



UNIVERSIDAD DEL ACONCAGUA
FACULTAD DE CIENCIAS SOCIALES Y ADMINISTRATIVAS

INGENIERÍA EN TELECOMUNICACIONES

**DISEÑO DE UN MODELO DE REESTRUCTURACIÓN DE SISTEMAS
INFORMÁTICOS, MEDIANTE LA UTILIZACION DE TECNOLOGÍAS WAN.**

AUTOR: Marcos Javier Benegas

LEGAJO: 15040

TUTOR: Guillermo Sandez

LUGAR: Mendoza, (fecha)

Fecha:

Calificación:

ÍNDICE

Calificación:.....	3
1. Resumen.....	10
2. Introducción	11
2.1. Problema.....	11
2.2. Hipótesis.....	12
2.3. Justificación.....	12
2.4. Objetivos.....	13
2.4.1. Objetivo general.....	13
2.4.2. Objetivos específicos.....	13
2.5. Alcances de la Tesina	14
2.6. Estructura Organizativa de la Tesina.....	14
3. Marco Teórico.....	16
3.1. Capítulo 1: Tecnologías WAN (Wide Area Network)	17
3.1.1. Introducción	17
3.1.2. Tipos de enlaces: conmutados y dedicados.....	17
3.1.2.1. Enlaces conmutados	17
3.1.2.2. Enlaces dedicados	17
3.1.3. Topologías WAN	18
3.1.4. Tecnologías actuales: PPP, XDSL y Cablemódem.....	18
3.1.4.1. Protocolo PPP (Point-to-Point Protocol).....	18
3.1.4.2. Tecnología ADSL	19
3.1.4.3. Acceso a Internet por cable (Cablemódem)	22
3.1.4.3.1. Ventajas y desventajas.....	23
3.2. Capítulo 2: MPLS (Multiprotocol Label Switching).....	24
3.2.1. ¿Qué es MPLS?.....	24

3.2.2.	Un poco de historia	25
3.2.3.	El Camino Hacia la Convergencia de Niveles: IP Sobre ATM	25
3.2.4.	Un Paso Más en la Convergencia Hacia IP: Conmutación IP.....	29
3.2.5.	Convergencia real: MPLS	31
3.2.6.	Ideas preconcebidas sobre MPLS	31
3.2.7.	Aplicaciones de MPLS	33
3.2.7.1.	Ingeniería de tráfico - TE	33
3.2.7.2.	Calidad de Servicio - QoS	35
3.2.7.3.	Redes virtuales privadas - VPN	36
3.2.8.	Comparación entre Enrutamiento convencional y Conmutación de etiquetas...	41
3.2.9.	Componentes de una red MPLS	42
3.2.9.1.	Etiquetas	43
3.2.10.	Beneficios del uso de MPLS	45
3.2.11.	Ventajas y desventajas de la tecnología MPLS.....	49
3.2.11.1.	Ventajas	49
3.2.11.2.	Desventajas	52
3.3.	Capítulo 3: Tecnología VPN.....	53
3.4.	Capítulo 4: Centros de Datos	54
3.4.1.	¿Qué es un Centro de Datos?	54
3.4.2.	¿Por qué el Centro de Datos es fundamental?.....	55
4.	Desarrollo	56
4.1.	Introducción.....	56
4.1.1.	Reseña histórica.....	56
4.1.2.	Sedes.....	58
4.1.3.	Descripción informática general	60
4.1.3.1.	Introducción	60
4.1.3.2.	Descripción de la infraestructura de Redes (Internet).....	60
4.1.3.3.	Descripción actual de la Infraestructura de Redes (Intranet)	63

4.1.3.4.	Descripción de la infraestructura de Centro de Datos.....	67
4.1.3.5.	Descripción de la infraestructura de Telefonía.	70
4.1.4.	Descripción del tipo de usuario.....	72
4.1.5.	Conclusiones sobre análisis de las Infraestructuras actuales: Redes (Internet e Intranet), Centro de Datos y Telefonía.....	73
4.2.	Análisis de las opciones encontradas	74
4.2.1.	Infraestructura de Redes (Internet)	74
4.2.1.1.	Internet residencial.....	75
4.2.1.2.	Internet empresarial	76
4.2.1.2.1.	Aspectos a favor.....	76
4.2.1.3.	Internet a través de la red MPLS.....	77
4.2.1.4.	Conclusiones sobre la mejor opción a la problemática para el acceso a internet. .	77
4.2.2.	Infraestructura de redes (Intranet).....	78
4.2.2.1.	Infraestructura basada en el uso de VPN	79
4.2.2.1.1.	Conclusión.....	81
4.2.2.2.	Infraestructura basada en MPLS.....	81
4.2.2.2.1.	Aspectos a favor.....	82
4.2.2.2.2.	Aspectos en contra	82
4.2.2.3.	Conclusiones.....	82
4.2.3.	Infraestructura de Centro de Datos	83
4.2.3.1.	Centro de Datos Centralizado tercerizado	84
4.2.3.1.1.	Aspectos en contra	84
4.2.3.1.2.	Aspectos a favor.....	85
4.2.3.2.	Centro de Datos distribuido tercerizado	85
4.2.3.3.	Centro de Datos distribuido compartido.....	85
4.2.3.3.1.	Aspectos a favor.....	88
4.2.3.3.2.	Aspectos en contra	89
4.2.3.4.	Conclusiones.....	89

4.2.4. Infraestructura de Telefonía.....	89
4.2.4.1. Centralita telefónica virtual.....	90
4.2.4.1.1. Aspectos a favor.....	91
4.2.4.1.2. Aspectos en contra.....	91
4.2.4.2. Centralita telefónica corporativa (IP PBX).....	92
4.2.4.2.1. Aspectos a favor.....	92
4.2.4.2.2. Aspectos en contra.....	93
4.2.4.3. Conclusiones.....	93
4.3. Diseño conceptual final de la solución para la Instituto.....	94
4.3.1. Esquema de conexión de la infraestructura de redes basadas en MPLS.....	94
4.3.1.1. Distribución de los servidores y servicios en los Centros de Datos.....	99
4.3.1.2. Esquema de conexión de la infraestructura de Telefónica.....	101
4.3.1.3. Controles de accesos.....	103
5. Resultados esperables (aspectos medibles).....	105
6. Conclusiones.....	106
7. Bibliografía general y especial.....	108
7.1. Libros.....	108
7.2. Sitios y páginas de Internet.....	108

ÍNDICE DE TABLAS

Tabla 1. Fuente: Elaboración propia.	21
Tabla 2. Fuente: Elaboración propia	53
Tabla 3. Fuente: Elaboración propia	62
Tabla 4. Fuente: Elaboración propia	78
Tabla 5. Fuente: Elaboración propia.	96
Tabla 6. Fuente: Elaboración propia	99
Tabla 7. Fuente: Elaboración propia	103

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Fuente: http://andresyjeffrey.tripod.com/PAGINA/ppp.htm	19
Ilustración 2. Fuente: https://sites.google.com/site/historiayconceptosdelinternet/internet/tipos-de-conexion/adsl	22
Ilustración 3. Fuente: http://es.ccm.net/contents/671-cable	23
Ilustración 4. Fuente: http://exa.unne.edu.ar/informatica/SO/MPLS.PDF	27
Ilustración 5. Fuente: http://exa.unne.edu.ar/informatica/SO/MPLS.PDF	28
Ilustración 6. Fuente: http://exa.unne.edu.ar/informatica/SO/MPLS.PDF	30
Ilustración 7. Fuente: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html	34
Ilustración 8. Fuente: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html	39
Ilustración 9. Fuente: http://calidaddeserviciosteleprocesos.blogspot.com.ar/2016_04_01_archive.html	43
Ilustración 10. Fuente: http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml	44
Ilustración 11. Fuente: https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching	44
Ilustración 12. Fuente: http://slideplayer.es/slide/10897165/	45
Ilustración 13. Fuente: http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/	54
Ilustración 14. Fuente: www.itu.uncu.edu.ar	59
Ilustración 15. Fuente: Elaboración propia	60
Ilustración 16. Fuente: Elaboración propia	63
Ilustración 17. Fuente: Elaboración propia	67

Ilustración 18. Fuente: Elaboración propia	70
Ilustración 19. Fuente: Elaboración propia	88
Ilustración 20. Fuente: Elaboración propia	98
Ilustración 21. Fuente: Elaboración propia	100
Ilustración 22. Fuente: Elaboración propia	101

1. Resumen

La presente tesina tiene como objeto el diseño de un modelo de reestructuración de los sistemas informáticos de transporte de datos y comunicaciones, mediante la utilización de modernas tecnologías WAN como mecanismo de transporte, el cual podrá ser aplicable a cualquier ente u organización que posea una casa matriz o central, con sedes dispersas geográficamente. Se realizara una descripción exhaustiva de las problemáticas encontradas sobre la *infraestructura de transporte de datos y comunicaciones* de un organismo real tomado como caso de estudio. Una vez comprendidas las problemáticas, se procede al *análisis comparativo de las distintas opciones de solución*, esto permitirá la elección de la tecnología que mejor logre la integración de los sistemas informáticos. Se finaliza con el *diseño conceptual final de la solución para la organización* que permita la integración de toda la infraestructura informática.

Palabras clave: Integración, transporte de datos y comunicación, diseño.

2. Introducción

2.1. Problema

Las redes informáticas están cada vez más distribuidas, por la necesidad de cubrir la demanda de mano de obra calificada en diferentes regiones. Debido a esto, el personal que forma parte de las empresas está ubicado en diferentes puntos geográficos. Y al mismo tiempo, con el objetivo de ahorrar dinero cada vez es más habitual tercerizar el resguardo de la información la cual es vital para cualquier organización educativa, provincial, nacional, ya sea en empresas públicas o privadas. Esta tendencia lleva a una situación en la cual sea la organización que sea, en general alojarán sus servicios, pero no sus centros de datos.

Los usuarios están cada vez más lejos de los datos y de las aplicaciones que se ejecutan en la red informática, haciendo que existan muchos problemas para lograr que estas redes distribuidas funcionen bien.

El personal también necesita asegurarse de que sus datos estén protegidos, desde el punto de vista de recuperación en casos de pérdida. Si estos se colocan todos en un solo lugar, habrá una gran cantidad de información que pueda perderse ante un evento que afecte ese emplazamiento, haciendo que sea necesario crear copia de esta en otros sitios.

Existen diversos problemas relacionados al movimiento de los datos, y algunas dificultades se presentan cuando:

- La organización está tratando de hacer una copia de información, pero no puede tener acceso a ella, debido a que los datos no se encuentran disponibles, por encontrarse alojados externamente.
- El personal que se encuentra en un lugar remoto puede no tener acceso a la información, si no cuenta con servicio de internet adecuado.

La mayoría de las iniciativas de diseño más importantes de la actualidad dependen de una WAN de alto rendimiento y fiabilidad. Sin embargo, con mucha frecuencia, el limitado ancho de banda de las WAN disponibles, las largas distancias y la congestión de la red impiden que estas iniciativas prosperen.

2.2. Hipótesis

A través del estudio teórico-conceptual de las características de distintas tecnologías WAN modernas y del adecuado diseño de un modelo de red, aplicando nuevas tecnologías que resuelvan de manera eficiente las problemáticas planteadas, se obtendrán mejoras considerables en la gestión del tráfico de información, entre las sedes o sucursales de una Institución descentralizada geográficamente.

2.3. Justificación

En base a la experiencia personal, sobre los problemas planteados anteriormente, se considera necesario, desde el aspecto técnico, el *diseño de un modelo de reestructuración de sistemas informáticos*, mediante la utilización de alguna tecnología WAN moderna como mecanismo de transporte de la información.

Como segundo enfoque, pero esta vez desde el aspecto práctico, la concreción de dicho diseño lograría que el intercambio de información entre sucursales por múltiples medios sea posible, optimizaría los factores calidad y tiempo en el intercambio de información, reduciría costos por contratos de diferentes proveedores de servicios informáticos y garantizaría la seguridad de la información.

Por lo antes expuesto, el diseño propuesto, pretende ser un modelo para organizaciones, que cumplan con las características de poseer sucursales distribuidas geográficamente, y un gran uso de servicios de información e informáticos propios y externos.

2.4. Objetivos

Los objetivos de la tesina se dividen en: un objetivo general y un conjunto de objetivos específicos.

2.4.1. Objetivo general

El objetivo de esta tesina es diseñar un modelo de reestructuración de sistemas informáticos distribuidos, mediante la utilización de nuevas tecnologías WAN como mecanismo de transporte de la información. El mismo puede ser aplicable a cualquier ente u organización que posea una casa matriz o central, con sedes dispersas geográficamente.

2.4.2. Objetivos específicos

- Recolectar información acerca de las nuevas tecnologías WAN disponibles que puedan ser utilizadas para satisfacer las necesidades del mercado en las áreas de redes privadas virtuales y redes de alto rendimiento, flexibilidad y calidad.
- Estudiar los elementos teóricos y técnicos para uso de las diferentes tecnologías WAN que permitan la resolución integral de la problemática.
- Analizar los aspectos a favor y en contra de las tecnologías elegidas, comparando unas con otras en el campo técnico, administrativo y económico.
- Compilar y estudiar información sobre la infraestructura de los sistemas informáticos del Instituto que se toma como caso de estudio, que incluya: Redes (Internet e Intranet), Centro de Datos y Telefonía.
- Diseñar el esquema de conectividad que permita la articulación integral de todos los sistemas informáticos que son necesarios para el funcionamiento de

la Institución, teniendo en cuenta la información recaudada y los estudios realizados previamente.

2.5. Alcances de la Tesina

La presente tesina se desarrollará tomando como modelo al Instituto de educación terciaria I.T.U.-UNCuyo, el cual posee 8 delegaciones que se encuentran en diferentes ubicaciones geográficas de la provincia de Mendoza, (Mendoza, Luján de Cuyo, Tunuyán, San Rafael, General Alvear, Rivadavia, San Martín), el que presenta toda las dificultades abordadas en los puntos anteriores.

2.6. Estructura Organizativa de la Tesina

Esta tesina ha sido estructurada en 8 secciones, y a continuación se presenta un resumen de los contenidos:

En primer lugar, se exponen cuáles son los problemas detectados sobre los que se basará el diseño del modelo.

En segundo lugar, se plantea la hipótesis a partir de los datos recolectados sobre la infraestructura tecnológica de la Institución elegida que servirán como base para iniciar la investigación.

En tercer lugar, se justifica el motivo del diseño propuesto por ser parte activa en la Institución elegida padeciendo diariamente los problemas de no tener una integración de todos los servicios mediante un red robusta, estable y escalable que interconecte todas Sedes.

En cuarto lugar, se plantean los objetivos de la tesina, que incluyen un objetivo general, el cual apunta a la solución de integral de comunicación basada en la utilización de

alguna tecnología WAN que dé solución definitiva a la problemática y permita crecer en el futuro; y objetivos específicos.

La siguiente sección se inicia con el marco teórico correspondiente, el cual se encuentra dividido en 8 capítulos, conteniendo una descripción precisa de la tecnología MPLS, otras tecnologías WAN y todo lo que contribuya para poder comprender mejor las necesidades expuestas en la problemática.

En sexto lugar, se realiza una descripción de las características generales de la infraestructura tecnológica de la institución que se tomará como base para la generación del modelo, incluyendo una reseña histórica y su ubicación geográfica de todas las sedes.

En séptimo lugar, se continuará con el desarrollo de opciones que permitirán dar solución a la problemáticas. Las mismas serán comparadas para luego elegir la tecnología con la que se logre la integración total de todas las infraestructuras informáticas tanto desde el aspecto técnico como administrativo.

En octavo lugar, se realiza el diseño conceptual que dará sustento a la implementación de la tecnología elegida como la mejor solución en base al estudio realizado en el instituto tomado como ejemplo práctico real para la tesina, con una descripción detallada y esquemática del mismo.

Finalmente, se presentan las conclusiones y recomendaciones que fueron fruto del desarrollo de la presente tesina, así como también la bibliografía consultada y anexos importantes.

3. Marco Teórico

La presente tesina tiene como pauta el diseño de un modelo de reestructuración de los sistemas informáticos de transporte de datos y comunicaciones, mediante la utilización de tecnologías WAN como mecanismo de transporte, el cual sea aplicable a cualquier ente u organización que posea una casa matriz o central, con sedes dispersas geográficamente. El diseño se justifica comenzando con conocer detalladamente cuales son las actuales *tecnologías WAN (Capítulo 1)* disponibles para así poder entender el *mecanismo de transporte de datos del protocolo MPLS (Capítulo 2)*, en el (*Capítulo 3*) se definirá que es y para que se usa la *tecnología VPN* y para finalizar el (*Capítulo 4*) se hará una representación de las características de los tipos de *Centros de Datos*. Posteriormente, y ya fuera de este marco teórico, se realiza una descripción exhaustiva de las problemáticas encontradas sobre la *infraestructura de transporte de datos y comunicaciones del organismo* modelo elegido. Una vez comprendidas las problemáticas, se procederá al *análisis comparativo de las distintas opciones de solución*, y se finalizará con el *diseño conceptual final de la solución para la organización* que permita la integración de toda la infraestructura informática.

3.1. Capítulo 1: Tecnologías WAN (Wide Area Network)

3.1.1. Introducción

En este primer capítulo se exponen los conceptos básicos de una red WAN la cual es utilizada como medio de comunicación de datos que funciona más allá del alcance geográfico de una red LAN (Local Area Network). Una red WAN puede ser construida por o para una organización en particular para uso privado.

3.1.2. Tipos de enlaces: conmutados y dedicados.

3.1.2.1. Enlaces conmutados

Los enlaces conmutados pueden ser de dos tipos: analógicos o digitales.

Los enlaces conmutados analógicos, fue la primer tecnología usada por el hombre para establecer redes privadas. Esto se pudo realizar gracias a la utilización de la Red de Telefonía Pública Conmutada (PSTN), estos enlaces podían llegar a la velocidad de 53 kbps de descarga hasta los 48 kbps de subida.

Los enlaces conmutados digitales, transmiten a mayores velocidades, 64 kbps y 128 kbps, y se los conoce como enlaces RDSI (Red Digital de Servicios Integrados).

3.1.2.2. Enlaces dedicados

Los enlaces dedicados son servicios de comunicación utilizados por empresas mediante la topología punto a punto con velocidades que van desde los 128 kbps hasta los 2 Mbps para el acceso a internet y para la transición de datos.

3.1.3. Topologías WAN

La topología de red es un mapa físico o lógico de una red para el intercambio de datos. Los tipos de topologías que existen son:

- Punto a punto (point to point, PtP) o peer-to-peer (P2P)
- En bus (“conductor común” o bus) o lineal (line)
- En estrella (star)
- En anillo (ring) o circular
- En malla (mesh)
- En árbol (tree) o jerárquica

3.1.4. Tecnologías actuales: PPP, XDSL y Cablemódem.

3.1.4.1. Protocolo PPP (Point-to-Point Protocol)

Es un protocolo de encapsulación de capa 2 que puede ser utilizado tanto en enlaces sincrónicos como en enlaces asincrónicos. El propósito principal del protocolo es transportar paquetes de capa 3 a través de enlaces de datos punto a punto.

Puede proveer:

- Autenticación de conexión.
- Cifrado de transmisión.
- Compresión.

Este protocolo es usado en varios tipos de redes físicas, incluyendo (cable serial, línea telefónica, línea troncal, telefonía celular), especializado en enlace de radio y enlace de fibra óptica como SONET (Synchronous Optical Network). También es utilizado en las conexiones de acceso a Internet de banda ancha. Los proveedores de servicios de Internet (ISP) han usado al protocolo PPP para que accedan a Internet los usuarios de dial-up o en

castellano (línea conmutada), ya que los paquetes de IP no pueden ser transmitidos vía módem, sin tener un protocolo de enlace de datos.

Dos derivados del PPP son:

- Point to Point Protocol over Ethernet (PPPoE).
- Point to Point Protocol over ATM (PPPoA).

Estas son las versión más usadas por los ISP para establecer una línea de abonado digital (Digital Subscriber Line, DSL) de servicios de Internet para clientes.

Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

En la siguiente ilustración se presenta una descripción general de cómo funciona el protocolo PPP.

