiene limite en el tamaño de los paquetes. - Permite transportar cualquier tipo de tráfico.	- Son dos tecnologías muy diferentes; funcionan en diferentes capas del modelo OSI - Aparición de tecnologías, como DWDM, que ofrecen mayor confiabilidad y velocidad - No resuelve probemas de retrasos o congestionamiento, ya que no puede aplicar la QoS de ATM - No soporta tráfico multicast
Ethernet	- Gran capacidad de velocidad. - Bajo costo de implementación y mantenimiento. - Flexible a la incorporación	- Tendencia a colisión de datos, al ser un medio compartido. - Altos niveles de retardo en la transmisión. - El servicio está en función del número de dispositivos.

	de nuevas tecnologías - Alto nivel de confiabilidad.	- Trafico total debe ser menor al 40% del ancho de banda

Tabla 2.1 Resumen de arquitecturas convencionales

CAPITULO III

ESTUDIO DE TRÁFICO

3.1 Descripción de la Empresa en donde se realizó la captura de tráfico

La captura y análisis de tráfico se realizó en la Jefatura de Infraestructura Agencias del Banco del Austro S.A en la Oficina Matriz en la Ciudad de Cuenca. Esta es la oficina encargada de la administración, instalación y mantenimiento de los dispositivos y complementos pertenecientes a la red del banco. La oficina cuenta con un ancho de banda de 100 Mbps; cada uno de los usuarios de la red se conecta a la misma a través de un "*hub*" (concentrador) ubicado en una de las oficinas. Los dispositivos conectados son computadoras, impresoras, máquinas de fax y teléfonos ip. A continuación un esquema simplificado de esta red.

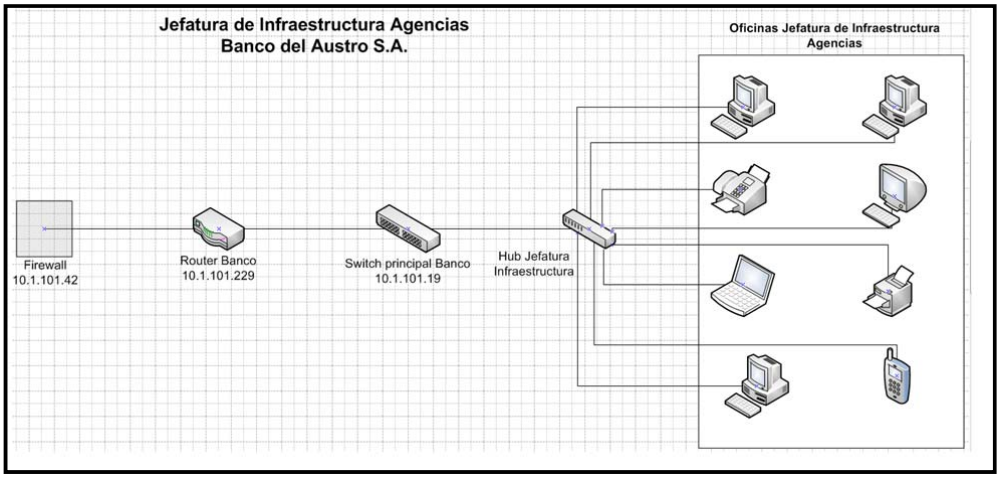

Figura 3.1 Esquema Jefatura de Infraestructura Agencias, Banco del Austro S.A

3.2 Descripción del programa utilizado

El programa utilizado para realizar las capturas y análisis del tráfico presentado en la red analizada es Wireshark, versión 1.6.2. Este programa es un analizador de protocolos y tráfico de red (popularmente conocido cono sniffer), se lo utiliza para realizar análisis y solucionar problemas en redes de comunicaciones, para lograr un correcto desarrollo de otro software o de protocolos; también es ampliamente usado como una herramienta didáctica. Es un programa de software libre, está disponible para los sistemas operativos Windows, Linux, Solaris y MAC OS.

La información que se puede obtener al realizar el análisis de tráfico con este programa es la siguiente:

- Direcciones IP, hostnames y routers que están siendo utilizados, y sus rutas de transmisión

- Datos transmitidos, generalmente la mayoría de datos que circulan en las redes se pueden ver como texto plano, por ejemplo si se están utilizando los servicios de FTP, Telnet, email). El programa para leer estos datos se daría en caso que éstos estén encriptados.

- Información sobre cada uno de los protocolos que están siendo utilizados en la red.

3.3 Análisis de la captura de tráfico.

Las capturas de tráfico se realizaron en la Jefatura de Infraestructura Agencias del Banco del Austro S.A. en la Oficina Matriz en la Ciudad de Cuenca, a continuación un detalle de los tipos de protocolo encontrados en estas capturas.

- **Captura #1:** Esta captura se la realizó el día jueves 10 de noviembre de 2011, por un lapso de 37 minutos. El número total de paquetes

capturados es de 41428. En la imagen 3.1 se puede observar un resumen de la jerarquía de protocolos encontrados en esta transmisión.

Se observa que el 100% de los paquetes transmitidos son Ethernet, esto concuerda con la información proporcionada por la empresa que indica que toda la red interna es de tipo LAN. También se puede apreciar los porcentajes totales que pertenecen a diferentes tipos de protocolos, tales como:

- **ARP (**Address Resolution Protocol**):** 28.15% de paquetes. El objetivo de este protocolo es encontrar la dirección física (MAC) relacionada con una dirección IP conocida.

- **Internet Protocol Versión 4:** 58.80% del total de tráfico capturado. Todos los dispositivos dentro de esta red tienen una IP fija que las diferencia dentro del entorno.

- **Logical Link Control:** 7.70% del total. Esta capa es una de las subcapas de la capa de enlace de datos del modelo OSI. Su objetivo es manejar el tráfico, tanto el flujo como el control de errores, a través del medio físico. También identifica los protocolos de línea, que pueden ser SDLC, NetBIOS o NetWare, asigna números de secuencia a las tramas.

- El 5.35% restante corresponde a otros protocolos, tales como IPX (Internetworking Packet Exchange), Internet Protocol versión 6 y Data

Los resúmenes de la jerarquía de protocolos de las capturas 2 y 3 son presentados en las imágenes 3.2 y 3.3, se tienen los mismos protocolos descritos anteriormente en detalle para la captura 1, cada uno con su porcentaje respectivo de aparición en la captura.

- **Captura #2:** realizada el jueves 10 de noviembre, por un lapso total de 18 minutos, y fueron capturados 17342 paquetes. En la figura 3.2 está el resumen de la jerarquía de protocolos.

- **Captura #3:** realizada el viernes 11 de noviembre del año en curso, por un lapso de 34 minutos, fueron capturados en total 30269 paquetes. En la figura 3.3 se puede apreciar el resumen de la jerarquía de protocolos.

