Departamento de Ingeniería Telemática

PROYECTO FIN DE CARRERA

Diseño de una solución de red privada virtual corporativa

Autor: Ignacio Del Olmo Martínez

Tutor: Dr. Manuel Urueña Pascual

Leganés, Mayo 2015

Quisiera agradecer en estas líneas a todas las personas que me han ayudado en la realización de este proyecto.
A mi familia, por darme la oportunidad de poder llegar hasta aquí y servirme de apoyo en todo momento.
A mi tutor, Manuel, por su predisposición e implicación desde el primer día que le propuse la realización de este proyecto y por su cooperación e inestimable ayuda durante su realización.
A mis compañeros y amigos, que han aportado su granito de arena para poder culminar lo que la finalización de este proyecto supone.
A todos ellos, gracias.

Índice de contenidos

Índice de figuras

Índice de tablas

Resumen

La evolución de las empresas viene marcada por el intento de globalización de sus servicios, siendo bastante habitual que no solo multinacionales sino también pequeñas y medianas empresas establezcan varias sedes distribuidas geográficamente por todo el territorio nacional para satisfacer la demanda de necesidades de sus clientes y expandir la oferta de sus productos.

Este modelo requiere una infraestructura de comunicaciones que le ofrezca a la empresa una serie de características específicas:

- Interconexión de las diferentes sedes de la empresa como si se tratara de una sede única.

- Intercambio de información entre sedes con diferentes medios de acceso.

- Manejabilidad, flexibilidad y escalabilidad de la solución implementada.

- Privacidad en las comunicaciones.

- Minimización de costes de implementación.

Orientado a lo anteriormente descrito, el objetivo de este Proyecto Fin de Carrera es el diseño de una solución de comunicaciones a medida para la empresa ficticia ACME S.A. que solicita a un operador de comunicaciones la creación de una red en las que todas las sedes que la componen se puedan interconectar entre sí de manera privada y que sea fácilmente escalable según las futuras necesidades que se requieran.

El resultado del proyecto ha sido el diseño de una red privada virtual (VPN - *Virtual Private Network,* en inglés*)* para interconectar todas las sedes de dicha empresa, que cumple los requisitos de prestaciones y disponibilidades solicitadas por la empresa y permite, una vez se encuentre operativa, poder incorporar o eliminar sedes de manera rápida y sencilla sin necesidad de realizar cambios en el resto de la red.

Así mismo se han evaluado unas herramientas de gestión para supervisar cada sede de la VPN obteniendo información sobre el rendimiento y uso de cada una de ellas y poder de esta manera optimizar los recursos que tienen asignados.

Abstract

The evolution of Companies aims to Service globalization, and it is pretty common that not only multinationals but also small and medium companies establish their sites across a nation in order to satisfy customer's requests and expand their portfolio offers.

This model needs an infrastructure of communications which offer set of specific characteristics:

- Interconnection of different sites as if they were just a single site.

- Information exchange across sites through different access technologies.

- Manageability, flexibility and scalability of the solution.

- Strong and private communications.

- Minimizing delivery costs

As previously stated, the goal for this Project is the design of a communication solution for an hypothetic ACME company who asked for a solution to a telecom operator in order to interconnect all their sites privately and with capacity to grow if needed.

The outcome of this project is a Virtual Private Network (VPN) design that connects all ACME sites, and fulfills all performance and availability requests of the company. It also allows, after the service deployment, any modification, adding, removing or upgrading sites in an easy way without impacting other sites within the network.

In addition, several management tools have been evaluated in order to monitor the different sites within the VPN, by obtaining information about the performance and resource usage for the purpose of optimizing the assigned resources.

Capítulo 1. Introducción

1.1 Motivación

La empresa ACME, S.A. [1] es una empresa aseguradora que oferta seguros en todos los ámbitos existentes, tanto en la vida privada como profesional de las personas, asegurando sus bienes patrimoniales, desde seguros de automóvil, hogar, vida y salud hasta inversiones o viajes.

Esta empresa tiene 32 sedes distribuidas, tal como muestra la Figura 1, en gran parte del territorio nacional; y su sede central se encuentra en Madrid. La empresa está estructurada en cuatro delegaciones (Centro, Norte, Sur y Este). Los empleados intercambian una gran cantidad de datos necesarios para la elaboración de las pólizas y cálculo de primas con sus servidores centrales alojados en Madrid, así como para la realización de balances dentro de sus delegaciones. Además realizan múltiples solicitudes de información vía web, tanto por sus empleados desde sus sedes, como para responder consultas de sus clientes.

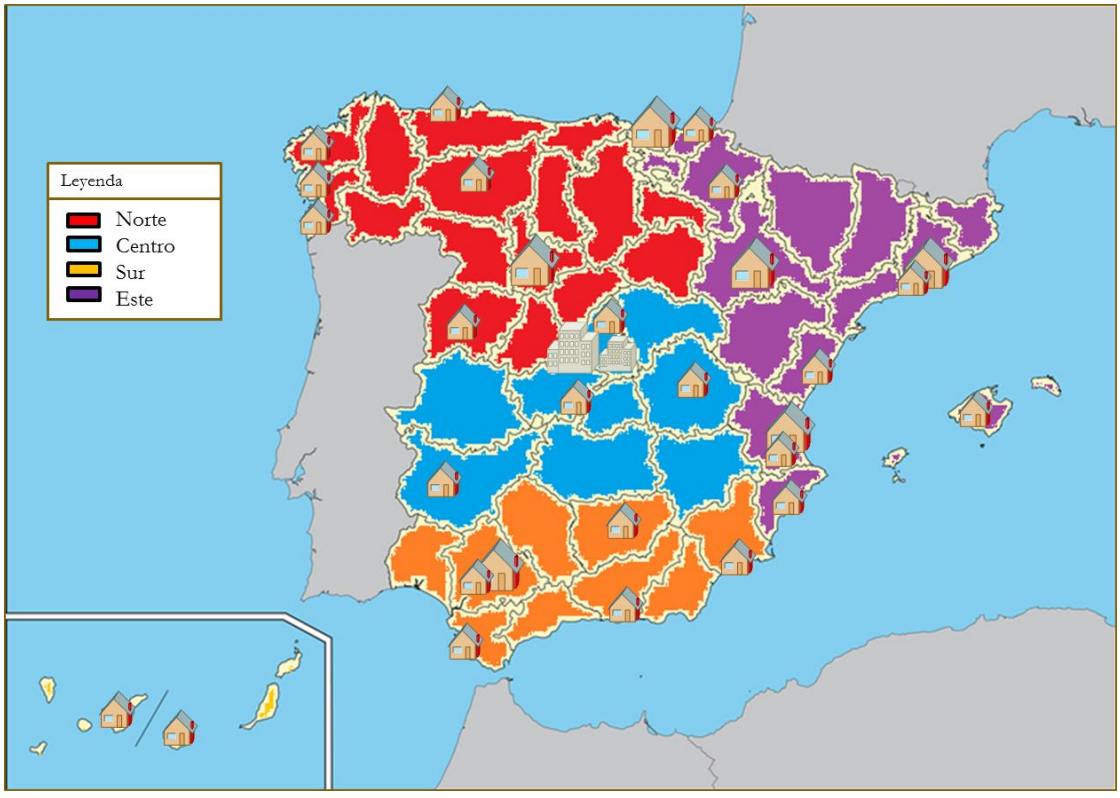

Figura 1. Distribución territorial de sedes de la empresa ACME S.A.

(1)Por motivos de confidencialidad el nombre de la empresa real y las ubicaciones de cada sede han sido sustituidos por nombres y localizaciones ficticias.

Esta empresa ha contactado con nuestro proveedor de servicios de telecomunicaciones para contratar una solución de comunicaciones de datos que permita a las sedes remotas ser operativas del mismo modo que la sede central, creando una red privada virtual que cumpla los siguientes requisitos:

1. La solución implementada debe ser flexible para poder añadir nuevas sedes sin necesidad de realizar modificaciones en las ya existentes, o eliminar éstas en caso que fuera necesario una vez estén operativas.

2. Todas las sedes deben poder intercambiar información de manera privada con el resto de ellas.

3. La disponibilidad de las sedes es un aspecto crítico para la empresa, ya que una incomunicación supone la pérdida de clientes potenciales. Es necesario que la solución contemple mecanismos de respaldo en las conexiones.

4. Los servidores centrales alojados en la sede central deben contar con redundancia en otra ubicación para que un problema en ellos no impida seguir funcionando al resto de sedes.

5. El coste de la solución no debe suponerle a la empresa un desembolso inicial muy elevado.

6. Los accesos definidos en cada sede deben proporcionar un caudal suficiente para dar servicio a la totalidad de los empleados ubicados en ella. Este caudal debe poder aumentar o disminuir en cada sede de manera independiente debido a la posible variación de trabajadores o el aumento de ancho de banda requerido por cada una de ellas. Se ha estimado que el ancho de banda necesario para cada usuario es de 200 Kbps.

Sede	Trabajadores	Direccionamiento	Sede	Trabajadores	Direccionamiento
Madrid I	50	192.168.0.0/24	Sevilla II	5	192.168.16.0/24
Madrid II	20	192.168.1.0/24	Cadiz I	3	192.168.17.0/24
Madrid III	10	192.168.2.0/24	Jaen I	5	192.168.18.0/24
Barcelona I	30	192.168.3.0/24	Motril I	3	192.168.19.0/24
Valencia I	30	192.168.4.0/24	Toledo I	15	192.168.20.0/24
Sevilla I	25	192.168.5.0/24	San Sebastian I	5	192.168.21.0/24
Bilbao I	25	192.168.6.0/24	Pamplona I	5	192.168.22.0/24
Zaragoza I	25	192.168.7.0/24	Cuenca I	5	192.168.23.0/24
Valladolid I	25	192.168.8.0/24	Barcelona II	15	192.168.24.0/24
La Coruña I	5	192.168.9.0/24	Castellón I	5	192.168.25.0/24
Santiago I	15	192.168.10.0/24	Valencia II	15	192.168.26.0/24
Vigo I	5	192.168.11.0/24	Alicante I	5	192.168.27.0/24
Gijón I	5	192.168.12.0/24	Murcia I	5	192.168.28.0/24
León I	15	192.168.13.0/24	Mallorca I	15	192.168.29.0/24
Salamanca I	5	192.168.14.0/24	Tenerife I	5	192.168.30.0/24
Badajoz I	5	192.168.15.0/24	Las Palmas I	15	192.168.31.0/24

Tabla 1. Sedes. Trabajadores y direccionamiento LAN

7. El acceso a Internet de todas las sedes se deberá realizar a través de un punto de acceso centralizado ubicado en la sede central de Madrid y dimensionarlo de manera óptima.

8. El dimensionamiento de cada sede facilitado por la empresa y el rango de red definido para cada una de ellas aparece reflejado en la Tabla 1. Todas las sedes se encuentran localizadas en el centro urbano de la ciudad a la que referencia.

9. La sede central de Madrid debe conectarse de manera privada con un servidor perteneciente a otra empresa, para la compensación de seguros con otras entidades, sin necesidad de desplegar infraestructura adicional y utilizando los mismos accesos que para la conexión de la red que se implemente. Se trata de una conexión para el intercambio de manera puntual de tráfico reducido.

10. La empresa requiere contar con una herramienta de monitorización de los elementos de la red para poder obtener una estimación del correcto uso de los recursos con lo que cuenta y ajustarlos en caso de ser necesario.

Esta empresa ya cuenta con un acuerdo con otro proveedor que se encarga del cableado y mantenimiento interior de las sedes, por lo que en este proyecto no se tendrá en cuenta la gestión de la parte LAN (switches) ni el equipamiento informático de las sedes.

1.2 Objetivo

El objetivo de este proyecto será por tanto el diseño de una red privada virtual que se ajuste a los requisitos previamente definidos por la empresa ACME S.A. utilizando las infraestructuras de las que disponga nuestro operador de telecomunicaciones.

1.3 Estructura de la memoria

Esta memoria está estructurada de la siguiente forma:

- En el capítulo 2 se repasarán las diferentes tecnologías y protocolos utilizados en el diseño de la red privada virtual.

- En el capítulo 3 se realizará el diseño de la red privada virtual, detallando los aspectos comunes del diseño, los diferentes accesos y equipamientos utilizados en cada una de los tipos de sede que la formen y la redundancia que se realiza en cada uno de ellos.

- En el capítulo 4 se estudiarán dos herramientas de monitorización de red para la elección de la más indicada dada las necesidades del cliente, se determinarán los parámetros a monitorizar para cada uno de elementos de la red y se hará una breve reseña a la herramienta con la que el proveedor de comunicaciones monitoriza los equipos que forman la red privada virtual.

- En el capítulo 5 se elaborará una planificación de la implantación de la red, un presupuesto del coste de los accesos, equipamientos y recursos utilizados en el despliegue y

una comparativa entre la opción de compra y de alquiler del equipamiento elegido para la red privada virtual.

- En el capítulo 6 se desarrollarán las conclusiones y los posibles trabajos futuros de los definidos en este proyecto.

- En el capítulo 7 se detallará la bibliografía con todas las referencias sobre tecnologías, protocolos y equipamientos utilizados para la realización de este proyecto.

Capítulo 2. Estado de la cuestión

En este apartado se proporciona una visión general de las tecnologías y principales protocolos que se han utilizado para desarrollar la solución de red privada virtual del cliente.

2.1 Tecnologías de acceso xDSL

Digital Suscriber Line (DSL) es el término utilizado para referirse de forma genérica a todas las tecnologías que proveen una conexión digital sobre la línea de abonado de la red telefónica tradicional, utilizando el par trenzado de hilos de cobre de las líneas telefónicas para la transmisión de datos a gran velocidad. En función de la velocidad (de subida/bajada) soportada y el rango de cobertura existen diferentes tipos de tecnologías xDSL.

2.1.1 Asymmetric Digital Subscriber Line (ADSL)

ADSL [G.992.1] es una tecnología de acceso a Internet de banda ancha mediante par de cobre, que utiliza una banda de frecuencias más altas de la utilizada por la voz convencional. Para ello, se emplea un *splitter* que se encarga de separar la señal de la telefonía, de la usada para conectarse a la red de datos. Permite utilizar ambos servicios, voz y datos, de manera simultánea. La conexión entre el abonado y la central del proveedor es un enlace punto a punto no compartido, y la distancia máxima entre ambos no debe superar los 5 kilómetros, si bien la capacidad de la línea se reduce cuando aumenta la distancia a la central.

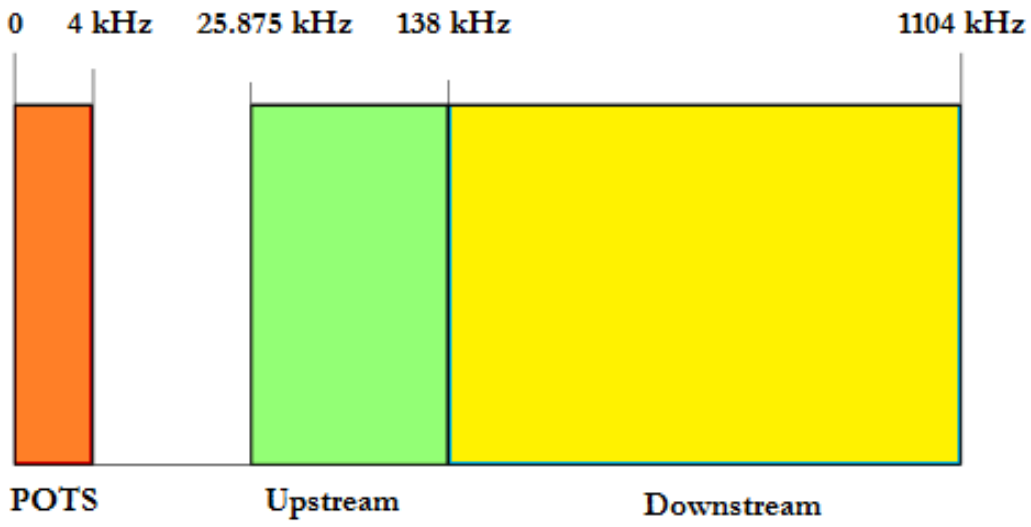

Figura 2. Banda de frecuencias empleados por ADSL

Es una tecnología asimétrica ya que ofrece mucho más caudal en el canal *downstream*, desde la red al usuario, que en el canal *upstream*, del usuario a la red. El ancho de banda del par de cobre se divide en tres secciones usando técnicas de multiplexación por división de frecuencia (FDM), una para el servicio telefónico, otro para el canal *upstream* y otra para el canal *downstream*, tal como muestra la Figura 2. Permite velocidades de hasta 8 Mbps en el canal descendente y hasta 1 Mbps en el ascendente.

Existen unos parámetros que determinan las capacidades máximas que puede ofrecer una línea ADSL.

- La **atenuación**. Es la diferencia entre la potencia de la señal transmitida y la potencia de la señal recibida en el otro extremo, expresada en decibelios. Crece con la distancia del nodo de acceso al usuario y con los valores altos de frecuencia.

- La **relación señal/ruido**. Es la diferencia en potencia entre el nivel de la señal y el nivel de ruido en el punto de la medición, expresado en decibelios. Mientras mayor sea su valor más calidad tendrá la línea.

La Figura 3 muestra el modelo de referencia de un sistema ADSL, definido por el ADSL-Forum [1], en el que se definen los elementos que forman el modelo y las interfaces de unión entre ellos:

- ***Access Node***. Nodo de acceso, punto de concentración para datos de banda ancha (*Broadband Network*) y banda estrecha (*Narrowband Network*). Generalmente está ubicada en una central del proveedor de comunicaciones.

- **ADSL *Transmission Unit Central*** (ATU-C). Es la unidad de transmisión del lado del operador. La ATU-C suele estar integrada en el *Access Node*.

- **ADSL *Transmission Unit Remote*** (ATU-R). Es la unidad de transmisión del lado del usuario. La ATU-C puede estar integrada en un SM (*Service Module*).

- ***Network Management***. Gestión de Red.

- ***Public Switched Telephone Network*** (PSTN). Es la Red Telefónica Pública Conmutada.

- ***Plain Old Telephone Service*** (POTS). Servicio telefónico.

- ***Splitters***. Filtros que separan las altas frecuencias en las que trabaja el ADSL de las bajas frecuencias que emplea el servicio POTS. Se coloca uno en la central y otro en el extremo del usuario.

- ***Loop***. El par de cobre que forma la línea telefónica o bucle de abonado.

- ***Premises Distribution Network***. Red de Distribución del Usuario.

- **B**. entrada auxiliar de datos.

- **T-SM**. Interfaz entre el ATU-R y la Red de Distribución del Usuario.

- **T**. Interfaz entre el Modulo de Servicios y la Red de Distribución del cliente.

- **T.E.** Equipos terminales.

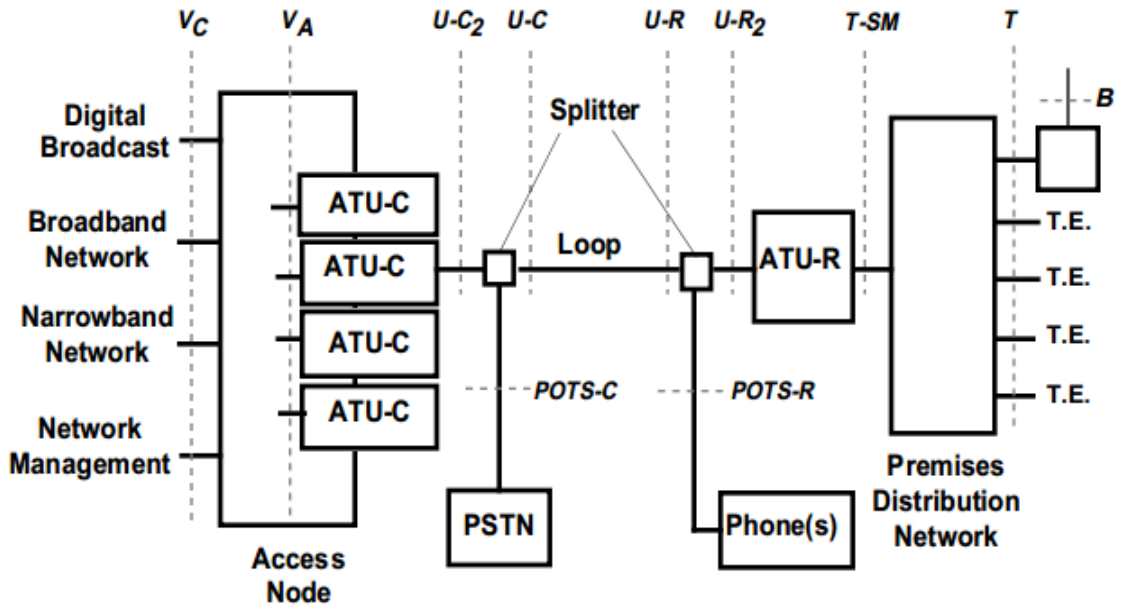

Figura 3. Modelo de referencia de un sistema ADSL [1]

- **Vc**. Interfaz entre el Nodo de Acceso y la red. Puede haber varias interfaces físicas, o puede haber una única que lleve todas las señales.

- **Va**. Interfaz lógica entre el ATU-C y el Nodo de Acceso.

- **U-C**. Interfaz analógica entre el bucle de abonado y la ATU-C.

- **U-C_2.** Interfaz entre el splitter y el ATU-C

- **U-R**. Interfaz analógica entre el bucle de abonado y la ATU-R.

- **U-R_2**. Interfaz entre el splitter y el ATU-R.

Según este modelo se necesita una pareja de terminales ATU-R/ ATU-C por cada línea de abonado. Desplegar una red completa como la del modelo por cada servicio independiente es inviable a la par de costoso, por lo que este problema se soluciona con el *Digital Subscriber Line Access Multiplexer* (DSLAM). Es un chasis situado en la central del proveedor de comunicaciones que agrupa un gran número de tarjetas, cada una de las cuales tiene varios ATU-C y concentra todo el tráfico de los enlaces ADSL hacia la red.

2.1.2 ADSL2+

Se trata de la evolución tecnológica posterior al ADSL que proporciona velocidades más altas de transmisión manteniendo el mismo alcance. Para conseguirlo en ADSL2+, definido en el estándar G.992.5 [2] de la ITU-T, se dobla el ancho de banda disponible en sentido *downstream* aumentando la frecuencia máxima de 1,1 MHz del ADSL a 2,2 MHz lo que permite velocidades de hasta 24 Mbps. Esta tecnología no es útil para distancias largas ya que las frecuencias más altas son más sensibles a la atenuación y al ruido.

2.1.3 VDSL/VDSL2

Very High Speed Digital Subscriber Line, estándar G.993.1[3] de la ITU-T, es la norma de comunicaciones xDSL más reciente, diseñada para soportar unas necesidades de ancho de banda muy altas ampliando el espacio de frecuencia desde los 2,2 MHz a las que llegaba el ADSL2+ hasta los 12 MHz. Puede operar tanto en modo asimétrico como simétrico.

Proporciona un servicio de transmisión de datos hasta un límite teórico de 52 Mbps en el canal descendente y 16 Mbps en el canal ascendente sobre una simple línea de par trenzado. Para conseguir estas velocidades de transmisión VDSL es necesaria una red de fibra hasta un nodo cercano al usuario (por ejemplo, una PON – *Passive Optical Network*). Desde el nodo óptico hasta el usuario se utiliza pares de cobre. En función de donde se encuentre el nodo óptico utilizaremos una tecnología concreta de FTTx (explicadas en el siguiente apartado). Cuanto menor sea la distancia del nodo al usuario, la velocidad de trasmisión será mayor. VDSL es aconsejable si la distancia es inferior a 1,5 kilómetros.

VDSL2, definido en el estándar G.993.2 [4] de la ITU-T, permite trasmisión de datos síncrona y asíncrona como velocidades superiores a 200 Mbps, si bien sufre una fuerte pérdida de la velocidad ofrecida con la distancia, que se reduce a unos 50 Mbps a un kilómetro de distancia al nodo. En VDSL2 las frecuencias pueden ser usadas tanto para el canal *downstream* como para el *upstream*.

2.2 Redes de acceso ópticas

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos de altas prestaciones que permite enviar gran cantidad de datos a grandes distancias, muy superiores a las permitidas por un par de cobre convencional. Una fibra es un conductor óptico de forma cilíndrica constituida por un núcleo, un recubrimiento con propiedades ópticas distintas a las del núcleo y una cubierta exterior que absorbe los rayos ópticos y protege al conductor, haciéndole inmune a las interferencias electromagnéticas. Puede ser monomodo, cuando la luz circula en un solo haz, o multimodo, cuando la luz circula en varios haces.

Debido a la reducción de costes y al desarrollo de nuevas aplicaciones (por ejemplo IPTV) que requieren un ancho de banda elevado, la fibra óptica ha comenzado a ser de interés en

el bucle de abonado y en accesos de corta distancia, y ya está siendo ofertado por los operadores de comunicaciones.