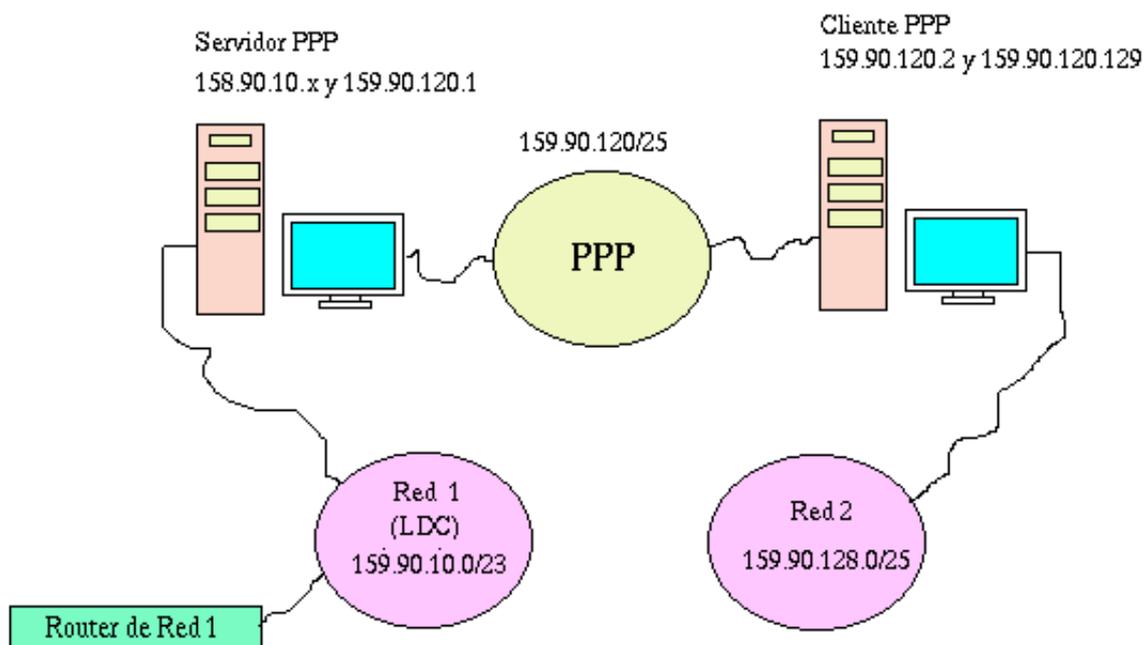


Ilustración 1. Fuente: <http://andresyjeffrey.tripod.com/PAGINA/ppp.htm>

3.1.4.2. Tecnología ADSL

Se conoce como XDSL a la familia de las tecnologías de acceso a internet de banda ancha basadas en la digitalización del bucle de abonados telefónicos. La principal ventaja de XDSL frente a otras soluciones de banda ancha (cablemódem, fibra óptica, etc.) es precisamente que reutiliza la infraestructura de telefonía ya desplegada, por tanto el servicio es más económico al abarcar casi una gran porción de la extensión geográfica entre la población.

El funcionamiento de XDSL se basa en la conversión del par de cobre de la red telefónica tradicional en una línea digital de alta velocidad capaz de soportar los servicios de banda ancha y el envío simultáneo de voz. Para esto se emplean tres canales independientes:

- Dos canales de alta velocidad (recepción de datos y envío de datos).
- Canal para la transmisión de voz.

Cada uno de ellos ocupa una banda de frecuencia diferente, de manera que no interfieran entre sí. El canal de voz se ubica entre las frecuencias de 200Hz y los 3,4KHz se transmiten en banda base, mientras que los canales de datos se encuentran entre las frecuencias que van aproximadamente entre los 24KHz y los 1,1MHz, distribuyéndose de forma variable entre el canal de subida y el de bajada según el tipo de tecnología XDSL empleada. Se transmiten mediante múltiples portadoras.

Para que los usuarios puedan hacer uso del servicio deberán colocar un dispositivo denominado splitter para filtrar la voz de los distintos canales de datos.

La variedad de XDSL más extendida es el ADSL (“Asymmetric Digital Subscriber Line”), su denominación asimétrico es por la relación que existe entre sus canales de Upstream y Downstream dando un mayor rango de frecuencias al canal de bajada y uno menor al canal de subida, esto lo hace ideal para el uso de Internet de alta velocidad, Video on Demand, y acceso a redes remotas LAN, aplicaciones donde típicamente se baja mayor información de la que se sube.

En la siguiente tabla se muestran las características de las diferentes tecnologías XDSL, por otra parte la ilustración 2 explica como es el esquema de conexión básico.

	ADSL	HDSL	SDLS	VDSL
Bits/segundo	De 1,5 a 9 Mbps de download De 16 a 640 Kbps de upload	1,544 o 2,048 Mbps	1,544 o 2,048 Mbps	De 13 a 52 Mbps de download De 1,5 a 2,3 Mbps de upload
Modo	Asimétrico	Simétrico	Simétrico	Asimétrico
Pares de cobre	1	2	1	1
Distancia				
Señalización	Analógica	Digital	Digital	Analógica
Código de línea	CAP/DMT	2B1Q	2B1Q	DMT
Frecuencia	De 1 a 5 MHz	196 KHz	196 KHz	10 MHz
Bits/ciclo	Variable	4	4	Variable

Tabla 1. Fuente: Elaboración propia.

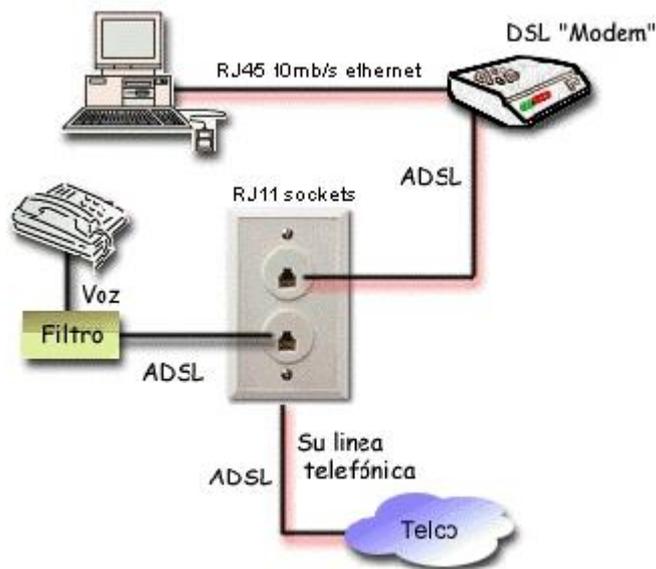


Ilustración 2. Fuente: <https://sites.google.com/site/historiayconceptosdelinternet/internet/tipos-de-conexion/adsl>

3.1.4.3. Acceso a Internet por cable (Cablemódem)

El cablemódem es un tipo especial de módem diseñado para el tratamiento de señales sobre la infraestructura de televisión por cable (CATV).

Estos dispositivos se utilizan para la distribución de Internet de banda ancha aprovechando el ancho de banda que no se utiliza en la red de televisión por cable. Los abonados que se encuentran conectados sobre la misma línea de cable coaxil, comparten el ancho de banda. Esto significa que la velocidad de la conexión dependerá de la cantidad de abonados que se encuentren utilizando el servicio al mismo tiempo.

Este tipo de servicio presenta dos debilidades a tener en cuenta:

1. Se considera una debilidad la idea de compartir la conexión entre múltiples usuarios y además como es importante el asegurar un buen desempeño de la red, se debe tener en cuenta cuán grande es el área geográfica que abarca.

2. Es considerada como la debilidad más importante que las redes de cables son bajas en protección de la privacidad. Es por ello que con la aparición de la tecnología DOCSIS (Data Over Cable Service Interface Specification) se logró mejorar el cifrado de datos y la privacidad.

La siguiente ilustración muestra como es el esquema de conexión de un servicio de CCTV con acceso a internet por medio de cable modem.

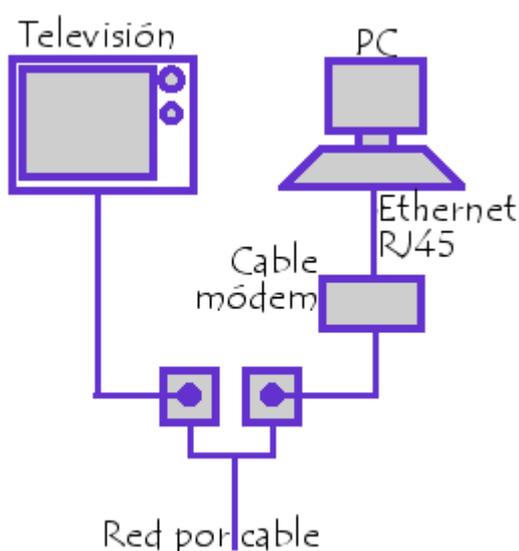


Ilustración 3. Fuente: <http://es.ccm.net/contents/671-cable>

3.1.4.3.1. Ventajas y desventajas

Ventajas

- El rendimiento de la conexión no depende de la distancia de la central respecto del usuario, pudiendo llegar fácilmente a las velocidades reales contratadas.
- Una muy baja latencia o Ping.
- Posibilidad de velocidades superiores a las ADSL.

Desventajas

- Como todas las tecnologías de internet residenciales (DSL, WiMAX, etc.), una capacidad de canal fija es compartida por un grupo de usuarios. Esto significa, la velocidad del servicio puede variar dependiendo de la cantidad de personas que usen el servicio al mismo tiempo.
- Mientras mayor sea la distancia de entre un repetidor, de señal por cable coaxial, mayor será la pérdida de señal lo que provocará una disminución en la velocidad de la conexión.
- Las divisiones de cable por medio de separadores, en el domicilio del abonado puede provocar fallas en el rendimiento de la conexión y en algunos casos la pérdida completa de la señal.

3.2. **Capítulo 2: MPLS (Multiprotocol Label Switching)**

3.2.1. **¿Qué es MPLS?**

“Es un mecanismo de transporte de datos estándar creado por la IETF (Internet Engineering Task Force) y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Multi Protocol Label Switching está reemplazando rápidamente frame relay y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.”¹

¹ https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching, consultada en junio de 2016.

3.2.2. Un poco de historia

“Como se sita en el párrafo anterior, MPLS es un estándar creado por la organización internacional IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es, a veces, algo un poco complejo de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son considerablemente complicadas. Según el interés que se ponga a la hora de explicar sus características y su utilidad, MPLS se puede presentar como un reemplazo de la arquitectura IP sobre ATM; también como un protocolo para hacer túneles; o bien, como una técnica para acelerar el encaminamiento de paquetes. En realidad, MPLS hace un poco de todo eso, debido a que integra sin interrupciones los niveles de enlace y red del modelo OSI, combinando eficazmente las funciones de control del ruteo de nivel 3 con la simplicidad y rapidez de la conmutación de nivel 2. Pero, se debe considerar a MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, resultaría importante revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la aceptación del estándar MPLS.”²

3.2.3. El Camino Hacia la Convergencia de Niveles: IP Sobre ATM

“A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos

² <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>, consultada en junio 2016.

años, estaban contruidos basados en routers conectados por líneas dedicadas T1/E14 y T3/E35. El crecimiento explosivo de internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaba mayores velocidades (155 Mbps) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router se comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la ilustración 4 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

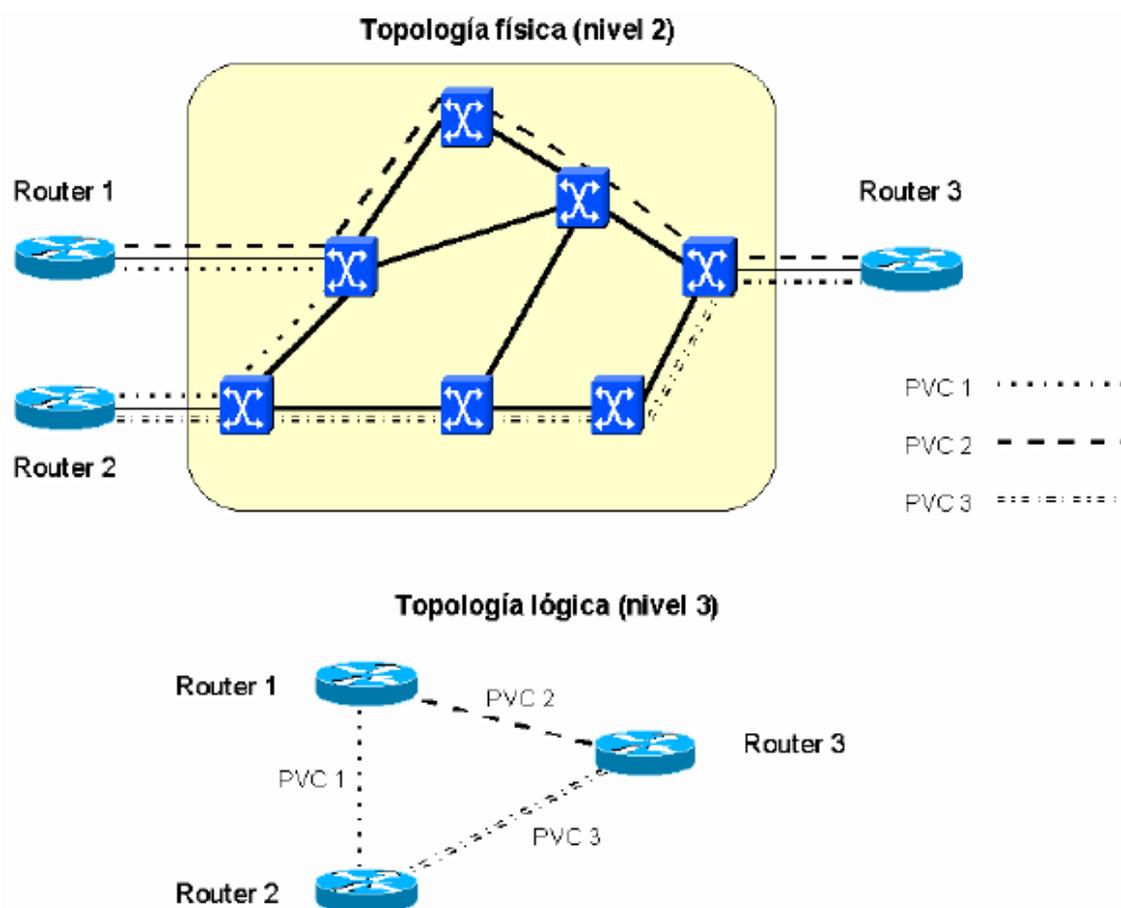


Ilustración 4. Fuente: <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la ilustración 5 se representa el modelo IP/ATM con la separación de funciones entre los que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura

física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

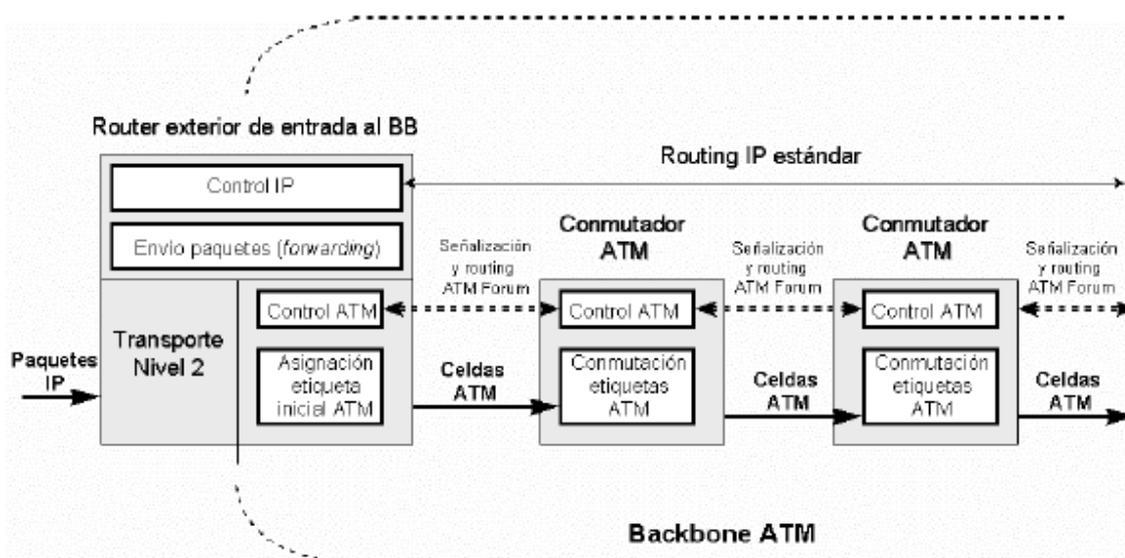


Ilustración 5. Fuente: <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de primer nivel (la mayor parte telcos), ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de las necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio).

La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par

de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

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

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

3.2.4. Un Paso Más en la Convergencia Hacia IP: Conmutación IP

“La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señaladas anteriormente. Esas técnicas se conocieron como "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas —entre las que merecen citarse: IP Switching

³ <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>, consultada en junio 2016.

de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba— condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

- La separación entre las funciones de control (routing) y de envío (forwarding).
- El paradigma de intercambio de etiquetas para el envío de datos.

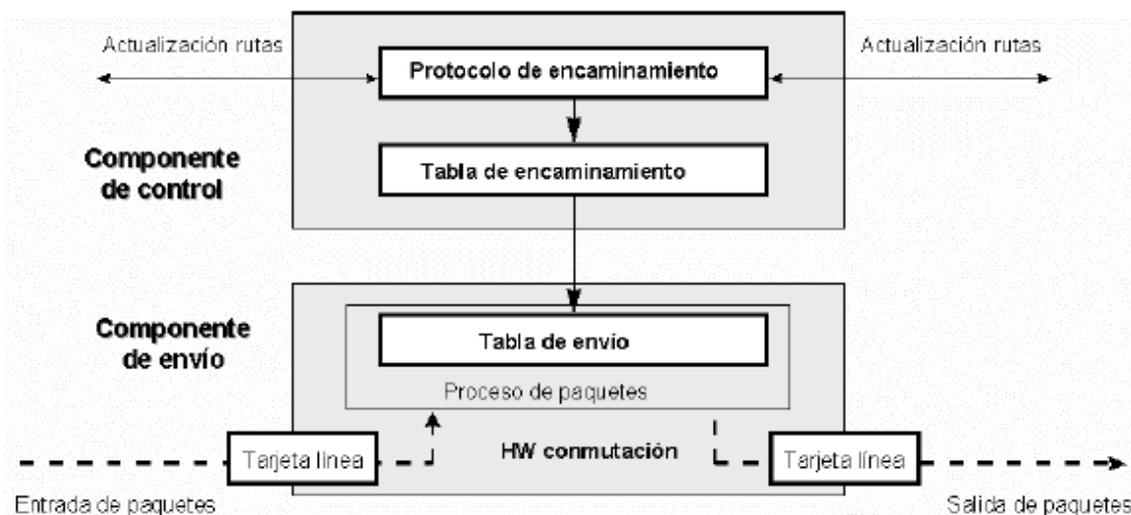


Ilustración 6. Fuente: <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>

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

interfaz de entrada al de salida a través del correspondiente hardware de conmutación. Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.”⁴

3.2.5. Convergencia real: MPLS

“Como se dijo anteriormente, el principal problema que presentan las numerosas tecnologías de conmutación multinivel era la falta de interoperabilidad entre productos privados de distintos fabricantes. La mayoría de las soluciones necesitaban ATM como transporte, dado que no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LAN). Por lo tanto, lo que se quería obtener era un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de capa de enlace.”⁵

3.2.6. Ideas preconcebidas sobre MPLS

“Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas equívocas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio (Circuito Integrado para Aplicaciones Específicas o ASIC, por sus siglas en inglés) permiten a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente

⁴ <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>, consultada en junio 2016.

⁵ <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>, consultada en junio 2016.

el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF.

Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP (Resource Reservation Protocol).
- MPLS debía permitir el crecimiento constante de Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

También ha habido quien pensó que MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en Internet por los siguientes motivos:

- El filtrado de paquetes en los firewall de acceso a las LAN corporativas y en los límites de las redes de los NSPs (Network Service Provider) es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.
- No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.

- Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.
- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.”⁶

3.2.7. Aplicaciones de MPLS

MPLS ofrece elementos para manipular el tráfico de diferentes aplicaciones con requerimientos de Calidad de Servicio QoS (Quality of Service), optimización del uso de recursos mediante Ingeniería de Tráfico TE (Traffic Engineering) y seguridad mediante Redes Privadas Virtuales VPN (Virtual Private Network).