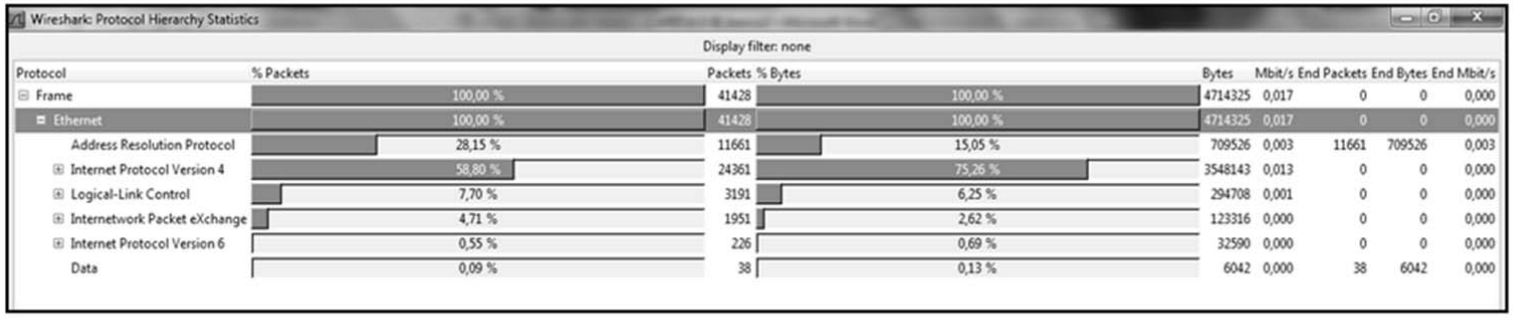

Figura 3.2 Resumen captura #1

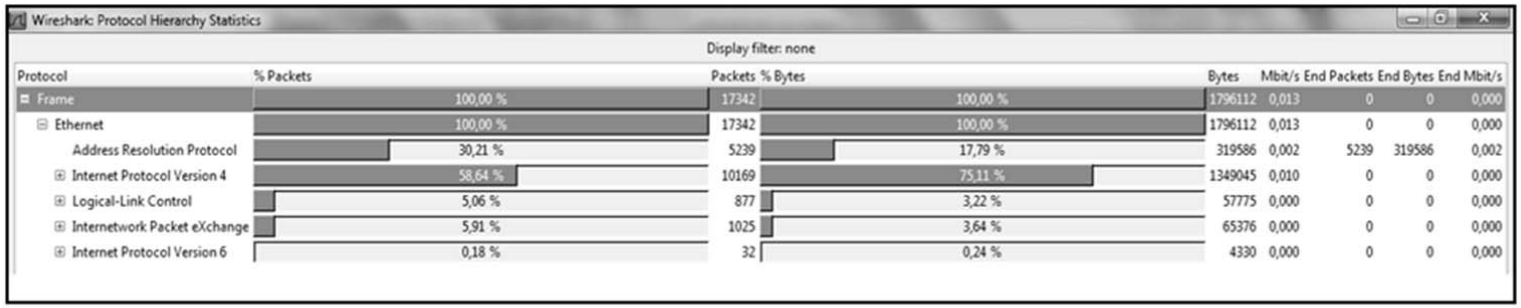

Figura 3.3 Resumen captura #2

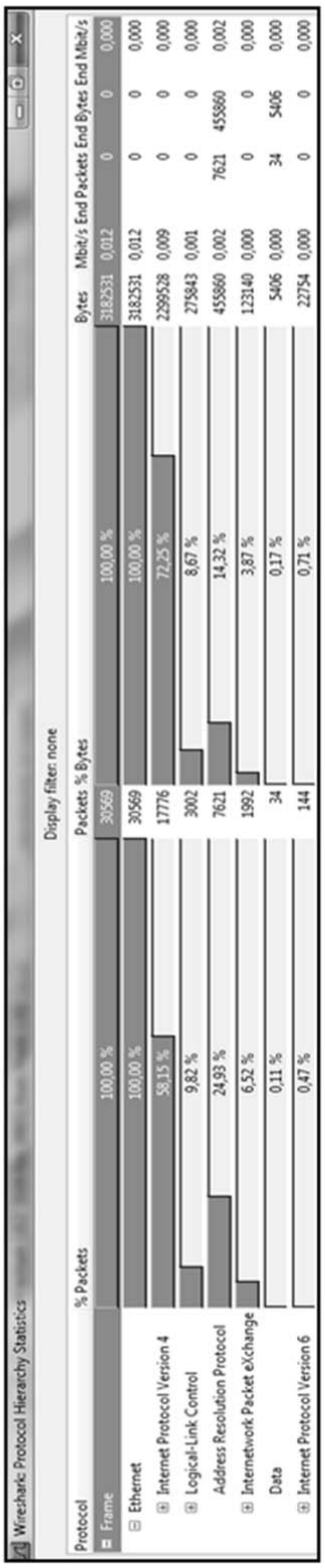

Figura 3.4 Resumen captura #3

Cada una de las capturas realizadas presenta un alto porcentaje de tráfico IPv4. Esto se debe a que de acuerdo a la configuración de red utilizada en esta oficina, los dispositivos de red posee una dirección IP única, estas direcciones están vinculadas a un nombre de dispositivo, para de esta manera reconocer al mismo dentro de la red.

Cuando se realiza una captura de tráfico, para su posterior análisis y establecimiento de características de la red es importante empezar por ver cuáles son los servicios que están siendo prestados. En el caso de las capturas realizadas con el programa Wireshark, el proceso empieza por aplicar filtros y decoders al tráfico capturado, para de esta manera segmentarlo en los diferentes protocolos. A continuación se presenta una explicación detallada de la Captura #1, donde se muestra los protocolos encontrados, y el porcentaje de los mismos respecto al total de paquetes capturados.

Captura #1

- Protocolo UDP: Al aplicar el filtro “udp” al total de paquetes obtenidos en la captura se obtiene que el total de paquetes de este tipo, que es un estándar no orientado a la conexión, es de 22313 paquetes. En la siguiente figura se muestra una captura de pantalla de las estadísticas de protocolo generado por el mismo programa, luego de aplicado el filtro.

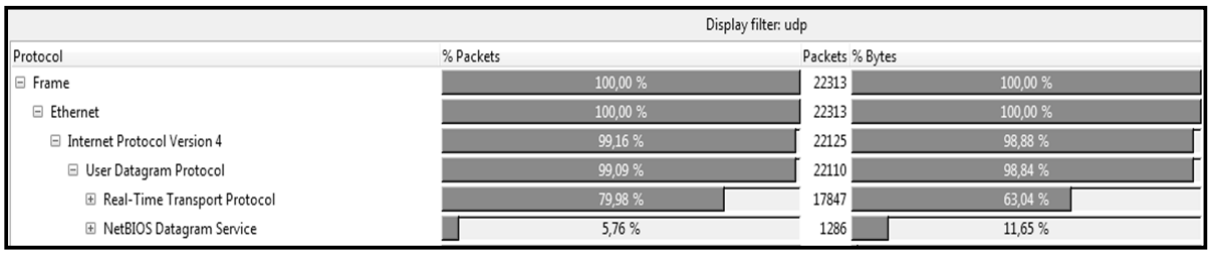

Figura 3.5 Porcentaje de paquetes UDP

Para analizar el tráfico UDP ya filtrado, se utiliza la opción Decode As, en el menú Analyze. En la ventana que se abre se muestran todos los protocolos soportados por UDP.

