6. Implantación de la Alternativa elegida

Antes de la implantación voy a explicar de forma somera como funciona la alternativa elegida. Para posteriormente implantarla la solución con los requerimientos descritos.

6.1 MPLS

MPLS (Multiprotocol Label Switching) es un esquema similar pero no igual a la "encapsulación" por la que una PDU[21] de un protocolo cualquiera puede ser transportada en una "PDU" del protocolo MPLS como si de datos de un nivel superior se tratara, añadiéndole su redundancia, etcétera.

MPLS es un esquema de envío de paquetes que no está formado exclusivamente por un protocolo que "encapsula" a otros sino que define y utiliza conceptos como FEC, LSR, dominio MPLS, LDP, ingeniería de tráfico… En los siguientes puntos explicaré estos conceptos.

Ilustración 6-1: Posición de MPLS dentro del modelo de referencia OSI

MPLS se encuentra situado entre los niveles de enlace y de red del modelo de referencia OSI; por tanto se podría decir que es un protocolo de nivel 2+. Esto a efectos prácticos significa que hace de nexo de unión entre los protocolos de red y el protocolo de nivel de enlace.

La cabecera de un paquete MPLS se encuentra también entre estos dos niveles, por tanto, entre la cabecera del nivel de enlace y la cabecera del nivel de red; de esta forma,

[21] *PDU: Protocol Data Units:* (Unidades de Datos de Protocolo). Se utiliza para el intercambio entre unidades parejas, dentro una capa del modelo OSI

para el protocolo de nivel de enlace un paquete MPLS serán datos empaquetados de niveles superiores del modelo OSI.

En la siguiente figura se puede apreciar lo comentado.

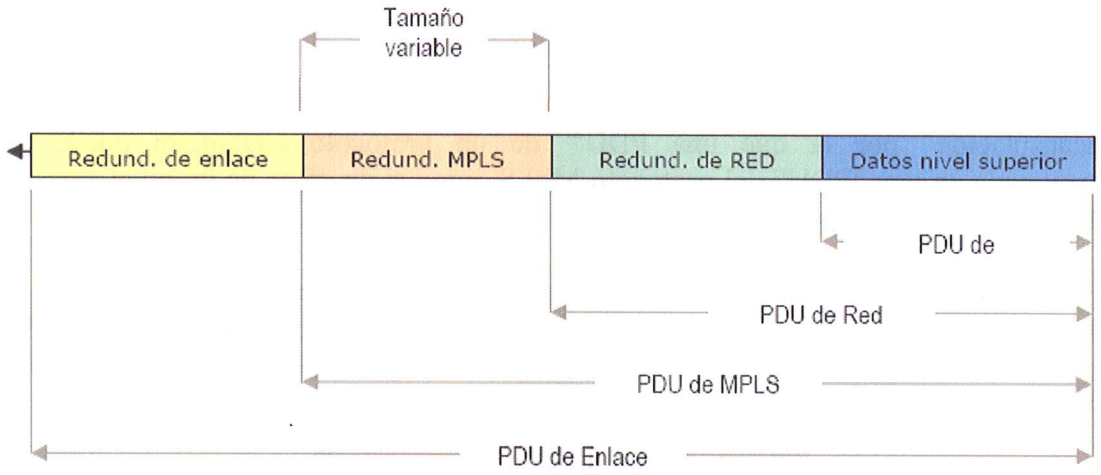


Ilustración 6-2: Posición de la cabecera MPLS dentro de una PDU

Para poder continuar explicado el funcionamiento de MPLS con propiedad voy a definir la terminología común básica que IETF[22] propone.

LER (Layer Edge Router): router frontera entre capas. Es el encaminador que se encuentra en el borde de la zona MPLS y se encarga de añadir cabeceras MPLS entre las cabeceras de red y de enlace de paquete entrante. Además también es el encargado de retirar esta información cuando un paquete sale de la zona MPLS.

LSR (Label Switch Router): conmutador de etiquetas. Sería el conmutador del interior de la zona MPLS que interpreta el valor de la cabecera MPLS y la modifica si es necesario. En principio no añade ni elimina cabeceras MPLS.

FEC (Forward Equivalente Class): clase de envío equivalente. Es el conjunto de paquetes o flujos de información a los cuales, tras entrar en la zona MPLS se le añade una cabecera que hace que sean tratados todos de la misma forma, independientemente de que sean paquetes de distintos tipos de tráfico. A efectos prácticos, es el conjunto de paquetes que ingresan por un mismo LER y a los cuales éste les asigna la misma etiqueta.

LSP (Label Switched Path): camino conmutado de etiquetas. Es el camino que describen el conjunto de encaminadores y conmutadores que atraviesan los paquetes de un FEC concreto en un único nivel jerárquico en cuanto a la zona MPLS de la que se está hablando. Todos los paquetes del mismo FEC siguen siempre el mismo LSP, de principio a fin dentro del dominio MPLS.

[22] *IETF: Internet Engineering Task Force*: organización internacional de normalización.

Label o Etiqueta: información o cabecera que se añade a un paquete cuando ingresa en una zona MPLS. Es la información que añade o quita el LER y que es interpretada por el LSR, gracias a la cual se entiende que diferentes tráficos forman parte de un mismo FEC. Generalmente la etiqueta define el FEC en el que se incluirá el paquete.

LS (Label Snack): pila de etiquetas. Es un conjunto de etiquetas dispuestas en forma de pila. Esto se utiliza porque pueden existir zonas MPLS dentro de otras zonas MPLS, gracias a esta característica se puede proporcionar esta escalabilidad.

Dominio MPLS: es el conjunto de encaminadores contiguos capaces de trabajar con MPLS para enrutamiento y/o conmutado encontrándose dentro de un mismo ámbito administrativo.

6.1.1 Estructura y características de un paquete.

La cabecera de un paquete MPLS tiene un tamaño fijo de 32 bits (4 octetos). Ningún campo es de tamaño variable y además siempre se encuentran localizados en la misma posición. Los encaminadores y conmutadores MPLS siempre leerán estos 4 octetos tras la redundancia de enlace.

6.1.1.1 Campos

Cada cabecera MPLS tiene 4 campos: Label, EXP, S y TTL dispuestos como se muestra en la siguiente figura.

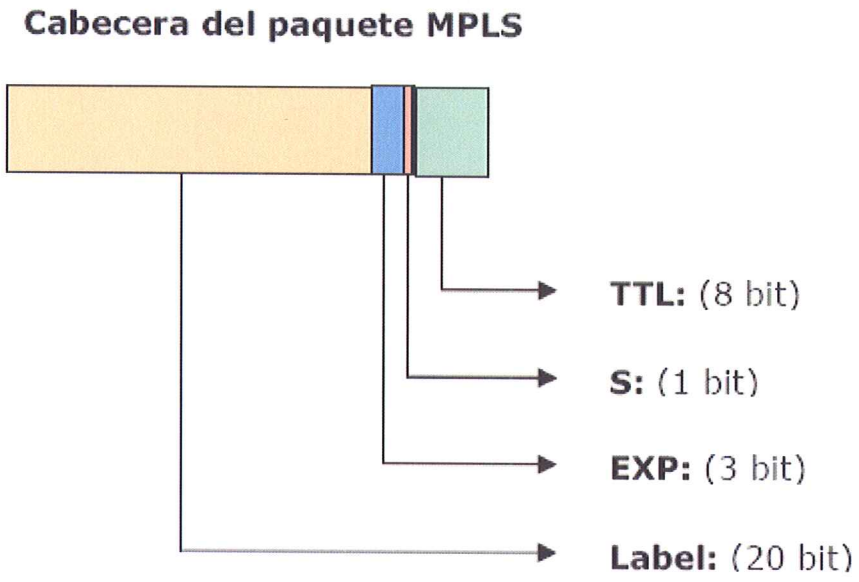


Ilustración 6-3: Estructura de la cabecera de un paquete MPLS

TTL (Time To Life): es el típico campo de casi cualquier paquete de datos que especifica el número de encaminadores por los que el paquete puede pasar antes de ser descartad. Como máximo podrá se en este caso 65536 saltos. El campo TTL puede tomar el valor del campo TTL del protocolo de red del paquee (si procede) e irse decrementando en cada salto por los encaminadores del dominio MPLS para posteriormente sustituir al valor de TTL del paquete original al salir del dominio MPLS.

