# MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA

**SHIRLEY CAROLINA QUINTANA TEJEDA**
**MELISSA OTILIA TABARES RODRÍGUEZ**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**
**FACULTAD DE INGENIERÍA**
**DIRECCIÓN DE PROGRAMA DE INGENIERÍA DE SISTEMAS**
**MINOR EN COMUNICACIONES Y REDES**
**CARTAGENA DE INDIAS, D. T Y C.**
**2011**

# MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA

**SHIRLEY CAROLINA QUINTANA TEJEDA**
**MELISSA OTILIA TABARES RODRÍGUEZ**

**Proyecto presentado como requisito final para optar al título de Ingeniero de Sistemas**

**DIRECTOR:**
**Ph.D. JAIRO ALBERTO GUTIÉRREZ DIAGO**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**
**FACULTAD DE INGENIERÍA**
**DIRECCIÓN DE PROGRAMA DE INGENIERÍA DE SISTEMAS**
**MINOR EN COMUNICACIONES Y REDES**
**CARTAGENA DE INDIAS, D. T Y C.**
**2011**

**Nota de aceptación**

_____

_____

_____

_____

**Jurado**

_____

_____

_____

Cartagena de Indias, D. T y C. Noviembre de 2011

**Señores**

**COMITÉ CURRICULAR**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

Ciudad

Respetados señores:

Con todo el interés me dirijo a ustedes para presentar a su consideración, estudio y aprobación la monografía titulada **"MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA"**, como requisito para obtener el título de Ingeniero de Sistemas.

Atentamente,

_____

**SHIRLEY CAROLINA QUINTANA TEJEDA**

Cartagena de Indias, D. T y C. Noviembre de 2011

**Señores**

**COMITÉ CURRICULAR**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

Ciudad

Respetados señores:

Con todo el interés me dirijo a ustedes para presentar a su consideración, estudio y aprobación la monografía titulada **"MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA"**, como requisito para obtener el título de Ingeniero de Sistemas.

Atentamente,

_____

**MELISSA OTILIA TABARES RODRIGUEZ**

Cartagena de Indias, D. T y C. Noviembre de 2011

**Señores**

**COMITÉ CURRICULAR**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

Ciudad

Respetados señores:

Por medio de la presente me permito hacer entrega de la monografía titulada **"MULTIPROTOCOL LABEL SWITCHING (MPLS): USOS, APLICACIONES Y ÁREAS PROMISORIAS DE LA TECNOLOGÍA"**, para su estudio y evaluación, la cual fue realizada por los estudiantes SHIRLEY CAROLINA QUINTANA TEJEDA y MELISSA OTILIA TABARES RODRÍGUEZ y de la cual acepto ser su director.

Atentamente,

_____

**PhD. JAIRO ALBERTO GUTIÉRREZ DIAGO**

Cartagena de Indias, D. T y C. Noviembre de 2011

**AUTORIZACIÓN**

Yo, **SHIRLEY CAROLINA QUINTANA TEJEDA**, identificada con cédula de ciudadanía número **1.128.059.327 de Cartagena**, autorizo a la Universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catálogo on-line de la Biblioteca.

_____

**SHIRLEY CAROLINA QUINTANA TEJEDA**

Cartagena de Indias, D. T y C. Noviembre de 2011

**AUTORIZACIÓN**

Yo, **MELISSA OTILIA TABARES RODRIGUEZ**, identificada con cédula de ciudadanía número **1.047.412.872 de Cartagena**, autorizo a la Universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catálogo on-line de la Biblioteca.

_____

**MELISSA OTILIA TABARES RODRÍGUEZ**

Cartagena de Indias, D. T y C. Noviembre de 2011

Dedicatoria de Shirley Carolina Quintana Tejeda

**A Dios, a mis padres, a mi familia,**
**en especial a mi tía-madrina Rochy;**
**igualmente a mis profesores, a mis amigos,**
**por ayudarme a pensar, decidir y ser**
**una persona, una profesional,**
**una mujer de bien.**

Cartagena de Indias, D. T y C. Noviembre de 2011

Dedicatoria de Melissa Otilia Tabares Rodríguez

**A Dios, a mis padres, a mi abuelita**
**a mis familiares y docentes de la universidad**
**por apoyarme, confiar en mí y hacer de mí**
**una profesional, una mejor persona**

## CONTENIDO

## LISTA DE FIGURAS

## ABREVIATURAS

- *ADSL: Línea de Abonado Digital Asimétrica (Asymmetric Digital Subscriber Line)*
- *API: Aplicaciones y Proyectos Informáticos*
- *ASIC: Circuito Integrado para Aplicaciones Específicas (Application Specific Integrated Circuit)*
- *ATM: Modo de Transferencia Asíncrona (Asynchronous Transfer Mode)*
- *B2B: Business-to-Business*
- *BGP: Border Gateway Protocol*
- *CoS: Clases de Servicio (Class of Service)*
- *CoS-Aware: Soporte de Clases de Servicio*
- *CPE: Equipo Local del Cliente (Customer Premises Equipment)*
- *DWDM: Dense Wavelength Division Multiplexing*
- *FEC: Reenvío de Clase de Equivalencia (Forwarding Equivalence Class)*
- *FIFO: Primero en entrar, primero en salir (First in, first out)*
- *GSM: Sistema Global para las Comunicaciones Móviles (Global System for Mobile Communications).*
- *IETF: Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force)*
- *IFX: Interactive Financial Exchange*
- *IGP: Protocolo De Pasarela Interno (Interior Gateway Protocol)*
- *IP: Protocolo de Internet (Internet Protocol).*
- *IPSec: Seguridad del Protocolo de Internet (Internet Protocol Security)*
- *IPv4: Protocolo de Internet versión 4 (Internet Protocol version 4).*
- *IPv6: Protocolo de Internet versión 6 (Internet Protocol version 6).*
- *ISP: Proveedor De Servicios De Internet ( Internet Service Provider)*
- *LAN: Red De Área Local (Local Area Network)*
- *LDP: Protocolo de Distribución de Etiqueta (Label Distribution Protocol)*

- *LER: Elemento que inicia o termina el túnel (Label Edge Router)*
- *LFIB: Label Forwarding Information Base*
- *LSA: Link State Advertisements*
- *LSP: Camino Conmutado de Etiquetas (Label Switching Path)*
- *LSR: Router Conmutador de Etiquetas (Label Switching Router)*
- *MD5: Algoritmo de Resumen del Mensaje 5 (Message-Digest Algorithm 5)*
- *MPLS: Conmutación de Etiquetas Multiprotocolo (Multiprotocol Label Switching)*
- *OSI: Modelo de Interconexión de Sistemas Abiertos (Open System Interconnection)*
- *OSPF: Open Shortest Path First*
- *PCI DSS: Estándar de Seguridad de datos para la Industria de la Tarjeta de Pago (Payment Card Industry Data Security Standard)*
- *PIM: Protocolo de Multidifusión Independiente (Protocol Independent Multicast)*
- *PPP: Protocolo Punto a punto (Point-to-point Protocol)*
- *PVC: Protocol Version Control*
- *QoS: Calidad de servicio (Quality Of Service).*
- *RDSI: Red Digital de Servicios Integrados*
- *RFC: Petición De Comentarios (Request for Comments)*
- *RIP: Protocolo de Enrutamiento de Información (Routing Information Protocol)*
- *RSVP: Protocolo de Reserva de Recursos*
- *RTC: Reloj en Tiempo Real (Real-Time Clock)*
- *SAR: Segmentación y Reagrupación de ATM*
- *SHDSL: (Single-pair High-speed Digital Subscriber Line)*
- *SLA: Acuerdo de Nivel de Servicio (Service Level Agreement)*
- *SSH: Órdenes segura (Secure Shell)*
- *TCP ACK: Transmission Control Protocol to Acknowledge*
- *TCP: Protocolo de Control de Transmisión (Transmission Control Protocol)*

- *TCP/IP: Protocolo de Control de Transmisiones/Protocolo de Internet (Transmission Control Protocol/Internet Protocol)*
- *TDM: Multiplexación por División de Tiempo (Time-Division Multiplexing)*
- *TI: Ingeniería de Tráfico (Traffic Engineering)*
- *TLV: Tipo-Longitud-Valor - Type-Length-Value*
- *VC: Circuito Virtual (Virtual Circuit)*
- *VLAN: Red de Área Local Virtual (Virtual LAN)*
- *VoIP: Voz sobre Protocolo de Internet (Voice over Internet Protocol)*
- *VPI/VCI: Identificador de Ruta Virtual/ Identificador de Canal Virtual (Virtual Path Identifier / Virtual Channel Identifier)*
- *VPN: Red Privada Virtual (Virtual Private Network)*
- *WAN: Red de Área Amplia (Wide Area Network)*
- *WRED: (Weighted Random Early Detection)*

## RESUMEN

MPLS es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031**.** Ésta, se define como una tecnología de transporte de paquetes a través de una red, usando información contenida en etiquetas añadidas a los paquetes IP. **[1]**

MPLS opera entre la capa de enlace de datos y la capa de red del modelo OSI. Está definida para funcionar sobre múltiples protocolos como Sonet, Frame Relay, ATM, Ethernet o cualquiera sobre el que pueda funcionar PPP. En un principio, también proporcionaba una mayor velocidad puesto que los routers sólo deben mirar la etiqueta para conmutar y no leer la cabecera de la capa 3 para después decidir por dónde enrutar en función del destino y/u otros parámetros. Sin embargo, hay tecnologías que han conseguido aumentar la velocidad de los routers para consultar las tablas de enrutamiento (como ASIC) **[2].**

MPLS aprovecha lo mejor de la capa 2, la rápida conmutación, sin perder de vista la capa 3, para no perder sus posibilidades. Esto se consigue separando de verdad la función de conmutación de la de enrutamiento. MPLS hace más viable la ingeniería de tráfico, permite enrutamiento rápido (porque en realidad hace conmutación, pero con información de enrutador), permite que los equipos de reenvío sean más baratos si sólo deben reconocer paquetes etiquetados, permite ofrecer QoS basándose en diferentes CoS (clases de servicio), hace más fáciles y flexibles las VPN (redes privadas virtuales), y además parece el primer paso para conseguir redes totalmente ópticas. **[2].**

Las capacidades más relevantes de dicho protocolo son cuatro: Soporte de Calidad sobre servicio (QoS), Ingeniería de tráfico, soporte para Redes Privadas Virtuales (VPNs) y soporte multiprotocolo.

**Soporte QoS**

Le da al administrador un mayor control sobre su red, lo que significa menores costos y mayor satisfacción del cliente o usuario final. Además MPLS impone un marco de trabajo orientado a conexión en un ambiente de Internet basado en IP y facilita el uso de contratos de tráfico QoS exigentes.

**Ingeniería de tráfico**

- Facilita la asignación de recursos en las redes para balancear la carga dependiendo de la demanda y proporciona diferentes niveles de soporte obedeciendo a las solicitudes de tráfico de los usuarios.
- Es esencial para los ejes troncales de proveedores de servicios, los cuales deben soportar un uso elevado de su capacidad de transmisión.
- La ingeniería de trafico MPLS envía el flujo de éste a lo largo de la red basándose en los recursos que dicho flujo requiere y en los recursos disponibles en toda la red.
- MPLS emplea la ruta más corta que cumpla con los requisitos del flujo de tráfico, que incluye: requisitos de ancho de banda, de medios y de prioridades sobre otros flujos.

**Soporte de Redes Virtuales Privadas**

- Las VPNs creadas con tecnología MPLS tienen una mayor capacidad de expansión y son más flexibles en cualquier red, principalmente IP. MPLS se encarga de reenviar (forward) paquetes.
- MPLS se encarga de reenviar (forward) paquetes a través de túneles privados utilizando etiquetas que actúan como códigos postales. Dicha etiqueta tiene un identificador que la aísla a esa VPN, más adelante se mostrará ampliamente el funcionamiento de las etiquetas.

**Soporte Multiprotocolo**

Los routers MPLS pueden coexistir con routers IP tradicionales, lo que les facilitaría la introducción de dicha tecnología a redes existentes. MPLS está diseñado para trabajar sobre redes ATM y Frame Relay en las capa 2, pero sólo se implementó con redes IP en la capa 3, debido al dominio total del protocolo en ese espacio.

**Funciones de MPLS**

MPLS posee las siguientes funciones:

- Especifica los mecanismos para gestionar los flujos de tráfico en tamaños diferentes, tales como los flujos entre diferente hardware, las máquinas, e incluso los flujos entre diferentes aplicaciones.
- Es independiente de los protocolos de las capas 2 y 3.
- Proporciona un medio para asignar direcciones IP, por medio de la etiqueta de longitud fija, la cual es utilizada por diferentes reenvíos de paquetes y tecnologías de conmutación de paquetes.
- Utiliza interfaces con los protocolos de enrutamiento como el Protocolo de Reserva de Recursos (RSVP) y el protocolo que calcula la ruta más corta posible (OSPF).
- Apoya a los protocolos de la capa 2 ATM y frame-relay y el protocolo IP. **[3]**

**Beneficios y ventajas**

Una de las principales ventajas de MPLS es el hecho de que es una implementación basada en estándares de etiqueta de la tecnología de conmutación.

Se espera que cuente con el apoyo de la industria ya que eventualmente sustituirá a las redes de conmutación de paquetes actuales. Entre sus beneficios estan:

- Rutas Explícitas: Una característica clave de MPLS es su facilidad para definir rutas. Explícitamente encamina Label Switched Paths, los cuales son mucho más eficiente que la opción de ruta de origen en IP. También proporcionan algunas de las funciones necesarias para la ingeniería de tráfico.

- Redes privadas virtuales (VPNs): Muchas organizaciones utilizan redes privadas construidas con líneas dedicadas para conectar múltiples sitios. Una oferta de transporte que emula el comportamiento seguro, confiable y predecible de estas redes a través de instalaciones de transporte compartido mantiene la promesa de proporcionar ingresos adicionales de servicios al transportista, al tiempo que reduce el coste de propiedad a cargo del cliente. Las VPNs son una emulación de estas redes privadas a través de instalaciones de transporte de tal manera que cada cliente percibe a sí mismo que se ejecuta en una red privada. La infraestructura de los operadores han sido "virtualizados" para apoyar muchas redes independientes y entre sí invisible. MPLS es un ingrediente clave en la construcción de tales redes; las etiquetas MPLS pueden ser utilizadas para aislar el tráfico entre las VPN.

- Multiprotocolo y soporte Multilink: El componente de reenvío de la conmutación de etiquetas no es específico de una capa de red en particular. Por ejemplo, el mismo componente de reenvío puede ser usado cuando se hace la conmutación de etiquetas con IP, así como con IPX. La conmutación de etiquetas es también capaz de funcionar sobre prácticamente cualquier protocolo de Capa de Enlace de transmisión, aunque el énfasis inicial es sobre ATM. El "Multi" en MPLS se aplica por encima y por debajo de la capa de conmutación de etiquetas.

- Capacidad de evolución: La conmutación de etiqueta también tiene la ventaja de una limpia separación entre el control y la expedición de funciones. Cada parte puede evolucionar sin ser afectada por la otra, lo que hace que la evolución de las redes sea más fácil, menos costoso y menos propensa a errores.

- Inter-dominio de enrutamiento: La conmutación de etiquetas permite una separación más completa entre enrutamiento inter e intra-dominio. Esto mejora la escalabilidad de los procesos de enrutamiento y, de hecho, reduce el conocimiento que la ruta requiere de un dominio. Este es un beneficio para los ISPs y las compañías que pueden tener una gran cantidad de tráfico en el tránsito (es decir, el tráfico cuyo origen y destino no se encuentra en la red).

- Intra-dominio de enrutamiento: Mejora la escalabilidad de los procesos de enrutamiento y reduce el conocimiento de las líneas necesarias dentro de un dominio. Este es un beneficio para los ISP y las compañías que pueden tener una gran cantidad de tránsito de tráfico (es decir, el tráfico cuyo origen y destino no está en la red).

- Apoyo para todos los tipos de tráfico: Otra de las ventajas de cambiar la etiqueta que es generalmente no visible para el usuario es que ofrece soporte de todos los tipos de transmisión: unicast, con el tipo de servicio, y los paquetes de multidifusión. La conmutación de etiqueta también mejora los distintos métodos que han sido probados para la integración de IP con subredes basadas en ATM. Esto puede disminuir la necesidad de complejos procedimientos y protocolos que se ocupan de cuestiones como la resolución de la dirección y los distintos modelos de multidifusión y de recursos que reserva la conmutación de etiquetas que se pueden utilizar con los atributos de QoS, que, a su vez, permite que las diferentes clases de acceso a ISP. La conmutación de etiqueta puede permitir que el actual encabezado de IP en

un paquete para cifrar debe estar a disposición de la LSR de la propia etiqueta. De esta manera las fuentes y destinos de los datos no son observables mientras que estén en tránsito **[4].**

**Usos y Aplicaciones de MPLS**

Entre las principales aplicaciones de la tecnología se destacan las siguientes:

- MPLS mejora y simplifica el reenvío de paquetes a través de routers utilizando paradigmas de switches capa 2.
- MPLS es simple, lo que permite una fácil implementación.
- MPLS aumenta el rendimiento de la red, ya que permite el enrutamiento conmutado a la velocidad del cable.
- MPLS es compatible con QoS y CoS para la diferenciación de servicios.
- MPLS utiliza ingeniería de tráfico para su configuración y de ésta manera ayuda a lograr un mejor nivel de garantía del servicio.
- MPLS incluye disposiciones sobre la restricción basada en rutas explícitas de instalación.
- MPLS es una tecnología que aún no está estandarizada por la IETF y se está iniciando la implementación en los proveedores de banda ancha**.[5]**

# INTRODUCCION

A través de la presente monografía, se pretende analizar las características, funcionamiento, beneficios, ventajas y aplicaciones de la tecnología MPLS.

Por medio de diferentes investigaciones se ha llegado a definir que MPLS es una solución clásica y estándar al transporte de información en las redes. Aceptado por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando enrutamiento de paquetes con ciertas garantías de entrega (QoS).

MPLS Integra el control del enrutamiento IP (capa 3) con la simplicidad de la conmutación de la capa 2. Además, MPLS permite a los proveedores de servicios construir redes altamente confiables y escalables, ofrece a los clientes de IP servicios diferenciados en función de calidad de servicio y otras características.

El propósito del grupo de trabajo de MPLS es estandarizar una tecnología que sirva de base y que combine el empleo de la conmutación de paquetes con el routing, para ello, se necesita integrar este módulo en el componente de control (que utiliza routing) en la capa de red. Para llevarlo a cabo, se desarrolló esta propuesta, con el propósito de satisfacer los siguientes requerimientos:

- MPLS podrá ejecutarse sobre cualquier tecnología en la capa de red, como puede ser, ATM.
- Deberá soportar flujos de trafico tanto unicast como multicast.
- Deberá ser compatible con el modelo de Servicios Integrados de la IETF, incluyendo RSVP.
- Deberá ser escalable, para soportar el crecimiento constante de las estructuras corporativas, y, más globalmente, la expansión de Internet.

- Deberá admitir herramientas de soporte, administración y mantenimiento al menos tan flexible como las que soportan las redes actuales IPV4.

La finalidad de la integración de redes es  poder optimizar el servicio brindado por las redes actuales de transporte masivo; ya que tanto los nuevos abonados como los nuevos servicios que se les puede ofrecer requieren una utilización del medio más eficaz y productivo.

# OBJETIVOS

## Objetivo General

Identificar y describir, a través de un documento escrito, las características principales de la tecnología Multiprotocol Label Switching (MPLS) que la convierte en una de las tecnologías más promisorias.

## Objetivos Específicos

- Determinar las razones por las cuales se utiliza la tecnología MPLS como método para proporcionar calidad de servicio en las redes.

- Describir las características de la tecnología MPLS, por medio del análisis crítico de la literatura.

- Indicar el potencial que tiene MPLS como protocolo básico de redes más robustas y sus funciones, para que sirva de guía en la elaboración de propuestas de mejoramiento a soluciones telemáticas.

- Identificar las áreas promisorias de implementación de la tecnología MPLS y su aplicación en un futuro cercano.

## JUSTIFICACIÓN

MPLS surge como una solución para mejorar el desempeño de las redes de conmutación por paquetes y subsecuentemente se reconocieron y aprovecharon sus características para implementar redes con mejoras en el área de calidad de servicio.

Es muy importante difundir los beneficios de la tecnología MPLS, porque ésta permite la gestión de flujos de tráfico con características diferentes, prestándoles un servicio diferencial y un manejo más sofisticado en áreas como ingeniería de tráfico y redes privadas virtuales.

Esta monografía tiene como fin familiarizar al lector con las características y funcionalidad de MPLS y también identificar áreas promisorias para el uso de la tecnología. El estudio de este reporte permitirá a las empresas y proveedores de servicios construir redes inteligentes de próxima generación que ofrecen una amplia variedad de servicios avanzados de valor añadido sobre una infraestructura moderna de conmutación de paquetes.