- Ingeniería de Tráfico - TE
- Calidad de Servicio - QoS
- Redes Privadas Virtuales – VPN

Se observarán rápidamente las características de estas aplicaciones y las ventajas que MPLS presume para ello frente a otras soluciones tradicionales.

3.2.7.1. Ingeniería de tráfico - TE

“El objetivo básico de la Ingeniería de Tráfico (TE) es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar la utilización de estos recursos de la

⁶ <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>, consultada en junio 2016.

forma más óptima posible de manera que no haya algunos que estén muy utilizados con posibles cuellos de botellas, mientras que otros estén casi sin ser utilizados. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP (Interior Gateway Protocol) correspondiente. En caso de congestión en alguno de los enlaces, el problema se resolvía añadiendo más capacidad a los enlaces. La Ingeniería de Tráfico (TE) permite trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces menos congestionados, aunque estén fuera de la ruta más corta (menos saltos).

La siguiente ilustración compara dos tipos de rutas para el mismo par de nodos origen-destino.

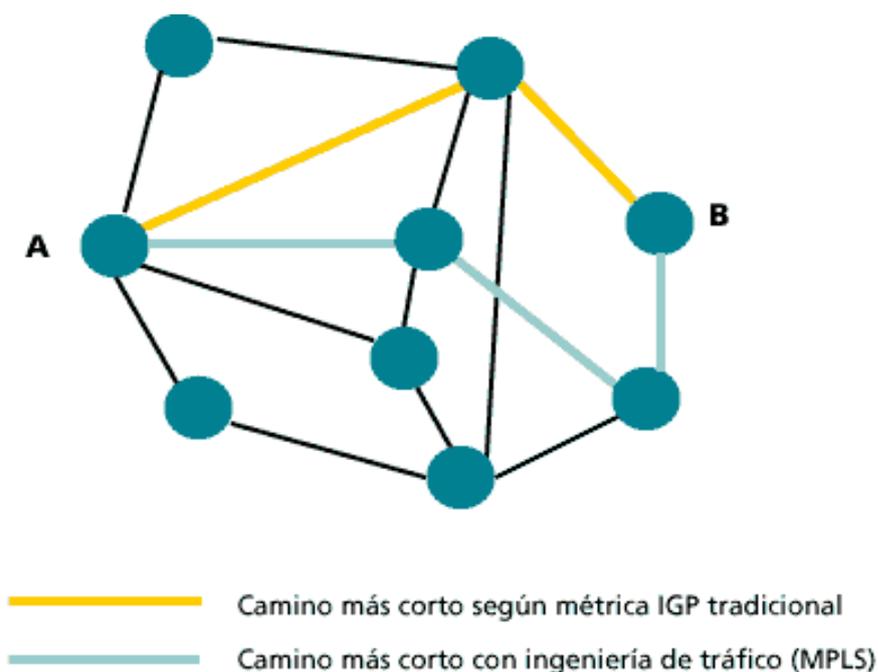


Ilustración 7. Fuente: <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>

El camino más corto entre A y B según la métrica normal de IGP es el que tiene solo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga recomendable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en backbones grandes, porque:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la Ingeniería de Tráfico (TE) en MPLS es que se puede hacer directamente sobre una red IP, todo esto de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.”⁷

3.2.7.2. Calidad de Servicio - QoS

“MPLS está diseñado para poder gestionar servicios diferenciados, según el modelo DiffServ (Servicios Diferenciados) del IETF. Este modelo delimita una variedad de elementos para poder clasificar el tráfico en un pequeño número de clases de servicios con diferentes preferencias. Según sean los requisitos del usuario, DiffServ permite diferenciar servicios tales como: WWW, correo o transferencia de archivos, de otras aplicaciones muchos más sensibles al retardo como son el video y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

⁷ <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>, consultada julio 2016.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, debido a:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo: un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, que, lógicamente, tendrán distintos precios.”⁸

3.2.7.3. Redes virtuales privadas - VPN

“Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones internas y externas, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráfico por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo

⁸ <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>, consultada julio 2016.

de solución presentan, es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costos asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec del IETF
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para

asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- Están basadas en conexiones punto a punto (PVCs o túneles)
- La configuración es manual
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales
- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar

de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una intranet entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En la ilustración 5 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

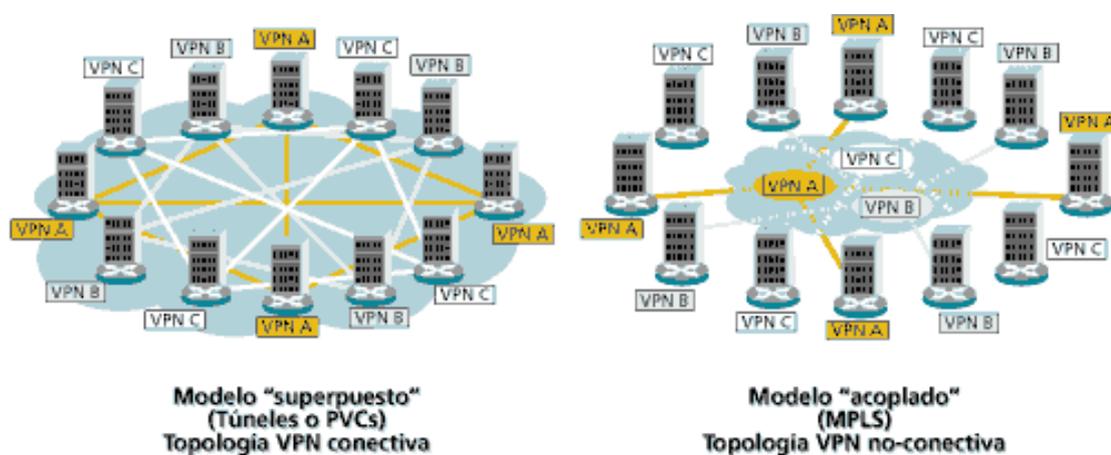


Ilustración 8. Fuente: <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router.
- Tiene mayores opciones de crecimiento modular.
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.”⁹

⁹ <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>, consultada julio 2016.

3.2.8. Comparación entre Enrutamiento convencional y Conmutación de etiquetas

“El protocolo IP (Internet Protocol) es un protocolo de capa de red no orientado a la conexión y no confiable. En una red IP tradicional, los paquetes IP no se catalogan, no se marcan, y no pueden procesarse de diferentes maneras. Estos viajan desde un router al siguiente, y cada router toma una decisión de reenvío independiente para cada paquete. Todos los routers tienen su propia tabla de ruteo construida estáticamente o mantenida por un algoritmo de ruteo dinámico de capa de red que se ejecuta en cada uno de ellos. De esta forma, un router IP independientemente selecciona el siguiente salto para el paquete, basándose en el análisis del encabezado del paquete y en la tabla de ruteo. Esto significa que los paquetes fluyen por la red sin rutas predeterminadas.

Internet provee de un servicio de transporte de datos conocido como de “mejor esfuerzo”, pero no es plausible para aplicaciones que requieren un servicio de transporte de datos con ciertas condiciones. Por ejemplo, aplicaciones de tiempo real, videoconferencia, etc. Es por ello que es necesario incorporar cambios tecnológicos que puedan proporcionar una respuesta menos aleatoria.

MPLS resuelve este problema, integrando sin discontinuidades los niveles de capa de enlace y de red, y combina eficazmente las funciones de control de ruteo con la simplicidad y rapidez de la conmutación de nivel de capa de enlace. Además funciona sobre cualquier tecnología de capa de enlace. MPLS puede agregar capacidades notables a las redes IP existentes en la actualidad, incluyendo: Ingeniería de tráfico; Proveer tráfico con diferentes Clases de Servicios (CoS); Proveer tráfico con diferente Calidad de Servicio (QoS); y Proveer Redes Privadas Virtuales (VPN) basadas en IP. Cuando los paquetes ingresan a una red MPLS, son etiquetados por los LER (Label Edge Router). Cada paquete tiene una pila de etiquetas, y cada una de ellas identifica una FEC (Forwarding Equivalence Class). Una FEC es un grupo de paquetes que son reenviados de la misma manera. Por ejemplo, sobre el mismo camino, y con el mismo tratamiento de reenvío. Cada paquete sigue una ruta predeterminada llamada LSP (Label Switched Path) dependiendo de la FEC que tiene

asignada. Un LSP se relaciona con un solo nivel de la jerarquía. Los LSP son unidireccionales, es decir, dos LSP son necesarios para comunicación duplex. Cada dispositivo que atraviesa el paquete es llamado LSR (Label Switching Router). Un LER es un LSR de ingreso o egreso. En MPLS, la asignación de un paquete a una FEC se realiza una sola vez, cuando el paquete ingresa a la red. En los saltos subsecuentes, no hay un análisis adicional del encabezado de capa de red de los paquetes. La etiqueta es utilizada como un índice dentro de una tabla que especifica el siguiente salto, y una nueva etiqueta. La etiqueta anterior es reemplazada con la nueva, y el paquete es reenviado a su siguiente salto. No siempre se reemplaza una etiqueta, también pueden apilarse para soportar un diseño de ruteo jerárquico, y por supuesto, otras veces simplemente serán desapiladas.”¹⁰

3.2.9. Componentes de una red MPLS

A continuación se esquematiza como están distribuidos los dispositivos dentro del dominio MPLS:

¹⁰http://sedici.unlp.edu.ar/bitstream/handle/10915/21310/Documento_completo.pdf?sequence=1, consultada en julio 2016.

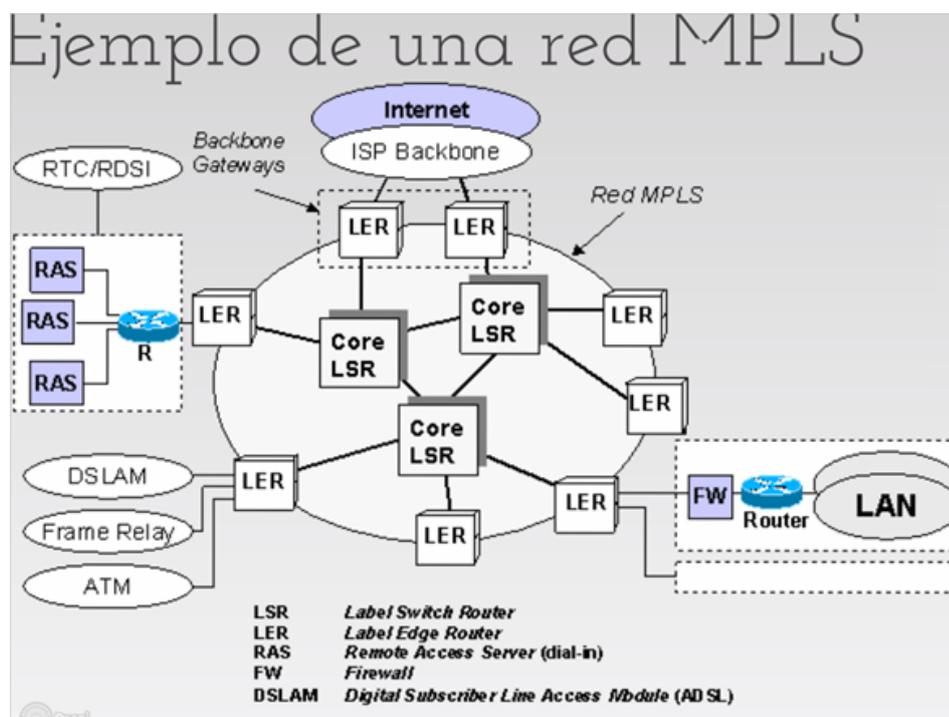


Ilustración 9. Fuente: http://calidaddeservicioteleprocesos.blogspot.com.ar/2016_04_01_archive.html

- **LER (Label Edge Router):** Router (encaminador) de borde, añade y retira etiquetas y luego los envía al dominio MPLS.
- **LSR (Label Switching Router):** Router (encaminador) de conmutación de etiquetas en el dominio MPLS.
 - Utiliza protocolos de ruteo IP para el intercambio de rutas.
 - Utiliza el protocolo de distribución de etiquetas LDP (Label Distribution Protocol) para distribuir rutas.
- **L (Label):** Etiqueta.
- **LSP (Label Switched Path):** Se llama así a los caminos virtuales que son unidireccionales. Cada LSP se crea de un LER a otro.

3.2.9.1. Etiquetas

La ilustración 7 es una etiqueta MPLS, comprendida por un campo de 32 bits con una determinada estructura.

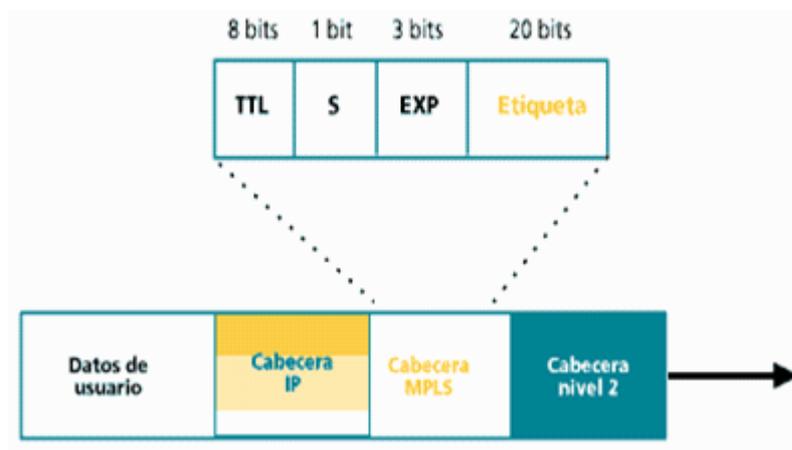


Ilustración 10. Fuente: <http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml>

- Valor de la etiqueta de 20 bits.
- Prioridad de Calidad de Servicio (QoS) de 3 bits. También llamados bits experimentales.
- Bandera de "fondo" de la pila de 1 bit.
- Tiempo de Vida (TTL) de 8 bits.

Al conjunto de etiquetas se le llama pila o "stack".

Los routers MPLS podrían necesitar más de una etiqueta para formar un paquete y encaminarlo a través de la red MPLS. Esto se realiza gracias al apilado de etiquetas. La primera etiqueta de la pila recibe el nombre de top label o etiqueta más externa y la última es la bottom label o etiqueta más interna. Entre ambas puede haber cualquier número de etiquetas.



Ilustración 11. Fuente: https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching.

Se observa que en la pila de etiquetas de la ilustración 8, el bit BoS está puesto a 0 en todas las etiquetas menos en la bottom label, donde su valor es 1.

Estos paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP, la búsqueda de etiquetas y el envío por etiquetas eran más rápido que una búsqueda RIB (Base de información de Ruteo), porque esta búsqueda se realiza en los switch (conmutadores).

Además, MPLS puede ser usada sobre cualquier protocolo de capa de enlace, como se demuestra en la ilustración 9:

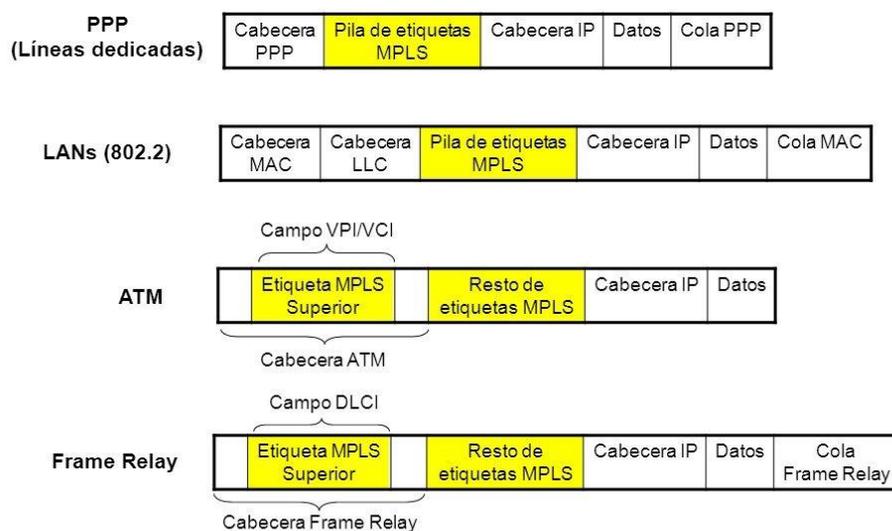


Ilustración 12. Fuente: <http://slideplayer.es/slide/10897165/>

3.2.10. Beneficios del uso de MPLS

A continuación se darán 10 beneficios claves a la hora de analizar una migración hacia MPLS.

1. Flexibilidad.

Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se

montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera) realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

2. Escalabilidad.

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

3. Accesibilidad.

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

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

4. Eficiencia.

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

5. Calidad de servicio (QoS) y Clases de servicio (CoS).

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

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

6. Administración.

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

7. Monitoreo y SLAs.

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

8. Fácil Migración.

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

9. Seguridad.

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

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

10. Bajo Costo.

Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "más por menos", entre ellos podemos destacar:

1- Independencia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.

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

3.2.11. Ventajas y desventajas de la tecnología MPLS

3.2.11.1. Ventajas

- “La conmutación de paquetes mediante el uso de etiquetas es un proceso más rápido que el encaminamiento basado en el análisis de la cabecera.
- La clasificación del paquete dentro de una clase de equivalencia particular es posible realizarla atendiendo diversos criterios y no sólo el valor de su dirección de destino; por ejemplo, examinando otros campos de la cabecera de red, de la cabecera de transporte o de aplicación, el puerto de entrada en el dispositivo de encaminamiento, etc.
- Se admite mayor complejidad en el proceso de clasificación, sin que esto tenga impacto en los dispositivos de encaminamiento intermedios, ya que estos solo se encargan de encaminar paquetes etiquetados. Es suficiente con añadir esta funcionalidad en los dispositivos de encaminamiento que se encuentran en la entrada del dominio. El sistema resulta, por consiguiente, fácilmente escalable.

- La clasificación de un paquete puede atender a la calidad de servicio con que se desea que éste se propague en la red, asignándose etiquetas distintas para cada clase de servicio. El valor de la etiqueta determinará cómo son tratados los paquetes de esa clase (su disciplina de servicio, si son descartados en caso de congestión, etc.). Adoptando esta estrategia, el protocolo MPLS se utiliza para proporcionar servicios semejantes a los servicios diferenciados.
- El uso de etiquetas simplifica la gestión de rutas explícitas cuyo establecimiento puede formar parte de la ingeniería del tráfico en la red. Las rutas explícitas sirven también para emular circuitos virtuales sobre una tecnología no orientada a la conexión.
- Un aspecto de MPLS con impacto significativo es su capacidad de proporcionar un encaminamiento jerárquico, gracias a la posibilidad de encapsular un “camino” LSP en otro, mediante la anidación de etiquetas, sin necesidad de eliminar la identificación del camino LSP original, de resolución más fina. Diversos caminos LSP con características dispares pueden ser agregados, transportados juntos en la red central y finalmente, separados en caminos individuales, simplemente añadiendo y eliminando una etiqueta. La resolución permanece al pasar a la periferia, donde es relevante, pero queda oculta en la red tránsito central, donde podría dificultar el escalamiento. Una aplicación directa de esta habilidad es la implantación de redes conmutadas MPLS que sirvan como redes de tránsito para paquetes de cualquier tipo de protocolo, incluyendo IP o el mismo MPLS.
- Las aplicaciones que comprenden el envío de flujos en tiempo real son extremadamente sensibles a las fluctuaciones en el retardo. Para estas aplicaciones, las modificaciones en el camino seguido por los paquetes resultan muy perjudiciales, pues alteran el retardo que éstos sufren. Cuando los flujos son transportados sobre un camino conmutado MPLS, éste permanece inalterable ante los cambios en la tipología y condiciones de red, reduciendo las llamadas fluctuaciones.

