# UNIVERSIDAD POLITÉCNICA SALESIANA

# SEDE QUITO

**CARRERA: INGENIERÍA EN SISTEMAS**

**Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS**

**TEMA:**
**FUNCIONALIDAD, DISEÑO, SIMULACIÓN Y CONFIGURACIÓN DE DISPOSITIVOS PARA UNA RED MPLS EN ENTORNO IPV6**

**AUTOR:**
**ROLANDO JAVIER REYES ALTAMIRANO**

**DIRECTOR:**
**JORGE ENRIQUE LÓPEZ LOGACHO**

**Quito, marzo de 2014**

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO**

Yo Rolando Javier Reyes Altamirano autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Quito, marzo de 2014

---

Rolando Javier Reyes Altamirano
CC. 1719309989

## DEDICATORIA

A mis padres, que gracias a su incondicional apoyo moral, económico, me sacaron adelante, dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi vida, y porque el orgullo que sienten por mí fue lo que me hizo ir hasta el final. Esto va por ustedes, por lo que valen, porque admiro su fortaleza, su sencillez y por lo que han hecho de mí, gracias a eso me han enseñado que los grandes éxitos se consiguen con esfuerzo, dedicación y sobre todo con mucha humildad.

A mis hermanas gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

A dios por darme una segunda oportunidad de vida y permitirme ver el valor de la vida.

Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles. A todos, espero no defraudarlos y contar siempre con su valioso apoyo sincero e incondicional en mi vida.

## AGRADECIMIENTO

A todos mis profesores que desde mi infancia fomentaron en mí los mejores valores, enseñanza. Fue un honor haber podido contar con profesores dedicados, comprometidos y responsables que ponen muy en alto el nombre de cada institución.

Al llegar a nuestros principales objetivos, sentimos una gran alegría, cuando alcanzamos mejores resultados interpretamos que estamos haciendo lo correcto.

Lo cierto de todo esto es que muchas veces es importante la ayuda de una o más personas para alcanzar nuestra meta deseada, gracias a todos los profesores que fomentaron ese deseo de superación y lucha.

# ÍNDICE

## ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

## RESUMEN

El trabajo final de grado tiene la finalidad de dar a conocer el funcionamiento, diseño, elementos de infraestructura, simulación de una red MPLS en entorno IPv6, debido a la gran demanda de usuarios al internet, incremento de dispositivos smartphone, pc, tablet, alta calidad de servicio QoS, video conferencia, VoIP, datos. MPLS es la tecnología dominante en el núcleo de la red es capaz de abrir varios caminos entre un origen y un destino, además de integrar varios servicios por un mismo canal, esto unido al protocolo IPV6 que suple muchas deficiencias del anterior protocolo IPV4 como, mayor número de direcciones, posibilidad de paquetes con carga útil, calidad de servicio, seguridad integra, infraestructura de direcciones y enrutamiento eficaz y jerárquica, IPv6 puede usar cualquier circuito de transporte para la instalación sobre redes MPLS, IPv6 no requiere de cambios en la configuración de los routers de core o de provider edge. En lo que se refiere a infraestructura se conocerá cuáles son los elementos necesarios para construir una sala de equipos o telecomunicaciones, con elementos indispensables para el correcto funcionamiento, se realizaron planos de las salas de equipos para tener una idea clara y concisa de los elementos necesarios de infraestructura necesarios para el funcionamiento de una sala de telecomunicaciones, para respaldar esto se realizará una simulación con el software GNS3 el cual nos permitirá verificar de una forma real el funcionamiento una red MPLS en entorno IPv6, con elementos reales como son routers, pc, swtichs, los cuales permitirán consolidar los conceptos.

## ABSTRACT

This work aims to raise awareness of the operation, design, infrastructure elements, simulating an MPLS network IPv6 environment, due to the high demand from users to the internet, increased smartphone, pc devices, tablet, high QoS quality of service, video conferencing, VoIP, data. MPLS is the dominant technology in the core of the network is able to open multiple paths between a source and a destination , and integrate multiple services for the same channel , MPLS makes significant changes to the networks in which they are integrated as scalability, flexibility ,efficiency, safety this coupled with the IPv6 protocol that covers many deficiencies of the previous protocol IPv4 as greater number of directions, possible packet payload , quality of service , security integration , address infrastructure and efficient and hierarchical routing , IPv6 may use any circuit transport over MPLS networks installation , IPv6 does not require configuration changes to core routers or provider edge . In regards to infrastructure know what are the necessary elements to build an equipment room or telecommunications, with essential elements for proper operation, planes equipment rooms was made for a clear and concise idea of the necessary elements infrastructure necessary for the operation of a telecommunications room , to back this up with GNS3 simulation software will be made which will allow us to check in a real way running an MPLS IPv6 network environment , elements used in real life such as routers, pc, swtichs.

# INTRODUCCIÓN

La necesidad de proporcionar una respuesta más rápida y eficaz en las redes actuales hace que aparezca este nuevo stantard que introduce cambios tecnológicos fundamentales. Cabe destacar la importancia de la inclusión en red de nuevas aplicaciones y la posibilidad de ofrecer diferentes niveles de servicio, todo ello ligado a una mayor fiabilidad. MPLS es el perfecto sustituto de la actual arquitectura IP sobre ATM, suple las necesidades de su anterior arquitectura en cuanto a la creación de túneles y VPNs. Integra las capas de enlace (nivel 2) y de red (nivel 3) utilizando las funciones de control de enrutado y beneficiándose la rápida conmutación de nivel 2. (locortes.net, 2005)

MPLS encuentra la solución a muchos de los actuales problemas que genera la integración de las actual IP sobre ATM, como puede ser la expansión sobre una topología virtual superpuesta. Debemos tener en cuenta que se trata de dos tecnologías diferentes, por lo tanto precisan de gestión compleja. Al combinar la inteligencia del routing con la rapidez del switching, MPLS ofrece interesantes características en la gestión de los backbones. (locortes.net, 2005)

MPLS 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. Esta tecnología ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia, intenta conseguir las ventajas de ATM, asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers. (polartel.es, 2012)

Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente).
- Policy Routing.
- Servicios de VPN.

- Servicios que requieren QoS.
- MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).
- MPLS realiza la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiqueta dichos paquetes según la clasificación establecida por la QoS.
- MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.(polartel.es, 2012)

Una red MPLS es una solución estándar al transporte de información en redes, tanto en entornos IPv4 como IPv6. Aceptado por toda la red de internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando routing de paquetes con ciertas garantías de entrega. Una red MPLS con un protocolo IPv6, proporciona múltiples ventajas: mayor cantidad de direcciones, seguridad incorporada, aplicaciones multimedia, extensibilidad, VoIP. Para complementar la solución a MPLS, IPv6 sobre redes troncales MPLS permite dominios aislados IPv6 para comunicarse entre sí a través de una red de núcleo de MPLS IPv4. Esta aplicación requiere sólo unas cuantas mejoras de infraestructura troncal y no reconfiguración de routers de núcleo porque el reenvío se basa en etiquetas en lugar de la cabecera IP en sí, ofreciendo una estrategia muy rentable para el despliegue de IPv6.

El uso de cualquier transporte de circuito para el despliegue de IPv6 sobre redes MPLS no tiene impacto en la operación o infraestructura de MPLS, y no requiere cambios de configuración en el núcleo o proveedor de routers de borde. La comunicación entre los dominios remotos IPv6 son con protocolos IPv6 nativos más de un enlace dedicado, donde los mecanismos subyacentes son completamente transparentes para IPv6. El tráfico IPv6 se hace un túnel mediante cualquier transporte MPLS Ethernet.

# CAPÍTULO 1
# CONCEPTOS GENERALES

## 1.1 Antecedentes

Desde mediados de los años 90 creció una notable necesidad de separar el tránsito de red y el flujo de control entre dispositivos que integran las redes de alta velocidad, en ese mismo periodo se concreta la funcionalidad y composición de la tecnología MPLS.

Se optó por defender ventajas del standard MPLS para soportar procedimientos de encaminamientos y envío de paquetes en backbones IP, además de estas ventajas proporciona nuevos soporte para servicios como QoS(calidad de servicio) y VPNs(Protocolo de redes virtuales) a los que dota de mejoras en sus prestaciones respecto a los tradicionales túneles y circuitos virtuales.

Las nuevas tecnologías que aparecieron de la mano de la fibra óptica, tales como DWDM (Dense Wavelength División Multiplexing), son una alternativa eficaz a ATM para multiplexar servicios sobre circuitos. Se debe sumar a este hecho, la creciente sustitución de conmutadores ATM por enrutadores en el núcleo de las redes. MPLS surge del IETF (International Engineering Task Force), grupo de trabajo de ingeniería de internet, entidad que regula las propuestas y los estándares de internet. Con este desarrollo se intenta dar soluciones de conmutación multinivel. (locortes.net, 2005)

Cuando se comenzó a utilizar internet, los backbones IP de los proveedores estaban construidos por enrutadores conectados entre sí, lo cual generó saturación de las redes y provocó congestión en las transmisiones. Entonces, lo más lógico fue aumentar el rendimiento de los enrutadores, dándose a conocer los conmutadores ATM con ciertas capacidades de control IP. Se generaron entonces varios tipos de problemas que tenían que ver con el rendimiento óptimo y para lo cual se implementaron soluciones de integración de niveles que fueron conocidos como conmutación IP, sin embargo, estas soluciones causaban congestionamiento y no eran operativas entre las distintas tecnologías de capa 2 y 3 que se conocían.

En los últimos años se han desarrollado diferentes tecnologías como MPLS, y se han puesto al servicio de las empresas para que éstas puedan mezclar la alta velocidad de operación de ATM basada en conmutación con el proceso de enrutamiento IP de Internet de la capa de Red.

## 1.2 Planteamiento del Problema

Es factible la teorización para dar a conocer un modelo de implementación, configuración de dispositivos de una red MPLS en entorno IPv6, debido a la necesidad de integrar y aprovechar las ventajas que proporciona MPLS integrando múltiples servicios por un mismo canal con calidad de servicio.

## 1.3 Objetivos

### 1.3.1 Objetivo General

- Realizar el análisis de funcionalidad, diseño, simulación, configuración de dispositivos de una red MPLS en entornos IPv6.

### 1.3.2 Objetivos Específicos

- Conocer los conceptos de la funcionalidad, operación, etiquetado, flujo de paquetes de una red MPLS.
- Analizar una topología posible para la implementación de una red MPLS, así tener una idea clara y concisa de la conformación de este tipo de redes.
- Investigar las características, elementos, beneficios que proporciona la implementación de una red MPLS.
- Dar a conocer los elementos de infraestructura que se utiliza en la implementación de este tipo de redes.
- Conocer los resultados de una simulación en GNS3 obtenidos de una red MPLS en entorno IPv6.

## 1.4 Justificación

El trabajo de grado tiene la finalidad de dar a conocer el funcionamiento, diseño, elementos de infraestructura de una red Multiprotocol Label Switching (MPLS) en entorno IPv6, debido a la gran demanda de usuarios al internet, incremento de dispositivos smartphone, pc, tablet, alta calidad de servicio QoS (video conferencia, VoIP, datos). MPLS se puede implementar sin problemas tanto sobre el IPv4, así como las redes IPv6.

IPv6 puede usar cualquier circuito de transporte para la instalación sobre redes MPLS con el protocolo IPv6, no tiene ningún impacto en la operación o en la infraestructura de MPLS, no requiere de cambios en la configuración de los routers de core o de provider edge, la comunicación entre los dominios IPv6 remotos se ejecuta nativamente con IPv6 sobre enlaces dedicados, los mecanismos subyacentes son completamente trasparentes a IPv6, el tráfico IPv6 es encapsulado en un túnel sobre cualquier transporte en MPLS.

IPv6 entre las principales ventajas que proporciona es mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionables. IPv6 provee paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers alineados a 64 bits y con una cabecera de longitud fija, las opciones más comunes de IPv6 sobre MPLS permiten que dominios aislados de IPv6 se comuniquen entre si sobre un backbone de MPLS IPv4, este tipo de implementación, requiere de pocas actualizaciones o cambios en la infraestructura del backbone, no requiere la reconfiguración de los routers de core, ya que el reenvió de tráfico se hace basado en las etiquetas más que en IP. Todo esto resulta en una estrategia muy efectiva (coste, trabajo, tiempo) para la instalación y uso de IPv6 en una red MPLS. Una red MPLS constituye ya una alternativa de mayor alcance debido a sus ventajas. La creciente necesidad de incluir voz, datos y video por una mismo camino, aumentar la productividad, soportar más aplicaciones y elevar la seguridad, han llevado a grandes operadores a migrar sus servicios a redes MPLS. La creciente necesidad de migrar a redes MPLS se debe a su gran capacidad para integrar varios servicios en una plataforma común con garantías de calidad de servicio (QoS), hay que sumar las

mejoras del rendimiento y la disponibilidad que se obtienen con esta tecnología, así como su soporte de una amplia y escalable gama de servicios.

Su topología de muchos-a-muchos (any-to-any) ofrece a los administradores la flexibilidad para desviar tráfico sobre la marcha en caso de fallo de enlaces y congestión de red. Además, la ingeniería de tráfico y la precisión e inteligencia del encaminamiento basado en MPLS permiten empaquetar más datos en el ancho de banda disponible y reducir los requerimientos de procesamiento a nivel de router. Se trata, pues, de una tecnología de red efectiva, rápida y altamente escalable.

## 1.5 Situación Actual de redes MPLS

Hoy en día las tecnologías más utilizadas para el manejo de redes son: MPLS y IPSec, las dos en proceso de estandarización por el IETF. Las operadoras telmex, avantel, grupo TVClable, CNT EP, están optando por migrar sus redes ATM a MPLS debido a las ventajas que tiene en costo y las herramientas que maneja para mejorar el desempeño de la red en general. Ambas tecnologías se están desarrollando a la par, MPLS por un lado se enfoca principalmente en los backbones e IPSec por otro en los clientes. Por esta razón se busca hibridar ambas tecnologías en un futuro para que IPSec maneje la encriptación de la información y MPLS la provisión de servicios y de ruteo inteligente de tráfico. (catarina.udlap.mx, 2006)

MPLS opera entre la capa de enlace de datos y la capa red del modelo OSI, está diseñado para unificar el servicio de transporte de datos para redes basadas en circuitos y paquetes. MPLS se caracteriza por ofrecer niveles de rendimiento diferenciado, priorización de tráfico, mayor velocidad de transmisión, facilita la gestión de recursos en la red y sobre todo es una tecnología que permite ofrecer calidad de servicio QoS independientemente de la red sobre la cual se implemente. MPLS es una arquitectura que provee una eficiente designación, enrutamiento, envío y conmutación de flujos de tráfico a través de la red. (catarina.udlap.mx, 2006)

## 1.6 Evolución de las redes MPLS

MPLS es un estándar emergente del IETF, desarrollado a mitad de los años 90's y ha tomado diferentes aportes o propiedades de IP Switching (Ipsilon), cell switching enrutador (Toshiba), tag switching (Cisco) y switcheo IP basado en rutas agregadas o ARIS (IBM). Las anteriores empresas o tecnologías utilizaban conmutación de etiquetas como un método para el envío de datos. La idea central de MPLS es adicionar una etiqueta a cada paquete que se quiere enviar. A estos paquetes se les asigna un par de valores de longitud corta que sintetizan el origen y destino de dicho paquete.

MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"), o bien, como una técnica para acelerar el encaminamiento de paquetes incluso, para eliminar por completo el enrutamiento, en realidad MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del enrutamiento con la simplicidad y rapidez de la conmutación de nivel 2.

MPLS es un avance de la tecnología de IP que eficientiza los tiempos de transporte y la elección de rutas. Además es una solución versátil dirigida a los actuales problemas al nivel de redes como la velocidad, escalabilidad, calidad de servicio y aplicación de la ingeniería de tráfico.

MPLS ha surgido como una solución inteligente al manejo de ancho de banda y requerimientos de servicio proveyendo una eficiente asignación, envío y conmutación de información o datos a través de redes, también agrega seguridad al transporte de la información y simplifica el manejo de direcciones. El multiprotocolo de conmutación de etiquetas reduce significativamente el procesamiento de paquetes que se requiere cada vez que un paquete ingresa a un enrutador en la red.

# CAPÍTULO 2
# MARCO TEÓRICO

## 2.1 IPv6

"IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4." (RAU, 2011)

"En esta versión se mantuvieron las funciones del protocolo IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características." (RAU, 2011)

> El protocolo de internet (Internet Protocol, IP) es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI. La versión 6 del protocolo de internet (IPv6) es la nueva versión del protocolo de internet, las direcciones disponibles en IPv4, y la versión actual del protocolo de internet, prácticamente se han agotado. (RAU, 2011)
>
> El espectacular crecimiento del tráfico en internet y la tan ansiada convergencia de voz, datos, imagen y video en una única red, hacen necesaria la evolución de las comunicaciones que van de la mano de las siglas IP. El internet protocol (IP), es el medio que le permite a una red comunicarse, aparece ahora también como el elemento integrador, capaz de hacer converger todas las necesidades de comunicación de compañías y usuarios, en una misma infraestructura. (34t.com, 1995)
>
> Internet protocol version 6 (IPv6) llamado también "Ipng**"** desarrollado mediante una serie de especificaciones por la IETF ha sido creado para reemplazar la actual versión del protocolo de internet IPv4 e introducir mejoras significantes como cambiar las direcciones IP de 32 a 128 bits con lo que se corrige ya la actual escasez de direcciones de red. IPv6 modifica las direcciones de modo que ahora son de 128 bits, particionados en 64 para la

red y 64 para el equipo (esto, permite 18446744073709551616 redes cada una con una cantidad a los efectos prácticos infinita de equipos conectados). (repositorio.espe.edu.ec, 2005)

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento. (RAU, 2011)

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la calidad de servicio (QoS), seguridad (IPsec) y movilidad. (RAU, 2011)

El crecimiento explosivo de los dispositivos móviles como los celulares, computadores portátiles y dispositivos de mano inalámbricos ha creado la necesidad de bloques adicionales de direcciones IP. IPv4 es compatible actualmente con un máximo de aproximadamente 4,294,967,296 o ($2^{32}$) direcciones IP únicas. IPv6 admite un máximo teórico de 340,282,366,920,938,463,463,374,607,431,768,211,456 o $2^{128}$ direcciones, los recientes avances en la tecnología de red, incluyendo la traducción de direcciones de red (NAT) se han reducido temporalmente la urgencia de nuevas direcciones IP, sin embargo, estimaciones recientes indican que las direcciones IPv4 podrían agotarse.

IPv6 e IPv4 comparten una arquitectura similar, la mayoría de los protocolos de capa de transporte que funcionan con IPv4 también funcionará con el protocolo IPv6. Se espera que la mayoría de los protocolos de capa de aplicación para que funcione con IPv6, una dirección IPv6 consiste en ocho

grupos de cuatro dígitos hexadecimales. Si un grupo está formado por cuatro ceros, la notación se puede acortar utilizando dos puntos para sustituir los ceros. (RAU, 2011)

### 2.1.1 Características principales del protocolo IPv6 e IPv4

**IPv6**

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Simplificación del formato del header. Algunos campos del header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones aggregatable global unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC, en este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.

- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad.
- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Las nuevas extensiones de encabezado reemplazan el campo opciones de IPv4 y proveen mayor flexibilidad.
- En el protocolo IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.
- IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.
- Hay que resaltar que no existen las direcciones de difusión (broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast. No hay direcciones broadcast (su función es sustituida por direcciones multicast). (ipv6.mx, 2013 )

**IPv4**

- IPv4 es la versión 4 del protocolo versión anterior de IPv6. Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet. IPv4 usa direcciones de 32 bits, limitándola a $2^{32}$ = 4.294.967.29, direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).
- IPv4 es capaz de generar aproximadamente 40000 millones de combinaciones de direcciones, donde estas mismas solo contienen 32 bits por lo que es muy limitada y lenta para transmitir videos y voz.
- El protocolo IPv4 contiene enlace con fibra óptica. (venio.info, 2013)

Para tener una mejor comprensión se describirá en la tabla 1 las características de IPV4 respecto a IPv6

Tabla 1: Características IPv4 e IPv6

| Protocolo | Concepto | Estructura | Ventajas | Desventajas | Direcciones admitidas |
|---|---|---|---|---|---|
| Ipv4 | Es la cuarta versión del protocol internet, y la primera es ser implementada a gran escala | Está compuesta de 4 grupos de 8 bits(32 bits), cada uno 8x4=32; se puede decir que 4 grupos decimales donde cada uno está formado por 3 dígitos . | Direcciones de32 bits. Formato de cabecera más grande. Configuración manual. DireccionesBroadcast. Contiene enlaces con fibra óptica | Elevada demanda de direcciones IP. No posee seguridad. Limita el crecimiento del internet. | Soporta 4.294.967.296 (232) direcciones de red diferentes |
| Ipv6 | Es la versión 6 del protocolo de Internet(Internet protocol) un estándar en desarrollo del nivel de red encargado de dirigir y encaminar los paquetes através de una red. | Está compuesto de ocho grupos de cuatro caracteres cada uno, compuestas por un prefijo de 64 bits y un identificador de interfaz también de 64bits. Además se complica un poco ya que los grupos en vez de expresarse en notación decimal lo harán en hexadecimal y la separación no sehará por un punto si no por dos puntos. Por ejemplo:2001:DB8:0:2F3B:2AA:FF:FE28:9C5A | Direcciones de128 bits. Formato de cabecera más sencillo. Configuración automática Direccionesmulticast. Seguridad incorporada(encriptación de la información | La necesidad de extender un soporte permanente para IPv6 através de todo Internet y de los dispositivos conectados a ella. Para estar enlazada al universo IPv6 durante la fase de transición,todavía se necesita una direcciónIPv4 o algún tipo de NAT | Soporta 340282366920938463374607431768211456 (2 elevado a 128) de direcciones |

Elaborado por: Rolando Reyes

La configuración de direcciones IP en equipos como routers, switch, se lo realiza en cada interface tal como se puede ver en el último capítulo del presente trabajo, las direcciones se configuran ingresando a cada interface de los dispositivos antes mencionados. Para la configuración en PCs la configuración se la realiza ingresando a la tarjeta de red de cada dispositivo, se la puede realizar manualmente o automáticamente.

### 2.1.2 Tipos de direcciones IPv6

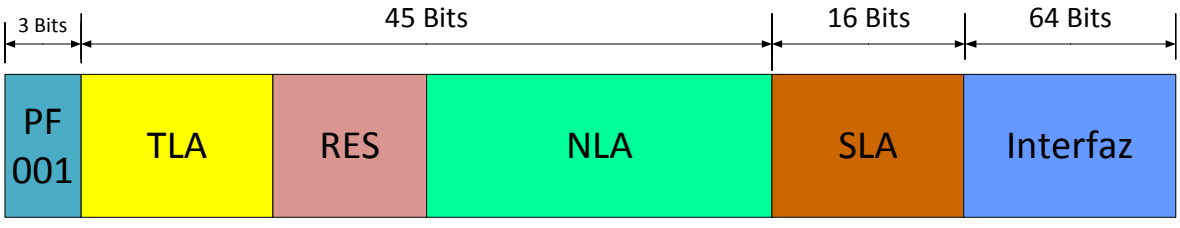
#### 2.1.2.1 Direcciones unicast (Unidifusión)

Este tipo de dirección es similar a las direcciones IPv4, las direcciones de unidifusión identifican una única interfaz, es decir, cuando se envía un paquete a una dirección de unidifusión se envía por una interfaz con dicha dirección. Asignación de direcciones unicast en IPv6:

- Direcciones unicast basadas en el proveedor global.
- Direcciones unicast basadas en la región geográfica.
- Direcciones NSAP (Network Service Access Point).
- Direcciones jerárquicas IPX (Internet Protocol Exchange).
- Direcciones para el uso del sitio local.
- Direcciones para el uso del enlace local.
- Direcciones de host habilitadas para IPv4 (utn.edu.ec, 2011)

**Direcciones unicast basadas en el proveedor global.-** Son usadas para la comunicación global. Tienen el siguiente formato, como se muestra en la figura 1, tiene los siguientes campos

Figura 1: Dirección unicast basada en el proveedor global




Fuente: http://repositorio.utn.edu.ec

**PF.-** Prefijo de formato, con valor 001.

**TLA.-** Identificador de agregación de nivel superior.

**RES.-** Campo reservado para usos futuros.

**NLA.-** Identificador de agregación de siguiente nivel.

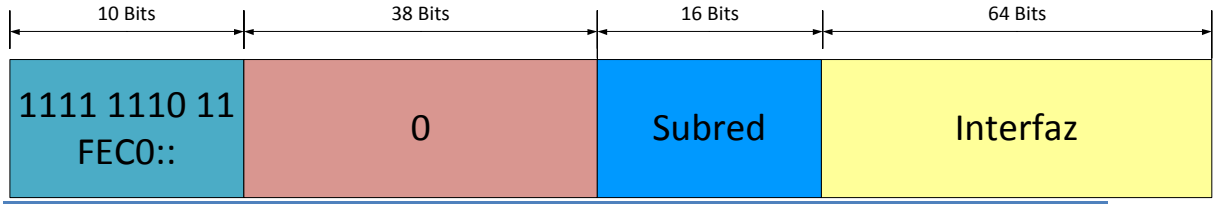
**SLA.-** Identificador de agregación de nivel del sitio.