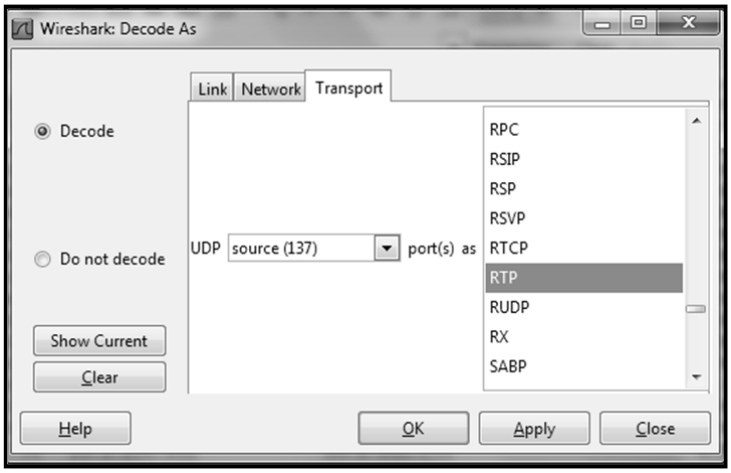

Figura 3.6 Ventaja de herramienta *Decode As*.

Luego de ejecutar esta herramienta se encontraron los siguientes resultados:

- Paquetes RTP (Real-Time Transfer Protocol), este protocolo transporta tráfico generado por aplicaciones que transmiten en tiempo real, como audio o video. Este protocolo normalmente utiliza a UDP como su protocolo de transporte, pero no tiene un puerto UDP asignado, aunque la IETF recomienda los puertos 6970 o 6999. Lo que normalmente hace este protocolo es seleccionar un puerto de manera dinámica, y luego señalizarlo mediante otros protocolos. En esta captura se obtuvo un total de 17847 paquetes de este RTP, mismos que equivalen al 79.98% del total de tráfico UDP. Dentro de este filtro se encontraron varios tipos de protocolos transmitiendo tráfico en tiempo real, estos son:

  - Paquetes puramente RTP, un total de 17222, es decir un 96.55% se refiere a llamadas de Voz sobre IP. La oficina de la Jefatura de Infraestructura cuenta con alrededor de 10 teléfonos Ip para la comunicación. Estos teléfonos son de marca Grandstream, los modelos son GXP280 y BT210. El códec utilizado por estos teléfonos para la compresión de audio es el G.723.1, mismo que comprime los datos de audio en paquetes de 30ms; puede

transmitir a velocidades de 6.4kpbs o 5.3 kpbs. Por lo tanto, tomando en cuenta que se tienen instalados diez teléfonos únicamente en las oficinas de la Jefatura de Infraestructura Agencias se tiene que el ancho de banda mínimo necesario para esta comunicación es de 64kbps. A partir de esto se puede deducir que la red total del banco tiene una capacidad de expansión, en lo que se refiere a teléfonos, muy amplia. Se recomienda continuar con el uso de esta marca de teléfonos, pues el códec utilizado por los mismos presenta un gran rendimiento. A continuación se presenta una gráfica donde se puede ver de manera clara la predominancia de tráfico RTP dentro del filtro udp. el tráfico UDP está representado por la línea en la parte superior del gráfico, mientras que el protocolo UDP es la parte sólida del mismo. Se puede observar que durante todo el tiempo de captura se mantiene más o menos constante el tráfico que fluye en esta red, a excepción de momentos en que aumenta de manera significativa, pero no es más que eventos aislados que no representan riesgo en el rendimiento general de la red.

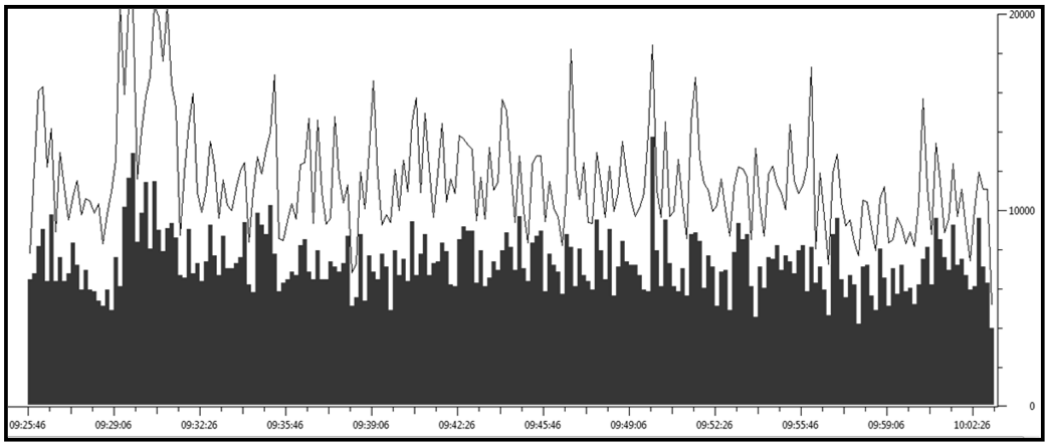

Figura 3.7 Protocolo UDP y RTP

- Otra parte de los paquetes RTP encontrados son de tipo RTPevent, se tiene 201 paquetes de este tipo, es decir el 1.13% del total de eventos transmitidos en tiempo real. Estos paquetes se refieren a transmisiones realizadas por fax, que es un porcentaje muy bajo debido a que la mayoría de comunicaciones entre usuarios se realiza mediante correo electrónico

- Los 424 paquetes restantes, que corresponden al 2.4% del total representan a cinco otros protocolos de bajo uso, siendo estos G.723.1 (códec para compresión de audio), H.261 (estándar de video), H.263 (estándar para compresión de videos con codificación), MPEG-1 (estándares de codificación de audio y video), JPEG (estándar de compresión y codificación de archivos de imágenes fijas)

- Protocolo TCP (Transmission Control Protocol): Es un protocolo orientado a la conexión, que se utiliza para transportar los datos del protocolo de Internet. La red de la Jefatura de Infraestructura del Banco del Austro S.A. está formado por varios dispositivos, como computadoras, impresoras, teléfonos IP, router; cada unos de los cuales dispone de una dirección IP propia. Estas utilizan el protocolo TCP para crear canales de conexión entre ellas, y de esta manera enviar flujo de datos a través de los mismos.

  Este tipo de protocolo garantiza que los datos serán entregados en su destino sin errores ni pérdidas. Además es posible identificar el tipo de aplicación a utilizarse mediante los puertos. TCP puede soportar varias aplicaciones muy populares en el Internet que utilizan protocolos de aplicación tales como HTTP (navegación), SMTP (correo electrónico), SSH (navegación segura) y FTP (transferencia de archivos). Al realizar el análisis de los paquetes capturados, se encuentra que el 5.05% del total de paquetes corresponde a este protocolo. Esto representa la información enviada a través de correo electrónico. No existe un alto nivel de tráfico TCP ya que ninguna computadora en la red del Banco tiene acceso a navegación en Internet.

Dentro de la captura filtrada como tráfico TCP se han encontrado paquetes de tipo TLSv1, este es un protocolo de seguridad en la capa de transporte, utilizado generalmente para Internet. En el caso de los paquetes encontrados, estos provienen de un equipo de la red que intenta acceder a la navegación en la red. Finalmente, se observa un pequeño porcentaje de tráfico DNS, igualmente esto se debe a que no existe navegación en Internet.

