

**UNIVERSIDAD NACIONAL DE INGENIERÍA**  
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**“CALIDAD DE SERVICIO EN REDES IP-VPN MPLS”**

**INFORME DE SUFICIENCIA**

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO ELECTRÓNICO**

PRESENTADO POR:

**JORGE ISAÍAS NAVARRO GAMARRA**

PROMOCIÓN 1994 - I  
LIMA – PERÚ  
2003

A mis padres por su apoyo.  
A mi alma mater por sus enseñanzas.

## SUMARIO

La globalización de la actividad económica y la apertura del mercado de las telecomunicaciones ha traído como consecuencia la disminución de la lealtad de los clientes, los que enfrentados a una enorme variedad de ofertas de servicios que a primera vista no se diferencian entre ellos, se han transformado en un mercado exigente que responde enérgicamente a la **Calidad del Servicio (QoS)** recibido.

Dada ésta situación, en el ámbito de las telecomunicaciones, la QoS se ha convertido en un asunto prioritario de todos los proveedores de servicios de comunicaciones, más aún cuando el tráfico de voz, imágenes y datos convergen en una sola red de comunicaciones.

En éste entorno, se debe recurrir a tecnologías de la QoS, que proporcionarán los bloques elementales que se usarán para las aplicaciones de los negocios actuales y futuros que corren sobre las redes de comunicaciones.

En éste informe se detallará los principios básicos y necesarios para diseñar una red de comunicaciones con QoS, sobre tecnologías emergentes como el MPLS, dado que en la actualidad los equipos que combinan el switching y el routing están tomando una relevancia creciente y los grandes Carries de Telecomunicaciones del mundo están optando por esta tecnología para brindar sus servicios de conectividad y valor añadido.

## **CALIDAD DE SERVICIOS EN REDES IP – VPN MPLS**

## ÍNDICE

<b>INTRODUCCIÓN</b> .....	1
<b>CAPITULO I</b> .....	11
<b>CALIDAD DE SERVICIO - QoS</b> .....	11
1.1 Foros ATM y Frame Relay .....	12
1.2 IEEE .....	12
1.3 IETF .....	13
<b>CAPITULO II</b> .....	15
<b>HERRAMIENTAS DE CALIDAD DE SERVICIO</b> .....	15
2.1 Clasificación y certificación .....	15
2.2 Impedimento de la congestión .....	15
2.3 Administración de la congestión .....	15
2.4 Condiciones del tráfico .....	16
2.5 Señalización .....	16
2.6 Mecanismos de eficiencia de los enlaces .....	17
<b>CAPITULO III</b> .....	18
<b>IMPLEMENTACIÓN DE LA CALIDAD DE SERVICIO</b> .....	18
3.1 Implementación en las Aplicaciones .....	19
3.2 Implementación en las Estaciones de Trabajo .....	19
3.3 Implementación en el Equipo .....	19
3.4 Clasificación .....	20
3.5 Formateo del Tráfico Entrante y Saliente .....	21

3.6	Gestión de Colas .....	21
3.7	Marcajes de la QoS .....	22
3.8	Implementación en la Administración de la Red .....	22
<b>CAPITULO IV .....</b>		<b>23</b>
<b>CALIDAD DE SERVICIO EN REDES I .....</b>		<b>23</b>
<b>CAPITULO V .....</b>		<b>25</b>
<b>APLICACIÓN PRACTICA DE QoS EN UNA RED CORPORATIVA.....</b>		<b>25</b>
5.1	Objetivos.....	25
5.2	Proceso de Diseño de Redes con Calidad de Servicio .....	26
5.3	Auditoria de la Red Actual .....	27
5.4	Toma de Requerimientos de Comunicaciones .....	28
5.5	Objetivos del Diseño de Red .....	29
5.6.1	Revisión de Tecnologías y Servicios .....	30
6.6.1	Evolución hacia una Red IP - MPLS.....	30
5.6.2	Convergencia del IP sobre ATM.....	31
5.6.3	Ventajas de la Arquitectura IP sobre ATM.....	34
5.6.4	Desventajas de la Arquitectura IP sobre ATM.....	35
5.6.5	Convergencia hacia IP: Conmutación IP .....	36
<b>CAPITULO VI.....</b>		<b>40</b>
<b>CONMUTACIÓN MULTINIVEL MPLS .....</b>		<b>40</b>
6.1	Objetivos Principales del Estándar MPLS .....	40
6.2	Descripción funcional del MPLS .....	41
6.2.1	Funcionamiento del Envío de Paquetes en MPLS .....	42
6.2.2	Control de la información en MPLS .....	47

<b>CAPITULO VII</b> .....	50
<b>LINEAMIENTOS TÉCNICOS DEL DISEÑO</b> .....	50
7.1 Calidad de Servicio en el Borde de la Red WAN.....	50
7.1.1 Clasificación de los Paquetes.....	50
7.1.2 Asignación de la Tasa de Acceso.....	51
7.1.3 Evitar la Congestión y Probabilidad de Pérdida.....	52
7.1.4 Enrutamiento basado en normativas .....	52
7.2 Calidad de Servicio en el Backbone de la Red WAN .....	53
7.2.1 Tráfico en espera y programado.....	53
7.2.2 Núcleos Frame Relay y ATM.....	55
7.2.3 Conmutación de etiquetas multiprotocolo.....	55
7.3 Implementación del Sistema de Contingencia.....	56
7.3.1 Plan de Sistemas.....	56
7.3.2 Plan de Comunicaciones .....	57
7.3.3 Factores que afectan la disponibilidad de red .....	57
7.3.4 Alternativas ante Contingencias .....	59
7.4 Estrategia de la Gestión de la Red .....	59
7.4.1 Gestión básica.....	59
7.4.2 Gestión VIP .....	60
<b>CAPITULO VIII</b> .....	61
<b>RESPONSABILIDADES DEL PROVEEDOR Y CLIENTE</b> .....	61
8.1 Responsabilidades del proveedor .....	61
8.2 Responsabilidades del cliente .....	62
<b>CONCLUSIONES</b> .....	63

<b>GLOSARIO</b> .....	66
<b>BIBLIOGRAFÍA</b> .....	74



## INTRODUCCIÓN

La Calidad de Servicio hoy en día se ha convertido en una función indispensable para muchos de los grandes Proveedores de Servicios de Red y Servicios de Valor Añadido, debido a la gran diversidad de necesidades y exigencias de los Clientes.

Los sistemas informáticos actuales se suelen basar en una red de datos, a la cual se pide que soporte cada vez más, una amplia gama de aplicaciones. El Protocolo Internet (IP) utilizado en las redes de datos durante los últimos 30 años para intercambiar datos entre ordenadores de diferentes fabricantes, se ha convertido, después de sucesivas mejoras, en el protocolo más utilizado.

El desarrollo actual de las redes se está enfocando hacia la Calidad de Servicio (QoS), la cual se requiere para permitir que los diferentes tipos de información se transporten con distintas prioridades. El objetivo es prevenir que la congestión no llegue a ser un problema crítico en aplicaciones sensibles a los retrasos, tales como la transmisión de voz y video.

Existen dos formas de cumplir con este objetivo:

- Entrar en la carrera de la velocidad de conmutación y del ancho de banda. Esto implica una inversión a largo plazo para asegurar que el rendimiento de la red se mantenga a pesar de los constantes cambios. Este método puede llegar a ser muy costoso.

- Gestionar inteligentemente el ancho de banda disponible, compartiéndolo de forma desigual o adaptando el tráfico de una aplicación a la fuente. No obstante, las redes y protocolos IP son independientes de las aplicaciones que transportan: No distinguen entre aplicaciones de ocio (por ejemplo, navegar en Internet) y aplicaciones críticas (por ejemplo, recoger un pedido utilizando SAP) Esto requiere que las funciones QoS sepan reconocer las aplicaciones y asignarles la prioridad deseada.

En los siguientes capítulos, la Calidad de Servicio en Redes IP-VPN MPLS, es enfocada desde la fase de Diseño de una Red y su posterior Implantación, considerando para ello los lineamientos técnicos necesarios y gestión personalizada para su óptima puesta en operación. Con la finalidad de formular los criterios básicos de diseño e implementación de redes de comunicaciones basadas en un Backbone IP-MPLS, a través de la cual se brinde no sólo la conectividad full mesh, sino también la convergencia de servicios de voz, datos y video sobre una misma plataforma garantizando Calidad de Servicio de extremo a extremo.

## **CAPITULO I CALIDAD DE SERVICIO - QoS**

La capacidad de garantizar Calidad de Servicio (QoS) a cada una de las aplicaciones, es quizás la característica más relevante de las tecnologías de redes última generación. Para poder satisfacer los requerimientos específicos de cada aplicación, la red debe implementar una serie de mecanismos destinados al control de tráfico y a la administración de los recursos de la red.

Dadas éstas características, para acercarnos a una definición de QoS, recurriremos a la recomendación de ITU-T donde se define QoS como “El efecto integral del funcionamiento de la red de servicios, el cual se determina por el grado de satisfacción del usuario final del servicio”. Este grado de satisfacción se puede expresar directa o indirectamente a través de algunas de las siguientes medidas cuantitativas:

- El retardo(delay) de extremo a extremo.
- Variación del retardo o jitter.
- El throughput.

Tener en cuenta que para brindar Calidad de Servicio debemos utilizar solamente esquemas estándar, para ello debemos revisar las recomendaciones elaboradas por las organizaciones que elaboran las especificaciones técnicas de QoS, tales como ATM Forum, Frame Relay

Forum, Institute of Electrical and Electronics Engineers (IEEE) e Internet Engineering Task Force (IETF):

### **1.1 Foros ATM y Frame Relay**

En el caso de redes ATM y Frame Relay con Calidad de Servicio, la QoS se implementa configurando parámetros tales como:

- Ancho de Banda garantizado.
- Pico de Ancho de Banda.
- Retrasos.
- Disponibilidad, entre otros.

Y definiendo canales virtuales que no tienen en cuenta la importancia del tráfico transportado. Los elementos de red (terminales, centrales, Routers, etc.) aseguran que el canal utilizado tiene suficientes recursos para transportar las aplicaciones.

### **1.2 IEEE**

Los estándares 802.x se aplican principalmente a Redes de Área Local (LAN), tales como ethernet, Token Ring y Fiber Distributed Data Interface (FDDI). El estándar 802.1Q/P indica como un elemento de red puede clasificar el tráfico de nivel 2 para asignarle una prioridad. Para cumplir esto, se ha definido un nuevo formato de trama que utiliza 12 bits para designar las Redes Virtuales de Área Local (VLAN) y 3 bits (u 8 niveles) para clasificar las tramas.

Las estaciones de trabajo, servidores, Routers y centrales pueden enviar o modificar una trama con uno de esos ocho valores. Este nuevo formato de trama requiere una tarjeta de interfaz específica.

### 1.3 IETF

El IETF trabaja con la especificación de la capa 3 de OSI, y en concreto sobre IP. Se pueden distinguir cuatro categorías principales de QoS:

- Marcado.
- Reserva dinámica de recursos.
- Etiquetado.
- Seguimiento.

**Marcado**, es la técnica que consiste en insertar información de prioridad de red en cada trama utilizando el campo Tipo de Servicio (ToS). La definición del ToS hace posible pedir que la red utilice simultáneamente el coste más bajo, el tránsito más rápido y el máximo ancho de banda.

Dado las diferentes variables que se puede utilizar para asignar una prioridad y los posibles conflictos que esto podría ocasionar, se ha creado una nueva definición de Servicios Diferenciados (DiffServ) basada en comportamientos estándar, las cuales pueden clasificarse en tres (03) categorías, tales como:

- Envío de datos acelerado para aplicaciones sensibles a los retardos,
- Envío de datos asegurado para aplicaciones que requieren un ancho de banda garantizado,
- Y mejor esfuerzo para el resto.

**Reserva dinámica de recursos**, mejor conocida por la sigla RSVP (Resource reSerVation Protocol), es un protocolo de señalización la cual consiste en una petición de reserva que utiliza las tablas estándar de

enrutamiento. No es posible suministrar ancho de banda a un canal cuando se utiliza enrutamiento dinámico.

Los recursos sólo se reservan después de que el destino ha dado su acuerdo. Esta reserva se mantiene mediante un dialogo de control.

