La nueva red convergente del Ministerio de Justicia

Durante los últimos tres años, el Ministerio de Justicia ha experimentado un fuerte desarrollo tecnológico a raíz de la creación de una unidad tecnológica en los servicios centrales del Ministerio, denominada División de Informática y Tecnologías de la Información (en adelante DITI). A esta unidad se le asignaron las competencias de elaborar y ejecutar los planes informáticos y de tecnologías de la información y comunicaciones, así como la prestación de asistencia técnica a los distintos órganos del Ministerio.

POR LUIS RODRÍGUEZ VEGA

En lo que respecta a las infraestructuras de comunicaciones, el Ministerio contaba en ese momento con dos redes de voz y datos disjuntas, que prestaban servicio a un conjunto de sedes de mediano y gran tamaño situadas en Madrid. Cabe indicar aquí que estas redes son distintas de las que prestaban servicio, a nivel nacional, a las sedes de la Administración de Justicia. Las redes de la Administración de Justicia están caracterizadas por una problemática distinta y quedan fuera del ámbito de este artículo.

Las redes del Ministerio habían tenido en el pasado un crecimiento poco planificado, por lo que su estructura resultaba excesivamente compleja y adolecía de ciertas debilidades, debilidades que redundaban en unos costes de operación y gestión demasiado elevados para la organización. Por este motivo, se acometió la realización de un conjunto de proyectos de mejora, orientados en base a tres ejes principales:

* Reducción de costes: costes de operación y gestión de la red, reducción de la facturación de telefonía y datos emitida por los operadores, etc.

* Mejora de los niveles de servicio, maximizando la disponibilidad de los servicios ofrecidos por la red y el tiempo medio entre fallos (TMEF) para las diferentes líneas de voz, datos y servicios en conjunto.

* Aumento del número de servicios ofrecidos por la red corporativa.

La meta última de esos proyectos de mejora era la realización de una transición suave entre la situación de partida – redes heterogéneas, con baja redundancia en los servicios y con una solución de telefonía tradicional de elevado coste – y la situación deseada de una auténtica red corporativa multiservicio, con elevada disponibilidad, integración de todos los servicios de voz y datos y facilidad de gestión.

Antecedentes y situación de partida

A principios del año 2005, las redes de voz y datos del Ministerio daban servicio a un conjunto de ocho sedes distintas, situadas en Madrid, que contaban con unos mil cuatrocientos usuarios.

El servicio de voz estaba proporcionado mediante una solución de telefonía tradicional, tal y como se muestra en la *Figura 1*.

En la figura se pueden observar los elementos principales que constituyen la solución tecnológica de voz. Por un lado, cada sede del Ministerio está conectada a la red pública de telefonía a través de enlaces primarios RDSI (en adelante, PRI). Estos enlaces garantizan la accesibilidad de cada sede desde la red pública, siendo además el único camino existente para realizar llamadas entre la mayoría de las sedes.

Adicionalmente, existe una conectividad parcial mediante enlaces privados QSig (tendidos sobre fibra óptica propiedad del Ministerio) entre las cuatro sedes de la Calle San Bernardo. La tecnología de centralitas utilizada – *Nortel Meridian* OP11C y OP61C – permite aprovechar estos enlaces QSig para integrar las cuatro centralita, de manera que operen como una única. De esta manera, se facilita la movilidad de usuarios entre sedes, y se permite la configuración de ciertas soluciones de redundancia de tráfico, si bien estas soluciones son limitadas y únicamente permiten garantizar cierta resistencia ante fallos para el tráfico saliente.

Por último existe un sistema de telefonía móvil corporativa que da servicio a unas doscientas extensiones móviles cuya numeración está integrada en el plan de numeración privado del Ministerio.

Tras la realización de un análisis detallado, se identificaron las áreas en las que existían necesidades de mejora:

* *Infraestructuras de voz:* La planta de voz en servicio está compuesta en su totalidad por terminales tradicionales, (30% de terminales digitales y un 70% de analógicos). Estos terminales tienen una edad media elevada y no permiten el desarrollo de aplicaciones colaborativas.

* *Sistema de telefonía móvil corporativa:* La red de telefonía móvil es casi exclusivamente una red de voz en la que se utilizan una serie de servicios básicos. No existen prácticamente servicios de datos ni otras aplicaciones avanzadas.

La conexión entre la red corporativa fija del Ministerio y la red del operador de telefonía móvil se hace a través de un único enlace y sede. Si existe una caída en ese enlace o en la centralita asociada, se pierden todas las funcionalidades asociadas al sistema de telefonía móvil corporativa: marcación corta, desvíos fijo-móvil, facturación en base a tarifas corporativas, etc.

* *Inexistencia de una RPV global de voz:* La inexistencia de una red privada global de voz, supone un importante coste extra para el Ministerio, ya que las llamadas entre sedes son tarificadas por el operador. Desde el punto de vista de funcionalidad, la inexistencia de esta red privada restringe enormemente el número de servicios de voz que pueden ser ofertados a los usuarios del Ministerio.

* *Inexistencia de mecanismos de redundancia:* En general, las centralitas del Ministerio no disponen de caminos alternativos o de respaldo para su conexión a la red pública por lo que ante una caída en un PRI, la sede afectada pierde conectividad telefónica con el exterior.

La red de datos

Sobre la red de datos se realizó un análisis similar a dos niveles: a nivel MAN (red de conexión entre sedes) y a nivel LAN, (debilidades de la red local en cada una de las sedes).

En lo que respecta a la MAN de interconexión, se detectaron tres debilidades.