2.2.1 Arquitecturas de red óptica

FTTx (*Fiber to the x*) es la terminología utilizada para definir a los accesos de banda ancha por fibra óptica. En función del punto de terminación de la fibra, la última letra indica las diferentes tipologías que se pueden dar.

Fiber to the Curb (**FTTC**). La fibra llega hasta un punto más cercano al usuario que dispone el operador de comunicaciones y continúa con par de cobre o cable coaxial hasta el abonado.

Fiber to the Building (**FTTB**). La fibra llega hasta un edificio en el que conviven varios usuarios finales, y continúa internamente con otros medios no ópticos, par trenzado, cable coaxial o conexión inalámbrica.

Fiber to the Home (**FTTH**). La fibra llega hasta el usuario final y el trazado entre el usuario y la central del operador es enteramente de fibra.

Mientras menor sea la distancia desde la terminación de fibra hasta el usuario las velocidades de acceso serán mayores.

Se pueden diferenciar dos tipos de arquitectura para los accesos de fibra óptica, la arquitectura activa y la arquitectura pasiva. La diferencia radica en que en la pasiva el ancho de banda disponible de una fibra se multiplexa dividiéndolo en partes iguales o preestablecidas entre todos los usuarios, mientras que en la activa, el ancho de banda es dedicado por fibra y usuario. Sin embargo los accesos que utilizan arquitectura activa tienen un coste mucho más elevado que los accesos con una arquitectura pasiva puesto que es necesario alimentar y mantener los dispositivos activos que la forman.

Passive Optical Network **(PON)**

Las redes PON son aquellas en las que todos los componentes de la red óptica que se encuentran entre ambos extremos de la red son totalmente pasivos. Está definido en los estándares G.983 [5] y G.984 [6] de la ITU-T.

La estructura PON se compone de los siguientes elementos, representados en la Figura 4:

-***Optical Line Terminal*** (OLT). Situado en el extremo del proveedor de comunicaciones, es el encargado de realizar la conversión de señales eléctricas a señales ópticas en sentido descendente y a la inversa en ascendente.

-***Splitter***. Es el elemento óptico pasivo que divide la señal óptica que entra por un extremo en varias señales de salida en la comunicación descendente y las acopla en el ascendente. No requiere de alimentación

-***Optical Network Unit*** (ONU). Situado en el extremo del usuario, es el encargado de realizar la conversión de señales ópticas a eléctricas en sentido descendente y a la inversa en el ascendente.

El funcionamiento de una red PON requiere diferenciar entre el canal de bajada o *downstream* (del OLT a los ONUs) y el canal de subida o *upstream* (de un ONU hasta el OLT). Como el medio de transmisión es compartido (se emplea una solo fibra para el canal ascendente y descendente de todos los abonados), se realiza multiplexación por longitud de onda diferente utilizando técnicas *Wavelength Division Multiplexing* (WDM), por lo que se requiere el uso de filtros ópticos para separarlos. Como normalmente el tráfico es asimétrico, en el canal *downstream* suele ser mayor que en el canal *upstream*.

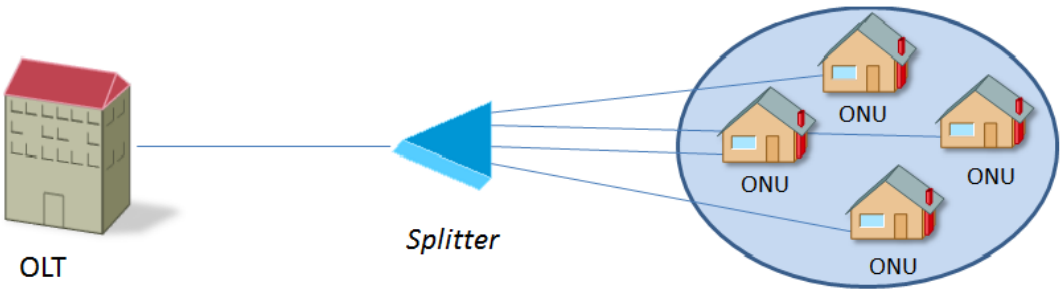

Figura 4. Estructura de una red PON

En sentido descendente la red PON es una red punto-multipunto, en el que el OLT envía los datos a todas las ONUs, ya que el *splitter* replica la señal óptica a todos las ONUs, y éstos se encargan de filtrar los contenidos y enviar al usuario solamente los dirigidos a él.

En sentido ascendente la red PON es una red multi punto-a-punto, en el que las ONUs envían datos al OLT utilizando *Time Division Multiple Access* (TDMA). El OLT asigna *Time Slots* a cada ONU permitiendo a varios usuarios utilizar la misma frecuencia de subida y compartir el medio sin colisiones.

Active Optical Network **(AON)**

Las redes ópticas activas permiten un ancho de banda simétrico de altas prestaciones utilizando una fibra óptica en cada sentido o una única fibra óptica con dos longitudes de onda multiplexadas, de manera que se crea un canal para la transmisión y otro canal para la recepción. En ambos casos se consigue una transmisión *full-duplex* en un enlace punto a punto con todo el ancho de banda dedicado para el usuario.

Este tipo de redes permite mayor distancia que las redes PON y se suele utilizan para conectar dos sedes de una empresa o el proveedor con el usuario final de manera exclusiva

aumentando su fiabilidad. Al tratarse de un enlace dedicado para cada cliente, el coste de este tipo de redes es mucho más elevado que el de las redes de acceso PON.

2.3 Redes ópticas de transporte

2.3.1 Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH)

SDH [G.783] es un estándar definido por el ITU para la transmisión de gran cantidad datos síncronos a altas velocidades. Emplean transmisión óptica pero conmutación electrónica.

La unidad mínima de transmisión en SDH es una trama STM-1 de 155,52 Mbps, representada en la Figura 5. Tiene una estructura rectangular de 9 filas y 270 columnas. Los bytes son transmitidos y recibidos en secuencia, de izquierda a derecha y de arriba a abajo. Cada trama se transmite en 125 µs con lo que se tiene una frecuencia de 8000 tramas/segundo, lo que permite la transmisión eficiente de canales de voz de 4 KHz digitalizada. Agrupando canales se obtienen velocidades superiores multiplexando byte a byte varias señales STM-1 (e.g. STM-4, STM-16, STM64).

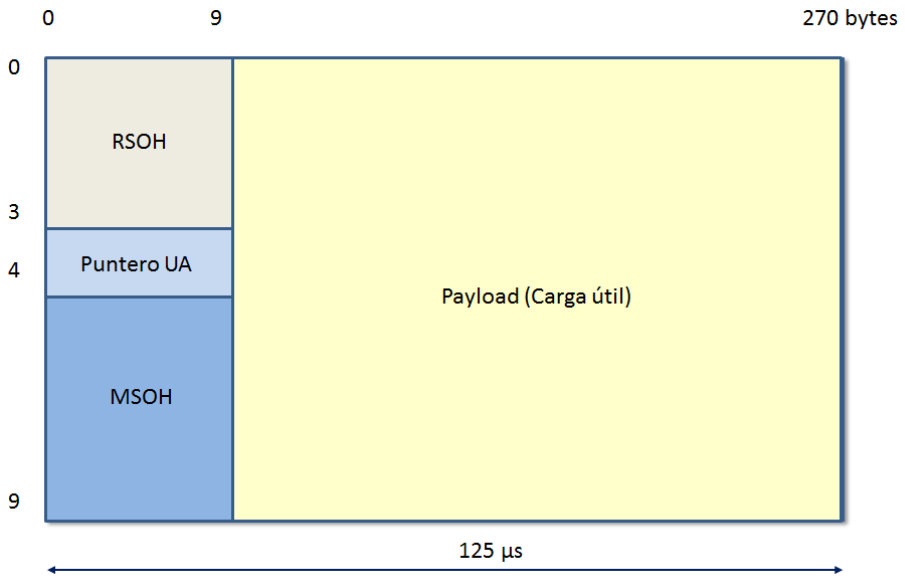

Figura 5. Estructura de una trama STM-1

Las redes SDH están formadas por 4 tipos de elementos:

- **Regeneradores**. Se encargan de regenerar el reloj y la amplitud de las señales de datos entrantes que hayan sido atenuadas y distorsionadas por la dispersión de la fibra óptica.

- ***Terminal Multiplexers*** (TM). Son los sistemas finales de la red que se emplean para combinar señales de entrada plesiócronas (PDH) y síncronas en STM-n de mayor velocidad.

- ***Add-Drop Multiplexers*** (ADM). Permiten insertar (o extraer) señales de menor velocidad en el flujo de datos SDH. Son capaces de localizar la información de un determinado canal sin necesidad de descomponer toda la trama multiplexada gracias al uso de los punteros que indican dónde comienzan los datos del usuario.

- ***Digital Cross-Connect*** (DXC). Es el encargado de la conmutación, inserción y extracción de señales SDH.

Una trama STM está dividida en dos grandes bloques; la carga útil (*payload*) y el *OverHead* (OH*)*, que aportan las funciones que precisa la red para ser operada eficazmente.

El *OverHead* se utiliza para dirigir y controlar cómo se transfiere la información del usuario dentro de la red SDH, así como para detectar y corregir los errores que pueda haber en los datos que se están enviando. Se divide en dos partes, el *Regenerator section overhead* (ROH) y el *Multiplexer section overhead* (MOH). El ROH contiene la información necesaria alineación e identificación de las tramas STM-1 que utilizaran los elementos regeneradores. El MOH provee las funciones necesarias para la multiplexación de las señales.

Toda la información útil se coloca en contenedores antes de ser trasmitida. A cada contenedor se le agrega el *Path overhead* (POH) a lo que se denomina *Virtual Container* (VC). El POH está destinado a manejar toda la información referente al camino por el cual circulará la información. Se agrega al formar el VC al comienzo de la ruta y se evalúa solamente al final de ésta.

Una de las principales características del SDH es su mecanismo de punteros, diseñado para ajustar las diferencias de temporización que se dan a lo largo de la red. El puntero contiene un número entre 0 y 783 que indica el desplazamiento en saltos de 3 bytes entre el puntero y el primer byte del VC. Debido al desajuste en las velocidades, el puntero se incrementa o decrementa según sea necesario, permitiendo a la carga "flotar" dentro de las tramas STM manteniendo el sincronismo. Cuando el puntero se añade al VC se forma la unidad administrativa (UA).

No es necesario que cada trama STM contenga un único VC, ya que con el puntero la información transportada no tiene que ajustarse a la carga útil de cada trama. Un VC puede transportarse dentro de otro VC de mayor tamaño o transportarse en dos STM consecutivas.

SONET [T1.105] es un estándar para la transmisión de señales ópticas definido por el ANSI y utilizado exclusivamente en Norteamérica y parte de Asia, que a pesar de definirse antes puede considerarse como un subconjunto de SDH.

SONET define los Synchronous Transport Signals (STS). El nivel base para SONET es STS-1. Está formada por un conjunto de 810 bytes distribuidos en 9 filas de 90 bytes. Esta trama se transmite, al igual que la unidad básica de SDH, cada 125 μs (8 bits/muestra), correspondientes a la velocidad del canal telefónico básico de 64 kbit/s, por lo que la velocidad binaria de la señal STS-1 es 51,84 Mbps. Así, STM-1 de SDH es equivalente a

STS-3 de SONET, como se puede ver en la Tabla 2 de equivalencias entre ambos estándares.

Nivel SONET	Nivel SDH	Tasa de línea (Mbit/s)
STS-1	-	51,84
STS-3	STM-1	155,52
STS-12	STM-4	622,08
STS-48	STM-16	2488,32
STS-192	STM-64	9953,28

Tabla 2. Equivalencias SDH/SONET

2.3.2 Wavelength Division Multiplexing (WDM)

Wavelength Division Multiplexing (WDM) es una tecnología que permite transmitir varias señales sobre una sola fibra óptica utilizando diferentes longitudes de onda para aprovechar mejor el ancho de banda total de la fibra.

Una red WDM requiere un terminal en cada extremo de la conexión (emisor/receptor). A la entrada, un transpondedor (*transponder*) acepta señales provenientes de distintos medios físicos y con diferentes tipos de tráfico asignándole una longitud de onda a cada una. Posteriormente las longitudes de onda se multiplexan, combinándolas en una sola señal óptica mediante un multiplexor antes de ser enviadas por la fibra. En el enlace de fibra se pueden añadir amplificadores ópticos para darle ganancia a la señal. A la salida un demultiplexor debe separar las diferentes longitudes de onda que serán procesadas según el tipo de salida recibido.

Dentro de la tecnología WDM se diferencian dos grandes tipos:

Coarse WDM (CWDM). La multiplexación por longitudes de onda "gruesas" [G.694.2] se basa en la separación de longitudes de onda de 20 nm en el rango de 1.270 a 1.610 nm; pudiendo así transportar hasta un máximo de 18 longitudes de onda en una única fibra óptica monomodo. Puede alcanzar distancias de hasta 50 km y permite topologías en anillo, punto a punto o PON. Se usa principalmente en redes metropolitanas.

Dense WDM (DWDM). La multiplexación por longitudes de onda densas [G.694.1.29] reduce la separación entre longitudes de onda en el rango cercano a 1550 nm (banda C). Actualmente se permiten entre 64 y 160 canales en paralelo espaciados entre 0.2 y 0.4 nm. Puede utilizarse para redes metropolitanas sin amplificadores hasta 80 km o para redes de largo alcance. Se puede implementar de manera unidireccional y bidireccional, si bien esta última es la más frecuente ya que el unidireccional necesitaría una segunda fibra adicional para permitir tráfico *full-duplex*.

Los proveedores de comunicación utilizan la tecnología WDM para ofertar una conexión de altas prestaciones con posibilidad de redundancia utilizando doble fibra y/o doble camino formando un anillo de conexión simple o doble.

2.4 *Multi-Protocol Label Switching* (MPLS)

MPLS es un estándar del IETF definido en la RFC3031 [7]. Surge como una tecnología de transporte de datos que combina la escalabilidad y flexibilidad de las tecnologías de capa de red (encaminamiento en el nivel 3 del modelo OSI) con el rendimiento y fiabilidad de las de la capa del nivel de enlace (conmutación en el nivel 2 del modelo OSI). Se puede definir por tanto como un protocolo ubicado entre ambas capas, diseñado para la integración del servicio de transporte de datos, tanto para las redes basadas en circuitos como para las basadas en conmutación de paquetes.

Las principales características de MPLS son:

- **Conmutación por etiquetas**. El reenvío de paquetes se realiza basándose exclusivamente en las etiquetas con las que están marcados. Con la conmutación de etiquetas el análisis de la cabecera de nivel 3 se realiza una sola vez, al ingresar en la red MPLS. De esta manera se toman decisiones de envío basadas en una sencilla etiqueta, en lugar de realizar una búsqueda en función de la IP destino en cada salto o la calidad de servicio (QoS)

- **Multiprotocolo**. Es aplicable a cualquier protocolo de red e independiente del nivel de enlace utilizado.

- **Ingeniería de tráfico**. Los flujos de tráfico se pueden repartir entre los distintos recursos físicos de la red para evitar congestionar el camino más corto que utilizaría IP.

2.4.1 Arquitectura de la red MPLS

Una red MPLS está formada por los elementos representados en la Figura 6:

- ***Forwarding Equivalent Class*** (**FEC**). Es el conjunto de paquetes que son tratados de la misma manera en el proceso de reenvío, y que utilizarán la misma ruta independientemente de su destino final.

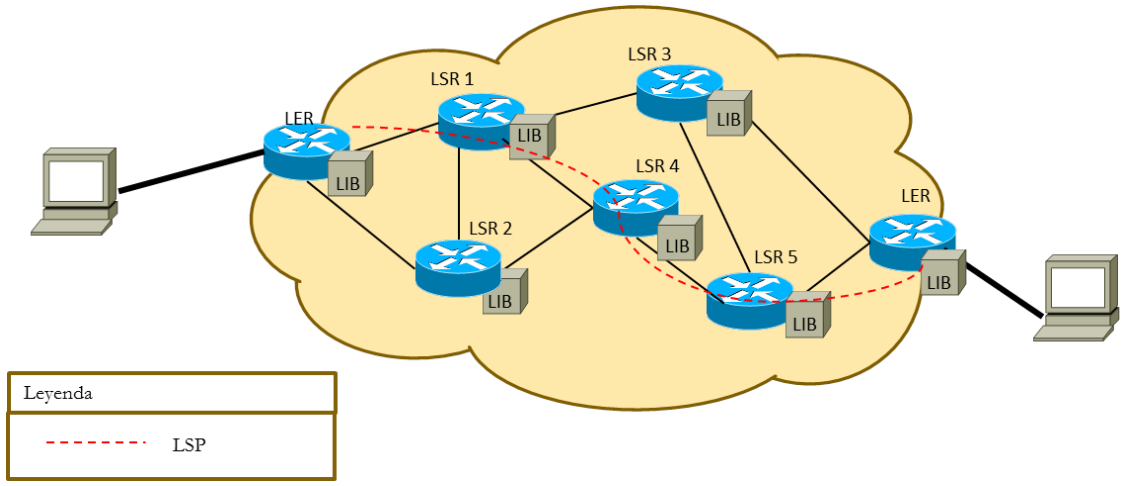

Figura 6. Arquitectura MPLS

- ***Label Switching Router*** (**LSR**).Es un *router* que se encarga de conmutar las etiquetas de los paquetes, e intercambiar información con otros LSRs que forman la red para establecer las asociaciones de flujo y etiquetas.

- ***Label Edge Router*** (**LER**). Es un *router* frontera que constituye la entrada y salida de la red MPLS. A la entrada de la red el LER se encarga de procesar los paquetes, agrupándolos y aplicándoles la etiqueta que corresponda en función de su FEC, mientras que a la salida es el encargado de suprimir las etiquetas y reenviar los paquetes hacia el destino mediante el reenvío de capa 3.

- ***Label Switched Path*** (**LSP**). Es el camino que se establece dentro de la red MPLS para todo el tráfico agrupado en la misma FEC. Todos aquellos paquetes identificados con una clase FEC seguirán el mismo encaminamiento a través de la red MPLS. Este camino se trata de manera unidireccional, por lo que será necesario definir un LSP para cada sentido de una comunicación y se establece antes de que la transmisión de datos comience.

- ***Label Forwarding Information Base*** (**LIB** o **LFIB**). Es la tabla de etiquetas que hay en cada LSR, que permite determinar en función de la etiqueta de entrada, la etiqueta de salida y el punto por el que se debe reenviar el paquete.

2.4.2 La etiqueta MPLS

Es un identificador que se encuentra dentro de la cabecera de las tramas MPLS y que permite clasificarlas con respecto al LSP al que pertenece. Un LSP puede tener varios FECs asociados aunque los LSRs de dentro de la red MPLS no los conocen, sino que se basan únicamente en las etiquetas MPLS. La cabecera MPLS tiene un tamaño de 32 bits tal como muestra la Figura 7.

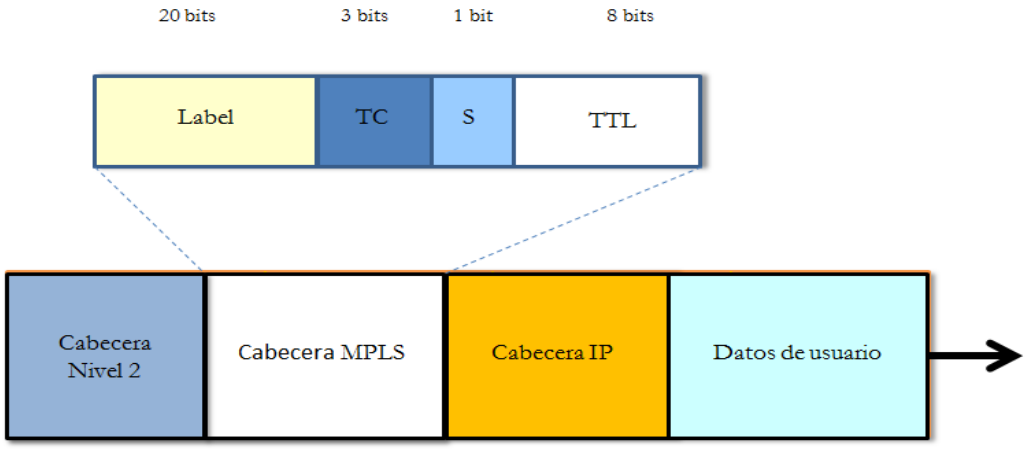

Figura 7. Etiqueta MPLS

La cabecera MPLS se inserta entre la cabecera de capa 2 y la de capa 3 y se compone de los siguientes cuatro campos:

- ***Label***. Identificador de la etiqueta de 20 bits de tamaño.

- ***Traffic Class*** (**TC**). Campo de 3 bits que, aunque inicialmente estaban reservados para uso futuro (EXP), actualmente se emplean para indicar la calidad de servicio (*Quality of Service* – QoS).

- ***Label Stacking*** (**S**). Este bit se utiliza para el apilado de etiquetas. Cuando tiene valor 0 indica que hay más etiquetas a continuación, mientras que el valor 1 indica que ya no hay más etiquetas y estamos al final de la pila.

- ***Time-to-live*** (**TTL**). Campo de 8 bits que realiza la función de limitar el número de saltos. Reemplaza al TTL de la cabecera IP durante el viaje del paquete por la red MPLS. Se va decrementando en cada LSR y si llega a 0 se descarta para evitar bucles.

Generalmente las etiquetas tienen significado local (por interfaz) y es el LSR el encargado de elegir de manera independiente el siguiente salto para cada LSP. Es posible también que el LER de entrada especifique la lista de nodos por los que pasaran los paquetes asociados a cada FEC, creando rutas explicitas, lo que permite implementar la ingeniería de tráfico.

La arquitectura MPLS permite dos mecanismos para asociar etiquetas a una FEC:

- ***Unsolicited-downstream***: cuando un LSR establece una asociación FEC-etiqueta y la distribuye a otros LSRs aunque todavía no lo hayan solicitado.

- ***Downstream-on-demand***: en el que un LSR debe realizar una petición al siguiente nodo de la asociación FEC-etiqueta.

En cuanto al control de distribución de las etiquetas, ésta se puede hacer de manera independiente u ordenada:

- En el **control independiente**, cada LSR decide la asociación FEC-etiqueta, que comunica a los LSRs ascendentes y la anota en su tabla LIB como entrada.

- En el **control ordenado**, cada LSR espera a recibir la etiqueta del nodo descendente (a excepción del LSR de salida) y lo anota en su LIB como salida. A su vez asigna una etiqueta local a la FEC, que anota en su tabla como entrada y se la comunica a los LSRs descendentes.

Por último, existen dos métodos de retención de etiquetas en la arquitectura MPLS, el liberal y el conservador:

- En la retención **liberal**, el LSR conserva todas las etiquetas que recibe, incluso algunas no validas o que proceden de LSRs que no son su siguiente salto para una FEC determinada. Este método permite una adaptación más rápida a los cambios de encaminamiento pero requiere una mayor capacidad de almacenamiento.

- En la retención **conservativa**, el LSR sólo mantiene las asociaciones de etiquetas válidas para el siguiente salto y elimina el resto. El rendimiento es mayor y se reduce la capacidad

de almacenado de las etiquetas, aunque la adaptación frente a cambios de encaminamiento es más lenta.

La arquitectura MPLS normalmente utiliza *downstream-on-demand*, control ordenado y retención conservativa.

2.4.3 Protocolos de distribución de etiquetas

Los LSRs emplean protocolos de distribución de etiquetas para informar al resto de los LSRs de que ha establecido una asociación FEC-etiqueta.

MPLS no establece un protocolo específico para la distribución de etiquetas. Es posible utilizar otros protocolos existentes como BGP o RSVP, aunque el IETF definió un nuevo protocolo, LDP, para ello.

Label Distribution Protocol **(LDP)** se emplea para mapear las FECs a etiquetas, a partir de las cuales se establecen los LSPs. Está definido por el IETF en la RFC 3036 [8].

Las sesiones LDP se establecen siempre entre parejas de LSRs, conocidas como *LDP peers*, no necesariamente adyacentes. Para el establecimiento de sesiones utiliza TCP, e incluye mecanismos para el descubrimiento de LDP *peers* potenciales mediante mensajes UDP.

Se definen cuatro tipos de mensajes LDP:

- Mensajes de descubrimiento (*Discovery messages).* Anuncian y mantienen la presencia de los LSRs en la red.

- Mensajes de sesión (*Session messages).* Se encargan de establecer, mantener y liberar las sesiones entre LSRs

- Mensajes de anuncio *(Advertisement messages*). Se encargan de anunciar la correspondencia de etiquetas a los FECs, para su creación, cambio o borrado.

- Mensajes de notificación (*Notification messages*). Se encargan de señalizar errores.

El establecimiento de una conexión LDP se realiza en los siguientes pasos representados en la Figura 8:

1. Las sesiones LDP se inician cuando un LSR envía mensajes *Hello* periódicos sobre las interfaces permitidas para el reenvío MPLS. Si otro LSR está conectado a esa interfaz, el LSR directamente conectado intenta establecer una sesión con la fuente de los mensajes H*ello.* El LSR con el ID más alto es el LSR activo e intenta abrir una conexión TCP con el LSR pasivo utilizando el puerto 646.