**Etiquetado**, conocido por la sigla MPLS (Multi-Protocol Label Switching), permite al equipo enviar cualquier tipo de tráfico (IP, IPX, Decnet, etc.) con una etiqueta común al mismo puerto de salida. MPLS utiliza tablas sincronizadas con las tablas de enrutamiento.

## **CAPITULO II HERRAMIENTAS DE CALIDAD DE SERVICIO**

Las herramientas de Calidad de Servicio podemos dividirla en seis categorías principales:

### **2.1 Clasificación y certificación**

Las características de clasificación por paquetes permiten que el tráfico se divida en varios niveles de prioridad o clases de servicio. Los paquetes pueden clasificarse de muchas formas diferentes, desde la interfaz de entrada hasta reconocimiento de aplicaciones basadas en red, para las aplicaciones difíciles de clasificar o mediante listas de control de acceso arbitrarios.

### **2.2 Impedimento de la congestión**

El algoritmo Weighted Random Early Detection (WRED) permite evitar la congestión en las interfaces de la red al proporcionar administración de la memoria buffer y permitir que el tráfico TCP disminuya de velocidad antes de que se agote la memoria buffer. Esto ayuda a evitar caídas de cola y problemas globales de sincronización, aumentando así al máximo la utilización de la red y el rendimiento de las aplicaciones basadas en TCP.

### **2.3 Administración de la congestión**

Con frecuencia, una interfaz de la red puede encontrarse congestionada (incluso a altas velocidades se observan congestiones transitorias) y hace

falta técnicas de gestión de colas para asegurar que las aplicaciones de importancia fundamental reciben el tratamiento de envío necesario. Por ejemplo, es posible que las aplicaciones en tiempo real como VoIP, compra o venta de acciones, etc. necesiten enviarse con la menor latencia y fluctuación de fase posible (hasta un límite que se provee). Una solución para estos casos es utilizar la gestión de colas de baja latencia (LLQ), para otro tipo de tráfico que no sea sensible a los retardos (como FTP, HTTP, etc.), se puede utilizar otras técnicas de gestión de colas como CBWFQ y MDRR (Modified Deficit Round-Robin).

#### **2.4 Condiciones del tráfico**

El tráfico que entra en una red puede condicionarse mediante el uso de un normalizador o un mecanismo de formación de tráfico. Un normalizador simplemente aplica un límite de velocidad, mientras que un mecanismo de formación suaviza el flujo del tráfico a una velocidad especificada mediante la utilización de buffers. De nuevo, es posible configurar mecanismos como CAR (Tasa de acceso comprometido), GTS (Formación genérica de tráfico) y FRTS (Formación del tráfico Frame-Relay).

#### **2.5 Señalización**

En una red debe poder implementarse los diferentes modelos de aprovisionamiento de QoS, tales como el modelo IETF DiffServ [Servicios diferenciados ] con técnicas como CAR, GTS, marcación de paquetes L3, etc., como también el modelo de servicios integrados (IETF-IntServ). El protocolo RSVP (Resource Reservation Protocol) es el mecanismo principal para llevar a cabo el control de admisión de los flujos en una red.



Un ejemplo perfecto lo encontramos en el caso de VoIP (Voz a través de IP). Sólo se realiza una llamada si ésta cuenta con los recursos disponibles, lo que garantiza que una llamada que entra en una red no daña ni afecta a la calidad de las llamadas existentes. Otra técnica denominada QPPB (Propagación de normativas de QoS a través de BGP) permite la señalización indirecta (mediante el atributo de lista comunitaria de BGP) de la prioridad de envío para los paquetes destinados hacia un sistema autónomo, ruta AS o prefijo IP. Ésta es una característica de gran utilidad para los proveedores de servicios y las grandes empresas.

## **2.6 Mecanismos de eficiencia de los enlaces**

El tráfico de voz y vídeo constante usa el protocolo en tiempo real (RTP). Las cabeceras de los paquetes IP, UDP y RTP pueden comprimirse de unos 40 bytes a 5-8 bytes. De ese modo se ahorra una gran cantidad de ancho de banda en caso de enlaces de baja velocidad y cuando se admiten un gran número de flujos de medios. Además, FRF.12 (la especificación para la fragmentación de esquemas Frame-Relay Forum) permite la fragmentación de paquetes de datos de gran tamaño, intercalándolos con paquetes RTP y manteniendo el retardo y la fluctuación de fase a un nivel bajo para los flujos de medios.

## **CAPITULO III IMPLEMENTACIÓN DE LA CALIDAD DE SERVICIO**

Las especificaciones técnicas por si mismas no suministran Calidad de Servicio, sólo hacen posible la asignación de valores relativos de prioridades, no suministran una solución. La QoS sólo se puede alcanzar implementándolas de una forma coordinada las características necesarias para tal fin, en:

- La red.
- En el equipo.
- En la gestión de la red.
- En las estaciones de trabajo.
- Y en las aplicaciones.

Por analogía con el enrutamiento, que necesita la definición de un esquema de direccionamiento y el protocolo de cálculo de ruta, la implementación de la QoS requiere el acuerdo con la topología funcional y los métodos de señalización utilizados. La elección del método de señalización (802.1p, DiffServ, etc.) tiene poca importancia; sólo se tiene en cuenta la QoS esperada.

La QoS se debe elegir de acuerdo con las limitaciones de la aplicación y con las características físicas de la red, los cuales se tienen que identificar o evaluar antes de implementar la QoS. Esto permite identificar las partes de

una red que necesitan mejorarse, los cuales se pueden identificar en las siguientes partes:

### **3.1 Implementación en las Aplicaciones**

Actualmente, la mayoría de las aplicaciones ignoran la Calidad de Servicio. La próxima generación puede utilizar las nuevas Interfaces Application Programming (API) en sistemas operativos como los de Microsoft. Sin embargo, si todos los usuarios de una red piden tratamiento prioritario, puede ser imposible satisfacer sus peticiones. Por lo tanto, es necesario asegurar que las peticiones están bien fundadas, este es el papel de las funciones de supervisión.

### **3.2 Implementación en las Estaciones de Trabajo**

Las estaciones de trabajo pueden utilizar todas las técnicas de QoS. Sin embargo, sólo las nuevas interfaces de red, construidas desde principios de 1999, soportan el 802.1Q/P, así como su nuevo formato de trama. Una petición de QoS a nivel de estación de trabajo puede tener dos orígenes, o llega desde la aplicación o bien está implícita en la naturaleza de la estación de trabajo (servidor, pasarela, etc.).

### **3.3 Implementación en el Equipo**

Para implementar QoS, el equipo debe suministrar todas o alguna de las siguientes funciones:

- Clasificación;
- Formateo del tráfico entrante y saliente;
- Gestión de Colas;

- Modificación de los campos asociados a la QoS y ajuste a las tecnologías QoS;
- Conservación de la QoS mediante marcaje de los datos codificados de las cabeceras de trama cuando se implementan las Redes Privadas Virtuales (VPN);
- Mantenimiento de la QoS cuando se aplica la Traducción de Dirección de Red (NAT).
- Autenticación de la petición de reserva.

### **3.4 Clasificación**

Cuando las aplicaciones y las estaciones de trabajo no utilizan tecnologías de QoS, el equipo debe ser capaz de identificar el tipo de tráfico entrante (aplicación, usuario, destino, marcaje, etc.).

En la Figura 1 muestra las diferentes capas en las que está basada la clasificación. Las capas 1, 2, 3 del modelo se pueden usar para identificar exactamente la estación de trabajo de la red, no obstante, esta información no indica qué aplicaciones se están utilizando. Para conseguir esto, es necesario mirar detenidamente las tramas.

Como se muestra en la Figura 1 determinadas aplicaciones se pueden identificar con certeza en la capa 4 del modelo. En casos más complejos, tales como la voz y la distinción entre varios servidores de web en la misma máquina, es necesario referirse a la capa 7. Los resultados de la clasificación que se encuentran disponibles para otros módulos son: proceso de baja prioridad, garantía de ancho de banda, discriminación de servicio.

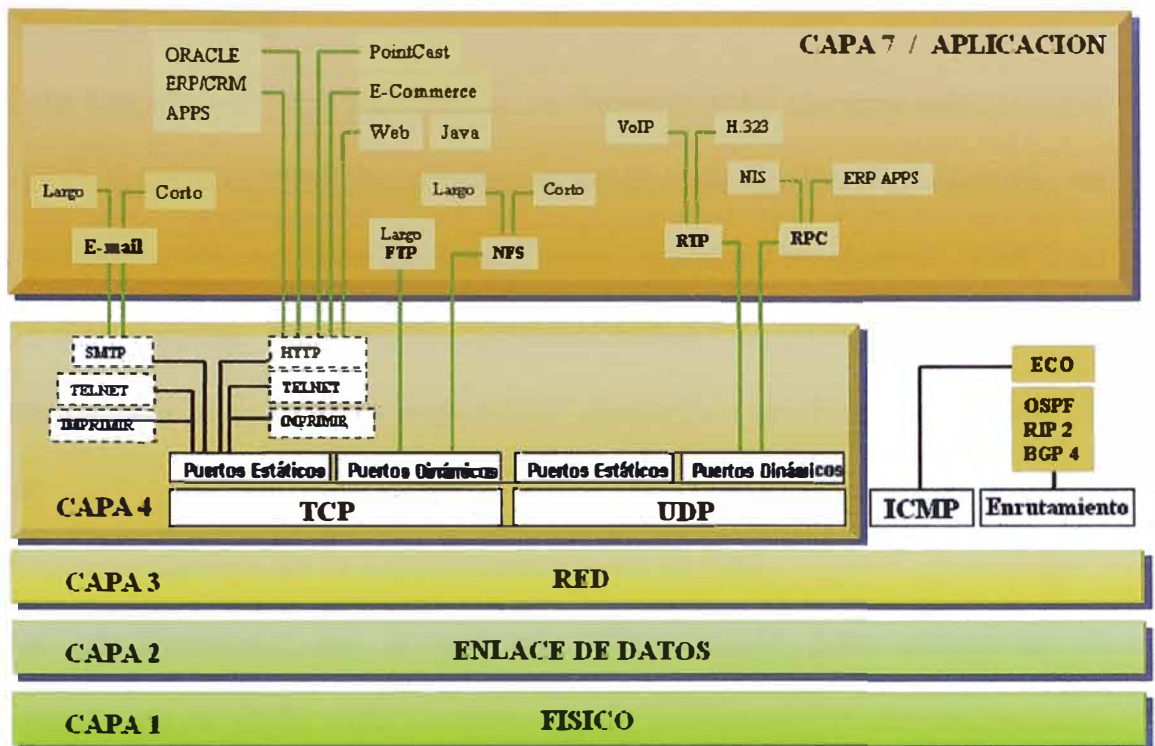


Figura 1. Clasificación del modelo de capas.

### 3.5 Formateo del Tráfico Entrante y Saliente

Se utiliza un control en la entrada para excluir cualquier tráfico que pudiese dar lugar a sobrepasar los parámetros contratados. En la salida se asegura que el tráfico se ajusta a esos parámetros, los cuales pueden relacionarse con el ancho de banda, la prioridad, etc.

### 3.6 Gestión de Colas

Esta función distribuye el tráfico a las colas de acuerdo con los resultados de la clasificación. También maneja el flujo de tráfico desde las colas a los puertos de salida de acuerdo a los principios que aseguran la QoS pedida (WFQ – Weighted Fair Queuing, FIFO – First In First Out, CBQ – Class Based Queuing, etc.). Además, en caso de desbordamiento de una cola, se implementan mecanismos de supresión de trama (WRED – Weighted Random Early Detection, RED – Random Early Detection, etc.).

### **3.7 Marcajes de QoS**

Esta función modifica los valores de determinados campos relacionados con la QoS de acuerdo a los resultados de la clasificación. Por ejemplo, en una red que utiliza equipos de nivel 2 en la periferia y equipos de nivel 3 en la red de backbone, esta función verifica el tráfico con un marcaje de nivel 3, o más sencillamente asigna la prioridad deseada a un determinado tipo de tráfico.

### **3.8 Implementación en la Administración de la Red**

La administración de la red es indispensable para simplificar el despliegue de la QoS. Esto permite que la configuración del equipo esté centralizada de forma que se reduzcan los errores originados por una configuración manual.