# 1. MPLS COMO MÉTODO PARA PROPORCIONAR CALIDAD DE SERVICIO EN LAS REDES

## 1.1 ANTECEDENTES DE MPLS

El Internet desde sus inicios tuvo igual tratamiento para los flujos de datos, utilizando el modelo de servicio "*best-effort*"**[6].**

MPLS comenzó su desarrollo en 1996, paralelamente en tres empresas: IP Navigator en cascada Comunicaciones, Tag Switching de Cisco Systems, y el período total de la ruta-Based Switching (ARIS) de IBM (y en menor medida, Ipsilon IP de conmutación y de la célula de Toshiba Switch Router) para resolver el mismo conjunto de problemas en las redes IP:

- En ese momento, el enrutamiento IP era difícil implementarlo en hardware, y las implementaciones de software limitaron el tipo de cambio forward de paquetes en los routers IP.
- El reenvío de paquetes IP en los routers se vinculaba al proceso de enrutamiento IP, que contribuyó sin hacer caso a las interrupciones de carga en la red, dando lugar a congestiones de la red, de las cuales algunas están sobreexplotadas, mientras que otras están subutilizadas.
- Las redes IP fueron estratificadas a través de redes ATM, lo cual era muy costoso en términos de gastos generales (añadiendo un 25 por ciento o más a todos los paquetes IP), pero había una gran ventaja: a los paquetes IP se les incluyó un proceso conocido como ingeniería de tráfico que obligó a aliviar la congestión.**[7]**

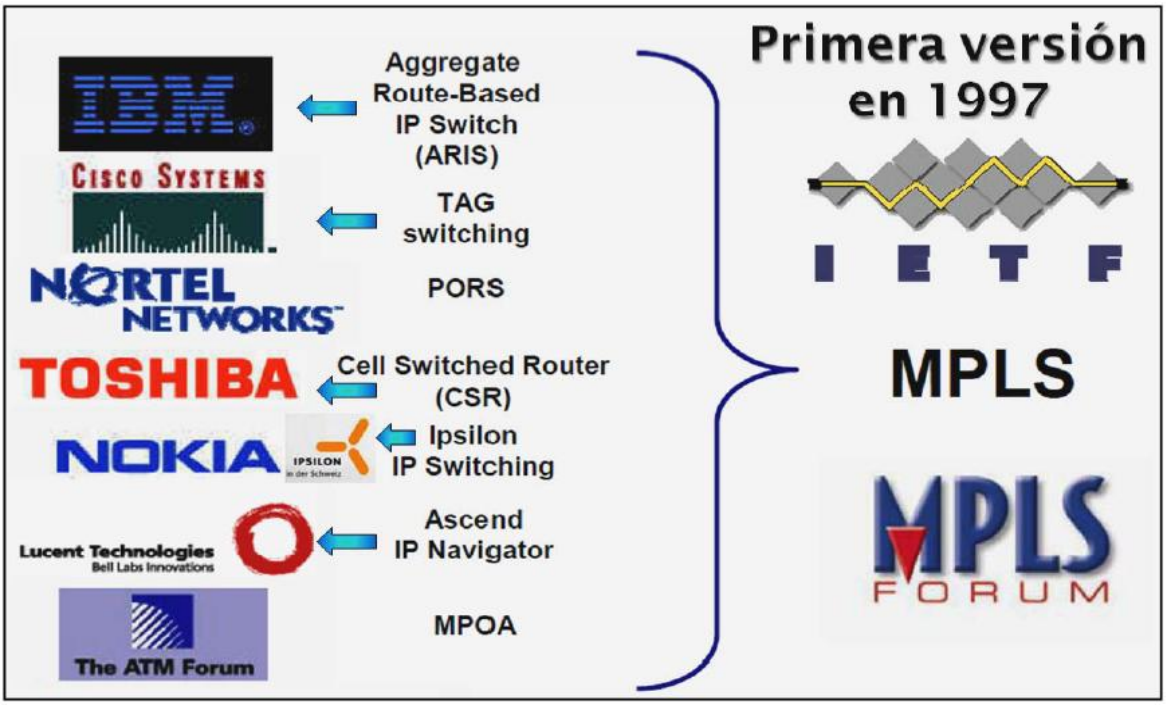


**Ilustración 1 . Origen de MPLS [10]**

Lo que los proveedores de servicios querían era una manera de hacer ingeniería de tráfico sin congestiones **[7].**

Si el internet es consolidado como la red de datos del futuro, es necesario introducir cambios tecnológicos que permitan ir más allá del nivel *best-effort,* es decir*, existía la necesidad de implementar garantías de calidad de servicio,* y para esto se considera la tecnología MPLS, fundamento para el acceso en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las garantías necesarias **[8].**

MPLS surgió como un acuerdo de diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los años 90’s, como una necesidad de satisfacer las demandas de QoS de los usuarios de la red causados

por el gran crecimiento que ha tenido el número de usuarios y el gran volumen de tráfico en la red.

MPLS, es una solución adaptable a varias aplicaciones para hacer frente a los problemas que se presentan en las redes tales como velocidad, escalabilidad, QoS, ingeniería de tráfico entre otros. Además de convertirse en una solución para cubrir el ancho de banda y los requisitos de servicio **[9].**

En síntesis, MPLS es una evolución de numerosas tecnologías propietarias de conmutación de etiquetas. Esas técnicas se conocieron como conmutación IP o conmutación multinivel. Todas ellas condujeron a la adopción del actual estándar MPLS conocido como REC 3031 IETF. **[10]**

## 1.2 INTRODUCCIÓN A LA TECNOLOGÍA MPLS

MPLS, es creado con el fin de mejorar la compatibilidad entre la Capa de Red, protocolo IP, y la capa de enlace, tecnologías como ATM, Frame Relay, PPP, entre otros. Posee nuevas características tanto de capa de red como de capa de enlace, lo cual lo hace atractivo para la Internet de la nueva generación. Además de estas facilidades, se provee de QoS y de Ingeniería de Tráfico tanto para la generación del camino como para la restauración de éste. **[11]**

MPLS se define como una tecnología de transporte de paquetes a través de una red, usando información contenida en etiquetas añadidas a los paquetes IP. **[10]**

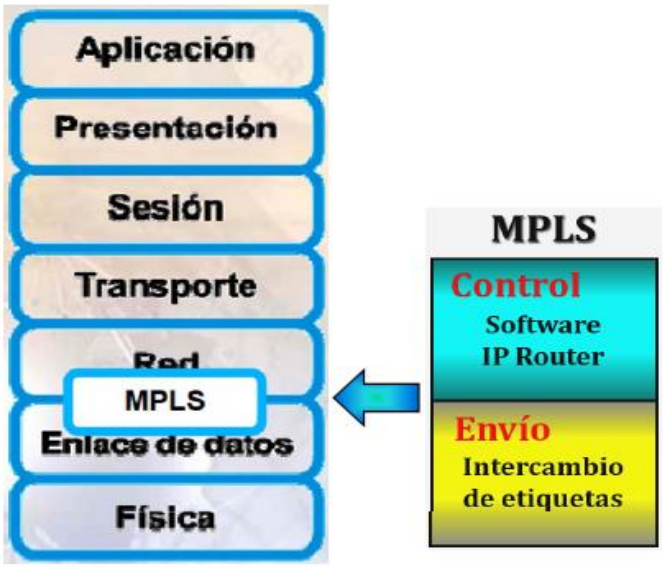


**Ilustración 2. . MPLS y el modelo OSI [10]**

Es importante destacar que MPLS no es un protocolo de nivel de red; éste no tiene enrutamiento ni direccionamiento propio, pero utiliza a IP. Además, esta tecnología tampoco es un protocolo de nivel de enlace, pero trabaja sobre diferentes tecnologías de esta capa. En otras palabras, MPLS no es una capa del modelo de referencia OSI. **[10]**

MPLS se implementa principalmente en redes IP, siendo capaz de interactuar con las tecnologías de la capa 2 más utilizadas. Asimismo, une la velocidad de las redes de capa 2 y la inteligencia de las redes IP. **[12]**

Igualmente, MPLS agrega nueva información a los paquetes: las etiquetas, que tienen un encabezado de valor fijo de 32 bits, que no es parte del encabezado de capa 3 ni del de capa 2. **[13]**

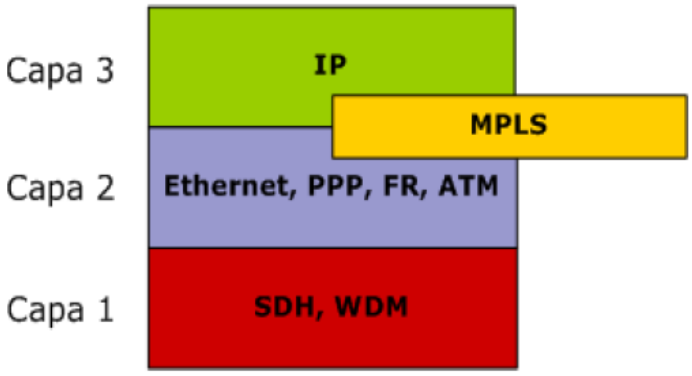


**Ilustración 3. Etiqueta en MPLS [13]**

## 1.3 ASPECTOS GENERALES DE MPLS

IP es una red privada que combina la flexibilidad de las comunicaciones punto a punto y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM. MPLS es una solución versátil para corregir los problemas presentados en las redes actuales como los son la velocidad, escalabilidad, calidad de servicio (QoS), administración e ingeniería de tráfico. MPLS tiene la posibilidad de coexistir sobre redes ATM y Frame Relay. Las características principales de una red MPLS se muestran a continuación:

- MPLS es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP
- Introduce una serie de mejoras respecto a IP:
  - Redes privadas virtuales.
  - Ingeniería de tráfico.
  - Mecanismos de protección frente a fallos
- MPLS tiene el potencial para implementar QoS, en otras palabras no es necesario que se trabaje QoS en MPLS (se puede o no se puede usar).

- La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA. Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.
- El etiquetado en la capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LANs.

  Es importante destacar que "La transmisión MPLS, se puede hacer por medio de switches que son capaces de hacer operaciones de búsqueda y reemplazo de la etiqueta, pero no son capaces de analizar los encabezados de capa de red ni de analizarlos a la velocidad adecuada". **[14]**

  "En MPLS, la transmisión de datos ocurre en los label-switched paths (LSPs). LSPs son una secuencia de etiquetas de cada y en cada nodo a lo largo de la trayectoria desde la fuente hasta el destino. LSPs se puede establecer antes de la transmisión de datos (control-driven) o sobre la detección de cierto flujo de los datos (data-driven). Se distribuyen usando el protocolo de distribución de niveles (LDP) o RSVP, o se llevan las etiquetas al igual que en protocolos de encaminamiento como el Border Gateway Protocol (BGP) y el OSPF. Cada paquete de datos encapsula y lleva las etiquetas durante su viaje de la fuente al destino. La conmutación de alta velocidad de datos es posible porque las etiquetas de longitud fija se insertan al inicio del empaquetado y puede ser utilizado por el hardware al cambiar los paquetes rápidamente entre los Links" **[1]**

## 1.4 INTRODUCCIÓN A MPLS CON QoS

Internet está cambiando aspectos en nuestro vivir del día a día, incluyendo la forma de trabajar, estudiar comunicarse y hasta divertirse. El mayor factor del éxito de Internet es su accesibilidad universal, fácil empleo y la convivencia práctica de las tecnologías basadas en aplicaciones Web. Al mismo tiempo, Internet es empleada para la utilización de aplicaciones variadas que requieren estrictos recursos. Como ejemplo de las aplicaciones en cuanto a términos de ancho de banda y otros recursos, se encuentran: Voz sobre IP (VoIP), videoconferencia en tiempo real, video de ráfaga, educación a distancia, transacciones financieras seguras, aplicaciones comerciales B2B (business-to-business), etc. Cada una de estas aplicaciones a su vez, poseen necesidades variadas en cuanto a retardo (delay), variación de retardo (jitter), ancho de banda (bandwidth), pérdida de paquetes (packet loss), y disponibilidad (availability). Todos estos parámetros forman la base de QoS. Las redes IP deben ser diseñadas para proveer la calidad de servicio requerido por estas aplicaciones.

Varios proveedores ofrecen servicios de privilegio definidos por medio de acuerdos de nivel de servicio SLA para priorizar tráfico de ciertos clientes o aplicaciones. QoS aplicada en redes IP provee de inteligencia suficiente a los dispositivos para manejar tráfico preferentemente de acuerdo al SLA y aseguran una política en la red. QoS que se define como aquellos mecanismos que permiten a los operadores de red controlar la mezcla de tráfico, el retardo, la desviación de retardo y la pérdida de paquetes dentro de la red. La calidad de servicio (QoS) no es una funcionalidad dentro de un dispositivo, sino que es una arquitectura de extremo a extremo. Las capacidades de IP QoS permiten a los proveedores darle mayor importancia a las clases de servicio, alojar ancho de banda, y evitar congestiones.

Los proveedores que ofrecen servicios IP sobre un backbone MPLS deberán soportar IP QoS dentro de su infraestructura de red. Esto significa que deberán soportar IP QoS sobre MPLS. **[15]**

Las capacidades de la red dependen de los routers y switches que implementan los protocolos y éstos se han convertido esenciales para la capacidad de hacer el avance hacia esa visión. Sin embargo, muchos expertos consideran que el tradicional hop-by-hop de procesamiento está empezando a llegar a su límite tecnológico.

El reto es desarrollar la arquitectura de red IP de tal manera que al mismo tiempo se prepare para la próxima generación de redes, que permita una transición manejable del entorno actual, donde se controlen los costos, y de esta manera proporciona oportunidades empresariales para los usuarios y proveedores.

Anteriormente se había asumido que sólo había un factor a considerar; la producción de router grandes, más rápidos y más baratos. El crecimiento explosivo de la Internet y su expansión proyectada para muchos millones de direcciones IP ha puesto el rendimiento bruto en el centro de atención (Fabricantes de enrutadores y han respondido bien a la capacidad tradicional de los routers). El desarrollo de conmutación de etiquetas, sin embargo, está siendo impulsado mucho más que la necesidad de velocidad. Dos de los aspectos más significativos son los siguientes:

- Diferentes clases de tráfico requieren un servicio específico con características que deben ser garantizadas a través de la ruta completa por medio de la red (y con frecuencia a través de múltiples sistemas autónomos). MPLS permite la creación de Label Switched Paths con diferentes características de servicio.

- Carrier-class, multi-cliente infraestructuras IP requieren potentes redes que pueden gestionar recursos con mayor eficacia. Desde la perspectiva de los transportistas, la utilización eficiente de los activos de red de clase es la clave de la rentabilidad. Las capacidades de ingeniería de tráfico MPLS de permitir a las compañías un grado de control sobre el comportamiento de la red es que las tecnologías convencionales de propiedad intelectual no lo hacen. Desde la perspectiva de los clientes de la parte inferior, la línea es un mejor servicio - la ausencia de congestión, por ejemplo: Las redes contemporáneas se enfrentan a retos importantes en las siguientes áreas:

  - **Funcionabilidad.** La conmutación de etiquetas proporciona nuevas funciones que no están disponibles o ineficientes con rutas convencionales. Encaminamiento explícito para seleccionar una ruta específica que no puede ser la ruta más corta, es un ejemplo. La elección de un camino sobre la base de otros atributos de la dirección de destino, como calidad de servicio, también son necesarios.

  - **Escalabilidad**. Las redes del futuro deben ser prácticamente ilimitadas en tamaño. La información de ruteo crece muy rápidamente a medida que la red crece, y los routers pueden eventualmente sobrecargarse por si mismos. Las técnicas actuales de despliegue de redes enrutadas por IP sobre circuitos virtuales ATM o Frame Relay exacerban este problema. MPLS requiere que los dispositivos L2 (por ejemplo, Switches ATM), sean capaces de ejecutar el plano de control IP, lo cual aminora el problema. La ingeniería de tráfico, en el sentido de que esta permite un uso más eficiente de los recursos de red también ayuda en la tarea de 'escalar' la red.

  - **Capacidad de evolución.** Uno de los desafíos más grandes será permitir el cambio y crecimiento sin grandes interrupciones en la red.

Los servicios de naturaleza determinista necesitan ser desplegados sobre redes IP no deterministas, múltiples tipos de tráfico IP deben ser aceptados, se necesita establecer y remover múltiples redes privadas virtuales. Aunque el núcleo de la red debe aumentar su capacidad de conmutación, gran parte de la evolución es impulsada por los equipos del borde - el punto de demarcación entre proveedor y usuario. Es esencial que se utilice un dispositivo de grado especial para los usuarios que incorporen nuevas capacidades IP dentro de un modelo de estándares industriales.

- **Integración.** La aplicación de la convergencia de la telefonía IP es un ejemplo de integración de sistemas y la superposición de la red IP en un soporte de infraestructura ATM es un ejemplo con éxito de integración de la red. La integración en todos los niveles es un requisito de diseño de una red eficaz. **[4]**

## 1.5 ARQUITECTURA MPLS Y QoS EN UNA RED IP

Configurado QoS, la red tiene la capacidad de proporcionar un mejor servicio a un tráfico selecto.

Las características de QoS son la asignación de ancho de banda evitando y/o administrando la congestión en la red, el manejo de prioridades a través de la red, políticas y funciones de administración de tráfico de principio a fin a través de la red y encolamiento de tráfico.

MPLS ofrece calidad de servicio bajo un concepto que ayuda a tener un control más completo del tráfico que pasa a través de la red.

### 1.5.1 Modelos de Calidad de Servicio punto a punto

Un modelo de servicio, también llamado nivel de servicio, describe un conjunto de capacidades de QoS punto a punto. Calidad de servicio punto a punto es la habilidad de la red de distribuir servicios requeridos por cierto tráfico específico de usuario desde un extremo de la red a otro. Existen tres modelos de servicio: de Mayor Esfuerzo, más conocido como Best Effort, el Servicio Integrado, conocido como IntServ, y el de Servicios Diferenciados, conocido como DiffServ.

Los modelos de servicio QoS difieren uno de otro en la manera que permiten a las aplicaciones transmitir datos y en cómo la red intenta entregar esos datos. Por ejemplo, se aplica un modelo de servicio diferente a aplicaciones de tiempo real, como son audio, videoconferencia y telefonía IP, de aquél aplicado a la transferencia de archivos y aplicaciones e-mail.

#### 1.5.1.1 Mejor esfuerzo

El servicio de mejor esfuerzo, Best Effort, es un modelo de servicio único en el cual la aplicación transmite datos, archivos o e-mail, siempre que deba, en cualquier cantidad y sin solicitar permiso a la red. Sin asegurarse que exista confiabilidad en recepción, retardos o bajo throughput. Utiliza encolamiento FIFO, el primero en ingresar es el primero en ser transmitido.

#### 1.5.1.2 Servicio Integrado

El servicio integrado, también conocido como hard QoS o IntServ, es un modelo de servicio múltiple que puede acomodar varios requerimientos de calidad de servicio. IntServ fue introducido por el IETF en 1994, RFC en 1633. En este modelo la aplicación solicita un tipo específico de

servicio a la red antes de transmitir los datos. Es decir, absoluta reservación de los recursos de la red para un tráfico específico. La solicitud se realiza por señalización explícita; la aplicación informa a la red de su perfil de tráfico y solicita un tipo particular de servicio que pueda satisfacer su ancho de banda y sus requerimientos de retardo.

La aplicación transmitirá sus datos solamente después que reciba una confirmación de la red.

La red realiza control de admisión, basándose en la información que le da la aplicación y en los recursos disponibles de la red. También se encarga de conocer los requerimientos de QoS de la aplicación mientras el tráfico se mantiene dentro del perfil especificado.

Las características que proporcionan servicio de carga controlada, la cual es un tipo de servicio integrado, son:

- El protocolo de reservación de recursos (RSVP) puede ser usado por las aplicaciones para indicar a los ruteadores sus requerimientos de calidad de servicio.
- Los mecanismos inteligentes de encolamiento pueden usarse con RSVP para proporcionar los siguientes tipos de servicio:
    - Servicio de tasa “garantizada”, RFC2212, la cual permite a las aplicaciones reservar ancho de banda para satisfacer sus requerimientos, para tener retardo asegurado y no ocurran pérdidas de datos. Por ejemplo, la aplicación de Voz sobre IP (VoIP) puede reservar 32 Mbps punto a punto utilizando este tipo de servicio. Empleando encolamiento equitativo priorizado (WFQ) con RSVP se puede proporcionar este tipo de servicio.

- Servicio de carga “controlada”, RFC2211, la cual permite a las aplicaciones tener bajo retardo y alto throughput incluso en momentos de congestión. La red aparece poco congestionada, con menos garantías, con servicio predictivo. Por ejemplo, las aplicaciones de tiempo real, como ser videoconferencia pueden usar este tipo de servicio. Empleando RSVP con detección anticipada de prioridad aleatoria (WRED) se proporciona este tipo de servicio.

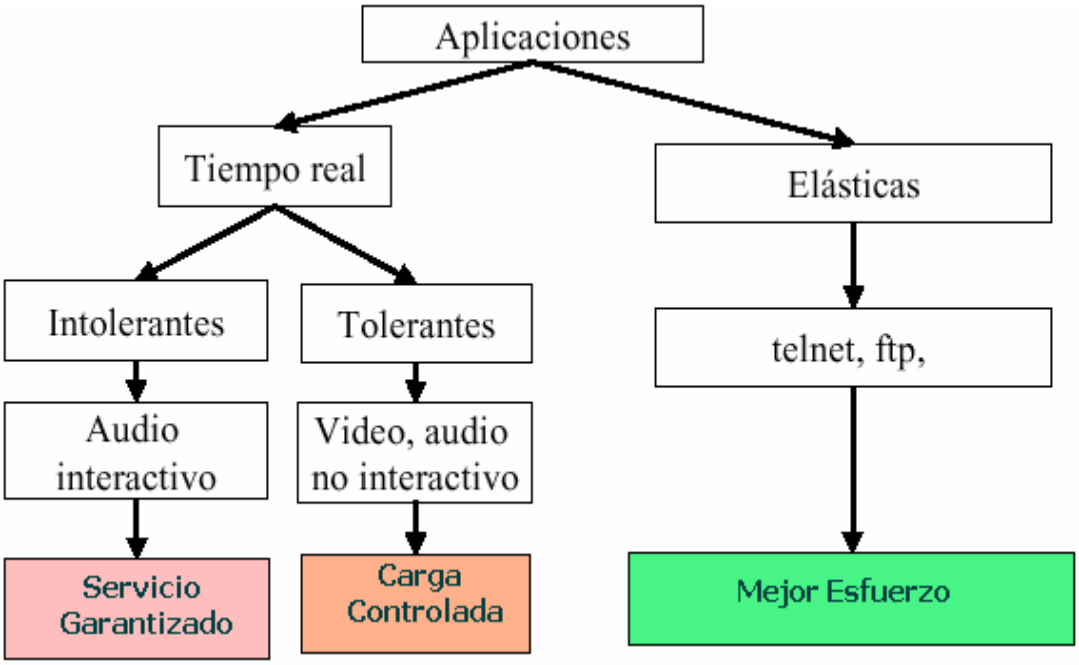


**Ilustración 4. Servicios Integrados [16]**

### 1.5.1.3 Servicios Diferenciados

El servicio diferenciado, también conocido como soft QoS, es un modelo de múltiples servicios que puede satisfacer necesidades de calidades de servicio diferenciables, es decir que cierto tráfico es mejor tratado que el

resto. De cualquier manera, a diferencia del modelo de servicio integrado, un modelo que usa servicio diferenciado no explícitamente informa al ruteador antes de transmitir los datos.