S (Snack Bottom): cuando está a 1 indica que esta cabecera MPLS es la última que hay antes de encontrarse con la redundancia de red. Si está a 0, indica que tras esta cabecera MPLS se encuentra otra cabecera MPLS y no la cabecera de red.

EXP (Experimental): estos bits están reservados para uso experimental. Sin embargo se pueden utilizar para albergar información sobre calidad de servicio del paquete.

Label: es la etiqueta MPLS, la que da nombre al protocolo. Cuando un paquete ingresa en un dominio MPLS se le asigna una etiqueta que marcará el resto de su viaje a través de la red MPLS.

6.1.1.2 Estructura de la pila de etiquetas

MPLS "encapsula" cualquier protocolo en un paquete MPLS, aunque este protocolo sea también MPLS. Cuando un paquete entra en un dominio MPLS se le añade una cabecera que tendrá hasta que salga de dicho dominio MPLS. Si durante el trayecto interior el paquete ya etiquetado se introduce en otro dominio MPLS sin haber salido del primero, se le añade una cabecera MPLS más, pero en este caso hay que indicar marcando el campo S con un cero que esa cabecera no es la última existente sino que tras esta hay otra.

De esta manera cuando un paquete MPLS abandona un domino MPLS el enrutador que le de la salida sabrá si debe enlutar el paquete con las reglas MPLS o si bien ya no hay más dominios MPLS y se debe encaminar el paquete con las reglas del protocolo de red que lo haya generado.

Creemos un ejemplo:

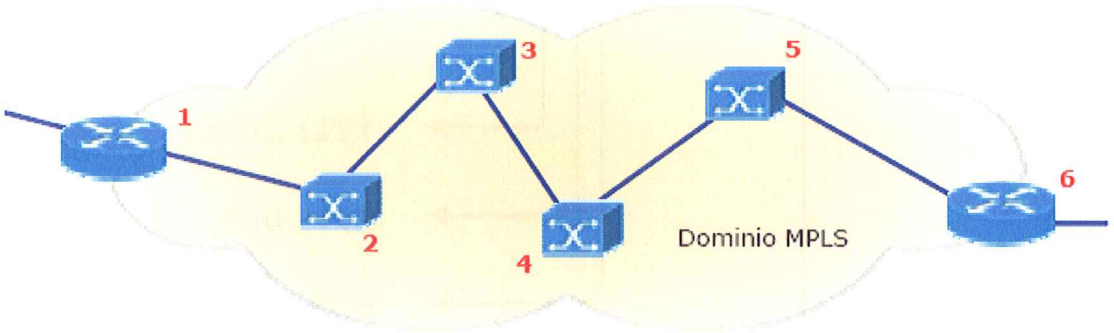


Ilustración 6-4: Ejemplo de dominio MPLS

Siguiendo la figura anterior, supongamos que un paquete entra en el domino MPLS, el enrutador 1 le inserta una cabecera MPLS entre sus cabeceras de enlace y de red. El paquete se encamina hacia el conmutador 2 el cual, simplificando, decrementa el campo TTL manteniendo la misma cabecera MPLS, sin añadir ni colocar nada. A continuación el conmutador 2 envía el paquete al conmutador 3. El proceso de TTL se repetirá en los conmutadores 3, 4 y 5, en caso de llegar a cero TTL el paquete será desestimado, supongamos que esto no sucede, cuando el paquete sea enviado del conmutador 5 al enrutador 6 nos encontraremos con el límite del dominio MPLS, esto será detectado por el campo S de la cabecera MPLS.

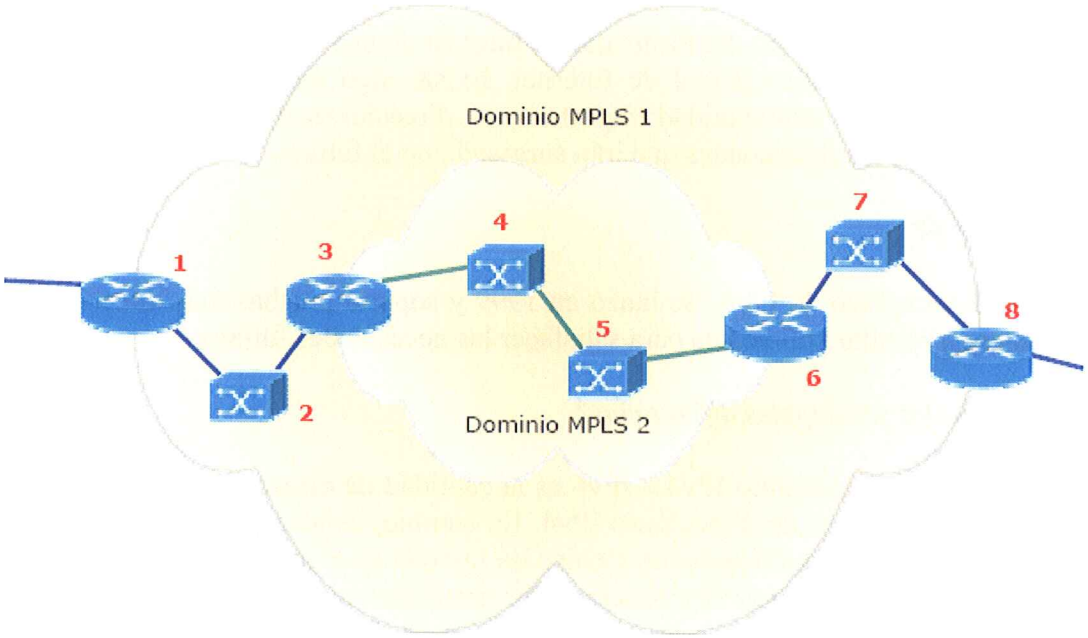


Ilustración 6-5: Ejemplo de multidominio MPLS

Sobre la figura anterior, se utilizaría la pila de etiquetas, el enrutador 1 pondría etiqueta MPLS del dominio 1 poniendo el campo S a uno y enviando el paquete al encaminador 2 que solamente modificaría el TTL y enviaría el paquete hacia en enrutador 3, el cual incorporaría otra etiqueta conteniendo en su campo de datos la anterior, modificando el campo S a cero enviaría este paquete al encaminador 4.

Al llegar el paquete al enrutador 6 se comenzará a deshacer la pila de etiquetas, quitando la primera y enviando el paquete con metodología MPLS al ver que el campo S esta a cero. Posteriormente a la eliminación de etiqueta el paquete será enviado al encaminador 7, que solamente realizará la acción de TTL y encaminará hacia el enrutador 8 el cual realizará la misma función que el enrutador 6 con la excepción de que verá que el campo S esta a uno, significando que el paquete será enviado con la mitología de la capa de red.

El proceso de introducirse en múltiples dominios MPLS antes de salir de algunos de ellos se puede repetir tantas veces como sea necesario y por cada dominio MPLS en el que se encuentra el paquete tendrá una cabecera MPLS.

Sin embargo hay un problema subyacente en lo que he explicado y es el siguiente:
Cuando un LER de salida de un dominio MPLS detecta que la cabecera MPLS del paquete es la última, sabe que lo siguiente que encontrará será la cabecera de red y que deberá usarla para encaminar el paquete conforme a los mecanismos de este tipo de red. MPLS soporta cualquier protocolo de red, y una cabecera IPv4 no tiene la misma estructura que la cabecera de IPv6 por lo que el LER aún sabiendo que es una cabecera de red, no sabe de que tipo es ¿Cómo soluciona esta situación LER?

6.1.2 Diferencia entre IPv4 e IPv6

¿Qué es IPv4?

IPv4 fue la primera versión del Protocolo de Internet de uso masivo, y todavía se utiliza en la mayoría del tráfico actual de Internet. Existe algo más de 4.000 millones de direcciones IPv4. Es una cantidad importante de direcciones IP, pero no es suficiente para cubrir todas las necesidades que irán surgiendo en el futuro.

¿Qué es IPv6?

IPv6 es el reemplazo de IPv4. Se lanzó en 1999 y soporta muchas más direcciones IP, que deberían resultar suficientes para satisfacer las necesidades futuras.

¿Cuáles son las principales diferencias?