- Finalmente, el modelo MPLS simplifica las tareas de monitorización del tráfico, ya que los paquetes pertenecientes a una misma clase de equivalencia FEC son fácilmente identificables gracias a su etiqueta.
- Se puede realizar la instalación de un dispositivo de Seguridad Multiuso en cada punto de la Red (Solución UTM “Gestión Unificada de Amenazas”, la cual integra funciones de seguridad como cortafuegos, antivirus, detección y prevención de intrusos.
- Gracias a la tecnología de etiquetado de MPLS, el tráfico se mueve de forma eficaz a través de la Red del proveedor de Servicios, es decir ofrece un rendimiento sólido de Ancho de Banda y garantías de nivel de Servicio.
- MPLS es una tecnología reciente que se utiliza en la sustitución de ATM o Frame Relay para la conexión de grandes emplazamientos.
- MPLS tiene la capacidad de almacenar una ruta secundaria, al fallar la ruta principal simplemente reenruta el tráfico por la ruta secundaria.
- Utiliza una combinación de etiquetado por paquetes con Conmutación punto a punto orientado a conexiones para añadir más seguridad.
- En términos de Calidad de Servicio (QoS), MPLS ofrece un ancho de Banda garantizado entre el emplazamiento y la Red del Proveedor de Servicios, ya que fue diseñado para ofrecer prestaciones de Clases de Servicios (CoS), es decir separar el flujo de datos en video, VoIP y datos.
- MPLS es una solución versátil para resolver los problemas a los que se enfrentan las redes actuales: velocidad, escalabilidad, gestión de la calidad de servicio e ingeniería de tráfico.

- MPLS tiene la capacidad de definir trayectos para diferentes tipos de tráfico a través de una red, a lo que se llama diseño del tráfico y la creación de túneles IP a través de una red, lo que facilita la creación de Redes Privadas Virtuales (VPN).

3.2.11.2. Desventajas

- En primer lugar, uno de los argumentos esgrimidos a favor de desarrollar MPLS, el incremento en la velocidad de proceso en los dispositivos de encaminamiento, ha declinado con la aparición de nuevos equipos más rápidos y potentes, como los denominados “Gigabit routers”.
- La Internet actual se caracteriza por poseer un elevado grado de fiabilidad, derivado de la naturaleza sin conexión del protocolo IP. Por otra parte, los protocolos de encaminamiento dinámico han sido diseñados para reaccionar frente a los potenciales fallos modificando las rutas seguidas por los paquetes. Sin embargo, el esquema MPLS es orientado a la conexión, lo que implica una mayor vulnerabilidad en situaciones de fallo. Por esta razón, resulta conveniente introducir mecanismos de recuperación de faltas asociadas a la arquitectura MPLS: notificación a los dispositivos de encaminamiento afectados, búsqueda de rutas alternativas, desvío del tráfico a las mismas, etc.
- Si bien la posibilidad de apilar múltiples etiquetas aporta beneficios indudables, el incremento de la proporción de cabecera transportada contribuye a reducir el rendimiento de la red.
- Identificar mediante una etiqueta la calidad de servicio deseada no implica que esta solicitud se satisfaga. Es imprescindible que las tecnologías de red subyacentes provean los mecanismos necesarios para garantizar dicha calidad.
- MPLS está limitado al ámbito de conectividad de la Red del proveedor de Servicios.

Comparadas con las redes IP puras, que requieren largos periodos de tiempo para reconfigurar y reconstruir tablas de enrutamiento, los LSP (trayectos conmutados por etiquetas) de MPLS pueden configurarse por adelantado para desviar el tráfico en caso de que se produzcan problemas en un trayecto primario y ofrecer así recuperaciones en 50-80 ms.

Tal y como se puede observar en la tabla 1, las VPNs basadas en MPLS pueden ofrecer una seguridad comparable, e incluso superior a las VPNs tradicionales basadas en Frame Relay o ATM.”¹¹

	MPLS	ATM – FRAME RELAY
Enrutamiento y separación de tráfico	SÍ	SÍ
Ocultación del núcleo de la infraestructura	SÍ	SÍ
Resistencia ante ataques	SÍ	SÍ
Resistencia a Spoofing de etiquetas	SÍ	SÍ
Cifrado de Datos	OPCIONAL	OPCIONAL

Tabla 2. Fuente: Elaboración propia

3.3. Capítulo 3: Tecnología VPN

“Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que de otro modo, no podrían. Sin embargo, conectar la computadora

¹¹<http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/1311/0046T172.pdf;jsessionid=7CB17992C04DEF816090DDF924E5F86D?sequence=1>, consultada en julio 2016.

de un empleado a los recursos corporativos es solo una función de una VPN. En conjunto con lo anterior, una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información.”¹²

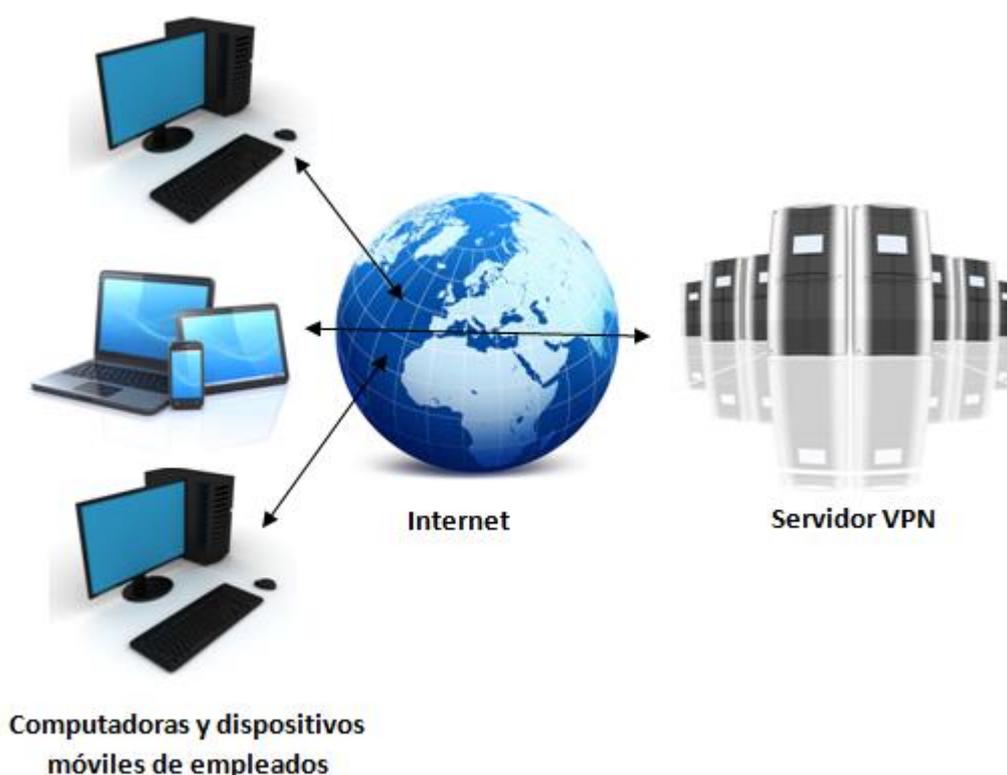


Ilustración 13. Fuente: <http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>

3.4. Capítulo 4: Centros de Datos

3.4.1. ¿Qué es un Centro de Datos?

Un centro de datos es un espacio exclusivo donde las empresas, las organizaciones, etc., mantienen y operan las infraestructuras TIC que utilizan para el procesamiento de datos e información sistematizada. Es el espacio donde se alojan los servidores y sistemas de almacenamiento en donde se ejecutan las aplicaciones y se procesan y almacenan los datos y el contenido.

¹²<http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>, consultada en septiembre 2016.

Un Centro de Datos ofrece espacio para el hardware en un ambiente controlado, por ejemplo, utilizando aire acondicionado para permitir que los equipos tengan el mejor nivel de rendimiento.

Poseen sistemas de comunicación redundantes que se activan en el caso de que falle el vínculo primario.

El principal objetivo de un Centro de Datos es el ejecutar las aplicaciones centrales de la empresa u organización y almacenar datos operativos, además de ofrecer medios de recuperación de desastres.

Los componentes más habituales incluyen firewalls, gateways VPN, routers y conmutadores, servidores de bases de datos, servidores de archivos, servidores de aplicaciones, servidores web y todos en hardware físico y virtualizadas.

3.4.2. ¿Por qué el Centro de Datos es fundamental?

La mayoría de las implementaciones de Centros de Datos se hacen por los siguientes motivos:

- **Disponibilidad:** maximizar la disponibilidad de los servicios IT (tecnología de la información) para la empresa, la organización, etc.
- **Continuidad:** la redundancia, el monitoreo y la infraestructura ofrecida por la mayoría de los Centros de Datos significa que la posibilidad de interrupción de las actividades es muy baja.
- **Seguridad:** Mantener la seguridad física, conservar los sistemas bajo llave y proporcionar la entrada solo al personal autorizado. Es importante recalcar que los activos más valiosos de cualquier empresa se encuentran en el centro de datos, además de las personas.

4. Desarrollo

4.1. Introducción

De acuerdo a lo planteado en los objetivos específicos, en esta sección se expondrá inicialmente un resumen de las características de la Institución elegida como caso de estudio, esto abarca: su historia, la ubicación geográfica de las sedes y la descripción de la infraestructura de transporte de datos y comunicaciones actuales, esto incluye elementos tales como: Redes (Internet e Intranet), Centro de Datos y Telefonía.

Posteriormente se analizarán diferentes tecnologías WAN que mediante la comparación de sus características técnicas, administrativas y económicas, permitiría la elección de la tecnología que mejor logre la integración de los sistemas informáticos.

Se finalizará esta sección con el desarrollo del diseño conceptual del modelo de conectividad aplicado a la Institución que permitirá la integración de todos los sistemas informáticos.

4.1.1. Reseña histórica

“La historia del “ITU” comienza en 1971, año en que la Universidad Nacional de Cuyo realiza el primero de los trabajos para analizar la problemática de los estudios cortos en el Nivel Superior, y en particular en el ámbito Universitario.

En 1982, un equipo de planificadores y educadores universitarios, realiza un trabajo de síntesis y propuesta basado en el estudio anterior y su actualización.

A partir de 1991, se realizan numerosos contactos y reuniones de estudio y programación, de las que participan el Ministerio de Cultura, Ciencia y Tecnología, la Dirección General de Escuelas y el Ministerio de Economía de la Provincia de Mendoza, las Direcciones de Cultura de diversos municipios de la provincia y la Universidad Nacional de Cuyo.

Como resultado de contactos y reuniones, teniendo en cuenta las demandas ocupacionales y articulando los intereses sectoriales del Gobierno de la Provincia, la Universidad Nacional de Cuyo, los Municipios y las Empresas, se concreta el 27 de octubre de 1993, la firma del Convenio que da origen al Instituto Tecnológico Universitario.

En 1994, comienzan las actividades académicas del Instituto Tecnológico Universitario, con un abanico de carreras cortas de nivel Superior, distribuidas actualmente, de acuerdo con las demandas zonales, en Mendoza Capital, Luján de Cuyo, San Rafael, Tunuyán, General Alvear, Rivadavia. Posteriormente se abrió una Sede en San Martín.

A estos servicios educativos formales de carreras cortas de nivel superior, vinculados estrechamente con los sectores productivos y de servicio, se le suman otros servicios de educación continua, capacitación a personal de empresas, actividades de investigación y desarrollo, diseño de materiales educativos, asesoramiento y servicios a Instituciones públicas y privadas, etc.

El ITU, inicialmente, estuvo a cargo de una Fundación, cuyos creadores fueron el Gobierno de la Provincia de Mendoza, la Universidad Nacional de Cuyo y su Fundación, que participan en el Consejo de Administración junto a la UCIM, La Universidad Tecnológica Nacional y la Federación Económica de Mendoza.”¹³

¹³ <http://www.itu.uncu.edu.ar/>, consultada en abril 2016.

4.1.2. Sedes

El ITU cuenta con 8 sedes con presencia en toda la provincia de Mendoza.

- **Mendoza**

Sede Central – Facultad de Ingeniería – UNCuyo

Predio Universitario - Ciudad de Mendoza

- *Sede Campus TIC*

Parque Gral. San Martín - Lencinas s/n - Ciudad de Mendoza

- *Luján de Cuyo*

Sede Facultad Ciencias Agrarias - UNCuyo

Alte. Brown 500 - Chacras de Coria - Mendoza

- **Este**

Sede Rivadavia

José Hernández 210 - Rivadavia - Mendoza

- *Sub-Sede San Martín*

25 de Mayo 630 - San Martín - Mendoza

- **Valle de Uco**

Sede Tunuyán

Alem y Sarmiento - Tunuyán - Mendoza

- **Sur**

Sede General Alvear

Chapeaurouge 163 - General Alvear - Mendoza

- *Sub-Sede San Rafael*

Bernardo Irigoyen 343 - San Rafael - Mendoza

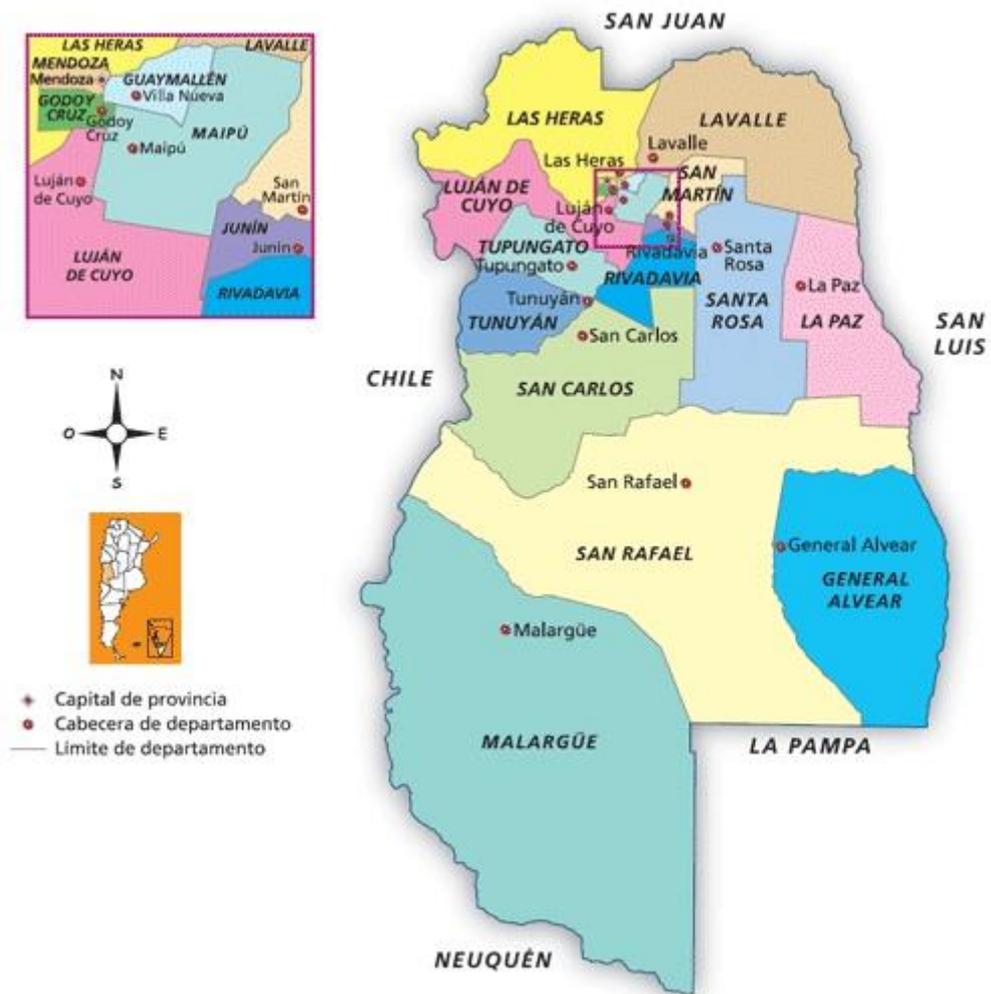


Ilustración 14. Fuente: www.itu.uncu.edu.ar

4.1.3. Descripción informática general

4.1.3.1. Introducción

En este punto se comenzará con la descripción de la que es en la actualidad la infraestructura informática de transporte de datos y comunicaciones de la organización tomada como caso de estudio. Se identificarán a cada una de las sedes, y se expondrán las problemáticas que se detectaron durante el estudio realizado.

Las infraestructuras informáticas que serán motivo de análisis abarca elementos tales como: Redes (Internet e Intranet), Centro de Datos y Telefonía.

4.1.3.2. Descripción de la infraestructura de Redes (Internet)

La ilustración 12, muestra como es la situación actual de las sedes para poder hacer uso del servicio de Internet.

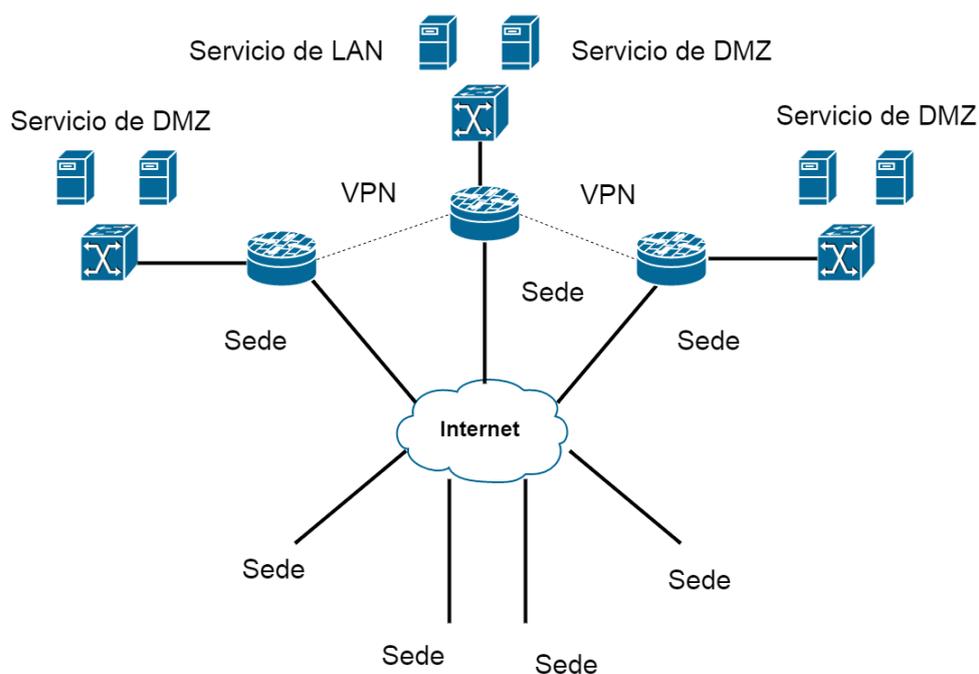


Ilustración 15. Fuente: Elaboración propia

Si bien las 8 Sedes cuentan con algún tipo de servicio de internet provisto por algún ISP, estas conexiones pueden ser de diferentes tecnologías como ADSL, cablemódem, acceso inalámbrico, etc.

Además, existe otra alternativa para tener acceso a internet, y es a través de la UNCuyo. Este tipo de servicio solamente puede ser utilizado por las sedes que comparten físicamente el espacio dentro del campus de la universidad ya que pueden hacer uso de la misma red LAN o MAN. Más adelante sabremos cuales son estas sedes.

A continuación, en la tabla 2, se definen las particularidades de los servicio de Internet. Se especifican características tales como: sede, ubicación, proveedor y ancho de banda.

Sede	Ubicación geográfica	Proveedor	Ancho de Banda
CAMPUS UNCuyo	Fac. De Ingeniería, Edificio de Aulas Universidad Nacional de Cuyo, Ciudad de Mendoza.	Suministrado por la UNCuyo.	10Mbps
CAMPUS TIC	Lencinas s/nro., Ex Predio Eureka, Parque General San Martín, Ciudad de Mendoza.	Suministrado por la WAN del Gobierno de Mendoza.	10Mbps
LUJÁN DE CUYO	Facultad Ciencias Agrarias UNCuyo, Alte.Brown 500, Chacras de Coria, Luján de Cuyo.	Provisto por la empresa ITC.	8Mbps.
TUNUYAN	Alem y Sarmiento, Tunuyán, Mendoza.	De tipo ADSL provisto por SPEEDY.	3Mbps.
ESTE	SEDE RIVADAVIA: José Hernández 210, Rivadavia. SEDE CAMPUS UNIVERSITARIO SAN MARTIN: 25 de Mayo 630, - San Martín.	De tipo ADSL provisto por SPEEDY	6Mbps.
SEDE GENERAL ALVEAR	ubicada en Chapeaurouge 163(M5620DFC) - General Alvear, Mendoza	Provisto por la cooperativa CECSAGAL	3Mbps.
SEDE SAN RAFAEL	Bernardo Irigoyen 343, San Rafael.	Suministrado por la UNCuyo	6Mbps

Tabla 3. Fuente: Elaboración propia

Como se puede observar en la tabla 2, las sedes utilizan diferentes tecnologías para acceder a Internet.