En servicios diferenciados, la red intenta entregar un tipo de servicio en particular basándose en la calidad de servicio especificada en cada paquete. Esta especificación puede ocurrir de distintas maneras, por ejemplo, utilizando las configuraciones de los bits del campo de precedencia IP en los paquetes IP o las direcciones fuente/destino. La red utiliza esta especificación de calidad de servicio para clasificar, formar y controlar tráfico, y realizar encolamiento inteligente. El modelo de servicio diferenciado es utilizado por varias aplicaciones de misión crítica para proporcionar QoS punto a punto. **[16]**

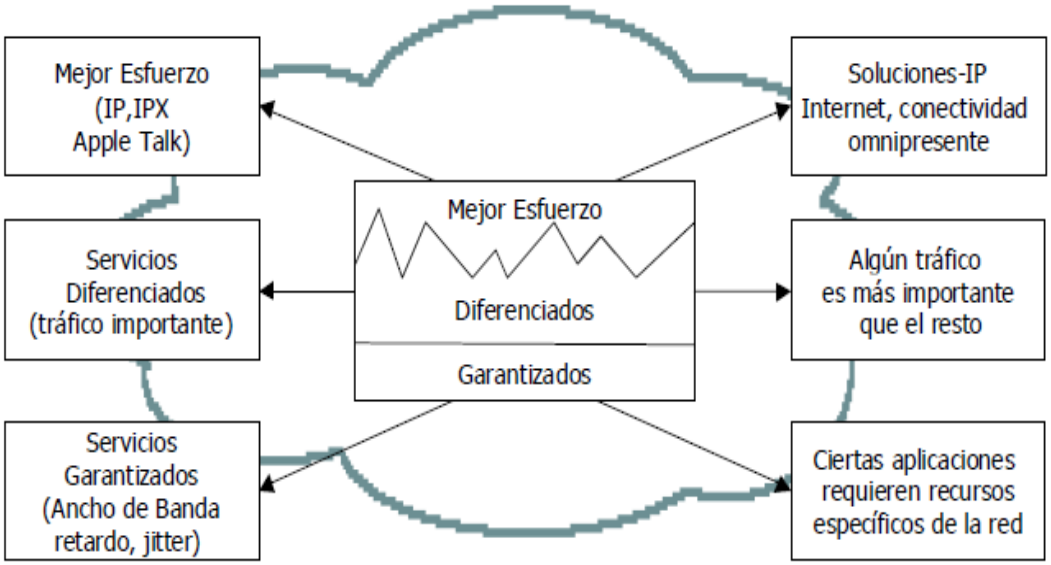


**Ilustración 5. Niveles de calidad de servicio punto a punto [16]**

La arquitectura MPLS nos provee de un circuito virtual o LSP a través de los diferentes nodos que conforman la red MPLS. Gracias a este tipo de

funcionamiento, el circuito virtual creado provee de un trato igualitario a los diferentes tráficos que se envían bajo un mismo túnel LSP bajo una etiqueta FEC en particular. Estudios relacionados a la Calidad de Servicio en diferentes escenarios son de interés actualmente dado que, en comparación con las demás arquitecturas, MPLS ofrece escalabilidad, simplicidad, velocidad, entre otros. Las facilidades que ofrece esta arquitectura para la implementación de Calidad de Servicio son las que se explicarán a continuación:

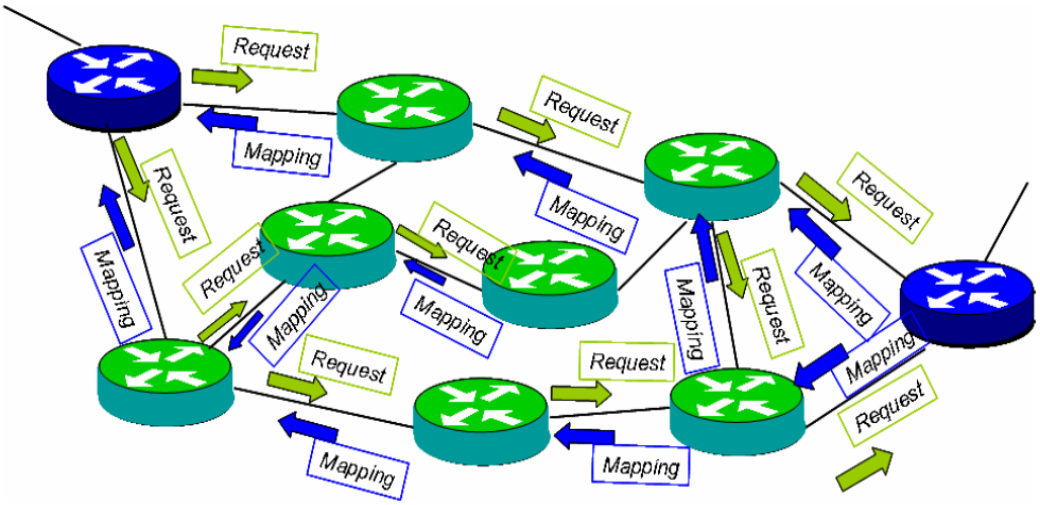


**Ilustración 6. Esquema de envío en la Arquitectura MPLS. Uso de etiquetas [16]**

- **Facilidad de Implementación**. Cualquiera de las formas que existe para el correcto funcionamiento de la arquitectura MPLS requiere de poca señalización entre los nodos. Las contramedidas que se pueden tomar en caso de fallas, protocolos de enrutamiento, entre otras tecnologías de capas superiores y/o inferiores no afecta el funcionamiento de la arquitectura; es decir, para cualquier cambio en cualquier capa la arquitectura se amolda a los posibles cambios sin la intervención del administrador de la red MPLS.

- **Adaptabilidad frente a la Capa de Red como a la Capa de Enlace**. La arquitectura MPLS se localiza entre la capa de red y la capa de enlace, se vale de la conmutación para el envío del tráfico y de los protocolos de enrutamiento para la creación de las tablas de conmutación y de rutas alternas para diferentes fines. Como se puede observar, MPLS utiliza la capa superior inmediata así como la inferior pero su funcionamiento no depende de éstas. Además, MPLS se adapta perfectamente a las tecnologías de capa de enlace; tales como ATM, PPP, Frame Relay, la Familia Ethernet; así como a cualquier tecnología de capa de red como IPv4, IPv6. El cambio se da en el Software y no en el Hardware. Los nodos que conformarían la red MPLS necesitan sólo los procesos correspondientes al manejo de MPLS independientemente de las tecnologías y funcionamiento de la capa de enlace y la capa de red. Para equipos actuales basta con una actualización al sistema operativo de los routers que conforman la Backbone.

- **Se acomoda a los modelos de QoS de la ITU-T**. Gracias al campo experimental EXP, el cual cuenta con 3 bits, se pueden priorizar los diferentes tipos de tráficos cursados en el mismo túnel LSP. Nótese que con 3 bits se pueden obtener 8 tipos de prioridades, lo cual coincide con el número de clases que ha sido propuesta por la ITU-T. Esta característica se suma al hecho de que MPLS es capaz de reservar recursos a través de si mismo así como de diferentes dominios. Puede entenderse que una Clase de Servicio pueda ser implementada bajo una reserva de recursos para ciertos tipos de tráficos provenientes de un cliente y dentro de esta reserva de recursos se daría prioridad a los tráficos que la necesiten.

- **Permite la implementación de Ingeniería de Tráfico.** Gracias a nuevos protocolos de enrutamiento como a mejoras en otros protocolos de capas superiores, MPLS tiene la capacidad de cambiar dinámicamente de ruta. Las nuevas rutas pueden ser generadas por protocolos de capa de red destinados a crear la tabla de enrutamiento bajo ciertas métricas, así también se aplicarán ciertas políticas en estos mismos protocolos para una mejor evaluación de los recursos de la red. Además estudios sobre posibles alternativas, impacto en la Calidad de Servicio (QoS) se llevan a cabo actualmente como la utilización del protocolo RSVP-TE RSVP Traffic Engieering

- **Reserva de Recursos Intradominio MPLS**. Gracias al túnel LSP que se crea para el envío de los tráficos correspondientes, se asegura que la red pueda soportar los requerimientos solicitados dado que si fuese el caso contrario, el túnel no puede establecerse. Así mismo, con el uso de algoritmos de enrutamiento como de protocolos de reserva de recursos

- **Garantía de Calidad de servicio sobre el esquema IP.** A diferencia del esquema actual de Internet Best Effort y de DiffServ, los cuales poseen un comportamiento salto por salto o hop by hop, es decir, no dan una garantía total sobre el envío del tráfico que se inserta a la red IP. MPLS, por su parte, antes del envío construye un túnel LSP, donde el comportamiento es igual en todos los nodos que constituyen este túnel LSP, es decir, los recursos que se destinan para este tráfico FEC serán destinados para éste exclusivamente hasta que el tráfico acabe y se liberen los recursos asignados y sean tomados por otro requerimiento. Aunque IntServ tiene un comportamiento muy parecido en lo que respecta a asignación de recursos, MPLS lo hace de red a red, es decir, crea un túnel LSP desde el router origen al router destino pero no de hosts a host como lo hace IntServ; otra diferencia entre estas

arquitecturas es el hecho que IntServ crea un comportamiento de recursos dedicados por cada flujo en la red, MPLS crea el mismo comportamiento de recursos dedicados, pero con la gran diferencia que los mismos recursos pueden ser usados por diferentes tráficos según los requerimientos especificados en el LSA.

- **Reserva de Recursos Interdominio MPLS**. Así como MPLS está habilitado para el envío como también para la reserva de recursos en las redes MPLS en una misma red de un solo proveedor; gracias al campo Stacking de MPLS se puede extender el túnel creado dentro de una sola red a las redes MPLS que se necesitarán atravesar hasta llegar al destino. En cada dominio MPLS externo se coloca una cabecera adicional al flujo de tráfico, por lo que, el tráfico que poseía una etiqueta será nuevamente etiquetado cuantas veces sea necesario; y estos paquetes se comportarán como paquetes convencionales en esta arquitectura, es decir, al egreso de cada red se les removerá la etiqueta que se les asignó inicialmente. La cabecera MPLS original, es decir, con la que salió de la red MPLS del proveedor tendrá marcado el campo Stacking en 1. Gracias a esta facilidad de MPLS, la reserva de recursos se extiende cuanto sea necesario de una forma muy sencilla en comparación a otras tecnologías.

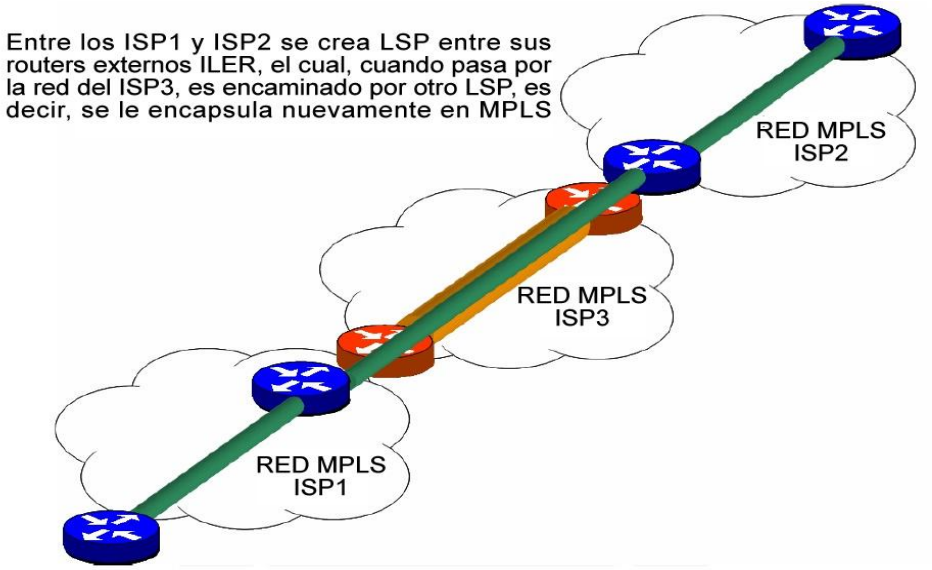


**Ilustración 7. Reserva de recursos Interdominio [16]**

- **Permite la implementación de Balanceo de Carga**. Al igual que la posibilidad de Ingeniería de Tráfico se puede implementar en los nodos que manejan MPLS y es proporcionada por los protocolos de capas superiores, así también el balanceo de carga se puede proporcionar a la red usando estos mismos protocolos según lo crea lo más conveniente el administrador de red. Esta funcionalidad se suele combinar con otras características de MPLS como ingeniería de tráfico ya que así se evitaría la creación de congestión como la subutilización tanto de los enlaces como de los recursos de los nodos con menores capacidades existentes en la red pero que en un instante de tiempo con media a alta congestión podrían convertirse en la mejor ruta de cierto tipo de tráfico con lo que se podrían evitar pérdidas y retardos en el tráfico que cursa la red. **[16]**

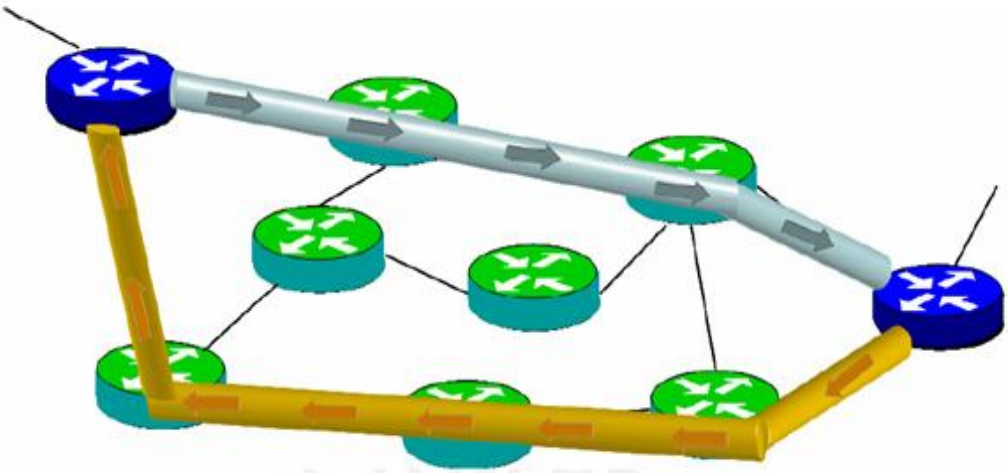

**Ilustración 8. Balanceo de carga en MPLS. Envío de tráfico por diferentes caminos para evitar congestiones [16]**

Otro aspecto para tener en cuenta es que con MPLS los proveedores de servicios pueden definir vías de acceso específicas de entrega de paquetes para el tráfico a través de las redes IP, en lugar de permitir routers intermedios para tomar las decisiones de reenvío de paquetes. Paquete convencional de enrutamiento envía el tráfico a lo largo del camino más corto disponible a través de la red. Moviendo los flujos de tráfico en las rutas menos congestionadas, MPLS mejor puede equilibrar una carga de tráfico de las redes y el tiempo total de respuesta de la red y el rendimiento. Multi-Protocol Label Switching (MPLS) resuelve el problema de calidad de servicio mediante la creación de rutas de acceso explícitas a través de la red. MPLS es una técnica que facilita el transporte de alto rendimiento de Tráfico IP a través de redes de área amplia. En particular, se casa con conexión IP tecnología orientados a la conexión de tecnologías como ATM. MPLS asigna etiquetas a los IP flujos de colocarlos en tramas IP. Los marcos pueden ser transportados a través de paquetes o basados en células de redes y conectar las etiquetas en vez de ser enviados usando IP hacia la búsqueda de

direcciones. Utilizando técnicas de MPLS es posible establecer rutas explícitas para los datos flujos que se ven limitados por la ruta, la disponibilidad de recursos y calidad de servicio solicitada.

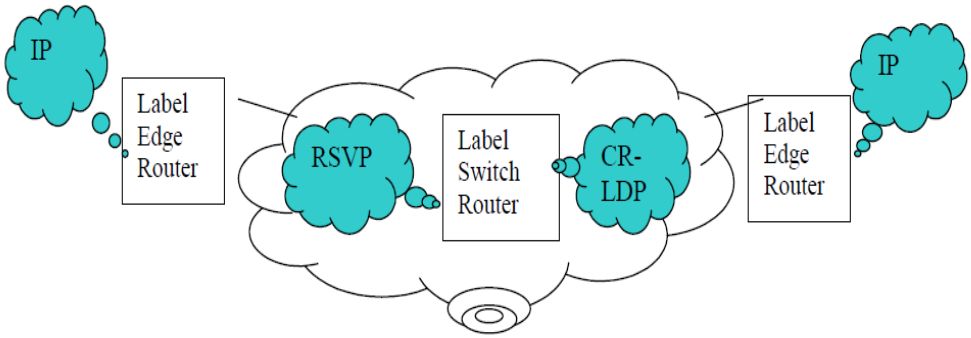


**Ilustración 9. Técnica MPLS para establecer rutas explicitas de datos [17]**

La ruta está definida por la secuencia de direcciones IP de los nodos que se atraviesan. A todos los datos que constituyen un flujo se le da misma etiqueta (formato fijo campo de datos insertados en el frente de cada paquete) a la entrada en la red MLPS. En cada nodo el paquete enrutado basado en el valor de la etiqueta y la interfaz de entrada, se envió en su camino con una nueva etiqueta de valor en la interfaz de salida. Los caminos se conocen como rutas de conmutación de etiquetas (LSP). Puesto que un LSP es un camino bien definido a través de una red IP, que proporciona un medio para asegurar una determinada calidad de servicio QoS, donde se proporciona por la subyacente infraestructura. La naturaleza multi-protocolo de MPLS significa que puede ser utilizado para apoyar IP redes a través de cualquier infraestructura de nivel 2 - el modo de transferencia asíncrono (ATM), en paquetes sobre-SONET, Gigabit Ethernet, Frame Relay, etc. **[17]**

# 2. CARACTERÍSTICAS DE LA TECNOLOGÍA MPLS

## 2.1 INTRODUCCIÓN A LAS CARACTERÍSTICAS DE MPLS

MPLS es una solución versátil para resolver los problemas actuales de las redes, tales como la velocidad, escalabilidad, calidad de servicio (QoS), gestión e ingeniería de tráfico. **[12].** Es por eso, que el principal objetivo de esta tecnología es crear redes flexibles y escalables con un incremento en el desempeño y la estabilidad. Esto incluye Ingeniería de Tráfico y soporte de VPNs, el cual ofrece Calidad de Servicio (QoS) con múltiples clases de servicio (CoS). **[18]**

## 2.2 ESTRUCTURA DE MPLS

La cabecera MPLS posee 32 bits de longitud, distribuidos en cuatro campos, cada uno con una función específica.

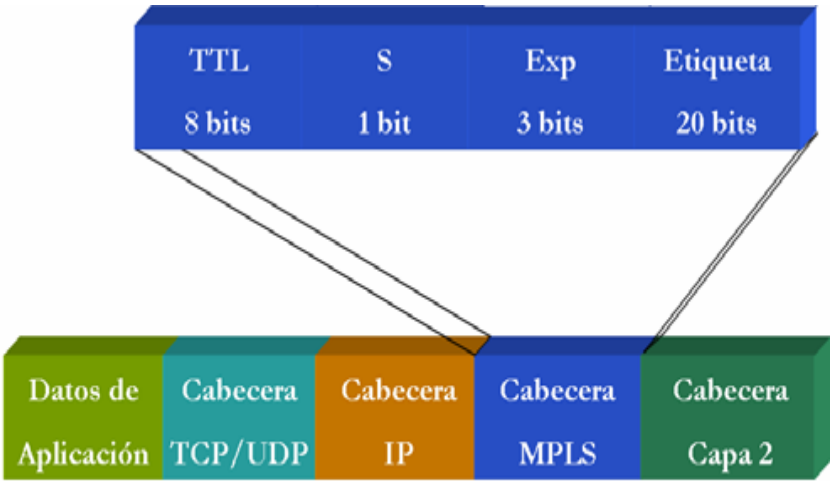


**Ilustración 10. Cabecera MPLS [11]**

- Campo Label o Etiqueta. En base a este campo, los LSR pueden efectuar la conmutación. Esta etiqueta es asignada por el Ingress LER según parámetros descritos en el LSA. Como se indicó antes, los LSP son los que cambian la etiqueta a lo largo de su recorrido para poder formar un túnel LSP y la última etiqueta es extraída por el Egress LER.

- Campo Experimental EXP. Campo para uso experimental, pero actualmente se utiliza para transmitir información DiffServ por la creciente demanda de prioridades en el protocolo IP con lo que se tendrían ocho niveles de prioridad incluyendo el esquema de Best Effort.

- Campo Stacking. Gracias a este campo, se tienen jerarquías de etiquetas. MPLS tiene la capacidad de etiquetar tráfico MPLS de una red vecina con lo que se forma una pila o stack. Toma el valor 1 para la primera entrada en la pila, y cero para el resto.