La principal diferencia entre IPv4 e IPv6 es la cantidad de direcciones IP. Existen algo más de 4.000 millones de direcciones IPv4. En cambio, existen más de 16 trillones de direcciones IPv6. El funcionamiento técnico de Internet es el mismo en ambas versiones y es posible que ambas continúen funcionando simultáneamente en las redes.
En la actualidad, la mayoría de las redes que usan IPv6 soportan tanto las direcciones IPv4 como las IPv6 en sus redes.

	Protocolo Internet versión 4 IPv4	Protocolo Internet versión 6 IPv6
Lanzado en	1981	1999
Tamaño de las direcciones	Número de 32 bits	Número de 128 bits
Formato de las direcciones	Notación decimal con puntos 192.168.1.16	Notación hexadecimal 2001:500:4::/48
Cantidad de direcciones	$2^{32} = \sim 4$ mil millones de direcciones	$2^{128} = \sim$ 16 trillones de direcciones

Tabla 6-1: Diferencias entre protocolo IPv4 y IPv6

Las cabeceras de los dos protocolos tienen muchas diferencias, este es un problema con el que se encuentra MPLS.

Cabecera IPv4:

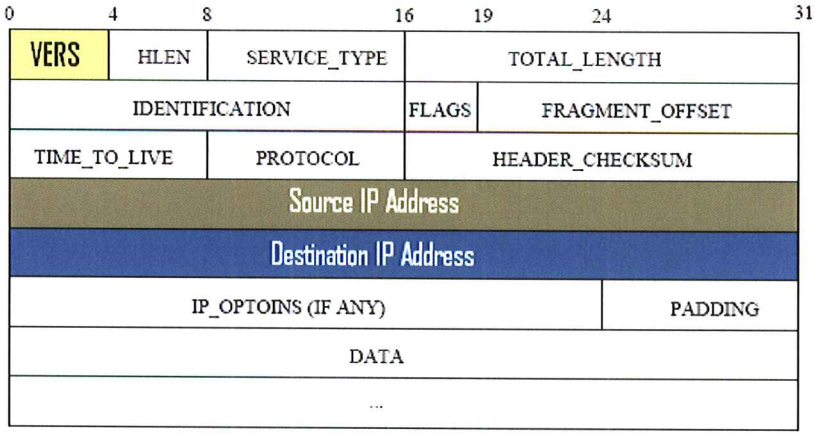


Ilustración 6-6: Cabecera IPv4

Simplificaciones más importantes:

- Formato fijo para todos los headers: no hay elementos opcionales
- No se hace checksum del header
- No hay fragmentación (excepto entre las puntas, path MTU discovery)

Cabecera IPv6:

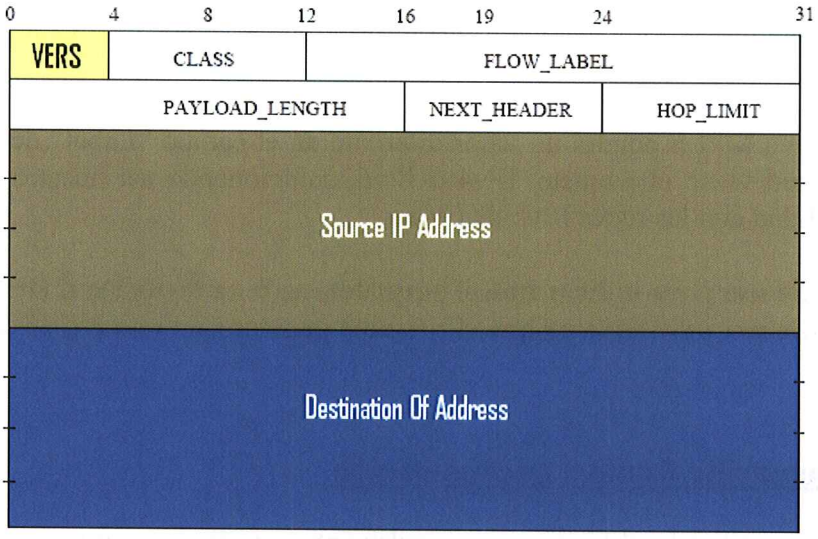


Ilustración 6-7: Cabecera IPv6

Campos eliminados o permutados:

- IHL o HLEN: ya no es necesario, porque todos los headers tienen el mismo largo
- Se eliminan los campos relativos a la fragmentación (Flags y Fragment Offset)
- TOS (Service_type): se elimina.
- Total_length se reemplaza por payload_length. Como son 16 bits, el máximo largo de un paquete es de 64k (excepto opción Jumbogram).
- Protocol type: se modifica por next_header (este último puede apuntar además a headers de extensión)

- TTL se renombra a HOP_COUNT: no cambia en la práctica.

Campos nuevos:

- Flow label: usado para distinguir "paquetes que requieren el mismo tratamiento" (que van de un mismo origen a un mismo destino con las mismas opciones). Usado para transmisiones "real time".

6.1.2.1 Como soluciona MPLS la diferencia entre IPv4 e IPv6

Un LER de salida de un dominio MPLS cuando detecta que la cabecera a eliminar es la última cabecera MPLS sabe que debe encaminar el paquete conforme a los mecanismos de red. LER para encaminar este paquete debe saber que de tipo de protocolo de red es la cabecera que contiene para poderla leer, entender y enviar.

El mecanismo de solución de este problema no esta debidamente documentado, debido a lo novedad del método. La última etiqueta MPLS (la primera que se añadió al paquete), llevará el campo S=1, al ver esto LER sabe que no es una cabecera normal, ya que en su campo "Label" lleva un valor de un rango de valores reservados que indican a que tipo de red pertenece el paquete; por lo tanto cuando un LER de salida detecta en un paquete MPLS el campo S=1, analiza el campo "Label" donde se le indicará el tipo de cabecera de red que se va a encontrar a continuación, gracias a esto LER será capaz de entender lo que éste le diga.

Por este motivo MPLS pondrá un valor diferente en el campo "Label" dependiendo de que tipo de red viene el paquete, IPv4 o IPv6, solucionando así nuestro problema de incompatibilidad con las redes IPv6 de China.

Label ='0': Se usa para indicar que el paquete proviene de una red IP versión 4.
Label ='2': Se usa para indicar que el paquete proviene de una red IP versión 6.

6.1.3 Etiquetación frente a encapsulación

Hasta ahora he utilizado el término encapsular entrecomillado porque realmente MPLS no encapsula la información sino que la etiqueta. Cuando se encapsula un protocolo en otro, se construye una PDU_{N-1} del protocolo que encapsula utilizando la información de la PDU_N del protocolo encapsulado, por tanto se adapta el tamaño de la PDU_N de la capa superior y se prepara para ser enviada como una PDU_{N-1}.

MPLS no lo hace así, sino que toma la PDU de red y la deja y transmite intacta; únicamente coloca una redundancia MPLS entre esta cabecera y la cabecera de enlace; esto significa que si el protocolo de red tiene tramas de tamaño fijo y pequeño, MPLS transmitirá con esas características. En la siguiente figura si expresa.

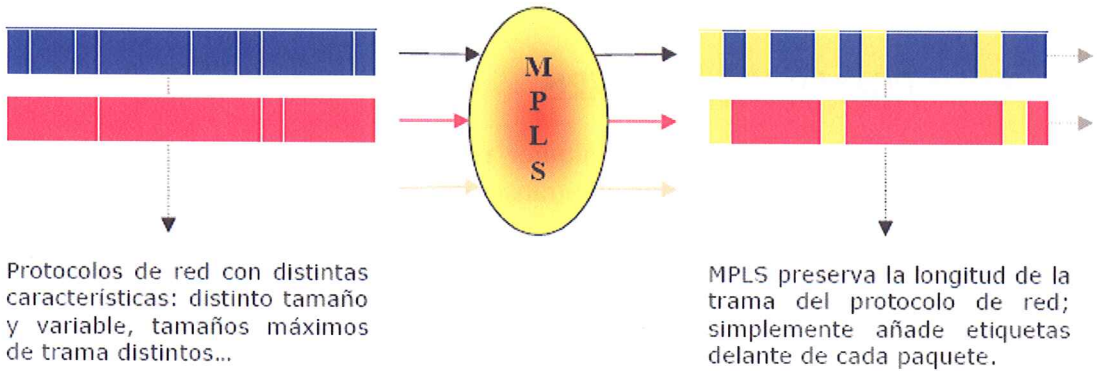


Ilustración 6-8: Preserva de longitud en del protocolo MPLS

6.1.4 Integración de IP y ATM

MPLS es un multiprotocolo como su nombre indica, esto significa que permite cualquier protocolo por encima, pero también permite cualquier tecnología de nivel de enlace o físico por debajo, por lo que se puede aprovechar fácilmente la infraestructura actualmente desplegada en el ámbito troncal. Esto es un punto a favor muy importante, puesto que facilita la migración de tecnologías.