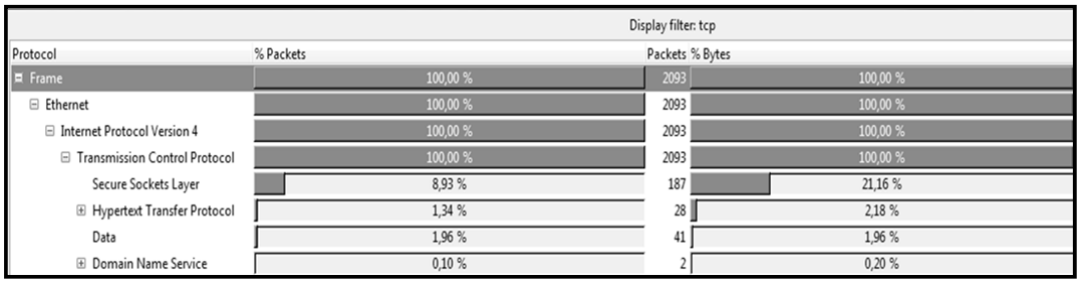

Figura 3.8 Porcentaje de paquetes TCP

- Protocolo ARP (Address Resolution Protocol): Como ya se indicó anteriormente, el objetivo de este protocolo es asociar las direcciones físicas o direcciones MAC, con las direcciones lógicas o IP de un equipo. Esto lo logra a partir de crear tablas de búsqueda donde están emparejadas la dirección lógica con su correspondiente física. El porcentaje de protocolo ARP presente en esta captura es del 28.15%. Los paquetes ARP son en su mayoría broadcast, esto provoca ruido en la conexión; cuando se tiene un exceso de este tráfico se puede estar frente a un ataque ARP (ARP spoofing), que es un tipo de ataque a la red con el propósito de lograr la caída de la misma.

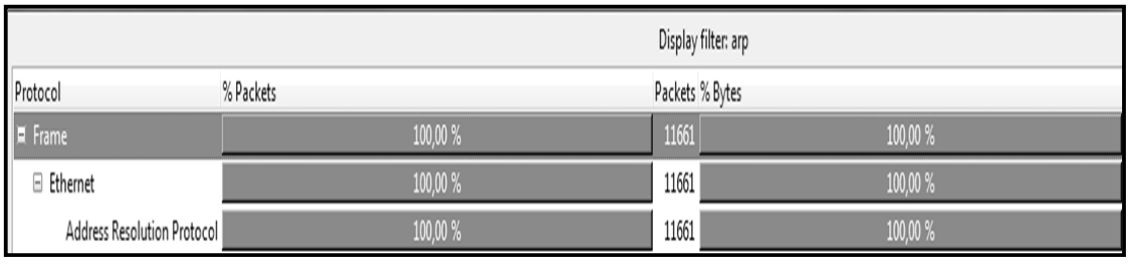

Figura 3.9 Porcentaje de paquetes ARP

- El porcentaje restante de tráfico, que es el 12.94%, corresponde a protocolos con baja presencia, tales como:

    - Protocolos de enrutamiento: SPT (Spaning Tree Protocol), el tráfico son las actualizaciones del árbol de enrutamiento, normalmente es tráfico de broadcast; e IGMP (Internet Group Management Protocol), mismo que se utiliza para conocer información sobre el estado de los routers IP que permiten multidifusión.

    - Protocolo Browser: este es un protocolo propietario de Windows. Su objetivo es almacenar los nombres NetBIOS de todas las computadoras que son parte de la red que se está analizando. NetBIOS es la especificación de una interface para acceso a servicios de red, es una parte del software que está diseñado para vincular un sistema operativo de red con un hardware.

3.4 Consideraciones de ingeniería de tráfico

La ingeniería de tráfico es una poderosa herramienta diseñada para mejorar el rendimiento de una red al manejar el flujo de tráfico de manera que no existan enlaces sobre usados o sin uso aparente. Igualmente mejora la confiabilidad de la red, al tener la capacidad de controlar el ancho de banda se puede determinar prioridades para el tráfico que va a fluir a través de la red.

El problema principal que se encuentra al manejar una red en la que no se ha aplicado ningún concepto de ingeniería de tráfico es que los datos empiezan a transportarse siempre siguiendo la misma ruta, sin tomar en cuenta las rutas alternativas que se puedan encontrar. Esto se debe a que los protocolos de enrutamiento utilizados son de tipo Vector Distancia, mismos que para seleccionar el camino a través del cual van a transportar el tráfico, realizan la elección del mismo basándose únicamente en los costos de la ruta (métricas, número de saltos) sin tomar en consideración otros elementos, tales como ancho de banda, prioridad de tráficos a transportarse, velocidad de la conexión, etc.

Esta limitación se ve más claramente en el siguiente gráfico, donde el tráfico desde los routers A y B hasta el router C viajan únicamente a través de la ruta D–E, creando de esta manera un exceso de tráfico en ese enlace, y además, dejando al enlace que pasa por el router F sin uso; es así como se crean los conocidos “cuello de botella”, que son acumulaciones de tráfico en una sola ruta.

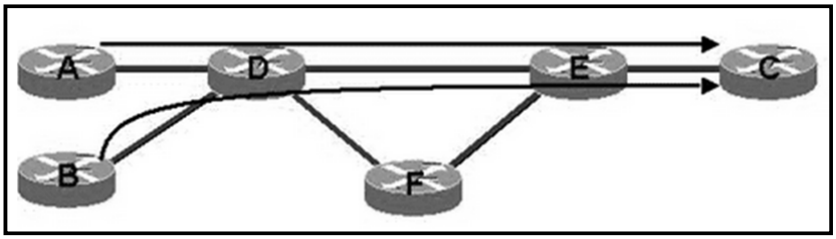

Figura 3.10 Protocolo IGP
Fuente: Cisco Packet Tracer

Para solucionar este problema se requiere de la implementación de técnicas de ingeniería de tráfico, siendo una de sus necesidades básicas la creación de caminos virtuales de extremo a extremo a través de la red, herramienta imposible de configurar en redes IP no orientadas a la conexión. Al introducir la técnica de MPLS, automáticamente se tiene la posibilidad de crear los caminos virtuales, en este caso llamados LSP.

El proceso de establecer criterios de ingeniería de tráfico en una red soportada por MPLS es conocido como MPLS TE. Esta solución junto con los conceptos de MPLS VPN proporciona varias ventajas para el estado y uso de una red.

3.4.1 Clases de servicio y Calidad de servicio (QoS)

Uno de los criterios necesarios para mejorar el rendimiento y estabilidad de una red mediante MPLS TE son las clases de servicio. El objetivo de éstas es diferenciar el tráfico que está circulando dentro de la red, y priorizar los servicios de acuerdo a las necesidades de la empresa.