Desde el punto de vista práctico, el conectarse a Internet usando diferentes tecnologías tiene consecuencias de diferentes tipos: económicas, de tiempo, de eficiencia, etc. Incluso existen, en la práctica, restricciones físicas al tipo de conexión al que podemos acceder, de modo que cuando se dispone de varias posibilidades no está de más tener algunos elementos de reflexión para seleccionar la más conveniente.

Entonces, de acuerdo a lo expresado en el párrafo anterior, se deberá buscar una alternativa de solución que logre que los accesos a Internet para todas las sedes sean suministrados por un mismo proveedor y que sean de la misma tecnología. Esto permitiría integrar las características del tipo: económicas, de tiempo, de eficiencia y administrativas.

4.1.3.3. Descripción actual de la Infraestructura de Redes (Intranet)

La ilustración 13, muestra como es la situación actual de la infraestructura para hacer uso de los sistemas y los servicios de la Intranet.

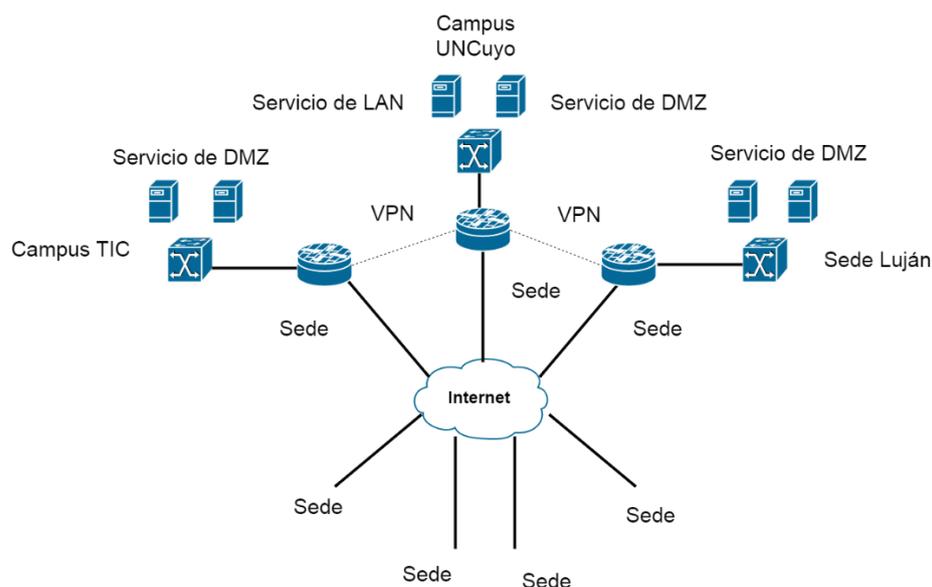


Ilustración 16. Fuente: Elaboración propia

Una Intranet es una red informática que sirve para compartir información y hacer uso de los servicios de red (DNS, DHCP, Servicio de directorios, Servicios de Impresión, etc.) dentro de una organización. Estos servicios son uno o más servidores que permiten compartir recursos a computadoras clientes.

Además, nos encontramos con diferentes aplicaciones informáticas, (la aplicación es un tipo de programa informático diseñado como herramienta para realizar algún tipo de tarea propia del trabajo).

En este punto el enfoque estará centrado en la descripción de los siguientes dos puntos: sistemas de uso interno y externo y servicios de red de la Institución.

Un sistema de uso interno significa que solamente puede ser accedido por medio de la Intranet, en cambio un sistema de uso externo puede ser utilizado tanto desde la Intranet como desde Internet.

El primer punto se centrará en la descripción de los sistemas de uso internos y externos encontrados.

- Sistemas de gestión SITU

- Este es sin dudas uno de los puntos más fuertes, donde es necesario contar con una red LAN entre todas las sedes que sea bien robusta y estable. Los sistemas de uso privado son utilizados para incorporar datos importantes de: personal, clientes, datos económicos, etc., lo que significa tener aplicativos web, por ejemplo, y detrás una o más bases de datos. Si no se poseen buenos sistemas de seguridad y buenas prácticas de programación lo más probable es que el sistema sea fácil de hackear provocando pérdidas o daños en los datos que son vitales para el Instituto. Como se dijo anteriormente, solo 3 Sedes pueden hacer uso de los sistemas por la LAN y el resto utilizan Internet para acceder. Las buenas prácticas de seguridad Informática recomiendan que los sistemas internos estén en un entorno controlado dentro de una LAN de servidores donde se vigilen los accesos tanto del personal que lo mantiene, como el personal que lo usa, permitiendo incorporar diferentes políticas de control y calidad en el todo el tráfico hacia los sistemas de uso privado.

- Plataformas elearning para educación a distancia.

- Es un software diseñado para ayudar a los profesores a crear cursos en línea de alta calidad y entornos de aprendizaje virtuales. Las principales características de estas plataformas sobre otros sistemas es que está hecho en base a la pedagogía social constructivista, donde la comunicación tiene un espacio relevante en el camino de la construcción del conocimiento. Una de las fortalezas es que es Software Libre. Esto significa que su creador inicial, al momento de publicarlo en Internet, decidió utilizar la Licencia Pública GNU (GPL) y por lo tanto puede ser utilizado sin pagar “licencias”. La institución que lo instale está autorizada a copiar, usar y modificar la plataforma. Las principales ventajas para el cliente, como la plataforma para gestión de cursos:

- Para profesionales IT y sistemas
 - Para profesores y capacitadores

El segundo punto se centrará en describir todos los servicios de red que se encontraron:

- Controlador de dominio

- El servicio de Controlador de Dominio permite a los administradores reducir los costos y el esfuerzo de la administración de una red basada en dominio. El Controlador de Dominio facilita la centralización de los recursos y de gestión, así como la autenticación y autorización de usuarios. No existe un esquema de este tipo que vincule a todas las Sedes. Solamente hacen uso de un Controlador de Dominio las Sedes CAMPUS UNCuyo y CAMPUS TIC pero, para integrar las cuentas de correo institucional, no para beneficiarse con lo descrito en el inicio de este punto. Entonces, tomando la pequeña descripción realizada en la introducción es, sin dudas necesario la implementación de un Controlador de Dominio y es otro punto a favor para la creación de la red LAN entre todas las Sedes.

- Servicio de directorios y servicios de impresión

- Con el esquema actual de red solamente 3 sedes pueden compartir recursos por medio de un servicio de directorios compartidos y de impresión. Pero como en el caso del Controlador de Dominio, cada sede posee sus propios servicios de directorios e impresión, básicamente el motivo es la falta de confianza sobre la infraestructura de red de la universidad, el no querer depender de los tiempos del propio personal de la universidad ante algún pedido técnico y porque están totalmente afuera de dicha red. Con la implementación de una red que que integre y vincule todas las sedes, se podría utilizar un esquema donde uno o dos servidores concentren el tráfico por zonas

logrando de esta manera que no se cargue todo en uno solo y que además posean una sincronización entre ambos. En el caso de la impresión, debería ser un esquema similar a la de los directorios.

- Cámaras de seguridad (en algunas sedes).
 - Se repite el esquema de los anteriores servicios, ósea cada uno tiene localmente lo suyo.

- Servicios de DHCP, DNS.
 - Se repite el esquema de los anteriores servicios, ósea cada uno tiene localmente lo suyo.

Luego haber descripto los sistemas y servicios que se utilizan en la Institución sumado al esquema de conexión mostrado en la ilustración 6, rápidamente se llega a la conclusión de que no todas las sedes pueden hacer uso de ellos por medio de la Intranet. Solamente 3 sedes tiene la posibilidad de que el transporte de datos y comunicaciones sea por medio de la intranet ya que forman parte de la red LAN o MAN de la UNCuyo, para las 5 sedes restante solo es posible el acceder por medio de Internet a los aplicativos, y por otro lado, al no compartir la misma red se necesitan realizar configuraciones locales de red (DHCP, Servicio de directorio, Servicio de impresión, etc.), lo que implica tener algún responsable técnico en el sitio.

Es importante resaltar que el tener sistemas que no está pensado para ser utilizado hacia Internet puede significar una gran falla de seguridad. Segundo, al no estar todas las sedes integradas, es necesario contar con equipos y personal especializado en cada una de las sedes lo que también implica un costo económico que no siempre se justifica, ya sea porque es una sede pequeña y porque no tiene tantos dispositivos informativos para verificar o cuidar de su funcionamiento.

Para finalizar, debido al esquema de conexión actual, existe una dependencia técnica peligrosamente alta hacia la UNCuyo. Si por ejemplo la red LAN o MAN está mal configurada o defectuosa físicamente se producirán fallas en los accesos a los sistemas que son propios del Instituto y si es necesario realizar una ampliación o modificación solo será posible si el personal técnico de la UNCuyo tiene la predisposición necesaria.

Entonces, luego de describir los sistemas y servicios de la Institución y de mencionar que el esquema actual de conexión de red que en algunos caso es muy dependiente de la universidad y en otros están totalmente aislados, será necesario logra conseguir una solución tecnológica a nivel de conectividad que permita la integración total de las sedes, de los sistemas y de los servicios como así también lograr la independencia de otro ente.

4.1.3.4. Descripción de la infraestructura de Centro de Datos

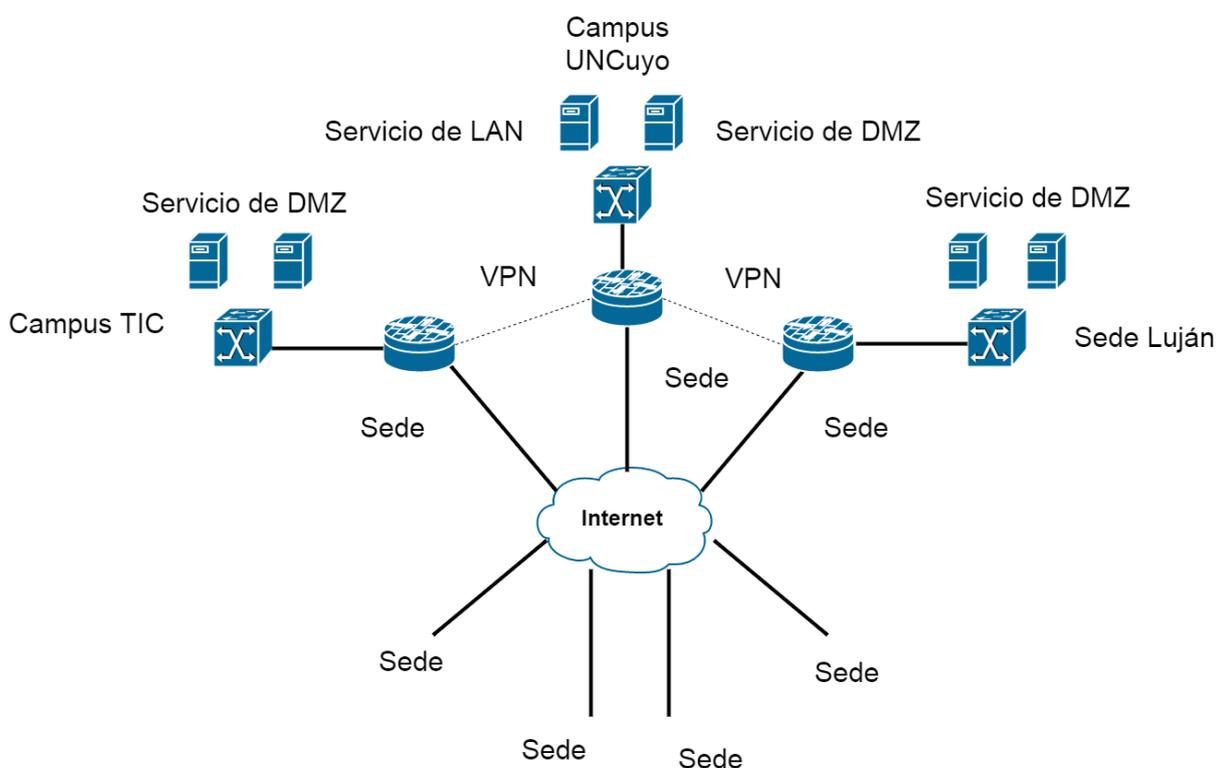


Ilustración 17. Fuente: Elaboración propia

Como se puede observar en la ilustración 14, y como en los dos casos anteriores (Internet e Intranet), solo 3 Sedes poseen servidores en sus instalaciones: Campus UNCUYO, Campus TIC y la Sede de Luján.

Dichas Sedes cuentan con personas capacitadas en la administración de dicha infraestructura y en el mantenimiento de redes de datos y comunicación.

Los servidores con los que se cuentan son:

- Sistema de gestión de alumnos
- Correo
- WWW
- DNS
- Autenticación de usuarios por ldap

A continuación se detallan las características de cada uno:

- Sistema de Gestión de alumnos del Instituto: es el sistema de mayor uso que tiene el Instituto y se encuentra almacenado en la Sede Central, en él se aloja la base de datos con toda la información de los alumnos, cobro de analíticos, estadísticas, etc. Para su funcionamiento, el sistema corre en 1 servidor donde se encuentran instalados los servicios: Apache, PHP5 y MySQL, todo bajo Linux Ubuntu y virtualizado.

- WWW: el Instituto cuenta con una página principal más algunas páginas secundarias enlazadas entre sí, y nuevamente se ubicación es la Sede Central. Dentro de los aplicativos principales para dar soporte a este servicio están: Apache, MySQL y Wordpress, bajo Linux Ubuntu y virtualizado.

- DNS: es el principal servicio de Internet que traduce los nombres de los dominios en direcciones IP y viceversa. También funciona para la traducción de nombres locales (PC, impresoras, servidores locales). Este servicio se encuentra replicado entre las 3 Sedes principales y mediante el uso del servicio de VPN se realiza una sincronización de los archivos de configuración principales. La aplicación está bajo Linux Ubuntu y virtualizado donde se encuentra instalado el servicio bind9.

- Correo: al igual que el servicio de DNS, el CORREO principal esta replicado entre las 3 Sedes principales y utiliza la VPN para la sincronización de buzones y archivos de configuración. Dentro de los aplicativos principales para dar soporte a este servicio están: Postfix, Dovecot, Apache, MySQL y SquirrelMail, todos bajo Linux Ubuntu y virtualizado. Actualmente cuenta con más de 100 cuentas de correo operativas.

- Autenticación de Usuarios: es para la validación de los usuarios de la red, el Instituto cuenta con un controlador PDC que utiliza SAMBA y LDAP. La aplicación está bajo Linux Ubuntu y virtualizado.

Es importante remarcar que cada sede además de los servicios expuestos, tiene la libertad de tener algún sistema de información o aplicación para uso local , como por ejemplo una plataforma educativa o el sistema que sea útil para el funcionamiento de la misma.

Luego de realizada la investigación en cada Sede lo que permitió explicar qué servicios informáticos y de información hay y cuáles son sus funciones, se llega a la conclusión que sería necesario que exista un centro de datos preparado para soportar dicha infraestructura y que además permita acompañar el crecimiento de la institución en lo que a sistemas se refiere.

Un Centro de Datos posee las siguientes características:

- Estabilidad energética
- Conexiones a Internet a través de varios proveedores.
- Sistemas redundantes de enfriamiento.
- Monitoreo del funcionamiento las 24 horas.
- Controles de acceso

Si bien hay muchas más características en lo que hace a la definición de un Centro de Datos, esos cinco puntos son difíciles de encontrar en la sedes que alojan los servidores y son considerados críticos para su correcto desempeño.

Con la infraestructura actual, el solo hecho de que se produzca un corte energético en la sede Central deja sin los servicios anteriormente descriptos al resto de las sedes, tanto los que utilizan la red de la UNCuyo como los que los acceden por Internet. Para el caso de los servicios de correo y DNS estos seguirán en funcionamiento debido al esquema de tener los servidores replicados en otras sedes y que esas sedes tengan otro vínculo provisto por algún proveedor externo de internet.

Los que se trata de expresar, es que sea cual fuera la característica de la organización, tener incorporado en sus instalaciones un Centro de Datos es algo complejo debido al servicio que prestan.

En conclusión, el diseño del modelo debería lograr que los sistemas informáticos del instituto tenga un espacio de almacenamiento que otorgue estabilidad y continuidad para su correcto funcionamiento.

4.1.3.5. Descripción de la infraestructura de Telefonía.

La ilustración 15, muestra la situación actual de la Infraestructura de Telefonía.

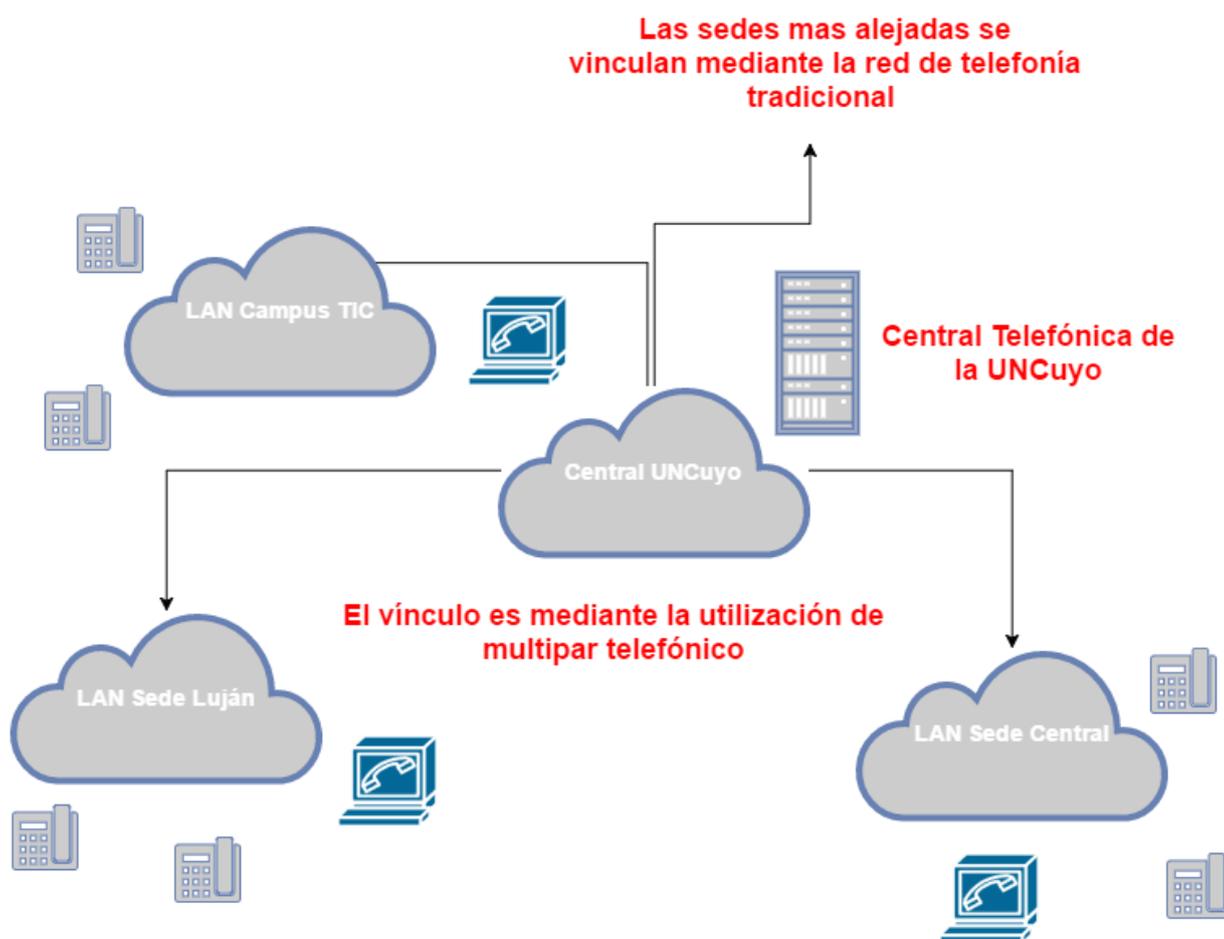


Ilustración 18. Fuente: Elaboración propia

Del mismo modo que en los 3 casos anteriores, la Infraestructura Telefonía no tiene la posibilidad de ser utilizada por 5 de las 8 Sedes del Instituto.