También proporciona gestión centralizada de la hora, por ejemplo, a un determinado tipo de tráfico sólo se le puede dar prioridad de 8 de la mañana a 5 de la tarde, de lunes a viernes. Además , sus funciones de Gestión de Nivel de Servicio, facilitan la gestión del servicio.

## **CAPITULO IV CALIDAD DE SERVICIO EN REDES IP**

Hace algunos años la pregunta “IP o ATM” llevó a intensos debates, ahora vemos que IP ha sobrevivido en el tiempo. Sin embargo la construcción de redes de backbone no ha mejorado, se sigue discutiendo sobre la función de las redes ATM y la evolución de las redes IP para soportar servicios diferenciados. Un nuevo fenómeno es la llegada de DWDM y las Redes Ópticas, ambas muy prometedoras ya que conmutan muy grandes anchos de banda sobre una única fibra. Ya hay quienes piensan que IP sobre redes ópticas ofrece todo lo necesario y que tanto el SDH como ATM quedarán pronto obsoletas.

El primer intento del IETF de especificar calidad de servicio en redes IP fue la definición del RSVP(Resource Reservation Protocol). Sin embargo, no ha sido ampliamente aceptado ya que se considera que su modularidad no es adecuada, aunque si se usa para la creación de servicios diferenciados.

Por otro lado debemos indicar, que la Calidad de Servicio (QoS) no crea ancho de banda, su función es administrarla de acuerdo a la demanda de las aplicaciones y los escenarios de gestión de red, para conseguir la Calidad de Servicio de extremo a extremo se requieren los siguientes elementos:

- Los nodos de la red han de ser capaces de garantizar la calidad de servicio.

- Existe un procedimiento para identificar una ruta entre el origen y el destino que puede ofrecer la calidad de servicio requerido.
- Existe reserva de recursos, es decir, notificar a todos los nodos que se encuentran a lo largo de la ruta que necesitan reservar los recursos para garantizar la calidad de servicio solicitado.

En tal sentido, el enfoque de muchos proveedores de servicios sobre la calidad de servicio IP, se basa en la utilización del establecimiento de la ruta explícita de MPLS, con dos elementos distintos:

- El conmutador de IP. Es el que puede ofrecer garantías de calidad de servicio a los flujos de paquetes IP de forma similar a como un conmutador de ATM que proporciona calidad de servicio a un flujo de celdas. La clasificación de paquetes, la puesta en cola de espera y la programación están implementadas en el hardware y utilizan los algoritmos más avanzados disponibles en la industria.
- Herramientas de ingeniería de tráfico con el diseñador de VPN. Este permite calcular de forma óptima encaminamiento del tráfico a través de una red basándose en requisitos de conectividad.



## **CAPITULO V**

### **APLICACIÓN PRACTICA DE QoS EN UNA RED CORPORATIVA**

#### **5.1 Objetivos**

Tradicionalmente, los proveedores de servicios ofrecen servicios básicos de transporte de datos a través de líneas dedicadas arrendadas, tales como Frame Relay, TDM, modo de transferencia asíncrona (ATM) y servicios básicos de conexión.

Sin embargo la necesidad actual de comunicaciones del gran sector empresarial, demanda una conexión refinada entre grupos de usuarios de modo Intranet y Extranet a través de toda la infraestructura pública.

Por ello los proveedores de servicios de todo el mundo están considerando las tecnologías IP VPN, como el vehículo para ofrecer servicios VPN administrados, para cumplir con los requisitos de convergencia.

Dada las condiciones planteadas el objetivo de este capítulo, es explicar los pasos a seguir para desarrollar y proponer una Plataforma de Red Corporativa de voz y datos, asegurando la Calidad de Servicio de extremo a extremo, Escalabilidad, Flexibilidad y alta performance, dirigido al sector Empresarial Público o Privado del País, a través de una Red Pública de Transmisión de Datos IP MPLS.

Es importante señalar en este punto que la Calidad de Servicio que debe ofrecer un proveedor de servicios empieza desde el primer contacto con el cliente. En el campo de las Telecomunicaciones esto se refleja con un nivel de atención personalizado y especializado, los interlocutores deben hablar y entenderse en mismos términos técnicos y económicos, a fin de viabilizar y consolidar las necesidades actuales y futuras de sus Clientes.

## **5.2 Proceso de Diseño de Redes con Calidad de Servicio**

Previo a desarrollar el diseño de una red de comunicaciones, se debe establecer un proceso de diseño que permita conocer la red actual a rediseñar o implantar, definir los objetivos y necesidades de comunicaciones, encontrar la mejor solución y tecnologías existentes, análisis de costos, etc. Para esto es conveniente dividir dicho análisis en los siguientes pasos:

- Auditoria de la Red Actual.
- Toma de requerimientos de comunicaciones.
- Objetivos del Diseño de la Red.
- Revisión de tecnologías y servicios.
- Lineamientos del diseño garantizando Calidad de Servicio de Extremo a Extremo.
  - Calidad de Servicio en la Fase de Pre-Venta.
  - Calidad de Servicio en la Fase de Venta.
  - Calidad de Servicio en la Fase de Implantación.
    - QoS en el Borde de la Red
    - QoS en el backbone de la red.
  - Y Calidad de Servicio en la fase de Post-Venta.
- Planeación de capacidad y crecimiento.

- Compromisos del Nivel de Servicio(SLA-Service Level Agreement) del proveedor.
- Responsabilidades y compromisos del Cliente.
- Análisis Financiero.

### **5.3 Auditoria de la Red Actual**

Dentro del proceso del diseño de red, este es un paso fundamental e importante para el Ingeniero de Diseño, desde el punto de vista técnico y económico. Técnicamente por que le permitirá conocer el objetivo actual de comunicaciones, su funcionalidad, tipo de aplicaciones en operación, evaluar el tráfico existente, entre otros, y, económicamente por que le permitirá evaluar los costos de operación y mantenimiento de la red actual implementada.

Los alcances que nos permitirá conocer este paso del diseño podemos listarlo de la siguiente manera:

- Conocer el parque de equipos instalados.
  - Costos de operación y mantenimiento.
  - Capacidades de hardware y software.
- Conocer los servicios y aplicaciones en producción.
- Evaluar el tráfico cursado LAN/WAN.
- Calidad de servicio implementado.
- Costos de instalación, operación y mantenimiento del servicio actual de comunicaciones.

- Proyectos futuros.

#### **5.4 Toma de Requerimientos de Comunicaciones**

En este punto es importante que el interlocutor encargado por el proveedor de servicios en un trato directo con el Cliente, previamente conozca el negocio o giro del mismo a fin de que pueda interpretar correctamente sus necesidades de comunicaciones y más aún sugerir la mejor manera de implementarlo.

En otros caso los requerimientos de comunicaciones vienen determinados e indicados en documentos que forman parte de un Concurso Público o Adjudicaciones Directas, para tomar los servicios de comunicaciones. En este caso solo queda aprovechar en la fase de consultar solicitar toda la información posible para diseñar la solución a los requerimientos indicados.

En general, se puede listar como requerimientos de comunicaciones, los que a continuación se indican:

- Implementar una Red Privada de voz y datos, que permita las funcionalidades de Intranet y Extranet.
- La plataforma de red del proveedor debe ser de última generación tecnológica, de acuerdo a las tendencias del mercado mundial.
- La red propuesta debe contemplar una gran flexibilidad y escalabilidad, debido al continuo dinamismo de los clientes.
- Garantizar un servicio de primera línea con calidad de servicio de extremo a extremo y alta disponibilidad.

- El proveedor de servicios debe tener la capacidad de implementar soluciones Globales de alcance local, nacional e internacional.
- El proveedor de servicios debe tener la capacidad y herramientas necesarias para brindar servicios de Outsourcing.
- Los servicios ofrecidos deben contemplar Niveles de acuerdos de Servicios, donde se estipulen los compromisos del proveedor y responsabilidades del cliente.

### **5.5 Objetivos del Diseño de Red**

De acuerdo a la información obtenida en los dos primeros pasos el diseño de red y en conjunto con el Cliente debe fijarse los siguientes ítem:

- Que servicios de comunicaciones deberán mantenerse de la red actual y que nuevos servicios deberán implementarse.
- Definir el conjunto de aplicaciones de uso Local (LAN) y de uso Remoto (WAN), los cuales cursarán tráfico a través de la red en desarrollo.
- Se recomienda fijar los niveles de prioridad o precedencia de los diferentes tipos de tráfico cursados por la red, de acuerdo a la criticidad para el negocio del Cliente.
- Dependiendo de la antigüedad y/o características del parque de equipos de comunicaciones instalados, se deberá recomendar cambiar o reutilizar dichos equipos.
- Cual será la cobertura del servicio, local, nacional y/o internacional.

- Acordar cual será el nivel de disponibilidad requerido para la red en desarrollo.
- Acordar el tiempo de contrato, por los servicios prestados.

Esto debe quedar claramente establecido a fin de poder fijar los entregables del proyecto y los hitos importantes durante la implantación del mismo.

Es recomendable también, indicar que no está involucrado como parte del proyecto en desarrollo, a fin de no encontrar ambigüedades o vacíos que perjudiquen la implantación del Proyecto ni la relación con el cliente.

### **5.6.1 Revisión de Tecnologías y Servicios**

En el pasado, las redes públicas solían basarse en la transmisión de jerarquía digital plesiócrona (PDH) y conmutadores de banda estrecha digitales, el resultado es que eran inflexibles con respecto a la asignación de recursos y se limitaban a cursar tipos de servicios específicos. Hoy sin embargo la revolución de las redes se ve dominada por la implementación de redes transparentes a los servicios, esta evolución va estrechamente relacionada con la introducción de las tecnologías SDH, ATM, IP, MPLS, DWDM, etc. Por consiguiente, las redes actuales y futuras se distinguirán sensiblemente de las anteriores, no sólo con respecto a su arquitectura, sino también a su modo de operación y la convergencia de servicios.

### **6.6.1 Evolución hacia una Red IP - MPLS**

Desde la década de los 90 el IP ha ido ganando terreno como protocolo de red a las arquitecturas tradicionales en uso (SNA, IPX, AppleTalk, OSI...).

Por otro lado, hay que recordar que los backbones de los proveedores habían sido contruidos sobre la base de enlaces conectados por líneas dedicadas T1/E1 y T3/E3. Sin embargo el crecimiento explosivo del tráfico de datos y del tráfico Internet han generado un déficit de ancho de banda en éste esquema de enlaces individuales.

La respuesta inmediata de los proveedores de servicios fue el incremento del número de enlaces y la capacidad de los mismos. Por otro lado plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Se pensó entonces en la convergencia de los servicios de voz datos y video sobre la misma plataforma de red, frente a este entorno había considerar la mejora de las características del backbone en cuanto a la capacidad, performance, flexibilidad, calidad de servicio, entre otros, así como idear otras alternativas de ingeniería de tráfico, respecto a los tradicionales.