Al analizar el tráfico de la red estudiada, se encuentra que la forma ideal de trabajar con los datos generados dentro de la misma sería al diferenciarla según los servicios que está prestando, y dependiendo de esto asignarla a una clase diferente. Se recomienda el uso de tres clases de servicio en esta red, siendo estas:

- En una primera clase, a la cual se le asignaría mayor prioridad, corresponde los servicios de transporte de datos propios del banco, tales como tráfico generado por las cajas de todas las sucursales y de los cajeros. Este tráfico es crítico para el funcionamiento correcto del banco, por lo tanto se necesita que sea entregado con confiabilidad y sin demoras.

- Dentro de otra clase se puede incluir al tráfico generado en tiempo real, tal como videoconferencias y llamadas de voz sobre ip, mismas que necesitan que el retardo sea mínimo, pero que pueden aceptar la pérdida de algunos paquetes-

- Luego de los servicios en tiempo real, la siguiente clase de servicio se asignaría a los servicios propios del Banco, tales como consulta de saldos por parte de los clientes en la página web, esto implica que el acceso a la base de datos general del banco debe estar activo en todo momento.

- El tráfico menos crítico se lo pude ubicar en otra categoría, siendo éste correo electrónico y transferencia de datos dentro de la red del banco, ya que no dependen de un retardo crítico para su funcionamiento, pueden permitirse una cierta demora en la entrega entre dos usuarios.

3.4.2 MPLS VPN

El uso de “túneles” para el transporte de tráfico se lo realiza mediante las conocidas VPN (Virtual Private Network), mismas que forman un circuito virtual entre dos puntos, para mantener una comunicación constante. Luego de determinar los LSP a través de los cuales va a viajar determinado tráfico se pueden crear las VPNs para la transmisión de datos. Lo importante acerca de estos túneles es que el tráfico entre, por ejemplo, dos túneles viajando por un mismo LSP, no se “ve” entre ellos. De esta manera se garantiza la seguridad y confiabilidad de los datos que se transmite, y al mismo tiempo, se aprovecha totalmente el ancho de banda disponible.

La red general del Banco del Austro tiene implementadas VPNs únicamente hacia el exterior, cada una de estas está dirigida a una sucursal del banco, en un número de alrededor quince VPNs funcionando, para de esta manera asegurar la comunicación continua entre todas las sucursales y la matriz. Toda la comunicación mediante las VPNs se realiza sobre el Internet, que es un medio no controlado por la empresa, por esto que se considera necesario implementar técnicas de codificación de datos antes de ingresar los mismos al backbone MPLS, como por ejemplo IPSec.

En la red interna de la matriz no se tiene configuradas VPNs, todo el tráfico viaja por un mismo canal, al momento no se recomendaría la creación de una VPN dentro de esta LAN ya que el volumen de tráfico existente no compensaría la creación del circuito.

3.4.3 Protocolos de transporte

Es recomendable utilizar protocolos de estado de enlace, tales como OSPF (Open Shortest Path First) o IS-IS, para que de esta manera la topología de red y la disponibilidad de uso de los recursos de la red sean conocidas por todos los nodos que forman parte de la red. En el análisis de tráfico se ha encontrado paquetes con protocolos STP e IGMP; lo más recomendable es habilitar los

protocolos indicados anteriormente, ya que STP bloquea los enlaces redundantes, dejando así ancho de banda sin usar. También otro inconveniente de STP es que en el caso de una falla en algún dispositivo se deberá esperar a que los relojes de STP se den cuenta que el enlace se ha caído y de esta manera bloquear el mismo para evitar que continúe fluyendo tráfico a través del mismo. Con OSPF se tiene a todos los enlaces activos, transmitiendo tráfico, de manera que si existiera una falla en uno de ellos no tendrá un impacto alto en la red, esto es decir que la red tiene redundancia completa.

Es necesario considerar que la red analizada corresponde a una mínima parte de la totalidad de la red del Banco del Austro S.A. En base al estudio de los endpoints de cada una de las capturas, se determina que para el tráfico Ethernet el sitio más accedido es la dirección MAC 3com_a4:1c:81, misma que corresponde al switch principal al cual está conectada esta oficina; atrás de este switch no es posible monitorear el tráfico desde el punto de red en la Jefatura de Infraestructura.

Para terminar, el uso de ingeniería de tráfico es un beneficio muy grande para las empresas que deseen implementarlo, debido a las ventajas que presenta en cuanto al manejo del ancho de banda, permitiendo determinar la manera de usarlo mediante las clases de servicio y la priorización de tráfico. Para la red en general del Banco del Austro se recomienda la implementación de MPLS VPN para la comunicación entre sucursales y diferentes oficinas, de esta manera se asegura un servicio confiable y continuo a todo momento, además de la posibilidad de administrar el ancho de banda de acuerdo a las necesidades de la empresa.

Al unir estos conceptos de ingeniería con los encontrados en el servicio MPLS, se obtiene una red con una amplia superioridad frente a sus predecesoras en términos de manejo de la velocidad, seguridad de la información a transmitirse y administración de la red. Se reduce el número de plataformas a utilizarse, ya que la tecnología MPLS soporta varias de las tecnologías anteriores, y al mismo tiempo reduce costos de operación y administración.

3.5 Resumen de capturas

Como indicado anteriormente, se realizaron tres capturas de tráfico en la red de la Jefatura de Infraestructura Agencias del Banco del Austro S.A, cada una con un diferente número de paquetes. Al realizar el análisis de cada de estas capturas se encuentra que los tipos de protocolos encontrados son similares, es por esto que se presentó una análisis completo de la captura #1; y en la siguiente tabla se establece un resumen de los porcentajes de las tres capturas

	# Paquetes Total	UDP (%)	TCP (%)	ARP (%)	Otros (1) (%)
Captura #1	41428	53,86	5,05	28,15	12,94
Captura #2	17342	56,15	2,59	30,21	11,05
Captura #3	30569	55,80	2,73	24,93	16,54

Otros (1)	STP
	Browser

Tabla 3.1 Resumen general de capturas

Cada una de las capturas tiene un número diferente de paquetes, debido a la longitud de tiempo que fueron tomadas y la cantidad de tráfico fluyendo al momento de las mismas. Se observa que, pese a la diferencia en el número de paquetes capturados, los porcentajes se mantienen constantes, con poca variación dependiendo de las capturas. Esto indica que el tráfico en la red analizada es constante, siendo el servicio más utilizado el de voz sobre Ip. A continuación, en la siguiente tabla, se realiza un resumen de la cantidad de paquetes y porcentajes de los mismos al analizar el tráfico UDP encontrado, mediante estos tráficos se concluyó sobre el servicio más utilizado, ya que los porcentajes más altos pertenecen al tráfico RTP, estando estos porcentajes sobre el 95% del total de paquetes UDP.

	# Paquetes Total	RTP (%)	RTP Event (%)	Otros (2) (%)
Captura #1	22313	96,55	1,13	2,4
Captura #2	9737	96,21	0,56	3,25
Captura #3	17057	97,11	0,78	2,11

Otros (2)	MPEG-1 JPEG G.723.1 H.261 H.263

Tabla 3.2 Resumen de paquetes UDP

CAPITULO IV

VENTAJAS DE MPLS SOBRE UN ESQUEMA DE ARQUITECTURA DE RED CONVENCIONAL

4.1 Consideraciones Generales

A lo largo de los capítulos anteriores, se ha mostrado las grandes ventajas que presentaban las tecnologías convencionales de red para transmisión y transporte de datos, algunas de las cuales todavía siguen en uso, especialmente en redes intranet que funcionan al interior de empresas para la comunicación y transporte de datos dentro de la misma.