A pesar de esto tiene un punto en contra, evidentemente al añadir complejidad el rendimiento siempre es pero. El caso es que los millones que han estado invirtiendo desde hace años las operadoras para tener IP sobre ATM siguen sirviendo para IP sobre MPLS y MPLS sobre ATM. Esto no nos implica puesto que contrataremos un servicio con unas capacidades establecidas.

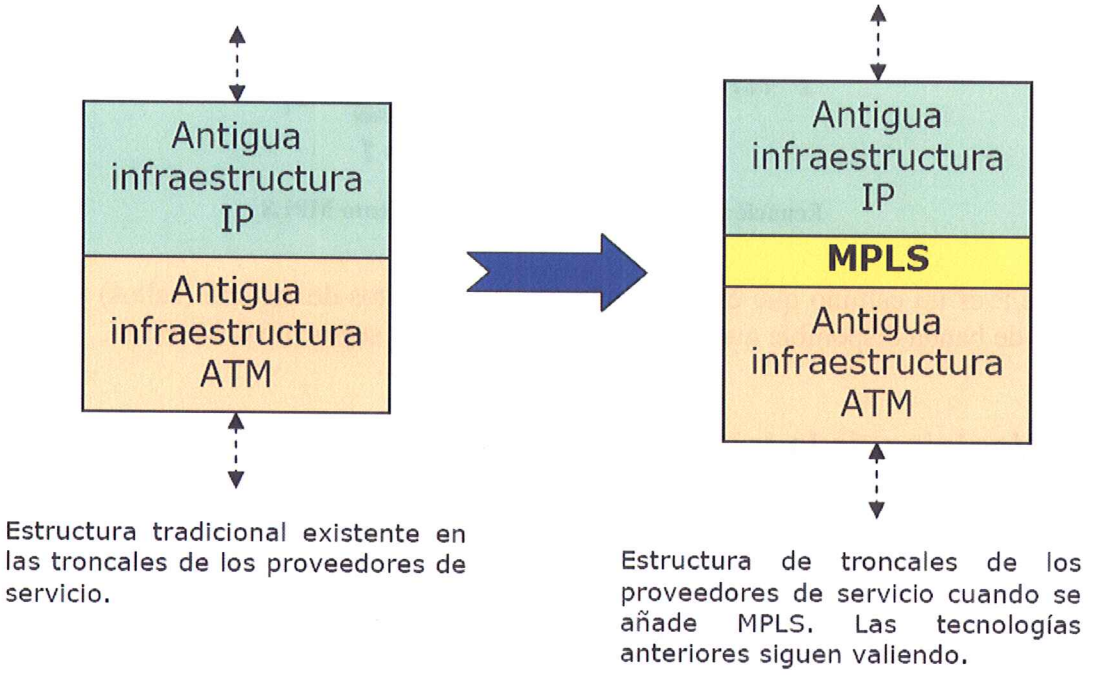


Ilustración 6-9: Posicionamiento MPLS dentro de la estructura de troncales

6.1.5 Redes Privadas Virtuales - VPN

Por el motivo anterior, al soportar cualquier protocolo y al estar el reenvío MPLS basado en etiquetas y no en los datos que transporta, cualquier cosa que esté creada por encima del nivel de enlace, será soportada fácilmente por MPLS y así es el caso de las redes privadas virtuales (VPN), se basen en túneles IP, en protocolos seguros como IPSec (como el que implantaremos) o cualquier otra tecnología.

6.1.6 Clases de servicio y QoS

Como he comentado en el punto 6.1.1.1 la propia cabecera MPLS tiene un campo EXP de 3 bits que se puede redefinir para diferenciar las clases de servicio distintas que la operadora quiera ofrecer. Implementando el modelo de servicios diferenciados propuesto por IETF.

Gracias a esto MPLS tiene una capacidad radicalmente distinta al paradigma del tráfico *best effort* / servicios integrados.

De todas maneras, MPLS no tiene definido aún un método por el cual los protocolos de encaminamiento sean capaces de calcular una ruta con restricciones de calidad de servicio y ancho de banda. El IETF está trabajando en extensiones para que los algoritmos de encaminamiento tradicionales puedan soportar esta característica. A pesar de esto se puede conseguir que para un LSP con requerimientos de ancho de banda pueda calcular una función de encaminamiento tal que:

$$Función\ (P) = \sum_{i=1}^{k} \frac{1}{r_i}$$

Ecuación 6-1: Función de encaminamiento MPLS

Donde P es un camino que está formado por k segmentos de camino (saltos) y r_i es el ancho de banda disponible que ofrece el canal para cada segmento del camino.

6.2 Ventajas de la tecnología elegida respecto a las otras

He comentado durante las páginas anteriores varias ventajas que ofrece MPLS, en este punto haré una relación de las que para el proyecto considero más importantes.

- MPLS es un esquema de reenvío de paquetes independiente tanto a la tecnología de nivel de red que esté sobre él, como de la de enlace que esté por debajo. Esto posibilita que se puedan aprovechar tecnologías existentes mientras se migra a otras más modernas.

- Es una tecnología escalable. Debido a la estructura de pila de etiquetas MPLS permite construir jerarquías de dominios MPLS por lo que se puede pasar de ámbitos más reducidos a ámbitos más globales de forma casi transparente.
- Permite usar cualquier protocolo de distribución de etiquetas tradicional o de última generación.
- Soporta el modelo de servicios diferenciados de IETF.
- Es orientado a la conexión por lo que los paquetes llegan en orden desde el origen del destino MPLS hasta el destino.
- No encapsula las tramas de red sino que les coloca una etiqueta, dejándolas con el mismo tamaño y propiedades que como le llegaron.
- Proporciona una conmutación basada en etiquetas que es rápida y eficiente.
- Realiza una única clasificación de los paquetes entrantes al dominio MPLS por lo que este proceso se reduce enormemente con respecto a tecnologías como IP.
- Permite caminos virtuales con calidad de servicio y ancho de banda asegurados si se usan los protocolos de enrutamiento y señalización de etiquetas convenientes.

6.3 Necesidades Plan escogido

Hay una necesidad clara que es la calidad de servicio QoS[23].
Pero primero debo definir que es calidad de servicio y las diferencias entre lo recibido y la percepción de lo recibido.
La calidad de servicio es la capacidad de dar un buen servicio, las operadoras para ello usan tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*).

La calidad de servicio viene requerida por el cliente siguiendo el siguiente esquema:

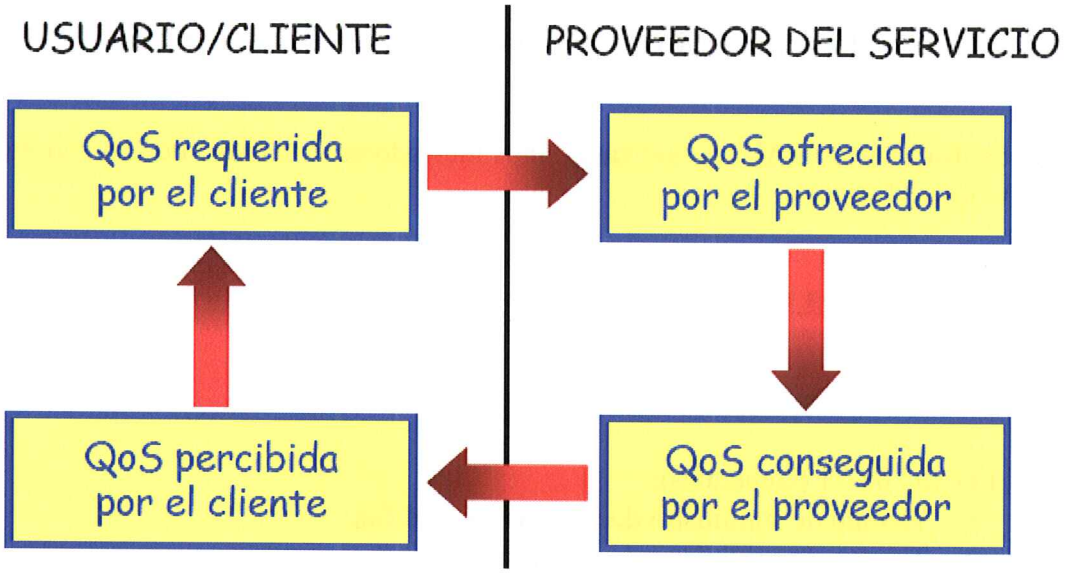


Ilustración 6-10: Esquema de requerimiento de calidad

[23] *QoS: Quality of Service:* son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio.