2. El LSR activo envía un mensaje de *Initialization* al LSR pasivo, que contiene la información del método de distribución de etiquetas, tiempo de sesión, longitud máxima de la *Protocol Data Unit* (PDU)...

3. El LSR pasivo responde con otro mensaje de *Initialization* si los parámetros son aceptables, o con un mensaje de notificación de error si no lo fueran.

4. Si acepta los parámetros de conexión, el LSR pasivo empieza a enviar mensajes de *Keepalive* al LSR activo después de enviar el mensaje de inicialización.

5. El LSR activo envía otro *Keepalive* al LSR pasivo y finalmente se establece la sesión LDP. A partir de este momento se pueden comenzar a enviar el mapeo de FEC-etiquetas entre los LSR que establecieron la conexión LDP.

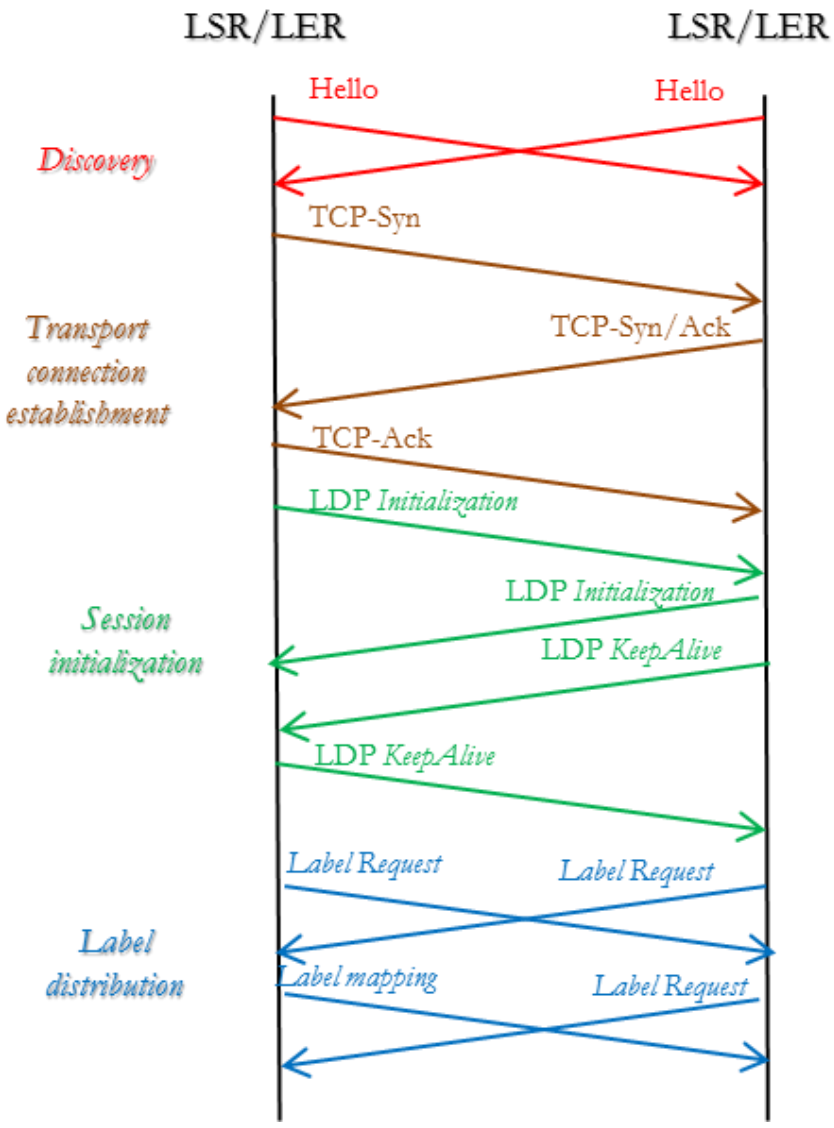

Figura 8. Establecimiento de una sesión LDP

2.4.4 Operación de MPLS

Las principales operaciones para el transporte de paquetes de datos a través de la red MPLS son:

• Descubrimiento de la topología de red.

• Creación y distribución de etiquetas.

• Creación de los LSPs a partir del intercambio de etiquetas.

• Reenvío de paquetes.

• Eliminación de etiquetas a la salida de la red.

Descubrimiento de la topología de red

El descubrimiento de la topología de red se realizada utilizando la propia información que manejan los protocolos de encaminamiento IP. A partir de la información proporcionada se construyen las tablas de encaminamiento en los LSRs.

Creación y distribución de etiquetas

Los LSRs establecen las asociaciones FEC-etiqueta y construyen sus LIBs antes de que comience el envío de tráfico. Para ello intercambian información de las asociaciones e información de características de tráfico o capacidades MPLS mediante LDP u otro protocolo de distribución de etiquetas.

Interfaz entrada	Etiqueta entrada	Interfaz salida	Etiqueta salida	Siguiente salto
Int.1	20	Int.2	2	LSR2
Int.2	8	Int.6	25	LSR3
Int.3	101	Int.7	47	LSR4

Tabla 3. Tabla LIB del LSR 1 de la Figura 6

La tabla LIB establece el mapeo de la asociación FEC-etiqueta y, en función de la interfaz y etiqueta de entrada, permite conocer la interfaz y etiqueta de salida y el siguiente LSR al que se encamina. Las entradas de la tabla LIB se actualizan cada vez que se establezca una nueva asociación FEC-etiqueta. La Tabla 3 muestra un ejemplo de tabla LIB perteneciente a un LSR.

Creación de los LSPs

Los LSPs se crean en dirección inversa a la creación de entradas en las tablas LIB, es decir, se crea del nodo destino hacia el origen.

Cuando el nodo origen recibe un paquete del cual no tiene etiqueta en su tabla LIB, solicita mediante un *Request* la ruta que necesita. Esta solicitud se va propagando hasta llegar al

LER de salida. Una vez recibido el paquete, el LER envía un *Mapping* en dirección ascendente. Cuando este envío va pasando por todos los nodos intermedios hasta el nodo origen, se completa la tabla LIB relacionada con el LSP que está siendo creado.

El LER de entrada a la red MPLS utiliza la información de las tablas para encontrar cuál es el próximo salto y con ello la etiqueta asociada a un determinado FEC.

Reenvío de paquetes

Cuando un paquete entra en la red, el LER de entrada comprueba si dispone de una etiqueta para él. Si no dispone de ella, tendría que crear un LSP para el FEC al que corresponde ese paquete siguiendo el procedimiento anterior.

Si el LER de entrada dispone de una etiqueta, la inserta en el paquete y la reenvía al LSR del primer salto. A partir de ese punto cada LSR examina la etiqueta del paquete recibido, la sustituye por la etiqueta de salida y la reenvía hacia el LSR del siguiente salto por el interfaz de salida especificado en la LIB.

Eliminación de etiquetas a la salida

Una vez que el paquete llega al LER de salida, éste elimina la etiqueta, puesto que una vez fuera de la red MPLS ésta no aporta información, y lo entrega al destino utilizando el encaminamiento IP convencional.

2.4.5 Aplicaciones de MPLS

Las principales aplicaciones que permite MPLS son:

- Ingeniería de tráfico.
- Protección y recuperación ante errores de red.
- Diferenciación de niveles de servicio (QoS).
- Servicio de redes privadas virtuales (VPN).

2.4.5.1 Ingeniería de tráfico

La Ingeniería de tráfico busca adaptar los flujos de tráfico a los recursos de la red, de tal forma que exista un equilibrio entre dichos recursos. Así conseguiremos que no haya recursos sobrecargados mientras existan otros poco utilizados, mejorando así el uso global de la red.

Por ejemplo en las redes IP tradicionales todos los paquetes suelen seguir el camino más corto, provocando que algunos enlaces puedan verse saturados mientras que otros no estén casi utilizados.

La ingeniería de tráfico se consigue desviando parte de los flujos de los enlaces más cargados a los que se encuentren menos congestionados, aunque estos no pertenezcan al camino más corto, a base de modificar las métricas de los enlaces, o bien repartiendo la carga entre varios enlaces. Este encaminamiento también puede estar basado en restricciones, de manera que la red pueda seleccionar determinadas rutas según el nivel de calidad requerido (ancho de banda, retardo, carga, fiabilidad, etc).

En el caso de las redes MPLS, la ingeniería de tráfico es sencilla de realizar ya que la red permite crear rutas explícitas definiendo el camino exacto por el que pasa un LSP.

Hay dos maneras de operar con rutas explícitas dentro de la red MPLS. La más sencilla es que el administrador de la red configure determinados LSPs para servicios específicos, estableciendo niveles de calidad diferentes en función de la ruta a seguir. La otra forma es el establecimiento y mantenimiento de las rutas explícitas (túneles) de forma automática desde los LERs de acceso. Para ello es necesario que cada uno de los LSR de la red MPLS disponga de una base de datos con información de los recursos disponibles en la red con capacidades de ingeniería de tráfico, por ejemplo utilizando OSPF-TE [RFC3630] y emplear algún protocolo de intercambio de etiquetas que permita indicar un LSP explícito como RSVP-TE o LDP-CR.

2.4.5.2 Protección y recuperación ante errores en red

Gracias al establecimiento de túneles, la red MPLS permite la protección y recuperación frente a fallos en la topología, estableciendo túneles de respaldo (*backup*) que se utilizarán en caso de caída del túnel principal. Se pueden predefinir LSPs de respaldo en cualquier punto del camino, lo que permite recuperarse ante fallos de enlace o de un LSP completo.

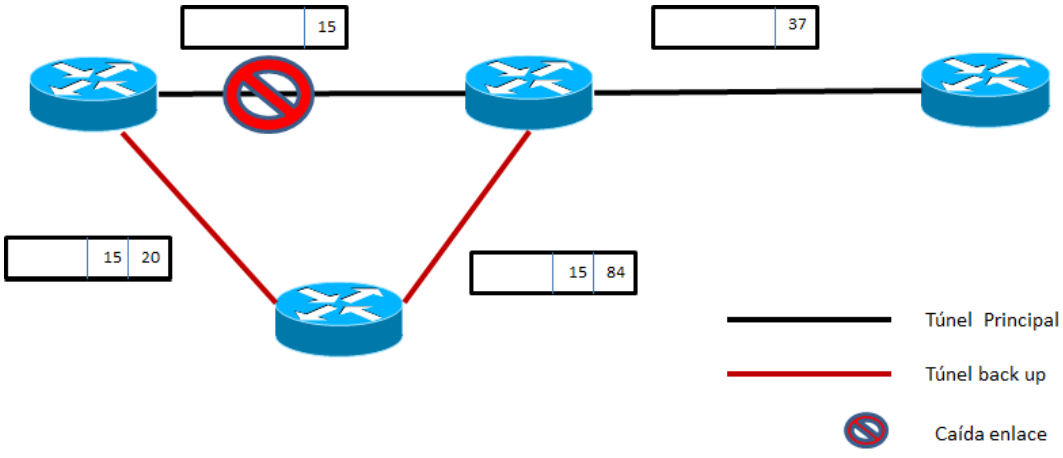

Figura 9. Recuperación ante fallos

El funcionamiento, que se puede observar en la Figura 9, consiste en que cuando un paquete se desvía por el túnel de respaldo, se le añade una etiqueta provisional (i.e. mediante *label stacking)* para encaminarle al LSP de respaldo de forma que luego éste le reencamina de vuelta al LSP principal, tras evitar el punto de fallo. Una vez en el LSP principal, el LSR le quita la etiqueta provisional y deja la original a la vista para encaminarla al siguiente LSP.

2.4.5.3 Calidad de Servicio (QoS)

Las aplicaciones y servicios actuales necesitan unos requerimientos de ancho de banda y retardo en su transmisión muy distintos, por lo que no solamente necesitamos técnicas de ingeniería de tráfico sino también poder clasificar y priorizar ese tráfico.

Existen dos posibilidades estandarizadas por el IETF que permiten asegurar un tratamiento requerido para un paquete clasificado con una calidad específica:

- El modelo *Diffserv*, recogido por el IETF en la RFC 3270 [9], se basa en la clasificación del tráfico a la entrada de la red por clase de servicio, y éste se marca utilizando el campo *DiffServ Code Point* (DSCP), definiendo así flujos de paquetes que recibirán un tratamiento específico en la red en función de su QoS. Esta diferenciación de servicios permite clasificar un reducido número de clases de servicio con diferentes prioridades.

- El modelo *IntServ* que utiliza el *Resource Reservation Protocol* (RSVP), definido por el IETF en la RFC 2205 [10], para reservar recursos por cada flujo. Este método proporciona servicios garantizados a través de la red.

MPLS se adapta perfectamente al modelo *Diffserv* ya que el encaminamiento se realiza en función de las etiquetas, y a las clases de servicio se pueden mapear a FEC diferentes incluyendo la información del DSCP en la dentro de la etiqueta MPLS en el campo *Traffic Class*.

En función del valor de este campo, al tráfico que se encamina por un determinado LSP se le puede asignar a diferentes colas de salida o los LER pueden establecer múltiples LSPs, cada uno de ellos con diferentes prestaciones, y enviando el tráfico por uno de ellos en función de la calidad de servicio que se necesite.

Por otro lado, la integración de RSVP con MPLS opera de la siguiente manera:

- El emisor envía al receptor un mensaje *path* de RSVP, que circula a través de un trayecto establecido dentro de la red MPLS.

- El receptor responde con el mensaje *resv* de RSVP que será tratado por los LERs de acceso a la red MPLS creando un LSP que cumpla los requisitos de QoS.

2.4.5.4 *Virtual Private Network* (VPN)

VPN es una tecnología que nos permite emplear una red pública para interconectar múltiples emplazamientos con la seguridad y las funcionalidades de una red privada, comunicándoles como si estuvieran dentro una red independiente.

Para poder desplegar este tipo de redes privadas, tradicionalmente era necesario recurrir a enlaces dedicados o a infraestructuras de transmisión compartidas como *Frame Relay* o *ATM,* en los que se establecían *Private Virtual Circuits* (PVCs) entre los nodos de la red.
Estas soluciones tenían un coste muy elevado, inviable si era necesario construir un camino dedicado entre dos nodos alejados, y muy poco escalable, pues el incorporar o eliminar un

nodo de la red ocasionaba tener que reconfigurar todos los PVCs. Al interconectar todas las sedes entre sí (i.e. *full mesh*) los circuitos virtuales crecían de manera exponencial al ir aumentando los nodos que componían la red.

Las redes VPN sobre MPLS surgen como alternativa para crear redes privadas virtuales proporcionando una mayor escalabilidad y facilidad para añadir nuevos nodos a la red y su gestión, así como en los mecanismos de QoS.

Además utilizar una red de conmutación de paquetes (e.g. IP o Ethernet) que los operadores de comunicaciones ya disponen, permite obtener una reducción de costes significativa ya que no es necesario desplegar una infraestructura nueva y simplemente tendremos que unir el emplazamiento donde se encuentre la sede con el punto de acceso a la red del operador.

2.5 *Border Gateway Protocol* (BGP)

BGP es un protocolo de encaminamiento basado en el intercambio de la información de rutas entre *peers* (vecinos). Una sesión BGP se establece entre dos *peers*. Utiliza el puerto 179 de TCP para establecer sus conexiones. Cuando comienza la conexión, un enlace BGP intercambia toda su tabla de rutas completa con el vecino, mientras que una vez está establecida, solo intercambiará las modificaciones que se producen en su tabla de rutas, siendo un protocolo eficiente cuando el número de rutas anunciadas es elevado. BGP-4 definido en la RFC 4271[11] es la última versión estandarizada por el IETF.

En este protocolo es importante el concepto de sistema autónomo (*Autonomous System*, AS). Se denomina sistema autónomo a la red o grupo de redes bajo una administración común y con unas políticas de encaminamiento comunes. Asociado a esta definición se definen dos tipos de protocolos BGP:

- BGP externo (eBGP). El intercambio de información rutas se produce entre dos sistemas autónomos diferentes y conecta la frontera de ambos.

- BGP interno (iBGP). Enlaza routers dentro del mismo sistema autónomo intercambiando información de rutas entre ellos.

Existen 4 tipos de mensajes en BGP que se intercambian entre los *peers* (vecinos) una vez establecida una conexión a nivel de transporte TCP, tal como se puede observar en la Figura 10:

- *Open*. Es el mensaje se envía al inicio de una sesión BGP para su establecimiento. En él se intercambian los parámetros definidos para esa sesión. El receptor debe aceptar este mensaje para que la sesión pueda establecerse.

- *Keepalive*. Es un mensaje que se envía periódicamente después de estar establecida la sesión y sirve para comprobar que el otro extremo de la sesión permanece activo.

- *Update*. Es un mensaje que se envía cada vez que existe una actualización en la tabla de rutas de uno de los extremos, ya sea la incorporación de una ruta nueva o la modificación de una existente.

- *Notification*. Es un mensaje que se envía cuando se produce un error, y provoca el cierre de la sesión BGP establecida.

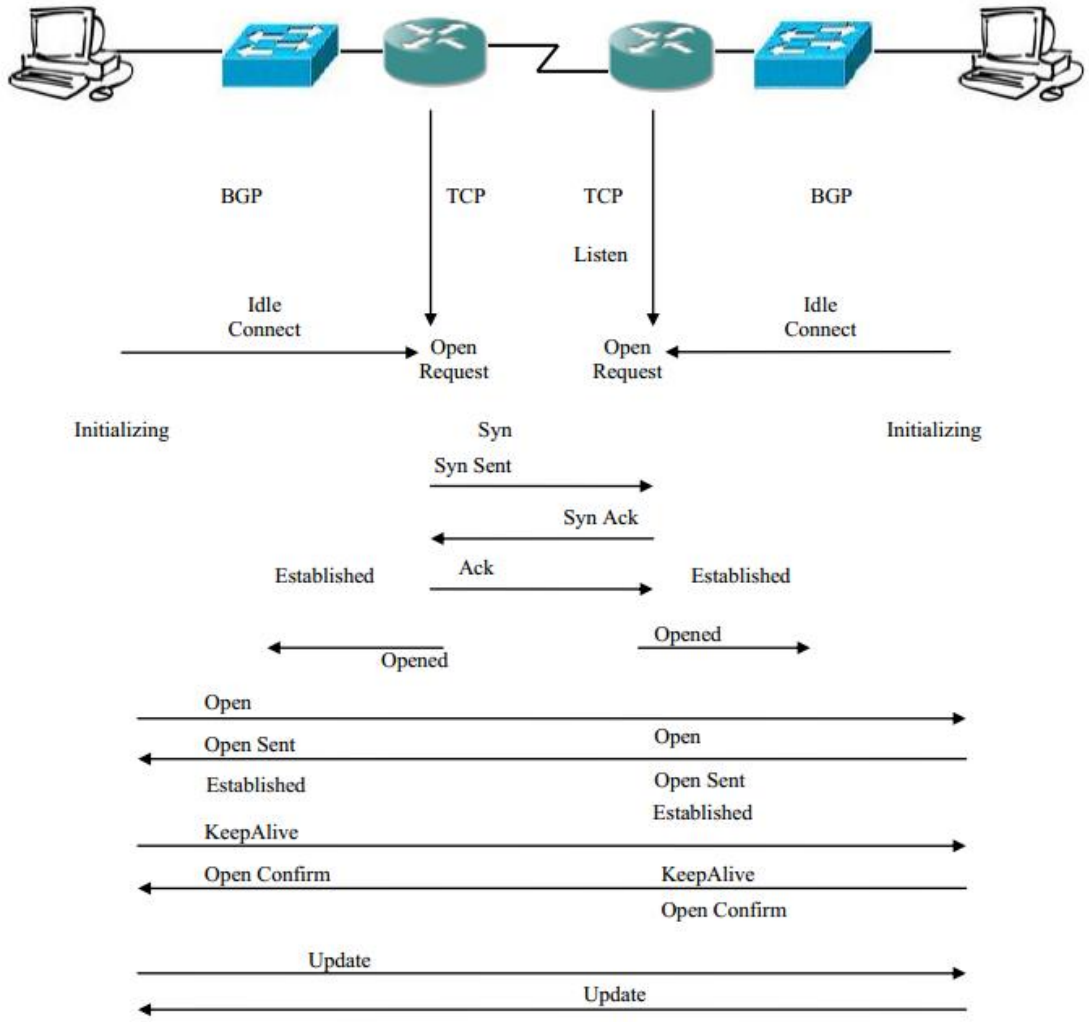

Figura 10. Establecimiento de una sesión BGP. [12]

BGP no es un protocolo de encaminamiento basado simplemente en encontrar el camino más corto entre un origen y un destino, sino que elige la ruta más adecuada entre ellos mediante una serie de atributos.

Los atributos en los que se fundamenta esta elección viajan en los mensajes *update* y son:

Next-hop. IP del vecino que anuncia la ruta. Un *next-hop* anunciado por un eBGP permanece inalterable en una sesión iBGP. Este atributo es obligatorio en todos los mensajes *update* de rutas.

Origin. Indica el mecanismo que origina el anuncio de ruta. Puede ser un protocolo interno al AS (0), un protocolo externo al AS (1), o de forma estática (2). El valor más bajo tiene mayor preferencia. Este atributo es obligatorio en los mensajes de rutas.

AS-Path. Es el camino de ASes a atravesar para llegar a una red. Se inicia con el AS que genera el update y se añaden los AS por los que pasa. Este atributo no tiene en cuenta los saltos que se producen dentro de cada AS.

Local-preference. Se trata de un atributo con sentido dentro de un AS e indica el camino preferido para salir del AS.

*Multi-exit-discriminator (*MED). Indica a los vecinos externos el camino preferido para entrar en un AS cuando existen varias opciones.

La prioridad en la elección del camino óptimo se realiza en el siguiente orden:

1. *Local-preference* más alta.

2. AS-Path más corto.

3. MED menor.

4. Se prefieren rutas aprendidas por eBGP sobre aprendidas por iBGP.

5. En caso de misma prioridad se elegirá el que cuenta con un ID más bajo o sea más antigua.

2.6 Las redes VPN-MPLS

La solución de VPN sobre MPLS está estandarizado por el IETF en la RFC 4364 [13]. También se la conoce como BGP/MPLS ya que se emplea BGP para distribuir la información de encaminamiento a través de la red del proveedor de comunicaciones, y MPLS para el reenvío de tráfico entre los nodos que forman la VPN.

Es necesario utilizar el protocolo BGP ya que éste permite utilizar direccionamiento solapado, de forma que varios clientes pueden utilizar la misma subred privada dentro de la MPLS, mediante el direccionamiento ampliado para poder distinguirlo de otros clientes.

Este modelo de VPN, mostrado en la Figura 11, está formado por varios elementos:

- *Customer Edge Router* (**CE**). Se trata del *router* ubicado en domicilio de cliente que le proporciona acceso a la red del proveedor de comunicaciones sobre un enlace de datos. Este equipo puede utilizar cualquier tecnología de acceso a la red y cualquier protocolo de encaminamiento contra el punto de acceso del proveedor.

- *Provider Edge Router* (**PE**). Se trata del *router* de entrada a la red del proveedor de comunicaciones, al que se conectan los *routers* de cliente y con los que intercambia

información de encaminamiento. Este equipo puede proporcionar el servicio de VPN a múltiples clientes. El PE tiene las tablas de encaminamiento específicas de cada VPN a la que da servicio. A nivel MPLS se trata del equipo LER, por lo que tiene capacidad de conmutación de etiquetas.

- ***Provider Router*** (**P**). Cada uno de los *routers* internos que se encuentran en la red del proveedor de comunicaciones. Se comunican con los PE y con otros P, pero nunca se encuentran conectados con el *router* de cliente. Estos routers no tienen información de rutas de la VPN y funcionan como un LSR conmutando etiquetas.