**Interfaz.-** Identificador de la interfaz, campo de 64 bits.

**Direcciones unicast de uso local.-** Son direcciones unicast que solo tienen alcance de enrutamiento local. Hay dos tipos de direcciones de uso local:

- **Direcciones para el uso del sitio local.-** Están diseñadas para ser usadas en direccionamiento por un enlace simple, para propósitos como configuración de autodirección, detección de vecinos o cuando no hay routers presentes, ver figura 2. (utn.edu.ec, 2011)

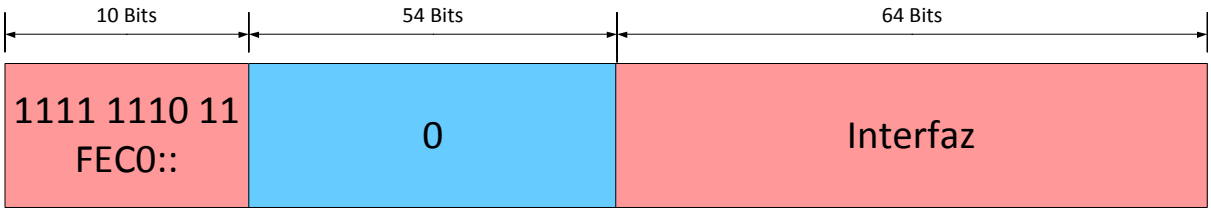
Figura 2: Dirección unicast de uso del sitio local




Fuente: http://repositorio.utn.edu.ec

- **Direcciones para el uso del enlace local.-** Pueden ser usadas por sitios u organizaciones que no están conectadas a la red global internet, como se puede observar en la figura 3. (utn.edu.ec, 2011)

Figura 3: Dirección unicast de uso del enlace local




Fuente: http://repositorio.utn.edu.ec

#### 2.1.2.2 Direcciones anycast (Monodifusión)

> Las direcciones de monodifusión identifican un grupo de interfaces, generalmente pertenecen a diferentes nodos. Un paquete enviado a una dirección de monodifusión se entrega a una de las interfaces identificadas por la dirección. Se escoge la dirección más cercana, según la distancia del protocolo de enrutamiento que se utilice. (utn.edu.ec, 2011)

Posibles usos de las direcciones de monodifusión en un conjunto de routers:

- Identificar un proveedor de servicios de Internet.
- Identificar subredes en particular.

> Los formatos definidos para las direcciones de unidifusión son asignadas para las direcciones de monodifusión. Las direcciones de monodifusión no se diferencian de las direcciones de unidifusión. Una dirección de monodifusión parte de cuando se asigna a más de una interfaz una dirección de unidifusión. Los nodos deben ser configurados explícitamente para que sepan que la dirección es una dirección de monodifusión. (utn.edu.ec, 2011)

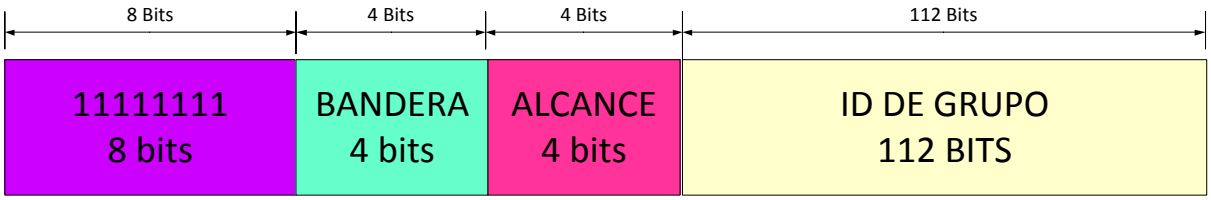
Restricciones a las direcciones anycast de IPv6:

- No se utiliza una dirección de monodifusión como dirección de origen en un paquete IPv6.
- No se asigna una dirección de monodifusión a un host IPv6. Sólo se puede asignar a routers IPv6. (utn.edu.ec, 2011)

#### 2.1.2.3 Direcciones multicast (Multidifusión)

Una dirección multidifusión es un identificador para un grupo de interfaces, y su formato se muestra en la figura 4:

Figura 4: Formato de una dirección de multidifusión




Fuente: http://repositorio.utn.edu.ec

La descripción de los campos es la siguiente:

**11111111.-** Ubicado al inicio de la dirección específica que es una dirección de multidifusión.

**Bandera.-** Campo de 4 bits. Los primeros tres bits están reservados y se inicializan en cero. El cuarto bit si es cero indica que es una dirección de multidifusión permanente, mientras que si este bit es 1 indica que no es una dirección de multidifusión permanente (dirección transitoria). (utn.edu.ec, 2011)

**Alcance.-** Se utilizan 4 bits para limitar el alcance del grupo de multidifusión.

Los valores de alcance se muestran en la tabla 2.

Tabla 2: Valores de alcance de una dirección multicast

| Valores | Significado |
|---|---|
| **0** | Reservado |
| **1** | Alcance de nodo local |
| **2** | Alcance de enlace local |
| **3,4** | No asignado |
| **5** | Alcance de sitio local |
| **6,7** | No asignado |
| **8** | Alcance de organización local |
| **9 - D** | No asignado |
| **E** | Alcance global |
| **F** | Reservado |

Fuente: http://repositorio.utn.edu.ec

**ID de grupo.-** Sirve para identificar el grupo de multidifusión.

"Las direcciones de multidifusión no deben ser utilizadas como dirección de origen en los datagramas IPv6 ni aparecer en cualquier cabecera de enrutamiento." (utn.edu.ec, 2011)

### 2.1.3 Arquitectura de direcciones IPv6

En el protocolo de internet versión 6 (IPv6), las direcciones son de 128 bits, la ventaja de direcciones tan grandes es para subdividir direcciones disponibles en una jerarquía de dominios de enrutamiento que reflejan la topología de internet. IPv6 representa una capacidad inherente de resolver direcciones en el nivel más bajo, que está en el nivel de interfaz de red, y también tiene capacidades de configuración automática. (RAU, 2011)

Existen tres formas de representar las direcciones IPv6 como strings de texto.

- x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo cómo se muestra en la tabla 3. (RAU, 2011)

Tabla 3: Representación 1 de dirección IPV6

| Dirección IPV6 |
| --- |
| FEDC: BA98:7654:3210: FEDC: |
| BA98:7654:3210 1080:0:0:0:8:800:200C:417A |

Fuente: http://www.rau.edu.uy

- Para utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente :: (dos puntos) para representarlos. El uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección como se muestra en la tabla 4 y 5.

Tabla 4: Representación de 16 bits de ceros en una dirección IPV6

| | |
|---|---|
| **1080:0:0:0:8:800:200C:417A** | **unicast address** |
| **FF01:0:0:0:0:0:0:101** | **multicast address** |
| **0:0:0:0:0:0:0:1** | **loopback address** |
| **0:0:0:0:0:0:0:0** | **unspecified addresses** |

Fuente: http://www.rau.edu.uy

Podrán ser representadas como:

Tabla 5: Representación dirección IPV6 con los :: (dos puntos)

| | |
|---|---|
| **1080:: 8:800:200C:417A** | **unicast address** |
| **FF01::101** | **multicast address** |
| **:: 1** | **loopback address** |
| **::** | **unspecified addresses** |

Fuente: http://www.rau.edu.uy

- Para escenarios con protocolos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:

  x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4 como se muestra en la tabla 6 y 7. (RAU, 2011)

Tabla 6: Representación escenarios con protocolos IPv4 e IPv6

| **Dirección IPV6** |
|---|
| **0:0:0:0:0:0:13.1.68.3** |
| **0:0:0:0:0:FFFF:129.144.52.38** |

Fuente: http://www.rau.edu.uy

Forma comprimida

Tabla 7: Representación escenarios con protocolos IPv4 e IPv6 comprimido

| **Dirección IPV6 Comprimida** |
|---|
| **::13.1.68.3** |
| **::FFFF:129.144.52.38** |

Fuente: http://www.rau.edu.uy

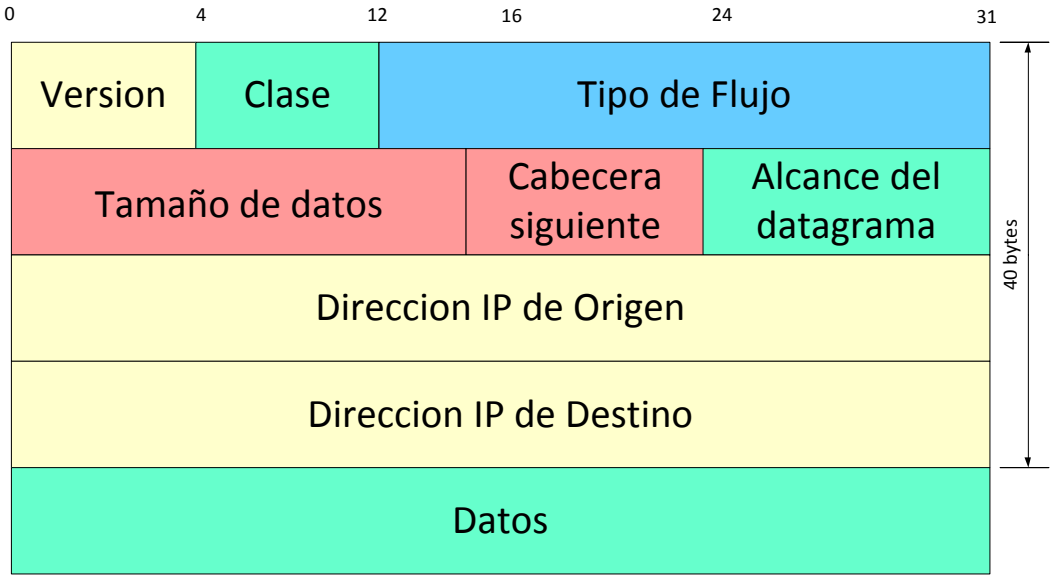
### 2.1.3.1 Estructura de datagrama IPv6 e IPv4

El protocolo IPv6, en la capa de red inserta cabeceras en cada paquete para permitir el manejo de flujos extremo a extremo. Tiene una cabecera de longitud fija de 40 octetos, distribuidos en 8 campos.

"IPv6 incrementa las capacidades para los requerimientos actuales en direccionamiento y enrutamiento." (epn.edu.ec, 2011)

IPv6 ha simplificado el formato de la cabecera, algunos campos de la cabecera IPv4 se han eliminado, cambiado de posición, modificado, mantenido y otros nuevos se han establecido. Los campos de la cabecera IPv6, como se pueden ver en la figura 5, son los siguientes:

Figura 5: Formato de la Cabecera IPv6




Fuente: http://bibdigital.epn.edu.ec

**Versión.-** Campo de 4 bits, indica el número de la versión del protocolo. El valor es igual a 6 para IPv6.

**Clase de tráfico.-** Campo de 8 bits, asigna prioridad a cada paquete, es decir distingue entre paquetes con requisitos diferentes de entrega en tiempo real, aún si es de la misma fuente.

**Tipo de flujo o etiqueta de flujo.-** Campo de 20 bits, sirve para tráfico con requisitos de calidad de servicio no estándar o servicio en tiempo real.

**Tamaño de los datos o longitud de carga útil.-** Campo de 16 bits, específica la longitud de los datos IPv6 en bytes y no incluye la cabecera IPv6.

**Cabecera siguiente.-** Campo de 8 bits, identifica el tipo de cabecera que sigue inmediatamente a la cabecera básica de IPv6.

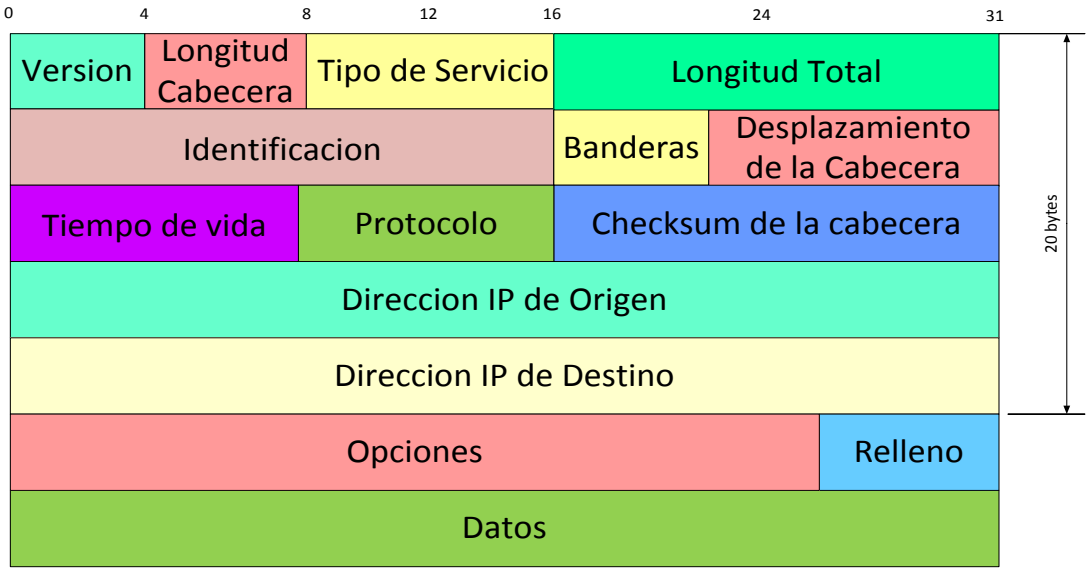
**Alcance del datagrama o límite de saltos.-** Campo de 8 bits sin signo. Se disminuye en una unidad por cada nodo que reenvía el paquete. Se descarta el paquete si el límite de saltos llega a cero.

**Dirección origen.-** Campo de 128 bits, contiene la dirección IP del host origen. (epn.edu.ec, 2011)

**Dirección destino.-** Campo de 128 bits, contiene la dirección IP del destino (posiblemente no es el último destino deseado, si está presente una cabecera de enrutamiento).

**IPv4.-** Los datagramas también se denominan paquetes. Si a los datos se le añaden un encabezado que contiene información de la dirección IP destino se obtiene un datagrama. Un datagrama IP está formado por una cabecera y un campo de datos. La cabecera está formada por 20 bytes fijos y una parte opcional de longitud variable. En la figura 6 se muestra la estructura del datagrama IPv4. (epn.edu.ec, 2011)

Figura 6: Datagrama IPv4




Fuente: http://bibdigital.epn.edu.ec

**Versión.-** Campo de 4 bits, indica la versión del protocolo IP usado.

**Longitud de la cabecera.-** Campo de 4 bits, específica la longitud de la cabecera IP en palabras de 32 bits.

**Tipo de servicio.-** Campo de 8 bits, especifica cómo un protocolo de capa superior desea que se le envíe el datagrama.

**Longitud total del datagrama.-** Campo de 16 bits, define la longitud total del datagrama incluyendo la cabecera y los datos, expresada en bytes.

**Identificación.-** Campo de 16 bits, contiene un número entero que identifica al datagrama. Si un datagrama es fragmentado, cada fragmento tendrá el mismo identificador.

**Banderas.-** Campo de 3 bits.

**Desplazamiento de cabecera.-** Campo de 13 bits, indica la posición del fragmento en bytes dentro de un datagrama. Este campo se incrementa en cada fragmento del datagrama que se envía comenzando en cero. Cada datagrama tiene un máximo de 8.192 fragmentos.

**Tiempo de vida (TTL).-** Campo de 8 bits, específica en segundos el tiempo que puede viajar por una red un datagrama antes de ser descartado. El tiempo máximo es de 255 segundos. Cada vez que un datagrama llega a un router, éste disminuye el valor contenido en el campo TTL en una unidad.

**Protocolo.-** Campo de 8 bits, indica de qué protocolo proviene el datagrama.

**Checksum de la cabecera.-** Campo de 16 bits, permite detectar errores que pueden ocurrir en la cabecera y no en los datos del datagrama durante su transmisión por la red, es decir asegura la integridad de la cabecera.

**Direcciones IP del origen.-** Campo de 32 bits, contiene la dirección IP del host origen.

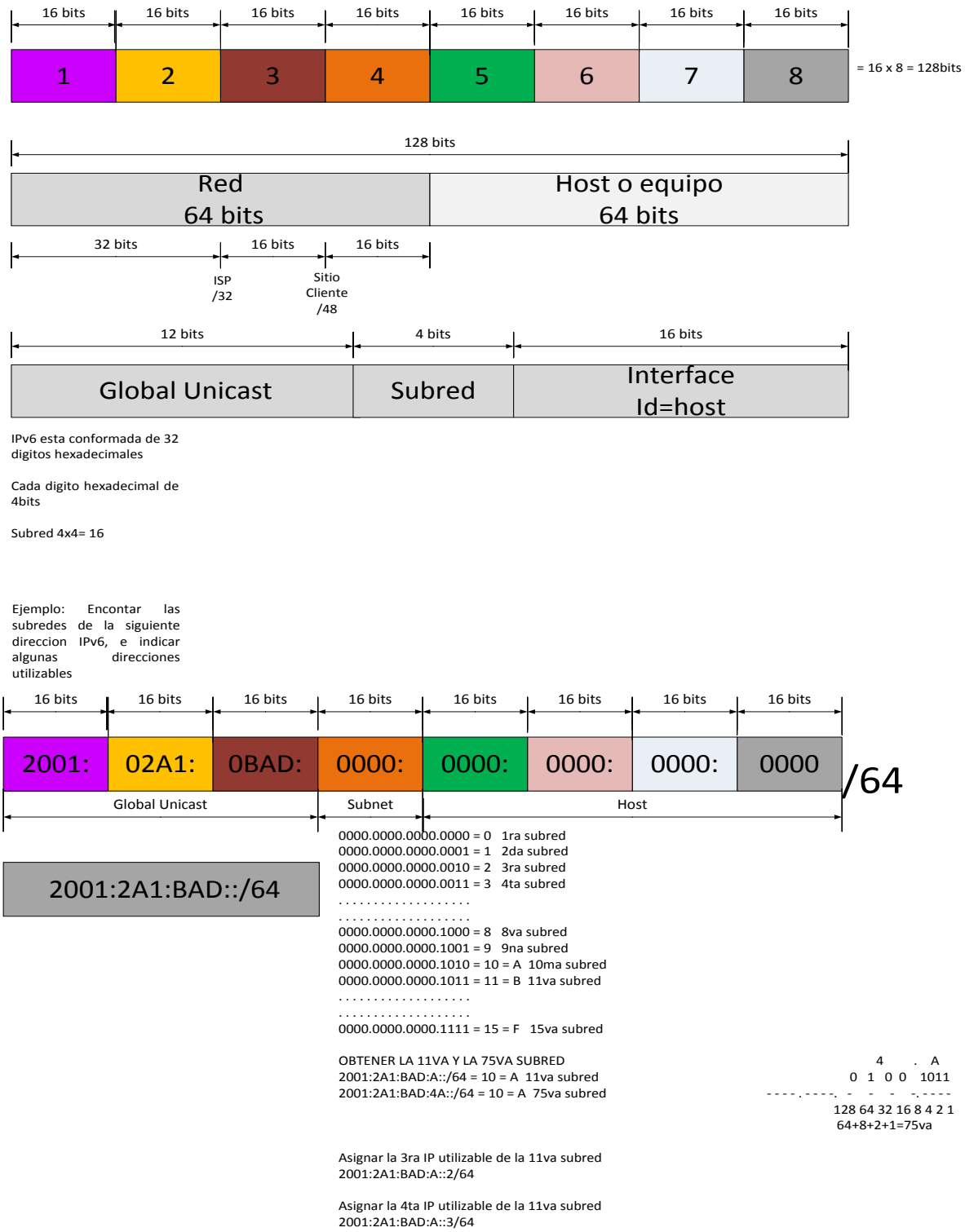
**Direcciones IP del destino.-** Campo de 32 bits, contiene la dirección IP del host destino.

**Opciones.-** Campo opcional y de longitud variable, permite implementar pruebas y control de la red.

**Relleno.-** Campo de longitud variable, se utiliza cuando la cabecera no tiene un tamaño múltiplo de 32 bits, se rellena con ceros. (epn.edu.ec, 2011)

Para entender cómo funciona el subneting en IPV6 se realizara un ejemplo a continuación, ver figura 7.

Figura 7: Subneting IPv6




Elaborado por: Rolando Reyes

### 2.1.3.2 Ventajas y desventajas IPv4 frente a IPv6

En la tabla 8 se describe las ventajas y desventajas de IPv4 frente a IPv5

Tabla 8: Ventajas y desventajas IPv4 frente a IPv6

| | **IPv4** | **IPv6** |
|---|---|---|
| **Direcciones** | Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes). | Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes). |
| **IPSec** | La compatibilidad es opcional. | La compatibilidad es obligatoria. |
| **Identificación del número de paquetes** | No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4. | Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo). |
| **Fragmentación** | La llevan a cabo los enrutadores y el host que realiza el envío. | No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío. |
| **Encabezado** | Incluye una suma de comprobación. | No incluye una suma de comprobación. |
| **Opciones** | El encabezado lo incluye. | Todos se trasladan a los encabezados de extensión IPv6. |
| **Marcos de solicitud ARP** | El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo. | Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión. |
| **Administrar la pertenencia a grupos locales de subred** | Se utiliza el Protocolo de administración de grupos de Internet (IGMP). | IGMP se sustituye con los mensajes de Descubrimiento de escucha de multidifusión (MLD). |
| **Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada** | Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional. | El Descubrimiento de enrutadores ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio. |
| **Direcciones de multidifusión** | Se utilizan para enviar tráfico a todos los nodos de una subred. | No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección |

| | | |
|---|---|---|
| | | de multidifusión para todos los nodos de ámbito local del vínculo. |
| **Configuración manual** | Debe configurarse manualmente o a través de DHCP. | No requiere configuración manual o a través de DHCP. |
| **DNS** | Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4. | Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6. |
| **Tamaño de paquete** | Debe admitir un tamaño de 576 bytes (posiblemente fragmentado). | Debe admitir un tamaño de 1280 bytes (sin fragmentación). |

Elaborado por: Rolando Reyes

### 2.1.3.3 Integración de IPv4 frente a IPv6

IPv6 es una nueva versión de internet protocol, diseñada para suceder a la actual (IPv4). La transición entre ambas será un largo proceso durante el que se ha de garantizar la coexistencia.

Pasar de IPv4 a IPv6 no es sencillo y los mecanismos que permiten la coexistencia y la transición entre las dos versiones han de estar estandarizadas.

La implementación de IPv6 implica que IPv4 estará coexistiendo con IPv6, siendo las aplicaciones las responsables de decidir cuál protocolo usarán. En la implementación de IPv6 se pueden tener dos escenarios básicos:

- Implementar utilizando sólo IPv6
- Implementar IPv6 en conjunto con IPv4

Actualmente el soporte de IPv6 se encuentra en proceso de maduración en las aplicaciones comerciales y productos. Esto influirá en la decisión de adoptar un esquema de doble pila que usa IPv6 cuando está disponible o IPv4 en caso contrario. Las redes actuales utilizan IPv4. La introducción de IPv6 a las redes será incremental, por lo tanto los clientes y los routers deberán ser capaces de comunicarse utilizando cualquiera de los protocolos, este esquema es conocido

como doble pila (dual-stack). La elección del protocolo dependerá directamente de la aplicación. La desventaja de este modelo es que se basa en una conectividad a IPv6 confiable, de otro modo, el desempeño de la aplicación se podría ver con un rendimiento más bajo que solo usando IPv4.