Pero, al mismo tiempo que se tienen todas estas ventajas, también se ha mostrado que, a pesar de los beneficios que pueden ofrecer dichas tecnologías, también pueden presentan grandes y variados problemas y desventajas al momento de ser aplicadas y de trabajar sobre ellas.

También se ha analizado una nueva técnica para transmisión de datos, llamada Multi Protocol Label Switching (MPLS), misma que ofrece una gran cantidad de beneficios para los usuarios de la red como para las empresas proveedoras de los servicios de Internet.

Por esto, teniendo en cuenta tanto los beneficios como las desventajas que presentan cada una de estas tecnologías se puede realizar un análisis comparativo con la técnica MPLS, obteniendo las siguientes conclusiones:

En el caso de tecnologías como SDH o TDM, la mayor dificultad que se encuentra al migrar a MPLS es que se debe hacer un cambio total de los equipos que ya están

instalados en la red, ya que estos no soportan las características necesarias para trabajar con MPLS. Además, tanto PDH como SDH son redes 2G, mismas que soportan casi en su totalidad tráfico de voz, y en la actualidad todas las redes son orientadas a prestar y transportar servicios de voz, video y datos; algo que MPLS lo hace en su totalidad.

Frame Relay y ATM son las redes más usadas antes de la llegada de MPLS, por lo tanto son las que se han estado, y están reemplazando en los últimos años. A continuación se presentará las ventajas de aplicar la tecnología MPLS sobre estas dos tecnologías de transmisión de tráfico de red.

4.2 Frame Relay vs. MPLS

Frame Relay es una tecnología ampliamente usada por las empresas que proveen servicios de telecomunicaciones, aunque tiene varias ventajas, como el disponer de una velocidad de hasta 1.5 Mbps o que un solo puerto serial en la oficina central puede dar soporte a múltiples PVCs. Al mismo tiempo posee varias limitaciones, mismas que en gran medida pueden llegar a ser cumplidas por el servicio de MPLS.

Entre estas limitaciones se tiene:

1. Frame Relay no maneja Calidad de Servicio (QoS), por lo tanto todo el tráfico que cursa su red es tratado de la misma manera, sin importar que clase de tráfico sea. Mientras que en MPLS se puede aplicar conceptos de Calidad de Servicio a lo largo de la red, de esta manera se determina que aplicaciones o servicios son las que necesitan prioridad durante el transporte de los datos, entonces se puede determinar el LSP más apropiado para estos paquetes, y tendrán prioridad sobre cualquier otro paquete de datos que esté ingresando a la red. Además es la única tecnología que maneja Calidad de Servicio.

2. En el caso de Frame Relay, el proveedor de servicios garantiza una mínima parte del ancho de banda, el CIR (Commited Information Rate). Se puede trabajar sobre este límite CIR, pero en casos de congestión en la red, los

primeros paquetes en ser descartados son los que estén sobre el CIR. En MPLS se puede dividir el ancho de banda en Clases de Servicio, de esta manera el servicio se adapta a las necesidades del usuario. Por ejemplo, para las aplicaciones más críticas, que requieren ancho de banda constante (como videoconferencias), se les asigna una clase con mayor prioridad, donde se tenga bajo retardo en la comunicación y además el ancho de banda asignado no será compartido con otras aplicaciones; así mismo, otra clase de servicio se puede diseñar para tráfico de datos, mismo que no tiene una prioridad tan alta, en este caso el ancho de banda es el resultado del ancho de banda total contratado menos el asignado para las clases de prioridad alta

3. Comúnmente a Frame Relay se lo configura como una red “hub and spoke” (topología de estrella). MPLS puede implementarse sobre cualquier topología física de red, ya sea esta de malla completa, de malla parcial o la propia de MPLS. Esta proporciona el mejor enrutamiento entre los puntos a comunicarse. (Hipólito Jean)

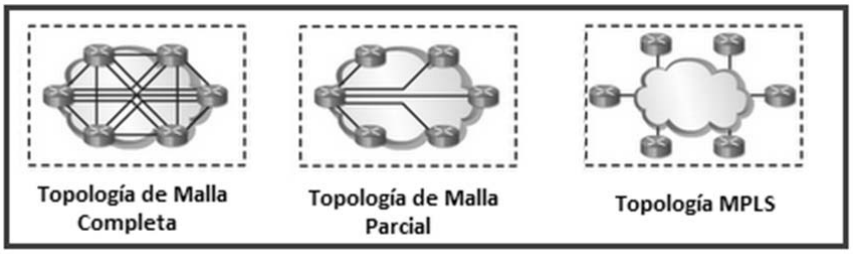

Figura 4.1 Topologías de Red

Fuente: http://itt-technology.blogspot.com/2010/10/funcionamiento-de-mpls.html

4.3 ATM vs. MPLS

La mayor similitud que presentan estas dos tecnologías es que ambas prestan el servicio de transporte de datos mediante una red orientada a la conexión, esto quiere decir que las dos conexiones tienen señalizados sus puntos de comienzo y final, que

la conexión se mantiene entre cada uno de los nodos involucrados en la comunicación y que los datos a transmitirse son encapsulados mediante diferentes técnicas antes de ser enviados.

En cuanto a las diferencias, y al mismo tiempo grandes ventajas que MPLS presenta sobre ATM tenemos:

1. **Encapsulación:** Mientras ATM trabaja con paquetes de tamaño fijo (53 bytes), MPLS puede transportar paquetes de cualquier tamaño, sin restricciones al respecto. Para transportar paquetes más grandes, ATM debe primero segmentarlos de manera que cumplan con las exigencias de tamaño que tiene este protocolo, y luego de transportarlos, unir nuevamente todas las partes en su destino, para lo cual necesita de una capa de adaptación, lo que significa más complicaciones en el transporte y que el flujo de datos se vuelva más pesado. Por otro lado, MPLS únicamente añade una etiqueta a la cabecera de cada paquete y lo transmite a través de la red.

2. **Conexiones:** Las conexiones punto a punto de ATM, o circuitos virtuales, son bidireccionales, esto quiere decir que en el mismo camino están transitando los datos de ida y regreso, lo que lleva a la formación de cuellos de botella y acumulación de tráfico en un solo punto. En cambio, las conexiones de MPLS, llamadas LSP son unidireccionales, lo que significa que los datos fluyen en un solo sentido entre dos conexiones puntuales. Para establecer una comunicación de dos vías (ida y vuelta) es necesario establecer dos LSP, mismos que no necesariamente van a seguir el mismo camino, lo que implica que el tráfico que está viajando en un sentido no siempre va a viajar por el mismo camino que el tráfico de regreso. Esto es un gran beneficio ya que de esta manera el tráfico se puede balancear a través de toda la red y evitar congestionamientos en algunos sectores de la misma.