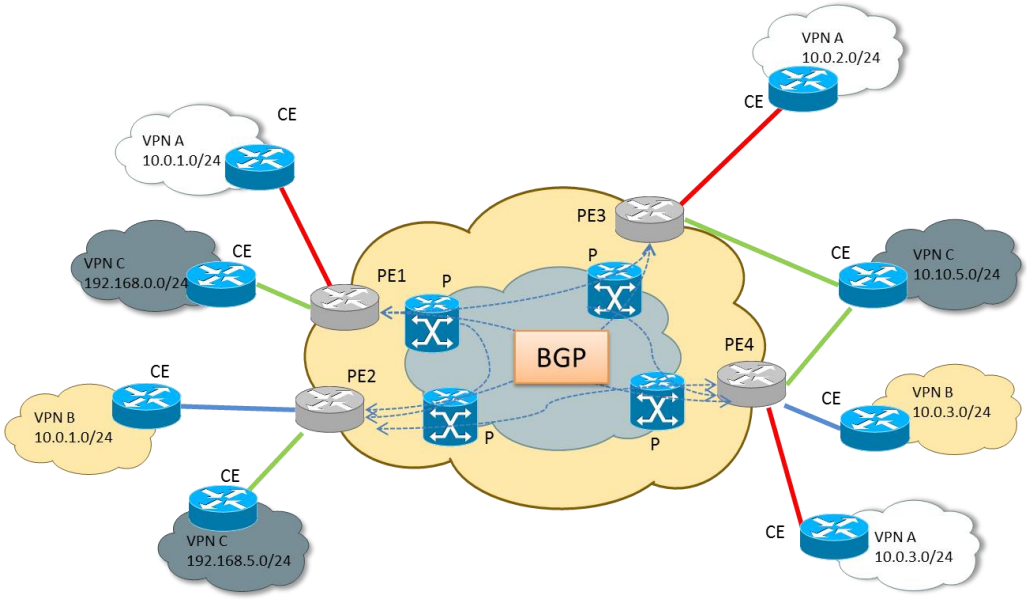

Figura 11. Redes VPNs sobre infraestructura MPLS compartida

La comunicación entre PEs y Ps se realiza mediante el protocolo MP-BGP (Multiprotocol BGP) [14].

En cada PE se crea una tabla de rutas única para cada VPN a la que da servicio, denominada **VRF** (*VPN Routing and Forwarding Table*). De esta manera el PE se comporta como si fuera un router dedicado para cada VPN, proporcionando seguridad ya que aísla el tráfico entre las diferentes VPNs. El PE recibe un paquete del CE, comprueba su tabla de rutas del VRF correspondiente y determina el enrutado por el que saldrán los paquetes.
El principal beneficio de esta característica es poder utilizar el mismo direccionamiento por diferentes clientes en diferentes VRFs como se observa en la Figura 12.

En el PE la asociación con el VRF se establece a nivel de interfaz (puerto) de conexión, por lo que si existen varias conexiones del PE con CEs de la misma VPN, todas ellas pueden asociarse con el mismo VRF.

Este modelo es altamente escalable y fácil de administrar, ya que como son los PEs que dan accesos a los CEs los que almacenan las tablas de encaminamiento de las VPNs, y éstas se

anuncian mediante BGP, no se requieren modificar ningún elemento más de las red si queremos añadir un elemento adicional. Tan solo sería necesario configurar el CE y el PE que le proporciona el acceso a la red del proveedor de comunicaciones para añadir una sede nueva a la VPN.

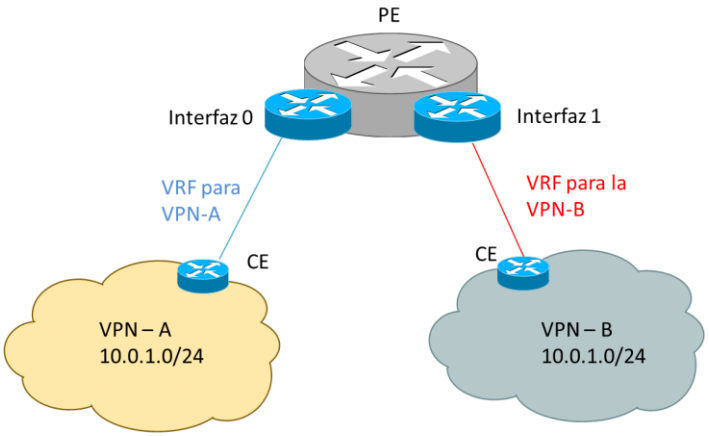

Figura 12. VRFs en el PE para varias VPNs

Existe la posibilidad de que un CE pueda pertenecer a distintas VRFs, lo que se define como MultiVRF [15], como se puede observar en la Figura 13, permitiendo que un mismo equipo cliente forme parte de varias VPNs de manera aislada, sin compartir información entre ellas.

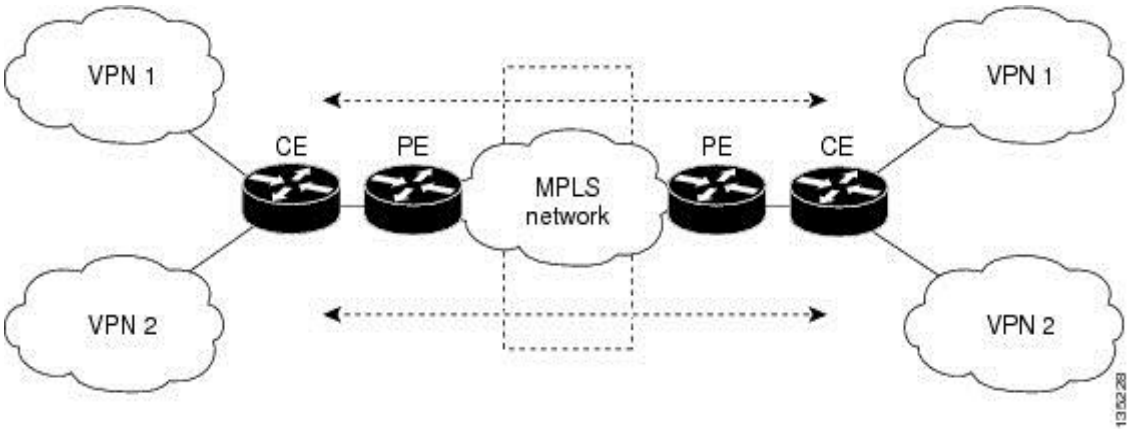

Figura 13. MultiVRF

Con MultiVRF dos o más clientes pueden compartir un CE y tener solamente un enlace físico CE-PE, con planos de rutas separados, lo que permite al CE actuar como un *router* virtual para cada VPN a la que pertenezca. Mediante puertos troncales con diferentes *VLANs* en la misma conexión se identifican los paquetes de cada uno de las VPNs. Cada cliente utiliza una *VLAN* diferente.

Para el PE esta solución es completamente transparente, puesto que actúa como si se trataran de CEs diferentes en función de la *VLAN* por la que le llega, que está asociada a la VRF correspondiente.

2.6.1 Encaminamiento en una red VPN-MPLS

Como se ha comentado anteriormente, en las redes VPN MPLS hay dos tipos de flujos de información de enrutamiento: el que se produce entre el CE y el PE, en el que se puede utilizar rutas estáticas o cualquier protocolo de encaminamiento entandar (RIP, OSPF, BGP,…), y otro entre los PEs y los Ps de la red MPLS, para el que siempre se utiliza BGP.

Las VRFs por si solas no son operativas, ya que únicamente permiten separar el encaminamiento a nivel local en un mismo PE. Es necesario distinguir las direcciones IP de las VRFs de un PE de las de otros PEs, así como transportar información de encaminamiento entre ellos. Se debe enviar información adicional junto con las rutas para poder diferenciarlas, para ello BGP utiliza el RD (*Route Distinguisher*) y el RT (*Route Target*).

La RFC 4364 define el concepto de dirección VPN-IPv4 para poder realizar una distinción entre rutas. Una dirección VPN-IPv4 tiene 12 bytes ya que a un prefijo de dirección IPv4 se le añade un campo RD (*Route Distinguisher*) de 8 bytes, lo que permite el solapamiento de espacio de direcciones entre distintas VPNs y mantener rutas separadas para los rangos de direcciones que tengamos en cada VPN. El RD no contiene información acerca del origen de la ruta o del conjunto de VPNs sobre los que se va a distribuir la ruta. Las direcciones VPN-IPv4 solo se intercambian entre los PEs finales independientemente de los Ps por lo que transiten.

Por último hay un parámetro que nos indica cuales de todas las rutas que se intercambian entre los PEs deben ser visibles en cada VRF concreta. Para ello se define el RT (*Route Target*), valor que viaja junto con el anuncio de rutas e indica cuales de ellas serán visibles por la VRF. Existen dos tipos de RT:

-RT *Export*. Valor que le va a dar el *Route Target* de las rutas del PE cuando se envíen a otros PEs.

- RT *Import*. Para las rutas que se reciben en el PE, las que lleguen con valor RT *Import* son las se introducen en la tabla de rutas de dicha VRF

Los valores de *Route Target* se indican a la hora de definir la VRF, (al igual que los de *Router Distinguisher*). Una VRF puede tener tantos *Route Target Import* y *Export* como sean necesarios.

2.6.2 Reenvío de tráfico en una red VPN-MPLS

El reenvío de tráfico en una red VPN MPLS se basa en la información de rutas almacenada en las tablas VRF de los PEs, tal como muestra la Figura 14.

Dado que los *routers* P de la red del proveedor no almacenan información de enrutamiento de cada VPN, se tiene que utilizar un doble nivel de etiquetas. Cada PE asocia una etiqueta por cada interfaz de entrada que inserta en las rutas que anuncia hacia el resto de la red:

- El PE1 se configura para asociar el VRF A con el interfaz por el que aprende las rutas anunciadas por CE1. El PE1 asigna una etiqueta MPLS al interfaz por el que recibe las rutas y la anuncia hacia el PE2 junto con la etiqueta MPLS, estableciendo su dirección IP como siguiente salto BGP para esa ruta.

- El PE2 recibe el anuncio de ruta del PE1 y, en función de las políticas de distribución de rutas, comprueba que entre las que tiene definidas pertenece a la VRF A y la incluye en su tabla de rutas. El PE2 anuncia a la ruta a CE4.

Para enviar el tráfico MPLS de la VPN a través de la red del proveedor de comunicaciones se establecen LSPs. El establecimiento de los LSPs se hace utilizando un protocolo de distribución de etiquetas como LDP o RSVP. Dentro de la RFC se establece que como mínimo debe implementarse LDP para garantizar la interoperabilidad entre fabricantes.

LDP se utiliza para el establecimiento de LSPs sin QoS garantizada, mientras que RSVP se utiliza cuando se necesitan LSPs que soporten QoS o ingeniería de tráfico. Entre cada pareja de PEs se pueden establecer varios LSPs en paralelo si se necesita enviar tráfico con diferentes tipos de QoS.

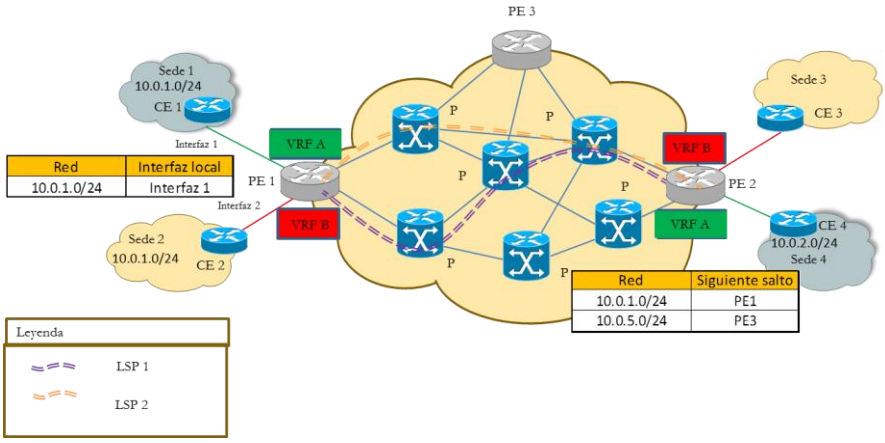

Figura 14. Reenvío de tráfico en red VPN MPLS

Cuando queremos enviar información entre dos puntos de la red, el proceso de la Figura 14, sería el siguiente:

- Un equipo ubicado en la sede 4 quiere enviar información a un equipo ubicado en la sede 1. Para ellos el equipos de la sede 4 enviará el trafico hacía el CE4 que actúa como *gateway* de la sede y que envía los paquetes hacia el PE2.

- El PE2 realiza una búsqueda de la ruta destino dentro de la tabla del VRF A. Obtiene la etiqueta MPLS añadida a la ruta por el PE1, el siguiente salto (la dirección IP del PE1), el

interfaz de salida para el LSP establecido entre ambos PEs y la etiqueta inicial para este LSP. El PE2 coloca la etiqueta MPLS correspondiente a la ruta al fondo de la pila de etiquetas y la etiqueta inicial al principio, y la envía los paquetes por el interfaz de salida correspondiente para el LSP.

- Cuando el PE1 recibe los paquetes enviados por el PE2, toma la etiqueta MPLS del fondo de la pila, identifica que la etiqueta corresponde con CE1 y se los reenvía eliminando las etiquetas MPLS añadidas por el PE1. El CE1 por último, le entregará los paquetes al equipo dentro de la sede 1.

2.6.3 Beneficios de las redes VPN-MPLS

La utilización de redes VPN-MPLS ofrecen numerosas ventajas tanto al cliente que las utiliza como al operador de comunicaciones que las oferta.

Utilización de red del operador de comunicaciones
El proveedor ofrece un servicio sobre una tecnología ya desplegada, por la que no tiene que realizar una inversión adicional en su red, pudiendo ofrecer el servicio a los clientes a un precio interesante. Solo es necesaria una conexión entre la sede del cliente y el punto de acceso a la red MPLS más cercano. El cliente se aprovecha de que esta solución es mucho más económica que los enlaces dedicados o PVCs, y le facilita poder añadir nuevas sedes.

Flexibilidad de la tecnología de acceso
Las redes VPN-MPLS permiten cualquier tecnología de acceso para conectar las sedes de los clientes con el punto de acceso del operador. Al operador le permite ofertar la mejor tecnología de acceso de la zona y al cliente le da la opción de poder elegir el tipo de acceso según sus necesidades, tanto de económicas como de rendimiento.

Escalabilidad de la red
Las redes VPN-MPLS proporcionan una alta escalabilidad para la red VPN del cliente. Para añadir una nueva sede solo es necesario instalar el acceso entre el CE y el PE y configurar ambos puntos, sin necesidad de tener que realizar modificaciones en el resto de la red. De la misma manera, en caso de eliminar una sede, bastaría con eliminar el interfaz de acceso al PE, con lo que dejaríamos de anunciar las redes utilizadas en esa sede y el resto de la red dejaría de recibirlas.

Flexibilidad en el direccionamiento
Estas redes permiten el solapamiento de espacio de direcciones entre distintos clientes, permitiendo al cliente utilizar los rangos de direccionamiento que desee sin necesidad de realizar modificaciones adicionales en su red interna para acceder a la VPN-MPLS.

Definición de clases de servicio
La red MPLS permite definir clases de servicio de la VPN que se adapten a las necesidades de las aplicaciones de las que disponga el cliente y garanticen dichos requisitos.

Privacidad de la red
Las redes VPN-MPLS separan el tráfico entre los distintos clientes que las utilizan como si fueran redes privadas separadas físicamente.

Administración de la red
La utilización de redes VPN-MPLS permite al cliente simplificar el mantenimiento de su propia red, pues es el operador de comunicaciones el encargado de la administración y gestión de la red global sobre la que se proporcionan. El cliente solo debe encargarse de la parte que se encuentre detrás del CE.
El operador de comunicaciones también se beneficia ya que el mantenimiento de la red global es común para todos los clientes, y el enlace PE-CE es la única parte independiente de la infraestructura VPN que oferta.

Disponibilidad de la red VPN-MPLS
La red del operador de comunicaciones ofrece unos niveles de redundancia y alta disponibilidad de los que los clientes se aprovechan al utilizarlo como red de interconexión de los nodos que formen su VPN.

Coste
Una solución de red VPN-MPLS permite al cliente contar con una red de altas prestaciones con un coste muy reducido en comparación con otras tecnologías, especialmente las redes privadas dedicadas.

2.7 *Simple Network Management Protocol* (SNMP)

SNMP, definido en su versión 1 en la RFC 1157 [16] por el IETF, actualmente su versión 3 se encuentra definida en la RFC 3410, es un protocolo de la capa de aplicación que permite supervisar, gestionar y monitorizar los dispositivos que forman una red mediante el intercambio de información estructurada.

El modelo SNMP se compone de tres partes:

- **Gestor *SNMP* (*SNMP manager*).** Es el sistema encargado de controlar y gestionar los dispositivos de la red. Normalmente recibe el nombre de *Network Management System* (NMS).

- ***Management Information Base*** (*MIB*). Es una base de datos contenida en el dispositivo gestionado que contiene la información referente a él estructurada en forma de objetos. Cada objeto tiene un identificador único (*Object Identifier* - OID).

- **Agente *SNMP* (SNMP *agent*)**. Es un módulo software ubicado en los dispositivos gestionados y que obtienen información de los mismos a través de la MIB que posteriormente es enviada a los NMSs.

Para activar el agente SNMP del dispositivo debe definirse el gestor SNMP que lo gestiona y los permisos que cuenta (*read-only, read-write*) asociando el agente a una *community* en la que se definen esos permisos. Un mismo agente puede comunicarse con varios gestores [17].

Existen dos formas de intercambio de información entre el agente y el gestor SNMP:

- Mediante un mecanismo de petición-respuesta. El gestor solicita al agente cierta información sobre el dispositivo en el que se aloja. El agente recoge el dato de la MIB y responde con el dato solicitado. Utiliza el puerto 161 de UDP.

- Mediante *traps*. El agente manda una notificación al gestor sin que éste se la haya solicitado, informándole que un evento ha ocurrido en el dispositivo en el que está alojado. El gestor normalmente muestra una alarma para que el administrador de la red tenga constancia del evento ocurrido o bien actúa automáticamente para solucionarlo. Utiliza el puerto 162 de UDP.

SNMP define diferentes tipos de mensajes que se intercambian entre el agente y el gestor. Los más importantes son:

- *GetRequest*. El agente pide que le devuelva el valor del objeto que le ha solicitado (OID).

- *SetRequest*. Este mensaje es usado por el gestor para solicitar al agente que modifique valores de objetos.

- *GetResponse. E*l agente utiliza este mensaje para devolver al gestor el valor de la petición realizada anteriormente. En función del tipo de OID solicitado el valor devuelto es de un formato concreto (*integer*, *counter*, *gauge*…)

- *Traps*. Este mensaje se genera por el agente para reportar al gestor de la ocurrencia de algún evento inusual ocurrido en el equipo en el que está alojado. Añade en el campo de datos la dirección IP del equipo para que el gestor lo reconozca.

SNMP define un formato para estos mensajes que se divide en tres partes, como se muestra en la Figura 15:

- *Version*. Es el número de versión del protocolo SNMP que utiliza el mensaje. Toma valor 1 cuando es SNMPv1, para SNMPv2 es 2 y 3 para SMNPv3.

- *Community*. Palabra que define la comunidad para la autenticación. Permite el acceso entre el gestor y el agente así como el control de acceso (lectura y/o escritura).

- PDU. Contiene los datos del protocolo. Tiene un tamaño variable en función del tipo de mensaje que se envíe. Excepto en un mensaje de *traps*, la PDU se estructura en las siguientes partes:

- *Type*. Define el tipo de mensaje SNMP.

- *Request-id*. Identificador único para cada petición. Este valor será el mismo en la respuesta de la petición.

- *Error-status*. Indica si se ha producido un error cuando se procesa una petición. En los mensajes *getRequest* y *setRequest* su valor es 0. Otro valor en la respuesta indica el tipo de error producido.

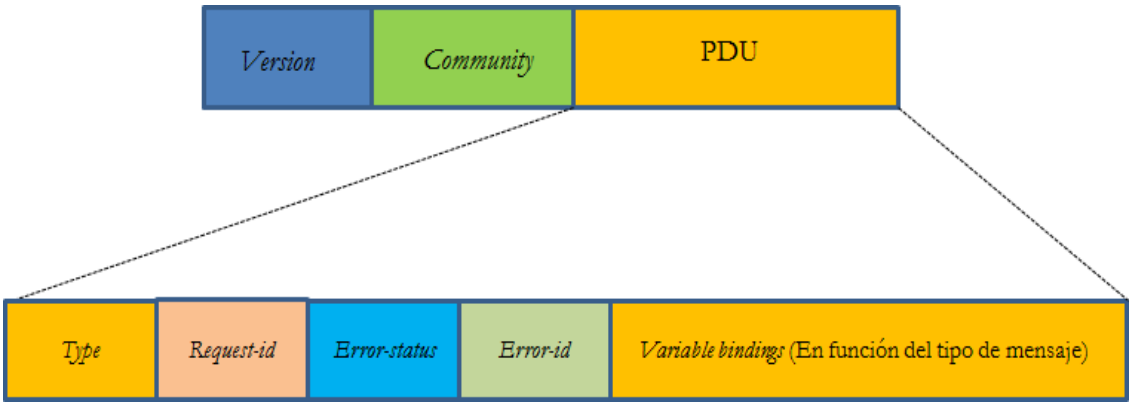

Figura 15. Estructura mensaje SNMP genérico

- *Error-id*. Cuando se produce un error proporciona más información, indicando que instancia de la *variable bindings* lo ha producido. En los mensajes *getRequest* y *setRequest* su valor es 0.

- *Variable bindings*. Es una lista de los nombres de las variables (OIDs) y sus correspondientes valores. En los mensajes *getRequest* o *getResponse* toma valor NULL.

Basado en SNMP y en las formas de intercambio de información entre el gestor y el agente existen muchas herramientas que permiten la monitorización de redes para su supervisión mediante la recogida, almacenamiento y presentación de resultados.

2.8 *Virtual Router Redundancy Protocol* (VRRP)

El VRRP [RFC2338] es un protocolo definido por IETF y ampliado en la RFC 5798 [18] que permite el despliegue de *routers* redundantes en una red. Este protocolo evita la existencia de puntos de fallo únicos mediante técnicas de redundancia y comprobación de estado de los routers.

En una red LAN con VRRP se establece como siguiente salto y salida hacia la red WAN una IP virtual compartida por los *routers* y a la que siempre apuntan los clientes, de manera que el *router* que realmente la tiene es transparente a los clientes. Se trata por tanto de un

protocolo que ofrece redundancia de manera automática sin necesidad de intervención humana. Todos los *routers* deben pertenecer a la misma red LAN y tener visibilidad entre ellos.

En cada uno de los *routers* se define una prioridad, que por defecto tiene valor 100. El *router* de mayor prioridad es el que se establece como activo y el que responde a la IP virtual. El resto de *routers* quedan en estado pasivo.

Basándonos en un ejemplo de VRRP entre dos *routers*, el funcionamiento sería el siguiente:

- Se determina el *router* activo que se configura con una prioridad mayor a 100 y se define en él la comprobación periódica de una ocurrencia.

- Si esta ocurrencia deja de producirse el valor de la prioridad del *router* se decrementa a un valor inferior que la del *router* pasivo, de modo que éste pasa a ser el activo y se hace cargo de la IP virtual.

- Cuando esta ocurrencia vuelve a producirse, se incrementará nuevamente la prioridad del equipo en la que se realiza la comprobación y recuperará el estado activo.

La ocurrencia definida en el *router* que en condiciones normales actuará como activo, puede ser la caída del interfaz de salida a red o preferiblemente, para abarcar también una posible incomunicación sin caída física, la recepción de una ruta global de la red siempre activa. El cambio de *router* activo se realiza en pocos segundos y es prácticamente imperceptible para el usuario.

Este protocolo es compatible entre diferentes fabricantes. Cisco cuenta con un protocolo estandarizado propio (*Hot Standby Router Protocol*, HSRP [RFC2281]) cuyo funcionamiento es similar al VRRP y es el utilizado si ambos equipos fuesen Cisco.

Capítulo 3. Diseño de la red privada virtual

Este proyecto se va a centrar en el diseño a alto nivel de la arquitectura y la elección de las tecnologías utilizadas para la creación de una solución de red global de interconexión para la empresa ACME S.A., que satisfaga las necesidades presentadas por el cliente y sea ajustada en costes de inversión (CAPEX) y operación (OPEX).

Para el desarrollo de la solución se han tenido en cuenta una serie de consideraciones de diseño que cumplen con los condicionantes que ha solicitado esta empresa de la manera más eficiente.

Basándose en estas premisas se ha planteado como la solución más adecuada establecer una red VPN-MPLS entre todas las sedes del cliente. Dentro de las ventajas descritas anteriormente en el apartado 2.5.3 las razones fundamentales para esta elección son:

- Escalabilidad. Posibilidad de incorporar nuevas sedes de manera sencilla y sin impacto en el resto.

- Flexibilidad. Este tipo de red permite utilizar la tecnología de acceso que mejor se adecue a las necesidades de cada sede.

- Disponibilidad. Utilizar la red del proveedor asegura una alta disponibilidad en la red así como disponer de un punto de acceso cercano a la ubicación de la sede.

- Coste. Este tipo de red permite una solución de altas prestaciones con un coste reducido.

3.1 Consideraciones previas de diseño

3.1.1 Topología de red

Se han contemplado dos posibles topologías: una solución de red con topología en estrella, en la que todos los nodos se conectan con un nodo central y deben pasar por él para comunicarse con otro nodo (*hub and spoke)*; y bien una topología de red mallada, en la que todos los nodos que la forman tienen visibilidad directa sin necesidad de pasar por un nodo central (*full mesh*).