Existen diferentes modelos a ser implementados para la integración de IPv4 a IPv6

- Doble pila (dual-stack)

Servidores/ dispositivos hablando ambos protocolos

- Túneles

IPv6 se encapsula a través de enlaces de IPv4
Los paquetes de IPv6 son el payload de los paquetes de IPv4

- Métodos de traducción (de IPv4 únicamente a IPv6 únicamente)

La información de los encabezados debe ser re-escrita
Es necesario utilizar las capas de aplicación de los gateways

Para la transición de IPv4 a IPv6 existen distintos factores a ser tomados en cuenta:

Técnicos: Planear actualizaciones de equipo y aplicaciones
Políticas: Métodos de administración y manejo del tráfico IPv6
Educativo: Capacitación adecuada del personal para el uso de IPv6

> La transición a IPv6 es necesaria debido al agotamiento de direcciones públicas de IPv4, siendo útil también para disminuir el tamaño de las tablas de enrutamiento y por el crecimiento en volumen de dispositivos móviles. IPv6 tiene en general el objetivo de ofrecer una transición suave de IPv4 a IPv6, debido a la extensa utilización e inversión en infraestructura basada en IPv4, ofreciendo esquemas que permitan utilizar o encapsular los protocolos en ciertos momentos durante el transporte de paquetes o discriminando su uso según sea necesario. (NEXICA, 2013)

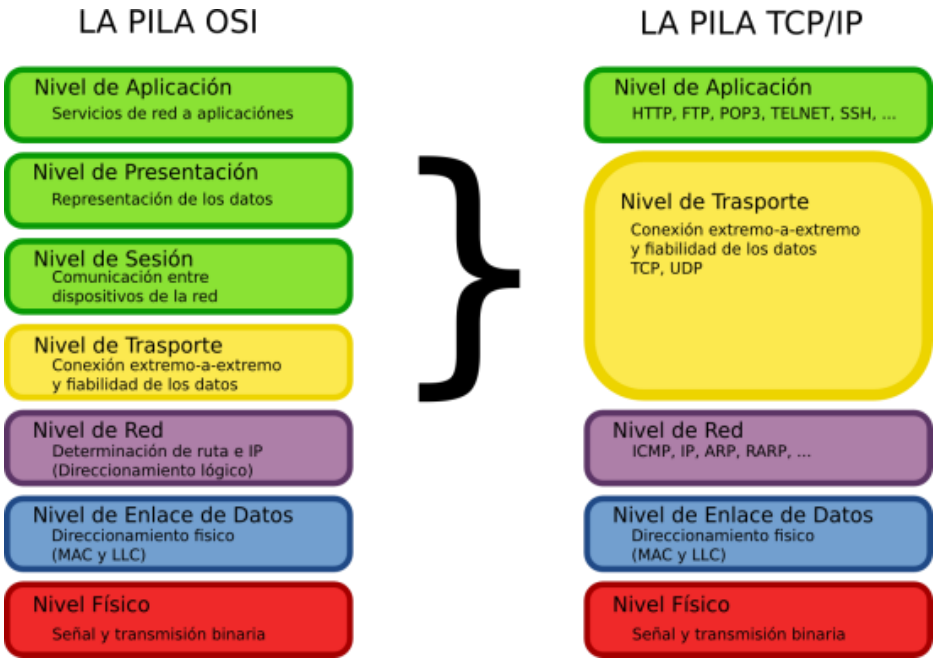
## 2.2 TCP/IP

Protocolo de control de transmisión/protocolo de internet (Transmission Control Protocol/Internet Protocol*)*, es un sistema de protocolos que hacen posibles servicios telnet, ftp, e-mail, y otros entre computadores que no pertenecen a la misma red. El protocolo de control de transmisión (TCP) permite a dos anfitriones establecer una conexión e intercambiar datos. TCP garantiza la entrega de datos, es decir, que los datos no se pierdan durante la transmisión y también garantiza que los paquetes sean entregados en el mismo orden en el cual fueron enviados. Internet se encuentra estrechamente unida a un sistema de protocolo de comunicación denominado TCP/IP (Transmission Control Protocol/ Internet Protocol), que se utiliza para transferir datos en internet además en muchas redes de área local. Los dos protocolos más importantes y que fueron también los primeros en definirse y también los más utilizados, son TCP (Protocolo de Control de Transmisión o Transmission Control Protocol) e IP (Protocolo de Internet o Internet Protocol), de ahí que se denomine también como conjunto de protocolos TCP/IP. (protocolotcpip.galeon.com, 2014)

Los tipos de protocolos existentes superan los cien, entre los cuales se puede mencionar como los más conocidos a HTTP, FTP, SMTP, POP, ARP. TCP/IP es la plataforma que sostiene internet y que permite la comunicación entre diferentes sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN). El protocolo TCP IP se ha dividido en diversas capas, cada uno de estas realiza una tarea específica en orden, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información llamado encabezado y los envía a la capa siguiente. TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de internet. Por este motivo se debe tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP, sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales de TCP/IP es proporcionar una abstracción del medio de forma que sea posible

el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles. Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. El modelo TCP/IP es muy similar al modelo OSI (modelo de 7 capas) que fue desarrollado por la organización internacional para la estandarización (ISO) para estandarizar las comunicaciones entre equipos, a continuación se detallara en la figura 8 las capas en los modelos OSI (Open System Interconection) y TCP/IP. (resplandorrc.blogspot, 2013)

Figura 8: Pila OSI y TCP/IP




Fuente: http://resplandorrc.blogspot.com

### 2.2.1 Modelo OSI: 7 capas

El modelo OSI es un modelo que comprende 7 capas OSI. La función del modelo OSI es estandarizar la comunicación entre equipos para que diferentes fabricantes puedan desarrollar productos (software o hardware) compatibles (siempre y cuando sigan estrictamente el modelo OSI), a continuación de describirá las 7 capas del modelo OSI.

• La capa física: Específica un estándar para la interconexión física entre computadoras anfitrión y conmutador de paquetes de red para transferir paquetes de una máquina a otra. Ejm pulsos eléctricos, modulación de luz

• La capa de enlace de datos: 2da capa define la interfaz con la tarjeta de interfaz de red y cómo se comparte el medio de transmisión.

• La capa de red: 3era capa permite administrar las direcciones y el enrutamiento de datos, es decir, su ruta a través de la red.

• La capa de transporte: 4ta capa se encarga del transporte de datos, su división en paquetes y la administración de potenciales errores de transmisión.

• La capa de sesión: 5ta capa define el inicio y la finalización de las sesiones de comunicación entre los equipos de la red.

• La capa de presentación: 6ta capa define el formato de los datos que maneja la capa de aplicación (su representación y, potencialmente, su compresión y cifrado) independientemente del sistema.

• La capa de aplicación: La capa le brinda aplicaciones a la interfaz. Por lo tanto, es el nivel más cercano a los usuarios, administrado directamente por el software.

### 2.2.2 TCP/IP: 4 capas

El modelo TCP/IP, influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero sólo contiene cuatro.

Las funciones de las diferentes capas son las siguientes:

• Capa de acceso a la red: específica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.

• Capa de internet: es responsable de proporcionar el paquete de datos (datagrama).

• Capa de transporte: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.

• Capa de aplicación: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP.). (KIOSERA, 2014)

## 2.3 Enrutamiento

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. Un protocolo de enrutamiento es el que define el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento. (PREZI, 2014)

### 2.3.1 Clasificación de algoritmos de enrutamiento

**2.3.2 Algoritmos no adaptables:** No basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico ni en la topología. La desventaja de este tipo de algoritmos es que no es posible responder a situaciones cambiantes como por ejemplo saturación, exceso de tráfico o fallo en una línea, evita la congestión de paquetes en alguna parte de la subred, y como consecuencia el rendimiento de ésta baja. (protenruta.blogspot, 2012)

"Para tomar decisiones de encaminamiento dinámicas, los dispositivos involucrados en el ruteo deben intercambiar información usando algoritmos de encaminamiento especiales." (protenruta.blogspot, 2012)

**2.3.3 Algoritmos adaptables:** Contrarios a los algoritmos no adaptables, éstos cambian sus decisiones de enrutamiento para reflejar los cambios de

topología y de tráfico. Difieren de los algoritmos estáticos en el lugar de obtención de su información por ejemplo localmente, en los routers adyacentes o de todos, el momento del cambio de sus rutas por ejemplo cada Δt seg, o cuando cambia la carga y la métrica usada para la optimización por ejemplo distancia, nº de escalas, tiempo estimado del tránsito.

Este tipo de algoritmos no pueden ser demasiado complejos ya que son implementados en los routers y deben ejecutarse en tiempo real con recursos de CPU y la memoria con que el router dispone. (protenruta.blogspot, 2012)

### 2.3.4 Algoritmos estáticos

#### 2.3.4.1 Enrutamiento por trayectoria más corta

El concepto de trayectoria más corta se debe a que la forma de medir la longitud de la ruta es usando alguna métrica, los cuales podrían ser el número de saltos, la distancia física, el retraso de transmisión por un paquete de prueba, el ancho de banda, el tráfico promedio, el costo de comunicación. Cada nodo se etiqueta con su distancia al nodo de origen a través de la mejor trayectoria conocida. Inicialmente todas las etiquetas son tentativas. Al descubrirse que una etiqueta representa la trayectoria más corta posible del origen a ese nodo, se vuelve permanente y no cambia más. (protenruta.blogspot, 2012)

#### 2.3.4.2 Inundación

Cada paquete de entrada se envía por cada una de las líneas de salida, excepto aquella por la que llegó. Genera grandes cantidades de paquetes duplicados. Se convierten infinitos si no se tiene un control sobre ellos. Inundación selectiva, no se envían paquetes por todas las líneas, sino en las que van en la dirección correcta. (protenruta.blogspot, 2012)

### 2.3.5 Algoritmos dinámicos

#### 2.3.5.1 Enrutamiento vector de distancia

Los algoritmos de enrutamiento por vector de distancia operan haciendo que cada enrutador mantenga una tabla que da la mejor distancia conocida a cada

destino y la línea a usar para llegar ahí. Estas tablas se actualizan intercambiando información con vecinos. Cada enrutador mantiene una tabla de enrutamiento que contiene el registro de la subred y el enrutador de la subred. Esta entrada comprende dos partes: la línea preferida de salida hacia ese destino y una estimación del tiempo o distancia a ese destino. La métrica usada podría ser la cantidad de escalas, el retardo de tiempo en milisegundos, el número total de paquetes en cola por la trayectoria. (protenruta.blogspot, 2012)

"Los protocolos de vector de distancia más nuevos, como EIGRP y RIP-2, introducen el concepto de actualizaciones desencadenadas, una actualización desencadenada es una nueva tabla de enrutamiento que se envía de forma inmediata, en respuesta a un cambio." (protenruta.blogspot, 2012)

Los paquetes que contienen el mensaje de actualización podrían ser descartados o dañados por algún enlace de la red, las actualizaciones desencadenadas no suceden de forma instantánea. Es posible que un router que no haya recibido aún la actualización desencadenada genere una actualización regular que cause que la ruta defectuosa sea insertada en un vecino que hubiese recibido ya la actualización. (protenruta.blogspot, 2012)

#### 2.3.5.2 Enrutamiento por estado de enlace

Se describe en cinco partes. Cada enrutador debe:

- **Descubrir a sus vecinos y conocer sus direcciones de red**

  Al ponerse en operación un enrutador, su primera tarea es averiguar quiénes son sus vecinos; esto se logra enviando un paquete HELLO por cada línea punto a punto. Se espera que el enrutador del otro extremo envíe de regreso su dirección única.

- **Medición del costo de la línea**

  Se mide el tiempo de ida y vuelta que demora el ECHO y lo divide entre dos, el enrutador transmisor puede tener una idea razonable del retardo. Se realizan varias pruebas para promediar y así tener mejor resultado.

- **Construcción de los paquetes de estado de enlace**

  Cada enrutador construye un paquete con todos los datos, este paquete comienza con la identidad del transmisor, seguida de un número de secuencia y una lista de vecinos.

- **Distribución de los paquetes de estado de enlace**

  La parte más complicada del algoritmo es la distribución confiable de los paquetes de estado de enlace. A medida que se distribuyen e instalan los paquetes los enrutadores que reciban los primeros cambiarán sus rutas. En consecuencia, los distintos enrutadores podrían estar usando versiones diferentes de la topología, lo que puede conducir a inconsistencias, ciclos, máquinas inalcanzables, y otros problemas.

- **Cálculo de nuevas rutas**

  Se usa ampliamente en redes actuales, algunos protocolos que lo usan son: el protocolo OSPF, que se emplea cada vez con mayor frecuencia en Internet. (imaginar.org, 2009)

### 2.3.6 Protocolos de enrutamiento: RIP, OSPF, BGP

La función principal es hacer llegar los paquetes de una máquina a otra dando igual cual sea el medio físico que utilicen y los datos que estén transmitiendo, el enrutamiento es justamente eso. Una maquina tiene que conocer que máquinas están es su red y también debe conocer la maquina a la que enviar los paquetes que vallan a maquinas que no estén en su red (router, gateway).

Así se sabrá que debe hacer con cada paquete que quiera enviar. Existen varias formas de enrutar paquetes, el uso de una no excluye de otra, sería muy raro que un paquete que recorre una distancia larga no pasara por todas ellas o por lo menos por las más conocida para tener una idea más clara vamos a conocer algunas formas de enrutamiento. (slideshare.net, 2014)

- **RIP (Routing information protocolo, protocolo de información de enrutado)**

  RIP es un protocolo de enrutado interno, es decir para la parte interna de la red, la que no está conectada al backbone de internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

  Cuando un usuario se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.

  Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino. (licrgarcia.webnode, 2009)

- **OSPF (Open shortest path first, El camino más corto primero)**

  OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a qué distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.

  Así por ejemplo un router que tenga tres conexiones a red, una a una red local en la que hay puesto de trabajo, otra (A) una red rápida frame relay de 48Mbps y una línea (B) RDSI de 64Kbps. Desde la red local va un paquete a W que esta por A, a tres saltos y por B a dos saltos. El paquete iría por B sin tener en cuenta la saturación de la línea o el ancho de banda de la línea.

  La O de OSPF viene de abierto, en este caso significa que los algoritmos que usa son de disposición pública. (licrgarcia.webnode, 2009)

- **BGP (Border gateway protocol, protocolo de la pasarela externa)**

  BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet.
  Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes. para enviar un paquete por una ruta o por otra.

  Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre routers, no utiliza RIP. (licrgarcia.webnode, 2009)

## 2.4 MPLS (Multi-protocol label switching)

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.

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red, entre las principales características tenemos:

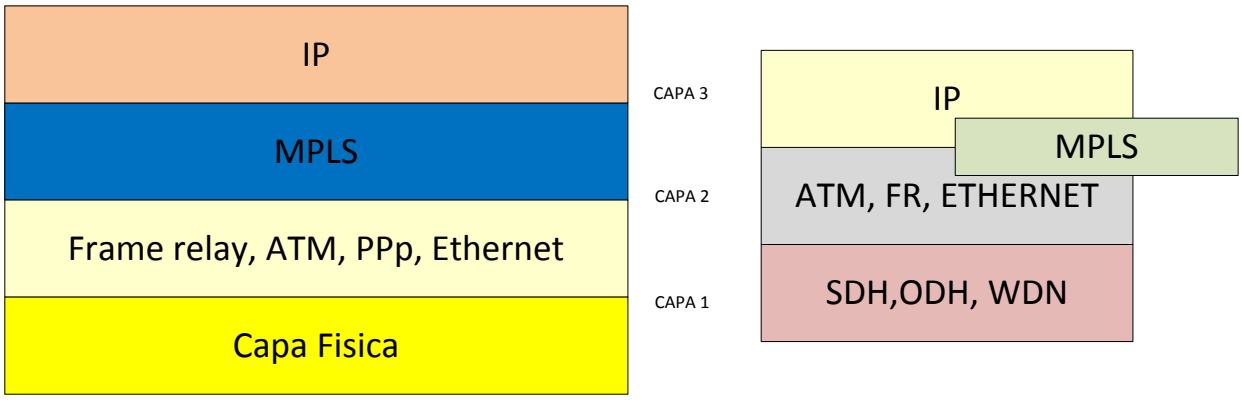
- Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino)
- Las principales aplicaciones de MPLS son:
  - ✓ Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
  - ✓ Policy Routing
  - ✓ Servicios de VPN
  - ✓ Servicios que requieren QoS
- MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).

- 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.
- MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.
- El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, frame relay, líneas dedicadas, LANs. (polartel.es, 2012)

La necesidad de las operadoras de que sus redes tuviesen una cierta calidad de servicio, ha llevado a la búsqueda de una tecnología que ofreciese ese QoS por sí misma. Las tecnologías como ATM o SDH se han quedado obsoletas y aplicar calidad de servicio es una tarea muy complicada. (upcommons.upc.edu, 2011)

Por estas razones surgió MPLS. Definida en el RFC 3031, es una tecnología orientada a paquetes muy flexible. Si la situásemos en el modelo ISO/OSI (International Standard Organization / Open System Interconnection) se encontraría en la capa 2.5 entre la capa de enlace 2 y de red, o sea, entre la capa 2 y 3 como se muestra en la figura 9. El hecho de que se encuentre entre dos capas, le proporciona el nombre de "Multi Protocol". Eso le da la ventaja de poder usar las características de los protocolos de las capas adyacentes sin ninguna restricción. (upcommons.upc.edu, 2011)

Figura 9: Posición de MPLS en el modelo OSI




Fuente: http://upcommons.upc.edu

## 2.5 Conceptos básicos MPLS

MPLS proporciona la posibilidad de administrar el tráfico de una red a través de etiquetas en las cabeceras de los paquetes y a routers específicos capaces de reconocerlas. Principalmente consiste en integrar los niveles de enlace y red eficazmente. Es decir, combina la inteligencia del routing con la velocidad del switching. MPLS usa un esquema de etiquetado de tráfico, marcándolo en la entrada de la red, pero no en su salida. Es usado únicamente en los routers y es independiente del protocolo usado, lo que le permite ser utilizado sobre otros protocolos distintos a IP, como IPX, ATME, PPP, ethernet, frame relay.

Los protocolos de enrutamiento de nivel 3 como OSPF o IS-IS se usan únicamente para funciones de control, ya que las decisiones de enrutamiento se toman en función de la etiqueta MPLS y no de la cabecera IP. (upcommons.upc.edu, 2011)

MPLS mejora la escalabilidad de la red (reduciendo las tablas de enrutamiento) y el retardo de proceso en los routers, combinando algunas prestaciones de las redes orientadas a conexión con la de las redes sin conexión. Así, un router asigna una etiqueta a cada una de las entradas de la tabla de enrutamiento y las distribuye a sus routers vecinos. Luego, cuando se pasan paquetes entre ellos, los routers solo tienen que leer la etiqueta MPLS para identificar el siguiente salto donde enviar el paquete. De esta forma los paquetes fluyen de un extremo a otro de la red sin que los routers tengan que mirar su dirección. (upcommons.upc.edu, 2011)

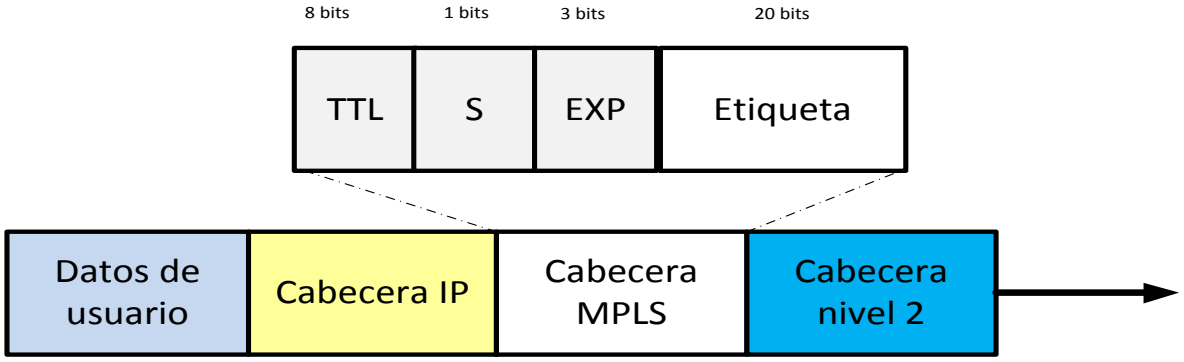
## 2.6 Componentes básicos

### 2.6.1 Label (Etiqueta)

La etiqueta MPLS es un identificador de 20 bits encapsulado dentro de la cabecera MPLS de 32 bits. Esta contiene la información necesaria para enrutar un paquete hasta su destino. Las etiquetas se utilizan en los routers para diferenciar entre los distintos FECs (Forward Equivalance Class) y por lo tanto determinar el siguiente salto donde el paquete debe ser enviado.

Generalmente el valor de la etiqueta se asigna a partir de la dirección IP destino y es local, ya que solo tiene validez entre dos routers vecinos. Por otro lado, un mismo paquete puede ser etiquetado con un valor distinto dependiendo de cuál sea su router de entrada a la red MPLS (LSR). También cabe añadir que un paquete puede disponer de múltiples etiquetas (pila de etiquetas). (upcommons.upc.edu, 2011)

Figura 10: Cabecera MPLS




Fuente: http://upcommons.upc.edu

Como puede observarse en la figura 10, la cabecera MPLS se incluye entre las cabeceras de nivel 2 y 3 y contiene los siguientes campos:

- TTL (Time to live): es un valor que se disminuye cada vez que el paquete es reenviado por un router de la red MPLS (LSR). Cuando el valor es 0, el paquete se descarta. Su función es evitar que un paquete viaje indefinidamente por la red, provocando tráfico innecesario.
- S (Bottom of stack): Si su valor es 1 indica que el paquete solo contiene una etiqueta. Si por el contrario vale 0, significa que el paquete posee una pila de etiquetas.
- EXP (Experimental): Anteriormente era denominado CoS (class of service) pero ahora se considera un campo experimental. Se suele usar para proporcionar QoS.
- Etiqueta (Label): Valor local que usa el router para identificar un FEC en el proceso de forwarding, para determinar el próximo salto del paquete o su encapsulación. (upcommons.upc.edu, 2011)

### 2.6.2 FEC (Forwarding equivalence class)

El FEC es la agrupación de etiquetas que permite la asociación de un conjunto de paquetes sobre el mismo camino y con un destino común.

Todos los paquetes de un mismo FEC se tratan de la misma forma hacia su destino, y cuantos más FECs se obtenga, mayor granularidad para diferenciar entre distintos tipos de flujos. Aunque el hecho de tener más FECs nos afecta en la escalabilidad de la red, y por lo tanto, tendremos que llegar a un compromiso entre el número de FECs y la eficiencia de la red. (upcommons.upc.edu, 2011)

Cada FEC tiene un camino específico a seguir a través de la red MPLS y es independiente en cada router. Puede darse el caso que para una misma dirección IP haya más de un FEC a través del mismo LSP (Label switched path), lo que significa que paquetes con un mismo destino pueden pertenecer a FECs distintos si se tienen que tratar de forma distinta. (upcommons.upc.edu, 2011)

Así, la etiqueta de un determinado paquete representa al FEC al cual pertenece. Los LSR de entrada, que son los que etiquetan a los paquetes, son los encargados de asociar cada paquete a un FEC y se basan principalmente en la dirección destino para hacerlo, aunque también puede depender de otros factores como de la dirección de origen, los puertos de origen y destino, el protocolo o los requerimientos de servicio. Los FECs están diseñados para agrupar a un conjunto de etiquetas, en la práctica lo normal es que cada FEC esté asociado a una única etiqueta. (upcommons.upc.edu, 2011)

### 2.6.3 LSR (Label switched router)

Los LSR son todos aquellos routers que son capaces de usar MPLS. A diferencia de un router convencional, estos routers reenvían los paquetes en función de las etiquetas de los paquetes recibidos, y no en función de la dirección IP de destino. En una red MPLS podemos encontrar dos tipos de LSR:

- Label Edge Router (LER): Los LER son los routers frontera que operan en los bordes de una red MPLS. Estos routers son los encargados de convertir los paquetes IP en paquetes MPLS, o viceversa. Dependiendo de esta función, podemos diferenciar entre los tipos Ingres Edge Router (router de ingreso) y los egress edge router (router de salida). Los primeros se sitúan en la entrada de la red y se encargan de asignar un FEC a los paquetes que reciben y de etiquetarlos para que lleguen a su destino. Los routers de salida son los encargados de hacer la acción contraria, eliminar la etiqueta (label pop). Estos se sitúan al final de la red. (upcommons.upc.edu, 2011)

- Core Router: Estos son los routers que forman el núcleo de la red y permiten el tránsito de los paquetes hacia su destino. Estos routers están capacitados para hacer un label swapping (intercambio de etiquetas), label push y label pop.

### 2.6.4 LSP (Label switched path)

El LSP es el camino compuesto por uno o varios LSR a través del cual se transmiten todos los paquetes pertenecientes a un determinado FEC.

"Estos caminos son unidireccionales (simplex) y solo transmiten hacia un sentido de tráfico. Si queremos que una red sea dúplex, se deben establecer dos LSPs, uno para cada sentido." (upcommons.upc.edu, 2011)

"Los LSPs se pueden diseñar para minimizar el número de saltos de los paquetes, para evitar congestiones en putos críticos de la red, para tener un cierto ancho de banda o simplemente para forzar que el tráfico pase a través de un cierto nodo. (upcommons.upc.edu, 2011) "

MPLS proporciona dos opciones para crear un LSP:

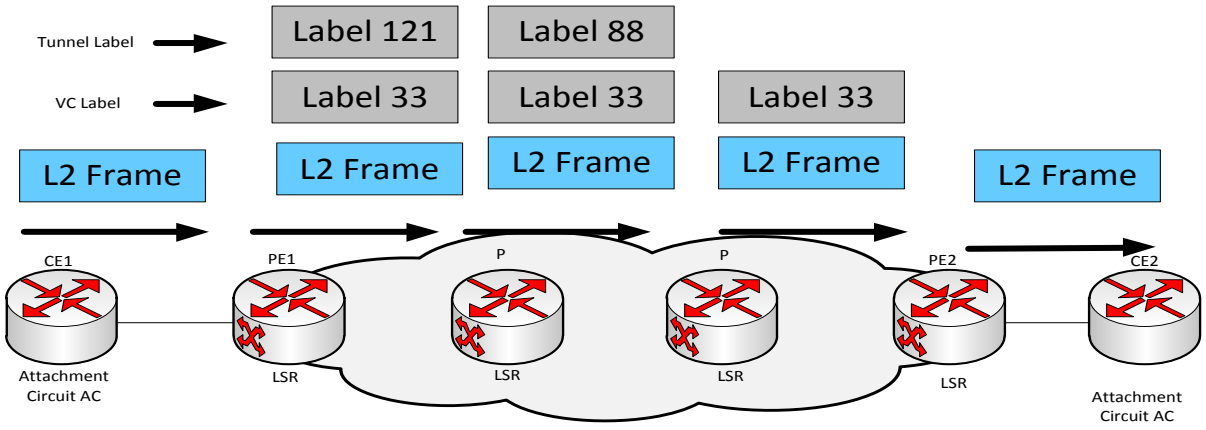
- Punto a punto: Desde el LSR de origen, se especifica punto a punto los saltos que tiene que dar el paquete. No suele ser el LSP más óptimo, pero es el más fácil de gestionar ya que el administrador controla por donde pasa el tráfico.