3. **Túneles:** las dos tecnologías soportan la utilización de túneles para transportar los datos, cada una basada en una técnica diferente. ATM utiliza los circuitos virtuales, donde el indicador de camino virtual (VPI) y el indicador de circuito virtual (VCI) son transportados junto a la cabecera de la celda, de esta manera limitando el funcionamiento de ATM a un solo nivel de túneles. Al contrario MPLS utiliza el apilamiento de etiquetas, mediante lo que puede crear túneles dentro de túneles, y de esta manera mejorar la transmisión y la seguridad de los datos que están viajando en la red.

4. Finalmente, la ventaja más grande que MPLS presenta sobre ATM es el hecho que fue diseñada para trabajar junto con la tecnología IP. Originalmente los routers ATM son incompatibles con MPLS, y requieren de gran trabajo e inversión para lograr su compatibilidad, problema que no se encuentra con los nuevos routers, ya que estos tienen la capacidad de soportar MPLS e IP en un mismo puerto, de esta manera se obtiene una gran flexibilidad al momento de diseñar y operar estas redes.

4.4 Protocolo IP vs. MPLS

En una red tradicional IP el enrutamiento se realiza mediante la búsqueda en las tablas de enrutamiento en cada router por donde va a transitar el paquete. Hacia donde se envía el paquete es una decisión únicamente de dicho router. Al contrario, al utilizar MPLS se reduce el número de búsquedas en las tablas de enrutamiento, ya que las rutas están marcadas por el LSP, y además en cada router lo único que se toma en cuenta es la etiqueta. Esta característica de MPLS permite el transporte de datos sin la necesidad de trabajar con un solo protocolo de enrutamiento en cada router.

Otra técnica para transportar datos en una red IP es mediante túneles, el objetivo de estos es crear un “enlace” entre dos puntos, con la finalidad de que parezcan estar conectados permanentemente, q pesar de que IP es una tecnología no orientada a la

conexión. Lo que se crea es unas “tuberías” privadas, y por estas se envía únicamente el tráfico designado para esa IP VPN. Presentan varias desventajas, entre ellas que la configuración es manual, la gestión es complicada, ya que al introducir una nueva conexión es necesario alterar todas las ya existentes y la QoS es posible, pero no a lo largo de todo el enlace. Para suplantar esto se puede fácilmente utilizar la técnica MPLS, ya que evita la complejidad de los túneles, y además, al ampliar la red, esta conexión afecta únicamente a un router. Y finalmente, permite garantizar la QoS en todo el enlace, y tiene los beneficios de la Ingeniería de Trafico

4.5 Ventajas de MPLS

Como ya se ha estudiado, MPLS es una técnica para transporte de paquetes de datos muy eficiente, principalmente debido a su capacidad para transportar diferentes protocolos, tales como Frame Relay, ATM y Ethernet. Esta es la razón por la cual en los últimos años esta tecnología ha empezado a dominar el mercado de las redes de telecomunicaciones; la mayoría de proveedores de servicios de red alrededor del mundo ya han migrado, o están en proceso de migración hacia esta red. La fortaleza de MPLS, que es la convergencia de las otras técnicas sobre un mismo camino se debe al sistema de “etiquetado” de paquetes en el que se basa, ya que cualquier paquete, al ingresar a esta red, únicamente se transporta basado en los parámetros de su etiqueta, esto es lo que lee cada router para enviar el paquete hacia el siguiente salto, no hay necesidad de tomar en cuenta cualquier otra característica, como las cabeceras de celda o trama, para continuar con el transporte.

Se tiene también el hecho que MPLS, además de su técnica de encapsulado mediante etiquetas, utiliza protocolos de señalización, que son necesarios para descubrir los LSR que están en la red, configurar y administrar las conexiones necesarias. Estos protocolos de señalización pueden ser tres: LDP (Label Distribution Protocol), CR-LDP (Constraint-Based Routed Label Distribution Protocol) y RSVP-TE (Reservation Protocol Traffic Engineering). Las características básicas de LDP es que conecta directamente entre un LSR o LER para de esta manera realizar un intercambio de información sobre las etiquetas; la desventaja se encuentra en que este protocolo de señalización signa las etiquetas en cada salto, de manera que no se

puede determinar QoS a lo largo de toda la conexión. Esta dificultad se resuelve con CD-LDP, que es un modo de enrutamiento basado en las restricciones, ya sean estas de camino a seguir el paquete, de QoS, o cualquier otra restricción aplicada a la red; así que en este caso la distribución de etiquetas es de extremo a extremo del LSP, con lo que se asegura QoS en todo el enlace, mismo que es definido a partir de las clases de servicio.

El tercer tipo de señalización es RSVP-TE, éste ocupa datagramas IP y UDP para realizar la comunicación entre LSRs y LERs, se asemeja a CD-LDP ya que también trabaja de extremo a extremo del enlace, pero se diferencia en que la QoS es definida por la prioridad del flujo (IntServ), y que, debido a su uso de UDP, es necesario actualizar periódicamente el estado de cada uno de los LSP para asegurarse que los paquetes no se estén perdiendo en el camino, o que un LER se haya caído y se esté perdiendo toda esa información.

Gracias a la flexibilidad que tiene MPLS no obliga a utilizar uno de estos protocolos, sino que la elección depende de las necesidades del usuario y de las características de Ingeniería de Tráfico requeridas para cada caso. En adición a estos protocolos de señalización, MPLS también utiliza protocolos de resistencia, tales como Fast Re-route o Bi-directional Fault Detection, su función es determinar fallas en la red, para de esta manera enviar el tráfico a enlaces de reserva.

Gracias a todas estas características y a la popularidad que ha ganado MPLS en los últimos años, se ha convertido en la primera opción para la migración de redes, esto se debe también a su capacidad de escalabilidad y la gran flexibilidad que presenta para adaptarse a nuevas topologías de red o a ampliaciones de la misma. Los proveedores de hardware han creado routers MPLS con puertos capaces de soportar las tecnologías en proceso de cambio.

Otra gran ventaja que presta MPLS es la reducción de costos de los servicios de telecomunicaciones debido a la convergencia de las redes de datos, ya que en una sola infraestructura se pueden transportar diferentes tecnologías (Frame Relay, ATM, Ethernet e IP), reduciendo así los costos de inversión en equipos, y los costos de operación de dichas redes, pudiendo ser esta reducción hasta de un 40% comparado

con los costos necesarios para una red Frame Relay (Shop for Bandwith). MPLS logra esta reducción de costos debido a su capacidad de integrar la entrega de múltiples servicios a través de un backbone común. Esta integración permite a los proveedores de servicios de red ofrecer mejores planes, con características mucho más precisas para las necesidades de cada cliente, y de esta manera incrementar las ganancias para la empresa al reducir la inversión en equipos diferentes para cada tecnología y los costos de operación de cada una de estas se ven todo reducidas a una sola red.

MPLS combina en una sola red las capacidades para manejar tráfico y múltiples servicios de ATM con la escalabilidad presente en las redes que manejan paquetes, para de esta manera crear la mejor tecnología para transporte de datos para un proveedor de servicios. En la figura a continuación se puede observar la manera en que las diferentes tecnologías para transmision de datos pueden converger en una sola: MPLS.