El proveedor de comunicaciones no permite utilizar ambas topologías a la vez, por lo que no sería posible una solución hibrida *hub and spoke* con la sede central y mallada por delegaciones, y enfoca la VPN MPLS como *full mesh* en la que todas las redes anunciadas por cada una de las sedes son conocidas por el resto. Existe la posibilidad de implementar una solución *hub and spoke* en la que el punto central sea la sede principal pero limitaría la

posible diversificación de servidores fuera de la sede central y futuras modificaciones en la ubicación de los servicios centrales respecto del diseño inicial, por lo que siguiendo las recomendaciones del proveedor de comunicaciones se va a optar por una topología *full mesh*.

En la topología *full mesh* la sede central de cliente, que asumirá la mayor parte del tráfico generado en la red, se trata con un punto más de la red por lo que una incomunicación en él no implica la incomunicación entre el resto de sedes que componen la red, como ocurriría al utilizar una topología *hub and spoke*. Además, como el tráfico que se genere entre las sedes remotas no tiene que pasar por la sede central, se podrá ajustar los caudales definidos en ella permitiendo reducir costes en los caudales que se contraten. La comunicación entre sedes que forman parte de una delegación es independiente al nodo central.

Para conexiones centralizadas, como pueden ser el acceso remoto a servidores o la conexión a Internet, con la topología mallada el cliente puede controlarlos mediante políticas de firewalls o proxys en el punto central del mismo modo que en una topología en estrella con todo el tráfico que pasa por él.

3.1.2 Equipamiento de conexión para las sedes

Se ha escogido la opción de alquilar el equipamiento de comunicaciones frente a la compra en propiedad por los siguientes motivos:

- Desembolso inicial:

Realizar la compra de *routers/switches* en propiedad supone un desembolso inicial mucho mayor que realizar un pago mensual/anual por su alquiler. El proveedor de comunicaciones oferta un paquete completo de acceso, equipamiento y mantenimiento para cada nodo de la red VPN MPLS con una cuota mensual, sin cobrar alta.

- *Stock* adicional:

Si se decide tener los *routers/switches* en propiedad sería necesario contar con equipos de repuesto de cada uno de los modelos utilizados, para que en caso de avería se pueda disponer de uno sin esperar a solicitarlo al proveedor y que éste lo suministre. Además sería preciso contar con personal especializado en la gestión y mantenimiento del equipamiento, lo que supone un coste adicional.

Por el contrario con el alquiler del equipamiento viene incluido el mantenimiento de cada *router/switch*, lo que permite no tener que disponer de stock adicional y cuenta con la reparación y sustitución de los equipos averiados sin personal propio, ahorrando en costes y tiempos de resolución de las averías.

- Renovación tecnológica:

Contar con un *router* en propiedad supone que a medio plazo el equipo elegido pueda ser descatalogado por el fabricante y deje de tener stock o soporte ante roturas y fallos,

mientras que con el equipo en alquiler, si el equipamiento fuese descatalogado, en caso de que fuese necesario sería sustituido por otro modelo actual de similares características al anterior.

3.1.3 Redundancia en acceso y tecnología

Para aumentar la disponibilidad de cada sede, se ha decidido contar con dos accesos diferenciados para que en caso de caída del acceso principal, la sede pueda funcionar por el acceso de respaldo.

En las sedes remotas, el acceso de respaldo será degradado y de diferente tecnología respecto del principal, para el ahorro de costes, ya que este acceso solo funcionará una media estimada del 1 o 2 % del tiempo.

3.1.4 Redundancia en equipamiento

También se ha contemplado la necesidad de contar con doble equipo de acceso en las sedes para reducir la probabilidad de incomunicación en caso de fallo en este equipamiento. Sin embargo esta premisa no se ha tenido en cuenta para las sedes con pocos trabajadores en los que, para reducir costes, se utilizará un equipo único.

3.1.5 Protocolo de r*outing* entre la sede y su punto de acceso a la red

El proveedor de comunicaciones requiere que entre el PE de acceso a la red y el CE se defina encaminamiento a nivel WAN. Por lo tanto se ha decidido utilizar el protocolo de encaminamiento BGP en el acceso de la sede a la red del proveedor frente a RIPv2 ya que el tiempo de convergencia en caso de fallo bien en red o en el equipamiento es mucho menor. Con BGP una caída se detecta en torno a los 30 segundos mientras que con RIPv2 necesita de unos 3 minutos. Además con BGP la red VPN estaría preparada para soportar telefonía IP sin realizar modificaciones en la configuración de la red ya que es el protocolo de encaminamiento necesario para implementarlo.

Internamente en la sede se ha determinado no utilizar *routing* pues el *router* de acceso pertenece a la propia red LAN y todas las maquinas son visibles de manera directa. En caso de necesidad de contar con redes adicionales, se definirán rutas estáticas que apunten hacia el firewall interno de cliente y serán anunciadas al resto de la red MPLS por el *router/switch* de la sede.

3.2 Solución de acceso adoptada por sede

En función de los empleados de cada una de las sedes y sus necesidades de ancho de banda se ha realizado una agrupación de éstas en tres tipos: sede central, sedes Tipo I y sedes Tipo II. Cada uno de los tipos de sede va a contar con una solución específica, variando los caudales en función de los recursos que necesiten cada una.

3.2.1 Accesos sede central (CPD) y respaldo de la sede central

Para la solución de la sede central, Madrid I, con 50 trabajadores y del punto más importante de la red donde se encuentran ubicados sus servidores, se ha decidido redundarlo en dos ubicaciones diferentes extendiendo su parte LAN mediante tecnología WDM, tal como se representa en la Figura 16. Se utilizará la sede Madrid II, con 20 trabajadores, como sede de respaldo. Esta sede se encuentra a cinco kilómetros de la sede Madrid I.

En ella, el cliente duplicará sus servidores para que en caso de aislamiento de la sede Madrid I, los servidores de Madrid II puedan ser accesibles por el resto de sedes. Se creará un circuito dedicado mediante fibra óptica entre ambas ubicaciones, utilizando dos caminos independientes formando un anillo para garantizar la alta disponibilidad de las comunicaciones y la seguridad por cortes en el servicio. Los servidores de cliente estarán en todo momento sincronizados utilizando la infraestructura WDM provisionada. Todo el tráfico que se transmita entre ambas sedes utilizará la fibra del anillo WDM. Además esta sede contará con un punto centralizado de salida a Internet para todas las sedes del cliente, y estará igualmente redundada en la sede de respaldo. Las sedes remotas se conectarán a Internet mediante proxy HTTP, facilitando al cliente la gestión de los contenidos accesibles a los usuarios y el control del uso realizado.

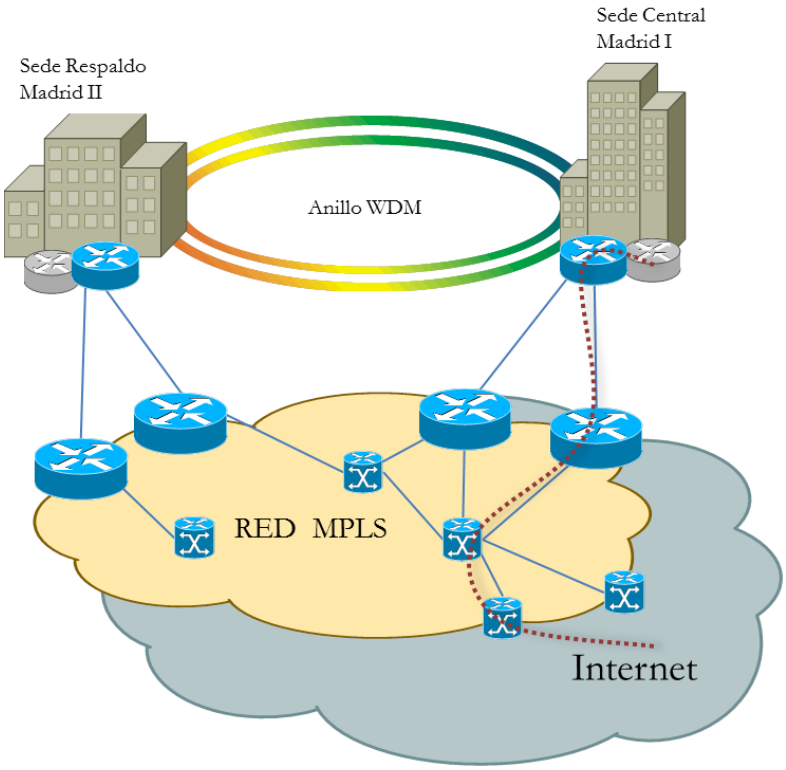

Figura 16. Detalle conexión a la red de sede central y sede respaldo con salida a Internet

Para la conexión a la red VPN MPLS de la sede central y la sede de respaldo se utilizará una conexión de fibra óptica en cada una de las sedes con dos puntos de acceso a la red (conexión PE-CE). El proveedor de comunicaciones oferta para la conexión accesos de fibra de 10 Mbps, 100 Mbps y 1 Gbps. Se ha elegido un servicio Metro Ethernet de 100 Mbps desde el PE al CE, puesto que es el más se ajusta a los necesidades de ancho de banda requeridas por el cliente. Se ofrece en la interfaz de un adaptador de fibra óptica, denominado conversor de medio, que constituye física y funcionalmente el punto de terminación de red. La interfaz ofrecida es 100BaseTX, según IEEE 802.3, con un conector RJ45. La conexión con el CE se hará con cable UTP categoría 5.

El servicio de VPN MPLS que oferta el proveedor de comunicaciones no cuenta con salida a internet por defecto y tiene que incorporarse adicionalmente. Ambos accesos de fibra óptica tendrán el servicio de salida a Internet añadido. Para este servicio se ha utilizado un equipo independiente al que suministra el acceso de fibra que colgará de él como segundo nivel en cada acceso de fibra. Los accesos de ambas sedes a la red VPN MPLS serán idénticos.

Es necesario también asociar un caudal a cada conexión de fibra óptica que se provisione. Este caudal es el tráfico de datos que se le permitirá cursar al cliente por cada uno de los enlaces, limitando la capacidad máxima que permitiría el enlace a nivel de red. En función de las estimaciones del cliente (200 Kbps/usuario) se asignará a cada sede el caudal necesario para poder proporcionar a todos los trabajadores de cada sede el ancho de banda de manera simultánea. El proveedor de comunicaciones garantiza el caudal contratado en su totalidad.

Para esta sede se ha decido duplicar el caudal necesario según las estimaciones acordadas con el cliente, puesto que se trata de la sede donde se encuentran los servidores centrales y es el punto donde recibe mayor tráfico del resto de las sedes remotas. Los caudales de acceso a la red VPN MPLS de la sede central y la sede de respaldo serán por tanto de 30 Mb.

En cuanto la salida a Internet, se ha determinado establecer un caudal de 20 Mb para las necesidades que los trabajadores puedan tener. La empresa cuenta actualmente con una plantilla de 421 trabajadores y se estima en torno a unos 100 Kbps el uso de cada uno y que pueda ser usada por la mitad de los trabajadores de manera simultánea. La salida a Internet cuenta con un rango de direccionamiento público por defecto que puede ser utilizado tanto para navegación como para prestar servicios públicos. Es posible solicitar un rango de direccionamiento mayor del asignado. La utilización de este rango de direccionamiento público puede ser gestionado por el cliente, realizando NATs estáticos o dinámicos en sus *firewalls* o bien el *router* se encarga de traducción de direccionamiento privado a público para navegación o para prestar servicios públicos.

Al actuar ambas sedes como una única, el direccionamiento definido por el cliente para cada una de las sedes se anunciará al resto de la red VPN MPLS por cada uno de los

accesos, siendo el acceso activo el que curse el tráfico. Internamente el cliente enviará el tráfico hacia Madrid I o Madrid II en función del destino utilizando la conexión WDM si fuera preciso.

Para conectar los servidores centrales con el servidor de otra entidad para la compensación de seguros, se van a utilizar MultiVRF sobre los accesos ya definidos, de manera que se crea una nueva red privada virtual de conexión independiente a la red definida para todas las sedes de la empresa, compartiendo acceso y equipamiento. El tráfico producido para cada una de las VPNs se tratará de manera independiente y será transparente para la otra. Esta nueva VPN definida contará con un caudal independiente, de un 1Mb, el menor caudal que se puede contratar, debido a las bajas necesidades que requiere.

La conexión entre la sede principal y la sede de respaldo se realiza mediante dos enlaces de fibra óptica diversificados constituidos por dos fibras ópticas monomodo con tecnología WDM creando dos caminos alternativos e independientes en el trazado físico, tal como muestra la Figura 17. Se utiliza canalización existente de la red del proveedor de comunicaciones a la que se añade la nueva fibra, que será entregada en la arqueta de entrada de cada uno de los edificios. Uno de los caminos pasa por una central intermedia del proveedor de comunicaciones y mide 7 kilómetros y la otra realiza el camino de manera directa, con una longitud de 5,8 kilómetros. Se han decidido contar con los siguientes servicios:

- Dos canales Gigabit Ethernet
- Dos canales Fibre Channel

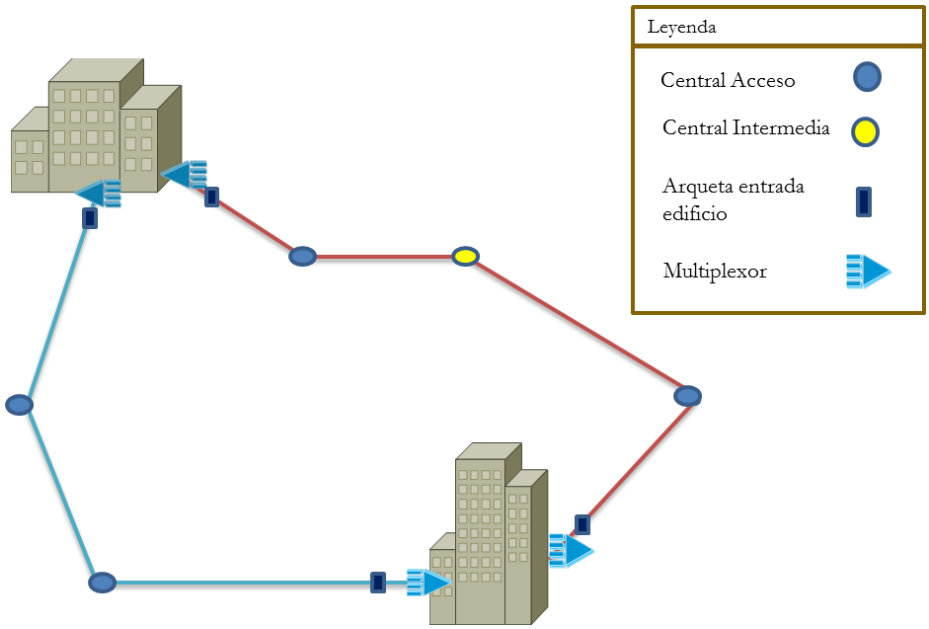

Figura 17. Trazado WDM entre sede principal y respaldo

Para contar con protección total ante fallos se ha determinado duplicar los equipos terminales de la interconexión de cada una de las sedes balanceando cada tipo de canal por cada uno de los equipos, y en caso de caída de uno de los equipos soportará ambos.

También se aconseja contar con dos canalizaciones independientes en el interior de las instalaciones de cliente para conseguir la diversificación física en toda la conexión.

3.2.2 Accesos sedes Tipo I

Se han clasificado como sedes Tipo I aquellas sedes que cuentan con 10 o más trabajadores detalladas en la Tabla 4 exceptuando Madrid II, que se ha utilizado anteriormente como respaldo de la sede principal por su cercanía a ésta.

Sede	Trabajadores	Sede	Trabajadores
Madrid III	10	Santiago I	15
Barcelona I	30	León I	15
Valencia I	30	Toledo I	15
Sevilla I	25	Barcelona II	15
Bilbao I	25	Valencia II	15
Zaragoza I	25	Mallorca I	15
Valladolid I	25	Las Palmas I	15

Tabla 4. Sedes Tipo I y trabajadores

En las sedes Tipo I se ha optado por una solución de doble acceso, representada en la Figura 18, para reducir la posibilidad de incomunicación de la sede. Para la conexión a la red VPN MPLS, el acceso principal utilizará fibra óptica con dos puntos de acceso a la red, y para el acceso de respaldo la línea xDSL de mayor capacidad disponible en la ubicación de cada una de las sedes.

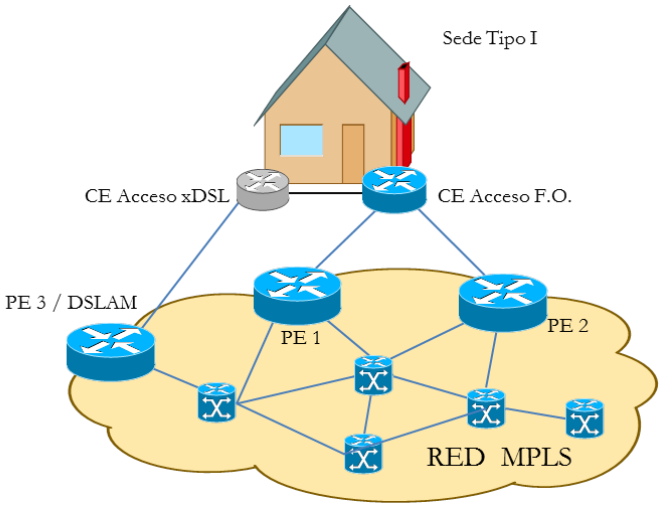

Figura 18. Detalle conexión de sede Tipo I a red MPLS

Entre los accesos ofertados por el proveedor de comunicaciones, se ha descartado el acceso de 1 Gbps, dado que para las necesidades de ancho de banda requeridas estaría sobredimensionado, y se ha elegido el acceso Metro Ethernet de 100 Mbps frente al acceso de 10 Mbps, pues el precio mensual del acceso de fibra junto con el respaldo y el equipamiento es el mismo. Las políticas comerciales ofertadas por el proveedor de comunicaciones permiten contar con un acceso de más capacidad sin aumentar el coste, puesto que la variación de precio estará determinada por el caudal que se contrate en cada una de las sedes. De esta manera la sede está preparada para posibles aumentos de ancho de banda por encima de los 10 Mbps sin necesidad de realizar ninguna modificación en él, ajustando el caudal a los requerimientos reales de la sede. Considerando que el flujo de datos para las sedes remotas será principalmente de bajada (petición de datos a servidores centrales y consultas a Internet) con el acceso de 100 Mbps obtenemos una ventaja considerable frente al acceso de 10 Mbps en la velocidad de descarga. En cuanto a la subida, se encontrará limitada por el caudal asignado a cada una de las sedes en función de los trabajadores que la compongan. Como en la sede central, el punto de terminación de la fibra se entrega mediante el conversor de medio 100BaseTX, según IEEE 802.3, con un conector RJ45 y la conexión con el CE se hará con cable UTP categoría 5.

En cuanto el acceso de respaldo, como las necesidades de las sedes remotas son mayores en el canal *downstream* que en el canal *upstream,* se ha optado por una solución degradada para conseguir un ahorro significativo en el coste. Este acceso de respaldo siempre está activo y sus anuncios se encuentran penalizados para que la fibra óptica sea la conexión preferida.

La Tabla 5 muestra en función de los trabajadores de cada sede, el caudal para cada acceso de fibra óptica que se ha determinado y la modalidad xDSL con mejores prestaciones de las ofertadas por el proveedor de comunicaciones con sus correspondientes valores máximos de tasa binaria.

Sede	Acceso Principal	Caudal	Acceso Respaldo	Tasa Binaria
Madrid III	Fibra 100 Mbps	2 Mb	ADSL2+	10 Mb/640 Kb
Barcelona I	Fibra 100 Mbps	6 Mb	VDSL	20 Mb/1 Mb
Valencia I	Fibra 100 Mbps	6 Mb	ADSL2+	10 Mb/640 Kb
Sevilla I	Fibra 100 Mbps	5 Mb	ADSL2+	10 Mb/640 Kb
Bilbao I	Fibra 100 Mbps	5 Mb	ADSL2+	10 Mb/640 Kb
Zaragoza I	Fibra 100 Mbps	5 Mb	ADSL2+	10 Mb/640 Kb
Valladolid I	Fibra 100 Mbps	5 Mb	ADSL	8 Mb/640 Kb
Santiago I	Fibra 100 Mbps	3 Mb	ADSL	6 Mb/640 Kb
León I	Fibra 100 Mbps	3 Mb	ADSL	8 Mb/640 Kb
Toledo I	Fibra 100 Mbps	3 Mb	ADSL2+	10 Mb/640 Kb
Barcelona II	Fibra 100 Mbps	3 Mb	ADSL2+	10 Mb/640 Kb
Valencia II	Fibra 100 Mbps	3 Mb	ADSL2+	10 Mb/640 Kb
Mallorca I	Fibra 100 Mbps	3 Mb	ADSL2+	10 Mb/640 Kb
Las Palmas I	Fibra 100 Mbps	3 Mb	ADSL2+	10 Mb/640 Kb

Tabla 5. Accesos por sede Tipo I

3.2.3 Accesos sedes Tipo II

Se ha clasificado como sedes Tipo II aquellas que cuentan con menos de 10 trabajadores, detalladas en la Tabla 6. Para este tipo de sede se ha optado por doble acceso en equipo único tal como se muestra en la Figura 19.

Sede	Trabajadores	Sede	Trabajadores
La Coruña I	5	Motril I	3
Vigo I	5	San Sebastian	5
Gijón I	5	Pamplona I	5
Salamanca I	5	Cuenca I	5
Badajoz I	5	Castellón I	5
Sevilla II	5	Alicante I	5
Cadiz I	3	Murcia I	5
Jaen I	5	Tenerife I	5

Tabla 6. Sedes Tipo II y trabajadores

El acceso principal para conectarse con la red VPN MPLS será la línea xDSL que mejores prestaciones ofrezca el proveedor para la ubicación de cada sede. En el extremo de cliente, el proveedor de comunicaciones suministrará e instalará en el punto de terminación de red un elemento de filtrado de las señales (*splitter*), en el que se ofrezca la interfaz física de conexión y facilite el uso compartido del bucle entre las comunicaciones telefónicas y el acceso indirecto mediante las tecnologías xDSL. La conexión del CE desde el splitter se realizará con un cable RJ11 de cuatro hilos. La línea telefónica será titularidad del cliente final y la cuota mensual irá incluida en el coste mensual asociado al acceso y al equipamiento de cada una de las sedes.

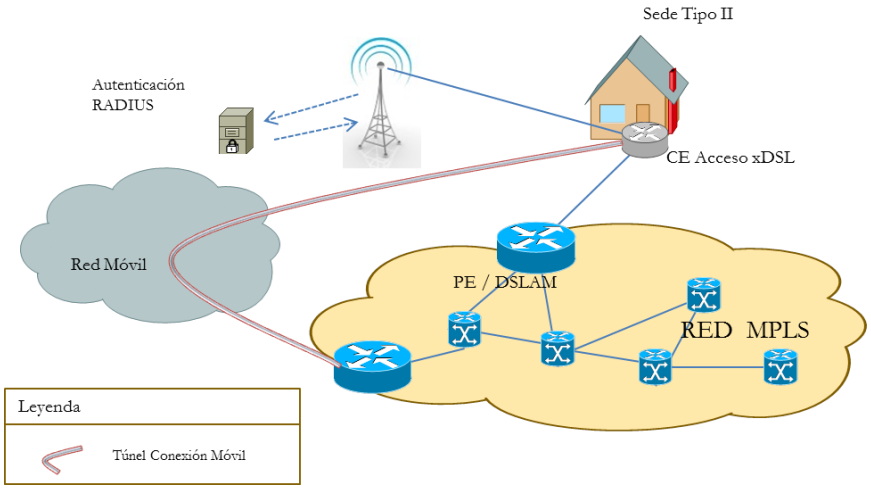

Figura 19. Detalle conexión sede Tipo II a red MPLS

Para el acceso de respaldo se ha contemplado la posibilidad de utilizar un respaldo móvil o bien un acceso conmutado RDSI. Se ha elegido el respaldo móvil con antena 3G sobre la línea conmutada RDSI porque la tecnología móvil ofrece un ancho de banda teórico mayor que el proporcionado por la línea conmutada RDSI. El ancho de banda del respaldo móvil aún no está garantizado por el proveedor de comunicaciones y puede verse reducido en determinados momentos por una demanda elevada o problemas de cobertura pero, al encontrarse las sedes en centros urbanos de grandes ciudades, la cobertura y los recursos disponibles parecen adecuados.

El funcionamiento de la conexión de respaldo de una sede une el CE con el PE de la red MPLS utilizando la red móvil mediante un túnel GRE. En primer lugar el número de móvil se registra en la red móvil validado con el PIN asignado a la tarjeta SIM. Cuando se encuentra registrado y se tiene que establecer la conexión, se autentica contra un servidor Radius de red con el identificador unívoco y password dentro del *Access Point Name* (APN) del cliente y se le asigna una IP al interfaz radio de la sede que será el origen del túnel que se establecerá como la IP de la subinterfaz del PE predefinida de acceso a la red MPLS para los accesos móviles del cliente. Con la creación de este túnel se permite la conexión del CE al PE atravesando la red móvil compartida de manera privada.