### **5.6.2 Convergencia del IP sobre ATM**

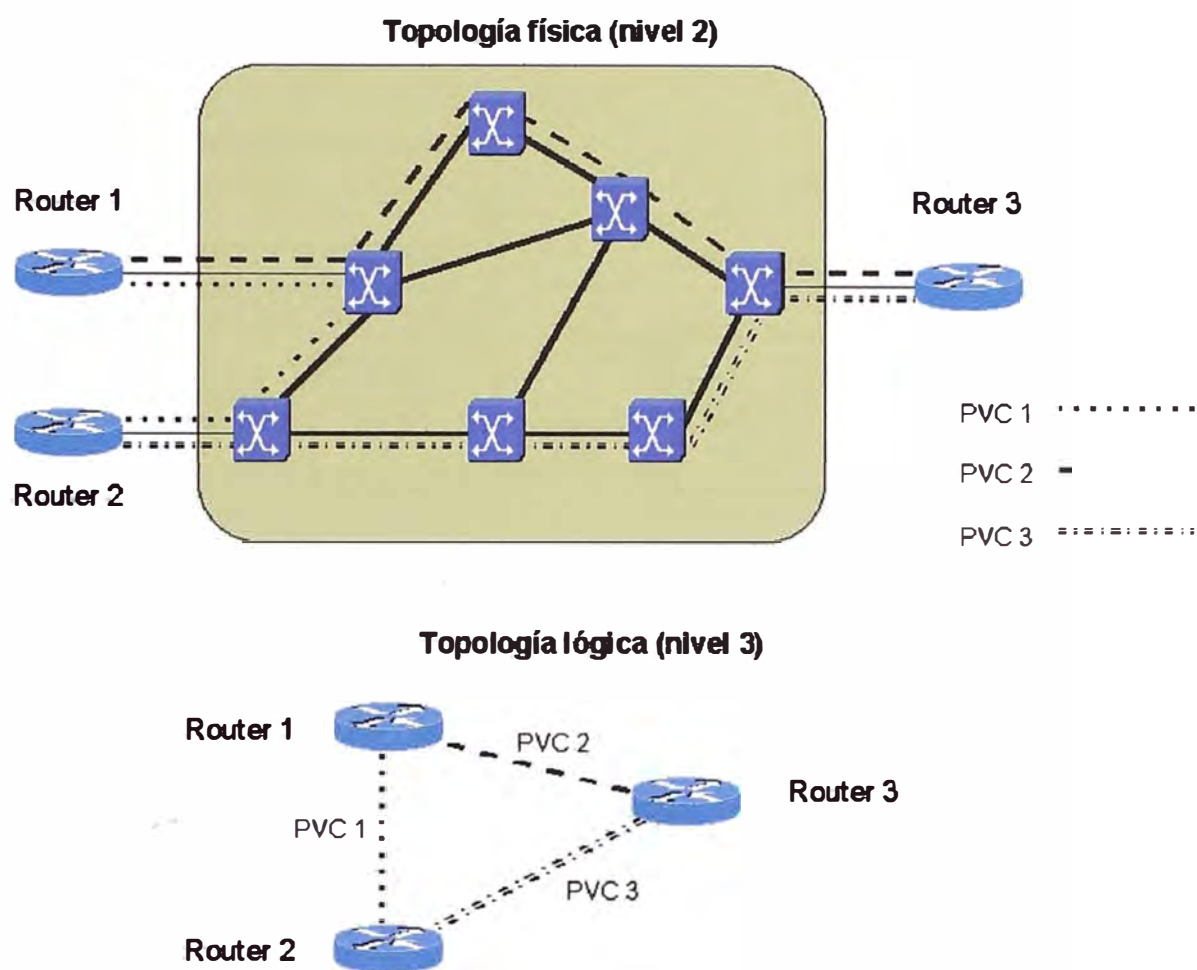
Se realizaron muchos esfuerzos para combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los Routers IP. A favor de esto estaba el hecho de que los proveedores de servicios habían desplegado infraestructura de redes ATM lo que favorecía la integración de los niveles 2 y 3 de OSI. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento, por un lado, proporcionaba mayores velocidades (155 Mbps) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de

tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de proveedores de servicios, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de Routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia.

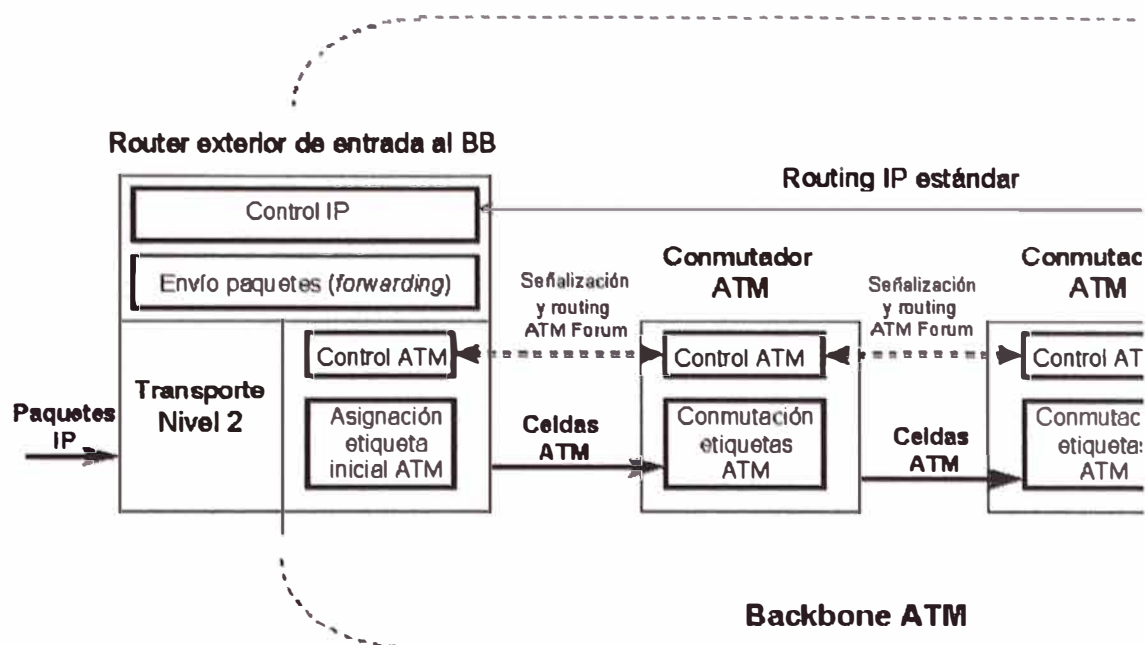
Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la **figura 2** se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.





**Figura 2. Topología física ATM y topología lógica IP superpuesta**

La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En **la figura 3** se representa el modelo IP/ATM con la separación de funciones entre los que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control / señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.



**Figura 3. Modelo funcional IP sobre ATM**

### 5.6.3 Ventajas de la Arquitectura IP sobre ATM

- El ancho de banda disponible a precios competitivos.
- Gran rapidez de transporte de datos proporcionados por los conmutadores de nivel 2.
- Los proveedores de servicio operan el backbone ATM al servicio de sus redes IP.
- La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada.
- El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian la información de encaminamiento correspondiente.

#### 5.6.4 Desventajas de la Arquitectura IP sobre ATM

- Hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes.
- Existe, además, un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible.
- Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial  $n \times (n-1)$  al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, p. ej., En una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios  $5 \times 4 = 20$  PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura ( $6 \times 5 = 30$ ).
- Una desventaja adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo de enrutamiento interno.

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades.

### 5.6.5 Convergencia hacia IP: Conmutación IP

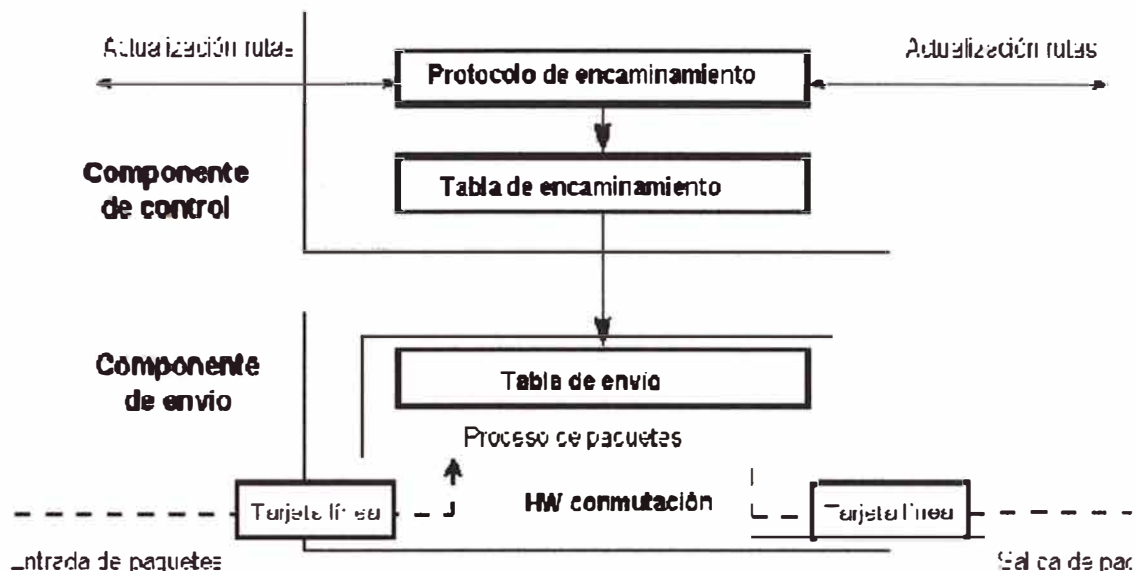
La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señaladas anteriormente. Esas técnicas se conocieron como "Conmutación IP" (IP switching) o "Conmutación Multinivel" (multilayer switching). Se desarrollaron una serie de tecnologías privadas entre las que merecen citarse:

- IP Switching de Ipsilon Networks,
- Tag Switching de Cisco,
- Aggregate Route-Base IP Switching (ARIS) de IBM,
- IP Navigator de Cascade/Ascend/Lucent,
- Y Cell Switching Router (CSR) de Toshiba.

Que condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

Debemos tomar en cuenta que todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes, las que resulta de separar las funciones de:

- Control (Routing), y
- Envío (forwarding).



**Figura 4. Separación funcional de Encaminamiento y Envío**

En la **figura 4**, se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de

encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

Con respecto a la etiqueta que marca cada paquete, se puede decir que:

- Es un campo de unos pocos bits,
- De longitud fija,
- Se añade a la cabecera de cada paquete,
- Identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes.

Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no

conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM.

## **CAPITULO VI CONMUTACIÓN MULTINIVEL MPLS**

### **MultiProtocol Label Switching - MPLS**

De acuerdo a lo descrito en el capítulo anterior, el problema principal que presentaban las diversas soluciones de conmutación multinivel era la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello, la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas tales como Frame Relay, PPP, SONET/SDH y LANs. Entonces se debía obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar Unificado e Interoperativo.

### **6.1 Objetivos Principales del Estándar MPLS**

Los objetivos principales establecido por el grupo de trabajo MPLS, en la elaboración del estándar eran:

- Debería funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- Debería soportar el envío de paquetes tanto unicast como multicast.
- Debería ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP.



- Debería permitir el crecimiento constante de la Internet.
- Debería ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

Por otro lado también se tuvo en cuenta que se debería mantener el encaminamiento tradicional de nivel 3, por los siguientes motivos:

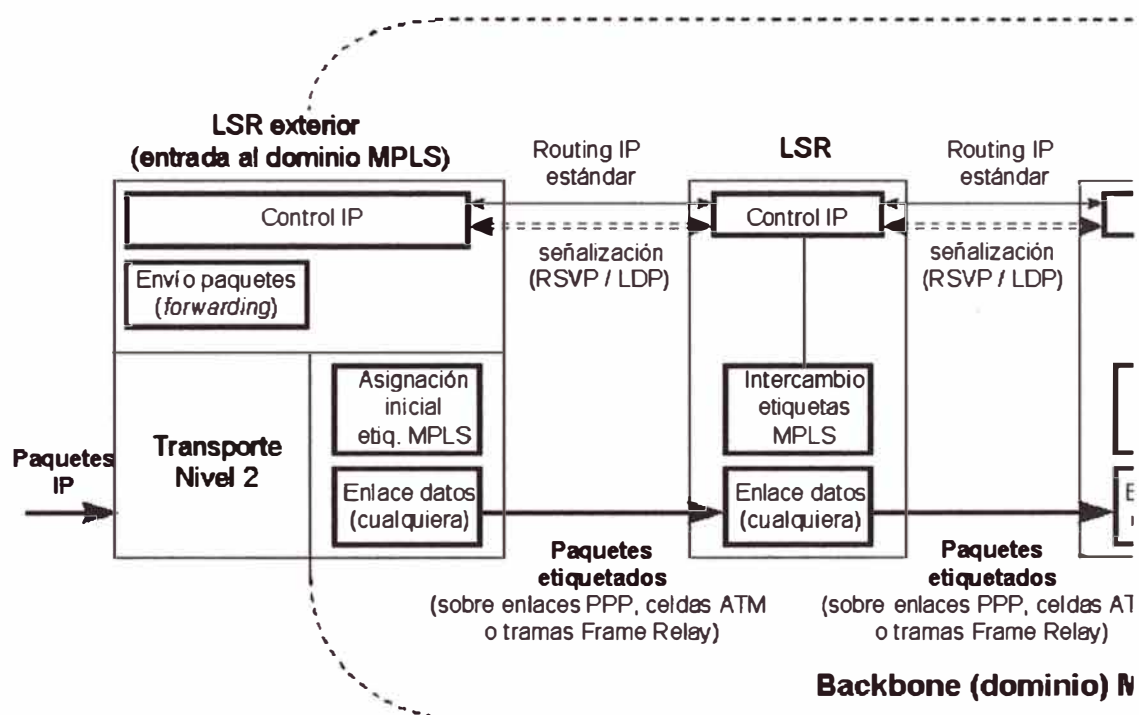
- Para el filtrado de paquetes en los cortafuegos (FW), para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.
- No es probable que los sistemas finales (hosts) implementen MPLS.
- Las etiquetas MPLS tienen solamente significado local. Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.
- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

## **6.2 Descripción funcional del MPLS**

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí.