Diferencias entre la prestación y percepción de la QoS

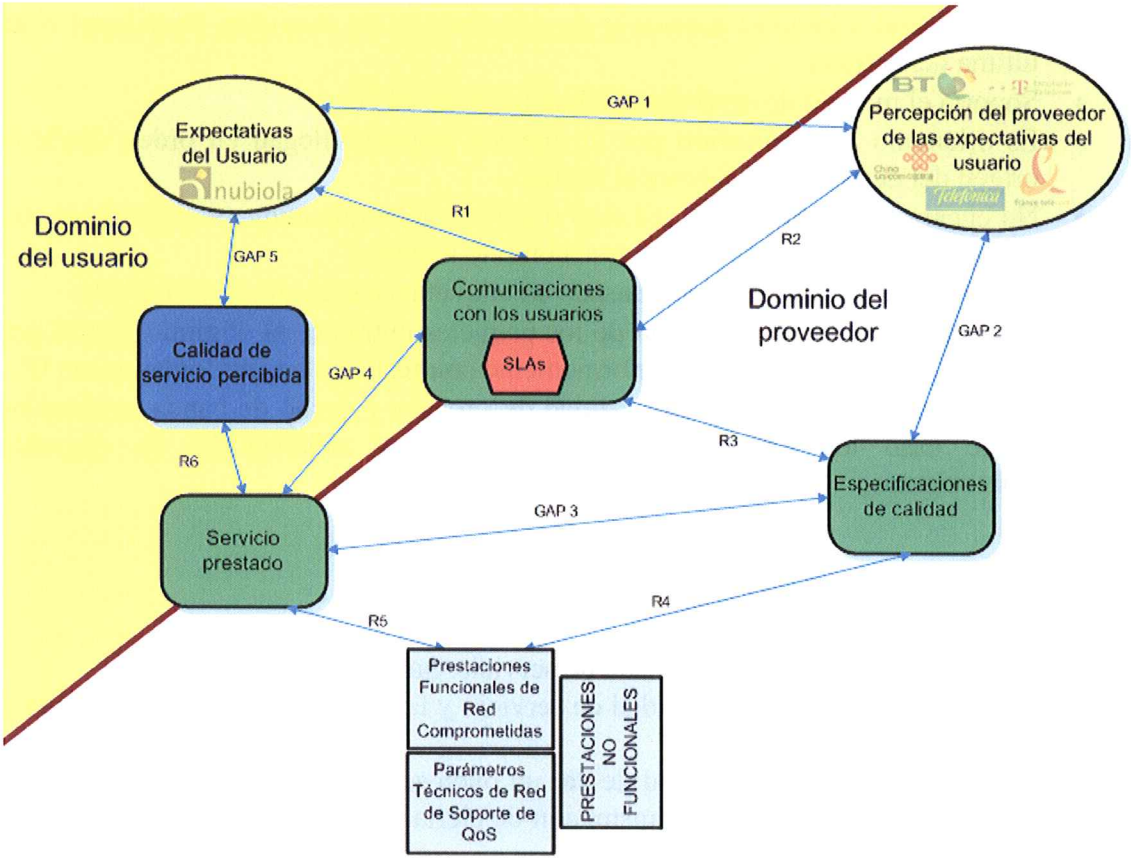


Ilustración 6-11: Diferencias entre la prestación y la percepción de la QoS

En la figura anterior se puede apreciar como puede haber cinco puntos "GAPS" donde se puede distorsionar la prestación y percepción del servicio, con lo cual puede no satisfacerse las necesidades de calidad.

Para controlar estos GAPS se utilizarán unos indicadores de calidad de servicio durante todo el uso del mismo.

6.3.1 Indicadores de QoS:

Indicadores normalizados de calidad de servicio

ETSI EG 202 057-1 (Generales):

- Tiempo de suministro de accesos a la red fija.
- Tiempo de suministro de accesos a Internet.
- Tiempo de reparación de averías.
- Tiempo de respuesta para los servicios de operador.
- Tiempo de resolución de reclamaciones.
- Profesionalidad de la línea de atención.

ETSI EG 202 057-2 (Voz, Fax, datos módem y SMS):

- Proporción de comunicaciones fallidas.
- Tiempo de establecimiento.
- Velocidad de transmisión de datos conseguida.
- Proporción de transmisiones de datos fallidos.
- Retardo (tiempo en un sentido de transmisión).

Estos indicadores de calidad seleccionados son solo algunos descritos en la ORDEN DE CALIDAD 2006 (Orden ministerial ITC/912/2006, de 29 de marzo).
Esta norma ministerial pretende establecer unas condiciones mínimas de calidad en la prestación de servicios de telecomunicaciones.

Indicadores no regulados de calidad de servicio

La orden de calidad 2006 no incluye ciertos servicios del mercado de las telecomunicaciones por este motivo se pactan indicadores no regulados con la compañía operadora.

Se pacta:

- SLO, Service Level Objective
  - Los operadores pueden incluir en sus ofertas y catálogos de servicios, indicadores de los niveles de calidad que esperan alcanzar.
- SLA, Service Level Agreement = Acuerdo de Nivel de Servicio, ANS.
  - Se pacta que para algunos de los parámetros se acepte una responsabilidad contractual en caso de incumplimiento.
  - Se pacta una compensación, generalmente económica, por el incumplimiento del SLA llamadas "penalizaciones"

Para proyectos especiales, grandes redes, servicios con QoS especiales, como seria este. Los operadores preparan soluciones a medida que permiten alcanzar los niveles de calidad requeridos. Con configuraciones de líneas y equipos especiales para obtener la máxima fiabilidad.

Un ejemplo de SLA pactado sería el siguiente:

SLA: Parámetro Retardo de tránsito en la red

Definición:

- El Retardo en red es el tiempo de transmisión medio en milisegundos entre los nodos de la red donde se conectan las distintas sedes.
  Se considera como tiempo de transmisión, el tiempo de ida y vuelta de un paquete de prueba.

Cálculo:

- El sistema de Gestión de Red realizará medidas periódicas de retardo entre los distintos nodos de la Red, generando una tabla con las sucesivas medidas.
- Diariamente se calculará la media aritmética de estas medidas para obtener un valor único para cada clase de servicio.

Condiciones:

- Al ser un parámetro de la red, no van incluidos en el cálculo de los tiempos los correspondientes a los accesos.
- Se excluyen los retardos relativos a los periodos programados de mantenimiento y actualización.

6.4 Desarrollo del plan escogido

Una vez seleccionada la alternativa global a implantar se solicita a la compañía que nos ofrece el servicio MPLS un sistema para interconectar las sedes locales con unas velocidades mínimas que vamos a marcar para cada país sobre la alternativa elegida.

Si nos planteamos esta pregunta sobre banda ancha la primera respuesta que surge es ADSL, y esta es la respuesta recibida.

ADSL es un tipo de línea DSL que consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva cualquier línea telefónica convencional, eso si, siempre y cuando el alcance no supere los 5,5 Km. medidos desde la Central Telefónica hasta el punto de conexión.

Pero para poder decidirnos por esta alternativa tenemos que contar con tres factores más.

- Como su nombre indica *Asymmetric **D**igital **S**ubscriber **L**ine* es asimétrica debido a que la velocidad de descarga (desde la red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la velocidad de descarga es mayor que la de subida.

- No todas las líneas telefónicas pueden ofrecer este servicio, debido a que las exigencias de calidad del par, tanto de ruido como de atenuación, por distancia a la central, son más estrictas que para el servicio telefónico básico. Esto puede ser un problema en nuestros países en vías de desarrollo.