En función de la ubicación de cada una de las sedes, teniendo en cuenta la distancia a la central o repartidor del proveedor de comunicaciones y tecnología del acceso se han determinado para cada una el tipo de xDSL con mejores capacidades entre los disponibles. En los accesos xDSL para empresas el proveedor de comunicaciones garantiza el 50% del valor teórico contratado tanto en el canal de subida como en el canal de bajada.

En la Tabla 7 se muestra el tipo de xDSL que podrán provisionar a cada una de las sedes determinados por los accesos potencialmente válidos que nos indica el proveedor de comunicaciones dada la ubicación de cada sede.

Sede	Acceso Principal	Tasa Binaria	Acceso Respaldo
La Coruña I	ADSL2+	10 Mb/640 Kb	Respaldo movil 3G
Vigo I	ADSL	6 Mp/640 Kb	Respaldo movil 3G
Gijón I	ADSL	8 Mb/640 Kb	Respaldo movil 3G
Salamanca I	ADSL2+	8 Mb/640 Kb	Respaldo movil 3G
Badajoz I	ADSL	6 Mb/640 Kb	Respaldo movil 3G
Sevilla II	VDSL	20 Mb/1 Mb	Respaldo movil 3G
Cadiz I	ADSL	6 Mb/640 Kb	Respaldo movil 3G
Jaen I	ADSL2+	8 Mb/640 Kb	Respaldo movil 3G
Motril I	ADSL	8 Mb/640 Kb	Respaldo movil 3G
San Sebastian I	ADSL2+	10 Mb/640 Kb	Respaldo movil 3G
Pamplona I	ADSL2+	10 Mb/640 Kb	Respaldo movil 3G
Cuenca I	ADSL2+	8 Mb/640 Kb	Respaldo movil 3G
Castellón I	ADSL2+	10 Mb/640 Kb	Respaldo movil 3G
Alicante I	ADSL2+	10 Mb/640 Kb	Respaldo movil 3G
Murcia I	ADSL	4 Mb/ 640 Kb	Respaldo movil 3G
Tenerife I	VDSL	20 Mb/1 Mb	Respaldo movil 3G

Tabla 7. Accesos para sedes Tipo II

3.3 Solución de equipamiento adoptada por sede

El equipamiento para cada una de las sedes se alquilará al proveedor de comunicaciones. Este alquiler cuenta con gestión y mantenimiento de los equipos para que, en caso de incidencia, ésta sea resuelta por personal especializado, ya sea remotamente o in situ en las dependencias del cliente.

Entre los fabricantes de equipos que el proveedor de comunicaciones oferta actualmente, se encuentran Cisco, Teldat y Juniper. Aunque los equipos de diferentes fabricantes pueden convivir en la misma solución, se ha preferido que todo el equipamiento desplegado sea del mismo fabricante.

Para la elección del fabricante, se ha tenido en cuenta la experiencia en el despliegue y en el mantenimiento de otros proyectos anteriores, motivo por el cual se ha optado por elegir Cisco. El equipamiento de este fabricante ha ofrecido más fiabilidad que Teldat en los anteriores proyectos que ya se encuentran en mantenimiento. El número de incidencias provocados por los equipos Teldat fue mayor que el producido por el equipamiento Cisco. Este punto es de gran importancia para el cliente, de modo que siendo sensiblemente más caro la fiabilidad se ha antepuesto sobre el aspecto económico. En cuanto a Juniper se trata de un fabricante que el proveedor de comunicaciones ha introducido en los últimos años como equipamiento de acceso a la red. Si bien los PEs de acceso a la red MPLS son equipamiento de este fabricante y está comprobada su eficiencia, se ha preferido elegir Cisco sobre Juniper puesto que actualmente la experiencia en gestión y mantenimiento del equipamiento Cisco es mayor que Juniper y a largo plazo no se cuentan con referencias del comportamiento que tendrán estos equipos específicos para actuar como CE frente a la estabilidad probada que aporta Cisco.

Al igual que con los accesos según el tipo de sede, el equipamiento elegido será diferente para cada tipo y éste se seleccionará en función de la tecnología utilizada para cada acceso y el coste de los modelos disponibles ofertados por el proveedor de comunicaciones, eligiendo el más económico de los que soporten los requisitos de la conexión.

3.3.1 Equipamiento sede central (CPD) y respaldo de sede central

Para la sede central y su sede de respaldo en otra ubicación se cuenta con un acceso de fibra óptica con la funcionalidad adicional de salida a Internet, unidas mediante tecnología WDM.

Tanto en los accesos de fibra óptica como en el servicio de salida a Internet, el proveedor de comunicaciones asigna una VLAN para la conexión PE-CE. Este número identificará el interfaz de conexión entre ambos, que será único en el PE al que se conecta el CE. Cada extremo, contará con un direccionamiento dentro de la red asignada a esta conexión.

En la solución diseñada se ha determinado que para el servicio de salida a Internet se va a utilizar un equipo de segundo nivel conectado al equipo de acceso a la red MPLS. Tanto la conexión a la red como el servicio de salida a Internet tienen VLANs diferentes, así que el equipo de conexión para la fibra óptica debe permitir pasar la VLAN del servicio de salida

a Internet de manera transparente hacia el equipo de segundo nivel. Para ello se va a utilizar un *switch*. El que ofrece el proveedor de comunicaciones es el modelo Cisco Catalyst 3560v2 [19]. Entre las variantes que ofrece este modelo de *switch* se ha elegido el que dispone de 24 puertos FastEthernet (Catalyst 3560V2-24TS-E) pues el cliente ya cuenta con *switches* internos que se conectarán a nuestro *switch* y no será necesario que cada usuario se conectase a puertos libres de éste. Las características de este modelo de equipo aparecen en la Tabla 8.

Características	Vista frontal
Dimensiones: 4,4 x 44,3 x 25,9 cm	
Peso (maximo): 3,7 Kg	
Fuente de alimentación integrada tipo AC	
24 Puertos 10/100	
Cable Ethernet RJ45	
Temperatura funcionamiento 0-45 ºc	

Tabla 8. Características Catalyst 3560v2 de 24 puertos

Adicionalmente en el Catalyst 3560v2 se definirá una VLAN de acceso para la VRF de conexión con la otra entidad, con un *Route Targe* : *Route Distinguisher* diferente, y un plano de rutas independiente de la red VPN MPLS de la empresa, de manera que se simula con el mismo equipo y dentro del mismo acceso dos conexiones completamente separadas.

Modelo	Fibra Optica	Salida Internet
CISCO881-K9-[Cisco 881-K9]	10 Mbps	10 Mbps
CISCO892FSP-K9-[C892FSP-K9]	100 Mbps	No soportado
CISCO1921/K9-[Cisco 1921/K9]	10 Mbps	10 Mbps
CISCO2901/K9-[Cisco 2901/K9]	10 Mbps	10 Mbps
CISCO2951/K9-[Cisco 2951/K9]	100 Mbps	100 Mbps
CISCO3925/K9-[Cisco 3925/K9]	100 Mbps	100 Mbps
WS-C3560V2[Catalyst 3560V2]	1 Gbps	1 Gbps
ASR1001-[Cisco ASR1001]	1 Gbps	1 Gbps

Tabla 9. Equipamiento Cisco para accesos de fibra óptica

Para los equipos de segundo nivel que proporcionarán la salida a Internet, dadas las necesidades de caudal que se han determinado, es necesario elegir uno de los equipos que soportan más de 10 Mbps, según aparece en la Tabla 9. El más económico de ellos es el modelo Cisco 2951-K9 [20].

Las características de este equipo aparecen en la Tabla 10. Este *router* se conectará con cable directo Ethernet a uno de los puertos del switch Catalyst 3560v2 y empleará la configuración destinada para la salida a Internet.

Características	Vista frontal y trasera
Dimensiones: 8,89 x 43,82 x 46,99 cm	
Peso (maximo): 15,5 Kg	
Temperatura funcionamiento 0-40 ºc	
Memoria DRAM:512MB (requerida para 100Mbps	
ampliacion a 1GB)	
Memoria FLASH:256MB	
Licencia IP Base	
3 puertos Ethernet 10/100/1000	

Tabla 10. Características Cisco 2951-K9

La conexión entre la sede principal y la sede de respaldo se realiza mediante fibra óptica dedicada y diversificada en el trazado de manera que existen dos caminos alternativos e independientes (en el trayecto) con tecnología WDM. En cada extremo del enlace se colocarán dos equipos receptores (del mismo modo que en los accesos de la red VPN MPLS) para eliminar el punto de fallo por equipamiento. El equipamiento elegido en este caso es el multiplexor CMUX-4 de Fibernet [21], cuyas características aparecen en la Tabla 11. Ha sido seleccionado frente a equipamiento de otros fabricantes porque es el que actualmente ofrece el proveedor de comunicaciones de manera más ventajosa para el cliente final. Este equipo cuenta con 4 entradas, necesarias para los canales a transportar que han sido definidos para la solución, aunque en condiciones normales solamente se van a utilizar dos.

Características	Vista frontal y trasera
Dimensiones: 43,28 x 4,36 x 23 cm	
4 canales bidireccionales ITU-T G.694.2 sobre una única fibra	
Redundancia de fuentes de alimentación y módulos de ventilación	
Distancias de 120 km sin amplificar ni regenerar	
Gestión y monitorización vía SNMP	
Modulable y escalable	

Tabla 11. Características CMUX-4

En cada una de las sedes se provisionará un equipo de supervisión de tecnología xDSL, modelo Cisco 887, cuyas características aparecen en la Tabla 14, que se conectarán a cada uno de los multiplexores para su monitorización.

3.3.2 Equipamiento sedes Tipo I

Las sedes Tipo I cuentan con dos accesos diferenciados, un acceso de fibra óptica y un acceso mediante tecnología xDSL, con equipos diferenciados.

El proveedor de comunicaciones dispone de un catálogo de equipamiento en el que para cada fabricante valida los equipos que pueden ser usados en función de la tecnología y velocidad del acceso, así como del servicio para el que se va a utilizar.

Características	Vista frontal y trasera
Dimensiones: 4.4 x 32.5 x 24.9 cm	
Peso: 2.5 Kg	
Fuente de alimentación integrada tipo AC	
Switch de 8 puertos 10/100/1000	
1 puerto GigabitEthernet 10/100/1000BASET	
Puerto consola y USB	
Licencia Advance IP Services	
Cable Ethernet RJ45	
Temperatura funcionamiento 0-40 °c	
Memoria DRAM 512 MB	
Memoria FLASH 256 MB	

Tabla 12. Características Cisco 892FSP

Para el acceso principal, en la Tabla 9, aparecen todos los equipos de Cisco que el proveedor oferta para una conexión de fibra óptica y la velocidad máxima para el que se aconseja. Aparecen ordenados de menor a mayor precio. Además se ha añadido el caudal máximo que soporta si se utilizase ese equipo como segundo nivel del acceso de fibra para proporcionar salida a Internet.

Como se ha decidido provisionar un acceso de 100 Mbps, se descartan aquellos que el proveedor aconseja solamente para accesos de hasta 10 Mbps y se elige el modelo Cisco 892FSP-K9 [22] cuyas características aparecen en la Tabla 12 sobre los otros que cumplen las necesidades de la conexión pues que se trata del modelo más económico entre ellos.

Modelo	xDSL
CISCO881-K9-[Cisco 881-K9]	Válido
CISCO887-VA-M-K9-[CISCO887-VA-M-K9]	Válido
CISCO892FSP-K9-[C892FSP-K9]	Válido
CISCO1921/K9-[Cisco 1921/K9]	Válido
CISCO2901/K9-[Cisco 2901/K9]	Válido
CISCO2951/K9-[Cisco 2951/K9]	Válido
CISCO3925/K9-[Cisco 3925/K9]	Válido
WS-C3560V2[Catalyst 3560V2]	No válido
ASR1001-[Cisco ASR1001]	No válido

Tabla 13. Equipamiento Cisco válido para accesos xDSL

Para el acceso de respaldo, en la Tabla 13, aparecen todos los modelos de Cisco que el proveedor ofrece, indicando si son aptos o no para ser utilizados como equipamiento para un acceso xDSL.

Vuelve a primar el aspecto económico para la elección del equipamiento de la conexión XDSL y se elige la serie 800 que se trata de los modelos más baratos. Entre los equipos de la serie 800 que hay disponibles se ha elegido el *router* CISCO887-VA-M-K9 [23] ya que es el modelo que el propio fabricante aconseja como óptimo para soportar los diferentes modos de xDSL. Las características de este equipo aparecen en la Tabla 14. En la solución de red planteada, debido a la ubicación de las diferentes sedes, el proveedor de comunicaciones proporciona diferentes tipos de acceso xDSL, por lo que con este modelo de equipo nos aseguramos que soporta la sincronización con todas las modalidades (ADSL, ADSL2+, VDSL) y concentradores (ATM, IP).

Características	Vista frontal y trasera
Dimensiones: 4.8 x 32.5 x 24.9 cm	
Peso (maximo): 2.5 Kg	
Fuente de alimentación integrada tipo AC	
Switch de 4 puertos 10/100 Mbps FastEthernet	
Licencia Advance IP Services (necesario para BGP)	
Firmware para Multimode DSL	
Cable Ethernet RJ45	
Temperatura funcionamiento 0-40 °c	
Memoria DRAM 256 MB	
Memoria FLASH 128 MB	
Antena 3G (En equipos de sedes pequeñas)	

Tabla 14. Características Cisco C887VA

3.3.3 Equipamiento sedes Tipo II

Las sedes Tipo II cuentan con doble acceso diferenciado en un único equipo, como acceso principal un tipo de xDSL y como respaldo una conexión móvil 3G. Como contamos con diferentes tipos de acceso XDSL se volverá a utilizar el modelo usado en las sedes Tipo I como respaldo, el router CISCO887-VA-M-K9, cuyas características se detallaron anteriormente en la Tabla 14, añadiendo una antena Teldat 3Ge-HSUPA externa [24] donde se colocará la tarjeta SIM que proporcionará la conexión móvil, cuyas características aparecen en la Tabla 15. Esta antena se conectara a uno de los puertos *FastEthernet* con los que cuenta el equipo y podrá moverse para obtener mejores valores de cobertura en caso necesario.

Características	Vista frontal y trasera
Dimensiones: 14.2 x 16 x 3 cm	
Peso: 0.45 Kg	
Fuente Externa de alimentación	
Un latiguillo 2m RJ-45 para la LAN	
2 antenas acodadas	
Tarjeta SIM del servicio	
Temperatura de funcionamiento: 30ºC a 75ºC	

Tabla 15. Características antena 3G externa

3.4 Redundancia entre el equipamiento de una sede

Con la solución desarrollada, se ha permitido a cada sede contar con redundancia en la conexión en caso de fallo del acceso principal. En función de si la sede cuenta con equipamiento redundado o equipo único, esta redundancia se realizará de diferente manera.

3.4.1 Redundancia con equipos diferenciados

Cuando la sede tiene equipos diferenciados para cada uno de sus accesos (en la sede central y sedes Tipo I) la redundancia se realizará automáticamente. Para ello, como el equipamiento utilizado es Cisco, se prefiere utilizar el protocolo HSRP en lugar de VRRP, ya que es totalmente equivalente y el fabricante ofrece mejor soporte.

Para configurar HSRP entre ambos equipos, se define en el equipo que queremos que actúe como principal una prioridad mayor que el equipo de respaldo. El equipo principal realiza una comprobación de ocurrencia de un evento predeterminado (*track*), y en caso de no producirse, éste decrementará su prioridad pasando a una menor que el equipo de respaldo, que se convertirá en el equipo activo, tal como se muestra en la Figura 20, donde se ejemplifica como sería la redundancia entre los dos equipos de la sede Madrid III. Cuando el evento vuelva a producirse, recuperará la prioridad preconfigurada y volverá a ser el equipo activo. Para abarcar tanto la caída física del equipo o puerto como la incomunicación de red se definirá la recepción de una red global del proveedor de

comunicaciones. Si el equipo principal deja de recibir esa ruta, su prioridad se decrementará por debajo de la prioridad del equipo pasivo y pasará a ser el activo.

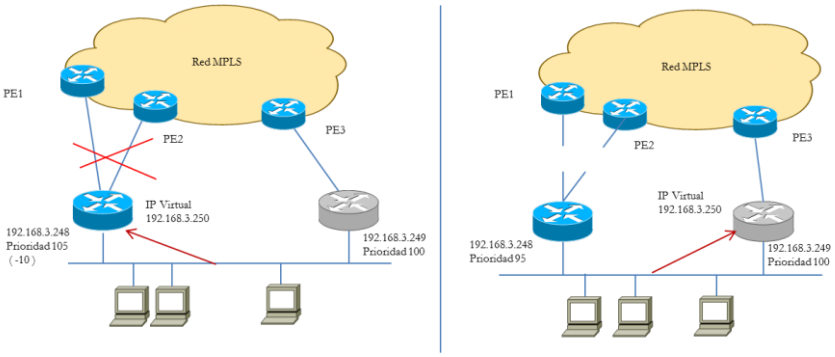

Figura 20. Funcionamiento respaldo en la sede Madrid III

A nivel LAN, los equipos de la sede apuntarán como ruta por defecto a la IP virtual dentro del rango de red de su sede, y así que el cambio de equipo en caso de incomunicación del router principal será transparente. Es necesario que el equipo principal y el equipo de respaldo tengan visibilidad entre ellos para el correcto funcionamiento del protocolo.

Del mismo modo que en el caso de la conexión de fibra óptica, los equipos de segundo nivel para la salida a Internet también estarán redundados mediante HSRP, por tratarse de equipamiento Cisco. Cada uno de los equipos contará con una IP del rango público asignado, y se definirá un grupo HSRP con otra IP pública.

Los accesos de respaldo de la sede central (de fibra óptica) y en las sedes Tipo I (con tecnología xDSL), se encuentran activos en todo momento, pero cuentan con una penalización en sus anuncios para que solamente se prefieran en caso de que el acceso principal no esté operativo.

3.4.2 Redundancia con único equipo

Cuando la sede cuenta con un único equipo para los dos accesos (en las sedes Tipo II) el acceso de respaldo móvil se activa únicamente cuando el acceso principal se cae. Para ello se define un *event manager* que, al caer el interfaz ATM de la conexión xDSL, levanta automáticamente el interfaz virtual de la conexión móvil y comienza a cursar el tráfico por esa conexión, tal como se muestra en la Figura 21.

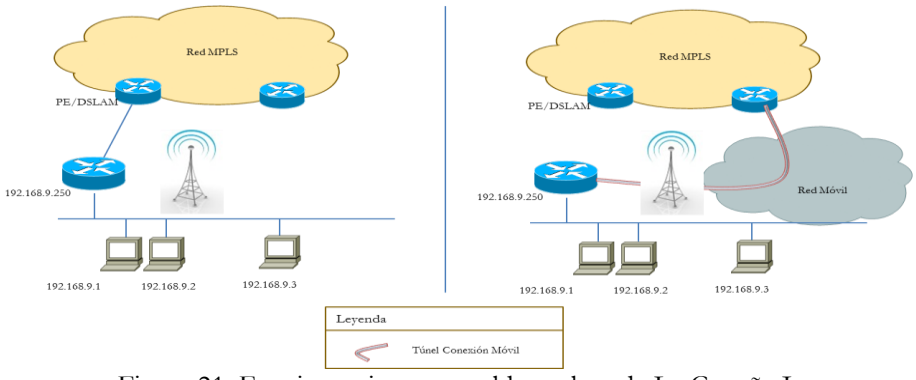

Figura 21. Funcionamiento respaldo en la sede La Coruña I

Una vez se reestablezca la conexión xDSL, se producirá el proceso contrario y el interfaz virtual pasará a estar caído hasta la siguiente incidencia.

El acceso de respaldo de las sedes Tipo II, mediante antena 3G, al contrario que los respaldos de fibra óptica y xDSL, se encuentran en *stand-by* hasta que una caída del acceso principal lo activa.

Capítulo 4. Gestión de la red privada virtual

Uno de los aspectos más importantes en los que la empresa ha incidido para el diseño de la red es el desembolso económico a realizar, sin ver reducidas las prestaciones que se han determinado como necesarias para sus trabajadores. Partiendo de una estimación proporcionada por el cliente se ha definido los caudales de cada una de las sedes para cubrir las necesidades de sus empleados, si bien puede ser necesarios modificar estos caudales ya sea por la variación del número de trabajadores de la sede, la implantación de nuevas aplicaciones o el uso que cada sede realiza de los recursos disponibles.

Por lo tanto se va a proporcionar una herramienta de monitorización basada en el protocolo SNMP para que el cliente disponga de la mayor información posible del uso de los recursos de su red, que le aporten una visión detallada y precisa de la utilización que cada una de las sedes realiza. De forma que sea posible determinar si los caudales contratados en cada sede se ajustan al ancho de banda utilizado o si se realiza una correcta utilización de los recursos por parte de sus empleados.

Para poder utilizar una de estas herramientas, es necesaria implantarla en una máquina del cliente que tenga conectividad con todos los *routers* y *switches* que componen la red, siendo posible posteriormente visualizarla desde cualquier punto de ella, accediendo mediante un navegador web a la dirección donde se encuentra alojado.

La herramienta de monitorización realiza consultas SNMP al *router/switch* del que se quiere obtener información, el cual contestará con el dato requerido. Contamos con varias opciones para identificar de manera unívoca cada máquina, definiendo una interfaz *loopback* con una IP *host* o utilizando la IP LAN que cuenta el equipo. Para facilitar el uso al cliente y no añadir más datos, se ha preferido utilizar la IP LAN física de cada equipo. En aquellas sedes que cuentan con doble equipo, se utilizará también el direccionamiento físico frente a la IP virtual definida por el protocolo HSRP que tendrá el equipo activo, puesto que de esta manera conoceremos en todo momento información de estado de cada uno de los equipos, sea activo o pasivo, mientras que en caso de utilizar la IP virtual lo tendríamos únicamente del equipo activo.

4.1 Elección de la herramienta de monitorización

Existen un gran número de herramientas para monitorizar redes con diferentes funcionalidades y apariencias. Para la elección de la herramienta de gestión de red que se va a implementar se ha optado por aquellas de código libre que no requieren el pago de licencia para su utilización, y que además el cliente final pueda utilizar de manera intuitiva.

Se han pre-seleccionado dos de ellas, y tras su estudio determinaremos cual resulta más útil en este proyecto.

Cacti® [25] es una herramienta de monitorización, basada en el mecanismo petición-respuesta SNMP, que permite la visualización gráfica del estado de los elementos de la red (ancho de banda, errores, consumo de CPU, memoria…) a través de un navegador web. Utiliza la herramienta RRDTools, que captura los datos mediante *Multi Router Traffic Grapher* (MRTG) y los almacena en una base de datos circular para mostrarlos posteriormente. Como realiza consultas al agente SNMP puede obtener información de todos los objetos OIDs definidos en la MIB del equipo gestionado.

El funcionamiento de la herramienta es sencillo: se definen todos aquellos *hosts* que se quieren monitorizar (denominados *devices*) y los parámetros a visualizar (*graphs)* de cada uno. Por cada *host* se crea una gráfica que muestra la evolución temporal de cada uno de los parámetros que se han determinado consultar. Para ayudar en la visualización de las gráficas, la aplicación permite agrupar los elementos ordenándolos de la manera que más interese con cabeceras y subniveles (por ejemplo mostrando las gráficas de los dos *routers* que componen una sede Tipo I) mediante *graphs tree* como los mostrados en la Figura 22.