- Campo TTL Time to Live. Al igual que en el protocolo IP, este campo sirve como un contador del número de saltos para poder evitar la creación de bucles o loops que se puedan generar en el envío de los paquetes etiquetados. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS y es disminuido en una unidad por cada nodo por el que pasa; si llegase a cero en algún LSP, será descartado.**[11]**

## 2.3 ELEMENTOS DE UNA RED MPLS

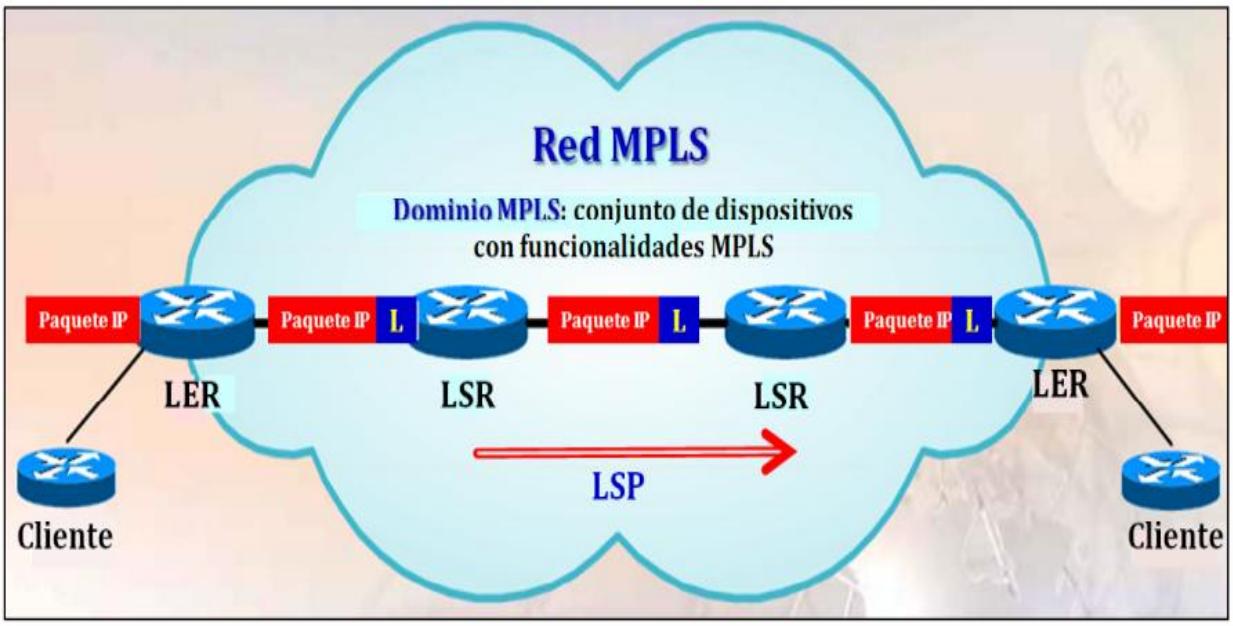


**Ilustración 11. Componentes de una red MPLS [10]**

En MPLS un concepto muy importante es el de LSP, que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs, tales como RSVP-TE o CR-LDP; siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos. Una red MPLS está compuesta por dos tipos principales de nodos, los LER y los LSR, tal y como se muestra en la figura. Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales

como OSPF, RIP y BGP, a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento.

Los LER están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias. **[19]**

## 2.4 CARACTERÍSTICAS DE MPLS

Las siguientes son características que posee la tecnología MPLS:

- **Flexibilidad.** Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a esta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

  La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera) entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

- **Escalabilidad.** Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del Service Provider que conecte este nuevo punto. De esta forma, se evitan tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-confgp
- igurar todos los puntos involucrados.

- **Accesibilidad.** La arquitectura de MPLS VPN permite utilizar prácticamente todas las tecnologías de acceso para interconectar las oficinas del cliente con su "Service Provider" (Proveedor de Servicios).

  Por dicho motivo, la versatilidad que permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, mientras que en el headquarter se utilizan leased lines (TDM) en altas capacidades como E3/T3, que permite dimensionar cada punto de la VPN acorde con sus necesidades sin limitar o restringir la de otros puntos.

  IFX Networks posee acuerdos de interconexión con proveedores líderes de Estados Unidos, Europa y Asia para extender su cobertura de servicios MPLS VPN a cualquier lugar del planeta.

- **Eficiencia.** En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son IP-based, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte introducen. Mediante IFX MPLS VPN - un servicio IP-Based VPN - este costo extra desaparece.

- **Calidad de servicio (QoS) y Clases de servicio (CoS).** Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía email, web u otras aplicaciones. Siendo incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma. Es por esto, que la ya mencionada Convergencia de datos con aplicaciones real-time y/o interactivas, voz y también video de alta calidad, necesitan de una eficiente plataforma de transporte.

Mediante la utilización de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS VPN para cumplimentar los requerimientos de cada servicio o aplicación.

- **Administración.** Las MPLS VPN son denominadas Network-Based, esta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del Service Provider; implicando, entre otras cosas, que la administración de enrutamiento es llevada a cabo por el Service Provider; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

- **Monitoreo y SLAs.** Las MPLS VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del Service Provider. Además, se extienden "Service Level Agreements" (acuerdos de nivel de servicio) para garantizar y asegurar la estabilidad y performance que el cliente necesite.

- **Fácil Migración.** La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el Service Provider; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.

  IFX ofrece, además, servicios profesionales para ayudar a que dicha migración sea transparente.

- **Seguridad.** Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM.

Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.

- **Bajo Costo.** Si las 9 razones previas no son suficientes, siempre que se hable de reducir costos contribuirá fuertemente a inclinar la balanza. Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "más por menos", entre ellos se pueden destacar: Independecia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.

  Convergencia: por ser una VPN CoS-Aware (Soporte de Clases de Servicio) se pueden integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios. **[20]**

## 2.5 REQUISITOS PARA MPLS

Los requisitos que debe tener un router para que emplee MPLS son:

- **Ancho de banda.** Así como el núcleo de Internet se hace cada vez mayor, el volumen de las conexiones dirigidas a dicho núcleo es cada vez más grande. Los proveedores de servicios han estado utilizando durante aproximadamente dos años los puertos de routers OC-192c/STM-64, que permiten que los

routers puedan enviar el tráfico a través de estas conexiones con sistemas avanzados de seguridad y funciones de filtrado a la velocidad de línea.

En el sector de las redes ATM que hacen de interfaz con la capa del paquete, se da una limitación de interfaz impuesta por la función de segmentación y reagrupación (SAR) de ATM. No está disponible en el mercado ningún chip SAR que satisfaga las necesidades de velocidad necesarias para las redes troncales IP existentes en la actualidad. Por tanto, ni los routers ni otros servicios de tramas podrán operar con tecnología ATM a las velocidades exigidas sin la presencia del chip SAR. Y lo que es más importante aún, MPLS, en su versión basada en células, precisa igualmente de la ya mencionada función SAR para su puesta en funcionamiento. En definitiva, la tecnología MPLS basada en células resulta igualmente afectada por esta limitación.

El cell tax, otra de las limitaciones de la tecnología ATM causadas por el ancho de banda, es especialmente grave cuando las células transportan tráfico IP, debido al gran desperdicio adicional de ancho de banda que se da, en la segunda de las dos células que se precisan para transmitir paquetes TCP ACK. La tecnología MPLS basada en células presenta el inconveniente del encabezado adicional del cell tax, inconveniente que está presente de igual forma en las redes ATM de transmisión IP.

- **Tamaño de la red.** Probablemente, la parte más complicada al implantar un router con funciones de operador reside en la ampliación de los protocolos de routing del plano de control. Tal escalabilidad es crucial en el sentido de que permitirá que el router opere de forma robusta y fiable, en una inmensa Internet. Los routers personalizados llevan admitiendo dicha escalabilidad desde hace algunos años, lo que les ha permitido a los fabricantes adquirir la experiencia necesaria en lo referente a algoritmos de routing IP y protocolos

MPLS de señalización. Esta función, necesaria si el plano de envío se basa tanto en células como en tramas, es primordial para el plano de control de la red MPLS. Los fabricantes de equipos basados en células no cuentan ni con la experiencia ni con los conocimientos necesarios para implantar algoritmos de routing para el plano de control que sean a su vez robustos, ampliables, de alta velocidad y carezcan de errores.

- **Seguridad.** La seguridad es algo más que la simple protección de ataques del puerto de gestión del sistema. También supone establecer una autenticación exhaustiva del routing, actualizaciones de las señalizaciones, cortafuegos, protección contra los ataques de negativas de servicio (DoS) y transmisión segura de datos.

  La seguridad supone examinar las cabeceras del paquete IP en varias ubicaciones y a varias profundidades para permitir únicamente el paso del tráfico que se adapta al perfil, proceso conocido como filtrado de paquetes. Los routers personalizados pueden efectuar el filtrado de paquetes IP mediante el hardware a la velocidad de la línea o próxima a ella. Sin embargo, debido a que los conmutadores celulares tienen que trabajar con los paquetes IP en forma de células de transporte, resulta imposible implantar filtros de paquetes basados en las cabeceras.

  Para garantizar la seguridad de sus equipos, los fabricantes de routers han diseñado igualmente un soporte de gestión para el protocolo Secure Shell (SSH) y han empleado el algoritmo de autenticación MD5 para conseguir un routing IP de plena seguridad. Además, los routers ofrecen IPSec para la transmisión segura del routing, señalización y paquetes para la gestión de redes, así como los datos de los usuarios.

- **QoS/CoS.** Del mismo modo en que aumenta la demanda de servicios, también aumenta la demanda de atención a diferentes niveles o clases de servicios. Los fabricantes de routers atienden esta necesidad ofreciendo múltiples CoS, que son más ampliables y manejables que la QoS "por flujo" de ATM. Elementos tales como las CoS y la QoS para MPLS y el almacenamiento temporal para MPLS son similares en el caso de IP.

  La tecnología MPLS se puede emplear en la asignación de recursos para LSP, pero, por razones de escalabilidad, MPLS se suele emplear con múltiples flujos de datos de los usuarios multiplexado en un flujo LSP de MPLS. Obviamente, esta multiplexación se da cuando los paquetes IP se envían a los LSP. La tecnología MPLS permite igualmente establecer una jerarquía de los LSP en uso, de manera que la gran cantidad de LSP más pequeños puede multiplexarse en un único LSP principal. La combinación de envío en IP y en MPLS, por tanto, permite mantener, con gran flexibilidad y cuando sea conveniente, el estado de la información; al mismo tiempo permite un planteamiento flexible y ampliable respecto a QoS. Mientras que los proveedores de routers han optado por esta medida, los proveedores de ATM se han inclinado por un método diferente y de menor escalabilidad.

  En la periferia de la infraestructura basada en células, los dispositivos dependientes de un circuito virtual (VC) celular o los LSP basados en células deben priorizar y programar los paquetes, de acuerdo con los requisitos de CoS, y segmentarlos en células. Este método hace que la función SAR sea aún más compleja, al tiempo que el mantenimiento de la velocidad necesaria se convierte en objeto de difícil cumplimiento. La tecnología MPLS basada en tramas permite la mera aplicación de los bits a la cabecera shim, proporcionando una mayor capacidad de CoS que se puede alojar fácilmente en los routers de conmutación de etiquetas (LSR) basados en tramas, de la misma forma que éstos utilizarían los bits IP en el dominio IP de origen. **[20]**

## 2.6 BENEFICIOS Y VENTAJAS DE MPLS

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporcionan a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering), cursar tráfico con diferentes calidades de clases de servicio o CoS (Class of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, descrita en la RFC 2702, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red. Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades

óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la Internet pública.

Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPN mediante MPLS, pero la mayoría se basan en la RFC 2547. **[19]**

### 2.6.1 Ventajas tecnológicas de MPLS

La tecnología MPLS aporta los siguientes beneficios:

- La seguridad se resuelve utilizando el protocolo MPLS que permite establecer un direccionamiento totalmente privado dentro de la VPN con seguridad total de que los enlaces internos a la VPN sólo pueden intercambiar datos dentro de la propia VPN, quedando a salvo de posibles intrusiones, al no disponer de direccionamiento público.

- Mejora el rendimiento de la VPN ya que los paquetes IP viajan sin cabeceras de túnel, lo que permite aprovechar el rendimiento completo de la línea. Los túneles IP suponen una sobrecarga del 30% de enlace de media y mucho más si casi todo el tráfico es de Terminal Server.

- Multiacceso, MPLS permite integrar diferentes tecnologías de acceso: Punto a Punto, ADSL, SHDSL, RTC, RDSI, GSM, VLAN, etc.

- Escalabilidad simplificada, la red permite añadir o eliminar sedes de manera sencilla y transparente para el resto de la red.

- MPLS es un protocolo de última generación que está diseñado para entornos actuales donde el ancho de banda es abundante y se busca minimizar el retardo.

- Direccionamiento IP privado: La asignación es a libre elección del cliente, permitiendo migrar a la nueva solución sin necesidad de plantearse cambios en la numeración de red.

- Integración de sedes internacionales en la VPN a través de tunelización.

- Definición de Políticas centralizadas de seguridad.

- Políticas de priorización a medida: El tráfico que más le interesa será priorizado sobre el resto de servicios para mejorar la eficiencia de sus comunicaciones.**[20]**

- Mejora desempeño de re-envío de paquetes en la red mediante la conmutación de etiquetas vs. el ruteo de paquetes en las redes IP convencionales.

- Clasificación y asociación de trafico en base a FECs y las interfaces de entrada lo que mejora el manejo del tráfico para su transporte en redes MPLS.**[21]**

### 2.6.2 Ventajas del uso de MPLS

- **Ahorros de costes**: dependiendo de la combinación específica de aplicaciones y de la configuración de red de una empresa, los servicios basados en MPLS pueden reducir los costes entre un 10 y un 25% frente a otros servicios de datos comparables (como Frame Relay y ATM).Y, a medida que se vayan añadiendo a las infraestructuras de networking el tráfico de vídeo y voz, los ahorros de costes empiezan a dispararse alcanzando niveles de hasta un 40%.

- **Soporte de QoS**: uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos.

- **Rendimiento mejorado**: debido a la naturaleza de “muchos a muchos” de los servicios MPLS, los diseñadores de red pueden reducir el número de saltos entre puntos, lo que se traduce directamente en una mejora de los tiempos de respuesta y del rendimiento de las aplicaciones.

- **Recuperación ante desastres**: los servicios basados en MPLS mejoran la recuperación ante desastres de diversas maneras. En primer lugar, permiten conectar los centros de datos y otros emplazamientos claves mediante múltiples conexiones redundantes a la nube MPLS y, a través de

ella, a otros sitios de la red. Además, los sitios remotos pueden ser reconectados fácil y rápidamente a las localizaciones de backup en caso de necesidad; a diferencia de lo que ocurre con las redes ATM y Frame Relay, en las cuales se requieren circuitos virtuales de backup permanentes o conmutados. *Esta flexibilidad para la recuperación del negocio es precisamente una de las principales razones por la que muchas empresas se están decantando por esta tecnología.*

- **Preparación para el futuro**. La mayoría de las empresas han llegado a la conclusión de que MPLS representa “el camino del futuro”**.** La inversión en servicios WAN convencionales, como los citados ATM y Frame Relay, prácticamente se ha paralizado. Según Current Analysis, si hoy el 44% de las empresas todavía utilizan Frame Relay y un 25% ATM, estos porcentajes pronto bajarán en favor de las nuevas alternativas como IP VPN o Carrier Ethernet, de las que MPLS constituye hoy uno de sus principales soportes.**[22]**

# 3. POTENCIAL Y FUNCIONAMIENTO DE MPLS

## 3.1. FUNCIONAMIENTO DE MPLS

La conmutación de etiquetas crea trayectorias predefinidas, por así decirlo, para que los paquetes circulen por la red sin la necesidad de que los Routers examinen el paquete a nivel de capa 3.

Los Routers simplemente envían los paquetes con base en la información de las etiquetas. Todo esto hace referencia a que, anteriormente los Routers tomaban los paquetes, los asignaban a un FEC específico y después asignaban este FEC a un siguiente salto. Esto se hacía cada vez que un paquete arribaba a un Routers y realizaban estas funciones independientemente. Con el modelo de Etiquetas Conmutadas, la asignación del FEC y la determinación de la ruta se hace sólo una vez y en los Routers de borde. La conmutación de etiquetas resume la información y permite conocer todos los destinos posibles y asignar una trayectoria de etiquetas conmutadas permitiendo así el óptimo envío de paquetes.

Para lograr lo anterior, la arquitectura de MPLS se vale de dos planos, el plano de control y el plano de envío. La siguiente figura muestra la arquitectura de estos planos.

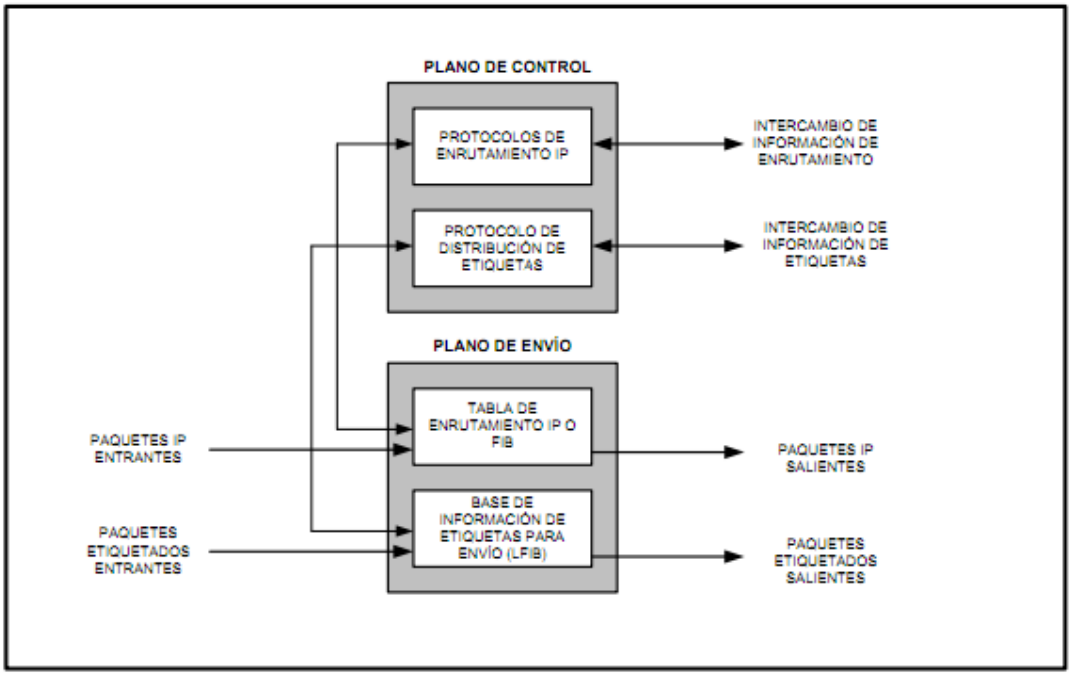


**Ilustración 12. Arquitectura de nodo [23]**

### 3.1.1. Plano de envío

El Plano de envío de paquetes es el responsable de enviar los paquetes con base en la información que se tenga en las etiquetas. Para realizar dicha tarea se vale de la base de información de envío de etiquetas o LFIB. Esta base de Información toma los mapeos contenidos en la base de información de etiquetas o LIB, que tiene los mapeos de etiquetas tanto locales como los de otros nodos, para asociar los siguientes saltos de los paquetes en la red en base a la etiqueta que se tenga y posteriormente enviar los mismos.

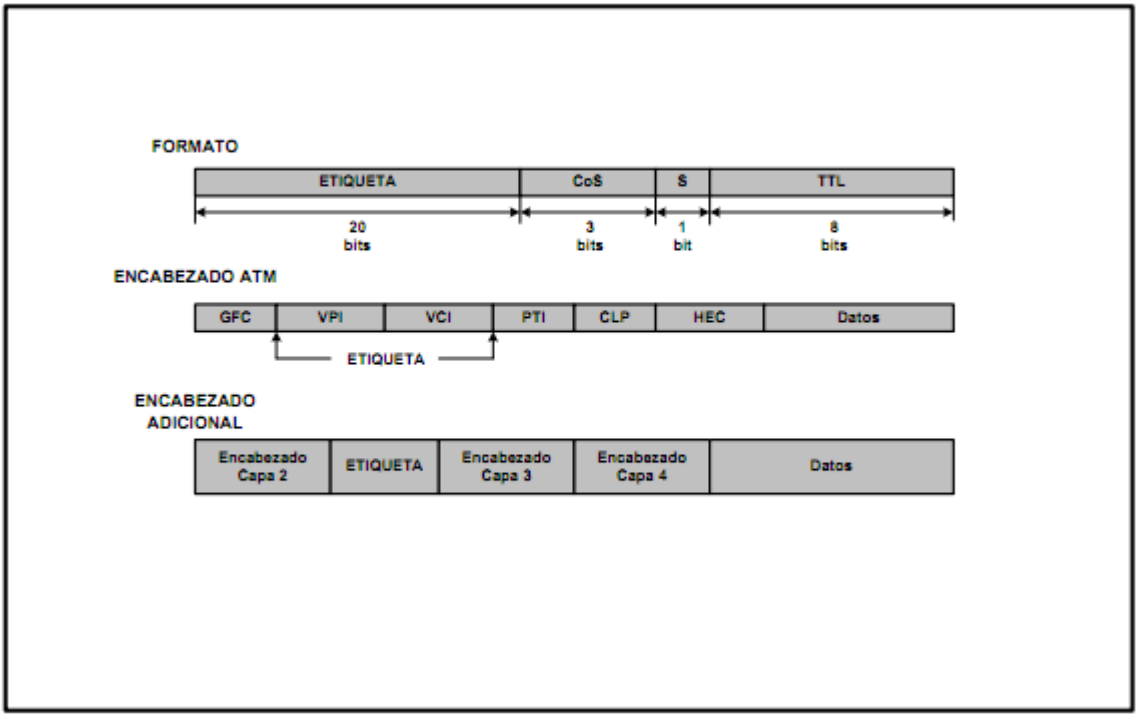


**Ilustración 13. Formato de etiquetas MPLS [23]**

Para el Modelo ATM la asignación de la etiqueta MPLS se hace utilizando el par de datos VPI/VCI. Esto se debe al tamaño fijo que tienen las celdas ATM, a las cuales no se les pueden insertar encabezados como sucede con otras tecnologías de capa 2. El encabezado adicional lleva la información de la etiqueta.

#### 3.1.1.1 Descripción de los campos en una etiqueta MPLS

- Campo de etiqueta: este campo lleva el valor de la etiqueta.
- Campo CoS: este campo lleva el valor de Clase de Servicio que se utiliza para marcar los paquetes y priorizar los mismos en las colas de las interfases.
- Campo de pila: lleva la información jerárquica de la Etiqueta cuando forma Pilas con otras Etiquetas.

- Campo TTL: provee la funcionalidad de tiempo de vida del paquete IP.

La razón de la existencia de la pila de etiquetas es debido a que en algún momento se necesita agregar más de una etiqueta a un paquete. Por ejemplo cuando se configuran VPN´s e Ingeniería de tráfico, se tienen más de una etiqueta, debido a la identificación adicional que se tiene que hacer a la trayectoria de etiquetas conmutadas. Estas subredes tienen una etiqueta que se pone a la salida, la interfase del Router por donde saldrá y el siguiente salto en la red.

La ventaja esencial del plano de envío es que en lugar de usar múltiples algoritmos para el envío de paquetes, utiliza un solo algoritmo basado en la conmutación de etiquetas, lo que trae como resultado que los dispositivos de red puedan hacer un envío de paquetes de alto desempeño y velocidad.