### 6.2.1 Funcionamiento del Envío de Paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Switching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.



**Figura 5. Esquema funcional del MPLS**

En la **figura 5** se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras 2 y 3 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS

separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera.

Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos basándose en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

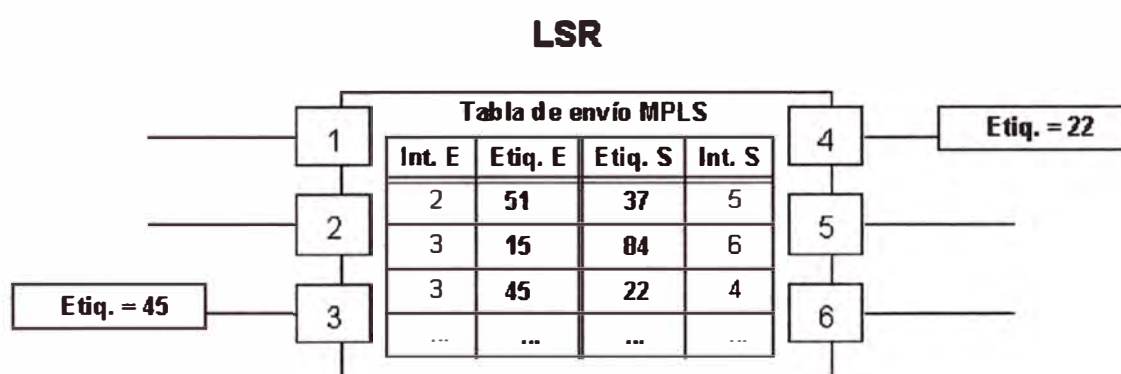
Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de

envío, el cual se construye a partir de la información de encaminamiento proporcionada por el componente de control.

Cada entrada de la tabla contiene un par de etiquetas entrada / salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola).

En la **figura 6** se muestra el funcionamiento paso a paso el recorrido de un paquete a través de un LRS ubicado en el núcleo MPLS:

1. El paquete llega al LSR por la interfaz 3 de entrada con la etiqueta 45.
2. El LSR revisa la tabla de envío verificando la interfase de entrada y la correspondiente etiqueta.
3. El LSR de acuerdo a la tabla de envío le asigna la etiqueta 22 y lo envía por la interfaz 4 de salida al siguiente LSR.

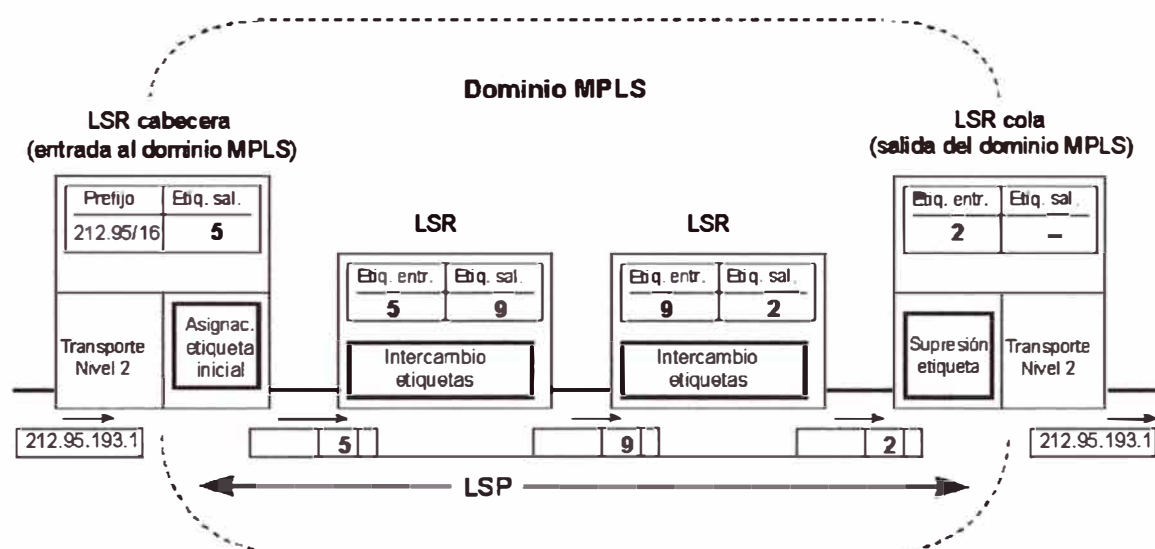


**Figura 6. Detalle de la tabla de envío de un LSR**

En la **figura 7** se describe paso a paso la entrada y salida de un paquete en los LSR externos:

1. El LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección IP destino es 212.95.193.1.

2. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16.
3. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.
4. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas.
5. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.



**Figura 7. Ejemplo de envío de un paquete por un LSP**

Asimismo se debe tener en cuenta lo siguiente:

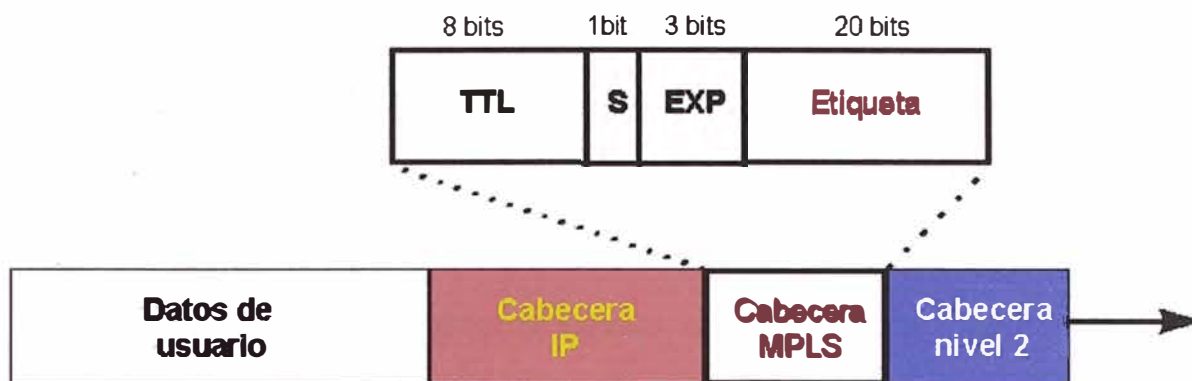
- Las etiquetas se insertan en cabeceras MPLS, ubicados entre los niveles 2 y 3.
- El MPLS debe funcionar sobre cualquier plataforma de transporte: PPP, LAN, ATM, Frame Relay, etc.

- Para el caso de los protocolos de transporte de datos, tales como el ATM y el Frame Relay, que tienen los campos VPI/VCI y DLCI respectivamente, estos se utilizan como campos nativos para las etiquetas.
- Para los protocolos de transporte de datos, tales como PPP o LAN, que no soportan un campo de etiquetas, se emplea una cabecera genérica MPLS, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y nivel 3.

En la **figura 8** se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en:

- 20 bits para la etiqueta MPLS,
- 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS),
- 1 bit de stack para poder apilar etiquetas de forma jerárquica (S), y
- 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP.

De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender la red.



**Figura 8. Estructura de la cabecera genérica MPLS**

### 6.2.2 Control de la información en MPLS

En el capítulo anterior hemos revisado el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Ahora debemos revisar dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs.
- Cómo se distribuye la información sobre las etiquetas a los LSRs.

El primero de ellos está relacionado con la información que se tiene sobre la red, tal como la topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son routers con funcionalidad añadida).

Esto es lo que hace MPLS precisamente: Para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada /

salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización", esto porque siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Aunque actualmente existen varios protocolos en proceso de estandarización, la arquitectura MPLS puede utilizar como protocolo de distribución de etiquetas los siguientes:

- Protocolo RSVP del Modelo de Servicios Integrados del IETF.
- Label Distribution Protocol (LDP).

### **6.2.3 Funcionamiento global de la Arquitectura MPLS**

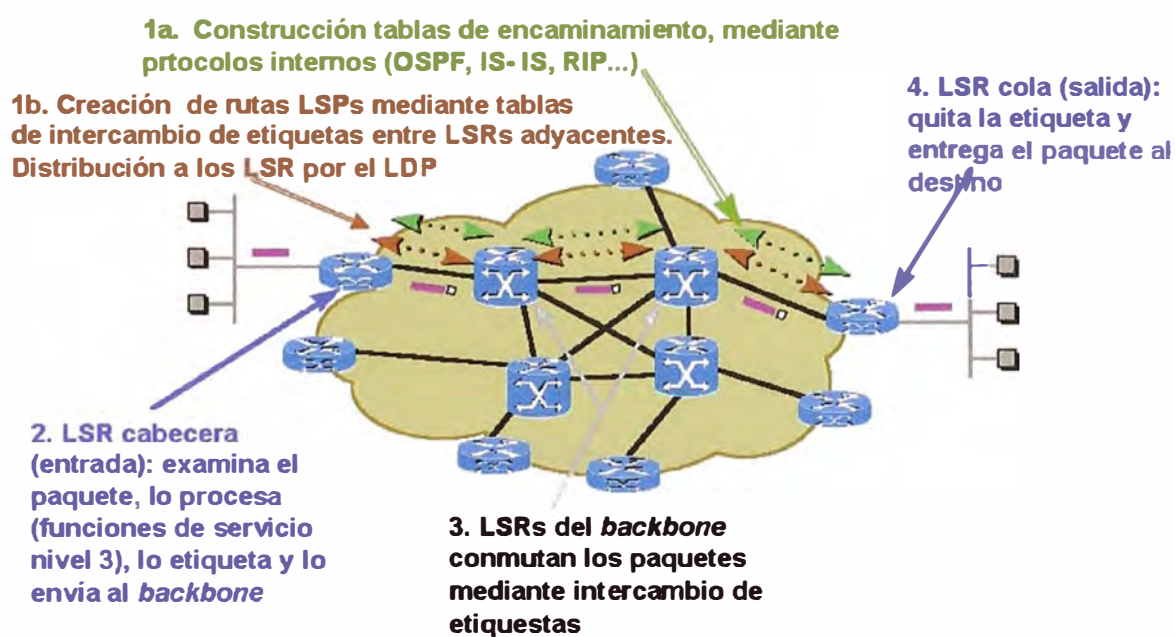
Después de describir los componentes funcionales, el esquema global de funcionamiento de la arquitectura MPLS es el que se muestra en la **figura 9**, donde quedan reflejadas las diversas funciones de cada uno de los elementos que integran la red MPLS.

Es importante destacar entre otros lo siguiente:

- En el borde de la nube MPLS tenemos una red convencional de routers IP.
- El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto.
- La distancia de un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers).



- Funcionalmente es como si estuvieran unidos todos en una topología mallada.
- La diferencia con topologías conectivas reales es que la construcción de caminos virtuales en la arquitectura MPLS es mucho más flexible.



**Figura 9. Funcionamiento de una red MPLS**

## **CAPITULO VII LINEAMIENTOS TÉCNICOS DEL DISEÑO**

El diseño de una red de comunicaciones es una tarea que se basa en disponer todos los elementos necesarios de tal forma que permitan establecer y desarrollar las comunicaciones con la calidad esperada y a un costo razonable, a la vez que se ofrezca la flexibilidad necesaria para su crecimiento en función de la demanda.