- Acoplados (merging): El camino escogido por los paquetes es determinado por el protocolo de enrutamiento interno, normalmente OSPF o IS-IS. Este camino puede ir variando si las condiciones de la red cambian. (upcommons.upc.edu, 2011)

### 2.6.5 Label stack (Pila de etiquetas)

Una de las características del protocolo MPLS es que permite apilar diversas etiquetas unas sobre otras. Esto se denomina pila de etiquetas, y consigue tener un LSP dentro de otro. El objetivo de esta técnica es el de crear túneles dentro de los otros LSPs, como se puede observar en la figura 11:

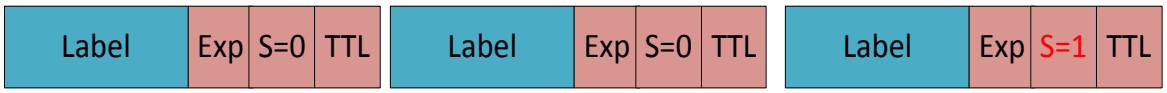
Figura 11: Ejemplo del Label Stack a través de la red




Fuente: http://upcommons.upc.edu

Un LSR en vez de intercambiar etiquetas lo que hace es añadir una etiqueta nueva arriba de la pila. Las etiquetas se añaden siguiendo un sistema LIFO (Last-in, Fisrt-out) y no altera el funcionamiento de enrutado, simplemente el router lee la etiqueta más externa y actúa únicamente en función de ese valor. (upcommons.upc.edu, 2011)

Figura 12: Detalle de una pila de etiqueta




Fuente: http://upcommons.upc.edu

### 2.6.6 LDP (Label distribution protocol)

EL LDP es el protocolo más extendido para la distribución de etiquetas y comunicación de ellas a los LSRs. Está definido que funciona sobre TCP y usa las tablas de enrutamiento IP existentes creadas por el protocolo de enrutamiento, como OSPF, para propagarse a lo largo de la red. El LDP, por un lado, asocia un FEC con cada camino LSP que se crea, y por el otro, intercambia y distribuye esta información de asociación de las etiquetas entre dos LSR vecinos. Esta asociación es bidireccional y permite que un LSR aprenda del otro. (upcommons.upc.edu, 2011)

La distribución de las etiquetas usa uno de los dos siguientes métodos:

- Unsolicited Downstream: En este método, el LSR distribuye su información sobre las etiquetas cuando las tiene disponibles, aunque no se la hayan solicitado.
- Downstream on Demand: Solo se envía información sobre las etiquetas cuando el vecino LSR pide información sobre ella. (upcommons.upc.edu, 2011)

### 2.6.7 Creación y distribución de etiquetas

Antes de que se inicie el tráfico de datos, cada router de ingreso (LER) une ciertas etiquetas con determinados FECs y construye la tabla de etiquetas FER. Una vez completado este proceso, se distribuyen estas uniones usando el protocolo LDP entre los distintos LSRs. Como ya se ha comentado anteriormente, el protocolo LDP usa TCP para comunicar las etiquetas, ya que aporta fiabilidad a la red. Un error en la distribución de las etiquetas resultaría fatal para el funcionamiento de la red. (upcommons.upc.edu, 2011)

### 2.6.8 Creación de la tabla LIB en cada LSR

Cada LSR construye una tabla de etiquetas LIB (Label information base) a medida que va recibiendo las etiquetas con el protocolo LDP. Las tablas LIB es donde se especifica el mapeo de cada etiqueta con un interfaz, tanto de

entrada como de salida. Esta tabla se actualiza cada vez que se efectúa una renegociación de las uniones de etiquetas. (upcommons.upc.edu, 2011)

Figura 13: Ejemplo de Label Information Base


Fuente: http://upcommons.upc.edu

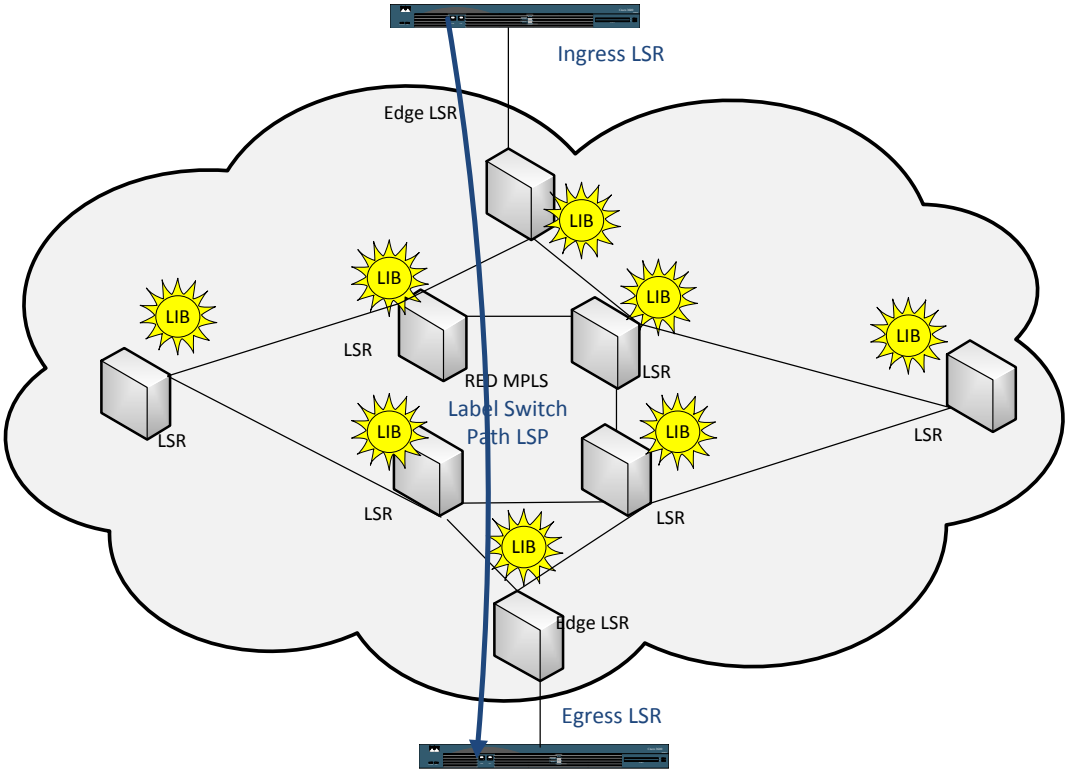
Esta tabla guía al LSR cuando tiene que realizar un intercambio de etiquetas, indicándole a que interfaz tiene que dirigir el paquete. En el ejemplo de la figura 13, un paquete de entrada por la interfaz 2 con la etiqueta 51, se redirigiría a la interfaz 5 con la etiqueta 37. (upcommons.upc.edu, 2011)

### 2.6.9 Creación de los LSPs

La creación de los LSP, los cuales se crean en orden inverso a la trayectoria del paquete. Lo que significa que el LSP se crea en el nodo destino hacia el nodo origen. El nodo origen, al recibir un paquete del cual no tiene etiqueta en la tabla LIB, solicita mediante un paquete request la ruta necesaria. (upcommons.upc.edu, 2011)

Este paquete request se irá propagando hasta llegar al nodo LER de salida. Una vez recibido este paquete, el LER enviará un paquete de mapping en dirección upstream. Este paquete, al pasar por los nodos hacia el nodo origen, irá completando la tabla LIB relacionada con el LSP que se está creando. (upcommons.upc.edu, 2011)

Figura 14: Red MPLS, con un LSP definido




Fuente: http://upcommons.upc.edu

### 2.6.10 Paso de un paquete por la red

Una vez definido los FECs, LDP y etiquetas, queda por analizar el proceso que sigue un paquete al entrar en una red MPLS.

Primero, llega un paquete sin etiquetar a un router LER de ingreso. El router entonces decide a que FEC pertenece y le asigna las etiquetas correspondientes. El proceso de asignar un paquete a un FEC solo se hace una vez, a diferencia de lo que ocurriría con un paquete IP tradicional, que se evalúa en cada nodo.

Una vez el paquete ya está etiquetado, se envía al siguiente salto LSR usando la tabla LIB. Este paquete va saltando de LSR en LSR basándose en la tabla LIB de cada router. Normalmente lo que hacen estos routers es hacer un intercambio de la etiqueta.

Finalmente, el paquete llega el router LER de salida, el cual es el encargado de quitar la última etiqueta y enviar el paquete hacia su destino por routing convencional. En este punto, el paquete ya no es del tipo MPLS porque ya no tiene etiquetas. Este último paso suele realizarlo en penúltimo router de la red (Penultimate Hop Popping). La razón de esto es para liberar al último router del trabajo, ya que este tiene que enrutar un paquete IP y si además tuviera que eliminar la etiqueta, tendría dos trabajos. De esta forma, el penúltimo router de la red MPLS hace un pop en el momento de enviar el paquete al interfaz que le indica la tabla LIB y el último router ya recibe un paquete IP convencional. (upcommons.upc.edu, 2011)

### 2.6.11 Fast reroute

MPLS introduce el mecanismo de Fast reroute para redirigir el tráfico por nuevas rutas no definidas por el protocolo IGP y minimizar el número de paquetes perdidos.

Normalmente, cuando se produce un fallo en un enlace o un nodo, se señaliza en las cabeceras de los LSPs que usan ese enlace o nodo. En ese momento el protocolo IGP recalcula la ruta para redirigir los paquetes. En este tiempo se pueden producir las pérdidas de paquetes, las cuales pueden ser significativas en aplicaciones en tiempo real como la voz o el video. (upcommons.upc.edu, 2011)

El mecanismo, aunque no asegura no tener pérdidas de paquetes, sí que las minimiza. Para usar este mecanismo eficientemente, se tiene que configurar un camino principal por donde se enrutará el tráfico, y simultáneamente implementar un camino de backup para dotar al enlace, o nodo de redundancia. (upcommons.upc.edu, 2011)

"Cuando se detecte un fallo en el enlace principal, fast reroute desviará el tráfico hacia el camino de backup. (upcommons.upc.edu, 2011)"

### 2.6.12 QoS en redes MPLS

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho banda. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridad que otras, sin embargo se garantiza que todas las aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable. . (catarina.udlap.mx, 2006)

QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción de usuario con el sistema y reduce los costos al asignar recursos con mayor eficiencia (bandwidth). Mejora el control sobre la latencia y jitter, por ultimo asegura la transmisión de voz sin interrupciones.
Al configurar políticas de calidad de servicio (QoS) debe existir un ancho de banda adecuado para todas las aplicaciones requeridas. La suma de todo el ancho de banda utilizado en cada aplicación representa el ancho de banda mínimo requerido para cada link utilizado. Esto no debe de consumir más del 75% del ancho de banda total disponible en el enlace. Cuando hay ancho de banda disponible el ruteador no aplicara políticas de servicio. (catarina.udlap.mx, 2006)

El bandwidth debe configurarse en el modo de configuración de la interfaz correspondiente