El motivo de esto es porque en los inicios del instituto como entidad educativa solamente se crearon 3 sedes (Campus UNCUYO, Campus TIC y la Sede de Luján) dentro de la infraestructura edilicia de la UNCuyo, por ese entonces, fue la UNCuyo la que facilitó la posibilidad de formar parte de su red de telefonía.

Debido al crecimiento de la demanda de las carreras que son ofrecidas por parte de la Institución; es que se fueron creando otras Sedes hasta llegar a las actuales 8 a lo largo y a lo ancho de la provincia.

De la misma forma que en los casos problemáticos anteriores, las sedes mencionadas (Campus UNCUYO, Campus TIC y la Sede de Luján) son las únicas que pueden hacer uso de la red de telefonía de la UNCuyo.

La UNCuyo posee Centralitas Telefónicas en cada una de las unidades académicas y controlan todo lo referente a configuraciones, permisos, etc desde un único punto. Esto significa que solamente la UNCuyo tienen la potestad de realizar configuraciones como por ejemplo: la configuración y control para realizar las llamadas, la configuración para el ingreso de las llamadas hacia el personal, etc. Es ahí donde surge el primer punto inconveniente, la dependencia absoluta a la hora de realizar alguna modificación en la configuración de alguno/s internos o la necesidad de más internos producto de una ampliación o reestructuración en alguna oficina.

Para las restantes 5 Sedes la telefonía es provista por la red de telefonía tradicional PSTN, este es el segundo inconveniente, significando un costo económico y administrativo muy importante para Instituto debido al uso de este recurso tan importante como es la telefonía.

En conclusión, la solución tendrá que permitir que todas las sedes estén integradas a una misma red LAN de altas prestaciones lo que admitirá por ejemplo el uso de VoIP . Por otra parte, se podrán colocar más de una centralita y así concentrar el tráfico en zonas y que gracias a esa red lograr el vínculo entre ellas.

Esta red deberá permitir la priorización de tráfico, la calidad de servicio y contingencias ante caídas de vínculos físicos. Si bien la llamada telefónica tradicional no implica grandes cantidades de consumo de ancho de banda, el uso de software IP permitirá video llamadas y, si bien se encuentran muy optimizados los códec, la priorización del tráfico es vital.

4.1.4. Descripción del tipo de usuario

En cuanto a la descripción de los usuarios que hacen uso de los sistemas informáticos y de información, los podemos agrupar en tres grupos bien diferenciados, esto son: personal no docente, personal docente y alumnos.

- Personal no Docente: Este grupo es el que más hace uso de los sistemas informáticos y de información. Lo constituye personal administrativo, bibliotecario, técnico y maestranza. Es normal escuchar quejas sobre el bajo desempeño de los sistemas, al punto de producir retrasos por fallas o errores en el funcionamiento.

- Personal Docente: El uso de los sistemas por parte de este grupo es bajo. Algunos de los motivos por el bajo uso de los sistemas se debe a:

- Desconfianza hacia los sistemas de gestión actuales (lentitud del acceso a los sistemas, conexión lenta, falta de capacitación del personal, etc.).

- No conoce sobre la existencia de los mismos.

- Desinterés.

- Alumnos: El uso se reduce a internet en laboratorios de enseñanza práctica o desde el WiFi. No hacen uso de sistemas propios, como por ejemplo una plataforma e-learning, debido a que son los mismos docentes quienes transmiten sus molestias a los alumnos generando desinterés de parte de ellos.

Queda claro que el mayor de los defectos que se poseen en la actualidad de los sistemas informáticos es lo desarticulado que se encuentran. Logra incorporar al Instituto dentro de una red

LAN propia de altas prestaciones, se lograrían mejoras sustanciales en el transporte de datos y las comunicaciones ayudando un mejor funcionamiento en todo el ámbito laboral de las sedes.

4.1.5. Conclusiones sobre análisis de las Infraestructuras actuales: Redes (Internet e Intranet), Centro de Datos y Telefonía.

La conclusión a la que se llega luego del estudio realizado sobre cada una de la problemáticas, es que no existe una correcta integración de los sistemas informáticos de transporte de datos y comunicaciones. De la manera en que se encuentran, es imposible que respondan a las necesidades de las personas que los utilizan tanto dentro como por fuera de la Institución. Además, tampoco permiten acompañar el potencial crecimiento tecnológico de la institución tomada como caso de estudio.

La solución deberá lograr la integración de todos los sistemas informáticos. Se debería diseñar un modelo que permita mejorar la funcionalidad de los sistemas, y que cuando se estén utilizando a pleno, poder analizar mediante mediciones los beneficios logrados y de esta manera justificar la posible inversión realizada.

Entonces, llega el momento de analizar concretamente que valor aporta la integración de los sistemas.

A partir del estudio realizado sobre las problemáticas, es que diseñara un modelo de reestructuración de los sistemas de transporte de datos y comunicaciones. Si bien es cierto que no todas las empresas, organizaciones, etc., han obtenido soluciones definitivas, el diseño permitirá situarse en el contexto de los potenciales beneficios e intentara definir cuáles son los pasos que hay que realizar para la reestructuración y así poder evaluar resultados.

Algunos de ellos son:

- Acceso a la información en tiempo real
- Integridad de la información
- Desarrollo y mantenimiento más simple y económico

- Mejorar la relación con los usuarios
- Mayor capacidad de respuesta
- Estandarización
- Mayor adaptabilidad ante lo que viene

Es importante considerar que los beneficios de la restructuración de los sistemas de transporte de datos y comunicaciones podrían ser progresivos y podrían determinarse después de mucho tiempo.

En el siguiente punto se pondrán en valoración distintas alternativas para solucionar las problemáticas planteadas, se analizarán y compararán para finalmente poder elegir la mejor de las opciones.

4.2. Análisis de las opciones encontradas

El objetivo de los siguientes puntos es lograr que mediante la búsqueda dentro de las tecnologías WAN modernas disponibles, seleccionar la mejor de las opciones que permitirá solucionar las problemáticas ya expuestas de la Institución elegida como caso de estudio.

4.2.1. Infraestructura de Redes (Internet)

En referencia al punto (5.1.3.2), la finalidad de este ítem es la de buscar una tecnología WAN moderna la cual permitiera dar solución a la problemática planteada sobre los accesos a Internet.

La solución se deberá dar mediante la contratación de un solo proveedor de servicios de Internet y de esta manera se lograrían los siguientes beneficios:

Desde el punto de vista técnico:

- Utilizar el mismo medio físico.
- Utilizar la misma tecnología y velocidades.

Y desde el punto de vista administrativo, permitirá concentrar todo lo referido a reclamos ante fallas, la centralización de pagos.

Además, ese proveedor debería conectar a todas las sedes con un mismo medio de transmisión (F.O., inalámbrico, par telefónico, etc.), lo que lograra una mejoría superior desde el punto de vista técnico.

La segunda dificultad encontrada durante la investigación, es que cada sede posee diferentes anchos de banda. No existe una justificación del porqué, por lo general la respuesta más escuchada es: es lo que se contrató o se podía pagar. Quizás por falta de asesoramiento.

Una correcta asignación del ancho de banda debería venir de la mano de un cálculo donde se consideren la cantidad de usuarios y el tiempo que más estaría en uso Internet. Esto daría un valor de ancho de banda que permitirá que la sede trabaje cómoda en los momentos donde más personas hacen uso.

A continuación, se darán a conocer las tecnologías WAN que mejor se adaptarían a la problemática. Estas son: servicio de *Internet compartido* esto abarca los siguientes servicios (Internet residencial, Internet corporativo), y los servicios de *Internet dedicado* (servicio a través de la tecnología MPLS).

4.2.1.1. Internet residencial

Un servicio de Internet residencial presenta los siguientes puntos a favor:

- Costo accesible
- Instalación simple
- Download/Upload (es importante remarcar que en la actualidad los usuarios no solamente descargan información, sino que también suben información, por ejemplo imágenes a las redes sociales).

Si se trata de un servicio de ADSL utiliza la infraestructura existente del cableado telefónico tradicional y si se trata de un servicio por medio de Cablemodem utiliza la red de televisión por cable.

¿Cuál sería el inconveniente de contratar servicios de internet residencial para todas las Sedes?

Los servicios de Internet residenciales son del tipo *Internet compartido*, esto significa que si por ejemplo, se contrata un ancho de banda de 3Mbps, este mismo es compartido por otros usuarios que están conectados al mismo concentrador que permite dar la conexión hacia Internet. En el caso de ser un servicio de ADSL, sería la Central Telefónica más cercana al domicilio.

Los servicios compartidos no garantizan la mejor de las calidades y en una sede donde se consumen durante varias horas seguidas Internet, esto podría generar lentitud, retardos, etc.

4.2.1.2. Internet empresarial

4.2.1.2.1. Aspectos a favor

Un servicio de Internet empresarial presenta los siguientes puntos a favor:

- Más velocidad
- IP fija (permite la creación de VPN)
- Seguridad de los datos

Este servicio comparte los cuatro puntos del servicio de Internet residencia e incorpora tres puntos más, pero siguen siendo un servicio de *internet compartido*, pero en menor cantidad, lo que permitiría más ancho de banda. Se podría garantizar un 60% del total del enlace contratado disponible, como en el peor de los casos.

Nuevamente, no se garantiza la totalidad del servicio en las Sedes que mayor cantidad de personas tiene a lo largo de todo el rango de cursado (8hs a 17hs) generando malestar.

4.2.1.3. Internet a través de la red MPLS

La utilización de la red MPLS como medio para el acceso a Internet hereda todos los beneficios que posee la tecnología MPLS. Si bien ya están mencionados y explicados en el Marcos Teórico, se detallan algunos puntos:

- QoS
- CoS
- Ingeniería de Trafico

El uso de la tecnología como medio de transporte va a permitir:

- Integración del medio físico de transporte
- Integración de los costos del servicio
- Anchos de banda SIMETRICOS garantizados
- Calidad de servicio de extremo a extremo
- Integración de las políticas de seguridad
- Integración de los esquemas para el acceso a ciertos sitios de Internet

Tiene con aspecto en contra su alto costo, pudiendo generar que no sea accesible a cualquier empresa u organización.

4.2.1.4. Conclusiones sobre la mejor opción a la problemática para el acceso a internet.

A continuación, y a través de un cuadro comparativo, se expondrán las características de las diferentes alternativas, permitiendo elegir cuál de todas es la mejor solución a la problemática del acceso a Internet.

	Internet domiciliaria	Internet empresarial	Internet a través de MPLS
Costo	X	X	
Instalación	X	X	
Ancho de banda		X	X
Asimétrico	X	X	
Simétrico			X
IP fija		X	X
Seguridad		X	X
Calidad de servicio			X
CIR garantizado			X

Tabla 4. Fuente: Elaboración propia

Es importante aclarar que MPLS no es una tecnología para dar Internet, es una tecnología WAN que permite integrar múltiples servicios gracias a sus características. La tabla comparativa simplemente permite dar cuenta de los beneficios de cada una, pero puede generar confusión si no se tiene bien claro el concepto de MPLS.

Para redondear, la mejor opción considerada es MPLS, y el motivo es porque se podrán concentrar múltiples servicios con una gran calidad y seguridad, logrando la premisa que busca esta tesis, la integración del transporte de datos y comunicaciones de la Institución. No se tiene que dejar de remarcar que los costos de MPLS son mayores con respecto al resto.

4.2.2. Infraestructura de redes (Intranet).

Tomando como punto de partida el punto (5.1.3.3) que hace referencia a las fallencias detectadas en la infraestructura de Redes (Intranet), es que analizarán como posibles opciones de solución, a las tecnologías VPN y MPLS.

La opción elegida de deberá permitir a los usuarios de cada una de las sedes poder hacer uso de todos los sistemas informáticos y hacer uso de la información disponible a través de una única red de datos.

4.2.2.1. Infraestructura basada en el uso de VPN

La tecnología VPN, que ya fue descrita en el punto Marco Teórico (4.3), permite crear túneles encriptados seguros a través de internet.

Para que esto sea posible, es necesario contar con algún dispositivo que permita realizar las configuraciones apropiadas. Puede ser un dispositivo físico como por ejemplo un *router* o también mediante una aplicación en una PC. Sea cual fuera el medio, en él se deben realizar todas las configuraciones necesarias para establecer la VPN.

Las VPN se configuran en el modo Cliente-Servidor y debido a la forma en que están interconectadas las sedes, ilustración 6, las VPN se deben configurar en el modo SITE TO SITE. Esto sería, definir una sede como la sede donde se van a concentrar todas las VPN y de ahí realizar los vínculos hacia el resto.

Con este modo de configuración se concentraría toda la administración de los accesos a cualquiera de los sistemas informáticos a través de un solo punto.

De acuerdo con lo expresado en los párrafos anteriores, esta opción parecería ser la opción que permitiera ser la solución, pero hay que considerar los siguientes aspectos:

Se lograría una óptima vinculación entre los extremos si los dispositivos encargados de establecer la VPN son de las mismas características técnicas, de este modo se obtendría una compatibilidad alta. Estos dispositivos deben ser de características avanzadas y reconocidos en el mercado.

En resumen, para considerar esta alternativa se debe contemplar lo siguiente:

- Se deberán colocar en cada Sede Routers de la misma marca, esto aseguraría una compatibilidad alta en la configuración y posterior vínculo.
- Sería adecuado contar con un lugar específico, con las condiciones mínimas e indispensables para su buen funcionamiento (rack, tensión estable, refrigeración, habitación segura, etc.).
- Se debería contar con personal en cada sitio o también la administración se puede realizar remotamente. Si se decide realizar administración remota, hay que considerar que ante una falla física, se deberá contar con repuestos y movilidad para realizar el cambio y la puesta nuevamente en marcha.
- La administración medio/avanzada requiere preparación. Si el personal no está correctamente capacitado, cada modificación o cambio va a implicar intermitencias en el servicio, produciendo molestia en el personal que trabajan en la sede, y en los alumnos también.
- Se debe elegir la VPN que mejor encriptación asegure así la información privada que fluye por Internet no sea captada y robada. La encriptación que permite mayores niveles de seguridad, implica equipos más robustos, y por lo tanto más costosos.

En la anterior descripción se exponen los puntos positivos y negativos si la opción elegida son vínculos mediante VPN.

Las conexiones VPN representan una alternativa económicamente posible, la metodología de conexión entre sedes sería ágil pero por razones técnicas propias de las VPN su capacidad es limitada cuando se necesitan grandes volúmenes de información, lo que sería un punto en contra.

No hay que olvidar de que el Instituto se necesitara dedicar recursos físicos, económicos y humanos para la implementación de la red, su operación y mantenimiento.

4.2.2.1.1. Conclusión

En conclusión, lo que se observa luego de analizar la características de la tecnología VPN y de la posibilidad de realizar conexiones entre sedes mediante su uso, es que se debería contar con recursos humanos especializados en cada sitio o contemplar la contratación de alguna empresa para realizar los mantenimiento tanto en las sedes que abarcan el gran Mendoza como para las sedes más alejadas, disponer de recursos económicos para la adquisición de equipamiento, algo con lo que no se dispone actualmente en el Instituto.

Además, recordando que las VPN no están pensadas para el tráfico de grandes volúmenes de información.

4.2.2.2. Infraestructura basada en MPLS

Nuevamente, se aclara que la tecnología MPLS es una solución que integra muchas soluciones, la posibilidad de configurar VPN son características propias del núcleo de MPLS.

Dicho esto, se expresara de qué manera MPLS podrá resolver la problemática de conectividad entre Sedes.

La red basada en MPLS se debe diseñar expresamente para proporcionar un mecanismo eficiente, fiable y escalable para la interconexión de las distintas Sedes entre las distintas localizaciones, estableciendo una única plataforma WAN completamente gestionada.

Una vez conectados los activos informáticos y que la información sea accesible por el personal, se podrá compartir información y acceder a los sistemas corporativos desde cualquier lugar. Se trata de un servicio completamente gestionado, que elimina la complejidad e incomodidad asociadas a la compra de equipamiento y la implementación de la red, y a su operación y mantenimiento a lo largo del tiempo.

4.2.2.2.1. Aspectos a favor

- Permite expandir una infraestructura segura y fiable tanto para sus usuarios como para los activos informáticos y para la información.
- Comunicación instantánea desde cualquiera de las Sedes y en cualquier momento.
- Posibilidad de ofrecer múltiples servicios y aplicaciones a través de una infraestructura común.
- Simplifica las operaciones de la red y su ampliación a lo largo del tiempo.
- Mejor aprovechamiento de los recursos, y mayor visibilidad y rendimiento.
- Prepara la red para el futuro, permitiéndola crecer.
- Integración transparente con una amplia variedad de productos y servicios afines.

4.2.2.2.2. Aspectos en contra

- Costos para adquirir el servicio.
- Costo mensual elevado.
- Cortes de servicio por fallas técnicas por parte de la empresa prestadora.
- Ante la caída del servicio en una Sede, en el caso de que la empresa no posea los repuestos necesarios para activar nuevamente la conexión, esa Sede quedara desconectada.
- Dependencia de terceros a la hora del mantenimiento.

4.2.2.3. Conclusiones

Luego de analizar los aspectos a favor y en contra de vincular las sedes usando VPN o MPLS es que se llega a la conclusión que la mejor opción sería:

La integración total de todos los activos informáticos y el acceso a la información mediante una única de red de transporte de datos para todas las sedes, y la única opción de las analizadas que

puede realizar esto es la tecnología MPLS ya que por sus aspectos técnicos siendo una plataforma completamente gestionada ofrece fiabilidad escalabilidad y seguridad entre otros. Pero el costo de contratar un servicio que ofrezca a la tecnología MPLS en comparación con la utilización de VPN se deberían considerar.

4.2.3. Infraestructura de Centro de Datos

Tomando como punto de partida el punto (5.1.3.4) en donde se describen las falencias de la Infraestructura de Centro de Datos o en algunos casos la no existencia, es que se proponen las siguientes alternativas de solución:

1. Centro de Datos Centralizado tercerizado
2. Centro de Datos Distribuido tercerizado
3. Centro de Datos Distribuido compartido

¿Qué es lo que se debe tener en cuenta a la hora de elegir uno u otro tipo de Centro de Datos?

Elegir la contratación de un Centro de Datos es una decisión que puede cambiar la forma de trabajo de dicha Institución por lo que hay que considerar muchos factores para elegir un Centro de Datos, para discutir:

- ¿Qué empresa prestara el servicio, en el caso de esta sea la mejor opción?
- Tener la administración del 100%, tercerizarlos o compartir la administración con algún proveedor.
- El aspecto económico es un punto realmente importante o solamente lo técnico.
- Personal propio o tercerizado.

Junto con los tres tipos de Centros de Datos considerados para dar solución a la problemática, más los últimos cuatro puntos del párrafo anterior, serán la base del análisis que permitirá elegir la mejor opción.

4.2.3.1. Centro de Datos Centralizado tercerizado

Un Centro de Datos tercerizado presenta las siguientes características:

- Capacidad de almacenamiento
- Seguridad
- Soporte técnico
- Sistemas energéticos extra
- Respaldos

Tomar la decisión de contratar un servicio externo puede ser producto de que el Centro de Datos propio este en los límites de espacio, potencia, refrigeración, etc. Esto seguramente es debido al continuo y desmesurado crecimiento de los datos y al despliegue de la virtualización.

Sea esta la situación o no, el plantearse la construcción o ampliación del Centro de Datos propio o de contratar servicios externos, seguramente será una las inversiones en infraestructura más importantes que se realicen.

Por tal motivo, antes de tomar la decisión es fundamental evaluar las diferentes opciones y el impacto económico que supone a la Institución.

4.2.3.1.1. Aspectos en contra

- Dependencia técnicas absoluta hacia la empresa que posee los servicios.
- No ser el dueño de la información
- Ante fallas, queda totalmente sin accesos a los servicios por parte de las Sedes.
- Administración compartida

Además, ya sea que se contrata un servicio básico de Centro de Datos o se adquiere un servicio más completo de almacenamiento, seguridad, soporte técnico, sistemas de energía extra y respaldos, implica recursos económicos considerables.

Como segundo punto a considerar, en el caso de solicitar una modificación sobre alguno de los activos informativos o servicios, los tiempos producto de la burocracia de las empresas con estas capacidades pueden ser muy altos y generar molestias, malestar, etc.

4.2.3.1.2. Aspectos a favor

Los aspectos a favor que tiene tercerizar absolutamente la gestión de los activos y servicios, son:

- Disponer de un staff externo que gestione las instalaciones.
- Tener los activos 100% en línea
- Tener respaldo de los activos en el momento que uno lo desee.
- Tener la seguridad de tener la información segura.