A la hora de construir una red de comunicaciones con calidad de servicio de extremo a extremo, las funciones y los mecanismos que contribuyen a lograrlo se distribuyen entre los dispositivos de borde y los conmutadores del núcleo de la red (backbone).

Las reglas y clasificación de los paquetes se aplican en los bordes de la red. El backbone de la red es responsable de la conmutación a alta velocidad, del transporte de la información y de la aplicación de las normativas de control de congestión y las técnicas de gestión de colas.

### **7.1 Calidad de Servicio en el Borde de la Red WAN**

#### **7.1.1 Clasificación de los Paquetes**

La clasificación de los paquetes permite a los administradores de la red especificar normativas que identifiquen el tráfico de la red que luego pueden ser divididos en varios niveles de prioridad o clases de servicio(CoS).

El administrador de la red puede definir hasta seis clases usando los tres bits de precedencia en el campo de tipo de servicio (ToS) del encabezamiento del paquete IP.

Tras la clasificación, el borde de la red garantiza que los paquetes de una determinada clase reciban los niveles de servicio apropiados, como por ejemplo tasas asignadas y probabilidad de pérdida. Otra opción que se suele utilizar en el borde es aplicar capacidades de normativas de enrutamiento.

Hoy en día los paquetes se clasifican basándose en criterios tales como puerto físico, dirección IP, puerto de aplicación, tipo de protocolo, o por otros criterios especificados por las listas de control de acceso(ACL). Los criterios que se utilizan para clasificar el tráfico pueden ser establecidos por el administrador de la red, cuando lo señale la aplicación.

### **7.1.2 Asignación de la Tasa de Acceso**

La función del Committed Acces Rate (CAR) también proporciona gestión del ancho de banda. El administrador de red puede usar el CAR para asignar las normativas de manejo de tráfico cuando éste cumpla o exceda los límites de tasa especificado.

Las normativas de límite de tasa CAR pueden determinarse de acuerdo a lo siguiente:

- Por puerto físico.
- Por dirección MAC (Media Access Control).
- Por dirección IP.

- Por puerto de aplicación.
- U otros criterios especificados por las listas de control de acceso.

Los límites de tasa de CAR pueden aplicarse al tráfico de entrada y de salida y a las interfaces ATM y Frame Relay.

El CAR también puede usarse para especificar normativas de gestión de ancho de banda más completas a través de límites de tasa en cascada, ofreciendo a los administradores un completo control sobre los recursos de la red.

### **7.1.3 Evitar la Congestión y Probabilidad de Pérdida**

La Weighted Random Early Detection (WRED), ofrece a los administradores de red la capacidad evitar la congestión que puede resultar de un trato preferencial a los diferentes niveles de CoS configurados.

La Random Early Detection (RED) coopera con las fuentes de tráfico TCP para máxima la tasa de transferencia útil y el uso de la capacidad de la red reduciendo al mínimo la pérdida, a la vez que evita el colapso por congestión.

WRED ofrece un tratamiento preferente para el tráfico más importante en situaciones de congestión, permitiendo a los administradores especificar unos límites RED distintos y normativas de desconexión en cascada para cada clase de servicio.

### **7.1.4 Enrutamiento basado en normativas**

El enrutamiento basado en normativas ofrece al administrador un sistema para definir las rutas de encaminamiento personalizadas para paquetes

seleccionados basándose en criterios tales como la dirección origen y el puerto de aplicación, que no se suelen ser considerados por los protocolos de enrutamiento basados en destino. Por tanto los tipos de tráfico concretos, tales como tráfico de voz, pueden enviarse a través de rutas especiales que reduzcan al mínimo el número de saltos y otros tipos de retrasos a fin de garantizar la máxima calidad del servicio.

Asimismo, el enrutamiento basado en normativas puede ser usado en Routers de gama media y baja, para clasificar y marcar paquetes usando el campo de precedencia IP, permitiendo así que los Routers den un tratamiento prioritario a los paquetes de voz cuando la red esté congestionada.

## **7.2 Calidad de Servicio en el Backbone de la Red WAN**

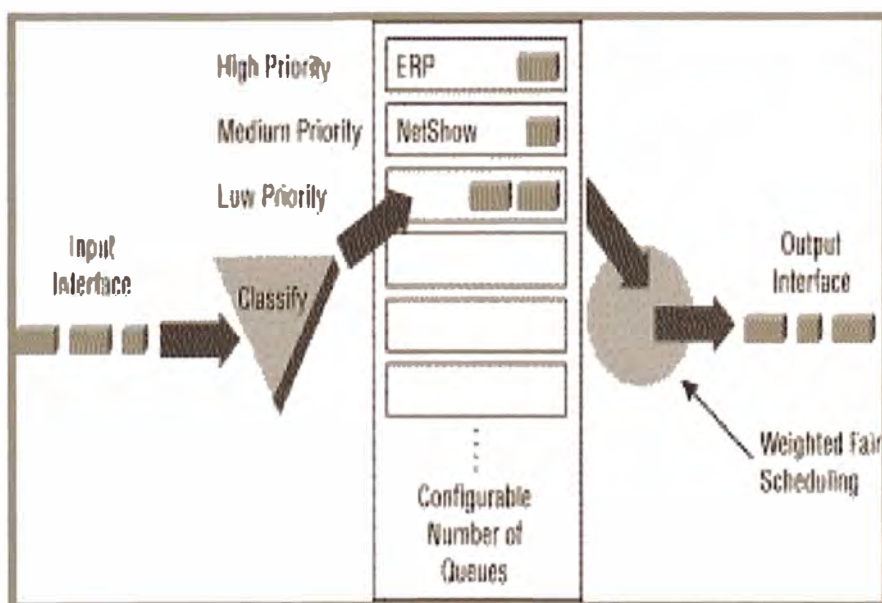
### **7.2.1 Tráfico en espera y programado**

La utilización de los mecanismos de gestión de cola y de programación de enrutamiento para cumplir con la asignación de un ancho de banda especificado o con límites de retraso se aplican tanto a la salida de los dispositivos de borde, como a los dispositivos del núcleo de la red.

El mecanismo utilizado de forma habitual, Weighted Fair Queuing (WFQ), segrega tráfico en múltiples flujos o clases y, seguidamente programa la salida de tráfico para satisfacer la asignación de ancho de banda especificado o los límites de retraso. Las clases WFQ pueden asignarse por precedencia IP, puertos de aplicación, protocolo IP o interfaz de entrada identificado por la clasificación en el borde.

El WFQ basado en clases, considera que los paquetes pertenecen a varias clases de tráfico definida por los usuarios. WFQ utiliza marcas de precedencia IP que se usan como criterio para asignar ID de clases y asignar los paquetes entrantes a las colas correspondientes a dicha clase. Una vez que están en sus respectivas colas, los paquetes pueden recibir tratamiento preferencial basándose en las ponderaciones definidas por el usuario asignado a dicha clase.

WFQ basado en clases permite garantizar un gran ancho de banda, las cuales son más apropiadas para aplicaciones tales como la voz, que tienen estrictos requisitos de demora y tolera mínimamente la pérdida de paquetes. Además todo el ancho de banda que no se utilice de una clase de voz puede asignarse automáticamente a otra clase de tráfico que tiene una mayor ponderación definida por el usuario. Con ello se garantiza el uso opcional del ancho de banda disponible.



**Figura 10.- Weighted Fair Queuing**

### **7.2.2 Núcleos Frame Relay y ATM**

Estos habituales medios WAN orientados a la conexión ofrecen tipos exclusivos de QoS, por ejemplo ATM cuenta con tipos de servicios como velocidad constante de bits (Constant Bit Rate – CBR) y velocidad no especificada de bits ( Unspecified Bit Rate – UBR).

Por lo tanto los mecanismos de calidad de servicio IP, como por ejemplo WRED, CAR e IP Precedence establecidos por la aplicación o durante la clasificación en el borde deberían ser asignados a los equivalentes de QoS apropiados en los circuitos ATM y Frame Relay.

Las clases de servicio IP, cada una con sus propios límites WRED pueden asignarse a conexiones virtuales ATM separadas con diferentes clases de servicios para proporcionar interoperación de clase de servicio IP a ATM.

### **7.2.3 Conmutación de etiquetas multiprotocolo**

El IETF cuenta con un grupo de trabajo denominado Multiprotocol Label Switching (MPLS) que trabaja para especificar la utilización de la conmutación por etiquetas sobre una variedad de tecnologías de medios, incluyendo ATM y Packet over SONET (PoS).

MPLS combina la capacidad de ampliación de enrutamiento (Routers) con la velocidad y la capacidad de ingeniería de tráfico de los switches (como por ejemplo los switches ATM). Así, en una red MPLS IP + ATM, los switches ATM ejecutan los protocolos de enrutamiento IP (OSPF, EIGRP, BGP y otros) para el tráfico IP, además de los protocolos UNI/PNNI que

pueden estar soportando orientado a la conexión. Así se mejora la capacidad de ampliación e integración de los servicios IP, como por ejemplo la calidad de servicio y VPN sobre un núcleo de red ATM.

MPLS lo reúne todo, permitiendo la asignación de calidad de servicio IP a los tributos QoS de cada nodo y enlace de conmutación sea cual sea su tipo, permitiendo una normativa uniforme de QoS de extremo a extremo para IP. Como MPLS no es específico a ATM ni a ningún otro tipo de tecnología, es posible utilizarla sobre una gran variedad de switches WAN.

### **7.3 Implementación del Sistema de Contingencia**

Los planes de contingencia de una empresa se derivan de los planes de Sistemas y de Comunicaciones.

#### **7.3.1 Plan de Sistemas**

##### **Recuperación ante Desastres**

Debido Agentes Internos, la caída de los procesadores centrales y/o servidor de comunicaciones, caída del servidor de aplicaciones y/o Base de Datos, fallo de energía, errores de operación, etc.

Debido Agentes Externos, tales como inundaciones, incendios, amenazas de bomba, huelgas, en general cualquier factor ajeno al centro que inhabilite el acceso u operación del mismo.



### **Disposición de un centro de respaldo que permita soportar temporalmente el procesamiento de información.**

El respaldo tiende a ser parcial por lo que se deben asignar prioridades a los procesos que mantengan las condiciones mínimas de operación de la compañía.

La restauración del servicio mínimo en el mejor de los casos es superior a cuatro horas.

#### **7.3.2 Plan de Comunicaciones**

La concentración de líneas y/o accesos en el Centro de comunicaciones requieren de un tratamiento diferenciado, con equipos y medios de transmisión redundantes, así como de un procedimiento de recuperación del servicio manual o automático.

Se debe contemplar mecanismos que permiten restaurar el servicio de extremo a extremo ante averías simples en la red de acceso (respaldo de terminales de usuarios).

Recuperación ante desastres, el sistema de comunicaciones deberá estar diseñado para conmutar el acceso de terminales hacia un nuevo sistema .

#### **7.3.3 Factores que afectan la disponibilidad de red**

- La calidad de los equipos de transmisión y conmutación, así como su operación.
- La calidad de las líneas o medios de transmisión que conforman la ruta de servicio.

- La velocidad con que se restablece el servicio, una vez que se presenta la avería.

### **Equipos de transmisión y conmutación**

El tiempo medio entre fallos (MTBF) indica la fiabilidad de los equipos de comunicaciones (indicada por el fabricante).

Los sistemas de alimentación eléctrica deben ser seguros y contar con respaldo.

Se debe monitorizar el funcionamiento de los equipos y contar con la gestión de la configuración de los mismos, especialmente de los conmutadores y enrutadores.

### **Líneas o Medios de transmisión**

Fundamentalmente la calidad de los medios de transmisión(Planta externa, radioenlace, fibra óptica, etc.).

Estabilidad de la planta tanto ante agentes externos(clima, accidentes, etc.), como internos (construcción, acciones de mantenimiento y asignación, etc.).

### **Tiempo de restauración / reparación**

- Sistemas de detección y diagnóstico de fallas.
- Capacidad operativa para reparar / restaurar.
- Capacidad interna de las redes para restaurar el servicio (redundancia y diversificación).

- Despliegue de los medios complementarios necesarios que permitan restaurar el servicio automática o manualmente.