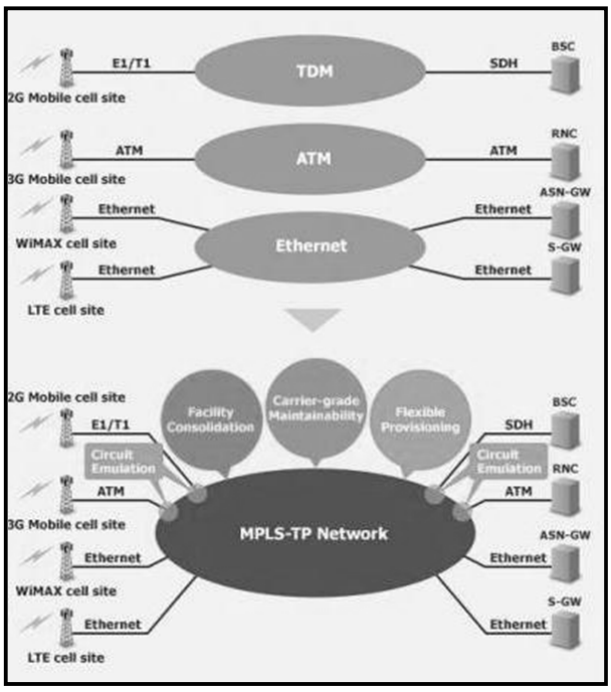

Figura 4.2 Convergencia de protocolos en MPLS

Fuente: IP Backhaul para redes móviles; Manuel Nakamurakare Higa, Diego Narvaez de la Fuente y Andrew Ramos Castellanos; http://blog.pucp.edu.pe/item/79314/ip-backhaul-para-redes-moviles

4.6 Tablas de resumen de ventajas de MPLS.

Frame Relay	MPLS
	Maneja QoS, por lo tanto el tráfico puede priorizarse
Garantizada mínima parte del ancho de banda (CIR)	Con las clases de servicio, el ancho de banda puede ser dividido de acuerdo a las necesidades
Topología “hub and spoke”	Cualquier topología

Tabla 4.1 Frame Relay vs. MPLS

ATM	MPLS
Paquetes de tamaño fijo (53 bytes)	Puede transportar paquetes de cualquier tamaño
Conexiones bidireccionales, lo que provoca acumulación de tráfico	Conexiones unidireccionales, mejor flujo de tráfico (LSP)
Un solo nivel de tuneles	Apilamiento de etiquetas, por lo tanto se puede tener tuneles dentro de tuneles.
	Soporta MPLS e IP en un mismo puerto.

Tabla 4.2 ATM vs. MPLS

Protocolo IP	MPLS
Búsqueda en tablas de enrutamiento en cada router.	Se reduce el número de búsquedas debido a que se conoce el camino a recorrer (LSP)
Cada router desencapsula los paquetes para chequear la información, y en base a eso, decidir el siguiente salto.	El router únicamente revisa la etiqueta MPLS, donde se encuentra la información sobre el LSP
Se utilizan túneles, para crear un enlace entre dos puntos	No necesita túneles, el LSP forma un circuito constante.
	Garantiza QoS y beneficios de Ingeniería de tráfico

Tabla 4.3 Protocolo IP vs. MPLS

CONCLUSIONES Y RECOMENDACIONES

Luego de realizado y analizado el presente documento, se presentan los siguientes criterios:

- La ventaja principal que ofrece la tecnología MPLS es la posibilidad de convergencia con otras técnicas de transmisión de datos, todo sobre una misma ruta. Esto se debe a su sistema de asignación de etiquetas a cada paquete que ingresa en la red; para la conmutación de los mismos lo único necesario es la información que contiene la etiqueta, ya no se tiene que revisar otras características como tramas o cabeceras, de esta manera se obtiene un considerable aumento en la velocidad de la red y conmutación de los paquetes.

- MPLS combina perfectamente las capacidades de transporte de datos de la capa de enlace de datos (capa 2) con la tecnología de ruteo IP de la capa de red (capa 3); es por esto que se le conoce como un protocolo de capa 2.5, ya que funciona entre estas dos capas.

- Al aplicar esta técnica es posible aplicar criterios de ingeniería de tráfico, calidad y clases de servicio, para de esta manera mejorar el rendimiento de una red, al administrar de mejor manera los anchos de banda y priorizar tráficos de acuerdo a la necesidad del usuario.

- Al tener una topología “muchos a muchos” en los servicios MPLS, es posible reducir el número de saltos entre routers, obteniendo así mejoramiento en los tiempos de respuesta de las aplicaciones y en el rendimiento de las mismas.

BIBLIOGRAFIA

Referencias bibliograficas

- DE GHEIN, Luc (2006), MPLS Fundamentals, Pearson Education.

- LUSA, J. M. (1999), ATM Networks Foster Convergence.

- PEPENJALK, Ivan, GUICHARD, Jim (2000), MPLS and VPN Architectures, CiscoPress.

Referencias electrónicas

- CISCO COMPANY (2006), Internetworking Technology Handbook. Class of Services.

- CISCO COMPANY, Guide to ATM technology, Septiembre de 2011, http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/12_1/pereg_1/atm_tech/techgd.pdf

- CISCO COMPANY, MPLS FAQ for Beginners, Agosto de 2011, http://www.cisco.com/en/US/tech/tk436/tk428/technologies_q_and_a_item09186a00800949e5.shtml

- CISCO NETWORKING ACADEMY (2003). Glosario CCNA v4.0. Definición.

- CISCO NETWORKING ACADEMY, (2003), Curriculo CCNA 1. Capas del modelo OSI

- HDLC: High-Level Data Link Control. (2003). Definición.

- HIPOLITO, Jean, Funciomaniento de MPLS, Agosto de 2011, http://itt-technology.blogspot.com/2010/10/funcionamiento-de-mpls.html

- METASWITCH,Network Technologies, Noviembre de 2011,http://www.metaswitch.com/mpls/what-is-mpls-and-gmpls.aspx

- Microsoft TechNet, ATM Model, Julio de 2011, http://technet.microsoft.com/en-us/library/cc976959.aspx

- Redes ATM. Conceptos, circuitos, arquitectura y conmutadores, Agosto de 2011,http://www.infcr.uclm.es/www/edguez/rap_0506/Transparencias/ATM_parte1.pdf

- Shop for Bandwith. Agosto de 2011, http://www.shopforbandwidth.com/mpls-vs-frame-relay.php

ANEXO

BANCO DEL AUSTRO
banco de apoyo

Yo, Sergio Bermeo C., Jefe de Infraestructura Agencias el Banco del Austro S.A.

CERTIFICA

Que, la Señorita **ALEXANDRA ELIZABETH BERMEO ARPI**, portadora de la cédula de ciudadanía 0104158423, realizó captura y mediciones de tráfico, como parte de su trabajo final de grado, en la Oficina de la Jefatura de Infraestructura de Agencias del Banco del Austro S.A., los días jueves 10 y viernes 11 de noviembre del presente año en horario de 09h00 a 13h00.

El presente certificado se emite para fines educativos.

Cuenca, 23 de noviembre de 2011.

Atentamente,

Sergio Bermeo C.
Jefe Nacional de Infraestructura Agencias.
BANCO DEL AUSTRO S.A.