4.2.3.2. Centro de Datos distribuido tercerizado

Comparte casi en su totalidad las características con el punto 5.2.3.1, a excepción de que podrían alojarse en diferentes Centros de Datos de la propia empresa en distintas localizaciones.

4.2.3.3. Centro de Datos distribuido compartido

Este tipo de configuración, implica compartir los puntos de almacenamiento, seguridad, soporte técnico, sistemas de energía extra, respaldos y administración entre la empresa que sea contratada para tal fin y el personal técnico especializado de la Institución responsable del Centro de Datos propio.

De tomar como la solución esta opción, es fundamental evaluar las diferentes opciones y el impacto financiero que suponen para la Institución la construcción o remodelación del que sea

definido como el Centro de Datos principal y también o no, de los Centro de Datos satélites o secundarios.

Entonces se requiere tener en cuenta lo siguiente:

- Tipo de Centro de Datos a construir.
 - Los aspectos fundamentales en este punto son: eléctricos, termomecánicos, edificios, cableado y comunicaciones.
- Equipamiento informático a instalar, considerando el presente y el futuro.
 - Cuáles serán los equipos que se instalarán dentro del Centro de Datos, entre servidores, storage, dispositivos de backup, switches de core, etc. De esta manera se podrá calcular el consumo eléctrico.
- Refrigeración.
 - Se destacan los sistemas de refrigeración perimetral que inyectan aire por debajo del piso técnico, los de refrigeración por hilera que extraen el calor de los pasillos calientes e inyectan frío por delante de los racks, los de enfriamiento por rack que inyectan el aire frío desde la parte superior del rack, o los sistemas que simplemente prevén la inyección de aire frío en toda la sala.
- Conectividad.
 - Se deberá pensar como estarán conectados e integrados a la red los servidores, storage o cualquier dispositivo que instalaremos en cada rack. Dejar previsto en los racks una cantidad determinada de cables de cobre y/o fibras que confluyan todos al área de comunicaciones del data center.

- Ubicación y espacio.
 - Si aspiramos estrictamente a cumplir con las normas deberíamos pensar en armar un espacio exclusivo para el alojamiento de los racks de servidores, un espacio diferente para los de comunicaciones, otro para la sala de UPS. Si nos adaptamos al tipo de Institución, se deberá tener en cuenta los espacios más reducidos y a un proyecto de menor envergadura unificando en un mismo espacio los racks de servidores y comunicaciones, y en algunos casos las UPS pueden también instalarse dentro de la fila de racks.

- Sistemas de control y seguridad.
 - Para resguardar el valor patrimonial y, aún más importante, el valor de los datos, debemos establecer sistemas de control y seguridad que protejan al Centro de Datos.

La descripción anterior es lo básico recomendado para la creación de un Centro de Datos.

Ahora, si no se está en las condiciones económicas para encarar tamaño proyecto, y se decide realizar la remodelación paulatina del Centro de Datos actual, se deberían tomar como guía los 6 ítems anteriormente descriptos.

Entonces, luego de estar constituido el Centro de Datos propio, se deberían definir cuáles de los activos que va a ser almacenados en el Centro de Datos propio y cuales en el Centros de Datos tercerizado.

Basado en experiencias personales por estar trabajando en un ente público de similares características del Instituto, es que el esquema de distribución de los servicios debería ser de la siguiente manera:

Se deja en claro que el Centro de Datos del Instituto cuenta en sus instalaciones con todo el equipamiento de comunicación y UPS.

Principalmente en el Centro de Datos de Datos del Instituto deberán estar todos los activos de *desarrollo, testing* y algunos servicios de menor importancia o impacto en el caso de que este fuera de línea durante un tiempo prudencial, que son producidos por personal interno o externo que trabajan para el Instituto.

De manera secundaria, también pueden ser almacenados otros activos que sean de producción pero no sean vitales para el funcionamiento del Instituto.

Por último, se debe utilizar el Centro de Datos propio para almacenar las copias respaldo de todos los activos que estén almacenados en el Centro de Datos externo.

El Centro de Datos externo, como cumple con los 6 puntos antes mencionados, es el mejor lugar donde ubicar los activos de información vitales para el funcionamiento del Instituto. De esta manera por más que se produzca alguna caída en el Centro de Datos propio o falla en los enlaces, la totalidad de las Sedes podrán seguir sus actividades sin problemas ya que siempre tendrá mejores respaldos eléctricos y de enlaces, ósea, siempre estará mejor preparado para contingencias.

A continuación la ilustración 16 muestra cómo sería la distribución propuesta.

Distribución de Servidores y Servicios

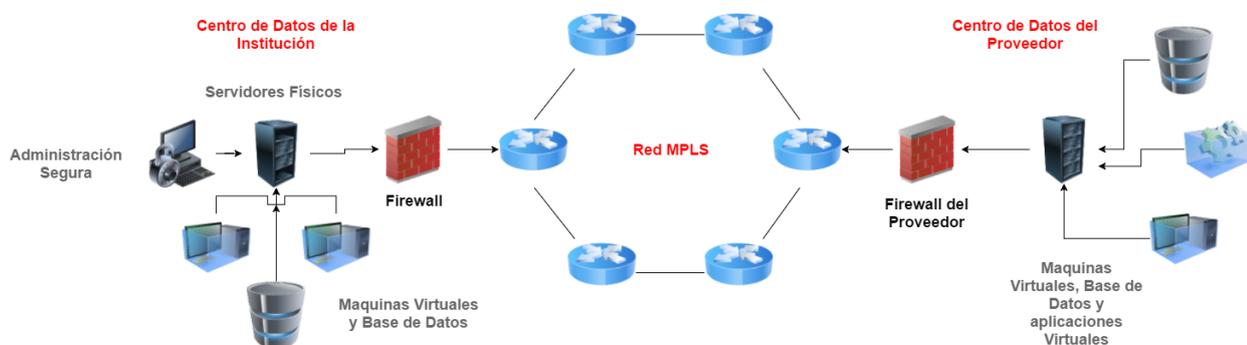


Ilustración 19. Fuente: Elaboración propia

4.2.3.3.1. Aspectos a favor

En el caso de no cumplimiento de los tiempo de respuesta por parte de la empresa, ya sea con una copia de respaldo o un cambio de configuración de los activos almacenado en su Centro de Datos, la Institución puede tomar esos activos y ponerlos en funcionamiento en su propio Centro de Datos.

4.2.3.3.2. Aspectos en contra

- Personal especializado
- Presupuesto para tecnología

4.2.3.4. Conclusiones

Como conclusión, en base al análisis de las tres opciones presentadas, es que la mejor de las opciones sería utilizar un esquema de Centro de Datos distribuido compartido, o sea, distribuir los activos de información entre el Centro de Datos propio y el Centro de Datos del prestador de servicios.

Al mismo tiempo, se lograra una mejor integración ya que el prestador de servicios del Centro de Datos debería ser el mismo que provee la infraestructura de telecomunicaciones basada en MPLS, de este modo, se puede aprovechar más aun todos los beneficios que da la tecnología MPLS, (QoS, CoS, políticas de firewall, ingeniera de tráfico, etc.) aplicada al acceso de los activos informáticos y de información por parte de los usuarios internos y también para los usuarios que hacen uso de alguno de los activos desde Internet.

4.2.4. Infraestructura de Telefonía.

En referencia a la problemática planteada en el ítem (5.1.3.5) en donde la falta de una infraestructura de telefonía unificada no permite a la mayoría de las sedes de la Institución establecer comunicaciones internamente (solo 3 de las 8 sedes usan la infraestructura telefónica de la UNCuyo), pero, si pueden realizar comunicaciones externas utilizando para ello a la telefonía

tradicional PSTN (par trenzado). Esta estructura hace dificultosa la comunicación entre sedes y además implica tener diferentes servicios con diferentes proveedores y costos.

La solución tendrá que permitir que la telefonía utilice la misma infraestructura de transporte de datos para las comunicaciones de voz.

Las señales de voz se envía de forma digital dividida en paquetes de la misma manera que un ordenador recibe y transmite datos ya sea en una Intranet como por Internet, esto significa que las comunicaciones de voz pueden utilizar como medio de transporte a la misma red de datos que vincularía a todas las sedes.

Como estaban las cosas en el momento de realizar el relevamiento y estudio correspondiente, ni siquiera en la mayoría de las sedes tienen la posibilidad de comunicarse dentro de las mismas oficinas mediante internos.

Los párrafos anteriores simplemente intentan plasmar un pequeño recordatorio de la problemática, pero en este punto se enfocara en encontrar la mejor solución en base a las opciones que permitirán una integración total con la nueva infraestructura informática del Instituto.

Dicho esto, las siguientes son las opciones que serán explicadas y comparadas para de esta manera poder elegir.

- Centralita telefónica virtual
- Centralita telefónica corporativa (IP PBX)

4.2.4.1. Centralita telefónica virtual

Las centralitas telefónicas virtuales poseen las mismas características técnicas de una centralita telefónica física convencional, pero en vez de estar en algún rack o habitación en la organización, están en el Centro de Datos de algún proveedor. Se ahorra cableado, espacio y costos asociados al mantenimiento de dicha infraestructura.

A la organización se le entrega el servicio más el equipamiento telefónico sin necesidad de adquirir hardware.

4.2.4.1.1. Aspectos a favor

- Escalabilidad
- Se adapta a la necesidad, se pueden agregar internos o líneas sin grandes inversiones.
- Flexibilidad
- Soluciones simples, rápidas y de calidad. Como por ejemplo la personalización del preatendedor, ayudando así a la imagen de la organización.
- Ahorro económico
- No requiere de grandes inversiones, se puede ampliar las líneas externas o los internos sin gastos extras.
- Movilidad
- Permite la integración de sedes remotas.

4.2.4.1.2. Aspectos en contra

Uno de los requerimientos básicos y al mismo tiempo crítico para disponer de una centralita telefónica virtual es la necesidad de un acceso a Internet de Banda Ancha con ciertos parámetros de calidad ya que todo el servicio de voz, se comunica a través de VoIP a través de Internet.

De acuerdo con los análisis de consumos de Internet realizados en todas las Sedes, y considerando los accesos actuales, se llegó a la conclusión que las 3 Sedes con mayor cantidad de alumnos, personal docente y no docente, necesitarían de ancho de banda de entre 10 a 20 Mbps, esto le otorgaría mejores prestaciones a la hora de establecer las comunicaciones. Para las sedes con menor cantidad de usuarios, el ancho de banda sería de 10Mbps lo que también daría buenas prestaciones al servicio de telefonía virtual.

Entonces, para poder implementar esta opción, se necesitan enlaces de Internet en cada sede de un costo aproximado que van desde los \$1000 a \$2000 más el costo del servicio de la centralita telefónica virtual, volviendo nuevamente a tener diferente proveedores, diferentes boletas de servicios y diferentes números para reclamos.

La mejor solución es lograr la integración a través de una tecnología permita a futuro la inclusión de nuevos servicios muy interesantes para toda la Institución tales como la utilización de teléfonos software ejecutándose en ordenadores, PDA's y teléfonos móviles de última generación.

4.2.4.2. Centralita telefónica corporativa (IP PBX)

La centralita telefónica corporativas físicas o IP PBX convencionales, son equipos instalados dentro de la organización.

En comparación con las centralitas telefónicas virtuales, tienen sentido en organizaciones de mediano o gran tamaño y donde se prefiere la administración del 100% y además, existe una integración de la telefonía en tiempo real con otros sistemas.

Las centralitas telefónicas deberán soportan tecnologías IP, digitales y analógicas para poder ser utilizadas con cualquier teléfono o línea así como la integración con terminales móviles, PC o tablets y combinar el teletrabajo y la movilidad con potentes opciones de comunicación y colaboración.

4.2.4.2.1. Aspectos a favor

- Trabajan mediante las redes de datos bajo el protocolo IP.
- Interactúan con la red de telefonía convencional PSTN, tanto analógicas RTB (Red Telefónica Básica) como digitales RDSI (Red Digital de Servicios Integrados) y móviles GSM/GPRS/UMTS.

- Pueden conectarse teléfonos estándar (teléfonos analógicos, fax o teléfonos inalámbricos).
- Las centralitas IP PBX pueden consistir en un equipo de hardware físico o en un sistema de software, denominadas Soft IP PBX.
- Fácil de entregar en la infraestructura de telecomunicaciones sobre MPLS.

La administración 100% de todas las configuraciones como ya se hizo mención y la posibilidad de colocar varias centralitas y así poder dar servicios sectorizados, es la opción que mejor se complementa con la integración de la infraestructura informática que se piensa para el Instituto.

4.2.4.2.2. Aspectos en contra

- Personal capacitado propio o tercerizado
- Inversión inicial alta

Estos dos únicos puntos son los más importantes que deberán ser bien analizados si la decisión es la de adquirir el dispositivo para el manejo de la telefonía propia por parte de la organización.

4.2.4.3. Conclusiones

En base al análisis desarrollado sobre las dos opciones que darían solución a la problemática, es que se decide utilizar a la Centralita Telefónica corporativa (IP PBX).

Esta infraestructura telefónica estaría formada de varios nodos IP que usarían la red de transporte de datos para interconectarse, de esta manera proporcionarían los servicios telefónicos para todas las sedes. Entonces, se lograra integrar datos y telefonía sobre la infraestructura de redes y así con todas las sedes. Cumpliendo de esta forma con la integración de todos los servicios.

Además, gracias a la conexión con la red de telefonía pública, las sedes donde estarían ubicadas podrán seguir conectadas con el exterior por más que se produzca alguna falla en la red que las vincula.

Se recomienda que una de las centrales tenga conexión con la red de telefonía móvil. Esto permitiría realizar llamadas directamente las llamadas a los móviles como si fueran internos.

4.3. Diseño conceptual final de la solución para la Instituto

Este es el punto se plasma el diseño conceptual final donde se integran todas las alternativas elegidas en los puntos anteriores.

De acuerdo a las conclusiones parciales de cada uno de los puntos, la solución a las problemáticas viene de la mano de la tecnología MPLS. Se justifica la elección de dicha tecnología, porque MPLS permite *la integración de todo el sistema informático y de información del Instituto sobre una única red de transporte.*

Por otra parte, adquirir un servicio de esta envergadura permitiría proyectar hacia adelante, es decir, ampliar cualquiera de los servicios, conectar nuevas sedes, ampliar el ancho de banda, concentrar la gestión de pagos y reclamos en un mismo proveedor, etc.

El diseño será dividido en varias secciones: diseño del esquema de las infraestructuras de redes, distribución de los servidores y servicios informáticos, infraestructura de telefonía y esquema de control para hacer uso de los servicios.

4.3.1. Esquema de conexión de la infraestructura de redes basadas en MPLS

En esta sección, se explica cómo es el proceso que deberá llevar a cabo para conectar todas las sedes con la nueva infraestructura.

A continuación, se realiza una descripción ordenada del proceso necesario para lograr que las sedes sean vinculadas con la red MPLS:

1. Actividades propias de la empresa que será la encargada de vincular a las sedes hacia la red de datos MPLS.

i) Vincular todas las sedes mediante la colocación de equipamiento específico, de propiedad de la empresa proveedora del servicio. Estos dispositivos estarán configurados para conectarse con la red de datos.

a. Los equipos utilizarán algún medio de transmisión conocido para conectarse, como por ejemplo: a través de la red de telefonía tradicional (par trenzado), a través de fibras ópticas o enlaces de radio. Lo más recomendable es que todas las sedes estén vinculadas por el mismo medio de transmisión y en base a características técnicas, es que se considera el uso de fibra óptica como el único medio de transmisión.

b. En el caso de que se presenten imposibilidades técnicas (falta de infraestructura en la zona donde se encuentra la sede), y no sea posible implementar los mismos medios de transmisión, se debe lograr que las sedes que mayor consumo de los servicios hacen, utilicen la fibra óptica. Además, debido a que en esas sedes seguramente se coloquen equipos de infraestructura, como por ejemplo: servidores, central telefónica, storage de backup, etc.

1) A continuación, se describirán las actividades que serán propias del Instituto, dentro de cada sede y entre sedes:

a) En cada una de las sedes debe existir un espacio físico específico para alojar los equipos, comprendido por un rack que cuente con un sistema de alimentación eléctrica y un respaldo como son las UPS, como elementos básicos. Si se trata de una sede que aloja equipamiento informático de comunicaciones, servidores o central telefónica, significa que debe dar servicio a sus usuarios locales y al resto de las sedes, motivo por el cual también debe contar con un sistema de refrigeración y acceso seguro al nodo, como adicionales importantes.

b) En lo referido a las configuraciones de red de cada sede, se debe definir una red que permita que cada sede tenga su propio bloque de red ,pero que sea parte de una red mayor, por ejemplo:

c) La red clase A 10.1.0.0/16 contiene direcciones IP que van desde la dirección 10.1.0.1 hasta la dirección 10.1.255.254, estos son unos 65534 dispositivos posibles de conectar, algo más que suficiente para proyectar cualquier posibilidad de crecimiento en cada una de las sedes.

d) Se debe realizar el subneteo para asignar a cada sede una red propia. Esto permite: una mayor organización de esa gran red, permite redes adicionales sin necesidad de tener IPs adicionales, se logra mayor control para los administradores y reduce el tamaño de los dominios de broadcast.

La siguiente tabla se indica una posible distribución de las subredes para cada sede.

Sede	Subred asignada
CAMPUS UNCUYO	10.1.40.0/21
CAMPUS TIC	10.1.48.0/21
LUJÁN DE CUYO	10.1.56.0/21
TUNUYAN	10.1.64.0/21
ESTE	10.1.72.0/21
SEDE GENERAL ALVEAR	10.1.80.0/21
SEDE SAN RAFAEL	10.1.88.0/21

Tabla 5. Fuente: Elaboración propia.

e) Una vez definidas las redes para cada sede, se deben colocar equipos (routers) propios del Instituto que hagan la asignación dinámica de las direcciones IP mediante el servicio de DHCP. Este servicio permite asignar dinámicamente las IP a cualquier dispositivo conectado tanto por cable como inalámbricamente. Dicho equipos serán administrados remotamente y serán los encargados de la asignación de IP por MAC.

f) Para lograr una administración más ordenada, que permita realizar controles y obtener reportes de los equipos informáticos de la red, se definirán pool de direcciones IP para PC, para impresoras y para equipos de comunicaciones.

g) Adicionalmente, los conmutadores, que a ubicarse en cada sede, deben ser administrables, dando más seguridad a la red y la posibilidad de configurar QoS.

2) Configuraciones de ruteo (encaminamiento) que será definido por la empresa prestadora de acuerdo a lo pedido por el Instituto.

i)Entonces, vinculadas las sede, definidas todas las redes, colocados todos los equipos de comunicación, el siguiente paso será definir las políticas de ruteo (encaminamiento) para que cada sede puede acceder a Internet y a todos los servicios de red que posea en Instituto a través de la MPLS.

ii) Como primera condición, todos lo referido al acceso a Internet deberá ser canalizado hacia un solo dispositivos de red, el cual deberá estar ubicado en una de las sedes más importantes. Desde ahí, el personal especializado del Instituto será en el encargado de la administración de los accesos para la navegación de Internet. Por ejemplo: redes sociales, radios, streaming, todo lo que no sea necesariamente importante para el trabajo.

iii) Se deberán asignar las redes para cada una de los servicios de red del Instituto. Estas redes deberán ser conocidas por la empresa y ruteadas para que cada sede pueda hacer uso de estos servicios.

La siguiente ilustración permite visualizar como sería el esquema de conexión entre las sedes con la red de datos.