### **7.3.4 Alternativas ante Contingencias**

#### **Aportadas en el lado del Clientes / Usuarios**

- Sistemas de proceso redundante (Duplicación de los Procesadores y/o servidores de aplicaciones, base de Datos y Comunicaciones).

#### **Aportadas por el lado de la red**

- Respaldo de acceso y respaldo de extremo a extremo.
- Equipos con alta disponibilidad y rutas alternativas.
- Enlaces alternativos de acceso a dos nodos de red distintos.
- Grupos de captura distribuidos en la red.
- Emplazamiento de equipos de red en instalaciones del cliente.

## **7.4 Estrategia de la Gestión de la Red**

### **7.4.1 Gestión básica**

El proveedor de los enlaces de comunicaciones debe incluir un nivel de gestión básica como parte del servicio, donde por lo menos se debe incluir:

- Acceso total a configuración de Router de cliente, desde el Centro de Gestión especializado del proveedor.
- Monitoreo de enlaces.
- Monitoreo de establecimiento de servicio.
- Manejo de estadísticas y generación de informes online.

### **7.4.2 Gestión VIP**

Para el caso de proyectos de Outsourcing se debe considerar una gestión de nivel VIP donde se contemple, adicional a la gestión básica, las siguientes actividades:

- Destinar en el local del cliente un terminal de Gestión a fin de permitirle conocer el estatus de su red en línea y ciertos niveles de gestión.
- Monitorizar el tráfico de cada uno de los enlaces de los clientes. De tal forma que se pueda ver la demanda del ancho de banda y pueda analizar la necesidad de un aumento del mismo.
- Analizar el porcentaje de utilización del CPU del Router, de tal forma que se lleve el control de la utilización de la capacidad de las memorias.
- Sondeo de Conectividad a nivel de IP de la red de los clientes, a fin de verificar la operatividad a nivel físico y de protocolo, para la toma de acciones preventivas.
- De contar con enlaces de contingencia, se debe verificar diariamente su operatividad, sin necesidad de interrumpir la conexión WAN del cliente.
- Coordinar de manera conjunta con el Cliente pruebas de Backup, de tal forma que ambos cliente y proveedor verifiquen su funcionalidad.

## **CAPITULO VIII RESPONSABILIDADES DEL PROVEEDOR Y CLIENTE**

Este punto es uno de los más importantes dentro de la fase del desarrollo del proyecto y la fase de la implantación del mismo.

Los deberes y responsabilidades entre el Proveedor del servicio y el Cliente, deben quedar bien establecidos a fin de evitar inconvenientes del alcance del proyecto y las condiciones que se deben cumplir para llegar a su óptima operación y las expectativas creadas, es conveniente indicar explícitamente lo que el Proyecto Incluye y lo que No Incluye.

### **8.1 Responsabilidades del proveedor**

- Empieza desde la fase de PreVenta, continua en la Implantación, puesta en marcha y Operación del servicio solicitado, manteniendo en cada fase una atención con personal especializado y personalizado.
- Desarrollar, planificar y gestionar la red de comunicaciones que satisfaga todos los requerimientos de los clientes.
- Garantizar la Calidad y Disponibilidad del Servicio en todo momento, de acuerdo a los compromisos adquiridos.
- Asesoramiento al personal designado por el cliente sobre el manejo, gestión y control de la red y equipos instalados.

- Ayudar al cliente a planificar y optimizar la funcionalidad de su red de comunicaciones e implementación de nuevos servicios de manera proactiva.
- Mantener la confidencialidad de toda la información suministrada por el cliente.

## **8.2 Responsabilidades del cliente**

- Conformar una mesa de trabajo que se encargue de realizar las coordinaciones, lleven el control de la implantación y operación del sistema de comunicaciones.
- Definir los límites de sus facultades de control y administración de la red de comunicaciones y equipos, en coordinación con el proveedor del servicio.
- Proporcionar los espacios físicos, condiciones ambientales y eléctricas adecuados, para el buen funcionamiento de los equipos de comunicaciones, de acuerdo a las especificaciones técnicas indicados por el proveedor.
- Mantener la confidencialidad de toda la información suministrada por el proveedor.

## CONCLUSIONES

### Desde el punto de vista de los usuarios

- No todo es el precio, cada vez es más importante la Calidad de Servicio que entrega el Proveedor, para ello se debe tener en cuenta la plataforma de red a través del cual el proveedor brinda sus servicios.
- En condiciones normales, la QoS no es necesario, pero hay eventos que impactan el rendimiento de las redes incluso cuando están bien diseñadas. Aunque la red se sobrecargue la QoS debe asegurar que el tráfico crítico no sea perdido ni retardado.
- Uno de las ventajas más prometedoras de las Redes IP basada en MPLS, es que permiten compartir el tráfico de voz con el tráfico de datos tradicionales y entre redes de área local, lo que permite normalmente a reducir los costos de las transmisiones.
- Los usuarios deben tener en cuenta que los servicios con QoS, debe garantizar entre otras cosas; Baja Latencia, Bajo Jitter y sin Pérdidas de Paquetes, incluso en presencia de congestión.
- Deben asegurarse que el proveedor de servicios haya desarrollado e implementado herramientas que permitan medir los parámetros de la QoS y tenga un plan de pruebas para medir el desempeño a nivel de aplicación y de red.

- A través de este informe se analiza y recomienda, una plataforma de red en base a la tecnología IP-MPLS, la cual está siendo implementada en la mayoría de Proveedores de Servicios en el mundo, por su flexibilidad de ser implantada sobre ATM, GigaEthernet, etc., facilitando la implementación de VPN con la QoS e Ingeniería de Tráfico.

### **Desde el punto de vista del proveedor**

- Cada vez más la QoS es un factor fundamental diferenciador tenido en cuenta por los usuarios a la hora de elegir un proveedor de servicios.
- Al proveedor de servicios le conviene establecer mecanismos de medida de la Calidad de Servicio al usuario, que sean objetivos e independientes tanto en el servicio de red como en la atención al usuario.
- El proveedor debe contrastar su QoS, es importante tener una referencia exacta del tipo de servicio que está ofreciendo comparativamente con la competencia.
- Las medidas de la QoS ayudan al proveedor a la detección de problemas en el servicio de red y a mantener los parámetros ideales de calidad, de forma que puedan dar soluciones adecuadas a los problemas que vayan surgiendo.
- Para soportar las aplicaciones que consumen grandes anchos de banda y los nuevos tráficos multimedia, no basta con dotar a la red de mayor capacidad, es preciso además, añadir determinados niveles de inteligencia que permitan controlar los tráficos dando prioridad al más crítico para la actividad de la empresa.



- El proveedor de servicios, debe tener en cuenta que el diseño de una plataforma de red de servicios debe hacer el mayor uso posible de los estándares del mercado para asegurar y estimular su evolución.
- Las aplicaciones de los clientes y sus requerimientos deben estudiarse cuidadosamente para diseñar, implementar y mejorar la funcionalidad de su red de comunicaciones, con el fin de ofrecer un soporte de la QoS satisfactorio.
- A fin de facilitar la implementación global de la QoS, es recomendable que el proveedor de servicios tenga implementado una herramienta de administración y gestión de extremo a extremo, de la plataforma de red de servicios.
- Para proporcionar Calidad de Servicio de extremo a extremo de forma eficaz, la señalización de la red precisa que los dispositivos de la red compartan la responsabilidad de distribuir tráfico con prioridad, para ello todos los equipos de lado de red y lado de cliente estén homologados en todas sus funcionalidades.
- Una red MPLS permite la asignación de Calidad de Servicio IP en cada nodo y enlace de conmutación, sea cual sea su tipo, permitiendo una normativa uniforme de la QoS de extremo a extremo para IP. Como MPLS no es específico a ATM ni a ningún otro tipo de tecnología, es posible utilizarla sobre una gran variedad de switches WAN.

## GLOSARIO

- **ADSL:** Asymmetric Digital Subscriber Line.

Tipo de DSL (Digital Subscriber Line) en el que el ancho de banda de bajada (de red a cliente) es mayor que el de subida (de cliente a red). Disposición adecuada para navegación en Internet y aplicaciones cliente-servidor, así como para video por demanda.

- **ATM:** Asynchronous Transfer Mode.

Estándar para la transmisión por conmutación de células (o paquetes) en sistemas avanzados de comunicaciones de banda ancha. Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea.

Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1.2 Gbps.

- **Backbone:** Nivel máximo de una red jerárquica.

- **Best Effort:** Clasificación de tráfico de red de baja prioridad.

Los distintos tipos de tráfico cursado requieren distintas prioridades. Las comunicaciones en tiempo real, como video-conferencia, requieren de un ancho de banda y retardo mínimo garantizado, por lo que deben ser de prioridad alta. El correo electrónico, por ejemplo, tolera demoras arbitrariamente largas por lo que puede ser clasificado como un servicio en calidad de "best effort".

- **BGP:** Border Gateway Protocol.

Protocolo de borde de red hacia el exterior.

- **CDMA:** Code Division Multiple Access.

Forma de multiplexación en la cual el transmisor codifica la señal usando secuencias numéricas pseudo-aleatorias las cuales son reconocidas por el receptor, y utilizadas para decodificar la señal.

Cada secuencia numérica pseudo-aleatoria corresponde a un canal de comunicación distinto.

Motorola utiliza CDMA para teléfonos celulares digitales.

- **CE:** Customer Equipment (equipo en casa del cliente).
- **CGP:** Centro de Gestión Personalizado.
- **CGRC:** Centro de Gestión de Redes de Clientes.  
Centro de Gestión ubicado en las oficinas principales de Telefónica Data Perú, desde el cual se gestionan las redes de los clientes en forma remota.
- **CoS:** Clase de Servicio.  
Propiedades de desempeño de un servicio de red, que incluye retardos y prioridades. Algunos protocolos como MPLS permiten que paquetes o caudales incluyan requerimientos de CoS.
- **CPI:** Centro Proveedor de Internet (en inglés, ISP).  
Compañía que provee a otras compañías o individuos, el acceso o presencia en Internet. La mayoría de CPI's son también proveedores de acceso a Internet (IAP); servicios extra incluyen diseño, creación y administración de sitios de laWorld Wide Web, capacitación y administración de Intranets.
- **Datagrama:** Se denomina así a una entidad de data independiente que lleva consigo la información que facilita su enrutamiento desde una fuente hasta un quipo destino, sin depender de intercambios entre ambos y la red de transporte.
- **DLCI:** Data Link Connection Identifier (Identificador de Enlace de Datos).  
Un número de canal adjunto a una trama de datos que indica su enrutamiento en una red Frame Relay.
- **DNS:** Domain Name System o Domain Name Server.  
Servicio utilizado en Internet para traducir direcciones IP de host en direcciones de Internet.  
Máquina dentro de una red que ofrece dicho servicio.

- **DSLAM:** Digital Subscriber Line Access Multiplexer.  
Término genérico para el equipo terminal donde se concentran las líneas xDSL. Las múltiples señales DSL pueden ser multiplexadas a un canal de banda ancha como ATM.
  
- **E1:** Especificación europea de transmisión de 2.048 Mbps
  
- **Extranet:** La extensión de la intranet de una compañía hacia una red pública como Internet, para de esta forma permitir a clientes y socios de negocio seleccionados el acceso a la información y aplicativos privados de una compañía, a diferencia del sitio web el cual puede ser accedido universalmente. Generalmente la extranet implica acceso en tiempo real a través de un Firewall para garantizar la seguridad.
  
- **Fibra óptica:** Fibra de vidrio o plástico más delgada que un pelo humano, usada para transmitir información por medio de haces de luz infrarroja e incluso luz visible. El haz es una señal electromagnética con una frecuencia de entre 10<sup>14</sup> y 10<sup>15</sup> Hz, muy poco susceptible al ruido de señales externas. El material que rodea la fibra provee reflexión total, para evitar la degradación de la señal. Asimismo se garantiza la seguridad contra intrusos en los tendidos de fibra ya que es muy difícil de intervenir.
  
- **Firewall:** máquina dedicada de ingreso a una red, configurada para brindar seguridad, especialmente en las conexiones a Internet u otras redes públicas y líneas de acceso. El típico Firewall es una máquina con un microprocesador de bajo costo basado en Unix, con modems y puertos de red pública, y una cuidada conexión a la red interna. Las precauciones especiales pueden incluir monitoreo contra amenazas, call-back (alarmas automáticas al usuario) y trampas para engañar intrusos con el fin de rastrearlos.
  