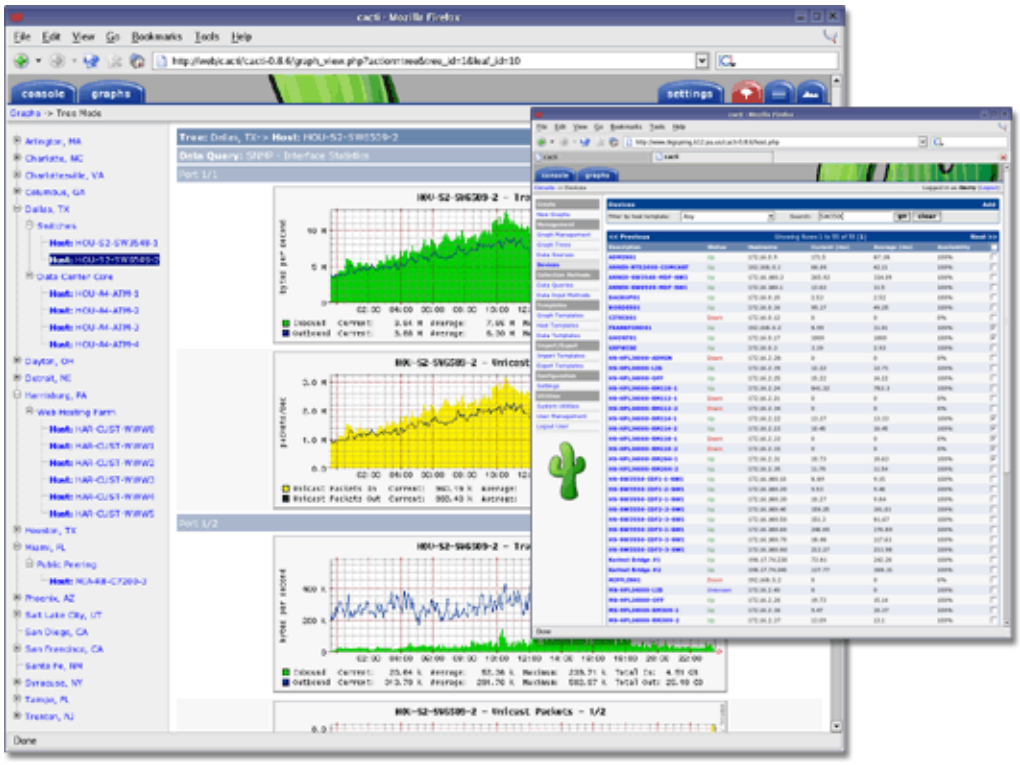

Figura 22. Visualización con Cacti de una red monitorizada [25]

De manera cíclica y en un periodo definido por el administrador (por defecto cada 5 minutos), se realiza una solicitud SNMP de cada uno de esos valores en cada *host* y se

almacenan en la base de datos. Cuando el espacio de la base de datos se completa, comienza a sobrescribir los valores más antiguos. Si el periodo de muestreo es más pequeño, la cantidad de datos aumentará y la resolución de la gráfica será mejor, pero aumentará la carga del sistema.

La herramienta Cacti permite personalizar completamente los parámetros y variables a visualizar y adicionalmente cuenta con unos *plugins* que aumentan las capacidades de análisis de la red.

Nagios® [26] es otra herramienta de monitorización de red basada en el mecanismo petición-respuesta SNMP que permite conocer el estado de las máquinas que se gestionan. La implementación de esta herramienta se realiza mediante un lenguaje de programación muy similar a C y define cada máquina monitorizada como un *host*. La agrupación y orden que se le puede dar a la posterior visualización es muy flexible, lo que permite ajustar a las necesidades del usuario final los subconjuntos de máquinas que se gestionen. Por ejemplo podríamos agrupar todos las sedes Tipo II en un mismo conjunto (la herramienta lo denomina *group*) para realizar comprobaciones del tasa binaria al cual el equipo se encuentra sincronizado.

Nagios permite crear las comprobaciones que más nos interesen de las maquinas monitorizadas de manera que tengamos para cada host o agrupación de hosts las consultas SNMP concretas. La herramienta define cada consulta SNMP a realizar como service. En ella se define el OID del parámetro que necesitamos obtener y por el cual la maquina nos devolverá el valor correspondiente a él. Se trata de una herramienta basada en código fuente y cuando se realizan cambios en ella debe volver a compilarse.

La pantalla de visualización de la herramienta muestra, cómo podemos observar en la Figura 23, en una parte el estado de todos los elementos monitorizados, separándolos si se encuentran en estado ok, down o unreacheable y por otro los services definidos que pueden estar ok, warning, critical o unknown.

Las consultas se realizan de manera cíclica. En el peor de los casos, si existe algún valor anómalo en las consultas que realiza, lo mostrará como máximo en el tiempo que tarde en volver a comprobar el estado del host que lo causa.

Con la información del *host* que nos muestra es posible observar el estado de todos máquinas monitorizadas conociendo aquellas que no responde y aparecerán como *down*. Si existe una máquina que cuelgue como segundo nivel de una que esta caída aparecerá en estado *unreacheable*. Con la información de los *services* la herramienta nos informa si la consulta SNMP que hemos definido devuelve un valor correcto (*ok),* da un valor anómalo (según el valor de severidad definido aparece como *warning* o *critical)* o el valor devuelto es erróneo o nulo (aparece un *unknown).* En ambos casos, cuando se introduce una maquina o consulta SNMP nueva y hasta que realiza la primera comprobación, aparecerá en la pantalla principal en estado *pending*.

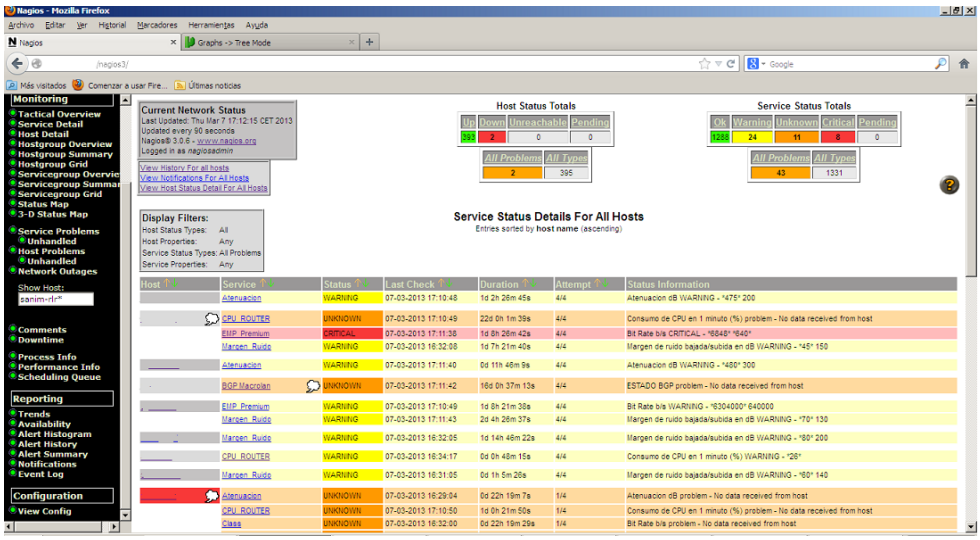

Figura 23. Visualización de Nagios sobre una red monitorizada

La herramienta permite además obtener informes de disponibilidad de los *hosts* o agrupaciones de *hosts* en periodos concretos que se soliciten, así como informar mediante correo electrónico de aquellas consultas que se deseen.

Tras utilizar estas herramientas en otros proyectos y conocer los requerimientos y necesidades que se especifican en éste se ha optado por implementar Cacti frente a Nagios por las siguientes razones:

- Interfaz gráfica más intuitiva y manejable.

- Posibilidad de realizar modificaciones en los elementos a monitorizar sin necesidad de volver a compilar el código.

- Facilidad de implementar nuevas consultas sin unos conocimientos elevados por parte del usuario final.

- Posibilidad de visualizar gráficamente un histórico de consultas en los periodos concretos.

- Posibilidad de visualizar un determinado parámetro en tiempo real sin necesidad de refrescarlo manualmente.

4.2 Parámetros monitorizados

Para este proyecto se va a implementar la monitorización de red mediante la herramienta Cacti en intervalos de un minuto para obtener información más precisa de los parámetros consultados.

Además de las funcionalidades que la herramienta cuenta por defecto, se van a incluir los siguientes *plugins* que nos servirán de gran utilidad para el seguimiento y supervisión de la red:

- *Real Time*

Este *plugin* permite observar la evolución de un parámetro monitorizado en tiempo real mostrando los valores obtenidos repitiendo la consulta en el intervalo de tiempo que se desee (como máximo cada 5 segundos) como se puede ver en la Figura 24.

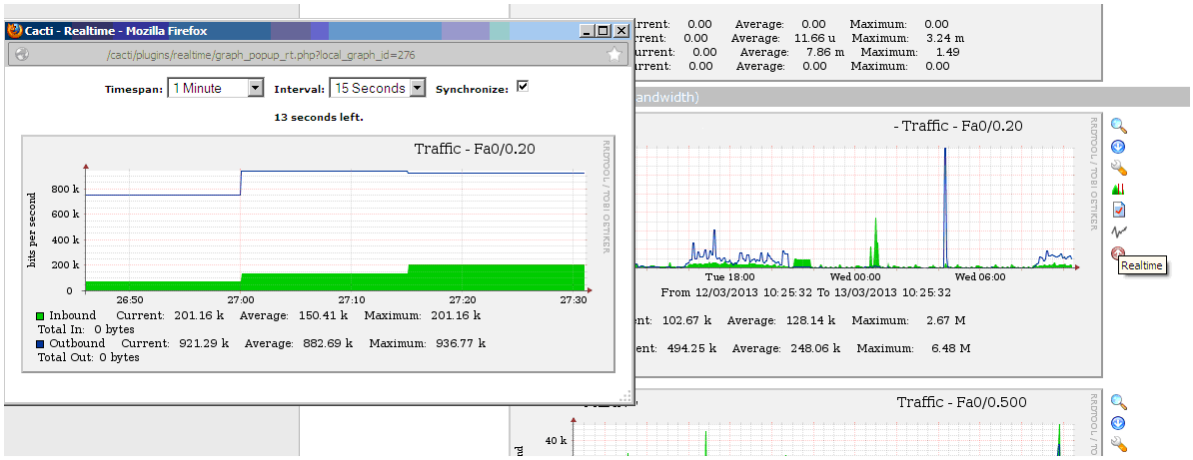

Figura 24. Funcionalidad del *plugin real time* de Cacti sobre una gráfica

-*Thold*

Este *plugin* permite definir umbrales para un determinado parámetro monitorizado y mostrar alertas si sobrepasan los rangos definidos. Además da la posibilidad de enviar correos informativos con la ocurrencia del parámetro en estudio. En la herramienta aparecerá una pestaña adicional en la que aparecerán todos los *tholds* definidos y en la parte superior aquellos que han generado una alerta como podemos observar en la Figura 25.

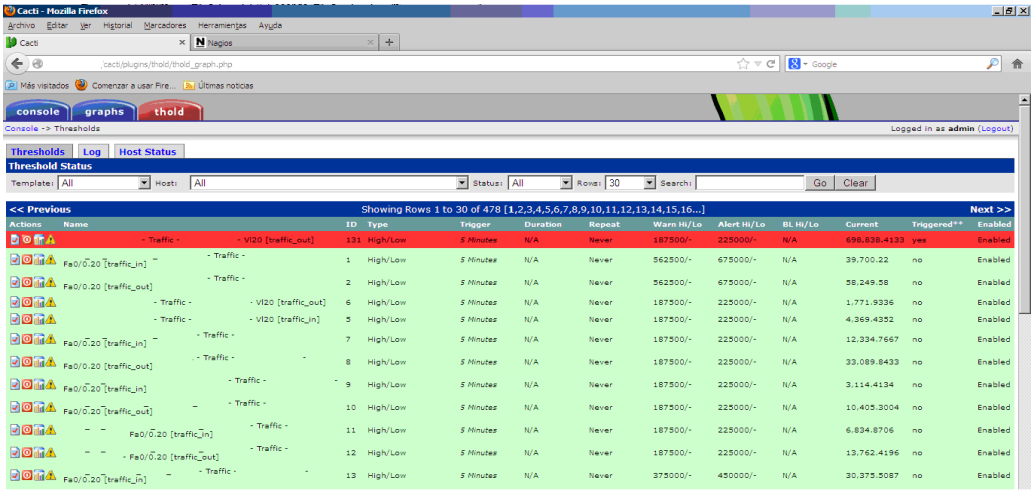

Figura 25. Funcionalidad thold sobre una red en funcionamiento

En este proyecto se va a implementar en primera instancia la monitorización de la red en intervalos de un minuto de los siguientes parámetros:

- Tráfico por puerto

Para cada uno de los *routers* y *switches* con lo que cuentan los accesos a la red VPN MPLS se va a graficar el ancho de banda utilizado, mostrado en la Figura 26, tanto en el puerto/interfaz WAN (conexión CE-PE) como en su parte LAN(conexión CE-red interna de la sede). La herramienta nos permite realizar un zoom de una zona concreta para obtener una visualización más detallada del intervalo que pueda interesarnos.

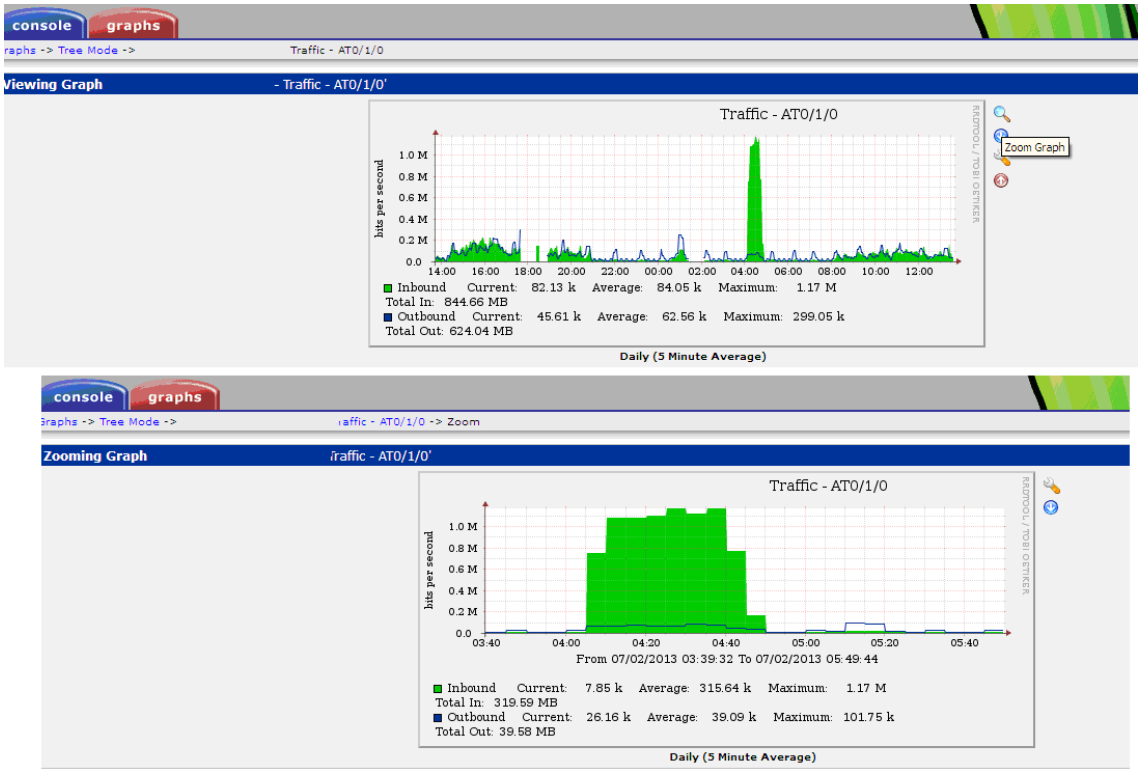

Figura 26. Grafica de ancho de banda de conexión PE-CE en un acceso xDSL

- Errores y descartes por puerto.

Del mismo modo que para el tráfico, se crearán gráficas de los errores y descartes producidos en los puertos definidos anteriormente.

Con estas dos gráficas se podrá visualizar el ancho de banda que se está utilizando por franja horaria y los posibles errores y descartes que se han podido producir. Si fuese necesario observar un determinado gráfico a tiempo real, se utilizará el *plugin real time* que se ha implementado como se ha detallado anteriormente en la Figura 24.

-Consumo de CPU

Se creará una gráfica con el porcentaje de consumo de CPU de las maquinas monitorizadas como en el ejemplo de la Figura 27.

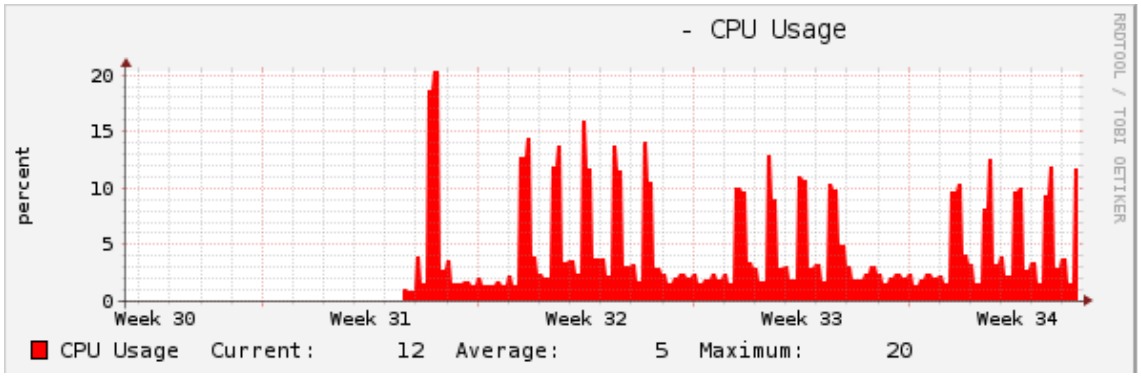

Figura 27. Consumo de CPU de una maquina monitorizada en intervalo semanal

Para ayudar a la empresa a saber cuáles de sus máquinas no tienen un rendimiento adecuado ya sea por exceso de tráfico o consumo de recursos, se utilizará el *plugin thold* para que genere una alarma en caso de acercarse al caudal contratado en cada sede. Se implementará una primera alarma cuando el tráfico generado supere el 70% del total contratado (que la herramienta denomina *warning)* y otra cuando éste sobrepase el 90% del total (denominada *alert*). En ambos casos, se informará vía correo electrónico a los responsables que el cliente indique para su posterior estudio. Este informe adjunta una gráfica del parámetro que ha producido la alarma con la información de la sede en cuestión, horario de la ocurrencia y una gráfica de las 24 horas anteriores al aviso como se puede observar en la Figura 28. Cuando el valor deja de estar fuera del rango que se ha definido en esta alarma, se volverá a recibir un correo informando de ello.

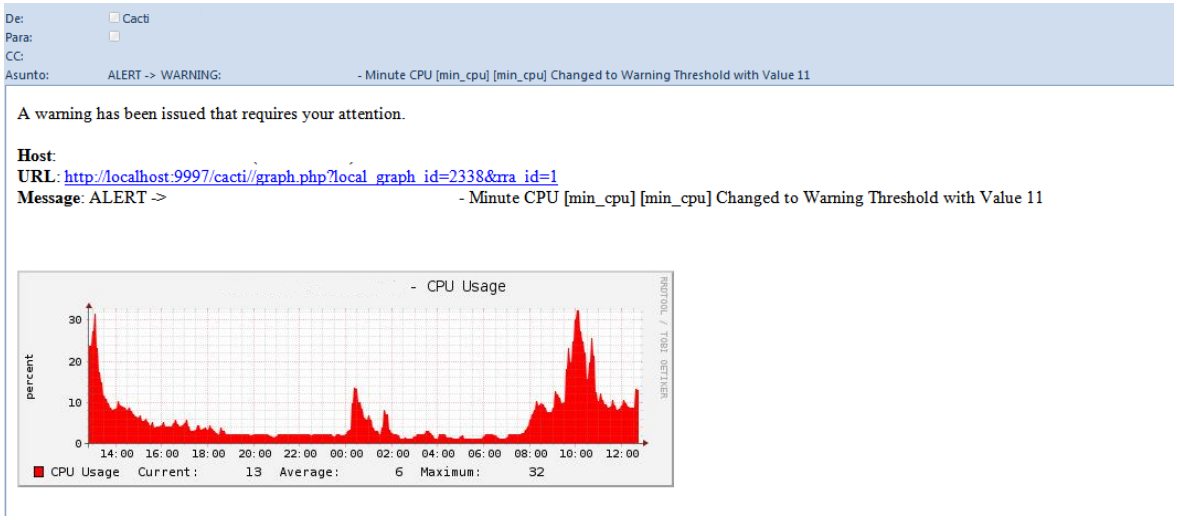

Figura 28. Correo recibido tras la ocurrencia de un exceso de tráfico en una sede monitorizada

Del mismo modo se creará una alarma cuando el consumo de CPU de la maquina supere el 50% del máximo. Estos valores pueden ser modificados en caso de necesidades posteriores, ya sea por ampliaciones de los caudales predefinidos o peticiones del cliente.

Igualmente como el usuario final va a poder acceder a la visualización gráfica de todas las sedes de la red VPN MPLS que la forman, podrá visualizar un parámetro en la fecha que le interese posteriormente y un log de los últimos 30 días con todas las alarmas que se han producido.

- Ventiladores

Dado que una temperatura elevada puede afectar al rendimiento de un *router*, obtener información de que un ventilador se ha averiado, permite anticiparse a posibles problemas que posteriormente pueda ocasionar. Un mal funcionamiento de un ventilador puede ser causado por la falta de ventilación suficiente en el rack donde se encuentre alojado el equipo.
La consulta SNMP que se realiza devuelve un valor numérico. Si este valor es 1, el ventilador funciona correctamente, por el contrario, si el valor devuelto es 2,3 o 4, el ventilador tiene alguna incidencia. Se definirá un *thold* que genere una alarma en caso de que el valor devuelvo sea distinto a 1 y la notifique por correo.

- Estado HSRP entre sedes con doble equipamiento

En aquellas sedes que cuentan con doble equipamiento en sus accesos, el cliente puede comprobar cuál de ellos está siendo utilizado realizando la consulta sobre el estado del protocolo HSRP ya que el tráfico es enrutado a la IP virtual y el *router* al que lo envía es transparente para el usuario final. La consulta devuelve un valor numérico. En caso de ser el equipo activo, devolverá un 5 y si se trata del equipo de respaldo un 6. Aunque el servicio se presta correctamente con ambos accesos, el de respaldo es degradado respecto del acceso principal y puede ser la causa de que el usuario final pueda notar un funcionamiento más lento.

4.3 Gestión de red del grupo especializado del proveedor de comunicación

Adicionalmente a la herramienta de monitorización de red que se implementará en la red VPN MPLS diseñada para esta empresa, el proveedor de comunicaciones cuenta con un grupo encargar de la gestión y mantenimiento de toda la infraestructura que ha sido provisionada al cliente. Para conocer las posibles incidencias producidas en los accesos y equipamiento del cliente se definen una interfaz *loopback* con una IP tipo *host* a la que se accede remotamente desde los centros de supervisión del proveedor. Además de contar con las herramientas Cacti y Nagios, también disponen de otra herramienta adicional que informa de las ocurrencias en las redes gestionadas.

IBM Netcool es una herramienta basada en el envío automático de *traps* que permite informar al administrador de la ocurrencia de un evento en los hosts monitorizados mediante una alarma, como puede ser por ejemplo, la perdida de conectividad o la caída de un interfaz físico/lógico. La interfaz gráfica muestra la información de los eventos ocurridos, agrupados en colores, según su criticidad como se puede ver en el ejemplo de la Figura 29.

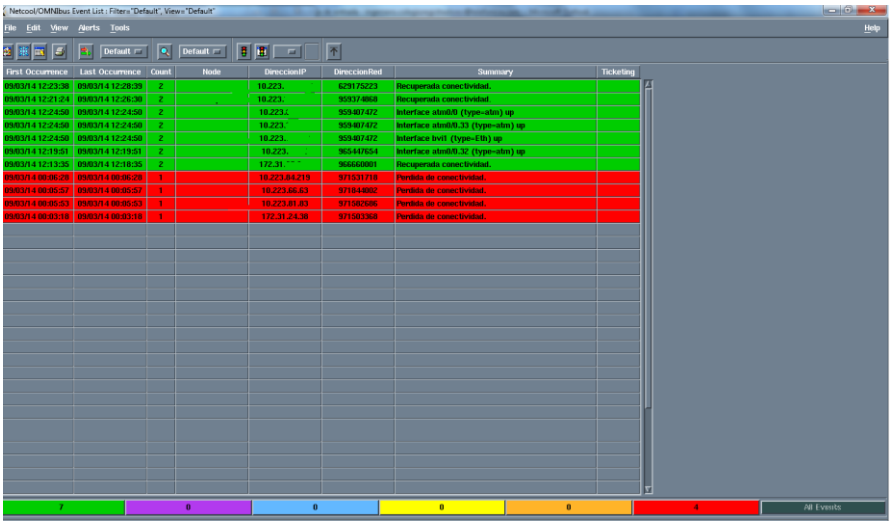

Figura 29. Visualización de IBM Netcool sobre red monitorizada

Capítulo 5. Presupuesto y planificación

Se realiza ahora una estimación económica de la implantación de la solución de red propuesta en este proyecto, en el que se han considerado la provisión de los accesos para cada una de las sedes, caudales y equipamientos, la realización del proyecto técnico y seguimiento de puesta en servicio, así como los gastos indirectos asociados a cada una de estas tareas.

El tiempo estimado para el despliegue del proyecto desde el diseño y tramitación hasta la provisión y puesta en funcionamiento es de cuatro meses, detallados en el diagrama de Gantt de la Figura 30.