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 128
Router(config-if)#ip address x.x.x.x.x.x.x.x.x.x.x.x/64
```

### 2.6.13 Arquitecturas para calidad de servicio

Hay dos grandes arquitecturas para QoS:

- Integrated services (IntServ): Se usa para redes pequeñas y medianas, pero no es escalable ya que usa mucha señalización entre los hosts de la red.

- Differenciated services (DiffServ): Es escalable, ya que se basa en una clasificación previa de los paquetes, de forma que se reduce mucho la señalización.

### 2.6.14 Servicios Diferenciados (Diffserv)

El modelo de arquitectura DiffServ permite distinguir diferentes clases de servicio marcando los paquetes.

El tráfico entra en la red, se clasifica y se asigna a un conjunto de comportamiento. Cada uno de estos conjuntos se identifica con un código de punto que se añade a la cabecera del paquete. Luego, estos paquetes son enviados por la red en función de lo que decida cada nodo en referencia a dicho codepoint.

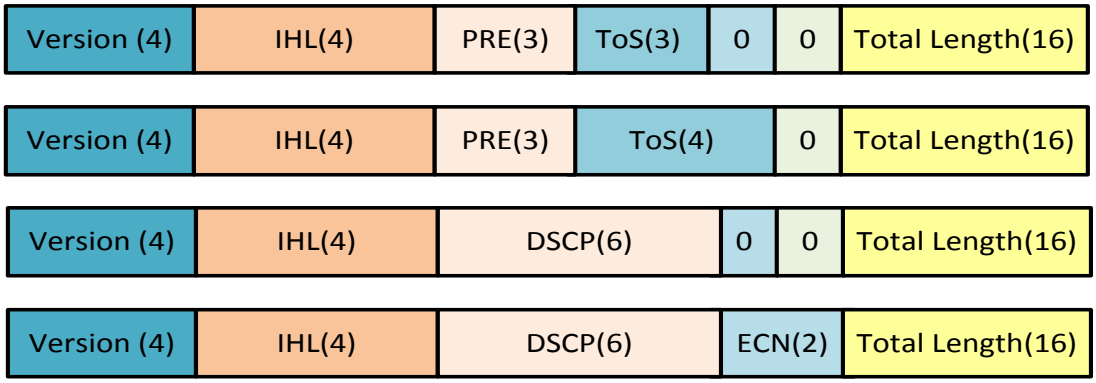
"Según los requisitos de cada usuario, Diffserv permite diferenciar distintos servicios como tráfico web, correo electrónico o transferencia de ficheros, donde el retardo no es muy importante, o servicios como videollamada y VoIP." (upcommons.upc.edu, 2011)

### 2.6.15 Diffserv y paquetes IP

> Diffserv tiene un campo en los encabezados de los paquetes IP conocido como DiffServ CodePoint (DSCP). Los hosts o routers que envían el tráfico a una red diffserv, marcan los paquetes IP con un valor DSCP, y los routers de la red, clasifican estos paquetes en función de dicho valor. Los tráficos con requisitos de QoS parecidos son marcados de igual forma. (upcommons.upc.edu, 2011)

Para proporcionar diferentes niveles de servicio, el campo DSCP consta de 8 bits, estando los dos últimos reservados. Estos 6 bits útiles dan un total de 64 combinaciones distintas para clasificar los paquetes. Los paquetes IP para ofrecer QoS han ido variando. La cabecera IP siempre ha tenido 8 bits destinados a ofrecer este servicio, pero ha ido cambiando tal como se muestra a continuación en la figura 15 con los 4 primeros bytes de la cabecera:

Figura 15: Cabecera IP  8 bits C




Fuente: http://upcommons.upc.edu

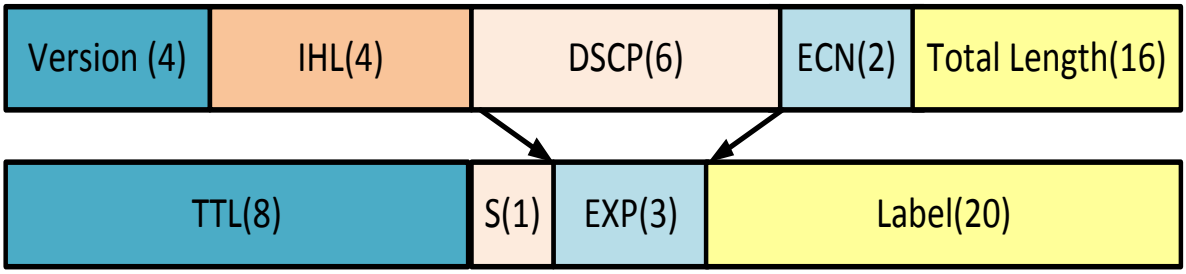
Originalmente en la cabecera existían 3 bits de precedencia (PRE) y 3 bits de tipo de servicio, con 2 bits no utilizados. Los bits de PRE se usaban para tomar decisiones para el tratamiento del paquete y los de ToS se querían usar para marcar los paquetes a los se quiere darle un trato especial. (upcommons.upc.edu, 2011)

### 2.6.16 DiffServ y paquetes MPLS

En la cabecera de los paquetes MPLS, tenemos el campo EXP para controlar el QoS, la cabecera IP tiene 6 bits destinados al DSCP para clasificar los distintos paquetes, pero la cabecera MPLS solo dispone de 3 bits de EXP.

"Por lo tanto se tendrán que mapear las distintas 64 clases en las 8 que permite MPLS. Esto no es un problema, ya que 8 clases de servicio suelen ser más que suficiente." (upcommons.upc.edu, 2011)

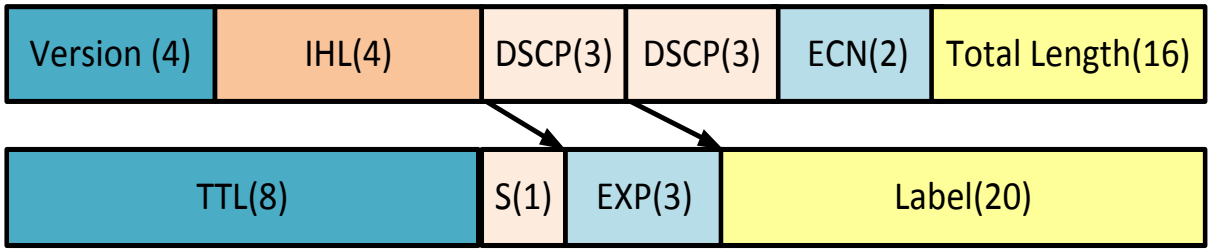
Figura 16: Detalle y relación de las cabeceras IP y MPLS




Fuente: http://upcommons.upc.edu

Por defecto, cuando un paquete llega a la red, el router MPLS de ingreso encapsula el paquete IP con su etiqueta correspondiente y, el campo EXP con los 3 primeros bits del campo DSPC (los 3 bits más significativos). Luego, cuando el paquete MPLS viaja por la red, se va copiando el valor del campo EXP en la etiqueta más externa de la pila de etiquetas. Así pues, el mapeo que se realizará será el siguiente:

Figura 17: Mapeo del campo DSCP en el EXP




Fuente: http://upcommons.upc.edu

"Cabe destacar, que paquetes con distintos DSCP, pero con los 3 primeros bits de este iguales, tendrán el mismo valor de EXP, y por lo tanto serán tratados de igual forma por la red MPLS." (upcommons.upc.edu, 2011)

## 2.7 Funcionamiento del protocolo MPLS

Con el enrutamiento IP los paquetes avanzan de salto en salto a través de la red, es decir que en cada router se encamina el paquete hacia el siguiente salto en función de su dirección IP destino y de la tabla de enrutamiento. En MPLS, los LSR también encaminan los paquetes basándose en la etiqueta de longitud fija, lo que significa que no usan la información de la cabecera IP.

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

etiquetados por MPLS. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). El envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM; en lugar de ello, en MPLS se utiliza el protocolo RSVP. (upcommons.upc.edu, 2011)

## 2.7 Beneficios de MPLS

- **Flexibilidad**

  Cada institución tiene autonomía en el diseño de su Red, es decir diseña su infraestructura interna de acuerdo a sus necesidades y disponibilidad económica.

- **Escalabilidad**

  La escalabilidad ahorra trabajo en el sentido que si se desea montar un nuevo punto en la red sólo será necesario configurar el equipo SP (Service Provider) y no es necesario reconfigurar todos los equipos de la red como se realizaba anteriormente con las redes frame relay y ATM.

- **Accesibilidad**

  La arquitectura MPLS permite utilizar cualquier tipo de tecnología de acceso (XDSL, wíreless ethernet) para lograr establecer una conexión entre el usuario y el proveedor de servicios.

- **Eficiencia**

  En una infraestructura 100% IP, el uso de servicios de transporte ATM o frame relay obligan al usuario a preocuparse por un costo adicional por el overhead que los productos de transporte introducen.

- **Calidad de servicios (Qos) y clases de servicio (Cos)**

  Muchas veces el envío de información de un punto a otro no es necesario que sólo llegue la información sino que algunas veces se requiere cierta prioridad y calidad, lo cual se logra con ciertas técnicas y herramientas de calidad de servicio (QoS) y clases de servicio (CoS) dentro de la red MPLS. 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 video en las redes de datos.

- **Administración**

  La administración para este tipo de redes es transparente para el usuario ya que es gestionado por el SP (Service Provider), esto debido a que está implementado sobre la infraestructura del SP, el cual también se encarga del enrutamiento de los paquetes.

- **Monitorización y SLA's**

  Las redes MPLS requieren de un constante soporte por parte de los SP debido al monitoreo y control permanente, además de proveer algunos tipos de acuerdos de servicios para garantizar y asegurar la estabilidad que el cliente requiere.

- **Fácil migración**

  Debido a que la tecnología MPLS es simple, se puede decir que las actividades de suministro, gestión y mantenimiento son sencillas para el SP, lo cual favorece directamente al usuario.

- **Seguridad**

  Los niveles de seguridad proporcionados por una red MPLS son muy similares a los entregados por los Circuitos Virtuales de Frame Relay y ATM, aunque en algunos casos puede obtener características como lo son encriptación y autenticación generando así mayor seguridad.

  Garantizar la seguridad de la información se convierte en una tarea cada vez más compleja. Al migrar a una nueva infraestructura de red hay que garantizar que no aumenten las amenazas de las redes y los sistemas. Con el desarrollado de MPLS se resuelven algunas de las debilidades potenciales que plantea la seguridad del protocolo IP. Cuando se habla de la seguridad en las redes MPLS no se puede ver como un elemento aislado, sino como un complemento de las redes de telecomunicaciones.

  Para la seguridad de redes MPLS se definen ocho dimensiones de seguridad que se tienen en cuenta ante la necesidad de elaborar e implementar las políticas y medidas de seguridad incluyendo la red de núcleo MPLS. Estas dimensiones son:

- control de acceso
- autenticación
- no repudio
- confidencialidad de datos
- seguridad de la comunicación
- integridad de los datos
- disponibilidad
- privacidad

Para MPLS también hay puntos peligrosos, por donde los intrusos tienen alguna posibilidad de entrar. Las amenazas son prácticamente las mismas en todas las redes. Las amenazas actuales a la seguridad de estas redes pueden dividirse en tres categorías.

Amenazas intrusivas como la denegación de servicio (DoS, Denial of Service), donde un atacante hace caer la red, a menudo sobrecargado un elemento clave, como son los servidores de DNS ( Domain Name System), los encaminadores, entre otros.

Ataques con virus que no solo pueden desactivar algunas instalaciones informáticas sino que pueden corromper permanentemente sus bases de datos.

La escucha ilegal, que permite a terceros obtener accesos a datos privilegiados de gran valor. Para la configuración de seguridad en redes MPLS, se deberá configurar las contraseñas de los dispositivos de la red como son, contraseña en modo privilegiado, contraseña para el acceso a telnet, contraseña para la interface, y si se desea tener mayor control de acceso de deberá implementar configuraciones de acces list que permiten negar o accede algún servicio de la red.

También tenemos la configuración para denegar o acceso de tráfico.

Router(config)# access-list 10 permit tcp any eq www any
(limitamos el trafico Web saliente)
Router(config)# access-list 11 permit tcp any any eq smtp
(limitamos el trafico smtp entrante)

Router(config)# access-list 12 permit tcp any eq smtp any
(limitamos el trafico smtp saliente)

- **Ahorro**

  La implementación de una Red MPLS respecto a los costos se puede decir que tiene varios puntos a favor, entre ellos tenemos: los equipos del cliente no requieren de un equipo específico ni con características técnicas complejas.
  Este costo también se refleja en la convergencia de servicios, es decir, que la integración de varios servicios en una misma plataforma.

  MPLS frente a otro protocolo como BGP, MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS). 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, las principales ventajas de esta red son:

- **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 rRelay 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 clave mediante múltiples conexiones redundantes a la nube MPLS y, a través de ella, a otros sitios de la red. (TIC TAC, 2014)

**BGP**

Es un vector de enrutamiento por vector de distancia usado comúnmente para enrurar paquetes entre dominios estándar en internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados sistemas autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios.
Sus características son:

- BGP utiliza un vector de caminos (path vector).
- Determina el orden de prioridad a cada ruta
- Divide el internet en sistemas autónomos.
- A cada SA (AS) se le asigna un número cuando va a participar en el internet. También existen números privados.
- Regularmente utilizado cuando se tiene más de una conexión hacia fuera de nuestra red.
- Permite tomar una mejor decisión sobre la ruta que los datagramas deben de enviarse/recibirse.
- Agrupa prefijos internos y los anuncia a los SA vecinos.

A continuación se dará a conocer un cuadro comparativo de MPLS y otras tecnologías, ver tabla 9. (sites.google.com, 2014)

Tabla 9: Ventajas de MPLS frente a otras tecnologías

| Tecnologia | VENTAJAS | DESVENTAJAS |
|---|---|---|
| MPLS | Mecanismo para manejar el flujo de tráfico de tamaños variados (Flow anagement)<br><br>Es independiente de protocolos de capa 2 y 3<br><br>Soporta QoS, escalabilidad de la red, reenvio de paquetes<br><br>Interconecta a protocolos de existentes (RSVP, OSPF)<br><br>Soporta ATM, Frame-Relay y Ethernet | Se agrega una capa adicional<br><br>Los router deben entender MPLS |
| ATM | Orientada a Conexión<br>- Provee QoS<br><br>"Switcheo" rápido de paquetes con paquetes (celdas) de largo fijo<br><br>Integración de diferentes tipos de tráfico (voz, datos, video) | Complejo<br><br>Caro<br><br>No ampliamente adoptado |
| FRAME RELAY | Puede ser implementado en software (por ejemplo en un encaminador), y por tanto puede ser mucho más barato.<br><br>Está orientado a conexiones, como la mayoría de las WAN's.<br><br>Flexibilidad del servicio: Frame Relay es la solución adaptable a las necesidades cambiantes | Sólo ha sido definido para velocidades de hasta 1,544/2,048 Mbps.<br><br>No soporta aplicaciones sensibles al tiempo, al menos de forma estándar.<br><br>No garantiza la entrega de los datos, retardos variables no es adecuada para enviar datos sensibles a retardos como vídeo audio de tiempo real. |

Elaborado por: Rolando Reyes

## 2.9 Routers

Router también conocido como, enrutador, ruteador o encaminador de paquetes es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.
Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador, y que por tanto tienen prefijos de red distintos.

Permiten interconectar tanto redes de área local como redes de área extensa, proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red.

Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas.

Los routers operan a un nivel mayor lo que los hace ser capaces de procesar una mayor cantidad de información. Sin embargo, requiere más procesador, lo que también los hará más caros.

A diferencia de los switches y bridges, que sólo leen la dirección MAC, los routers analizan la información contenida en un paquete de red leyendo la dirección de red. Los routers leen cada paquete y lo envían a través del camino más eficiente posible al destino apropiado, según una serie de reglas recogidas en sus tablas.

Los routers se utilizan a menudo para conectar redes geográficamente separadas usando tecnologías WAN de relativa baja velocidad, como ISDN, una línea T1, Frame Relay. El router es entonces la conexión vital entre una red y el resto de las redes.

Un router también sabe cuándo mantener el tráfico de la red local dentro de ésta y cuándo conectarlo con otras LANs, es decir, permite filtrar los broadcasts de nivel de enlace. Esto es bueno, por ejemplo, si un router realiza una conexión WAN, así el

tráfico de broadcast de nivel dos no es ruteado por el enlace WAN y se mantiene sólo en la red local.

“Eso es especialmente importante en conexiones conmutadas como RDSI. Un router dispondrá de una o más interfaces de red local, las que le servirán para conectar múltiples redes locales usando protocolos de nivel de red. Eventualmente, también podrá tener una o más interfaces para soportar cualquier conexión WAN.” (SEMANTIX, 2014)

Figura 18: Router


Fuente: http://www.networkhardware.com.es

### 2.9.2 Tipos de enrutadores

- **Acceso**

  Los routers de acceso, incluyendo SOHO, se encuentran en sitios de clientes como sucursales que no necesitan de enrutamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo

- **Distribución**

  Los routers de distribución agregan tráfico desde routers de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa.

Los routers de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN, y transformación sustancial de inteligencia. También pueden proporcionar conectividad a los grupos de servidores o redes externas.

En la última solicitud, el sistema de funcionamiento del router debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del router puede estar un cortafuegos o VPN concentrador, o el router puede incluir estas y otras funciones de seguridad.

Cuando una empresa se basa principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

- **Núcleo**

Interconecta la distribución de los niveles de los routers de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.
Cuando una empresa está ampliamente distribuida sin ubicación central, la función del core router puede ser asumido por el servicio de WAN al que se suscribe la empresa, y la distribución de routers se convierte en el nivel más alto.

- **Borde**

Los routers de borde enlazan sistemas autónomos con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo BGP y si quieren recibir las rutas BGP, deben poseer una gran cantidad de memoria. (coliicho.jimdo.com, 2014)

# CAPÍTULO 3

# INFRAESTRUCTURA RED MPLS

## 3.1 Infraestructura de una red

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 conocido como DWDM, 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 mecanismos de encapsulamiento. (ramonmillan.com, 2014)

La implementación de MPLS como una solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IP 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 cómo 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. (ramonmillan.com, 2014)

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. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6. (ramonmillan.com, 2014)

La implementación de MPLS como una solución IP sobre ATM también está muy extendida. MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. La aparición de switches ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM 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. (ramonmillan.com, 2014)

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 routers son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. (ramonmillan.com, 2014)

Los beneficios que MPLS proporciona 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.
>
> 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. MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes. (ramonmillan.com, 2014)

A continuación se conocerá las características de los elementos de infraestructura para una red.

### 3.2 Gabinetes o racks

"Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios." (sistemasencomunicaciones.blogspot.com, 2013)

> Externamente, los racks para montaje de servidores tienen una anchura estándar de 600 mm y un fondo de 600, 800, 900, 1000 y ahora incluso 1200mm. La anchura de 600 mm para racks de servidores coincide con el tamaño estándar de las losetas o techos en los centros de datos. De esta manera es muy sencillo hacer distribuciones de espacios en centros de datos (CPD). Para el cableado de datos se utilizan también racks de 800 mm de ancho, cuando es necesario disponer de suficiente espacio lateral para el guiado de cables. (PREZI, 2014)

Los racks son útiles en un centro de proceso de datos, donde el espacio es escaso y se necesita alojar un gran número de dispositivos.

### 3.2.1 Características gabinete o rack

- Solución total desarrollada a nivel gabinete que cubre los requerimientos de administración de cables y manejo térmico.
- (39.5” 81003mm) de ancho x 48.9” (1242mm) de fondo, que ofrece las salidas requeridas por el chasis, según las especificaciones de cada equipo.
- Gabinete de 39.5” de ancho con ducto de entrada y salida que permite el adecuado flujo de aire para aplicaciones pasillo caliente / pasillo frío.
- Prueba de validación térmica preliminar en el laboratorio térmico y prueba de validación térmica final.