### 3.1.2 Plano de control

El plano de control es el encargado de mantener y propagar a través de la red la LFIB. Para lograr esto, existe un protocolo adicional que se encarga de la distribución y el control de la información de la arquitectura del etiquetado. Existen diversos protocolos que realizan dicha función. El más difundido es el protocolo de distribución de etiquetas o LDP. Este protocolo distribuye la información de la arquitectura del etiquetado a través de todos los dispositivos que forman parte de la red MPLS.

El plano de control se vale de una segmentación de 5 módulos que se encargan de mantener la arquitectura de etiquetado. Estos módulos son:

- Módulo de enrutamiento Unicast: construye la tabla de FEC usando el protocolo de enrutamiento de la red.
- Módulo de enrutamiento Multicast: construye la tabla de FEC usando el protocolo que utilice la red para el tráfico Multicast, por ejemplo PIM.
- Módulo de ingeniería de tráfico: permite el manejo de las trayectorias conmutadas de etiquetas con fines de ingeniería de tráfico, es decir, se logran manejos de tráfico de una manera fácil, como por ejemplo, balancear carga en links de diferente ancho de banda, mejorar tiempos de respuesta para recuperación de falla, etc.
- Módulo de VPN: este módulo, como su nombre lo indica, es el responsable de la creación de redes privadas sobre la infraestructura MPLS existente.
- Módulo de calidad de servicio: permite el marcaje de los distintos FEC para la aplicación modular de calidad de servicio.**[23]**

## 3.2. APLICACIONES DE MPLS

- Ingeniería de tráfico
- Diferencia los niveles de servicio mediante clases (CoS)
- Servicio de Redes Privadas (VPN)

### 3.2.1. Ingeniería de Tráfico

Adapta el flujo de tráfico a los recursos físicos de la red. La idea principal es que no haya recursos que estén en cuellos de botellas y otros que están muy utilizados. En los años 90’s estos esquemas eran muy rudimentarios. El flujo de tráfico seguirá siempre el camino más corto calculado por el algoritmo IGP. En el caso de que se tenga una congestión en los enlaces se solucionará poniendo más capacidad en los enlaces.

En definición la ingeniera de tráfico se traslada de algunos flujos del algoritmo IGP a otros enlaces, los cuales están menos transitados aunque se encuentran en una ruta más larga.  En la siguiente figura se ve cómo hay 2 rutas para los mismos nodos de origen – destino.

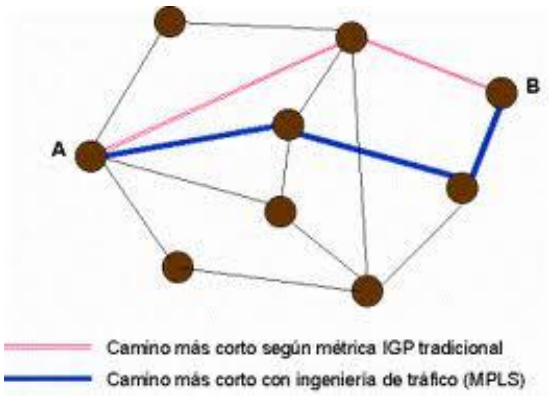


**Ilustración 14. Nodos de origen – destino [24]**

Según la métrica IGP, el camino más corto es el que tiene 2 saltos. Si el acceso de tráfico en los enlaces o en los routes puede ser que se lleve por caminos alternativos indicado con un salto más. MPLS es una herramienta efectiva para las aplicaciones de backbones  ya que:

- El establecimiento de las rutas explícitas específica el camino físico exacto LSP.
- Se obtienen estadísticas de uso LSP, que se puede utilizar para la planificación de la red y para los cuellos de botella y la carga de los enlaces.
- El administrador de la red puede hacer encaminamientos restringidos (Constraint-Based Routing) de tal manera que puede seleccionar rutas

para servicios especiales, como por ejemplo: Pérdidas de paquetes, fluctuación, ancho de banda, etc.

Una de las grandes ventajas de la ingeniería de tráfico de MPLS es que directamente se puede hacer encima de una red IP, en la cual se tenga o no una infraestructura ATM por debajo. Todo esto de manera que se tenga una mayor calidad del servicio, menos costes de planificación y de gestión.

### 3.2.2. Clase de Servicios (CoS)

El modelo DiffServ de IETF está diseñado para definir una variedad de mecanismos para clasificarlos en un tráfico de un reducido número de clases del servicio. El DiffServ permite diferenciar www, correo electrónico, etc. En estos no tienen retardo critico, en comparación con otras aplicaciones donde el retardo es mucho más importante como las de video y voz.

Las etiquetas de MPLS tienen un campo EXP para poder propagar la clase de servicio CoS con su correspondiente LSP.

La red MPLS transporta diferentes clases de tráfico:

- El tráfico que va a través del LSP se le asignan diferentes colas de salida.
- Con distintas prestaciones y con garantías diferentes de ancho de banda se pueden provisionar múltiples LSP mediante un par de LSR exteriores.

Ejemplo:
El LSP puede tener tráfico de máxima prioridad, prioridad media, y para tráfico best-effort, son tres niveles diferentes que tendrán también precios diferentes. **[24]**

### 3.3.3. Redes Privadas Virtuales (VPN)

La red privada virtual se basa en conexiones de infraestructura compartida con funciones de red y de seguridad. El objetivo de las redes virtuales es el soporte de las aplicaciones intra/extranet, donde se pueden integrar aplicaciones de multimedia de voz, de datos y de video. La seguridad supone aislamiento y privadacidad lo cual indica que el usuario cree, que posee los enlaces. Las VPN están basadas en el protocolo de red IP de Internet.

Las VPN más viejas se han construido sobre una infraestructura de transmisión compartida, con las características de seguridad y de respuesta predeterminadas. La seguridad y la garantía las da la separación de tráfico de PVC; Es parecido a ATM. Los inconvenientes son que las rutas se hacen de forma artesanal al tener que establecer cada PVC, si se quisiera conectar todos con todos de forma mallada, se tendría que retocar los CPE del cliente y restablecer los PVC.

La aplicación TCP/IP y las redes NSP han llegado a utilizar esta infraestructura IP para los soportes de Redes Virtuales Privadas, para intentar una mayor flexibilidad en la implementación y reducir el precio de gestión y provisión de servicio.

La forma para utilizar la infraestructura IP para el servicio VPN ha construido túneles IP de diversas clases.

Un túnel IP crea una asociación entre 2 extremos, y parecen que están conectados. Se utiliza una estructura no conectiva como IP para simular estas conexiones. Es una tubería privada que no permite que entre nadie que no sea IP VPN.

Hay dos tipos de túneles IP en conexión dedicada:

- Nivel 3
- Nivel 2, encapsulado de paquetes privados, sobre una red IP pública.

Las Redes Privadas Virtuales están basadas en túneles IPSec, la seguridad se garantiza por un cifrado de la información de datos y de la cabecera de los paquetes IP, que se encapsularán en una cabecera IP para el transporte de red. IPSec es un estándar que nos permite crear VPN a través de las redes de distintos NSP que sigan el mismo estándar.

El IPSec oculta cabeceras de los paquetes originales, entonces las opciones QoS son muy limitadas. IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo sobre los datagrama IP de la red. La red de proveedores no pierde la visibilidad de la IP, en lo que hay muchas más posibilidades de QoS para la priorización del trafico. Se puede mantener un esquema privado de14 direcciones, establecer grupos cerrados de usuario. Los túneles del nivel 2 están condicionados a un único proveedor.

Las ventajas de los túneles IP sobre PVC, tienen características comunes que las hacen menos eficientes frente a la solución MPLS:

- Se basan en conexiones punto a punto
- Configuración manual
- Provisión y gestión complicadas
- Hay problemas de crecimiento si se quiere añadir circuitos virtuales o nuevos túneles.
- La gestión de QoS no se puede mantener extremo a extremo a lo largo de la red.**[24]**

En el MPLS antes de tener conexiones extremo a extremo entre los diferentes emplazamientos de un Circuito Privado Virtual, lo que se tiene son conexiones IP a una “nube común” en la que sólo podrán entrar miembros de los circuitos Virtuales Privados. Las nubes representan las VPN mediante caminos LSP que son creadas por el mecanismo de intercambio de etiquetas de los MPLS. Los LSP son parecidos a los túneles porque la red transporta los paquetes del usuario. La diferencia es, que en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario y en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, el cual no se ve para nada en el proceso de routing IP. Si se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS, sino que ve una Internet privada (Intranet) entre los miembros de VPN. Se pueden aplicar técnicas de QoS basadas en cabeceras IP. La red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

## 3.3 TÓPICOS AVANZADOS DE MPLS

Existen algunas consideraciones que deben ser tomadas en cuenta al momento de la configuración de una red MPLS. Estos tópicos permiten hacer un mejor diseño de la red y a la vez proporcionan alternativas para solucionar problemas potenciales como los siguientes:

- Control de distribución de etiquetas.
- Encapsulación de MPLS a través de enlaces Ethernet.
- Detección y prevención de bucles en MPLS
- Resumen de rutas dentro de una red MPLS

### 3.3.1. Control de distribución de etiquetas

Cuando se utiliza el Control Independiente para la asignación de las Etiquetas, dentro de la configuración normal de MPLS no es posible evitar que se asignen etiquetas a FEC's que probablemente no se deseen. Como se sabe el Control Independiente asigna Etiquetas a todos los posibles FEC's que se tienen en la red MPLS, sin que exista un requerimiento específico de asignación. Suele suceder que en algunos escenarios de migración se desee evitar que algunos FEC's sean asignados con etiquetas. Para casos especiales como este deben aplicarse configuraciones especiales que permitan el filtrado de Etiquetas. El comando tag-switching advertise-tags en conjunto con listas de acceso permite controlar la distribución de etiquetas. A continuación se muestra cómo filtrar Etiquetas para el prefijo 192.168.1.0/24 hacia el LSR vecino con la dirección IP 10.10.10.1, ! tag-switching advertise-tags for 1 to 2 ! access-list 1 permit 192.168.1.0 0.0.0.255 access-list 1 deny any access-list 2 permit 10.10.10.1 **[23]**

### 3.3.2. Encapsulación de MPLS a través de enlaces Ethernet

Como es sabido**,** cuando se configura MPLS en una red de Routers, la generación de etiquetas traerá como resultado el incremento en el tamaño de los paquetes. El incremento generalmente supera los 1500 bytes, y esto genera un problema cuando a través de la red cursan paquetes cuyos bits para fragmentación no están activos. Dichos paquetes no pasan a través del enlace Ethernet. Para solucionar este problema se utiliza un comando que permite la fragmentación previa del paquete antes que ingrese a la red MPLS. El comando es tag-switching mtu. Este comando debe ser aplicado en todas las interfases que manejen la funcionalidad de MPLS. **[23]**

### 3.3.3 Detección y prevención de bucles en MPLS

Con el fin de mantener la estabilidad en la red de MPLS deben existir mecanismos que prevengan el hecho que un paquete se quede circulando por tiempo indefinido en la red. Para esto la arquitectura posee características que previenen dichas situaciones en particular. Existen dos tipos de detección y prevención de bucles, para modo de paquetes y para modo de celdas:

- Detección y prevención en modo de paquetes: existen dos formas. La primera, utiliza el campo TTL del paquete IP en el plano de envío y de esa manera se descartan los paquetes después de cierto tiempo. La segunda, que básicamente es para el plano de control, delega la función de detección y prevención a los protocolos de enrutamiento de capa 3.
- Detección y prevención en modo de celdas: para el caso del plano de envío se utiliza el parámetro TLV, que tiene una función similar al TTL, sólo que en este caso en lugar de ser un decremento del valor, el equipo incrementa el valor de este campo con cada salto hasta que el mismo llega a su valor máximo y el paquete es descartado. Para el caso del Plano de Control se hace una relación entre el valor del TLV y el TTL. Como resultado se tiene que el valor de saltos es trasladado al campo TTL del paquete IP después de restarle un salto para compensar el paso por la red ATM. De esta manera se tiene un control confiable para los posibles bucles que se presenten. **[23]**

### 3.3.4 Resumen de rutas en una red MPLS

El resumen de rutas en una red MPLS debe estudiarse detalladamente, ya que si se aplica de mala manera puede afectar la operación de la arquitectura MPLS. Para evitar problemas cuando se implemente una red

MPLS debe evitarse resumir las rutas de las direcciones que identifican los procesos de LDP (generalmente son direcciones Loopback). Esto se debe a que cuando se hace un resumen de rutas, el Router es obligado a hacer una búsqueda en su tabla de enrutamiento para enviar el paquete y al mismo tiempo genera una etiqueta nula implícita, creando una inconsistencia en la arquitectura de MPLS y rompiendo la trayectoria de etiquetas conmutadas. Esto afectará los servicios que provee la red MPLS. **[23]**

# 4. APLICACIONES Y AREAS PROMISORIAS DE LA TECNOLOGÍA MPLS

## 4.1 APLICACIONES MPLS

MPLS posibilitará la provisión de diferentes servicios, diferenciando Web, correo electrónico y transferencia de archivos de otras aplicaciones más dependientes, como son voz y video. Conjuntamente, esta funciona sobre variadas tecnologías de transporte y facilitará la migración hacia la próxima generación de Internet. Incluso permite a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP. **[20]**

Las redes MPLS permiten tres aplicaciones principales, de las cuáles dos de ellas se utilizan simultáneamente. A continuación se presentan algunas características de estas aplicaciones:

- **Integración IP+ATM:** MPLS integra completamente los servicios IP directos en los switches ATM. El enrutamiento IP y el software del LDP residen directamente en los switches ATM. Por lo tanto MPLS permite que los switches ATM puedan soportar un óptimo multicast IP, clase de servicio IP, Resources Reservation Protocol (RSVP) y redes virtuales privadas (Virtual Private Networks – VPN).

- **Servicio IP de redes privadas virtuales (VPN):** Un servicio VPN es la infraestructura necesaria para servicios de intranet o extranet ofrecidos por un proveedor a clientes corporativos. MPLS, en combinación con el BGP, permite al proveedor de la red soportar miles de usuarios de VPNs. En este sentido MPLS y BGP ofrecen una manera muy flexible, escalable y manejable de proveer servicios de VPNs a través de equipos ATM y equipos basados en conmutación de paquetes.

- **Enrutamiento IP Explícito e Ingeniería de Tráfico:** Un importante problema en las redes IP actuales, es la poca habilidad para ajustar de manera fija los flujos de tráfico IP y hacer un mejor uso de los anchos de banda disponibles en la red. Por otra parte, también existe una falencia en la capacidad de disminuir ciertos flujos por una ruta, al momento de ser necesitados por alguna clase particular de tráfico. MPLS utiliza “Label Switched Path” (LSPs), que son parecidos a los “Virtual Circuits” de ATM, los cuáles pueden ser implementados por equipos basados en ATM y en conmutación de paquetes. La capacidad que MPLS posee en cuanto a ingeniería de tráfico IP utiliza LSPs especiales, los cuales hacen un ajuste fino a los tráficos IP de la red. **[25]**

## 4.2 IMPLEMENTACIONES DE MPLS

En MPLS existen distintos tipos de implementaciones actuales que son: MPLS como una solución IP sobre Ethernet, IP sobre ATM, e IP sobre Frame Relay. No se contempla la aplicación de MPLS a las redes ópticas de próxima generación, conocida como GMPLS (Generalized MPLS), por encontrarse aún en proceso de estudio y estandarización por parte del IETF.

GMPLS es una extensión natural de MPLS para ampliar el uso de MPLS como un mecanismo de control y provisión, no únicamente de caminos en dispositivos basados en paquetes, sino también de caminos en dispositivos no basados en paquetes; como los conmutadores ópticos de señales multiplexadas por división en longitud de onda, los conmutadores de fibras ópticas, y los conmutadores de señales digitales multiplexadas por división en el tiempo. Es decir, GMPLS busca una integración total en la parte de control de las redes de conmutación de paquetes IP y las redes ópticas SONET/SDH y DWDM; dando lugar a las redes ópticas inteligentes de próxima generación, cuya evolución final será la integración

de IP directamente sobre DWDM utilizando algún mecanismo de encapsulamiento como los “digital wrappers”.

La **implementación de MPLS como una solución IP sobre Ethernet**, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, en este caso, la etiqueta MPLS está ubicada después de la cabecera de nivel 2 y antes de la cabecera IP. Los LSR saben como conmutar utilizando la etiqueta MPLS en vez de utilizar la cabecera IP. El funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad. Estas limitaciones propiciaron el desarrollo de la siguiente generación del protocolo Internet o IPv6, definido en la RFC 1883. La versión IPv6 puede ser instalada como una actualización del software en los dispositivos de red de Internet e interoperar con la versión actual IPv4, produciéndose esta migración progresivamente durante los próximos años. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6, estando su uso descrito en la RFC 1809.

La **implementación de MPLS como una solución IP sobre ATM** también está muy extendida. Primeramente indicar, que MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de switches ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (Private Network to Network Interface). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM, puesto que LDP entiende y

utiliza direcciones IP y los protocolos de encaminamiento utilizados en las redes MPLS son los mismos que los utilizados en las redes IP. En este caso, descrito en la RFC 3035, la etiqueta es el valor del VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) de la cabecera de la celda ATM.

Finalmente, MPLS también se ha desarrollado como una solución **IP sobre Frame Relay**. En este caso, descrito en la RFC 3034, la etiqueta es el DLCI (Data Link Control Identifier) de la cabecera Frame Relay. **[19]**

## 4.3 CASOS DE ESTUDIO SOBRE MPLS

A continuación se presentan tres casos de estudio reales de aplicaciones de MPLS en empresas, entre las cuales están el caso del Grupo ConektIA & Claranet, el caso de Cisco, Teldat y Telefónica y el caso de Verizon.

### 4.3.1 Caso Grupo ConektIA & Claranet

Éste caso de estudio hace referencia a la solución de red dada por la empresa Claranet a una empresa española llamada ConektIA.

La empresa ConecktIA, inició en Febrero de 1987, en Barcelona, cuando un grupo de técnicos emprendedores decidió formar parte del mundo de la tecnología punta del momento creando una empresa de software a la que se denominó Aplicaciones y Proyectos Informáticos, S.A., más conocida hoy en día como API.

API fue creada con la idea de dar una solución integrada en el ámbito informático y de gestión a cualquier tipo de empresas, llegando a disponer de un completo ERP para el entorno AS400. A lo largo de tiempo se fue

especializando en el área de Gestión de Personal y Recursos Humanos, siendo en la actualidad una de las empresas líderes en el sector, altamente posicionada con una solución integrada y total en el área.

En el año 1993 API fue premiada por IBM con el Premio "Q" a la Calidad como reconocimiento a su constante y eficaz labor de Servicio al Cliente. Ampliando el servicio a nivel nacional, en Diciembre de 1994 abren sus puertas las oficinas de Madrid, siendo estas ampliadas en dos ocasiones hasta la fecha. En 1999 la empresa R.P.S.3 Information Systems, S.L., conocida como IS3, se une a API formando el Grupo ConektIA, aportando los servicios de ASP y Outsourcing (BPO) de Gestión Laboral, Administración de Personal y RR.HH al conjunto de soluciones ofrecidas por API. En Septiembre de 2002, se inauguran las oficinas de la delegación de Andalucía, ampliándose posteriormente a finales del 2006.

El Grupo ConektIA está integrado por dos empresas, API y IS3 (R.P.S.3 Information System), y nació con vocación de prestar servicios relacionados con el área de la Gestión de Personal y los Recursos Humanos, que van desde la consultoría en servicios y tecnología para estas áreas hasta el diseño, desarrollo e implementación de productos específicos. Grupo ConektIA planteó las siguientes necesidades TI a Claranet:

- Externalizar una plataforma de servidores físicos y virtuales alojados en un rack dedicado para el cliente.
- Disponer de una solución de hosting gestionado de alta disponibilidad
- Conectar mediante una red privada las 3 sedes de la compañía
- Dotar a la compañía de una salida a Internet corporativa

Claranet fue Fundada en 1996 en el Reino Unido, el Grupo Claranet es un Proveedor europeo independiente de Servicios Gestionados. Actualmente, cuenta con oficinas y Datacenters en 6 países: Reino Unido, Francia, Alemania, España, Portugal y Holanda. Ofrece soluciones gestionadas en las áreas de Conectividad, Redes, Hosting y Seguridad, para que las empresas puedan centrarse en su negocio y no tener que desviar sus recursos a la gestión de su infraestructura de servicios TI . Claranet tiene como único objetivo ser su partner tecnológico y ayudarle a definir e implementar soluciones TI a la medida de su negocio.

**La solución de Claranet**

La solución diseñada por Claranet para Grupo ConektIA incluía:

- Implementar una plataforma mixta de servidores físicos y virtuales en un único rack dedicado para el cliente para la externalización de los servidores de la compañía, que garantizara Alta Disponibilidad.
- Diseñar una Red Privada MPLS entre las sedes de Barcelona, Madrid y Cádiz y dotar a las sedes con conectividad xDSL y conexión de respaldo en la central de Barcelona.
- Dotar a la empresa de una salida a Internet corporativa.

Para Grupo ConektIA, lo más importante era el compromiso de calidad. “En primer lugar, el proveedor debía adquirir ciertos compromisos con la calidad del servicio, en cuanto a tiempos, intercambio de información y control de procesos se refiere”. Por esto, Claranet diseñó una solución respaldada por estrictos SLA’s de garantía y nivel de servicio.

Oscar Roda añade: “Nos decidimos por Claranet porque nos podía ofrecer la flexibilidad necesaria para adaptarse a lo que realmente iba a ser más beneficioso para nuestro servicio y nuestros clientes”.