- **Frame Relay:** Protocolo de comunicaciones, basado en el protocolo X.25, que trabaja solamente en los dos primeros niveles del modelo OSI (nivel físico y nivel de enlace). De esta manera se consigue una velocidad de transmisión de datos de hasta 2 Mbps. Protocolo para intercambio de datos entre un "host" y una red de datos.
  
- **HTTP:** Hyper Text Transport Protocol, Protocolo TCP/IP del tipo cliente-servidor, usado en la WWW para el intercambio de documentos bajo formato HTTP (hipertexto).

- **HW:** Hardware.
- **Intranet:** Cualquier red que provee servicios similares dentro de una organización, a los proveídos por Internet, pero sin estar necesariamente conectado a Internet. El ejemplo más común es el uso que hacen las compañías de uno o más servidores World Wide Web en una red TCP/IP interna para distribuir información dentro de la compañía. El uso de intranets para la computación corporativa se ha extendido a partir de 1995 gracias a la disponibilidad de navegadores baratos o gratuitos y software para web Server que permiten una interfase simple y uniforme de hipertexto hacia información de muchos tipos y programas aplicativos.
- **IP:** Internet Protocol.  
Protocolo de comunicaciones que provee enrutamiento de paquetes, fragmentación y ensamble en el nivel 2 de OSI (enlace de datos). IPv4 es la Versión más usada. IPv6 se está usando cada vez más a partir del 2000.
- **Kbps:** Kilo Bits por segundo.
- **LAN:** Local Area Network.  
Red de datos geográficamente cercana (típicamente en un radio de hasta 1 Km) con fácil interconexión entre sus terminales, microprocesadores y computadoras distribuidas en edificios adyacentes. Las redes Ethernet y FDDI son ejemplos de LAN estándares.  
Debido a que la red sólo cubre un área limitada, los protocolos de señalización de red pueden ser optimizados permitiendo velocidades de transmisión de datos de hasta 100 Mbps.
- **LDP:** Label Distribution Protocol.
- **LER (PE):** Label Edge Switch Router.  
Componente situado en el borde de una red MPLS, que usa información de enrutamiento para asignar Labels a datagramas y enrutarlos al interior de la red MPLS.
- **LFIB:** Label Forwarding Information Base.
- **LSP:** Label Switched Path.

El trayecto que un datagrama sigue al interior de una red, de acuerdo a su label MPLS.

- **LSR (P):** Label Switch Router.

Componente que reside típicamente en medio de una red y es capaz de enrutar datagramas de acuerdo a sus Labels. En muchos casos, en especial en redes MPLS antiguas, un LSR es típicamente un switch ATM modificado que enruta datagramas basado en Labels del campo VPI/VCI.

- **MPLS:** Multi Protocol Label Switching.

Técnica que define protocolos y procedimientos que permiten que las altas capacidades de conmutación de ATM y Frame Relay sean usadas en redes IP. Representa el último nivel en la evolución de los estándares, que combina la capa dos (capa de enlace de datos) con la capa tres (capa de red) creando así redes flexibles, más veloces y de mayor escalabilidad. Esto incluye capacidades de ingeniería de tráfico que proveen, por ejemplo, aspectos de Calidad de Servicio (QoS)/ Clase de servicio (CoS) y facilitan el uso de redes privadas virtuales (VPN).

- **NA:** Nodo de Acceso.

- **NT:** Nodo de Tránsito.

- **Par de cobre:** tipo de cable en el que pares de conductores están entrelazados para evitar altas concentraciones de ruido generado por alambrados cercanos.

- **PE:** Point of Entry. Ver LER.

- **PPP:** Point to Point Protocol.

Protocolo de comunicaciones para la transmisión de datagramas de capa de red (p.ej. paquetes IP) a través de enlaces punto-punto.

- **Protocolo:** grupo de reglas formales que describen como transmitir data, especialmente a través de una red. Los protocolos de niveles bajos definen los estándares físicos y eléctricos, el ordenamiento de bits y bytes y la transmisión, detección de errores y corrección de cadenas de bits. Los protocolos de niveles superiores tratan acerca del formato de la data, incluyendo la sintaxis del mensaje, el diálogo entre terminal y

computadora, el grupo de caracteres, el secuenciamiento de los mensajes, etc.

- **Red IP:** nueva red de datos de TD, basada en tecnología IP MPLS.

- **RDSI:** Red Digital de Servicios Integrados (en inglés ISDN)

Conjunto de estándares de comunicaciones que permite que un único cable o fibra óptica cargue voz, servicios de red digital y video. La intención de RDSI es reemplazar eventualmente al antiguo sistema telefónico y utiliza switches y cableados de la RTB, permitiendo que las llamadas digitales de 64 Kbps, de extremo a extremo.

- **Router:** dispositivo que envía paquetes entre redes. Las decisiones de envío se basan en información de la capa de red (capa 3) y de tablas de ruteo construidas por protocolos de transmisión.

- **RTB:** Red Telefónica Básica (en inglés PSTN- Public Switched Telephone Network).

Colección de sistemas interconectados operados por compañías de teléfonos en el ámbito mundial. Actualmente se encuentra casi totalmente digitalizada, salvo en la conexión final al usuario (la "última milla"); La señal proveniente del aparato telefónico es analógica y se transmite sobre cable de cobre de par trenzado como señal analógica.

La digitalización se da en la planta interna del operador telefónico, a 8000 muestras por segundo y 8 bits, lo cual resulta en una velocidad de 64 Kbps. Estos canales son concentrados en canales E1 y mayores para el transporte, son separados antes de alcanzar al abonado receptor.

Estas conversiones son imperceptibles en la voz transmitida pero hacen difícil la comunicación digital, como resultado es virtualmente imposible superar velocidades de 56 Kbps debido a la compresión de la data para ahorrar ancho de banda, entre otros motivos.

- **SDH:** Synchronous Digital Hierarchy

Jerarquía digital síncrona estándar para las telecomunicaciones, con velocidades de transmisión de 51.84 Mbps (STS-1) y múltiplos (STS-3= 155Mbps). STS-3 es la mínima velocidad requerida para transportar tráfico ATM, y es más conocida como STM-1 (Synchronous Transport Module-Level 1).

SDH especifica cómo la carga útil de data es secuenciada y transportada sincrónicamente a través de enlaces de fibra óptica, sin requerir que todos los enlaces y nodos tengan la misma sincronización para transmitir



y recuperar data (i.e. tanto la frecuencia como la fase pueden tener variaciones o ser plesiócronas). Esta característica la hace más flexible y confiable que las redes rígidas PDH (plesiócronas). La secuenciación se da a una frecuencia de 8KHz o 125 microsegundos.

La versión americana de SDH es la red SONET (Synchronous Optical Network).

- **SLA:** Service Level Agreement (acuerdo de nivel de servicio con el cliente).
- **SNA:** Systems Network Architecture, protocolo de tráfico transaccional creado por IBM, donde los canales lógicos son creados entre terminales.
- **SNMP:** Simple Network Management Protocol.  
Protocolo estándar de Internet, desarrollado para manejar nodos en red. No se limita a TCP/IP. Puede ser usado para manejar y monitorear todo tipo de equipos incluyendo computadoras, Routers y Hubs.
- **Spoofing:** técnica usada para optimizar el uso del ancho de banda. Algunos protocolos de red envían, a través de dispositivos en una LAN, muchos paquetes dentro de la WAN, los cuales sirven para la administración de la red (actualizaciones de ruteo o mensajes para comprobar que la LAN remota esta comunicada). La técnica de Spoofing hace uso de puentes o routers en la red, los cuales responden a los paquetes de gestión de red, en vez de dispositivos de LAN remoto, esto ahorra ancho de banda dentro de la WAN.
- **SW:** Software.
- **TCP/ IP:** Transmission Control Protocol over Internet Protocol.  
Protocolo de comunicaciones estándar Ethernet, desarrollado para Internet y que engloba la capa de red (capa 3) y la capa de transporte (capa 4).
- **TDM:** Time Division Multiplexing.  
Tipo de multiplexación donde dos o más canales de información son transmitidos a través del mismo enlace, al colocarlos en intervalos de tiempo distintos (Time Slot) para la transmisión de cada canal. Es decir, el canal se turna el uso del enlace. Se requiere de una señal de sincronización digital periódica o identificador para que el receptor



reconozca el canal. TDM se vuelve ineficiente cuando el tráfico es intermitente porque el intervalo de tiempo (Time Slot) se otorga a un canal incluso cuando no transmite. Para salvar esta deficiencia, se desarrolló la multiplexación por división estadística del tiempo (STDM).

- **Túnel:** encapsulador de un protocolo A en otro B, de tal forma que el segundo trata al primero como si fuera una capa de enlace de datos. También se usa para obtener data entre dominios administrativos que usen un protocolo no soportado por la Internet que conecta dichos dominios.
- **VCI:** Virtual Channel Identifier (Identificador de Canal Virtual).  
Campo de 16 bits en el encabezado de una celda ATM. Su función es similar a la de un DLCI de Frame Relay.
- **VoIP:** Voz sobre IP.
- **VPI:** Virtual Path Identifier (Identificador de Trayecto Virtual).  
Campo de 8 bits en el encabezado de una celda ATM. El VPI, así como el VCI, es utilizado para identificar el destino sucesivo a medida que una celda pasa a través de una serie de switches ATM hacia su destino final.
- **VPN:** Virtual Private Network (Red Privada Virtual).  
Es el uso de encriptación en las capas inferiores de protocolo, para proveer una conexión privada o segura dentro de una red pública o insegura. Las VPN son por lo general más baratas que las redes privadas reales que utilizan líneas privadas pero dependen que en ambos extremos se utilice el mismo sistema de encriptación. La encriptación puede ser realizada por software de Firewall o posiblemente por Routers.
- **WAN:** Wide Area Network (Red de Area Amplia).
- **WWW:** World Wide Web.

## BIBLIOGRAFÍA

1. Srinivas Vegesma: "IP Quality of Service" de Cisco Press.
2. Data Communications: Calidad de Servicio en Redes IP, ATM y FR.
3. R. Redford : "Enabling Business IP Services with Multiprotocol Label Switching", Cisco System.
4. R. Redford : "Intranet and Extranet Virtual Private Networking", Cisco System Inc.
5. E. Rosen, A. Viswanathan and R. Callon, IETF Draft : "BGP/MPLS VPN".
6. Seminario Internacional : "The New World of Virtual Private Networking Services" – Cisco Perú.
7. Croll, E. Packman: "Managing Bandwidth, Deploying QoS in Enterprise Networks", Prentice Hall, Julio 1999.
8. Calidad de Servicio en Redes IP  
Ms. José Manuel Rodríguez  
Universidad Distrital – España
9. Calidad de Servicio: Una Solución Global para Empresas.  
Philippe Fischer, Philippe Levilla in Alcatel IND
10. Parámetros de medida de la Calidad de Servicio en ISPs.  
Ing. Armando Ferro, Marivi Higuero Escuela Técnica Superior de Ings. Industriales y Telec. de Bilbao.
11. <http://www.ls.fi.upm.es/doctorado/RedesArquitecturasIP.html>
12. <http://ls.fi.upm.es/doctorado/ArquitectRedesCalidad.html>
13. <http://gosforum..com>
14. <http://www.ietf.org/html.charters/mpls-charter.html>

15. <http://www.ietf.org/html.charters/diffserv-charter.html>
16. [http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls\\_wp.htm](http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.htm)
17. [http://www.cisco.com/warp/public/cc/cisco/mkt/serprod/dial/ievpn\\_rg.htm](http://www.cisco.com/warp/public/cc/cisco/mkt/serprod/dial/ievpn_rg.htm)
18. [http://www.cisco.com/warp/customer/3/latam/servicio\\_qos.html](http://www.cisco.com/warp/customer/3/latam/servicio_qos.html)
19. <http://cisco.com/go/mpls>
20. [http://www.tml.hut.fi/Opinnot/Tik-110.551/1996/qos\\_rout.html](http://www.tml.hut.fi/Opinnot/Tik-110.551/1996/qos_rout.html)
21. <http://www.isi.edu/rsvp>