Infraestructura de Telecomunicaciones

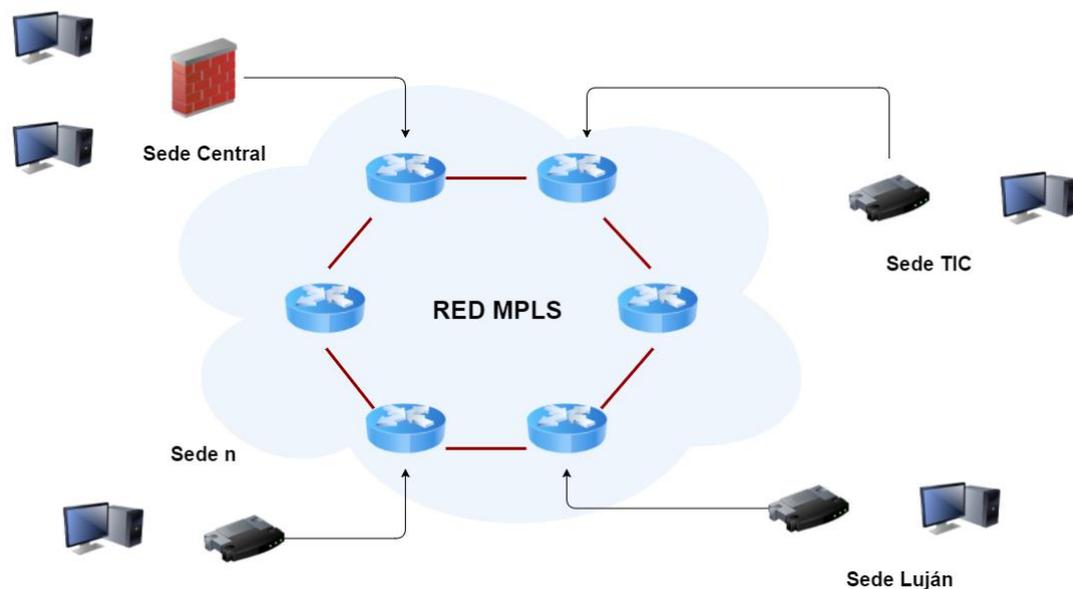


Ilustración 20. Fuente: Elaboración propia

El último de los puntos a definir es la asignación de ancho de banda para cada una de las sedes.

En la tabla 5, y de acuerdo con los análisis preliminares de la primera etapa del desarrollo, se recomendaría para cada sede lo siguiente:

	Ancho de banda asignado
Sede Central	40Mbps
Sede TIC	20 Mbps
Sede Luján	20 Mbps
Sede Rivadavia	10 Mbps
Sede San Martín	10 Mbps
Sede Tunuyan	10 Mbps
Sede General Alvear	10 Mbps
Sede San Rafael	10 Mbps

Tabla 6. Fuente: Elaboración propia

La asignación de banda ancha, serán para todo el tráfico de las sedes: Internet, telefonía, e Intranet.

En definitiva, esos son los pasos necesarios para logra poner en marcha la nueva infraestructura de red del Instituto.

4.3.1.1. Distribución de los servidores y servicios en los Centros de Datos.

En este punto se explica cómo se distribuyen los servidores físicos y virtuales que contienen la información en los nodos.

Ya definida la infraestructura de redes, es el momento propicio para definir el posible esquema de distribución.

El siguiente sería el criterio más apropiado para la distribución en los nodos: como se indicó en el ítem (5.2.3.1) la mejor opción es lograr un equilibrio en la distribución entre el Centro de Datos propiedad del Instituto y el Centro de Datos de la empresa prestadora.

Sería requisito básico que el servicio de alojamiento sea proporcionado por la misma empresa que vincula a todas las sedes con la red MPLS. De esa manera la integración y el aprovechamiento de la potencia de MPLS se verían reflejados.

A continuación se definirán las ubicaciones en los nodos:

Se recomienda alojar en el Centro de Datos externo, el o los servidores físicos que mayores recursos técnicos tenga, esto es (procesamiento, almacenamiento, etc.). El motivo de la elección se debe a que en el Centro de Datos del proveedor, se cuenta con todos los sistemas de contingencias homologados como también la refrigeración, la electricidad, la seguridad, etc. En dichos servidores se encontrarán una cierta cantidad de máquinas virtuales las que pueden corresponder a: bases de datos, aplicativos, backend, etc.

Los servidores backend son los encargados de la manipulación de los datos, es decir, se encargan de interactuar con la base de datos, verifican las sesiones de los usuarios y se encargan de “servir” todas las vistas al frontend.

El motivo por el cual alojar a los servicios principales en el Centro de Datos externo, es porque de acuerdo al esquema de red diseñado, todo el acceso a Internet será a través de una de las sedes, pero no será a través de ella el acceso a los recursos de red. Si se produjera un corte de energía en la sede en cuestión, dejaría al resto sin servicios, algo que justamente era parte de la infraestructura problemática.

De esta forma, el resto de las sedes podrá seguir su curso sin dependencia y la sede sin servicios volverá a trabajar cuando se solucionen los inconvenientes.

En el Centro de Datos local también se encontrarán alojados otros tantos servidores físicos y virtuales, de menores características técnicas, pero no por ello menos importantes. En estos servidores se podrán alojar: bases de datos secundarias, aplicativos de menor importancia, servicios de red, frontend y espacios de backups.

La siguiente ilustración esquematiza la distribución de los activos informáticos del Instituto.

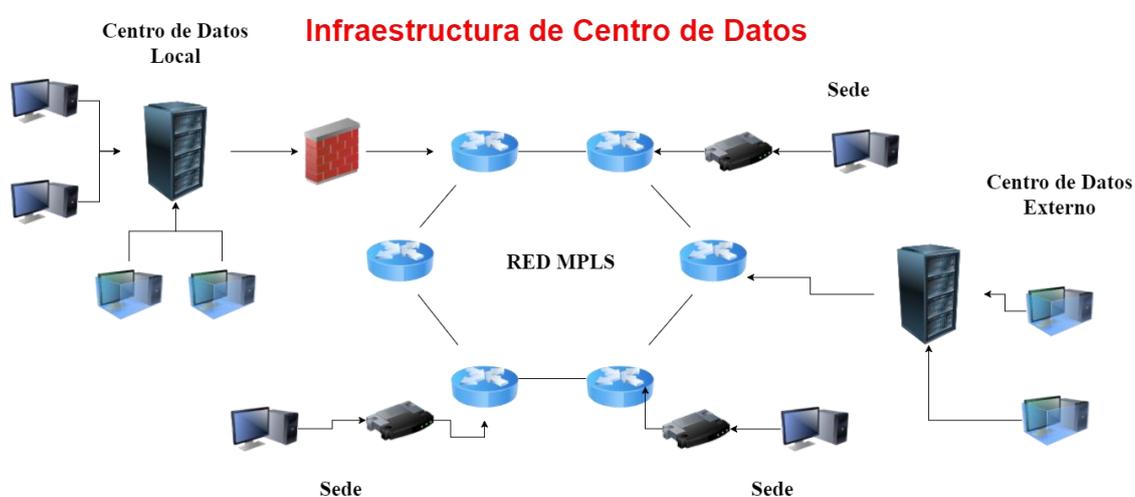


Ilustración 21. Fuente: Elaboración propia

En definitiva, no existe un ideal que permita tener siempre los accesos a los servicios 100% en línea, pero con el esquema de distribución explicado en los párrafos anteriores se logrará un punto de equilibrio, una mejora en la administración y una mayor integración con la infraestructura de telecomunicaciones soportada sobre MPLS.

4.3.1.2. Esquema de conexión de la infraestructura de Telefónica

En este punto, se detalla cómo será la infraestructura de Telefonía, tomando como referencia la siguiente ilustración.

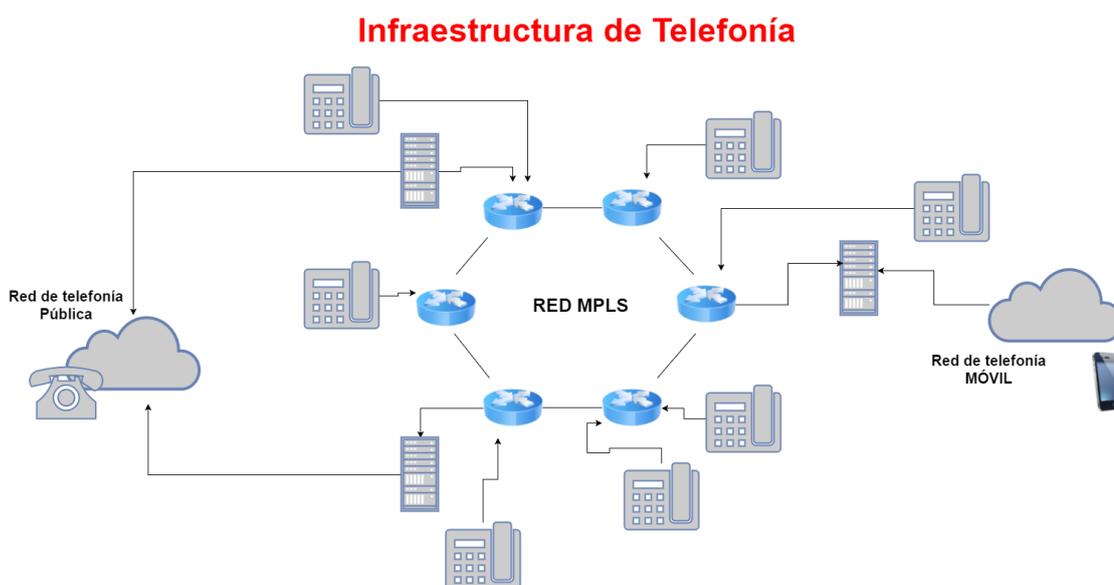


Ilustración 22. Fuente: Elaboración propia

La infraestructura estará compuesta por tres centrales con la posibilidad de incorporar módulos para telefonía IP, ubicadas en las sedes más importantes y con cierto sentido geográfico.

Utilizarán la red MPLS para que se vinculen entre ellas y de esta manera poder implementar telefonía IP en las sedes más alejadas.

Dichas centrales se deberán vincular con la red de telefonía tradicional PSTN. La elección de cuál de las centrales sería vinculada, dependerá de los costos que implica contratar la conexión de

varias centrales con la red de telefonía pública. Se recomienda que sean dos de las tres centrales ya que, ante la falla de una, se podrá seguir utilizando el servicio por las otras centrales.

De la misma manera, se deberá elegir cuál de las centrales se conectará con la red de telefonía móvil.

La comunicación entre las centrales es lo más importante de este esquema, la integración con la infraestructura de redes soportada sobre MPLS hacen posible vínculos estables, robustos y totalmente gestionable para flujo de voz.

De acuerdo al párrafo anterior, se deberán identificar los protocolos correspondientes para el establecimiento de llamadas y crear las políticas de QoS lo más optimas posibles para así lograr una comunicación rápida, clara y estable.

Las políticas deberán establecerse desde la red interna del Instituto como en la red MPLS, logrando que el flujo de información producido durante una llamada sea más estable.

Debido a la robustez de la red MPLS es que se podrán colocar teléfono IP o software VoIP en las delegaciones alejadas y, para las sedes donde estén las centrales, se podrá vincular los teléfonos de forma tradicional (par trenzado) e IP.

La telefonía IP es una gran solución cuando en una oficina, producto del crecimiento de personal o traslado del mismo no se encuentran las bocas necesarias para colocar otro teléfono. Entonces, gracias al cableado estructurado y con solo patchar un puesto en la regleta de telefonía, se resuelve el problema.

Entonces, al integrar toda la infraestructura de telefonía con la infraestructura de redes, se lograra: dar solución a la falta de telefonía en la sedes más alejadas, alternativas de conexión, estabilidad, fluidez, calidad para las llamadas, comunicación mediante alternativas por medio de la telefonía móvil y de la PSTN y, en el caso de producirse una falla en la red MPLS, al estar conectadas a través de PSTN, las sedes podrán seguir conectadas.

4.3.1.3. Controles de accesos

En el siguiente punto, se realizara un detalle de cómo será la administración y los controles para el uso de los activos informáticos, el acceso a la información y la navegación en Internet.

La metodología seleccionada para los accesos a los recursos será la utilización de listas que contengan las direcciones IP correspondientes para cada área al correspondiente recurso. Por ejemplo, si se trata del área de desarrollo, tendrán que poder utilizar aplicativos de desarrollo, testing y producción y lo mismo para la o las bases de datos.

El criterio será utilizar políticas de IP: PUERTOS

La tabla 6 muestra cómo sería el tratamiento básico para el acceso a los servicios y las aplicaciones.

	Puerto TCP	Puerto UDP
Servicio WEB	80, 443 y 8080	
Servicio de Directorio Compartido	135-139, 445	135-139
Controlador de dominio (DHCP, DNS)	119,135	53, 67-68, 88, 137-139, 389, 445

Tabla 7. Fuente: Elaboración propia

Como el acceso a estos recursos será por medio de la red MPLS, existirá un vínculo entre el Centro de Datos del proveedor y el router principal de la Institución, desde donde se manejarán los accesos a dichos servicios. Por ejemplo, si se trata de una base de datos, en el router se cargará la lista de acceso con las IP del área de análisis o desarrollo, junto con el puerto de la base usada. De esa manera se tendrá un control exhaustivo hacia los servidores y servicios.

Sea cual fuera el servidor, se utilizarán las mismas políticas de acceso: IP más puerto.

El dispositivo encargado de otorgar los accesos deberá tener una capacidad de procesamiento alta, como así la posibilidad de configuraciones de QoS, dando prioridad a los puertos de VoIP y estando en sintonía con la red MPLS.

Mediante la configuración de rutas por parte del administrador de la red MPLS, se encaminarán los accesos a los servicios por parte de las sedes hacia el Centro de Datos externo, es decir, que los servicios principales como son el DNS, DC y los aplicativos principales se deben alojar ahí.

Se lograra de esta forma, que ante una falla en la infraestructura de redes que afecte a la sede principal, no se queden sin el acceso a las herramientas de trabajo y los servicios. No tendrán acceso a Internet, pero si todos los servicios están alojados internamente y a la vez son estables, Internet será simplemente para servicios secundarios totalmente no indispensables.

5. Resultados esperables (aspectos medibles)

Antes del rediseño:

- Congestionamiento de los enlaces.
- Limitado ancho de banda.
- Enlaces inseguros.
- Debilidad de planes de contingencia.
- Red poco escalable, compleja y poco flexible.
- Criterios diferentes en lo que respecta a las administración y configuración de la red.
- Criterios diferentes en la adquisición de infraestructura de información.
- Personal distribuido sin conocimiento de las necesidades o inquietudes del otro.
- Diferentes proveedores.

Después del rediseño:

- Red Unificada, simple y escalable
- Red preparada para la evolución de Internet
- Calidad de servicio
- Ingeniera de Trafico
- Seguridad y eficiencia en el tratamiento de los datos
- Información segura.
- Planes de contingencia
- Unificación de criterios sobre el mantenimiento y la administración de la infraestructura.
- Uno o dos proveedores.
- Unificación de los pagos

6. Conclusiones

En este punto se indicarán las conclusiones a las que se llegaron a lo largo del desarrollo de la presente tesina, la cual se desarrolló con el propósito de diseñar una solución de red que unifique a todos los sistemas informáticos, mejorando la conectividad entre las sedes geográficamente distribuidas del Instituto tomado como caso de estudio; y así obtener una mejor calidad de servicio en el tratamiento de la información. Además, se considera que este diseño podrá ser aplicado a cualquier organización con similares características.

También, teniendo en cuenta el probable crecimiento y expansión de este tipo de Instituciones, basados en la incorporación de nuevas carreras y la expansión territorial mediante la apertura de sedes, es que surge la necesidad de ampliar su infraestructura, tanto para su sede principal como para las restantes, donde se llegó a observar que:

- existe congestionamiento en horas pico;
- hay limitado ancho de banda;
- los enlaces son pocos seguros;
- hay debilidad de planes de contingencia, etc.

En definitiva, este conjunto de situaciones dio lugar a una red poco flexible, poco escalable, un tanto compleja.

En síntesis, con el desarrollo de este trabajo se alcanzaron los objetivos planteados al inicio, es decir:

- A partir de la recolección de información y el estudio acerca de diferentes tecnologías WAN disponibles, se realizaron comparaciones sobre cada una de las alternativas elegidas en función de las problemáticas expuestas y, a medida que se avanzó en el análisis, se descartaron muchas de ellas porque, si bien permitían disminuir o erradicar las falencias, no se lograba una integración de todo el sistema informático.

- Se logró demostrar teóricamente que el protocolo MPLS es la tecnología que brindará la posibilidad de hacer frente al crecimiento y las demandas de los servicios informáticos para una Institución educativa u organización con sucursales descentralizadas.
- A través de su utilización, se logrará erradicar o disminuir las deficiencias detectadas en la actualidad sobre las infraestructuras de Redes (Internet e Intranet), Centro de Datos y Telefonía, logrando unificar, simplificar, optimizar e incrementar los aspectos técnicos, administrativos y económicos, como así también la productividad y el rendimiento de los sistemas y del personal que los utiliza en la Institución, cumpliendo a su vez con los objetivos planteados en lo laboral.
- Con el diseño del modelo de la nueva red de transporte de datos y comunicaciones propuesta, mediante la implementación del protocolo MPLS, se pretende flexibilizar y escalar a otras tecnologías y futuras sedes.

Finalmente, y como aspecto decisivo a tener en cuenta, es importante agregar que, en los tiempos que corren, en donde se abre el debate sobre si es mejor usar *cloud computing* en la nube o el almacenamiento privado de la información, y donde la seguridad y la privacidad de los datos son un punto crucial, este modelo permitirá gracias a su integración, flexibilidad, escalabilidad y equilibrio, un formato de nube híbrida obteniendo de cada una lo mejor.

7. Bibliografía general y especial

7.1. Libros

1. Tanenbaum; Wetherall; Redes de Computadoras; Quinta edición (2012).
2. Alejandro Corletti estrada; Seguridad en Redes; (2016).
3. William Stallings; Comunicaciones y Redes de Cumputadoras; Sexta edición; (2000).

7.2. Sitios y páginas de Internet

1. <https://tools.ietf.org/html/rfc3031>
2. <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/1311/0046T172.pdf;jsessionid=7CB17992C04DEF816090DDF924E5F86D?sequence=1>
3. <http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>
4. <http://exa.unne.edu.ar/informatica/SO/MPLS.PDF>
5. <http://www.ramonmillan.com/tutoriales/mppls.php>
6. <http://dspace.ups.edu.ec/bitstream/123456789/10297/1/UPS-GT001192.pdf>
7. <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/1311/0046T172.pdf;jsessionid=73D8C2BF2065680AE7F10A13E4AD11C6?sequence=1>
8. http://sedici.unlp.edu.ar/bitstream/handle/10915/21310/Documento_completo.pdf?sequence=1
9. http://iie.fing.edu.uy/investigacion/grupos/artes/fce/net-te/Ingenieria_de_Trafico_en_Redesc_MPLS.pdf
10. <http://www.ramonmillan.com/tutoriales/mppls.php#beneficiosmpls>
11. <https://www.dc.uba.ar/materias/tc/2012/2c/descargas/clasespracticas/mppls>
12. http://www.el.bqto.unexpo.edu.ve/~ltarazona/redes/redesc01_2.pdf
13. <http://www.isa.uniovi.es/docencia/redes/Apuntes/tema7.pdf>
14. <http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>

15. <https://docs.oracle.com/cd/E19957-01/820-2981/ipsec-mgtasks-8/index.html>
16. https://es.wikipedia.org/wiki/Red_privada_virtual
17. http://wiki.inf.utfsm.cl/index.php?title=Point-to-Point_Protocol
18. https://es.wikipedia.org/wiki/Point-to-Point_Protocol
19. <https://books.google.com.ar/books?id=yTSoYCiXYAAC&pg=PA219&lpg=PA219&dq=descripcion+de+ppp+protocolo&source=bl&ots=F3qVUF8tq4&sig=Xct-exEOIDJ59TQPFmgF1w91bb0&hl=es&sa=X&ved=0ahUKEwjCgfPPzMzQAhXFD5AKHbu1DowQ6AEIUDAI#v=onepage&q=descripcion%20de%20ppp%20protocolo&f=false>
20. http://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/indata/v04_n1/tecnologia.htm
21. https://www.mhe.es/cf/ciclos_informatica/844819974X/archivos/unidad2_recurso6.pdf
22. https://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital_asim%C3%A9trica
23. <http://www.ramonmillan.com/tutoriales/adsl.php>
24. <https://es.wikipedia.org/wiki/Cablem%C3%B3dem>
25. <http://www.interxion.com/es/centros-de-datos/>
26. https://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos
27. http://www.cisco.com/c/es_mx/solutions/data-center-virtualization/index.html
28. <http://conceptodefinicion.de/data-center/>
29. <http://definicion.de/centro-de-computo/>
30. https://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red
31. <http://redestipostopologias.blogspot.com.ar/2009/03/topologia-de-redes.html>
32. www.bloginformatico.com/topologia-de-red.php