- Escenarios de cableado desarrollados y bosquejados.

Figura 19: Rack vista frontal

Fuente: http://dosdigitos.com/telecomunicaciones/

## 3.3 Fibra óptica

La fibra óptica es una delgada hebra de vidrio o silicio fundido que conduce la luz. Se requieren dos filamentos para una comunicación bidireccional: TX y RX.

El grosor del filamento es comparable al grosor de un cabello humano, es decir, aproximadamente de 0,1 mm. En cada filamento de fibra óptica se pude apreciar 3 componentes:

- La fuente de luz: LED o laser.
- El medio transmisor: fibra óptica.
- El detector de luz: fotodiodo.

Un cable de fibra óptica está compuesto por: Núcleo, manto, recubrimiento, tensores y chaqueta.

Convencionalmente, un pulso de luz indica un bit 1 y la ausencia de luz indica un bit 0. El detector genera un pulso eléctrico cuando la luz incide en él. Éste sistema de transmisión tendría fugas de luz y sería inútil en la práctica excepto por un principio interesante de la física. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta (se dobla) entre las fronteras de los medios.

> El grado de refracción depende de las propiedades de los dos medios (en particular, de sus índices de refracción). Para ángulos de incidencia por encima de cierto valor crítico, la luz se refracta de regreso; ninguna función escapa hacia el otro medio, de esta forma el rayo queda atrapado dentro de la fibra y se puede propagar por muchos kilómetros virtualmente con poca pérdida. (neo.lcc.uma.es, 2013)
>
> La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un led. (ECUARED, 2014)
>
> Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional. Son el medio de transmisión por excelencia al ser inmune a las interferencias

electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión, como se muestra en la figura 20. (ECUARED, 2014)

Figura 20: Fibra Óptica

Fuente: http://www.panduit.com/

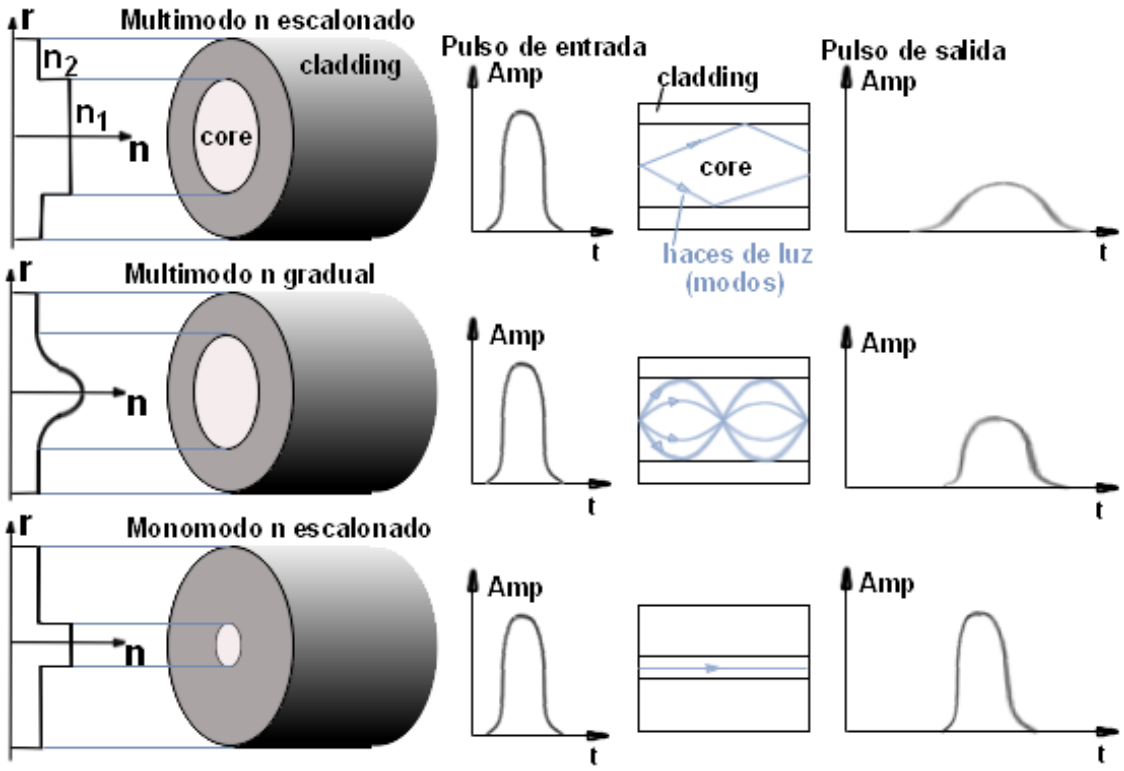
### 3.3.1 Tipos de fibra

- Monomodo.- Sólo se propagan los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo, en concreto un ancho de banda de hasta 50 GHz. Este tipo de fibras necesitan el empleo de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa. Resultan más caras de producir y el equipamiento es más sofisticado. Puede operar con velocidades de hasta los 622 Mbps y tiene un alcance de transmisión de hasta 100 Km. (www.uazuay.edu.ec, 2013)

- Multimodo.- Se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo. Las fibras multimodo son las más utilizadas en las redes locales por su bajo coste. Los diámetros más frecuentes 62,5/125 y 100/140 micras. Las distancias de transmisión de este tipo de fibras están alrededor de los 2,4 kms y se utilizan a diferentes velocidades: 10 Mbps, 16 Mbps, 100 Mbps y 155 Mbps, en la figura 21 se

observara de una manera clara las diferencias entre fibra óptica monomodo y multimodo. (www.uazuay.edu.ec, 2013)

Figura 21: Fibra monomodo y multimodo




Fuente: http://www.yio.com.ar/

### 3.3.2 Tipos de Conectores

- **ST.-** Los conectores ST fueron creados en los años 80 por AT&T y deriva del inglés “Straight Tip”, tienen un diseño tipo bayoneta que permite alinear el conector de manera sencilla al adaptador. Su mecanismo de acoplamiento tipo “Empuja y Gira” asegura que el conector no tenga deslizamientos y desconexiones. El cuerpo del conector sujeta la férula, ofreciendo una mejor alineación y previniendo movimientos rotatorios como se muestra en la figura 22. El ST ha sido el conector más popular en las redes de área local (LAN). (FIBREMEX, 2014)

Figura 22: Conector ST

Fuente: http://visiontelematica.wordpress.com/

- **SC.-** Los conectores SC, tienen un diseño versátil que permite alinear el conector de manera sencilla al adaptador como se muestra en la figura 23. Su mecanismo de acoplamiento tipo "Push Pull" lo asegura al adaptador de manera sencilla. El cuerpo del conector sujeta la férula, ofreciendo una mejor alineación y previniendo movimientos. El conector SC es el más popular tanto en LAN como en redes de transporte: operadoras telefonías, CATV. (FIBREMEX, 2014)

Figura 23: Conector SC

Fuente: http://visiontelematica.wordpress.com/

- **FC.-** Los conectores FC fueron creados en los años 80 por NTT por su nombre en inglés "Fiber Connection", tienen un diseño versátil tipo rosca que permite asegurar y alinear el conector de manera firme en el adaptador. Su mecanismo de acoplamiento tipo Rosca asegura que el conector no tenga deslizamientos o desconexiones. El cuerpo del conector sujeta el núcleo, ofreciendo una mejor alineación y previniendo movimientos, como se observa en la figura 24. (FIBREMEX, 2014)

Figura 24: Conector FC

Fuente: http://visiontelematica.wordpress.com/

- **LC.-** Desarrollados en 1997 por Lucent Technologies, los conectores LC tienen un aspecto exterior similar a un pequeño SC, con el tamaño de un RJ 45 y se presentan en formato simplex o dúplex, diferenciándose externamente los de tipo SM de los de tipo MM por un código de colores. El LC es un conector de alta densidad SFF diseñado para su uso en todo tipo de entornos: LAN como se observa en la figura 25, operadoras de telefonías, CATV. (FIBREMEX, 2014)

Figura 25: Conector LC

Fuente: http://visiontelematica.wordpress.com/

- **MU.-** El conector MU, cuenta con un mecanismo de fijación de tipo Push Pull cuando es empujado hacia adentro o jalado hacia afuera, como se observa en la figura 26. Este diseño previene el desalineamiento rotatorio. El conector ofrece un cuerpo pre montado y una cubierta plástica de moldeada precisión, y una férula libre de flotación que mide 1,25 mm de diámetro, sostenido con un resorte a presión. Las partes de los conectores son: férula (cilindro que rodea la fibra a manera de PIN), cuerpo (es la base del

conector), ojillo de crimpado (es el que sujeta la fibra al conector), bota (es el mango del conector). (FIBREMEX, 2014)

Figura 26: Conector MU

Fuente: http://visiontelematica.wordpress.com/

- **MTRJ.-** El conector MT-RJ, cuenta con un mecanismo es de tipo Push Pull cuando es empujado hacia adentro o jalado hacia afuera. Este diseño previene el desalineamiento rotatorio. En los conectores MT-RJ se utilizan dos fibras dentro de una misma férula, las férulas son fabricadas en procesos de molde de alta precisión.

  MTRJ son versátiles debido a que en un solo conector es posible conectorizar dos fibras al mismo tiempo. Los conectores se alinean de manera sencilla y se asegura en el adaptador para evitar desconexiones como se observa en la figura 27. (tecnicoteleco.hol.es, 2014)

Figura 27: Conector MTRJ

Fuente: http://visiontelematica.wordpress.com/

- **MTP.-** El conector MTP permite ahorrar espacio mediante el suministro de al menos doce posibles conexiones con una sola férula, en sustitución de hasta

un máximo de doce conectores de fibra óptica. Los conectores MTP proporcionan una interfaz intuitiva Push-Pull, mecanismo de enclavamiento para una fácil inserción, como se observa en la figura 28.

La mayoría de los usos son para rendimientos de procesamientos más altos que la tecnología estándar de la fibra no pueda manejar. Ofrecen una forma segura de terminar varias fibras en un diseño compacto. (tecnicoteleco.hol.es, 2014)

Figura 28: Conector MTP

Fuente: http:// www.fiberstore.com.mx/

### 3.4 Fiber runner

Es un sistema de enrutamiento, FiberRunner se compone de diversos canales de distribución y los accesorios a su ruta de fibra óptica y un alto rendimiento a través de un centro de datos, en la figura 29 se puede observar el montaje de fiber runner. Están diseñados para segregar, para encaminar y para proteger del rendimiento óptico de fibra el cableado de cobre y alto. Se adaptan para los usos del centro de datos donde el cable se encamina de áreas de distribución a los gabinetes o a los estantes del equipo. Se utilizan para encaminar los cables de puente ópticos de fibra entre los marcos de distribución de la fibra y las bajantes de equipo. Pueden ser desplegados sobre los estantes o en usos inferiores aprobados del piso.

Figura 29: Fiber Runner

Fuente: http://www.panduit.com/

Fiber runner como elemento de infraestructura normalmente se utiliza junto con bastidores y gabinetes en las salas de equipos, data centers, para distribuir, segregar y proteger cables, este sistema cuenta con accesorios ilimitados para obtener un tendido de cables seguro y eficaz en las salas de equipos. Fiber runner está compuesto de tuberías de policloruro de vinilo rígido, el fiber runner muestra un aspecto robusto, sin embargo, los acopladores y el diseño de soportes le permiten hacer una conexión mecánicamente segura en menos tiempo, ahorrando tiempo y dinero.

Figura 30: Fiber Runner en data centers

Fuente: http://www.panduit.com/

### 3.5 Manguera corrugada

Este tipo de elemento de infraestructura en muy útil para alojar y proteger cables de fibra óptica en encofrados, data centers, lozas de cemento o bajo tierra, en muros y sobre cielos falsos.

Conduce el cableado de instalaciones eléctricas, de fibra óptica, 100% flexible, por su construcción en forma de anillos, soporta giros de 360° en espacios cortos y limitados sin que se obstruya o colapse, es muy resistente a la humedad, durable y económico, de rápida instalación y fácil manejo en pisos, techos y paredes.

Figura 31: Manguera Corrugada

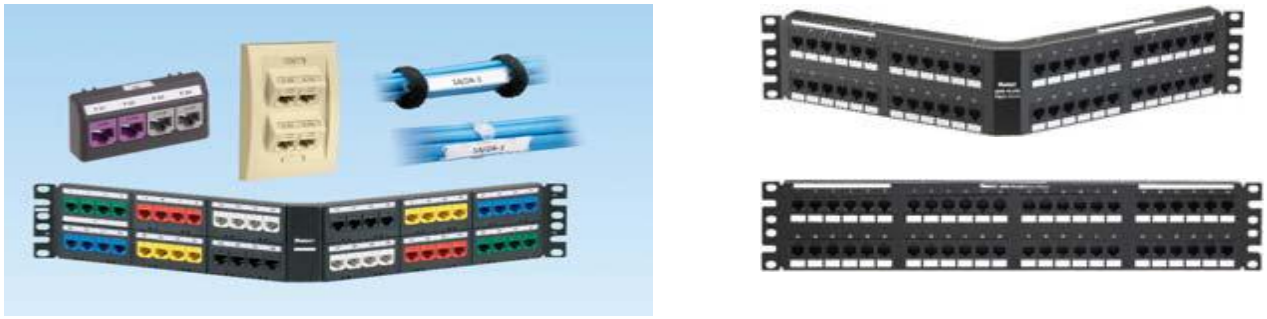
Fuente: http://www.lisoflexhg.com/

### 3.6 Patch panels

Un panel de conexiones, también denominado bahía de rutas o patch panel, es el elemento encargado de recibir todos los cables del cableado estructurado. Sirve como un organizador de las conexiones de la red, para que los elementos relacionados de la Red LAN y los equipos de la conectividad puedan ser fácilmente incorporados al sistema y además los puertos de conexión de los equipos activos de la red (Switch, Router.) no tengan algún daño por el constante trabajo de retirar e introducir en sus puertos. Los patch panels permiten hacer cambios de forma rápida y sencilla conectando y desconectando los cables de patcheo. Esta manipulación de los cables se hará habitualmente en la parte frontal, mientras que la parte de atrás del panel tendrá los cables más permanentes y que van directamente a los equipos

centrales (Switches, Routers, concentradores.). (manejoredesg.blogspot.com, 2013)

Figura 32: Patch Panel



Fuente: http://www.panduit.com/

### 3.7 Cableado de cobre

Es un cable de pares trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente, o incluso impidiendo, la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios. Como el nombre lo indica, "unshielded twisted pair" (UTP), es un cable que no tiene revestimiento o blindaje entre la cubierta exterior y los cables. El UTP se utiliza comúnmente para aplicaciones de redes ethernet, el término UTP generalmente se refiere a los cables categoría 3, 4 y 5 especificados por el estándar TIA/EIA 568-A standard. (diferentesponchados.weebly.com, 2014)

Los tipos de cable UTP son:

- Categoría 1: Utilizado para voz solamente
- Categoría 2: Datos 4 Mbps
- Categoría 3: UTP con impedancia de 100 ohm y carácter ísiticas eléctricas que soportan frecuencias de transmisión de hasta 16 MHz. Definida por la especificación TIA/EIA 568-A specification

- Categoría 4: UTP con impedancia de 100 ohm y carácter rísiticas eléctricas que soportan frecuencias de transmisión de hasta 20 MHz. Definida por la especificación TIA/EIA 568-A.
- Categoría 5: UTP con 100 ohm de impedancia y características eléctricas que soportan frecuencias de transmisión de hasta 100 MHz. Definida por la especificación TIA/EIA 568-A specification. El cable debe ser probado para asegurar que cumple con las especificaciones de la categoría 5e (CAT 5 enhanced "mejorada"). CAT 5e es un nuevo estándar que soportará velocidades aún mayores de 100 Mbps y consiste de un cable par trenzado.
- Categoria 6: La categoría 6 posee características y especificaciones para la diafonía o crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps.
- Categoria 7: La categoría 7 posee especificaciones aún más estrictas para diafonía y ruido en el sistema que Cat 6. Para lograr esto, el blindaje ha sido agregado a cada par de cable individualmente y para el cable entero. El estándar Cat 7 fue creado para permitir 10 Gigabit Ethernet sobre 100 metros de cableado de cobre.

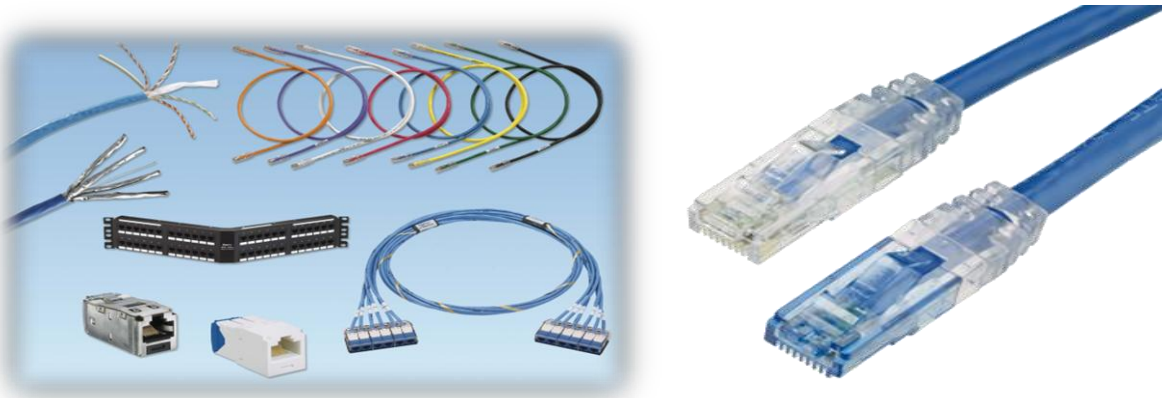
  El cable contiene, como los estándares anteriores, 4 pares trenzados de cobre. Cat 7 puede ser terminado tanto con un conector eléctrico GG-45o GigaGate-45 compatible con RJ-45. Cuando se combina con éstos, el Cat 7 puede transmitir frecuencias de hasta 600 MHz. (diferentesponchados.weebly.com, 2014)

Figura 33: Cable UTP

Fuente: http://spanish.adp-lancable.com

Conector RJ 45. - Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo de registered jack que a su vez es parte del código federal de regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. (WIKISPACES, 2014)

Figura 34: Conector y Cable UTP



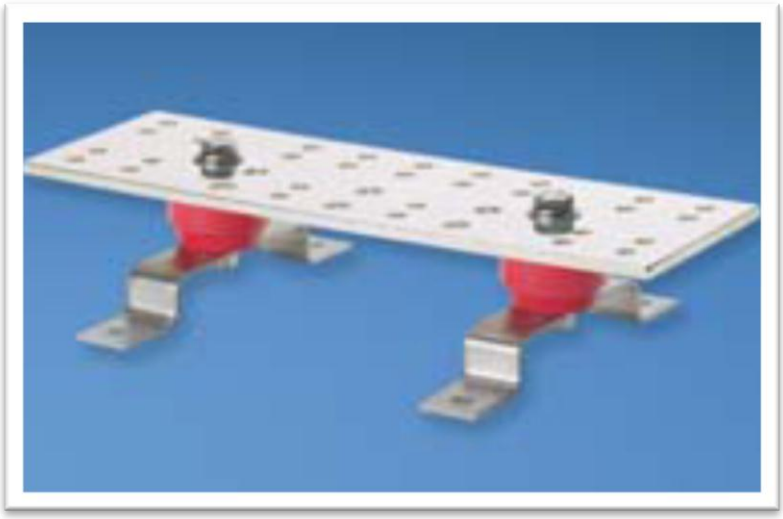
Fuente: http://www.panduit.com/

### 3.8 Sistema de tierra

Los aterramientos para los sistemas de telecomunicaciones parten del aterramiento principal del centro de telecomunicaciones (aterramiento eléctrico, jabalinas.). Desde este punto, se debe tender un conductor de tierra para telecomunicaciones hasta la "Barra principal de tierra para telecomunicaciones" (TMGB = "Telecomunications Main Grounding Busbar"). Este conductor de tierra debe estar forrado, preferentemente de color verde, y debe tener una sección mínima de 6. Asimismo, debe estar correctamente identificado mediante etiquetas adecuadas. En la sala de equipos y en cada sala de telecomunicaciones debe ubicarse una "Barra de tierra para telecomunicaciones" (TGB= "Telecommunications Grounding Busbar".

Esta barra de tierra es el punto central de conexión para las tierras de los equipos de telecomunicaciones ubicadas en la sala de equipos o sala de telecomunicaciones como se muestra en la figura 35.

Figura 35: TGB



Fuente: http://www.mostradorvirtual.mx/

El cálculo de la resistencia de un cable para el sistema eléctrico es importante para el uso de los equipos en las salas de telecomunicaciones.

La unidad de resistencia de un cable se la mide en ohmio (W o Ω): y ohmio es la resistencia que ofrece un conductor cuando por él circula un amperio (intensidad) y entre sus extremos hay una diferencia de potencial (tensión) de un voltio.

Físicamente, cualquier dispositivo o material intercalado en un circuito eléctrico representa en sí una resistencia para la circulación de la corriente eléctrica, y dependiendo de las características de dicho dispositivo o material se puede aumentar o disminuir la resistencia a una corriente eléctrica. Por lo tanto, la resistencia eléctrica de un conductor depende de la naturaleza del material, de su longitud y de su sección, además de la temperatura.

A mayor longitud, mayor resistencia. A mayor sección, menos resistencia. A mayor temperatura, mayor resistencia. Para calcular el valor de la resistencia que ofrece un material específico, con largo y grosor definidos, se aplica a fórmula

$$R = \mathrm{p}.\frac{\mathrm{L}}{S}$$

Resistencia (R) es igual al producto de rho (ρ) por la longitud (L) del conductor dividido o partido por la sección o grosor (área) (S) del conductor.

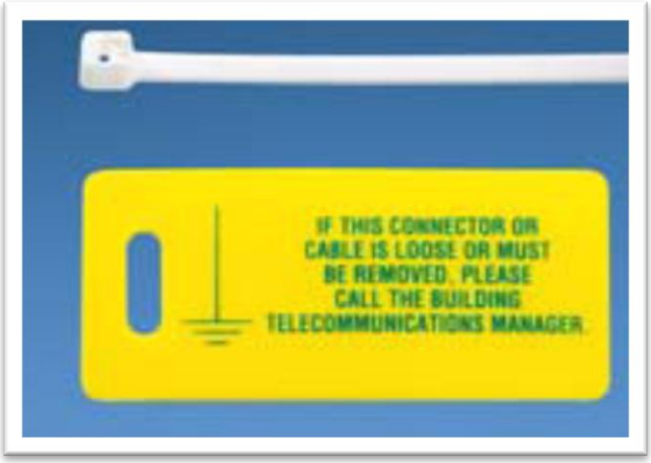
ρ (rho) es una constante (conocida y que depende del material), llamada resistividad.

L, es el largo o longitud (en metros) del cable o conductor, y S, es la sección o grosor (en $mm^2$) del cable o conductor

### 3.8.1 Etiquetas tierra

Las etiquetas de tierra según las normas de cableado estructurado ANSI/TIA/EIA-568 son de color amarillo como se muestra en la figura 36, y deben ir en todos los puntos de aterrizaje a tierra de la sala de telecomunicaciones.

Figura 36: Etiquetas de tierra




Fuente: http://www.panduit.com/

### 3.9 Etiquetas de patch cords, escalerillas, gabinetes

Las etiquetas están diseñadas en una línea completa de productos para el marcado, y la identificación de una manera rápida y ordenada de cualquier tipo de cable sea este de fibra o cobre, gabinetes, canastillas, la etiquetación en una red sirve para ayudar con el cumplimiento de la norma TIA/EIA-606-B, se observa en la figura 37 que se debe tener varios tipos de etiquetas como son las blancas que son para la identificación de los cables de fibra y cobre, y las amarillas para la canalización de la fibra óptica y cobre.

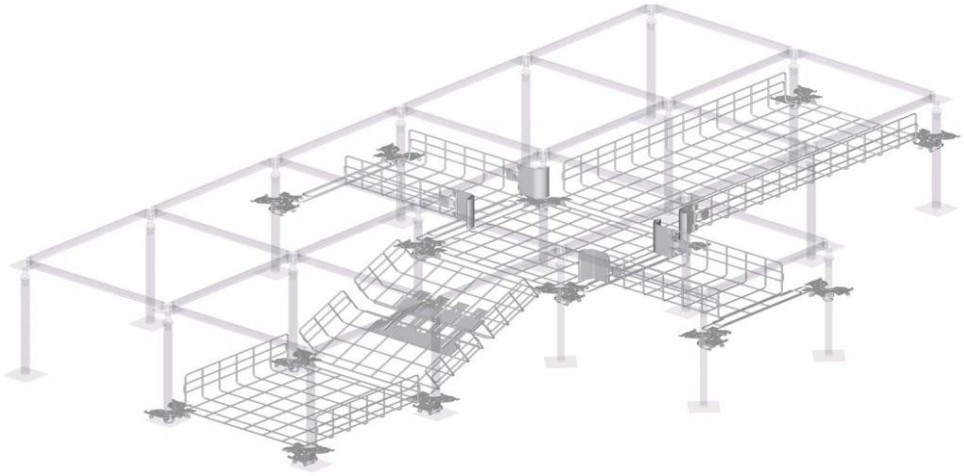
Figura 37: Tipos de etiquetas

Fuente: http://www.panduit.com/

### 3.10 Canalización de cobre

Las canalizaciones de cobre es aquella que vinculan las salas de telecomunicaciones con las áreas de trabajo. Estas canalizaciones deben ser diseñadas para soportar los tipos de cables recomendados en la norma TIA-568, entre los que se incluyen el cable UTP de 4 pares, el cable STP y la fibra óptica, para cumplir con esta norma se utiliza canastillas de 12 pulgadas por 3 metros como se muestra en la figura 38.

Figura 38: Canalización de cable eléctrico y cobre



.

Fuente: http://iie.fing.edu.uy/

### 3.11 Terminales de conexión

Un terminal es el punto en que un conductor de un componente eléctrico, dispositivo o red llega a su fin y proporciona un punto de conexión de circuitos externos. El terminal puede ser simplemente el final de un cable o puede estar equipado con un conector o tornillo. En teoría de circuitos, terminal significa punto donde teóricamente se pueden hacer conexiones a una red. No se refiere necesariamente a ningún objeto físico real. La conexión puede ser temporal, como para equipos portátiles, o temporal para equipos de telecomunicaciones, puede exigir una herramienta para montaje y desmontaje, o puede ser una unión permanente entre dos cables o dos aparatos.

#### 3.11.1 Tipos de terminales

Los conectores eléctricos se utilizan para conducir la corriente entre dos dispositivos, para facilitar el suministro de energía y de distribución, tales como conexiones entre cables de energía eléctrica. Estos terminales están aislados con caucho o plástico como medida de seguridad debido a la alta tensión. Los terminales de compresión se utilizan cuando el dispositivo que está conectado usará altas tensiones que necesitan una forma segura de conexión eléctrica. Otros usos incluyen conectar un cable a otro o varios cables, conectando aparatos eléctricos, tomas de corriente, fusibles o interruptores de carga y conexiones de cables o líneas eléctricas aéreas, los tipos de terminales dependen del espesor del cable y donde se vaya a realizar la conexión, existen diferentes tipos de conectores como se muestran en la figura 39.

Figura 39: Tipos de conectores