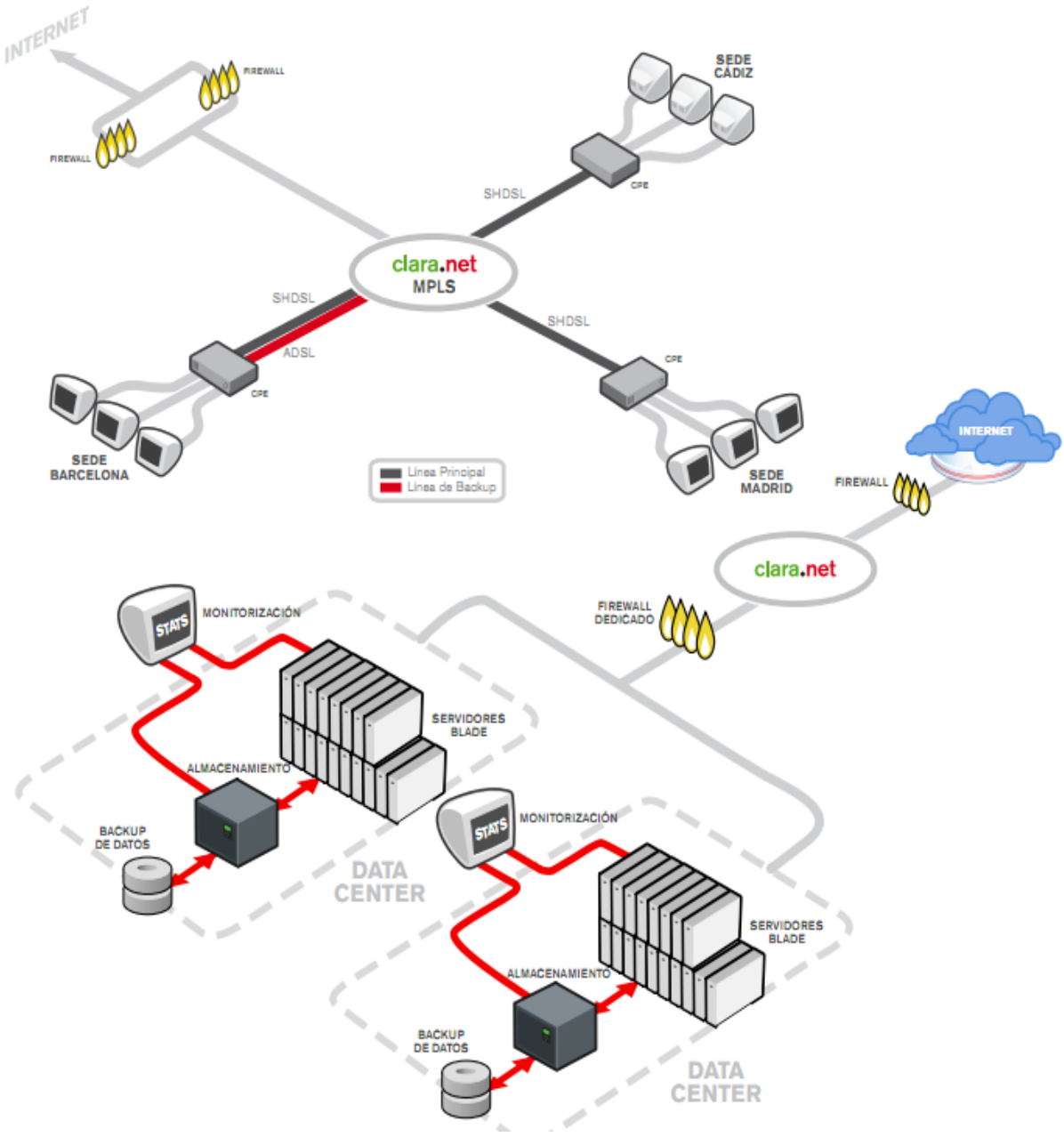


**Ilustración 15. Solución de diseño de una red MPLS por el grupo Claranet [26]**

**Para la implementacion de las VPNs en MPLS**

**Distribución de rutas de VPNs**

Los routers PE emplean el protocolo de ruteo BGP para distribuir las rutas de las VPNs entre cada router. Un router con BGP puede instalar y distribuir una ruta a un solo prefijo por defecto.

Queda claro que se necesita permitir que BGP instale y distribuya múltiples rutas a un solo prefijo IP, y además necesitamos asegurar una política que determine que sitios pueden emplear que ruta. Todas estas metas se alcanzan por medio del empleo de una familia de direcciones.

Las extensiones del Multiprotocolo BGP (MBGP) permiten al protocolo BGP convencional transportar rutas desde múltiples familias de direcciones. Se introduce aquí la noción de VPN-IPv4 address family, donde una VPN-IPv4 consiste en un valor de 12 bytes, donde los 8 primeros bytes corresponden al Route Distinguisher (RD), y siguen 4 bytes de una dirección IPv4.

En el caso de que dos VPNs empleen el mismo prefijo IP, los PEs trasladan estos prefijos a una univoca dirección VPN-IPv4, asegurando que si un mismo espacio de direcciones es empleado en dos VPNs distintas, cada una de ellas mantenga su unicidad intacta y en forma independiente de la otra. BGP propaga información de conectividad de prefijos VPN-IPV4 para cada VPN mediante extensiones del Multiprotocolo BPG (MB-iBGP), los cuales definen el soporte adicional de familias de direcciones que sean IPv4. Esto asegura que las rutas de una VPN dada sean aprendidas solo por los miembros de la misma, permitiendo así la comunicación entre ellos.

VPNs nivel 3 basadas en MPLS están definidas en el RFC 2547bis, publicado por el IETF L3VPN working group. Este RFC define VPNs basadas en el uso del protocolo de ruteo BGP para distribuir etiquetas de VPN (ver

próxima figura). Los routers de borde (PE) activan sesiones BGP entre ellos, en el caso de la figura se ejemplifican dos routers de bordes. El LDP será el encargado de distribuir las etiquetas en el núcleo de la red (core). También en el core, el envío y ruteo de VPN llamada “tablas VRF” son derivadas de las tablas globales de ruteo las cuales residen en cada router.

Con este método una VRF es asignada a cada cliente; por ende cada router de borde (PE) contendrá una tabla de ruteo global y varias tablas VRF, por lo que en una misma conexión el proveedor de servicios o Carrier puede ofrecer Internet y servicios de VPN.Cuando el trafico arriba sobre una VPN, la decisión de envió se realiza acorde a la VRF asociada. El tráfico de Internet podría permanecer siendo ruteado usando la tabla de ruteo global

**Comunidades para las rutas objetivo de VPNs**

La distribución de información de ruteo de una VPN es controlada a través de comunidades para las rutas objetivo de VPNs (VPN route target communities), implementado por medio de las comunidades de BGP extendido. La distribución de información de ruteo funciona de la siguiente manera:

Cuando una ruta aprendida desde un CE es inyectada dentro del MP-iBGP, asociándole una lista de atributos de comunidad extendida para las rutas objetivo de la VPN, y el atributo para dicha ruta es transportado en MP-iBGP hacia otros routers PEs. Típicamente, dicha lista de los valores de comunidad de ruta objetivo (route target community values) es configurada de una lista de exportación de rutas objetivo asociada con la VRF de donde la ruta provino.

Cada VRF, a su vez, es asociada a una lista de importación de comunidades extendida para rutas objetivo. La lista de importación define los atributos de

comunidad extendida que una ruta debe tener para poder ser importada dentro de dicha VRF desde MP-iBGP en un router PE, por ejemplo, la lista de importación de una VRF particular incluye las comunidades objetivo de rutas A, B, y C, y cualquier ruta de una VPN que transporte dicho atributo de comunidad extendida A, B o C será importada dentro de la VRF.

**Distribución de información de rutas de una VPN**

Las posibles técnicas de distribución de información de rutas entre dispositivos PE y CPE (o CE) son enumeradas a continuación:

- Ruteo estático: realizado por configuración, y muy empleado en VPNs con un único punto de salida.
- Ruteo RIP: El router CPE (o CE) y PE establecen una vecindad RIP, y el CPE (o CE) emplea RIP para publicar al router PE el conjunto de prefijos que son alcanzables desde el sitio donde se encuentra.
- Ruteo OSPF: El router CPE (o CE) y PE establecen una vecindad OSFP, y el CPE (o CE) emplea OSPF para publicar al router PE el conjunto de prefijos que son alcanzables desde el sitio donde se encuentra. Esta técnica solo deberá emplearse para VPNS con un único punto de salida.
- Ruteo BGP: El router CPE (O CE) y Pe establecen una vecindad BGP, y el CPE (O CE) emplea eBGP (external BGP) para publicarle al router PE el conjunto de prefijos que son alcanzables a través de él.

Esta técnica es empleada tanto para VPNs con un único punto de salida como para VPNS de tránsito. Desde la perspectiva técnica, el método de distribución mediante BGP resulta el más apropiado debido a:

- No requiere que el PE corra múltiples instancias de algoritmo de protocolo de ruteo para comunicarse con el CPE (o CE), como es requerido en los protocolos IGP (Interior Gateway Protocol).

- BGP fue explícitamente diseñado para la función de transporte de información de ruteo entre sistemas manejados por distintos administradores.
- Si el sitio contiene otra conexión BGP hacia otro router que no sea el PE (BGP backdoors), el correcto ruteo funcionará en cualquier circunstancia. Los demás métodos pueden no funcionar dependiendo de las circunstancias.
- El empleo de BGP facilita al CPE (O CE) pasarle al PE atributos de rutas, como por ejemplo, sugerir un objetivo particular para cada ruta dentro del rango de atributos autorizados en el PE vecino.

El empleo de CPE como salida de la red de routers del cliente (CEs) hacia el PE evita que el cliente deba interiorizarse con el protocolo de ruteo BGP (salvo que el cliente sea un ISP); el cliente solo deberá preocuparse por enviar las rutas que le interese ser transportadas a través del backbone MPLS.

BGP es un protocolo extremadamente escalable que soporta la provisión de un gran número de VPNs.

El protocolo BGP también soporta el intercambio de información de rutas entre routers que no se encuentren directamente conectados (la conectividad entre dispositivos es provista en ese caso por IGP).

**Envío MPLS**

Basándose en la información de ruteo almacenada en la tabla de ruteo IP VRF, los paquetes son enviados hacia su destino empleando MPLS.

El router PE vincula una etiqueta con cada prefijo aprendido desde el router CPE (o CE) e incluye la etiqueta en la información de conectividad de red

(información de vinculación) para los prefijos que son advertidos a otros routers PE. Cuando un router PE envía un paquete recibido desde un router CPE a través de la red, marca al mismo con la etiqueta que recibe del router de destino (en realidad el próximo salto hacia la red destino). Cuando el routers PE destino recibe el paquete etiquetado, remueve la etiqueta y la emplea para determinar el router CPE (o CE) correcto al cual enviar dicho paquete.

**Nota:** Los routers P no son parte del proceso MP-iBGP, y no transportan información de las VPNs.

Los routers P envían paquetes basándose en los valores de las etiquetas adosadas a los paquetes IP. A pesar de que los routers P participan en el intercambio de etiquetas, no terminan VPNs MPLS.

El protocolo LDP de MPLS asegura que todos los routers PE reciban las etiquetas asociadas a las diferentes rutas contenidas dentro de cada router PE, y una red MPLS se encuentra lista para transmitir paquetes cuando el router *PE de ingreso* recibe una etiqueta para el router *PE de salida*.

El envío basado en etiquetas dentro de la red backbone del proveedor se sustenta en la conmutación dinámica de etiquetas. Un paquete de datos de un cliente entonces transporta dos niveles de etiquetas; el primer nivel se emplea para enviar el paquete al próximo salto (hop) correcto, y la segunda etiqueta indica la VRF asociada con la interfase de salida hacia el CPE (o CE) destino. El mecanismo de dos niveles de etiquetas es comúnmente llamado conmutación jerárquica de etiquetas (hierarchical label switching).

Cuando un paquete IP es recibido a través de una interfase particular desde el CPE (o CE), el PE lo asocia a una VRF y obtiene una etiqueta relacionada

con el router PE de salida (el cual identifica la VRF objetivo y la interfaz saliente en el router PE destino: etiquetado de fondo de pila). El router Pe obtiene de la tabla de ruteo global otra etiqueta (tope de pila) que apunta al próximo salto (generalmente un router P), y combina ambas etiquetas en una pila de etiquetas MPLS. Dicha pila es asociada al paquete de la VPN y enviada hacia el próximo salto. Los routers P en la red MPLS examinan la etiqueta de tope y envía el paquete correctamente a través de la red hacia el próximo salto.

El router PE de salida es el encargado de quitar la etiqueta de tope y examinar el fondo de la pila (segunda etiqueta), que identifica la VRF objetivo y la interfaz de salida. La etiqueta del fondo de la pila es extraída y el paquete IP es enviado hacia el correcto router CPE (o CE). **[26]**

### 4.3.2 Caso Cisco, Teldat y Telefónica: Securización de la Red de Datos de Propósito General del Ministerio de Defensa sobre una red comercial IP/MPLS

En este caso de estudio se puede ver como las empresas Cisco, Teldat y Telefonica dan una solución al ministerio de defensa de España con el fin de mejorar su red

**Antecedentes**

La evolución de las comunicaciones corporativas soportadas en redes y tecnologías de caudal garantizado (Punto a Punto, Frame Relay, ATM, etc.) hacia redes WAN soportadas en tecnologías IP/MPLS y/o MetroEthernet proporcionan múltiples ventajas, pero también elevan el riesgo potencial de ver comprometidas la confidencialidad e integridad de las comunicaciones.

Con el fin de asegurar la confidencialidad e integridad de las comunicaciones cursadas sobre redes comerciales IP/MPLS, el Ministerio de Defensa ha acometido un proyecto pionero que interconecta 735 sedes del Departamento mediante túneles IPSec atendiendo a los requisitos dictados por la Autoridad Nacional de Seguridad (ANS).

**Objetivos**

El Ministerio de Defensa cuenta con una Red de Datos de Propósito General (WAN PG) que da soporte a la operativa administrativa del Departamento. Esta red no está sujeta a los requerimientos de seguridad de las redes específicamente militares, pero sí requiere, por la propia casuística del Ministerio, de los máximos niveles de protección.

La red administrativa del Ministerio (WAN PG), concebida en 2002, interconecta 735 emplazamientos, se soporta en operadores públicos y estaba inicialmente constituida sobre redes y tecnologías de caudal garantizado (Punto a Punto, Frame Relay, ATM, etc.).

El Ministerio tenía como un objetivo la migración de esta red hacia IP/MPLS y MetroEthernet, por las ventajas que estas tecnologías aportan (optimización del gasto, mayores caudales, topologías full-mesh, etc.). Sin embargo, había que asegurar, en esta migración, la integridad y confidencialidad de las comunicaciones. Por este motivo se fijó como un requerimiento el diseño de esta red con criterios de seguridad equiparables a redes clasificadas.

**Fases del Proyecto**

En una primera fase, el Ministerio de Defensa identificó, en colaboración con el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia(CNI), los requisitos necesarios para desplegar una Red Privada Virtual sobre redes comerciales IP/MPLS. Estos requisitos implicaban la

necesidad de implementar, con una determinada configuración, túneles IPSec entre los routers extremos de cada enlace. En esta fase se realizó el diseño de red, que establecía una topología en estrella mediante túneles estáticos para tráfico de datos, y una topología full-mesh para tráfico multimedia (ToIP, videoconferencia, etc.) mediante el establecimiento de túneles dinámicos bajo demanda.

En una segunda fase, se invitó a todos aquellos fabricantes interesados en el proyecto a certificar sus equipos en el cumplimiento de los requerimientos del CCN.

El Ministerio de Defensa financió este proceso de certificación, que fue realizado en los laboratorios de la Universidad Carlos III y en la empresa APPlus+. Fabricantes de equipos como Cisco, Juniper, Teldat y 3COM participaron de este proceso de certificación, lo que les obligó a realizar no sólo importantes modificaciones sino incluso nuevos diseños.

En una tercera fase, el Ministerio licitó mediante concurso público la Red de Propósito General. Los pliegos del concurso valoraban aquellas ofertas que incorporaban equipamiento certificado y especificaban la necesidad de implementar la configuración definida por el CCN. El adjudicatario del concurso fue Telefónica, y el equipamiento ofertado fue Cisco en los CPDs y sedes principales, y routers de Teldat en el resto de sedes.

La nueva red contratada incrementó sustancialmente los caudales ofrecidos, sin incrementar los costes asociados a esta partida de gasto. Tras la adjudicación, se inició la fase de despliegue de red. El proyecto contemplaba la posibilidad de establecer una topología full-mesh para servicios multimedia mediante el establecimiento de túneles IPSec dinámicos bajo demanda. El Ministerio de Defensa está desplegando tres pilotos de Telefonía IP de

distintos fabricantes, con el fin de verificar su viabilidad y comprobar que, tanto el tiempo de establecimiento de los túneles como el cifrado de las comunicaciones, no degradan su calidad, permaneciendo los parámetros de retardo, jitter y pérdida de paquetes por debajo de los umbrales recomendados.

**Resultados**

La migración de la Red de Propósito General del Ministerio de Defensa a una red IP/MPLS ha supuesto una mejora sustancial de los caudales ofrecidos a los emplazamientos, sin incrementar el coste asociado a esta partida.

La nueva red de Propósito General del Ministerio de Defensa, al contar con equipos certificados y configurarse de acuerdo con los requisitos exigidos por el CCN, tiene el potencial de acreditarse ante la Autoridad Nacional de Seguridad, lo que posibilitaría el despliegue de sistemas clasificados.

Este proyecto ha contado con una amplia acogida entre los fabricantes de equipos, lo que ha impulsado el desarrollo de nuevas capacidades de cifrado para dar respuesta a la normativa establecida por el CCN. Las nuevas capacidades, desarrolladas e implementadas por los fabricantes en sus equipos, están a disposición no sólo del Ministerio de Defensa, sino de otros Organismos, Entidades y Administraciones Públicas.

**Conclusiones**

El proyecto ha impulsado la implementación de nuevas capacidades de cifrado en el equipamiento de distintos fabricantes, lo que ha permitido soportar la red administrativa del Ministerio de Defensa en redes IP/MPLS comerciales. Esta evolución permite al Departamento optimizar sus comunicaciones desde el punto de vista técnico y económico, manteniendo unos niveles de seguridad equiparables a redes acreditadas.

El Ministerio de Defensa ha abordado con éxito un proyecto pionero e innovador, que no contaba con referencias previas en el mercado **[27]**

### 4.3.3 Caso Verizon: Las redes MPLS privadas extienden la empresa con total seguridad

Verizon Business, una unidad perteneciente a Verizon Communications (NYSE: VZ), con sede principal en Ashburn, Virginia, EE. UU. es líder global en soluciones de comunicaciones y tecnología de la información (TI). La empresa combina experiencia profesional con una de las redes de IP más conectadas del mundo para ofrecer sus galardonadas soluciones de comunicaciones, tecnología de la información, seguridad de la información y red. Conectan de manera segura las empresas extendidas de clientes, socios, proveedores y empleados móviles y dispersos, ofreciéndoles una mayor productividad y eficiencia, y ayudándoles a preservar el medio ambiente. Muchos de los gobiernos y empresas más grandes del mundo, incluyendo el 96 por ciento de las compañías incluidas en el listado de Fortune 1000 y miles de organismos oficiales e instituciones educativas, confían en los servicios profesionales y gestionados y en la tecnologías de red para facilitar sus operaciones.

**Introducción**

La globalización ha ejercido una profunda influencia en la economía mundial. Esto ha hecho que muchas empresas hayan decidido transformar la forma en que se organizan —más empleados con horarios flexibles y que trabajan desde casa— así como la forma en que organizan y gestionan las relaciones con todos aquellos de los que dependen sus negocios, es decir, los clientes, proveedores y socios. En resumen se puede decir que las empresas de hoy en día se han extendido para llegar a todos los rincones y proporcionar

acceso a la información crítica a todos aquellos que la necesitan, donde quiera que se encuentren.

La empresa extendida se fundamenta sobre la base de las redes IP pero, al extenderse a sus clientes, proveedores y contratistas, se encuentra más expuesta a sufrir un ataque electrónico. Esto significa que al haber más información que distribuir y gestionar, y más lugares donde se almacena, aumenta el riesgo de que puedan acceder a ella personas no autorizadas.

En el caso Verizon, se estudian las cuestiones fundamentales a abordar en este contexto y los recursos que servirán para proteger a la empresa extendida.

Para empezar, se examinará el panorama de la seguridad y se propondrá que el enfoque óptimo es aquel que considera a la empresa en su totalidad y, en particular, se hablará de la importancia del uso de una red MPLS privada para negociar con clientes, proveedores, distribuidores y socios dentro de la empresa extendida.

Además, este concepto de seguridad de la información no se puede sustentar únicamente en la adquisición de tecnología, sino que es importante suplementar dicha tecnología con servicios de seguridad prestados por socios de confianza. El objetivo es complementar los productos y servicios de seguridad de TI, que protegen contra amenazas conocidas, con los servicios de un proveedor que asista en la creación de soluciones para reducir el riesgo.

**El trabajo global y la empresa extendida**

A pesar de las dificultades por las que pasa la economía actual, la globalización sigue afectando a las empresas de todos los sectores. El

incremento de la presión competitiva, la rapidez con la que suceden los cambios tecnológicos y la creciente demanda tanto de clientes como de proveedores son el resultado de esta tendencia hacia la globalización.

Aunque las empresas siempre han buscado formas de incrementar las ventas y mejorar la rentabilidad, muchos aducen que la globalización no ha hecho más que imponer un ritmo más acelerado a la consecución de estos objetivos. La transformación que ha experimentado el mercado, en particular en lo que se refiere a las exigencias de los clientes y a las necesidades de los proveedores, ha hecho que las empresas necesiten reaccionar rápidamente a los cambios que afectan a los mercados en los que operan para mantenerse al ritmo de la economía mundial.

Una de las tendencias más influyentes es la reducción del ciclo de vida de los productos. En el sector de la electrónica móvil, por ejemplo, el desarrollo de nuevos productos y su entrada al mercado suceden con extraordinaria rapidez. Algunas de las tendencias más recientes, como por ejemplo la disminución de la demanda de camionetas y vehículos todoterreno (SUV) en Estados Unidos, han demostrado que, en un mercado global, las preferencias de los consumidores pueden afectar tanto a las organizaciones como a sus proveedores, distribuidores, clientes y empleados.

En respuesta a estas tendencias, la fuerza laboral también ha adquirido un carácter más global, con funciones y empleados dispersos que colaboran en los proyectos comunes. Las empresas también han comenzado a extenderse con el fin englobar a las redes comerciales, que incluyen a los clientes, la cadena de suministro, los distribuidores y los socios, para compartir información o contratar conocimientos y experiencia.
La principal necesidad de la empresa extendida es ser más flexible, adaptable y competitiva, además de ofrecer más información a sus

empleados dondequiera que se encuentren. A esto se une que muchas de las relaciones recién establecidas por la empresa extendida son provisionales y sólo duran lo que dura un proyecto específico durante un período de tiempo concreto.