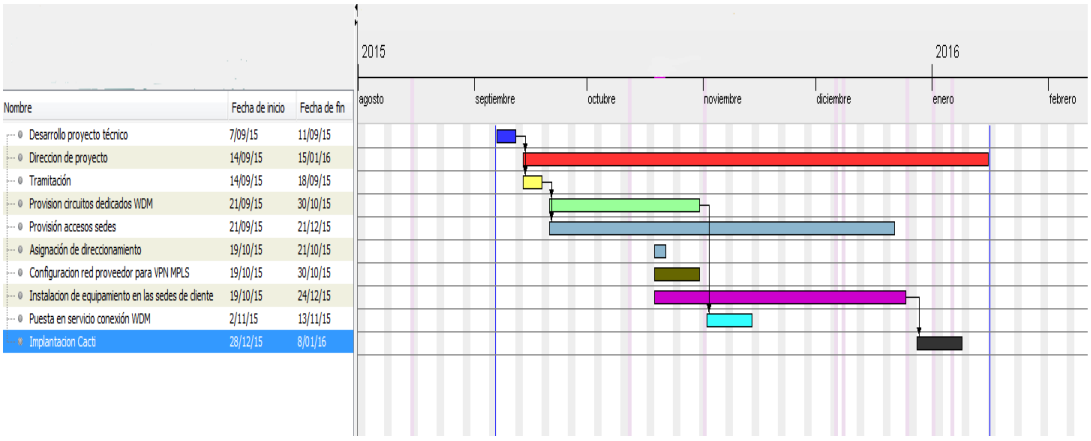

Figura 30. Diagrama de Gantt del proyecto

El presupuesto realizado contempla todas aquellas sedes y caudales con la que cuenta el cliente en el momento de la realización de este proyecto, si bien el acuerdo contempla la posibilidad de añadir o eliminar sedes y variar los caudales de cada una de ellas según las necesidades futuras del cliente. Estas modificaciones variarán el coste total del proyecto.

5.1 Accesos y equipamientos

El proveedor de comunicaciones ofrece los accesos a la red MPLS para empresas mediante el pago de una cuota mensual, sin coste de alta, con un acuerdo válido para cuatro o más años. En esta oferta ya está incluida la conexión desde el punto de acceso a la red hasta la sede de cliente (sobre canalizaciones ya desplegadas), la configuración del equipamiento de cada uno de los accesos, así como posteriormente la gestión y mantenimiento de los mismos.

Dado que las sedes de esta empresa están ubicadas en zonas urbanas de grandes ciudades, el proveedor de comunicaciones ya tiene desplegadas canalizaciones de fibra óptica y cobre, por lo que se han utilizado tecnologías de acceso compatibles con los recursos con los que cuenta el proveedor, no siendo necesario realizar nuevas infraestructuras con obra civil que incrementen el coste de los accesos.

Los accesos de fibra óptica deben contar con un caudal máximo asociado, y los accesos mediante tecnología xDSL llevan asociados el coste del alquiler de la línea telefónica.

En el caso de la fibra dedicada, el proveedor ofrece el servicio cobrando como alta el coste del cableado necesario, la acometida desde la central de comunicaciones más cercana, así como la necesidad de obra externa a realizar (en el caso de estudio este último punto no se ha tenido en cuenta puesto que no es necesario) y posteriormente una cuota mensual que cubre el alquiler del equipamiento y la gestión y supervisión de las conexiones.

Se van a desglosar los costes en función de los tipos de sede que se han determinado en el diseño del proyecto.

Sede principal y respaldo unidos con fibra dedicada WDM

La sede principal y su respaldo cuentan con dos accesos de fibra óptica idénticos con equipamiento diferenciado, y el servicio de salida a Internet asociado con un equipo adicional que cuelga de cada equipo de conexión a la red VPN MPLS. Tienen asociado con un caudal para el acceso a la red MPLS del cliente, un caudal específico para la salida a Internet y otro para la conexión con la otra entidad necesaria. En la Tabla 16 se detallan los costes y conceptos contemplados.

Concepto	Ud.
Acceso fibra óptica 100 Mbps	2
Despiece equipamiento	
Catalyst 3560v2	2
IOS 12.2(40)SE IP Services o versión posterior	2
Instalación, gestión y mantenimiento Catalyst 3560v2	2
Cisco 2951-K9	2
IOS 15.3.3M5 UNIVERSAL o versión posterior	2
Instalación, gestión y mantenimiento Cisco 2951-K9	2
Caudales	
Caudal Fibra óptica 30 Mb(400 €)	2
Caudal salida Internet 20 Mb (120€)	2
Caudal VRF adicional 1Mb (90€)	2
Alta 0,00 €	
Cuota Mensual 1800 €	

Tabla 16. Coste conexión sede principal a la red VPN MPLS

Ambas sedes se encuentran en ubicaciones diferentes y están unidas mediante dos líneas WDM independientes. La conexión punto a punto entre las dos sedes se realizada con una

fibra óptica dedicada y diversificada en el trazado. El proveedor de comunicaciones define como cuota de alta el coste de la acometida hasta la arqueta de entrada al edificio y el cableado de la conexión y posteriormente una cuota mensual por el equipamiento y supervisión del enlace, detallado en la Tabla 17.

Concepto	Ud.
Acometida Sede Principal - Central Proveedor (560 m)	1
Acometida Sede Backup - Central Proveedor (800 m)	1
Cableado WDM (12800 m)	1
Cuota única Alta 4200 €	
CMUX -4	4
Canales FiberChannel	2
Canales Gigabit Ethernet	2
Router Cisco 877 para supervisión	2
Instalación/ Puesta en marcha	1
Gestión, supervisión y mantenimiento 7*24	1
Cuota Mensual 980 €	

Tabla 17. Coste conexión WDM entre la sede principal y su respaldo

Sedes Tipo I

Las sedes Tipo I cuentan con dos accesos: fibra óptica y xDSL, con equipamiento diferenciado. En función del número de empleados, el caudal varía de una sede a otra, lo que conlleva distintos costes para cada sede. Según la distancia al DSLAM la capacidad será diferente, aunque el proveedor no aplicará variación de la cuota mensual y todos los respaldos se facturarán por el mismo precio. Si es posible mejorar el ancho de banda que ofrece la línea, también se modificará sin gasto adicional. Como costes comunes en todas las sedes se desglosa en la Tabla 18 los conceptos que se incluyen.

Concepto	Ud.
Acceso fibra óptica Tipo Principal 100 Mbps	1
Acceso xDSL Tipo Respaldo velocidad según sede	1
Alquiler línea telefónica (17 €)	1
Despiece router principal	
Cisco 892FSP-K9	1
IOS 15.2.4M5 UNIVERSAL o version posterior	1
Instalación, gestión y mantenimiento Cisco 892FSP-K9	1
Despiece router respaldo	
Cisco 887VA-M-K9	1
IOS 15.2.4M5 UNIVERSAL DATA o versión posterior	1
Instalación, gestión y mantenimiento 887VA-M-K9	1
Alta 0,00 €	
Cuota Mensual 420 €	

Tabla 18. Costes comunes sede Tipo I

Haciendo un cálculo global añadiendo el coste de cada caudal al total de las sedes Tipo I, obtenemos el coste económico mensual que le supone a la empresa las sedes de este tipo y aparece detallado en la Tabla 19.

Sede	Coste acceso (€)	Caudal asociado	Coste caudal (€)	Coste total sede (€)
Madrid III	420	2 Mb	110	530
Barcelona I	420	6 Mb	205	625
Valencia I	420	6 Mb	205	625
Sevilla I	420	5 Mb	180	600
Bilbao I	420	5 Mb	180	600
Zaragoza I	420	5 Mb	180	600
Valladolid I	420	5 Mb	180	600
Santiago I	420	3 Mb	125	545
León I	420	3 Mb	125	545
Toledo I	420	3 Mb	125	545
Barcelona II	420	3 Mb	125	545
Valencia II	420	3 Mb	125	545
Mallorca I	420	3 Mb	125	545
Las Palmas I	420	3 Mb	125	545
			Total	**7995**

Tabla 19. Coste mensual de las sedes Tipo I

Sedes Tipo II

Las sedes Tipo II también cuentan con dos accesos: xDSL y respaldo móvil 3G, pero en el mismo equipo. En función de las capacidades de cada una de las líneas, el proveedor de comunicaciones varía el coste mensual a pagar. Hay que añadirle además el pago del alquiler mensual de la línea telefónica necesario para el uso de la tecnología xDSL. En la Tabla 20 aparece reflejado el coste mensual de las sedes Tipo II que se han definido en el presente proyecto detallado por sede.

Sede	Bit Rate	Alquiler línea (€)	Coste xDSL (€)	Coste total sede (€)
La Coruña I	10 Mbps/640 Kbps	17	60	77
Vigo I	6 Mpbs/640 Kbps	17	50	67
Gijón I	8 Mbps/640 Kpbs	17	55	72
Salamanca I	8 Mbps/640 Kpbs	17	55	72
Badajoz I	6 Mpbs/640 Kbps	17	50	67
Sevilla II	20 Mbps/1 Mbps	17	70	87
Cadiz I	6 Mpbs/640 Kbps	17	50	67
Jaen I	8 Mbps/640 Kpbs	17	55	72
Motril I	8 Mbps/640 Kpbs	17	55	72
San Sebastian I	10 Mbps/640 Kbps	17	60	77
Pamplona I	10 Mbps/640 Kbps	17	60	77
Cuenca I	8 Mbps/640 Kpbs	17	55	72
Castellón I	10 Mbps/640 Kbps	17	60	77
Alicante I	10 Mbps/640 Kbps	17	60	77
Murcia I	4 Mbps/ 640 Kbps	17	40	57
Tenerife I	20 Mbps/1 Mbps	17	70	87
			Total	**1177**

Tabla 20. Coste mensual de las sedes Tipo II

5.2 Capital humano

Dentro del capital humano se ha considerado el coste del Jefe de Proyecto encargado del seguimiento de la implantación y del personal encargado del desarrollo del proyecto técnico detallado en la Tabla 21. El coste de la provisión y puesta en marcha de los accesos y equipamientos asociados a cada uno de ellos está repercutido en el coste de los propios equipos y no se ha considerado como capital humano.

Actividad	Recurso	Horas	Coste(€)
Desarrollo Proyecto Técnico	Ingeniero Superior	40 (1 semana, 8h/día)	3200
Dirección de proyecto	Ingeniero Técnico	320 (4 meses, 4h/día)	19200
		Total	**22400**

Tabla 21. Coste capital humano del proyecto

5.3 Costes indirectos (material)

Se han tenido en cuenta en este apartado los costes indirectos asociados al desarrollo del proyecto, líneas móviles de Jefe de Proyecto e Ingeniero de desarrollo, desplazamientos, reprografía y papelería detallados en la Tabla 22.

Concepto	Coste(€)
Telefonía	200
Gastos de locomoción	150
Reprografía	100
Papelería	50
Total	**500**

Tabla 22. Costes indirectos del proyecto

5.4 Coste total

El acuerdo con el proveedor de comunicaciones es por un periodo de cuatro años. Se abonará una cuota inicial al comienzo del proyecto y una vez provisionado una cuota mensual.

El proyecto requiere de un desembolso inicial que tiene que ser abonado tras la firma del acuerdo y que contempla los costes de alta asociados a los accesos, del capital humano implicado en el proyecto y todos los gastos indirectos agrupados en la Tabla 23.

Concepto	Coste (€)
Cuota alta accesos	4200
Capital humano	22400
Costes indirectos	500
Total	**27100**

Tabla 23. Coste inicial del proyecto

Una vez trascurrido los cuatro meses determinados para el despliegue del proyecto y siempre que al menos estén operativos el 75% de las sedes definidas en el proyecto se realizará el pago de una cuota mensual hasta la finalización del acuerdo. Esta cuota mensual podrá variar si se realizan modificaciones en el número de sedes y los caudales definidos en cada una de ellas. El coste mensual que se facturará tras el despliegue aparece detallado en la Tabla 24.

Concepto	Coste (€)
Sede central y respaldo	2780
Sedes Tipo I	7995
Sedes Tipo II	1177
Total	**11952**

Tabla 24. Coste mensual del proyecto

El coste inicial del proyecto es de **veintisiete mil cien** euros.

La cuota mensual proyecto es de **once mil novecientos cincuenta y dos** euros.

5.5 Alquiler frente a compra del equipamiento

Como se ha indicado anteriormente en el Capítulo 3, se ha preferido la opción de alquiler del equipamiento frente a la compra de éste por los siguientes aspectos:

- La oferta comercial del proveedor de comunicaciones promociona los costes de altas de los accesos para este equipamiento con la opción de alquiler.

- Desde el punto de vista económico:

- Se comienza a disfrutar del equipamiento sin realizar un desembolso inicial elevado.
- Se adapta mejor a la evolución tecnológica del equipamiento y a la de la propia empresa en un futuro.
- El *renting* lleva asociado una gestión integral del equipamiento con un pago mensual fijo, sin tener en consideración el gasto variable producido por averías y mantenimiento.

- Desde el punto de vista financiero y fiscal:

- Proporciona mayor liquidez para la empresa.
- Simplicidad en la gestión administrativa, agrupando todos los costes asociados al equipamiento en un solo pago.
- Al no ser de propiedad del cliente, evita controversias en la contabilidad de la amortización del equipamiento.

- Sobre la obsolescencia del equipamiento, permite la sustitución/renovación del equipamiento sin volver a realizar un desembolso elevado.

En cualquier caso, se va a realizar una comparativa entre las opciones de alquiler y compra del equipamiento y los accesos para cada una de las sedes del proyecto con los gastos asociados en cada una de las opciones. En esta comparativa no se han tenido en cuenta los costes comunes de ambas:

- Conexión WDM. Se trata de una conexión dedicada que el proveedor de comunicaciones oferta pagando una cuota de alta en función de la longitud del camino y un pago mensual del alquiler del equipamiento y su mantenimiento, no siendo posible su compra.

- Caudales accesos de fibra. El caudal de la conexión de fibra va asociado a la línea y el proveedor de comunicaciones lo oferta pagando una cuota mensual por el valor contratado tanto en el caso de que el equipamiento sea propiedad del cliente o sea alquilado.

- Línea de acceso. Al igual que con los caudales, el proveedor de comunicaciones cobra una cuota mensual por cada una de las líneas telefónicas de las conexiones xDSL.

Para la opción de compra del equipamiento, sería necesario contar con repuestos adicionales para utilizar en caso de necesidad y no tener que esperar al suministro por parte del fabricante. Se ha estimado un 40% más de cada modelo de equipamiento utilizado. Contar con equipos en propiedad requiere unos gastos adicionales de almacenamiento, mantenimiento, personal dedicado y transporte que se han estimado para este estudio como gastos adicionales y que en la opción de alquiler no se contemplan puesto que es un servicio añadido que ofrece el proveedor de comunicaciones en la opción de alquiler.

En la Tabla 25 se ha estimado el coste inicial para las opciones de compra y alquiler de los accesos y el equipamiento para cada una de las sedes que componen este proyecto.

	Nº Equipos alquiler	Nº Equipos compra	Coste Unitario Compra	Coste Alquiler	Coste Compra
Cisco Catalyst 3560	2	3	4.000 €	0 €	12.000 €
Cisco 2951	2	3	3.000 €	0 €	9.000 €
Cisco 892	14	20	1.500 €	0 €	30.000 €
Cisco 887	14	20	700 €	0 €	14.000 €
Cisco 887 + Antena	16	22	800 €	0 €	17.600 €
				0 €	**82.600 €**

	Numero de accesos	Coste Unitario Compra	Coste Alquiler	Coste Compra (+% adicional)
Acceso 100Mb	16 €	3.500 €	0 €	56.000 €
Acceso XDSL	30 €	1.500 €	0 €	45.000 €
Acceso Movil	16 €	50 €	0 €	800 €
			0 €	**101.800 €**

Tabla 25. Costes iniciales de accesos y equipamiento para cada opción

Para poder comparar cada una de las opciones en la Tabla 26 se ha estimado el coste mensual que conlleva cada una de las opciones. Como se ha indicado anteriormente en la opción de compra, se estima la necesidad de contar con dos personas (2000€/mensuales en

sueldo) y 1000€ adicionales que cubren el almacenamiento, mantenimiento y transporte del equipamiento de repuesto comprado.

	Alquiler Pago Mensual	Compra Pago Mensual
Sede central y respaldo	1.190 €	0 €
Sedes Tipo I	5.880 €	0 €
Sedes Tipo II	905 €	0 €
	7.975 €	**0 €**

	Alquiler Pago mensual	Compra Pago mensual
Materiales y recursos	0 €	4.000 €
Costes indirectos	0 €	1.000 €
	0 €	**5.000 €**

Tabla 26. Costes mensuales de accesos y equipamiento para cada opción

Una vez estimado los costes de cada uno de las opciones posibles, se ha realizado el cálculo global que supondría cada uno de ellos durante los cuatro años que contempla la opción de alquiler elegida en el proyecto, tal como refleja la Tabla 27, la opción de alquiler del equipamiento al proveedor de comunicaciones muestra un beneficio de **18080 €** sobre la compra en propiedad, además de suponer un desembolso económico inicial menor.

	Coste Inicial	Coste Mensual	Total 4 años
Alquiler	0	7.975 €	**382.800 €**
Compra	184.400 €	5.000 €	**424.400 €**

Tabla 27. Coste total para cada opción a cuatro años

Estas estimaciones están calculadas sobre la planta actual de sedes con las que cuenta la empresa, variando el beneficio si se añadieran nuevas sedes (el desembolso inicial en una sede Tipo I en la opción de compra de equipamiento es de 7200 euros frente al pago de 420 euros mensual de la opción de alquiler) y o eliminase alguna (se dejaría de pagar la cuota mensual).

Capítulo 6. Conclusiones y trabajos futuros

El objetivo de este Proyecto Fin de Carrera ha sido el diseño de una solución de red para un cliente ficticio denominado ACME S.A., de forma que le proporcione conectividad entre todas sus sedes, distribuidas geográficamente en todo el territorio nacional sin ocasionarle un alto desembolso económico. Esta red debía ser lo suficientemente escalable y flexible para permitir modificar el número de sedes que la componen así como los requerimientos de cada una de ellas.

La solución diseñada se ha basado en la utilización de una red VPN MPLS para interconectar las sedes que componen la empresa utilizando la infraestructura de red de datos del proveedor de comunicaciones, lo que permite aprovechar las ventajas de la misma (alta disponibilidad, gran capacidad, despliegue geográfica…) de manera transparente para el usuario y proporcionando una alta escalabilidad y flexibilidad a la red del cliente. Cuando se quiere añadir una nueva sede a la red VPN MPLS sólo es necesario provisionar el enlace entre la sede y el punto de acceso a la red que disponga el proveedor de comunicaciones, utilizando la tecnología de acceso que mejor convenga en cada caso y configurando el equipamiento de acceso. Si es necesario modificar los caudales de una sede sólo será necesario reconfigurar el punto de acceso red-sede sin tener que realizar ningún cambio en el resto de la red. Esta solución permite además contar con un punto de acceso a Internet centralizado para todas las sedes que componen la red.

Se ha buscado con el diseño realizado proporcionar también redundancia y alta disponibilidad a la red dentro del compromiso de coste de la solución. Todas las sedes cuentan con doble tecnología de acceso a la red y aquellas sedes calificadas como Tipo I tienen además equipamiento diferenciado para cada acceso, para limitar los puntos únicos de fallo posibles.

Además la provisión y el mantenimiento de la red se traslada al proveedor de comunicaciones, a través de un grupo especializado para la gestión de red proporcionando al cliente una supervisión constante de su red y una rápida actuación ante posibles incidencias.

Por último, y dada la preocupación mostrada por el cliente de optimizar los recursos con los que cuenta y ajustar el gasto, se han implantado unas herramientas de monitorización de la red gratuitas, para que en todo momento pueda tener una visión del uso de cada uno de los recursos con los que cuenta las sedes, y pueda anticiparse a las necesidades concretas de cada una, ya sea para ampliar los caudales definidos en una sede o para ajustar el exceso de

ancho de banda con los que cuenta, así como el rendimiento del equipamiento instalado en cada uno de ellas.

Como trabajo futuro para la ampliación del diseño de red creado, se podría integrar la telefonía a través de la red, sustituyendo la tradicional por VoIP. Para ello, se podría etiquetar el tráfico de voz con mayor prioridad que el tráfico de datos (QoS) y para la voz se definiría, tanto en el *router* como en red un caudal específico para que no tenga retardos y soporte un determinado número de llamadas simultáneas. La telefonía IP requeriría terminales específicos, que se colocarán entre el *router/switch* de la sede y el PC del usuario. En el *router* de la sede se definiría una nueva VLAN (o encapsulación) para el correcto etiquetado del tráfico de voz.

Otra posible línea de trabajo futuro sería la implantación de un servicio de Videoconferencia, de gran utilidad para formación y la comunicación de profesionales ubicados en diferentes sedes. Para ello se volvería a definir un tráfico específico para video, igualmente sensible al retardo, de manera que permita una conexión fluida y sin cortes, independiente de la utilización de recursos que está siendo utilizada en la sede. El servicio de Videoconferencia permite la opción de utilizarlo instalando software específico en herramientas de cliente (PC, tablets, móvil, salas de reuniones), así como la provisión y mantenimiento de todo el equipamiento preciso para ello.

Por último, como posible ampliación de la solución propuesta se contempla la provisión y gestión de puestos de trabajo para los empleados de la empresa y la dotación de puntos de acceso WiFi asociado a un equipo controlador que gestione el acceso de los usuarios y garantice la seguridad de los mismos. Dado que actualmente la empresa dispone de gestión de puesto de trabajo propio y a través de otro proveedor, se propondría la unificación de servicios de manera que toda la infraestructura sea mantenida por el mismo proveedor, lo que disminuiría tiempo de resolución de incidencias y simplificaría la comunicación con el usuario. Además seria de utilidad que las sedes contaran con acceso WIFI seguro a la red VPN MPLS para que posibles mediadores o clientes dispongan de conexión a Internet cuando se encuentre de visita en sus oficinas.

Capítulo 7. Bibliografía

[1] ADSL Forum. "System Reference Model". Mayo 1996.

[2] ITU G.992.5. Asymmetric digital subscriber line 2 transceivers (ADSL2) - Extended bandwidth ADSL2 (ADSL2plus). Enero 2009.

[3] ITU G.993.1. Very high speed digital subscriber line transceivers (VDSL). Junio 2004.

[4] ITU G.993.2. Very high speed digital subscriber line transceivers 2 (VDSL2). Diciembre 2012.

[5] ITU G.983.1. Broadband optical access systems based on Passive Optical Networks (PON). Enero 2005.

[6] ITU G.984.1. Gigabit-capable passive optical networks (GPON): General characteristics. Marzo 2008.

[7] E. Rosen, A. Viswanathan, R. Callon. Multiprotocol Label Switching Architecture. IETF RFC 3031. Enero 2001.

[8] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, LDP Specification. IETF RFC 3036. Enero 2001.

[9] F. Le Faucheur. Multi-Protocol Label Switching (MPLS).Support of Differentiated Services. IETF RFC 3270. Mayo 2002.

[10] R. Braden. Resource ReSerVation Protocol (RSVP). IETF RFC 2205. Septiembre 1997.

[11] Y. Rekhter, T. Li, and S. Hares. A Border Gateway Protocol 4 (BGP-4). IETF RFC 4271 (Draft Standard). Enero 2006.

[12] Roosevet Giles. All-in-one CCIE study guide. Second Edition Mc Graw Hill 1998. Marzo 2015.

[13] E. Rosen, Y. Rekhter. BGP/MPLS IP Virtual Private Networks (VPNs). IETF RFC 4364. Febrero 2006

[14] Cisco Systems. MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T [Mayo 2015]

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html

[15] Cisco Systems. MultiVRF. [Mayo 2015]
http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/vrflitsb.html

[16] J. Case. A Simple Network Management Protocol (SNMP). IETF RFC 1157. Mayo 1990.

[17] Cisco System. Configuring SNMP Support. [Mayo 2015]
http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html.

[18] S. Nadas, Ed. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. IETF RFC 5798. Marzo 2010.

[19] Cisco System. CISCO 3560V2. [Mayo 2015]
http://www.cisco.com/c/en/us/products/switches/catalyst-3560-series-switches/index.html

[20] Cisco System. CISCO 2951. [Mayo 2015]
http://www.cisco.com/c/en/us/products/routers/2951-integrated-services-router-isr/index.html

[21] Fibernet. FIBERNET CMUX-4. [Mayo 2015]
http://www.fibernet.es/es/index.php/productos/transporte/cwdm/cmux4

[22] Cisco System. CISCO 892. [Mayo 2015]
http://www.cisco.com/c/en/us/products/routers/892-integrated-services-router-isr/index.html

[23] Cisco System. CISCO 887. [Mayo 2015]
http://www.cisco.com/c/en/us/products/routers/887va-integrated-services-router-isr/index.html

[24] Teldat S.A. Habilitadores 3Ge - Tarjetas externas 3G WiFi. [Mayo 2015]
http://www.teldat.com/es/page.php?cnt_id=backup-para-routers-4G-3G

[25] Cacti. The complete RDDTools-Based graphing solution. [Mayo 2015]
http://www.cacti.net

[26] Nagios. The Industry Standard in IT Infrastructure Monitoring [Mayo 2015]
http://www.nagios.org/