Fuente: http://www.ab.com/

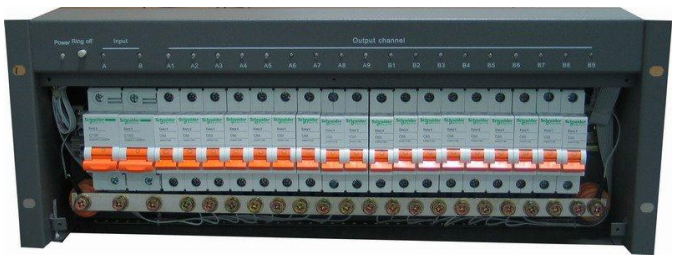
### 3.12 Sistema eléctrico PDU

Una unidad de distribución de energía (PDU) es un dispositivo equipado con salidas múltiples diseñado para distribuir la energía eléctrica, especialmente a los bastidores de computadoras y equipos de red ubicados en el centro de datos.

> El término (PDU) puede referirse a dos clases principales de dispositivos de potencia de hardware; la primera y por lo general el término no calificado general se refiere a la categoría de dispositivos de distribución de energía relativamente montados en el piso más alto costo que transforman uno o más grande la capacidad prima de alimentación en alimentaciones cualquier número de menor energía distribuida la capacidad de comer. En un centro de datos típico, por ejemplo, no habría relativamente pocos de estos dispositivos PDU montada en el suelo, que se encuentra a lo largo de las paredes o en lugares centrales para espacios más grandes. Cada planta de montaje de PDU ver figura 40, alimentaría un número mucho mayor de bastidores y filas de bastidores. (SCHNEIDER-ELECTRIC, 2014)

"El segundo tipo de PDU es a veces llamado un Smart-PDU, PDU de Rack o Intelligent PDU el cual es el más utilizado en centros de telecomunicaciones, como se muestra en la figura 40. gabinete. (SCHNEIDER-ELECTRIC, 2014)"

Figura 40: PDU




Fuente: http://www.aliexpress.com/

### 3.13 Interfaces y Módulos

Mediante las interfaces o módulos se pueden controlar de forma remota en un tiempo real, recibir la potencia óptica, transmite la potencia óptica, corriente de polarización del láser, la tensión de entrada y la temperatura de los módulos ópticos en el enlace de datos. Los usuarios pueden utilizar la función de diagnóstico para gestionar su red

con una eficaz herramienta de alta precisión, para un control fiable del rendimiento. Las interfaces o módulos (SFP) son fáciles de instalar permite añadir de forma sencilla capacidad 100BASE-FX a un switch. El módulo funciona con una longitud de onda de 1310 nm y soporta cableado de fibra óptima multimodo. En un entorno de funcionamiento típico, puede alcanzar distancias de hasta 10 Km, en función de la atenuación total de la planta de fibra.

Figura 41: Módulos SFP ZX, LX

Fuente: http://computienda.com.co/

### 3.14 Diseño de infraestructura

En el diseño de infraestructura se conocerá de una manera gráfica y detallada el diseño de una sala de telecomunicaciones con sus respectivos elementos necesarios para el funcionamiento de una manera efectiva de una sala de equipos, los planos que se muestran en las siguientes figuras representan a cada uno de los nodos que se mostrara en la simulación que está en el siguiente capítulo. Los elementos que están en cada uno de los nodos son los más importantes e imprescindibles para tener una comunicación sin problemas entre ellos, en la práctica, las salas de telecomunicaciones o nodos fueron diseñadas según las normas de cableado estructurado e instalaciones de equipos y racks. Elementos tales como centrales telefónicas, son necesarios en salas de telecomunicaciones para la telefonía de lugares cercanos a la sala de telecomunicaciones.

Rack de equipos, elemento imprescindible para la comunicación e instalación de los equipos de la sala de telecomunicaciones, se realizara la instalación de equipo, PDU, ODF.

ODF, DSLAM son elementos que permite la transmisión entre los nodos mediante fibra obscura o mediante protocolos de transmisión de datos como es SDH.

Banco de baterías y el rectificador son los que proporcionaran energía a toda la sala de telecomunicaciones en todo momento para el correcto funcionamiento. Aire acondicionado indispensable para el funcionamiento de los equipos ya que los equipo de telecomunicaciones necesitan de una buena ventilación para el funcionamiento.

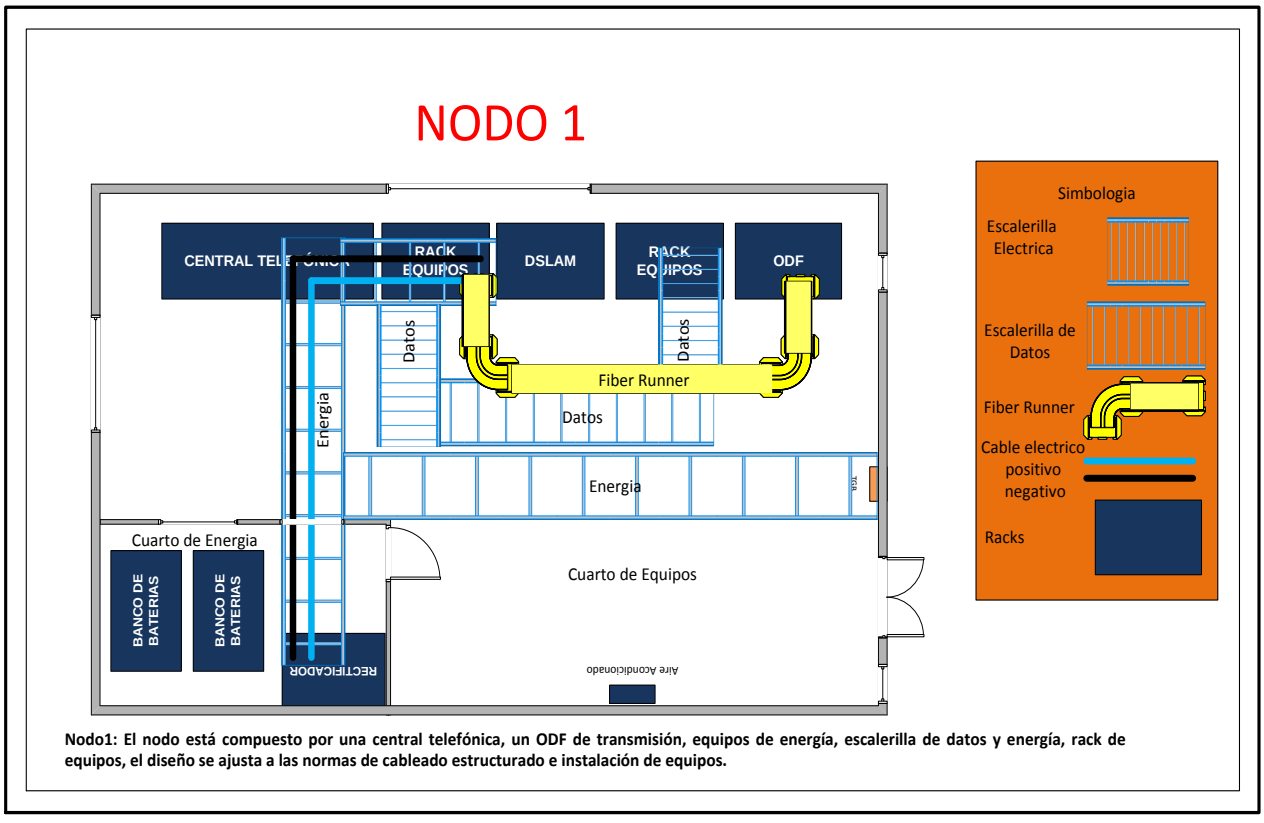
Escalerillas encargadas de guiar el cable eléctrico y el cable de datos a los racks de equipos.

Fiber runner es el elemento por el cual se guiara la fibra óptica entre los equipos que la necesiten para las transmisiones que se van a realizar.

TGB, es la descarga a tierra de todos los equipos de la sala de telecomunicaciones.

En las figuras 42, 43, 44, 45, 46, 47 se detallará el diseño de infraestructura de los nodos representados en la simulación por los routers.

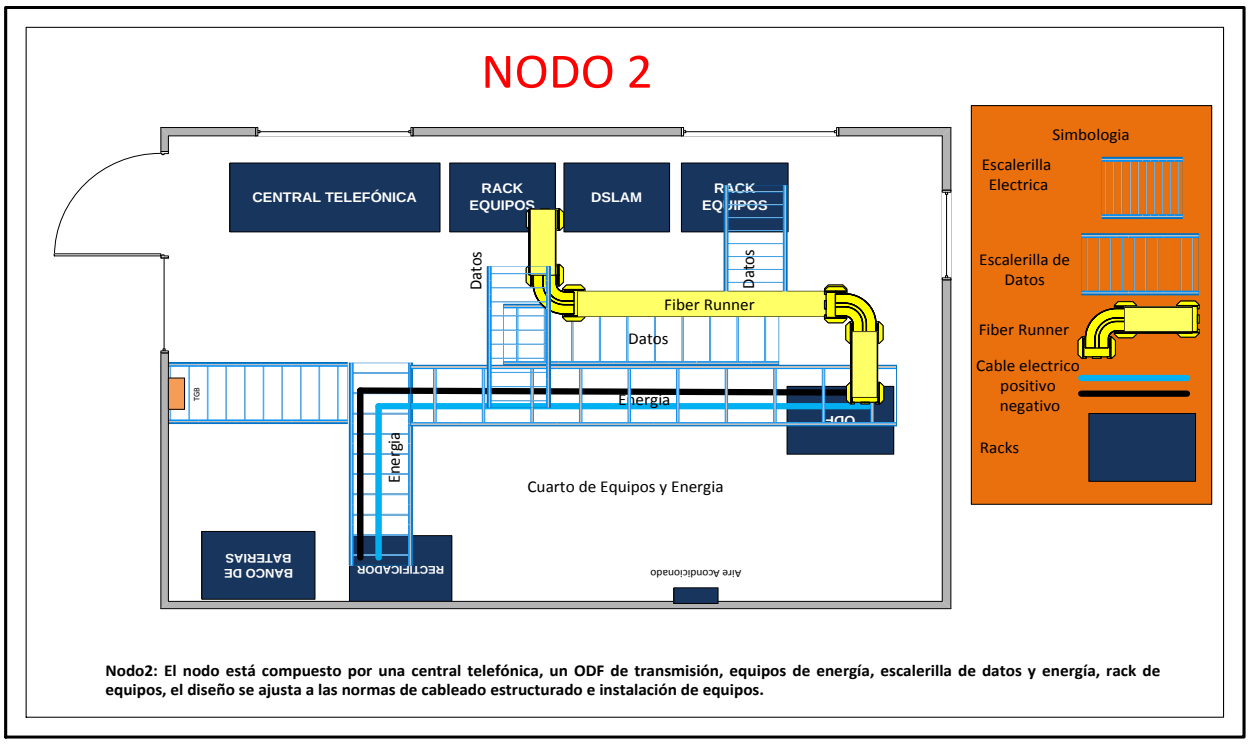
Figura 42: Diseño de Nodo1 con elementos necesarios para el funcionamiento




**Nodo1: El nodo está compuesto por una central telefónica, un ODF de transmisión, equipos de energía, escalerilla de datos y energía, rack de equipos, el diseño se ajusta a las normas de cableado estructurado e instalación de equipos.**

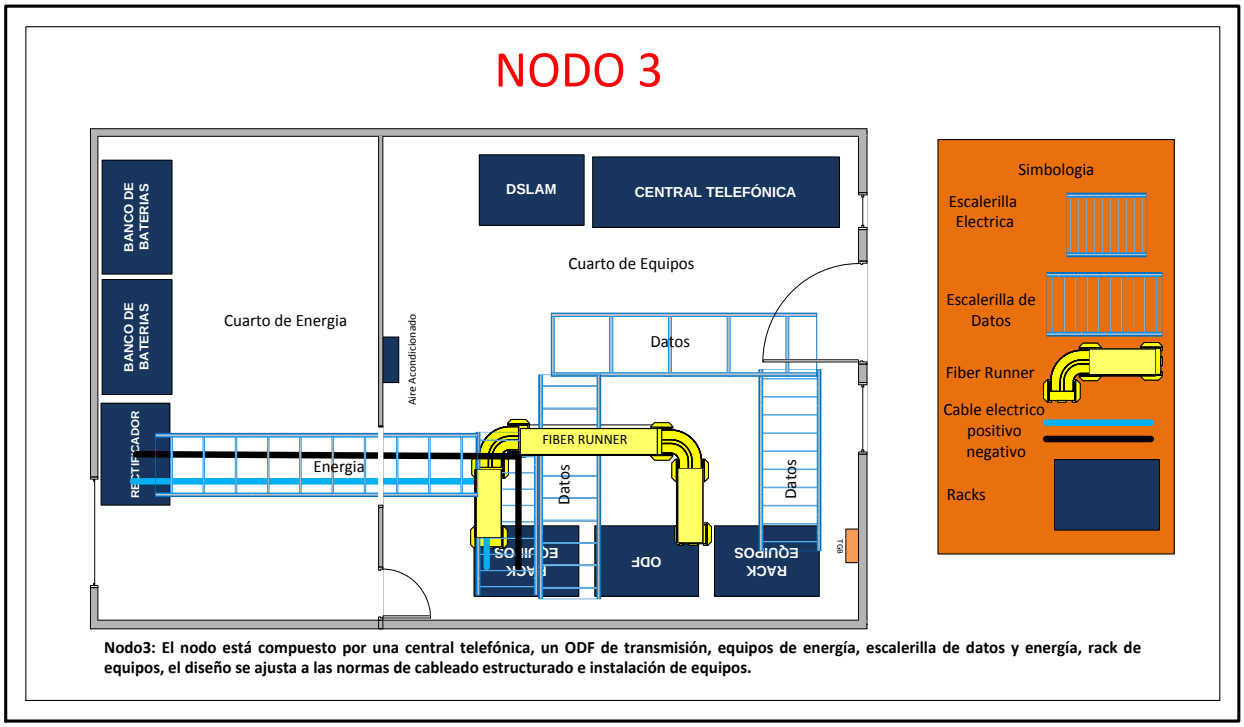
Elaborado por: Rolando Reyes

Figura 43: Diseño de Nodo2 con elementos necesarios para el funcionamiento



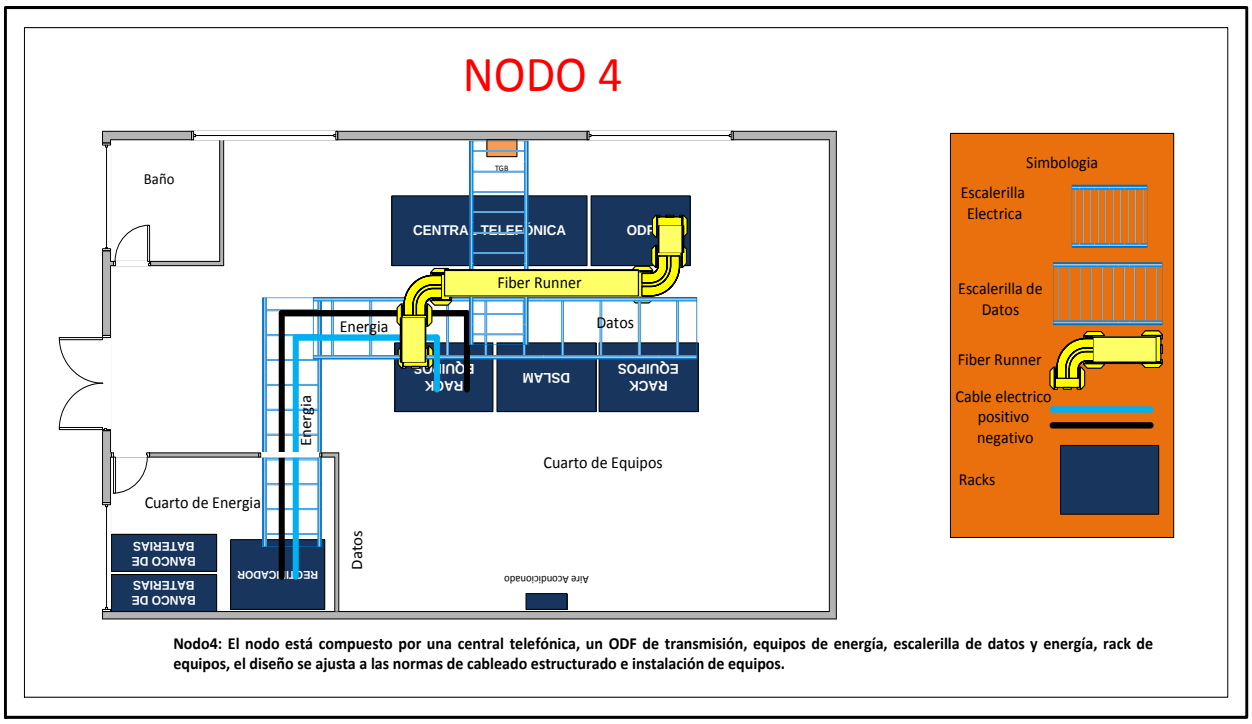

Elaborado por: Rolando Reyes

Figura 44: Diseño de Nodo3 con elementos necesarios para el funcionamiento




Elaborado por: Rolando Reyes

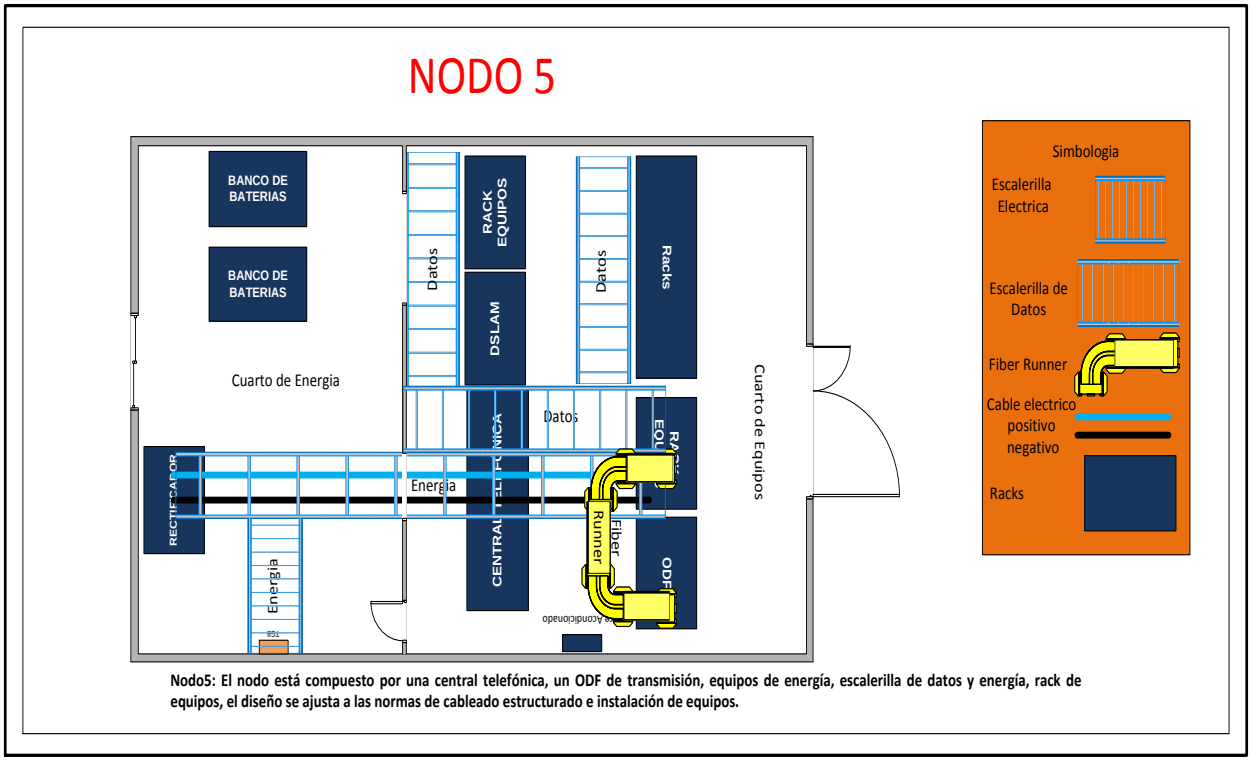
Figura 45: Diseño de Nodo4 con elementos necesarios para el funcionamiento




**Nodo4: El nodo está compuesto por una central telefónica, un ODF de transmisión, equipos de energía, escalerilla de datos y energía, rack de equipos, el diseño se ajusta a las normas de cableado estructurado e instalación de equipos.**

Elaborado por: Rolando Reyes

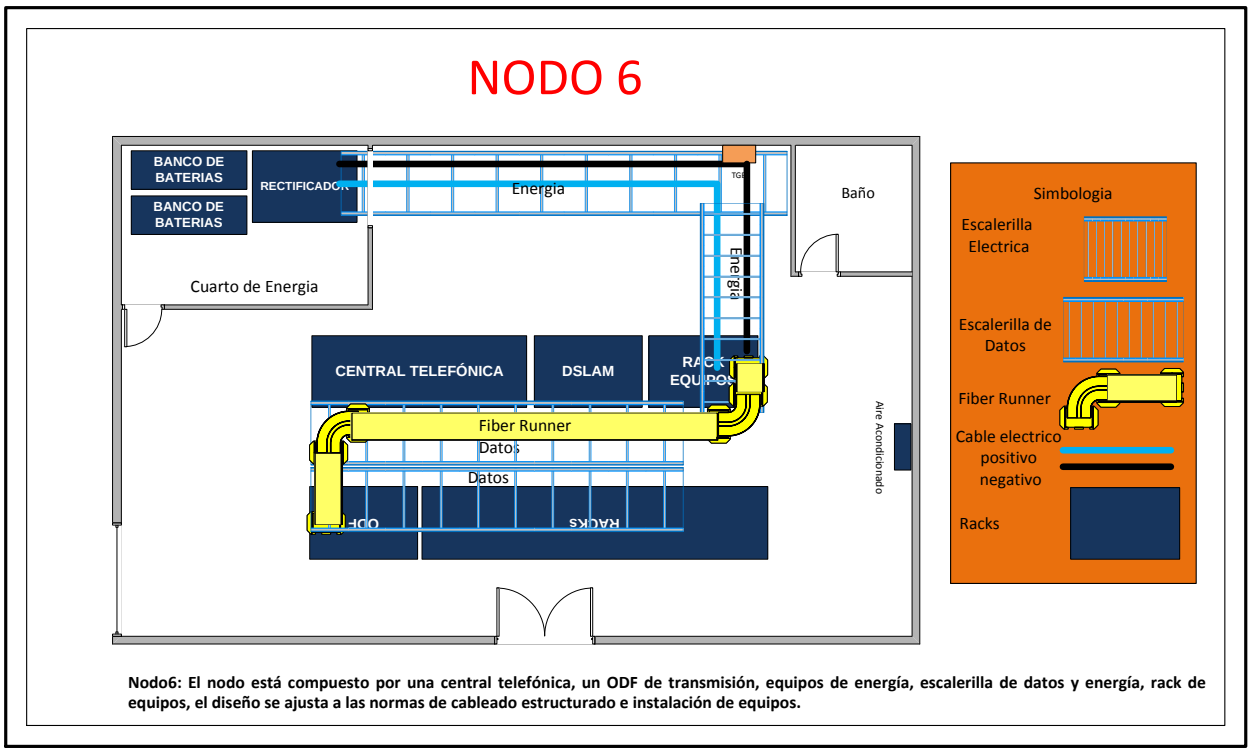
Figura 46: Diseño de Nodo5 con elementos necesarios para el funcionamiento




**Nodo5: El nodo está compuesto por una central telefónica, un ODF de transmisión, equipos de energía, escalerilla de datos y energía, rack de equipos, el diseño se ajusta a las normas de cableado estructurado e instalación de equipos.**

Elaborado por: Rolando Reyes

Figura 47: Diseño de Nodo6 con elementos necesarios para el funcionamiento




Elaborado por: Rolando Reyes

Cada uno de los nodos está representado en la simulación, que se conocerá en el siguiente capítulo, la representación de cada uno de los nodos se muestra en la tabla 10.

Tabla 10: Representación de nodos en simulación

| **Nodo** | **Router** |
|---|---|
| Nodo 1 | R1 |
| Nodo 2 | R2 |
| Nodo 3 | R3 |
| Nodo 4 | R7 |
| Nodo 5 | R8 |
| Nodo 6 | R9 |

Elaborado por: Rolando Reyes

# CAPÍTULO 4
# SIMULACIÓN

## 4.1 Introducción a GNS3

GNS3 es emulador, en el que funcionan simulaciones como redes reales, todo ello sin necesidad de hardware de red dedicada, como routers y switches.

El software proporciona una interfaz gráfica de usuario intuitiva para diseñar y configurar redes virtuales, que se ejecuta en hardware de PC tradicionales y se puede utilizar en múltiples sistemas operativos, incluyendo windows, linux y MacOS X.

A fin de proporcionar simulaciones completas y precisos, en realidad GNS3 utiliza los siguientes emuladores para ejecutar los mismos sistemas operativos como en redes reales:

- Dynamips, el conocido emulador de IOS de Cisco.
- VirtualBox, ejecuta los sistemas operativos de escritorio y de servidor, así como Juniper Junos.
- Qemu, un emulador de máquina de código abierto genérico, se ejecuta Cisco ASA, PIX y el IPS.

GNS3 es una herramienta complementaria a los laboratorios reales para ingenieros de redes, administradores y personas que estudian para certificaciones como Cisco CCNA, CCNP y CCIE, así como Juniper JNCIA, JNCIS y JNCIE.

GNS3 se puede utilizar para experimentar características o para comprobar configuraciones que necesitan ser desplegado en dispositivos reales.

GNS3 incluye características interesantes como; la conexión de la red virtual para los reales o captura de paquetes utilizando Wireshark, el cual permitirá monitorear la red.

GNS3 requiere la elección e instalación del sistema operativo del router o IOS. Además requiere gran cantidad de recursos del computador y hay que configurarlo correctamente o el computador podría llegar incluso a bloquearse. Otra característica interesante de GNS3 es la capacidad de conectar los dispositivos virtuales de nuestra red a dispositivos reales.

GNS3 también es compatible con otros programas de emulación, a saber, Qemu, Pemu y VirtualBox. Estos programas se utilizan para emular Cisco ASA y cortafuegos PIX, Cisco IPS, enrutadores Juniper, así como anfitriones (Linux, Windows, Mac OS X, FreeBSD, etc) GNS3 hace todo esto emulación trabajo magia juntos y permitir, por ejemplo, tener el router Cisco hablar con su servidor Linux.

GNS3 permite la emulación de Cisco IOSs en un equipo con Windows, Linux y Mac OS X. La emulación es posible que una larga lista de las plataformas de routers y otros dispositivos . El uso de una tarjeta de EtherSwitch en un router, plataformas de conmutación también pueden ser emulados con el grado de funcionalidad soportada de la tarjeta.

Con GNS3 está ejecutando una verdadera Cisco IOS, por lo que verá exactamente lo que produce el IOS y tendrás acceso a cualquier comando o parámetro con el apoyo del IOS.

Además, GNS3 es un código abierto, programa gratuito para que utilicen personas que lo necesiten. Sin embargo, debido a restricciones de licencia, tendrá que proporcionar su propia Cisco IOSs de usar con GNS3.

También, GNS3 proporcionará alrededor de 1000 paquetes por segundo de rendimiento en un entorno virtual. Un router normal, proporcionará cien a mil veces mayor rendimiento. GNS3 no toma el lugar de un router real, pero tiene la intención de ser una herramienta para el aprendizaje y las pruebas en un entorno de laboratorio. Uso de GNS3 de cualquier otra manera sería considerado inadecuado.

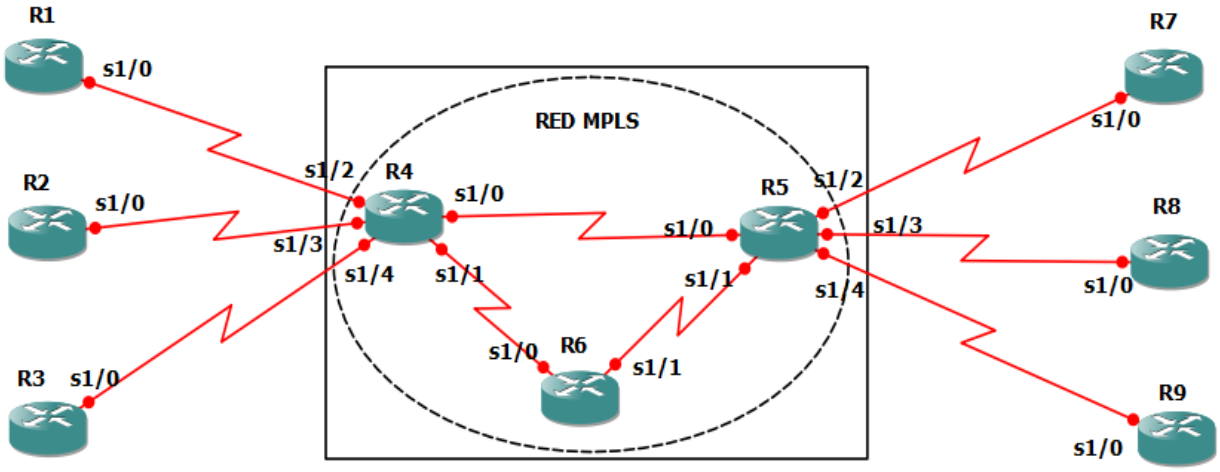
El equipo usado para la práctica es un pc con procesador intel core i5, con una memoria de 4gb, ya que el simulador utilizado consume gran cantidad de memoria por la utilización de los IOS que nos dan un entorno de trabajo real, se recomienda utilizar un pc con similares características o superiores para que no haya ningún tipo de problema al momento de realizar cualquier tipo de simulación.

### 4.1.1 Topologías

### 4.1.2 Topología Física

En la topología física de la simulación se conocerá como están conectados los dispositivos con las interfaces de cada uno de los dispositivos que se utilizará, para la simulación como se observa en la figura 48.

Figura 48: Topología física




Elaborado por: Rolando Reyes

Los elementos de infraestructura que se utilizaran son los siguientes:

- **Router 7200**

Los routers Cisco 7200 son routers de procesador único más rápidos de Cisco, ideales para empresas y proveedores de servicios que implementan MPLS, agregación de ancho de banda, periféricos WAN, seguridad IP, VPN e integración vídeo/voz/datos.

La serie 7200 integra diseño modular, opciones de conectividad y funciones de gestión.

Mejora notablemente el rendimiento de la red en la que se instale, por sus múltiples beneficios.

- **Switch 3600**

Conmutador diseñado específicamente para la convergencia de servicios inalámbricos y de líneas de cables, el Cisco ME 3600X extiende velocidad de transporte de la cartera a 10 Gbps en la capa de acceso para las aplicaciones empresariales y móviles. También permite a los proveedores de servicios para iniciar los servicios de VPN conmutación de etiquetas multiprotocolo (MPLS) con sede en desde dentro de la capa de acceso.

El 3600X Series Cisco ME ofrece a los proveedores de servicios la capacidad de expandir MPLS hacia su extremo de la red para obtener las ventajas de un único plano de control MPLS unificada a través de su red.

- **PC**

Las pcs seleccionada para la simulación son computadores con lo necesario para que soporte la tecnología implementada, las características que debe tener son: memoria ram 4gb, disco duro 500gb, procesador Intel core i5.

### 4.1.3 Topología Lógica

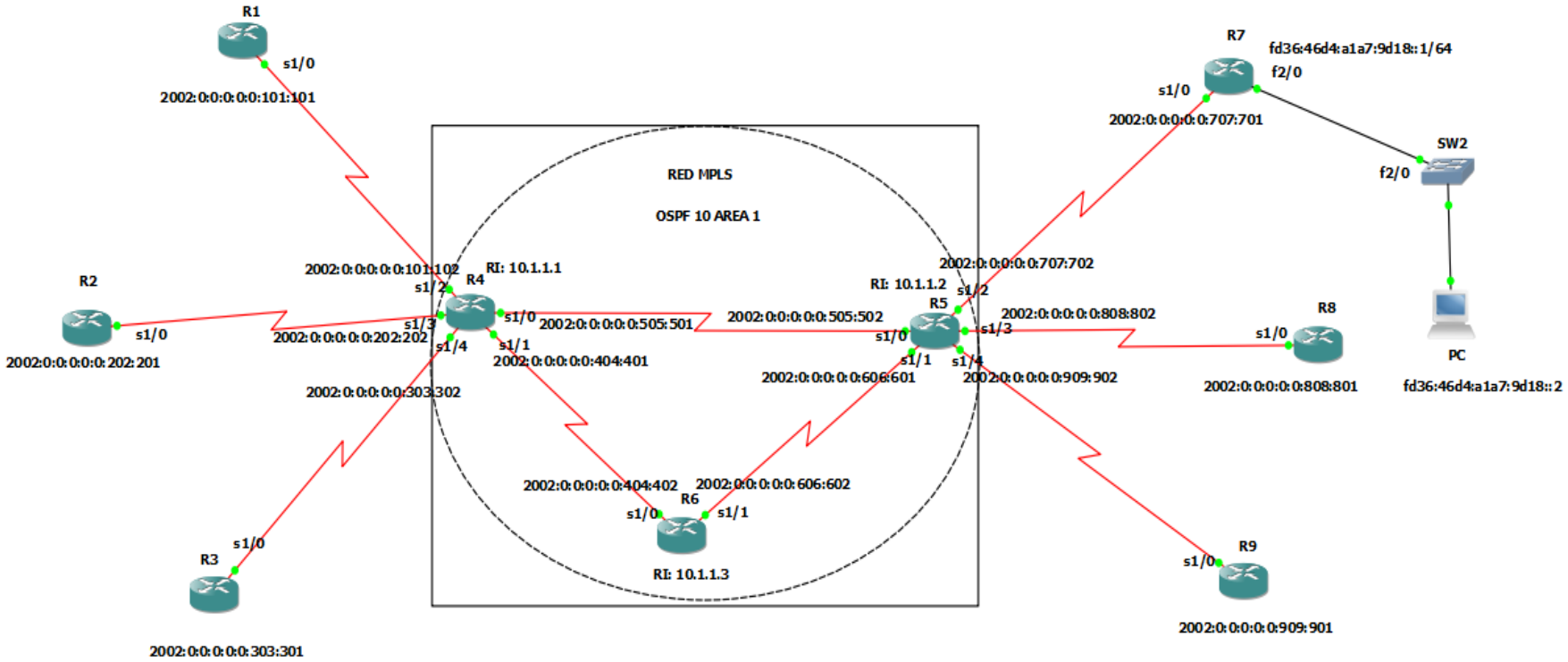
En la topología lógica se conocerán de una manera detallada las conexiones de las interfaces de todos los dispositivos que se utilizara en la simulación, como se muestra en la figura 49, además de su respectivo direccionamiento ver en la tabla 11.

Las direcciones que se utilizará en la simulación son direcciones unicast, ya que son direcciones que se utilizan para redes WAN y son redes públicas.

En la topología lógica se podra obserbar de una manera gráfica como estaran conectados los dispositivos que estaran representados por los nodos como se muestra en la tabla 10, mediante la simulación se consolidaran los conceptos descritos anteriormente.

En la topología lógica se describirá de una manera detallada las conexiones de los dispositivos con las interfaces, y direccionamiento de los dispositivos que se utilizaran en la simulación de la red MPLS en entorno IPV6, para la simulación se utilizará el protocolo de enrutamiento OSPFv3, protocolo de direccionamiento IPV6 y la tecnología MPLS.

Figura 49: Topología lógica




Elaborado por: Rolando Reyes

En la tabla 11 se describirá el direccionamiento con su respectivo nombre, interface, dirección IPV4, dirección IPV6 de los dispositivos que se utilizara en la simulación.

Tabla 11: Direccionamiento de dispositivos

| Dispositivo | Interface | Dirección IPV4 | Prefijo | Dirección IPV6 |
|---|---|---|---|---|
| **R1** | s1/0 | 1.1.1.1 | 24 | 2002:0:0:0:0:0:101:101 |
| **R2** | s1/0 | 2.2.2.1 | 24 | 2002:0:0:0:0:0:202:201 |
| **R3** | s1/0 | 3.3.3.1 | 24 | 2002:0:0:0:0:0:303:301 |
| **R4** | s1/0 | 5.5.5.1 | 24 | 2002:0:0:0:0:0:505:501 |
| | s1/1 | 4.4.4.1 | 24 | 2002:0:0:0:0:0:404:401 |
| | s1/2 | 1.1.1.1 | 24 | 2002:0:0:0:0:0:101:102 |
| | s1/3 | 2.2.2.2 | 24 | 2002:0:0:0:0:0:202:202 |
| | s1/4 | 3.3.3.2 | 24 | 2002:0:0:0:0:0:303:302 |
| **R5** | s1/0 | 5.5.5.2 | 24 | 2002:0:0:0:0:0:505:502 |
| | s1/1 | 6.6.6.1 | 24 | 2002:0:0:0:0:0:606:601 |
| | s1/2 | 7.7.7.2 | 24 | 2002:0:0:0:0:0:707:702 |
| | s1/3 | 8.8.8.2 | 24 | 2002:0:0:0:0:0:808:802 |
| | s1/4 | 9.9.9.2 | 24 | 2002:0:0:0:0:0:909:902 |
| **R6** | s1/0 | 4.4.4.2 | 24 | 2002:0:0:0:0:0:404:402 |
| | s1/1 | 6.6.6.2 | 24 | 2002:0:0:0:0:0:606:602 |
| **R7** | s1/0 | 7.7.7.1 | 24 | 2002:0:0:0:0:0:707:701 |
| **R8** | s1/0 | 8.8.8.1 | 24 | 2002:0:0:0:0:0:808:801 |
| **R9** | s2/0 | 9.9.9.1 | 24 | 2002:0:0:0:0:0:909:901 |

Elaborado por: Rolando Reyes

## 4.2 Configuración de dispositivos

En la configuración de dispositivos se conocerá la configuración de cada uno de los dispositivos, el protocolo de enrutamiento OSPFv3, el protocolo de direccionamiento IPV6, y la tecnología empleada MPLS.

- **OSPFv3 sobre IPV6 y MPLS**

La versión 3 de OSPF fue creada para que, a diferencia de la versión 2, pueda soportar direccionamiento IPv6.

En OSPF para IPv6, el routing process no necesita ser explícitamente creado, al habilitar OSPF para IPv6 en la interfaz, el proceso será creado. En OSPF para IPv6, cada interfaz debe ser habilitada con un comando en modo de configuración de interfaz. Esto lo diferencia de OSPFv2, donde las interfaces quedan automáticamente

habilitadas con un comando de configuración global, al mismo tiempo, se pueden configurar varios prefijos en una única interfaz.

El uso de cualquier transporte de circuito para el despliegue de IPv6 sobre redes MPLS no tiene impacto en la operación o infraestructura de MPLS, y no requiere cambios de configuración en el núcleo o proveedor de routers de borde. La comunicación entre los dominios remotos IPv6 corre protocolos IPv6 nativas más de un enlace dedicado, donde los mecanismos subyacentes son completamente transparentes para IPv6.

El tráfico IPv6 se hace un túnel mediante cualquier transporte sobre MPLS (MPLS / Atom) o ethernet sobre MPLS (EoMPLS) cuentan con los routers conectados a través de una interfaz ATM OC-3 o Ethernet, respectivamente.

Para implementar IPv6 en un circuito de transporte sobre MPLS, los routers IPv6 deben estar configurados para la conectividad IPv6 como se realizó en la configuración de OSPF.

### 4.2.1 Configuración de dispositivos

En la tabla 12 se conocerá la configuración de contraseña en modo privilegiado, la cual será aplicada a todos los dispositivos que estarán en la simulación. De esta manera se podrá tener mayor seguridad y control de acceso de usuarios no autorizados.

Tabla 12: Configuración de contraseña en modo privilegiado

| Habilitar la contraseña | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# enable password contraseña | // Ingresar contraseña. |

Elaborado por: Rolando Reyes

En la tabla 13 se describirá la configuración de acceso telnet a cada router, para permitir que los administradores de la red se conecten al router vía una sesión telnet

desde cualquier PC de la red, para lo cual se configurara 5 posibilidades de sesión telnet.

Tabla 13: Configuración de acceso telnet

| Habilitar la contraseña | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# line vty 0 4 | // Configura la posibilidad de 5 sesiones telnet. |
| Router(config-line)# password contraseña | // Introducir la contraseña. |

Elaborado por: Rolando Reyes

La tabla 14 describirá la configuración de cada interface para OSPF, en OSPF para IPV6 cada interfaz debe ser habilitada con un comando en modo de configuración de interfaz como se muestra en la siguiente tabla.

Tabla 14: Configuración de cada interface de los dispositivos

| Configuración de interface | |
|---|---|
| Router> enable | // Introducir la clave solicitada |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)#interface <interface> | // Permite el envío de datagramas IPv6 unicast. |
| Router(config-if)# ipv6 address <direccion ipv6> | // Ingresar la dirección ipv6 y prefijo. |
| Router(config-if)# ipv6 ospf<process-id>area<num-area> | // Define el process y área. |

Elaborado por: Rolando Reyes

En la tabla 15 se conocerá la configuración de banner de cada router, los banner son mensajes de advertencia que se muestran cuando alguien quiera establecer una sesión de telnet desde otro computador.

Tabla 15: Configuración de banner del dispositivo

| Configuracion de banner | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |

| | |
|---|---|
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# banner motd x Mensaje x | // Ingresar el mensaje que desea que aparezca. |

Elaborado por: Rolando Reyes

En la tabla 16 se realizara la configuración de hostname o nombre del dispositivo, el comando hostname modifica el nombre del dispositivo, con la configuración de hostname se tendrá una descripción acorde a la red.

Tabla 16: Configuración de nombre de dispositivo

| Configuración de hostname | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# hostname <nombre-dispositivo> | // Ingresar nombre del dispositivo. |

Elaborado por: Rolando Reyes