- Debido al cuidado que requieren estas líneas, el servicio no es económico en países con pocas o malas infraestructuras, sobre todo si lo comparamos con los precios en otros países con infraestructuras más avanzadas.

Una vez valorados los tres puntos deberemos solicitar un estudio para cada localización a interconectar, para saber si podemos disponer de este servicio o no, y con que velocidades máximas podremos conseguirlo.

Voy a representar en el siguiente esquema la situación Ideal como solución a nuestro problema de interconexión entre las diferentes sedes locales. Esta solución marca cada ADSL como una línea de 3Mb que como solución ideal las considero simétricas.

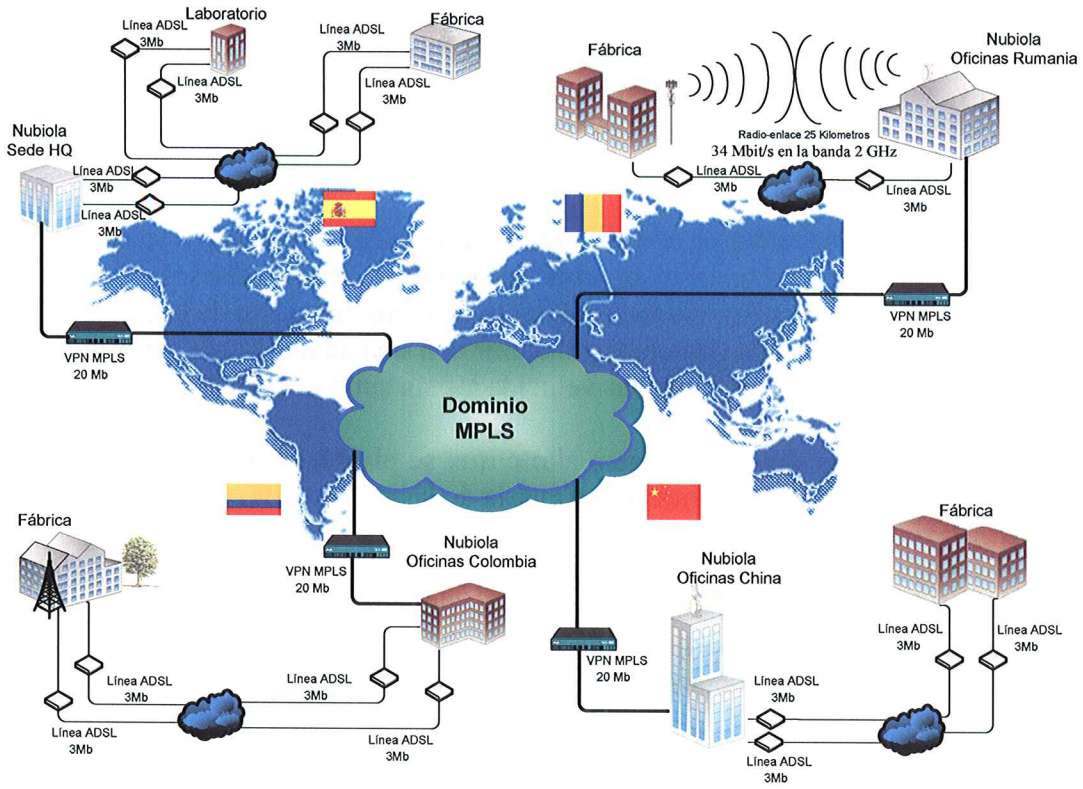


Ilustración 6-12: Solución de comunicaciones globales ideal después de la realización del proyecto

Una vez vista la situación ideal y recibiendo las soluciones aportadas a cada situación, la solución realizable será la siguiente:

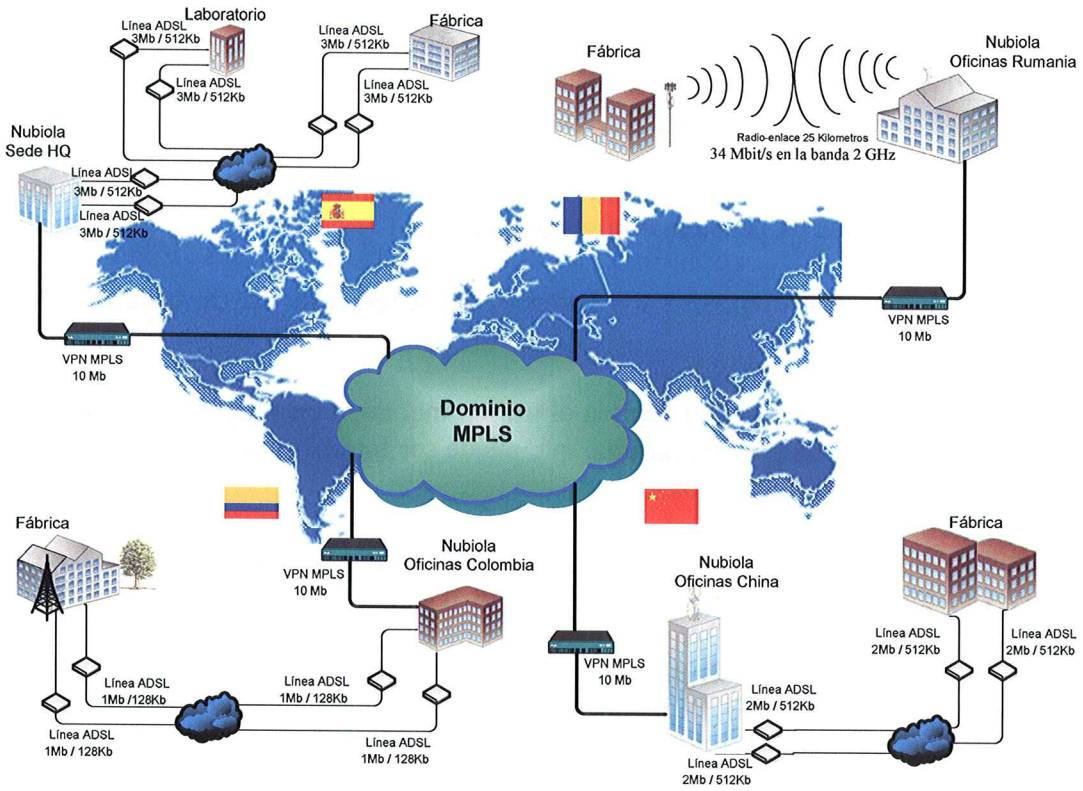


Ilustración 6-13: Solución de comunicaciones globales real después de la realización del proyecto

Curiosamente el único emplazamiento donde no se puede instalar una línea adsl es Rumania, el motivo es la distancia con la centralita telefónica, con el handicap de ser esta a su vez analógica. Por este motivo considero como mejor opción continuar usando el radio enlace, a la espera de un futuro proyecto de remodelación de esta comunicación en si. Como podría ser un cambio por WiMax[24].

En Colombia nos encontramos con una situación de bajas velocidades ya sea de subida como de bajada con un alto coste en proporción con los demás países. Esta situación es la surgida en todos los países europeos al inicio de la implantación de la banda ancha, se sabía de antemano que nos podíamos encontrar con una situación así, pero la previsión es que en los próximos años suban las velocidades sin subir el coste de la misma.

En España las líneas simétricas tienen alto coste, se planteará en caso de no funcionar adecuadamente las elegidas solicitar la simetría de las mismas.

Por último, las comunicaciones en China no tan potentes como deseábamos pero aún así son superiores a las de Colombia. El motivo de esta diferencia es por el emplazamiento de las sedes (Shanghai) y porque China esta implantando las últimas tecnologías, sin tener que sustituir infraestructuras actuales puesto que no existían.

6.5 Seguridad y criterios de encriptación

En este punto trataré la seguridad informática para en asegurar que los recursos del sistema de comunicación, en conjunto con la información que circula por el sistema de la organización sean utilizados de la manera y recibidos por las personas que se encuentren en la organización, acreditadas y dentro de los límites de su autorización.

6.5.1 VPN

Tecnología VPN
El nuevo modelo basado en la centralización de la información y de los recursos de conectividad, plantea un problema: la seguridad.

Si bien es importante compartir los recursos de la red, esto ha de hacerse de forma segura.