El problema es que el acto de compartir información dentro de esta empresa extendida aumenta el riesgo de exposición, filtración u obtención ilegal de la información por parte de personas no autorizadas. Esto significa que este riesgo se multiplica enormemente con el aumento del volumen de información a distribuir y gestionar, y de los lugares donde se almacena.

Los responsables de hacer llegar a la empresa a más lugares tienen que encontrar un difícil equilibrio entre incrementar el acceso y mantener un control más estricto. La red más segura que existe es aquella que no tiene ningún punto de acceso al mundo exterior, pero está claro que esto resultaría muy poco productivo. Por lo tanto, la única forma de disfrutar de los beneficios que reporta la empresa extendida es disponer de una red que ofrezca acceso a la información crítica, junto con diversos niveles de seguridad.

**Una visión integral de la seguridad**

Aunque, como la mayoría de las empresas, la suya seguramente ya cuenta con algunas soluciones de seguridad, la estructura completa tiene que formar parte de un proceso continuo que requiere que toda la tecnología esté perfectamente integrada.

Para las empresas que operan en el ámbito internacional, la seguridad no puede abordarse únicamente cuando ocurre un incidente o como una cuestión de responsabilidad, sino que tiene que ser parte integral de todas las decisiones que toma la empresa.

Tradicionalmente, la información electrónica se protegía con tecnologías de seguridad de TI diseñadas para combatir amenazas concretas. El cometido principal de una estrategia de seguridad solía ser evitar intrusiones en las instalaciones corporativas y en su perímetro operativo. Pero hoy en día, los orígenes de los ataques electrónicos, o vectores de amenazas, son mucho más variados y sutiles. Por este motivo, las organizaciones también tienen que plantearse la seguridad de una forma más sutil y variada para proteger los recursos críticos.

No debe asumirse que el acceso sin autorización solamente se produce desde fuera de la empresa, ya que muchas veces el origen está en recursos internos, como pueden ser los socios y la cadena de suministro. El Informe sobre investigaciones de brechas en la seguridad de los datos de 2009 que ha llevado a cabo el equipo RISK de Verizon Business hace hincapié en los cambios en el panorama de la seguridad de TI y en los nuevos vectores en juego.

El informe, basado en 90 brechas confirmadas que los forenses de Verizon Business investigaron en el año 2008, destaca la importancia de examinar todos los aspectos del negocio, tanto internos como externos y demuestra que aunque casi tres cuartos de las brechas procedían del exterior, un quinto de ellas las causaron personas dentro de la empresa, mientras que los socios fueron responsables de casi un tercio. Estos resultados no sólo ilustran la diversidad de las amenazas contra la seguridad, sino que además sugieren la gran complejidad a la que se enfrenta una empresa a la hora de protegerse contra ataques multifacéticos de diversos orígenes.

Debido a su posición como centro de las redes empresariales y los cambios frecuentes en sus relaciones con el mundo exterior, existen varios puntos débiles inherentes a la empresa extendida en lo que a la seguridad se refiere.

Ahora más que nunca, los intrusos atacan los puntos en los que se concentran o agregan datos para obtener la mayor cantidad posible de información de los clientes. Estas personas saben que las empresas se enfrentan con un dilema: por una parte necesitan extender sus límites y poner la información al alcance de quienes la necesitan, mientras que por otra tienen que tener siempre presente la posibilidad de que con ello creen nuevas vulnerabilidades.

Al nivel más básico, la gestión de la seguridad de la información consiste en encontrar un equilibrio entre los costes que puede suponer una brecha en la infraestructura de TI —tanto directos como indirectos— y los esfuerzos necesarios para proteger debidamente dicha infraestructura.

En este sentido es esencial que los recursos más importantes, es decir la información crítica para el negocio, estén protegidos contra amenazas internas y externas. Al proteger la transmisión libre de la propiedad intelectual, es posible ampliar el alcance de la empresa y limitar las interrupciones de las operaciones que puedan obstruir las fuentes de ingresos. Además de esto, los mecanismos de seguridad deben contribuir al cumplimiento de los requisitos externos de conformidad que atañen a la seguridad. Este aspecto ha cobrado una especial importancia en la gestión de riesgos, particularmente en los sectores que exigen el cumplimiento de códigos estrictos de conformidad y gobierno, en los que las ramificaciones de una brecha en la seguridad pueden poner en peligro a la organización entera.

La gestión de la seguridad no implica únicamente la implementación de tecnología, sino que exige la implantación de prácticas que protejan el nombre de la empresa, su reputación y la confianza de los clientes. Estos son los componentes clave de una proposición de valor. La frecuencia de los cambios que se producen en las relaciones o los socios provoca la reevaluación constante de la demarcación entre los recursos privados, los públicos y los compartidos dentro del ámbito de la empresa extendida.

Para proteger debidamente a la empresa extendida hace falta considerarla de manera global y tener en cuenta tanto los recursos internos como las relaciones con el mundo exterior. Es importante concentrarse en los siguientes aspectos:

- Proteger la información.
- Proteger la infraestructura.
- Cumplir con los requisitos de gobierno, riesgo y conformidad, en especial en lo que a normativa se refiere.

Esto también significa abordar la seguridad, no sólo desde el punto de vista empresarial, sino en relación con proveedores, socios y distribuidores.

Es importante adoptar una estrategia que responda a las necesidades de cada empresa y se centre en los procesos. Para ello, es necesario evaluar y priorizar las amenazas contra la información crítica y encontrar un equilibrio entre los riesgos contra la seguridad de la TI y las prioridades operativas, al tiempo que se controlan los costes y se implementan controles de seguridad adecuados para las necesidades específicas de la empresa.

Lo que se necesita es un marco de trabajo flexible que responda al perfil de riesgo y de conformidad de cada empresa en concreto y que simplifique la

seguridad de la información en toda la organización, con un análisis independiente y continuo de los controles implementados.

El principio fundamental es que, en el caso de la seguridad, no existe una única solución para todas las situaciones, sino que los proveedores de tecnología y servicios tienen que ofrecer soluciones diseñadas específicamente para el cliente y suministrarlas de la forma más conveniente para cada empresa, ya sea de forma externalizada, parcialmente externalizada o sin ningún tipo de externalización. La solución tiene que responder a los requisitos y prácticas de la empresa, además de servir de complemento a la red.

**La extensión segura de las redes MPLS privadas**

La aparición de las redes IP ha abierto todo un mundo de posibilidades y oportunidades para las empresas. La existencia de una arquitectura más flexible y abierta en la que poder combinar las comunicaciones de voz y de datos ha hecho desaparecer muchas de las limitaciones que imponían los límites y perímetros de los dispositivos. Esto ha resultado en la transformación total de la forma en que se abordan los negocios y la tecnología. Ahora las operaciones pueden desarrollarse alrededor de redes abiertas a gran escala, en las que ya no existen las fronteras tradicionales, que son capaces de virtualizar comunidades enteras de personas conectadas entre sí.

Este tipo de redes ofrece una amplia gama de opciones de acceso, que van desde soluciones inalámbricas a soluciones de Ethernet, pasando por soluciones de DSL y satélite. Todas estas opciones facilitan la conectividad en todas partes del mundo y ofrecen Clases de Servicio flexibles para priorizar las aplicaciones clave según los requisitos de cada empresa.

Una de las tecnologías de red más populares de la última década ha sido la conmutación de etiquetas multiprotocolo o MPLS. No obstante, la necesidad de abordar la seguridad desde todos los puntos de vista exige que no se dé por sentada la seguridad de la tecnología de red MPLS, sino que se examine la forma en que se emplea en relación con la infraestructura, la tecnología y los procesos. Además, es importante considerar una gran variedad de aspectos en esta evaluación.

La seguridad de la red empieza con el diseño mismo y en este aspecto no se pueden hacer concesiones. Cualquier red IP basada en MPLS debe contar con troncales diversificadas hacia el resto de la red del proveedor para evitar el aislamiento de los nodos. También habrá que evaluar en detalle los planes de expansión de los distintos proveedores para confirmar que serán capaces de cumplir con las garantías de disponibilidad del acuerdo de nivel de servicio.

El fundamento de una solución de comunicaciones seguras para la empresa extendida debe ser una red MPLS privada segura. En este tipo de red se pueden asignar prioridades al tráfico —ya sea de voz, vídeo, datos, etc.— al tiempo que se consolida el tráfico en una sola red. Esto ofrece una mayor flexibilidad para gestionar el tráfico en toda la red, dando prioridad al tráfico crítico y consiguiendo un mayor nivel de control siempre que no se compartan los elementos centrales de la red con ninguna red IP pública.

La red MPLS se puede configurar de forma que los datos públicos y privados estén separados desde el punto de vista lógico, pero los operadores de red que compartan el tráfico de IP público y privado sobre los mismos enrutadores y circuitos físicos pueden encontrar dificultades a la hora de gestionar las congestiones de tráfico debido al carácter impredecible del

tráfico de IP público. Estos operadores tendrán que proteger sus elementos periféricos, o PE, para evitar ataques y vulnerabilidades.

Además de esto, el núcleo de la red MPLS privada no debe ser visible para otras redes. Aunque el incumplimiento de este requisito no implica en sí mismo un problema de seguridad, siempre es conveniente que el direccionamiento interno y la estructura de la red permanezcan ocultos al mundo exterior. Esto haría que, por ejemplo, fuera más difícil lanzar un ataque de denegación de servicio, o DoS, contra los enrutadores centrales.

MPLS separa el espacio de dirección y el enrutamiento para que no se compartan los datos entre las redes virtuales privadas (VPN). Sin embargo, en teoría es posible aprovecharse del protocolo de enrutamiento para dirigir un ataque DoS contra el enrutador PE, lo que a su vez afectaría negativamente a las otras VPN. Por este motivo, los enrutadores PE tienen que estar perfectamente protegidos, especialmente en sus interfaces con los enrutadores de la periferia del cliente (CE), y la red debe configurarse de forma que únicamente se pueda acceder a los puertos del protocolo de enrutamiento y sólo desde el enrutador de CE.

Las empresas extendidas requieren flexibilidad y control. Por eso es importante valorar los servicios de evaluación, los informes de aplicaciones y las herramientas de control que puede ofrecer el proveedor de red IP como servicios complementarios, para que su empresa pueda mantener en todo momento el mismo nivel de visibilidad y control. Aunque algunas empresas no sepan exactamente las aplicaciones que se emplean en su red, está claro que ciertas aplicaciones no deben utilizarse en un entorno empresarial, ya que, en el mejor de los casos, consumen el ancho de banda de forma innecesaria y en el peor pueden permitir que un intruso abra una brecha en el sistema de seguridad.

La implementación de una red privada basada en MPLS es uno de los elementos más importantes del enfoque integral necesario para proteger debidamente a la empresa extendida, ya que ofrece un alto nivel de control y la seguridad más estricta, según las políticas y tolerancia al riesgo de cada empresa.

Si se necesita ampliar la red para llegar a oficinas más pequeñas, facilitar acceso a los empleados que están de viaje o que trabajan desde casa, o crear un medio económico para acceder a Internet, es importante planear cuidadosamente la mejor forma de hacerlo para no poner en peligro la seguridad de la red.

Con una red MPLS privada, es posible configurar una pasarela segura a la red IP pública para que empleados, clientes, proveedores y socios dispongan del alcance necesario. A este respecto, el proveedor del servicio tiene la obligación de controlar las pasarelas, al tiempo que garantiza la integridad y la seguridad de la red.

Cada elemento del tráfico de clientes, proveedores y empleados tiene que estar aislado de los demás y por este motivo todo el tráfico que fluye entre la red pública y la red MPLS privada deberá gestionarse en cada una de las VPN del cliente. La pasarela tendrá que ser capaz de aislar la red privada de la pública hasta que la conexión se haya establecido mediante un túnel IPsec y sólo deberá disponer de acceso a la parte privada de la red el tráfico que entre por dicho túnel.

**Los Servicios de seguridad profesionales extienden la seguridad de la red**

Las condiciones económicas actuales exigen que las empresas hagan más con menos y se concentren en crear sistemas más eficientes y económicos. Los extras se han convertido en lujos difíciles de justificar.

Pero está claro que la protección de los recursos más valiosos de una empresa no puede considerarse un lujo y a la hora de decidir la mejor forma de reforzar la seguridad de la red MPLS privada hay que tomar algunas decisiones complicadas para determinar cuál es la manera más eficaz de implementar el plan trazado.

Si se determina que la mejor manera de conseguir los objetivos es ocuparse de todo internamente, será necesario invertir en tecnología e infraestructura, además de contratar personal especializado. Dada la necesidad de controlar los gastos, es posible que la mejor forma de abordar la creación de una red MPLS privada sea encontrar un proveedor de confianza que se encargue de gestionar la seguridad de la red como parte de un programa externalizado que se adapte a la estrategia corporativa de gestión de riesgos y fomente la creación de mejores prácticas y el control de costes.

De esta manera no hay necesidad de grandes inversiones de capital en tecnología e infraestructura de red, ni de inversiones similares en personal especializado. Un programa gestionado puede evitar que la tecnología y los servicios se queden obsoletos, ya que su empresa disfrutará siempre de lo más avanzado sin necesidad de nuevas inversiones de capital. Otra de las ventajas es que la seguridad y la reducción del riesgo se encuentran en manos de expertos dedicados a tiempo completo a esta labor, que cuentan con un enorme caudal de conocimiento.

El proveedor de servicios debe ofrecer una gestión completa de la seguridad, respaldada por acuerdos de nivel de servicio, supervisión continua y asistencia técnica las 24 horas. Este servicio gestionado basado en la nube debe ser idéntico a un servicio de seguridad basado en el equipo del cliente (CPE), para que la empresa pueda combinar soluciones de cortafuegos de CPE y de red en toda la organización.

Uno de los aspectos a tener en cuenta al evaluar la red de IP de un proveedor es determinar si es capaz de proporcionar información de utilidad a las empresas cliente a partir del análisis de datos procedentes de la red global del propio proveedor. Las redes IP globales de algunos de los proveedores más importantes cuentan con herramientas de vigilancia y alarma, los llamados honey pots o tarros de miel. Estas herramientas funcionan como trampas que se colocan en la red para detectar intentos de acceso no autorizado a las redes y a los sistemas de TI. Esto sirve después para reunir la información que servirá para crear contramedidas concretas para reforzar la seguridad.

El programa de seguridad de la red deberá proporcionar una conexión segura para el transporte de datos. Además de esto, también tiene que haber mecanismos de seguridad que protejan los datos según entran en la empresa extendida y que mitiguen los riesgos que dichos datos puedan conllevar.

Otra forma de reforzar la seguridad de la información es contratar servicios profesionales que desarrollen planes de protección de los datos críticos que residen en la empresa extendida, efectúen investigaciones forenses de brechas y datos comprometidos, se encarguen de la gestión de identidades y acceso para ofrecer el nivel de acceso adecuado a los propietarios de los datos y a los usuarios, e implementen medidas de seguridad de la red y de las aplicaciones. También hay que considerar el nivel de asistencia que el

proveedor ofrece en la gestión y supervisión de la seguridad y de los dispositivos no relacionados con la seguridad, además de en la evaluación de políticas, el diseño de arquitecturas y la gestión de incidentes de seguridad.

Desde la perspectiva del gobierno, el riesgo y la conformidad, existen diversos programas de seguridad cuya función es asegurar que se cumplan los requisitos de seguridad de la información, validar la diligencia debida, mitigar los riesgos para clientes, socios y contratistas, y comprobar que se observen las políticas de seguridad.

Para que estos servicios sean realmente eficaces deben tener como objetivo la reducción del riesgo, en lugar de depender de soluciones puntuales que exigen una gestión intensiva y que suelen resultar muy costosas. Por todo ello, la forma más económica y eficiente de mitigar los riesgos para que la organización pueda concentrarse en lo que mejor sabe hacer es emplear servicios de seguridad profesionales como complemento a la seguridad de la red.

**Los fundamentos de la seguridad en la empresa extendida**

No hay duda de que el proceso de globalización seguirá intensificándose y que su empresa tendrá que esforzarse por llegar a más y más personas en cada vez más lugares.

Aunque esto representa una excelente oportunidad para volverse más flexible y aprovechar las oportunidades que se presenten en todas partes del mundo, también deja a la organización más expuesta a posibles ataques. Por eso es esencial que la seguridad de la información y la reducción del riesgo se consideren de forma global y se pongan al descubierto aquellas áreas en las que la empresa se encuentre más vulnerable.

En lo que a soluciones técnicas se refiere, las comunicaciones a través de la red MPLS privada son extremadamente accesibles y eficientes, lo que facilita la transmisión de información crítica a empleados, clientes, socios y proveedores donde quiera que se encuentren.

En lo referente a los costes, lo más conveniente es suscribirse al servicio que ofrezca las soluciones más avanzadas para reducir el riesgo activamente, sin necesidad de grandes inversiones de capital.

Los servicios de seguridad gestionados pueden crear un sistema de seguridad de la información que responda a los objetivos críticos de la empresa, y ayude en la tarea de establecer prioridades, asignar recursos y desarrollar una estrategia global. Una empresa extendida como la suya, con operaciones en todo el mundo, necesita un proveedor de servicios al que pueda confiar la seguridad fundamental de la red MPLS privada, que sea capaz de prestar un servicio fiable de calidad. El proveedor deberá facilitar el envío de tráfico y ofrecer controles de seguridad que sirvan para reducir el riesgo de ataques y para implementar herramientas de supervisión y gestión constantes de la seguridad.

Por todo lo dicho es esencial escoger un proveedor que ofrezca una solución con una relación calidad precio favorable y un enfoque preventivo que aborde las amenazas emergentes antes de que se conviertan en un riesgo real, para que de esta manera su empresa pueda concentrarse en lo realmente importante: su negocio. **[28]**

## 4.4 ASPECTOS DESTACADOS DE LOS CASOS DE ESTUDIO

En el primer caso de estudio se puede ver como la empresa Claranet le da una solución VPN MPLS a la empresa ConektIA.

En el segundo caso de estudio se puede ver que un grupo de socios tecnológicos: Cisco, Teldat y Telefónica, dan una solución VPN MPLS con ciertas características específicas al ministerio de defensa español.

El tercer caso correspondiente a la empresa Verizon, trata a cerca de las brechas de inseguridad que se presentan en las empresas, que en su gran mayoría son provenientes de fuentes externas.

Los dos primeros casos de estudios son soluciones a empresas españolas y el tercer caso es una empresa estadounidense, y los tres casos hablan de su solución con redes virtuales MPLS y de los requerimientos que deben tener estas redes para implementarlas, como lo son:

- Autenticación de usuario: verificando la identidad del usuario y restringiendo acceso a la VPN a usuarios no autorizados.
- Administración de dirección: deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las mismas se mantengan sin cambios.
- Encriptación de datos: a través de esta se asegura que los datos no serán leídos por usuarios no autorizados.
- Administración de llaves: generando y renovando las llaves de encriptación tanto para el cliente como para el servidor.
- Soporte de protocolo múltiple: la red VPN debe poder manejar protocolos comunes utilizados en redes públicas.

Los beneficios que éstos tendrán al implementar estas redes corresponden a:

- Reducción de costos operacionales
- Simplificación de la topología de red.
- Alta seguridad mediante la utilización de algoritmos complejos de autenticación, encriptación, etc.
- Escalabilidad de la red.
- Seguridad, fiabilidad, administración de la red menos compleja.

En el tercer caso de estudio, se tiene en cuenta a que una de las normas sectoriales que tienen que cumplir muchas empresas es la norma de seguridad de datos del sector de las tarjetas de pago, o PCI DSS por sus siglas en inglés. El primer requisito de la PCI DSS es construir y mantener una red segura. Se ha debatido mucho la eficacia de normativas y directivas de control a la hora de prevenir brechas en la seguridad, pero todavía no se han hecho suficientes estudios prácticos al respecto. La evaluación extraoficial de algunas de las brechas ocurridas en este sector, que se incluye en el *Informe sobre investigaciones de brechas en la seguridad de los datos de 2008* realizado por Verizon Business, indica que la tasa de conformidad media de las víctimas de este tipo de ataques se sitúa en un 29 por ciento de los 12 requisitos de la PCI DDS. En otras palabras: una organización típica cumple con menos de un tercio de los requisitos del sector. Algunas cumplen muchos más y otras aún menos, pero lo importante es señalar que la mayoría de las brechas investigadas no ocurrieron en organizaciones que cumplen con la PCI DSS. **[28]**

En noviembre de 2008, Verizon Business acudió a Symantec para efectuar una evaluación de la arquitectura de la red que se centrara en sus dos redes virtuales privadas de IP basadas en MPLS. El objetivo de este proyecto era efectuar un análisis físico y documentar los niveles de seguridad de ambas plataformas para confirmar que cumplían con las prácticas de seguridad empleadas en la norma

NIST 800-53 Revisión 2 al nivel moderado. En general, Symantec descubrió que la red IP privada era extremadamente robusta en términos de disciplina, redundancia y flexibilidad. También se llegó a la conclusión de que los marcos de trabajo y políticas de seguridad abordan la gestión y operación de las redes de manera integral y que han sido debidamente equipados con los mandatos, procedimientos y gobierno dirigido que atañen a los sistemas de información, y a los usuarios y grupos que los gestionan. **[28]**

**Análisis de seguridad de Internet de Verizon**

El servicio Internet Security Assessment ayuda a proteger a la empresa extendida. Los clientes de Verizon Private IP en todo el mundo pueden ahora beneficiarse del análisis de seguridad de Internet de Verizon Business. Esta solución ofrece un enfoque innovador y poderoso para analizar los aspectos más importantes de la estrategia de seguridad y evaluar los riesgos relacionados con la infraestructura de red basada en la web. El análisis incluye servicios profesionales de descubrimiento y clasificación virtuales, y de evaluación del riesgo externo. Estos dos componentes son una parte importante de la seguridad de los clientes, socios, contratistas y proveedores de la empresa extendida, ya que ofrecen un panorama completo de la seguridad basado en un análisis de las actividades de Internet, junto con exploraciones exhaustivas para descubrir vulnerabilidades. **[28]**

**Verizon ofrece servicios de seguridad basados en la nube**

Ahora los clientes de Private IP disponen de un servicio de seguridad basado en la nube totalmente gestionado, que les permite externalizar las tareas de gestión y administración del cortafuegos de red. Los expertos en seguridad de Verizon pueden ayudar a los clientes a definir e implementar directivas de cortafuegos estrictas, que sirvan de primera línea de defensa contra tráfico potencialmente peligroso. Verizon Business asistirá al cliente en la implementación de las directivas de cortafuegos apropiadas y las supervisará y actualizará cuando cambien los requisitos de la empresa.