La tabla 17 muestra la configuración de unicast OSPF para IPv6, el comando ipv6 unicast-routing servirá para habilitar el ruteo y él envió de datagramas con el protocolo IPV6 en cada interface que se requiera.

Tabla 17: Configuración de unicast ospf para IPV6

| Habilitar el ruteo para IPv6: | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# ipv6 unicast-routing | // Permite el envío de datagramas IPv6 unicast. |
| Router(config)# ipv6 cef | // Activa IPV6 Forwarding. |

Elaborado por: Rolando Reyes

En la tabla 18 se observará la configuración del comando ipv6 ospf <> area <>, el comando se configurará en cada interface del dispositivo para identificar el dispositivo que origina o procesa información del protocolo.

Tabla 18: Habilitación de ospf para IPV6

| | |
|---|---|
| Router> enable | //Introducir clave solicitada |
| Router# configure terminal | //Modo configuración global. |
| Router(config)# interface <type> <number> | //Ingresar interface. |
| Router(config-if)# ipv6 ospf <process-id> area <area-id> | //Ingresar process-id y area. |

Elaborado por: Rolando Reyes

La tabla 19 muestra la configuración del área y rango para OSPF IPv6, con el comando area < > range <> se activará el modo de configuración del router para el protocolo OSPF el área y el rango según los parámetros que se utilizará.

Tabla 19: Definir el área range para ospf

| Definir Area Range | |
|---|---|
| Router> enable | //Ingresar clave. |
| Router# configure terminal | //Conf global. |
| Router(config)# ipv6 router ospf <process-id> | //Process id-ospf. |
| Router(config-rtr)# area <area-id> range <ipv6-prefix/prefix-length> | //area y dirección ip. |

Elaborado por: Rolando Reyes

La tabla 20 muestra la configuración de MPLS en los routers asignados, una vez establecido los protocolos de ruteo se configurara las funcionalidades del protocolo de distribución de etiquetas en las distintas interfaces que se requerirán, se realizará la activación del protocolo de distribución de etiquetas LDP.

Tabla 20: Configuración de MPLS

| Habilitar MPLS | |
|---|---|
| Router> enable | // Introducir la clave solicitada. |
| Router# configure terminal | // Entrar en el modo de configuración global. |
| Router(config)# mpls ip | // Habilita globalmente el procesamiento mpls. |
| Router(config-if)# mpls mtu<num> | // Cambia el valor mtu para los paquetes mpls. |
| Router(config-if)# mpls label protocol<ldp/tdp/both> | // Indica si se debe utilizar ldp o tdp como protocolos de intercambio de etiquetas. |

| | |
|---|---|
| Router(config-if)# mpls ldp router-id <interface> | // Indica que el router-id de LDP se tome de la interface indicada. |

Elaborado por: Rolando Reyes

### 4.3 Pruebas de simulación

En las pruebas de simulación se conocerán los resultados obtenidos en la red, para ello se utilizará el software de captura de paquetes WireShark, el cual permitirá la captura de paquetes en toda la red para una mejor interpretación del tráfico que estará cursando por toda la red, a continuación se detallará los resultados obtenidos en la simulación.

### 4.4 Análisis de Resultados

En el análisis de resultados se utilizará un software de captura de paquetes llamado wireshark, el cual permitirá la captura de tramas y paquetes que pasan a través de las interfaces de red, el cual cuenta con características de un analizador de protocolos, wireshark permitirá capturar todo tipo de paquetes en la red.

WireShark es un analizador de paquetes de red también llamado sniffer, es utilizado por administradores para ver todo el tráfico en un momento específico, una de las ventajas de wireshark es opensource, además ofrece distintos tipos de filtros para leer paquetes.

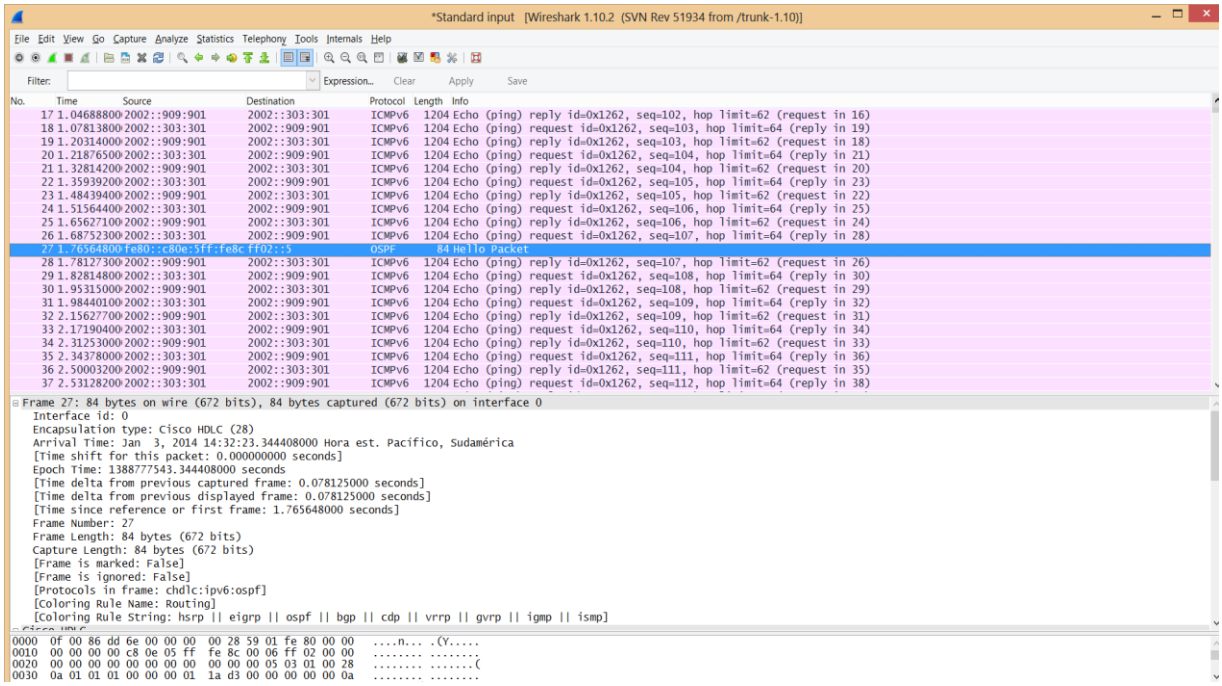
En la captura de paquetes se observará distintos resultados como gráficas estadísticas, gráficas de fluidez de tráfico, y así se tendrá un eficaz interpretación de una forma gráfica de lo que está ocurriendo en la red, en las siguientes gráficas se observarán los resultados obtenidos en la red.

En la figura 50 se muestra la captura de paquetes de toda la red en un momento específico, en la captura de paquetes se muestra el tiempo, el destino, la fuente, el tipo de protocolo, la información, el protocolo ICMPv6 echo request ping desde un punto hacia otro.

En la parte del frame se observará las características del paquete capturado hasta su más mínima expresión, otro resultado que se muestra es el identificador del

checksum que es el encargado de proporcionar información si el paquete ha llegado correctamente a través de un algoritmo matemático.

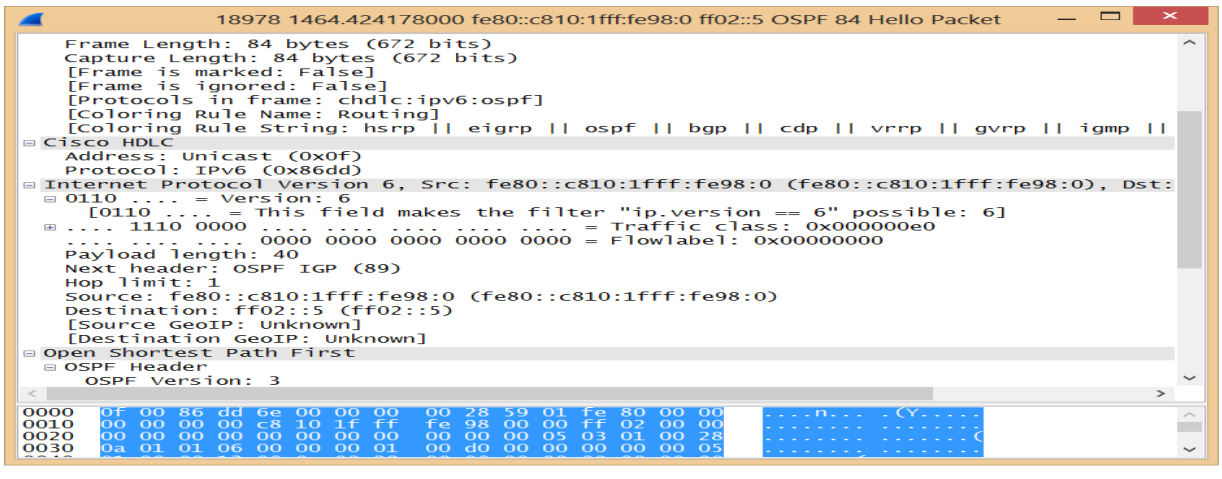
Figura 50: Captura de paquetes




Elaborado por: Rolando Reyes

En la figura 51 se detalla la captura del protocolo OSPF en la red, en la figura se puede observar la longitud del paquete, el tamaño de paquetes enviados y recibidos, el protocolo que se está utilizando, la longitud de carga útil del paquete, la cabecera de paquete, la fuente y el destino, se observa hasta el más mínimo detalle del protocolo utilizado en el caso es OSPF.

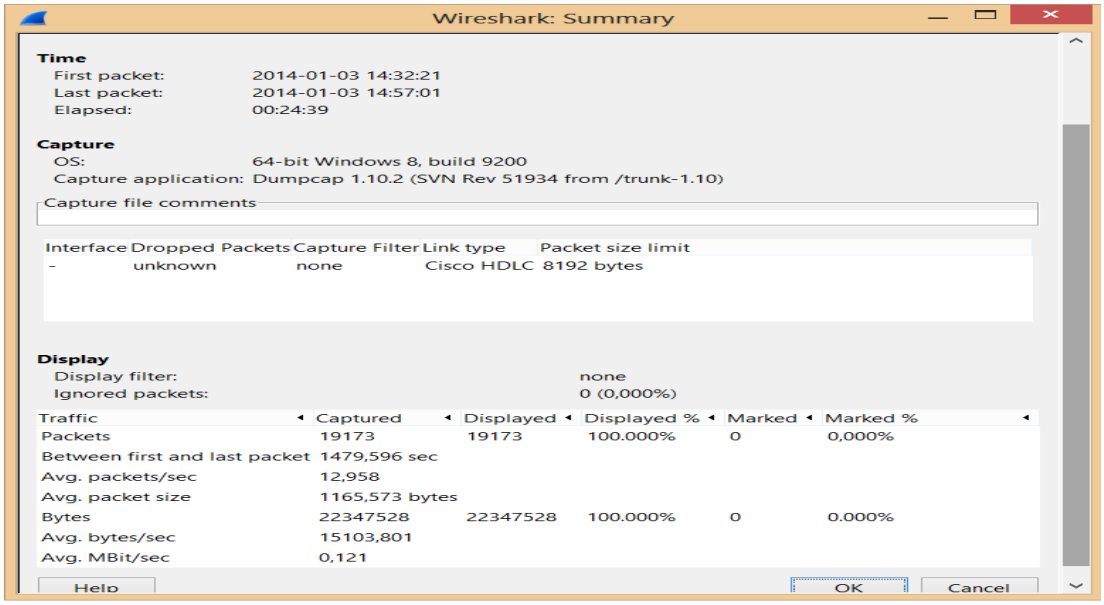
Figura 51: Captura de paquete OSPF




Elaborado por: Rolando Reyes

En la figura 52 se detalla de una manera clara y concisa el resumen de la captura de un paquete en un tiempo determinado, se observa la fecha y hora en la que el primer y último paquete salió y llegó a su destino respectivamente, se muestra el número, tamaño y porcentaje de los paquetes capturados e ignorados o perdidos, entre un punto y otro.

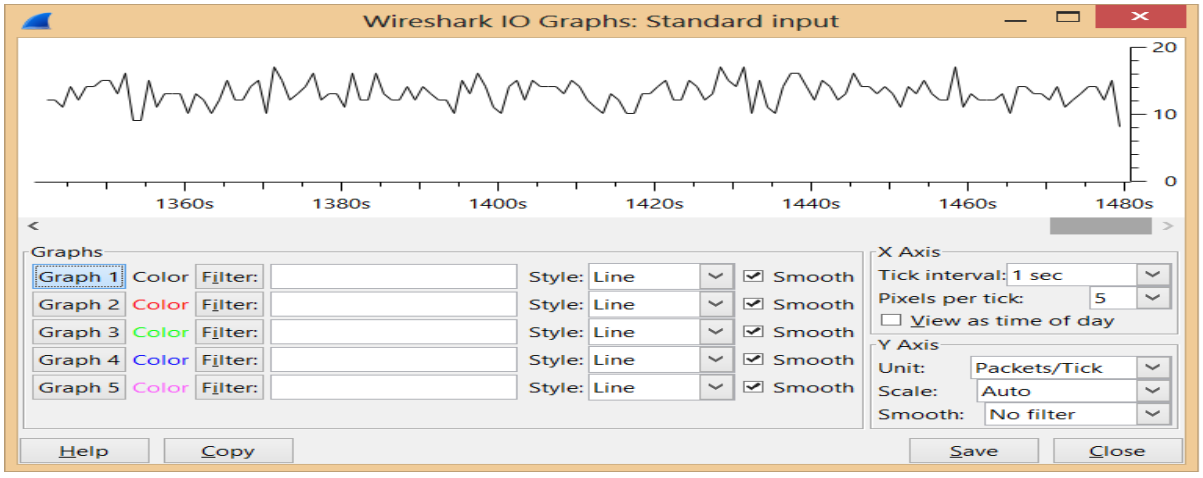
Figura 52: Paquetes enviados y recibidos




Elaborado por: Rolando Reyes

En la figura 53 se observa en función del tiempo la captura de paquetes en la toda la red, la gráfica muestra que la captura de paquetes en función del tiempo es una variable cuantitativa, según aumente la transmisión de paquetes en la red.

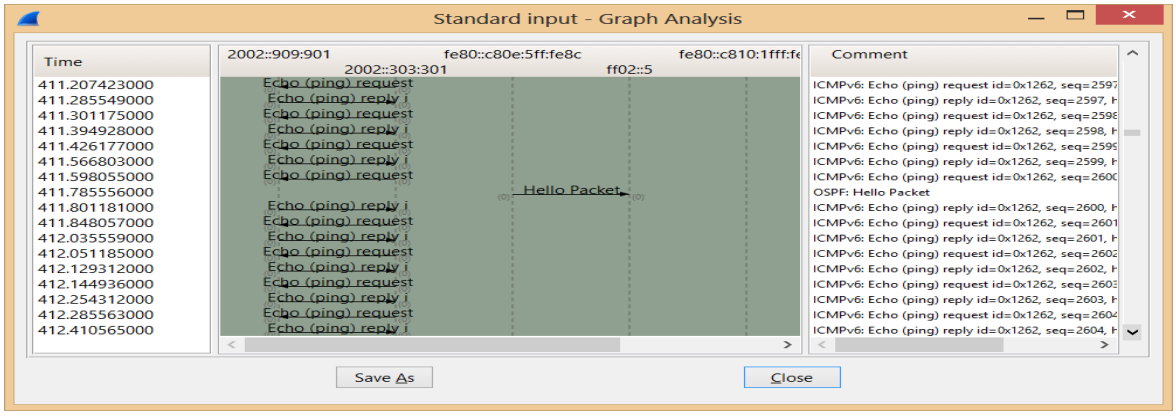
Figura 53: Representación de captura de paquetes




Elaborado por: Rolando Reyes

En la figura 54 se muestra la fluidez del tráfico de los paquetes en la red, además se observa el tiempo de cada salto de paquete, se conocerá la dirección IPV6 origen y destino, se observa el paquete hello el cual indica que el router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por cada router, indicando el tipo de relación que mantiene con cada uno, estos paquetes se envían periódicamente en todas las interfaces, lo que permite el descubrimiento dinámico de los enrutadores vecinos

Figura 54: Flow Traffic




Elaborado por: Rolando Reyes

## CONCLUSIONES

- Mediante la utilización de la tecnología MPLS en una red con el protocolo IPV6 se mejora la escalabilidad y se obtiene mayor flexibilidad para la entrega de servicios de enrutamiento en trasmisión de paquetes de la red, por medio de esta tecnología mencionada se observa un crecimiento en la funcionalidad de la red, dando como resultado una eficiente transmisión en todos los datos dentro de la red MPLS con la fusión del protocolo de enrutamiento OSPFv3.

- Con la utilización del protocolo IPV6 en una red, se puede suplir muchas deficiencias de la anterior versión de este protocolo, dando como conclusión que el protocolo IPV6 provee como la principal ventaja el aumento en el número de direcciones ip y la seguridad para solventar los problemas que tiene la versión anterior de este protocolo.

- El diseño de infraestructura de cada uno de los nodos, está basado en normas de instalación de equipos, infraestructura y dispositivos, los elementos utilizados para la construcción de los nodos son los necesarios para que los nodos funcionen sin ningún problema, y se ajusten a las necesidades de cualquier empresa que desee implementar estos servicios.

- Para tener una conclusión clara y concisa se realizó una simulación real de la red con imágenes IOS de equipos que el propio software proporciona, la principal ventaja de este software es que proporciona conexiones de red simuladas para el mundo real y gracias a ello pudimos crear una simulación tal y como en la realidad utilizando medios reales.

- En el análisis de resultados de la simulación se observó de una manera detallada gráficas estadísticas, indicando todo lo que pasa en la red, para tener para tener una interpretación correcta del tráfico en la red, pudimos observar de una manera detallada la descripción de cada uno de los paquetes siendo esto una ayuda para comprender al 100% como funciona

una red con tecnología MPLS en entorno IPV6 con el protocolo de enrutamiento OSPFv3.

## RECOMENDACIONES

- Realizar investigaciones profundas de temas relacionados, buscando conceptos correctos y reales, para tener ideas claras de los objetivos planteados, realizar investigaciones a futuro con las actualizaciones necesarias de las tecnologías que evolucionan en el tiempo, dando como resultado más eficiencia al momento de resolver problemas.

- Investigar en trabajos futuros las evoluciones de las tecnologías de una manera detallada, utilizando ejemplos prácticos para tener una mejor comprensión y seguir actualizando los conocimientos adquiridos.

## LISTA DE REFERENCIAS


- ARTES L (2003). *Quality of service parameters and link operating point estimation based on exective bandwidths.*
- FERNÁNDEZ A. *IPv6 in Latin America. Capítulo Mexicano del Foro IPv6. Presentada en: IPv6 Congress*, Las Vegas, E.U.A.
- Barbera, J. (2000). *MPLS una arquitectura de backbone para la INTERNET del siglo XXI*. España: Congreso Mundo Internet.
- Carpenter, B., Fink, B., and Moore, K., *"Connecting IPv6 Routing Domains Over the IPv4 Internet,"* The Internet Protocol Journal, Volume 3, No. 1.
- ALLAN, D (April 2003). *Guidelines for MPLS load balancing, draft-allan-mpls-loadbal-04.*
- D. Awduche and J. Malcolm IETF (1999). *Requirements for trafic engineering over MPLS RFC2702*. España
- E.Osborne and Ajay Simha (2003), *Trafc engineering with MPLS.* Cisco Press.
- Meyers, P., Degrande, N., Van den Bosch, S. *Alta Disponibilidad en Redes Basadas en MPLS*. Revista de Telecomunicaciones de Alcatel - 4º Trimestre. Alcatel España, S.A.
- *Multiprotocol Label Switching (MPLS).* White Paper. Recuperado el 24 de noviembre de 2013 de: http://www.iec.org/online/tutorials/mpls/index.html, 2001.
- *Multiprotocol Label Switching. International Engineering Consortium.* Recuperado el 15 de septiembre de 2013 de: http://www.ietf.org/dyn/wg/charter/mpls-charter.html, 2007.
- Narten, T. and Draves, R. (2001). *Privacy Extensions for Stateless Address Autoconfiguration in IPv6.* RFC 3041.

# GLOSARIO

**ARP:** Protocolo de resolución de direcciones, es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware que corresponde a una determinada dirección IP.

**ATM:** El modo de transferencia asíncrona (ATM) es una tecnología de comunicaciones desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

**BGP:** Border gateway protocol, es un protocolo mediante el cual se intercambian prefijos.

**CoS:** Clase de servicio, permite en una red trasportar distintas clases de tráfico.

**CPU:** Unidad central de proceso, interpreta las instrucciones contenidas en los programas y procesa los datos.

**CPD:** Centro de datos, es donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

**DSCP:** DiffServ CodePoint.

**DWDM:** Dense wavelength division multiplexing, es una técnica de transmisión de señales a través de fibra óptica.

**EIGRP:** Protocolo de enrutamiento de gateway interior mejorado, es un protocolo de encaminamiento vector distancia avanzado.

**EXP:** Experimental, define el tipo de servicio a utilizar en el LSP, asignando los recursos

**FC:** Fiber Connection, es un conector de fibra óptica con cuerpo roscado para su uso en entornos de alta vibración.

**FECs:** Forward equivalence class, conjunto de paquetes que tienen los mismos requerimientos para su transporte y son transmitidos por una misma ruta.

**FTP:** Protocolo de transferencia de archivos, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

**GMPLS:** Conmutación de etiquetas multiprotocolo generalizado, permite a los routers de la capacidad de señalizar de manera inteligente el nivel óptico, permitiendo a los proveedores establecer, cambiar o conectar enlaces ópticos en tiempo real.

**HTTP:** Protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web para acceder a internet.

**IETF:** International ingineering task force, Es una organización internacional abierta a la normalización, que tiene como objetivos el contribuir a la ingeniería de internet actuando en diversas áreas, tales como transporte, encaminamiento, seguridad, entre otras.

**IGP:** Interior gateway protocol, es un protocolo que genera tablas de enrutamiento dentro de un sistema autónomo.

**IP:** Protocolo de internet, dirección definida por el protocolo de internet.

**IPsec:** Protocol de internet seguro, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP.

**IPv4:** Protocolo de internet Versión 4, cuarta versión del protocolo de internet y la primera en ser implementada a gran escala.

**IPv6:** Protocolo de internet Versión 6, diseñada para reemplazar a IPv4, que en la actualidad se está implementando en la mayoría de dispositivos con acceso a internet.

**IPng:** Protocolo de internet de siguiente generación, nombre que se le a otorgado al protocolo IPV6

**IPX:** Protocolo de internet intercambio, es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red.

**IOS:** Sistema operativo inter red, es el software utilizado en la gran mayoría de routers y switches de Cisco Systems.

**IS-IS:** Protocolo de estado de enlace, maneja una especie de mapa con el que se fabrica a medida que converge la red.

**LAN:** Red de área local, son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión.

**LDP:** Label distribution protocol, LDP define el conjunto de procedimientos y mensajes a traves de los cuales los LSRs establecen LSPs en una red MPLS.

**LER:** Label Edge Router, es el encaminador que se encuentra en el borde de la red MPLS y es el encargado de añadir cabeceras MPLS entre las cabeceras de red.

**LIFO:** Last-in, Fisrt-outm se utiliza en estructuras de datos y teoría de colas primero en entrar es el primero en salir.

**LIB:** Label information base, es donde se guardan todas las etiquetas asignadas por este LSR.

**LSR:** Label Switched Router, es el conmutador interior de la red MPLS que interpreta el valor de la cabecera MPLS.

**LSP:** Label Switched Path, es el camino que describen el conjunto de routers y switches que atraviesan los paquetes.

**MAC:** Control de acceso medio, es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red.

**MPLS:** Multiprotocolo de conmutación de etiqueta, tecnología que permite conectividad de todas las sedes de un cliente entre si y que proporciona mayor eficiencia en las comunicaciones (menos retardo).

**NAT:** Network address translation, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

**NSAP:** Punto de acceso de servicio de red, es una etiqueta que identifica un punto de acceso de servicio que se utiliza en redes.

**OSI:** Sistema de interconexión abierta, es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

**OSPF:** Open shortest path first, es un protocolo de encaminamiento jerárquico que busca el camino más corto abierto.

**PDU:** Unidad de distribución de energía, utilizada para el soporte de energía en salas de telecomunicaciones.

**PNNI:** Private Network to Network Interface, es un algoritmo de encaminamiento utilizado en ATM muy similar a OSPF que proporciona diferentes niveles de la jerarquía de la distribución de información.

**POP:** Protoclo de oficina de correos, Es necesario para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar sus correos electrónicos recibidos sin que ellos estén conectados.

**PPP:** Protocolo punto a punto, es un protocolo de nivel de enlace para hacer conexión entre dos puntos.

**PVC:** Tuberías de policloruro de vinilo.

**QoS:** Calidad de servicio, medida de rendimiento de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad del servicio.

**RDSI:** Red digital de servicios integrados, red que integra servicios de voz, datos, video, etc. por medio de dos canales de 64 Kbit/s.

**RJ:** Registered Jack, es un estándar para interfaz física, tanto para la construcción de conectores como para el diseño del cableado, para la conexión de equipos.

**RIP-2:** Protocolo de información de encadenamiento, es un protocolo de vector de distancias ya que mide el número de saltos como métrica hasta alcanzar la red de destino.

**RX:** Receptor es aquel que capta una senal y la interpreta.

**SDH:** Jerarquía digital síncrona, es el estándar internacional de comunicaciones aceptado para redes de transmisión de alta capacidad.

**SFP:** Puerto para interfaces, es un transceptor compacto y conectable en caliente utilizado para las aplicaciones de comunicaciones de datos y telecomunicaciones.

**SMTP:** Protocolo para la transferencia simple de correo electrónico, es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

**SONET:** Red sincrónica óptica, es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

**SP:** Service Provider, empresa que ofrece a las organizaciones consultoría, auditoria.

***ST:*** Straight Tip, es un conector de fibra optica utilizado para redes.

**STP:** Protocolo de árbol atravesando, es un protocolo de red de nivel 2 del modelo OSI.

**TCP/IP:** Protocolo de control de transmisión/protocolo de internet, es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

**TE:** Traffic Engineering, es el proceso de dirigir el tráfico a través de la columna vertebral para facilitar el uso eficiente de ancho de banda disponible entre un par de enrutadores.

**TIA/EIA:** Estándares del cableado comercial

**TMGB:** Telecommunications main grounding busbar, un dispositivo principal de puesta a tierra de barras.

**ToS:** Tiempo de servicio

**TTL:** Tiempo de vida, sirve para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

**TX:** Transmisor, capta la variable en proceso y la transmite a distancia.

**UTP:** Par trenzado sin blindaje, usado en telecomunicaciones en el que dos conductores eléctricos aislados son entrelazados para anular las interferencias de fuentes externas y diafonía de los cables opuestos.

**VPNs:** Red privada virtual retrata de una o más WAN entrelazadas sobre una red pública compartida normalmente en internet o en un nucleo estructural de red IP.

**VoIP:** Protocolo de internet para voz, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

**WAN:** Red de área amplia, son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios

**XDSL:** Línea de suscripción digital, es una tecnología que ofrece un amplio ancho de banda a través del par de cobre convencional desplegado inicialmente para el servicio telefónico.