Para esto se creó la VPN, la cual envía el tráfico mediante un túnel privado más seguro a través de una red pública compartida, que puede ser Internet o, en el caso de MPLS, la red de un proveedor de servicios.

Las redes ATM y Frame Relay han permitido aumentar la capacidad y la velocidad de las WAN, ofreciendo una mayor facilidad de gestión mediante el uso de circuitos virtuales Frame Relay o ATM. No obstante, estas dos tecnologías de conexión en red tienen una capacidad limitada para transportar diferentes tipos de tráfico y están dando paso a nuevas alternativas VPN basadas en Protocolo Internet (IP). Estas VPN permiten una mayor flexibilidad, pues soportan distintos tipos de información en la red. Por este

[24] *WiMAX: Worldwide Interoperability for Microwave Access:* estándar de transmisión por ondas de radio de ultima generación orientada a la última milla que permite la recepción de datos por microondas y retransmitirla por ondas de radio

motivo las VPN basadas en IPSec y MPLS representan el siguiente nivel de la tecnología WAN, permitiendo la creación de redes multiservicio capaces de transportar cualquier tipo de tráfico.

Aunque el concepto de VPN continúa siendo el mismo, las nuevas VPN ofrecen hoy una mayor funcionalidad y un nivel de seguridad superior, así como la capacidad para transmitir diferentes tipos de tráfico. Además, como ocurre con cualquier tecnología, su coste se ha reducido, ya que las innovaciones más recientes ofrecen mejoras a un precio inferior.

Por ejemplo, ATM permite crear VPN múltiples en un área extensa, pero la implementación de una red ATM resulta cara y requiere una actualización costosa de los equipos. Además, su alcance se limita a los emplazamientos situados dentro de la nube ATM. Por el contrario, la tecnología VPN IPSec permite establecer conexiones remotas seguras usando un estándar abierto y aprovechando una infraestructura compartida ya existente. A los proveedores, les resulta cada vez más difícil conservar su base instalada Frame Relay y ATM: cada vez más clientes se deciden por VPN basadas en IP, dada su mayor utilidad y su coste considerablemente inferior.

Es evidente que la transmisión de datos corporativos por Internet puede generar numerosos problemas de seguridad. No obstante, cualquier VPN con prestaciones sencillas ofrece un nivel básico de seguridad, ya que permite separar los flujos de datos y formar grupos lógicos de usuarios, restringiendo de esta forma el acceso de cada usuario al contenido de su propia VPN. Sin embargo, el aislamiento de los recursos de la red como la única medida de seguridad resulta restrictivo e inadecuado para la mayoría de las redes corporativas. Por ello, las VPN basadas en tecnología IPSec van más allá: utilizan tecnologías de cifrado y autenticación para crear un túnel privado seguro a través de una red IP que, de otra forma, no sería segura.

6.5.2 Integración de IPSec en una VPN MPLS

IPSec contribuye considerablemente a reducir los gastos, a la par que introduce un nivel de encriptación y seguridad superior, independientemente de si se utiliza sobre Internet, la red interna IP privada o una red MPLS.

Sobre un servicio MPLS, con VPN IPSec se puede obtener una mejor escalabilidad, seguridad, funcionalidad del QoS y otras ventajas.

Normalmente, MPLS se ofrece como servicio gestionado y la VPN comienza y termina en la misma red IP del proveedor de servicios. Por el contrario, una VPN IPSec se origina y con frecuencia en la empresa cliente quién se encarga de su gestión como es nuestro caso.

Además de ampliar el alcance de la red MPLS, al integrarse ambas tecnologías se lograr una infraestructura redundante. Para ello se utiliza la VPN IPSec como enlace redundante, en lugar de una red MPLS redundante, que resultaría mucho más cara. La integración de las dos tecnologías es una opción ideal, esto lo demuestra que el grupo de trabajo MPLS dispone ya de una especificación para el encapsulado MPLS-in-IP.

La ventaja es evidente: al tiempo que se utiliza IPSec para enviar paquetes MPLS de forma segura por una red no MPLS, pueden añadirse funciones de autentificación y cifrado para proteger los datos.

En la siguiente tabla se muestra las diferencias entre la VPN IP antigua y la nueva VPN IPSec.

Prestación	VPN IP (VPN MPLS)	VPN IPSec
Conectividad entre sedes	Sí	Sí
Conectividad de malla completa	Sí	Sí
Gestión de QoS y ancho de banda	Sí (CoS)	Sí (QoS granular)
Cifrado AES 256 bits	No	Sí
Autentificación basada en PKI	No	Sí
Disponible en todo el mundo	No	Sí
Interoperabilidad entre operadores de servicios	No	Sí
Requisito del contrato con el proveedor de servicios	Sí	No
Costes de implementación	€€€€	€€
Coste mensual de ancho de banda	€€	€

Tabla 6-2: Comparación entre VPN IP y VPN IPSec

6.5.3 Encriptación L2TP / IPSec

En realidad, MPLS no fue diseñado para ser un protocolo seguro. El objetivo de sus creadores era desarrollar una forma de etiquetar paquetes para conseguir una transferencia más eficaz y esta función la cumple con creces. Sin embargo, MPLS no encripta dichos paquetes, por lo que pueden resultar muy vulnerables a la intrusión, las intervenciones y otros tipos de ataques nefastos.

También es posible falsificar el espacio de dirección del cliente o la propia etiqueta MPLS. Esto no significa que MPLS sea una tecnología deficiente, sino simplemente que no se debe implementar MPLS sin una función de seguridad añadida, como puede ser un punto de seguridad en el emplazamiento del cliente (ej: cortafuegos con VPN IPSec).

Una vez explicado esto hemos de contar en que para realizar una VPN, tiene que estar basada en un protocolo como puede ser PPTP o L2TP, en nuestro caso hemos elegido L2TP por el hecho de ser más seguro al usar claves compartidas y por la capacidad de soportar IPSec.

¿Qué es L2TP?

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

¿Qué es IPSec?

IPSec se concibió desde el principio como un estándar para autentificar y cifrar datos en una red IP, así como para proteger la privacidad de los recursos de la red.

Los costes de propiedad son un factor decisivo a la hora de implementar IPSec, ya que este protocolo permite adquirir una conectividad de Internet a bajo precio, sin perder por ello las ventajas de una red de malla extensa y segura basada en las tecnologías más recientes.

Además, como la VPN IPSec no necesita conexiones, al añadir ej: la funcionalidad VPN SSL remota para teletrabajadores individuales, es capaz de establecer diferentes tipos de conectividad, lo que permite enlazar dos o más puntos situados prácticamente en cualquier lugar del mundo.

Mientras que las VPN basadas en IP (ej: redes MPLS) presentan amplios agujeros seguridad, IPSec fue concebido como un protocolo seguro. La VPN IPSec ofrece confidencialidad e integridad de datos, siendo la mejor solución de acceso remoto para emplazamientos múltiples. Como parte del protocolo Ipv6 IETF, IPSec incluye cifrado, autentificación y gestión de claves – los tres pilares de la seguridad VPN, eliminando así las vulnerabilidades que, de otra forma, se darían en TCP/IP.

IPSec se ha convertido en un estándar para la implementación de redes VPN, no sólo por su nivel de seguridad inherente, sino también porque no requiere ningún cambio en las estaciones de trabajo clientes.

La mayoría de las empresas y organizaciones, además del acceso a las oficinas centrales también desean ofrecer acceso a Internet en cada punto terminal de la red. Dado que la propia VPN IPSec funciona sobre Internet, es fácil implementarlo sin necesidad de ningún equipo adicional. Existen diferentes opciones para conectar las VPN MPLS a Internet que, normalmente, implican una conexión separada a Internet.

Por regla general, para operar una VPN IPSec han de instalarse equipos en el emplazamiento del cliente. No obstante, muchos proveedores ofrecen servicios VPN IPSec en los que ellos mismos se encargan de gestionar la pasarela IPSec. Normalmente, este tipo de servicio gestionado incluye cierta garantía de rendimiento.

6.6 Implantación Alternativa

Una vez planificada la implantación, elegida la alternativa a implantar, definidos los plazos y recopilados todos los datos necesarios voy a proceder a la implantación.
Esta se realiza una vez solicitadas las líneas MPLS y ADSL, y estas hayan sido entregadas por la operadora de servicios.