# 5. CONCLUSIONES

Se afirma que MPLS es una nueva tecnología que se ha venido implementando con el fin de reducir el tráfico en la red y de brindar un mejor servicio de la red, lo cual incrementa la eficiencia y eficacia de las redes. Todos estos beneficios la hacen más llamativa para los proveedores de servicios de red ya que representa una reducción en los costos de implementación, mejora el rendimiento de los dispositivos usados entre otros.

En primer lugar, se puede afirmar que por medio de la revisión bibliográfica realizada, MPLS es un método para proporcionar calidad de servicio en las redes, beneficiando la asignación de ancho de banda y evitando y/o administrando la congestión en la red, el manejo de prioridades y encolamiento de tráfico.

Por otra parte, se llegó a que la tecnología MPLS se caracteriza por poseer velocidad, escalabilidad, flexibilidad, calidad de servicio (QoS) con múltiples clases de servicio (CoS), gestión e ingeniería de tráfico.

Así mismo, se llegó a determinar el potencial y funcionamiento de MPLS como protocolo básico de redes más robustas y eficientes. En donde se concluyó que ésta funciona entre la capa de enlace de datos y la capa de red, aprovechando lo mejor de ambas. Su funcionamiento se basa en la conmutación de etiquetas, la cual resume la información y permite conocer todos los destinos posibles y asignar una trayectoria de éstas permitiendo así el óptimo envío de paquetes.

Por último, se destacaron las aplicaciones y áreas promisorias que tiene MPLS. Las aplicaciones que posee esta tecnología traen muchos beneficios por lo que reduce el tráfico en la red y brinda un mejor servicio, incrementando la eficiencia y eficacia de las mismas. Se trataron casos de estudios reales aplicados a

organizaciones que presentaban principalmente problemas de inseguridad y que fueron solucionados por medio de la integración de MPLS en VPN.

# 6. GLOSARIO

**ATM:** Asyncronous Transfer Mode. Modo de Transferencia Asíncrona. Es una tecnología de alto desempeño, orientada a conmutación de celdas y con tecnología de multiplexaje. Ésta usa paquetes de tamaño fijo para llevar diferentes tipos de tráfico.

**BACKBONE:** Es un enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red.

**BANDWIDTH:** Ancho de Banda. Volumen de información que puede circular por un medio físico de comunicación de datos, capacidad de conexión. A mayor capacidad mayor velocidad. Se mide en hertz o bps (bits por segundo).

**BGP:** Border Gateway Protocol. Es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

**BUSINESS-TO-BUSINESS:** Es la transmisión de información referente a transacciones comerciales electrónicamente, normalmente utilizando tecnología como la Electronic Data Interchange (EDI).

**CALIDAD DE SERVICIO (QoS)**: Son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

**CAPA 2 O DE ENLACE DE DATOS:** Capa 2 del modelo de referencia OSI. Proporciona tránsito confiable de datos a través de un enlace físico. Se ocupa del direccionamiento físico, topología de red, disciplina de línea, detección y notificación de errores, entrega ordenada de las tramas y del control de flujo. A veces se le denomina simplemente Capa de Enlace. A este nivel se manejan las direcciones MAC.

**CAPA 3 O DE RED:** Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es en la que se produce el enrutamiento. A este nivel se manejan las direcciones IP.

**CLASE DE SERVICIO (CoS)**: Indicación de cómo un protocolo de capa superior requiere que un protocolo de capa inferior maneje sus mensajes. En el enrutamiento de subárea SNA, las definiciones CoS son utilizadas por los nodos de subárea para determinar la ruta óptima para establecer una sesión específica. Una definición CoS incluye un número de ruta virtual y un campo de prioridad de transmisión. También denominado ToS (Tipo de Servicio).

**CPE:** Son dispositivos cliente de red inalámbrica para profesionales con funcionalidades únicas, tales como soportar alto nivel de trafico, control de ancho de banda, disponer de QoS con priorización por IPs, rangos de IPs, protocolos o puertos.

**CR-LDP:** (Constraint Shortest Path First based LSP). Hacen uso los protocolos de enrutamiento tradicionales para hacer la reserva de etiquetas así como su anuncio a los vecinos. Cabe decir que con la implementación y/o ejecución de estos protocolos no se puede tener una protección ante fallas del camino principal ya que no contempla la formación de rutas alternativas hasta que un

fallo ocurra, pero si se cumple con el hecho de proporcionar QoS a los tráficos que lo requirieren.

**DATAGRAMA:** Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información de la Internet. Los términos trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

**DELAY:** (Retraso) Es un efecto de sonido que consiste en la multiplicación y retraso modulado de una señal sonora. Una vez procesada la señal se mezcla con la original. El resultado es el clásico efecto de eco sonoro.

**DSL:** Digital Subscriber Line (Línea de Suscripción Digital). Tecnología que permite enviar mucha información a gran velocidad a través de líneas telefónicas.

**ENCAPSULACIÓN:** Es el proceso desde que los datos son incorporados al ordenador hasta que se transmiten al medio. En otras palabras, es el proceso por el cual los datos que se deben enviar a través de una red, se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas.

**ETHERNET:** Es un estándar de redes de área local para computadores con acceso al medio por contienda CSMA/CD. ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. El nombre viene del concepto físico de ether.

Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

**ETIQUETA O LABEL:** Es el valor actual, con sentido únicamente local, de la etiqueta MPLS, empleado para identificar un FEC. Esta etiqueta es la que determinará el próximo salto del paquete y posee 20 bits.

**FEC:** Forwarding Equivalence Class. Clase de Equivalencia de Reenvío. Clase que define un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes.

**FRAME RELAY:** Intercambio de Tramas. Una técnica de transmisión extremadamente eficiente, usada para mandar información digital como voz, datos, tráfico de redes de área local (LAN), y trafico de redes de gran área (WAN) a muchos puntos desde una solo puerto de manera muy rápida.

**FULL-MESH:** Topología física de malla completamente conectada. Conecta cada nodo con cada uno de los nodos restantes, creando tolerancia y resistencia a las fallas, Implementarlo es caro y difícil.

**GMPLS:** (Generalized Multi-Protocol Label Switching) La Conmutación de Etiquetas Multiprotocolo Generalizada, extiende el concepto de MPLS hacia el mundo óptico, a través de conmutación de intervalos de tiempo (IT) TDM, hacia longitudes de onda ópticas (lambdas), y hacia conmutaciones espaciales entre fibras entrantes y salientes.

**HOP-BY-HOP:** Es un método común de enrutamiento en redes en las que hay nodos intermedios entre la fuente y el destino, en donde va a la dirección del siguiente nodo principal hasta el punto de destino en la lista.

**HUB-AND-SPOKE:** Es un sistema de conexiones colocadas como una rueda de carro, en la que todo el tráfico se mueve a lo largo de los radios conectados al concentrador en el centro.

**IETF:** Internet Engineering Task Force. Es una organización internacional abierta de normalización, que tiene como objetivos contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

**IP:** Internet Protocol. Protocolo de Internet. Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados no fiable de mejor entrega posible sin garantías.

**IPbased VPNs:** Redes Privadas Virtuales basadas en protocolo IP como los son las MPLS VPNs (Redes Privadas Virtuales basadas en Multiprotocol Label Switching).

**IPSec:** Internet Protocol Security. Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) legitimando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

**IPv4:** IP versión 4. Esta versión utiliza direcciones de 32 bits y es la usada actualmente en todas las redes de datos.

**IPv6:** IP versión 6. Esta es la nueva versión de IP que sustituirá la versión 4 y utilizará 128 bits.

**ISP:** Internet Service Provider. Proveedor de Servicios de Internet. Es una empresa que brinda conexión a Internet para sus clientes.

**JITTER**: Se denomina a la variabilidad temporal durante el envío de señales digitales, es una ligera desviación de la exactitud de la señal de reloj. El jitter suele considerarse como una señal de ruido no deseada. En general se denomina jitter a un cambio indeseado y abrupto de la propiedad de una señal.

**LAN:** Es una red que conecta ordenadores y periféricos en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

**LDP:** Label Distribution Protocol. Es un protocolo en el que dos LER intercambian información cartográfica de la etiqueta. Los dos LERs son llamados compañeros de LDP y el intercambio de información es bidireccional. LDP se utiliza para construir y mantener bases de datos LSP que se utilizan para reenviar el tráfico a través Multiprotocol Label Switching (MPLS).

**LER:** Label Edge Router. Estos routers son los que se encuentran en la entrada de los flujos a la red MPLS. Se encargan de clasificar los paquetes en FEC y colocar las etiquetas correspondientes a los tráficos que se enviarán a la red según los parámetros acordados con el ISP a través de un contrato. Estos routers, al tener la tarea de clasificación, deben que tener un muy alto poder de procesamiento para poder hacer esta tarea de manera muy rápida, eficiente y sin afectar al tráfico sensible a los retardos y al jitter.

**LFIB:** Desvío de Información de la Etiqueta Base. Es una estructura de datos y el modo de transmisión en la que la gestión de destinos y etiquetas de entrada están asociadas con las interfaces de salida y las etiquetas.

**LIB:** Label Information Base. Así como a nivel de capa de Red se tiene una tabla de ruteo con la cual el router puede tomar una decisión de envío para con el

tráfico entrante según a donde el paquete se dirija, existe una tabla de etiquetas que manejan los LSR muy semejante a la que existe a la de capa de red. Esta tabla relaciona interfaz de entrada - etiqueta de entrada con interfaz de salida - etiqueta de salida; es decir, si se recibe un paquete en un LSR, éste para su reenvío sólo cambiará la etiqueta y se conmutará a la interfaz correspondiente. Nótese que a pesar de que esta tabla LIB se forma en base a los protocolos de enrutamiento de la capa de red, funciona con una tabla de conmutación; Véase que a diferenta del modelo IPoverATM la capa de enlace tiene conocimiento de los sucesos que ocurren en capa de red.

**LSP:** Label Switched Path. Camino de Intercambio de Etiquetas. Es una ruta a través de uno o más LSRs en un nivel de jerarquía que sigue un paquete de un FEC en particular.

**LSR:** Label Switching Router. Enrutador de Intercambio de Etiquetas. Es un enrutador de alta velocidad especializado en el envío de paquetes etiquetados por MPLS.

**MEJOR ESFUERZO: (**Best Effort) para definir la forma de prestar aquellos servicios para los que no existe una garantía de calidad de servicio (QoS). Esto implica que no existe una preasignación de recursos, ni plazos conocidos, ni garantía de recepción correcta de la información.

**MPLS**: Multi-Protocol Label Switching. Es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM.

**MULTICAST:** Es el envío de la información en una red a múltiples destinos simultáneamente.

**OSI:** Open System Interconnection. El modelo de interconexión de sistemas abiertos, es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

**OSPF:** Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

**PPP:** Point-to-point Protocol. Protocolo punto a punto. Es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

**PRIVATE LINE:** En cableado de telefonía, una línea privada o línea de enlace es un servicio que consiste en circuitos dedicados, privada de conmutación arreglos, y/o predefinido de transmisión de los caminos, ya sean físicos o virtuales, que ofrecen las comunicaciones entre lugares específicos. La mayoría de las líneas privadas conectan sólo dos lugares a pesar de que pueden ser cambiados en cualquier extremo o en ambos. Algunos tienen múltiples puntos de caída.

**RFC:** Request for Comments."Petición De Comentarios". Son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

**RSVP-TE:** Resource ReSerVation Protocol for Traffic Engineering. El protocolo de reserva de recursos usado en un primer momento para la arquitectura IntServ se hicieron modificaciones para que sea más ligero, de fácil procesamiento. Así este protocolo sigue con la capacidad de reservar recursos (garantiza QoS) y establecer las etiquetas en los nodos MPLS, sea de manera explícita o dinámica. Como se crea un camino a través de los nodos, este camino se estable en los nodos activos en ese momento, así se permite la capacidad de reenrutamiento de los túneles LSP, recuperarse de caídas de red, evitar la cogestión, entre otras facilidades.

**SERVICIOS DIFERENCIADOS:** (DiffServ). Proporcionan un método que intenta garantizar la calidad de servicio en redes de gran tamaño, como puede ser Internet. Servicios Diferenciados analiza varios flujos de datos en vez de conexiones únicas o reservas de recursos. Esto significa que una negociación será hecha para todos los paquetes que envía una organización, ya sea una universidad, un proveedor de servicios de Internet o una empresa. Los contratos resultantes de esas negociaciones son llamados Acuerdos de Nivel de Servicio (SLA), e inevitablemente implican un intercambio oneroso. Estos SLA especifican qué clases de tráfico serán provistos, qué garantías se dan para cada clase y cuántos datos se consideran para cada clase.

**SERVICIOS INTEGRADOS:** (Intserv) Constituyen una arquitectura cuyo cometido es gestionar los recursos necesarios para garantizar calidad de servicio (QoS) en una red de computadores. El concepto que los servicios integrados proponen para cumplir con su cometido, requiere de una nueva arquitectura de protocolos que es difícilmente escalable. Esto se debe a que funciona realizando una reserva extremo a extremo de recursos en los elementos que conforman la red a nivel de aplicación.

**SLA:** Service Level Agreement. Acuerdo de Nivel de Servicio. Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

**SYMANTEC CORPORATION:** Es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática. Con la sede central en Mountain View, California y opera en más de cuarenta países.

**TE:** Traffic Engieering. Ingeniería de tráfico. Es un método para optimizar el rendimiento de las telecomunicaciones de la red de forma dinámica para analizar, predecir y regular el comportamiento de los datos transmitidos a través de la red. Ingeniería de tráfico también se conoce como ingeniería de teletráfico y gestión del tráfico. Las técnicas de ingeniería de tráfico se pueden aplicar a las redes de todo tipo, incluyendo la PSTN (red telefónica pública conmutada), LAN (redes de área local), WANs (redes de área amplia), de telefonía celular de redes, empresas de propiedad y la Internet.

**THROUGHPUT:** volumen de información que fluye en las redes de datos.

**TLV:** En el ámbito de los protocolos de comunicaciones, se denomina tipo-longitud-valor o valores de longitud tipo a un formato de representar información, de forma que haya información que pueda tener presencia opcional y longitud variable.

**TTL:** Tiempo de Vida o Time To Live. Es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

**UNICAST:** Es el envío de información desde un único emisor a un único receptor.

**VOZ SOBRE IP:** Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VozIP, VoIP (por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

**VPN:** Virtual Private Network. Red Privada Virtual. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

**VRF:** Virtual Routing and Forwarding (Enrutamiento Virtual y Reenvío) es una tecnología que permite que varias instancias de una tabla de enrutamiento coexistan dentro del mismo router, al mismo tiempo.

**XDSL:** (“Digital Subscriber Line”, Línea de Abono Digital), es una tecnología que ofrece un amplio Ancho de Banda a través del par de Cobre convencional desplegado inicialmente para el servicio telefónico.

## 7. REFERENCIAS BIBLIOGRÁFICAS


[1] Blanco, H. (2008). Estudios de mecanismos para el control de tráfico LAN y WAN que manejen convergencia de servicios, en una red MPLS sobre wireless. Trabajo de grado para optar al título de ingeniero de Sistemas. Cartagena de Indias D. T y C.: Universidad Tecnológica de Bolívar, 95 p.

[2] Anónimo(sin fecha) bajado de <https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06_07/trabajos/resumenes/gr14-MPLSEnLinux.pdf>

[3] Trillium.(sin fecha). Multiprotocol Label Switching (MPLS). <http://www.iec.org>

[4] The Applied Technologies Group, Inc. (1998). Multiprotocol Label Switching (MPLS). 26 p. bajado de <http://www.tspt.net.et/documentation/MPLS.pdf>

[5] Pereira, S., Sotomayor, A.(2004). MPLS sobre redes Metroethernet. Monografía presentada como Registro de aprobación de la especialización en Telecomunicaciones. Cartagena de Indias D. T y C.: Universidad Tecnológica de Bolívar, 165 p.

[6] Soldatos, J., Vayias, G. y Kormentzas, G. (2005). “On the Building Blocks of Quality of Service on Heterogeneous IP Networks”, IEEE Communications Surveys, Vol. 7, No. 1, p. 70-89

[7] Malis A.G.,(2006).“Converged Services over MPLS”. IEEE Communications Magazine, 7 p

[8] Canalis, M. S. (2000). MPLS “Multiprotocol Label Switching”: Una Arquitectura de Backbone para la Internet del Siglo XXI. Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina. 20 p. Bajado de <http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MPLS.PDF>

[9] Callon, R., Doolan, P., Feldman, N., Fredette, A., Swallow, G., Viswanathan, A. (1997, November). A Framework for Multiprotocol Label Switching. Network Working Group. Internet Draft <draft-ietf-mpls-framework-02.txt>

[10] COIMBRA, G Edison (2010). Tecnologías de transporte: Red de transporte MPLS. Bajado de <http://coimbraweb.com/documentos/telecom/9.8_mpls.pdf>

[11] DOMÉNICO, Javier Igor y GARCÍA, Luna Victoria (2008). Medición y análisis de tráfico en redes mpls. Tesis para optar el título de ingeniero de las telecomunicaciones. Lima, Perú: Pontificia Universidad Católica del Perú. 141 p. Bajado de <http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/212/LUNA_JAVIER_MEDICION_ANALISIS_TRAFICO_REDES_MPLS.pdf?sequence=2>

[12] GODINEZ, de la Piedra Mauricio (?). Tecnología IMPLS. Beraten Telecomunicaciones. Bajado de <http://www.beraten.com.mx/descarga/mpls.pdf>

[13] EMICURI, Javier (?). VPN IP MPLS: El camino para su red Multiservicio. Antel. Bajado de <http://www.antel.com.uy/ANTEL/datos-e-internet/Hogares/wps/wcm/connect/b8f4100044ff2b278da6ff412be27c8f/Charla_1_VPN_IP_MPLS_Ing_Emicuri.pdf?MOD=AJPERES&CACHEID=b8f4100044ff2b278da6ff412be27c8f>

[14] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol Label Switching Architecture,” IETF RFC 3031, Jan.2001. Bajado de <http://www.ietf.org/rfc/rfc3031.txt>

[15] RODRÍGUEZ, Damián (2008). Transmisión de voz, video y datos en Redes Privadas Virtuales VPN/MPLS. Buenos Aires, Argentina: Universidad de Belgrano, Facultad de Tecnología Informática. Departamento de Investigaciones. 98 p. Bajado de <http://www.ub.edu.ar/investigaciones/tesinas/259_rodriguez.pdf >

[16] Instituto Politécnico Nacional. Calidad de servicio en la red ATM-MPLS de PEMEX (2003). México D.F. 112 p. Bajado de <http://www.biblio-sepi.esimez.ipn.mx/mecanica/2003/Calidad%20de%20servicio%20en%20la%20red%20ATM-MPLS%20de%20PEMEX.pdf>

[17] HORNEY, Carter for Nuntius Systems, Inc (2002). Quality of Service and Multi-Protocol Label Switching. Bajado de <http://www.nuntius.com/docs/QoSandMPLS1.pdf>

[18] ZAMORA, Hugo (2002). Implementación de Redes MPLS-VPN. Casos de Estudio. Reunión de Primavera CUDI. México. Bajado de <http://www.cudi.mx/primavera2002/presentaciones/MPLSVPN.pdf>

[19] HUIDOBRO, José M. y Millán, Ramón J. (2002). MPLS (MultiProtocol Label Switching). Ericsson España. Bajado de <http://www.ramonmillan.com/documentos/mpls.pdf>

[20] IBUJÉS, María del Carmen. SUBÍA. Rafael. ROMERO, Harol. TORRES, Edwin. ZORRILLA, Angélica (2006). Comunicaciones IPv6: MPLS. Carrera de ingeniería en sistemas informáticos y de computación. Quito, Ecuador. Escuela Politécnica Nacional. Bajado de: <intechscialtda.com/IPv6/MPLS.doc>

[21] NAVEGA. Honduras. Bajado de <www.revistaitnow.com/bajar.php?a=td09/01_ni/02/Navega_final.pdf>

[22] TIC TAC: TIC (Tecnoloxías Información e Comunicacións) e TAC (Tamén Amigos e Colegas) (2010). Bajado de <http://tic-tac.teleco.uvigo.es/profiles/blogs/en-que-consiste-mpls-y-sus>

[23] REYES, Selvyn (2008). Diseño de redes privadas en equipo Cisco utilizando Multiprotocolo para Conmutación de Etiquetas (MPLS). Trabajo de grado de ingeniería electrónica. Guatemala: Universidad de San Carlos Guatemala. 159 p. Bajado de <biblioteca.usac.edu.gt/tesis/08/08_0219_EO.pdf >

[24] CHICA, Pamela. Muñoz, Marta y Roca, Tedi (2005). Trabajo sobre MPLS: Informe. Bajado de: <locortes.net/Vicenc/Telematica/Enginyeria%20de%20Xarxes/MPLS.pdf>

[25] IGA, Alexis Rodrigo (2007). Metodologías, herramientas y criterios para la planificación general de plataformas de telecomunicaciones. Resumen de la memoria Para optar al titulo de Ingeniero civil electricista. Santiago de Chile. Universidad de Chile. 217 p.

[26] ConektIA & Clarane. Case Study. Bajado de: <http://www.api.es/download/CS-PlataformaTecnologica.pdf>

[27] SITI As Lan (2010). Securización de la Red de Datos de Propósito General del Ministerio de Defensa sobre una red comercial IP/MPLS. Bajado de: <www.aslan.es/files/1149-24546-Archivo/MINISDEF.pdf >

[28] Verizon (2010). Las redes MPLS privadas extienden la empresa con total seguridad. Bajado de: <http://www.verizonbusiness.com/resources/whitepapers/wp_la-redes-mpls-privadas-extienden-la-empresa-con-total-seguridad_es_xg.pdf>