Para proceder a la implantación pasaré por cuatro pasos:

- Preparación de servidores VPN,
- Preparación de routers MPLS
- Implantación de una red VPN – MPLS internacional.
- Preparación de routers ADSL

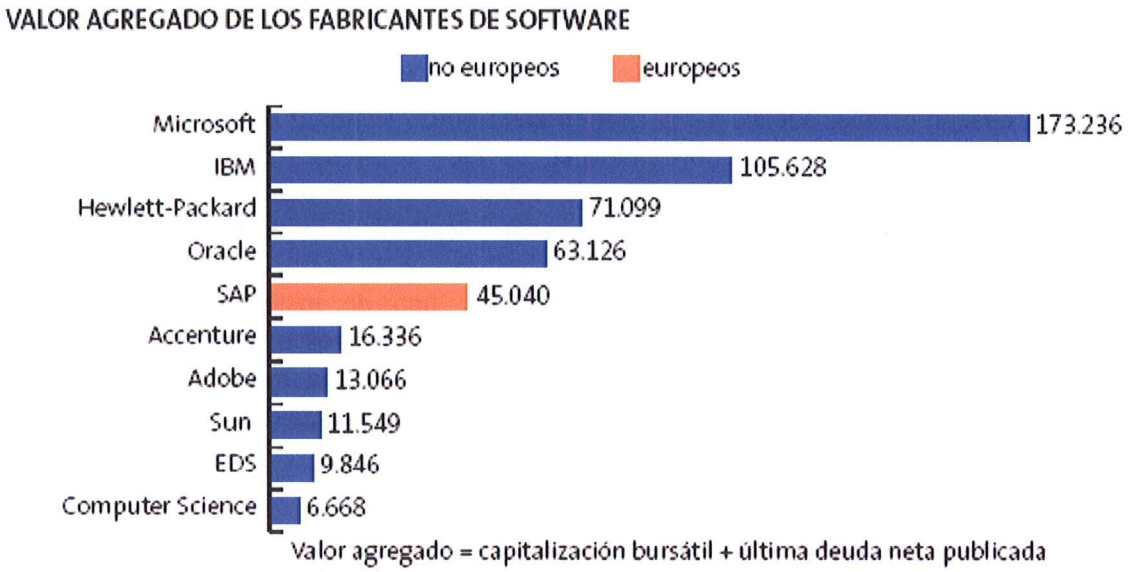
6.6.1 Servidores VPN

Un servidor para gestionar la VPN y controlar el tráfico no ha de ser necesariamente una máquina de última generación, grande y monstruosa. Puesto que las necesidades del servidor dependen del uso que se le va a dar.
Este servidor se encargará de gestionar las conexiones hacia los otros puntos de la red MPLS, a la vez que gestionará, encaminará y vigilará el tráfico.

El servidor realizará por ello las funciones de creación de la VPN con el proceso de entrega y recepción de información vía esta, y la función de firewall sobre las conexiones que se realizan por la VPN.

Esta gestión se realizará mediante una aplicación llamada Microsoft ISA Server 2004 instalada sobre un sistema operativo Windows Server 2003, Standard Edition.

Como punto de referencia para la elección de software para todos los países, se ha tomado aquel que tiene un soporte internacional.



Fuente Bloomberg. Datos de 30 de agosto de 2007.

Ilustración 6-14: Valor agregado por los fabricantes de software

Para la implantación de este proyecto necesitaremos preparar y configurar un servidor de la manera descrita en cada país que forma parte de este proyecto.

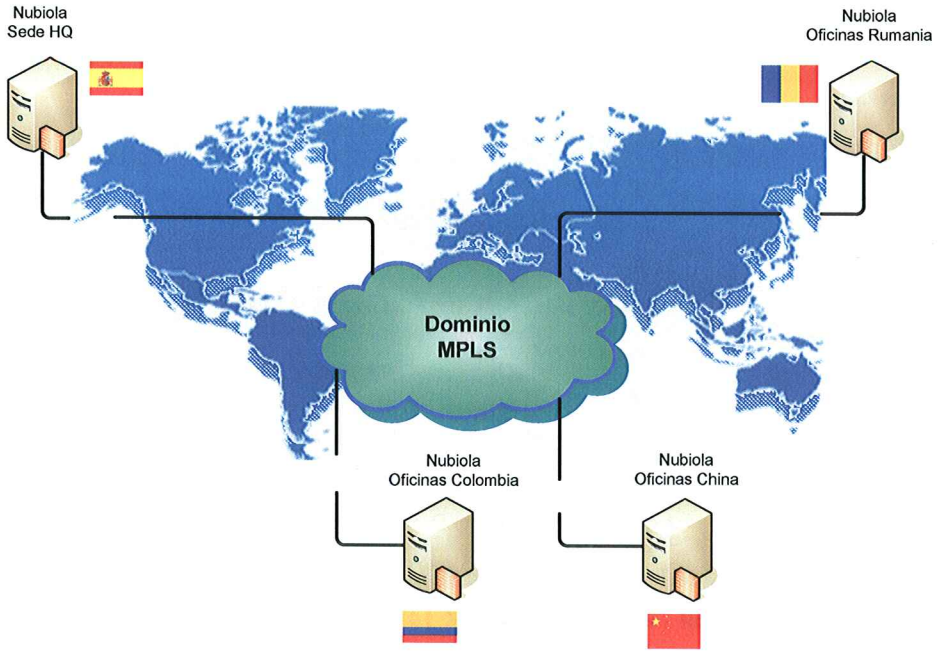


Ilustración 6-15: Implantación de Servidores VPN

Como cada país tiene unos servidores diferentes, muchas veces incapaces de cubrir nuestras necesidades se ha decidido comprar unos servidores enracables destinados a servidores VPN de cada país.

Para facilitar la gestión y estandarizar el sistema al máximo se comprarán todos iguales.

Dentro de las necesidades que tenemos he encontrado dos servidores económicos que pueden cubrirlas:

- DeLL PowerEdge SC1435
  - Precio: 1279€ + 16% iva

- HP ProLiant DL120 G5
  - Precio: 955,35€ + 16% iva

DeLL PowerEdge SC1435:

Especificación principal – DeLL PowerEdge SC1435	
Procesador	Dual Core AMD Opteron™ 2218; 2.6GHz, 2X1MB Cache, 95W, 1Ghz HyperTransport
Núcleo de Procesador	Dual-Core
Caché	2 MB de caché L2
Chipset	Chipset Intel® 3200
Bus del sistema	Bus frontal a 1333/1066/800 MHz
Memoria de serie	2 GB
Tipo de memoria	Intercalado de memória SDRAM DDR2 PC2-6400 (800 MHz)
Ranuras de memoria	4 ranuras DIMM
Memoria máxima	8 GB
Unidades óptica	Unidad de DVD-RW o DVD-ROM de 12,7 mm
Unidad Disco Duro	1 unidad SATA/SAS de 3,5" sin conexión caliente 15.000 rpm
Tarjetas Ethernet	2 Adaptadores de servidor D1304i Gigabit
Almacenamiento masivo interno	SATA: 80 GB (1 SATA de 80 GB)

Tabla 6-3: Especificación principal - Dell PowerEdge SC1435

HP ProLiant DL120 G5:

Especificación principal – HP ProLiant DL120 G5	
Procesador	Procesador Quad-Core Intel® Xeon® X3350 (2,66 GHz, 95 vatios, bus frontal a 1.333 MHz);
Núcleo de Procesador	Quad-Core
Caché	12 MB de caché L2 (procesador Intel® Xeon® X3350)
Chipset	Chipset Intel® 3200
Bus del sistema	Bus frontal a 1333/1066/800 MHz
Memoria de serie	2 GB
Tipo de memoria	Intercalado de memória SDRAM DDR2 PC2-6400 (800 MHz)
Ranuras de memoria	4 ranuras DIMM
Memoria máxima	8 GB
Unidades óptica	Unidad de DVD-RW o DVD-ROM de 12,7 mm
Unidad Disco Duro	60GB - 2 unidades SATA/SAS de 3,5" sin conexión caliente 15.000 rpm
Tarjetas Ethernet	2 Adaptadores de servidor NC105i Gigabit
Almacenamiento masivo interno	SATA: 1,5 TB (2 SATA de 750 GB)

Tabla 6-4: Especificación principal - HP Proliant DL120 G5