* *Heterogeneidad de tecnologías:* Debido al crecimiento ad-hoc de la red de datos, se había llegado a una situación en la que convivían gran número de tecnologías de una manera poco ordenada: esto tenía consecuencias negativas en aspectos como el coste de la solución de interconexión y la dificultad en su gestión.

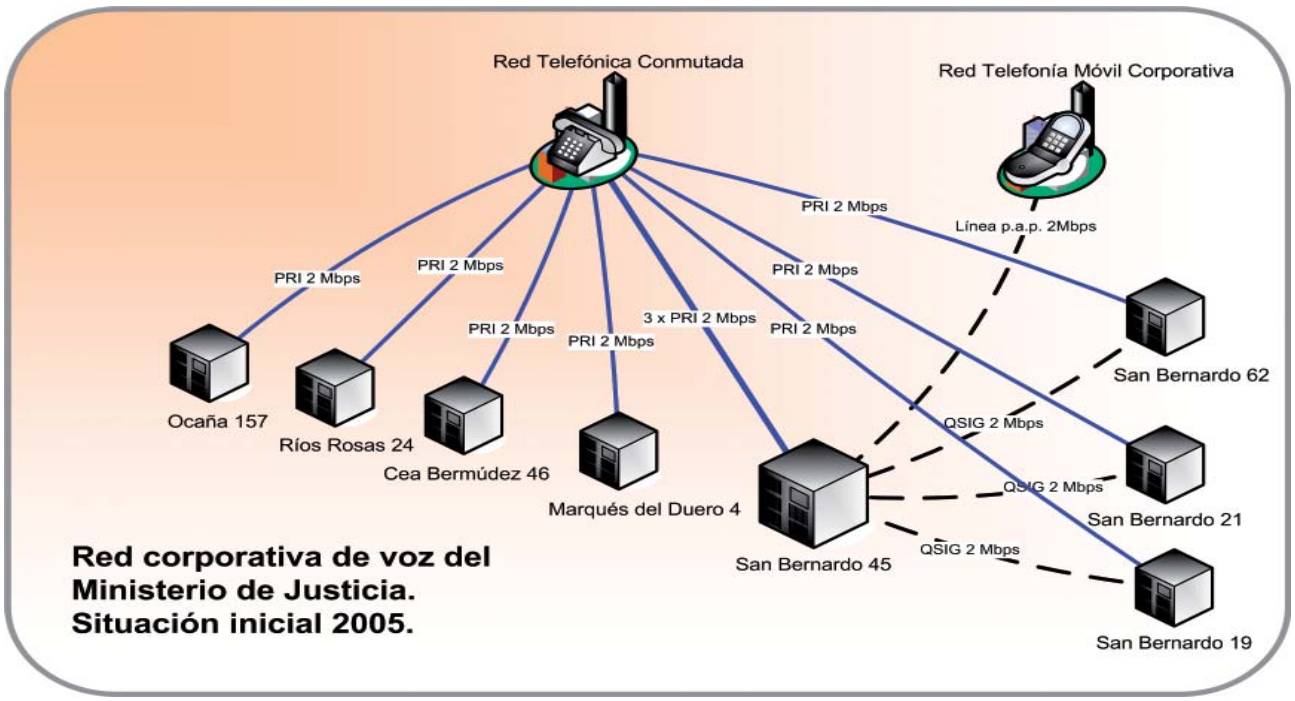
* *Inexistencia de líneas de respaldo:* En general, no existían líneas de respaldo, por lo que una caída en alguno de los enlaces causaba la pérdida de conectividad en la sede afectada.

* *Topología y caudales:* La topología de la red no era adecuada, por existir puntos únicos de fallo. Los caudales de datos se habían quedado desfasados para las necesidades del momento, existiendo periodos de saturación en los enlaces.

La arquitectura de LAN de las sedes no era la ideal, ya que no respondía a un diseño claramente estructurado, sino más bien a las necesidades de ubicación de equipos de usuario y servidores en diversas ocasiones en el pasado. Urgencias e imprevistos habían condicionado las sucesivas ampliaciones de la LAN en las sedes, que habían sido realizadas con soluciones técnicas no óptimas. Tampoco existía una separación física y lógica entre equipos de usuario, servidores, impresoras de red, etc. Por último, existía un reducido número de mecanismos de redundancia, por lo que en caso de fallo de alguno de los elementos críticos de la LAN, el servicio se veía seriamente afectado.

Como agravante, en la red se utilizaba exclusivamente enrutamiento estático, lo que dificultaba la gestión y ocasionalmente daba lugar a ciertos problemas difíciles de aislar. »

Figura 1. Red corporativa de voz a comienzos del año 2005



Proyectos de mejora

Realizado al análisis, se elaboró un catálogo de proyectos para ir tratando cada una de las áreas en las que se habían detectado necesidades. Los proyectos se dividieron en dos grupos:

* Proyectos de realización interna: Para ser desarrollados por el personal de la DITI, contando con contratación externa de los suministros necesarios y de algún servicio de manera puntual.

* Proyectos en colaboración: Por su naturaleza y volumen deberían ser ejecutados en estrecha cooperación con operadores de telecomunicaciones, integradores y suministradores. La decisión tomada fue realizar su contratación mediante un *concurso público* con duración cuatrienal.

Proyectos de realización interna

La decisión de que fuera el personal interno el que realizara ciertos proyectos se adoptó tanto por motivos económicos como técnicos y formativos. De esta manera, el personal interno tendría oportunidad de mejorar su competencia técnica, para posteriormente formar parte de los equipos de trabajo que se establecerían en el marco del concurso de comunicaciones.

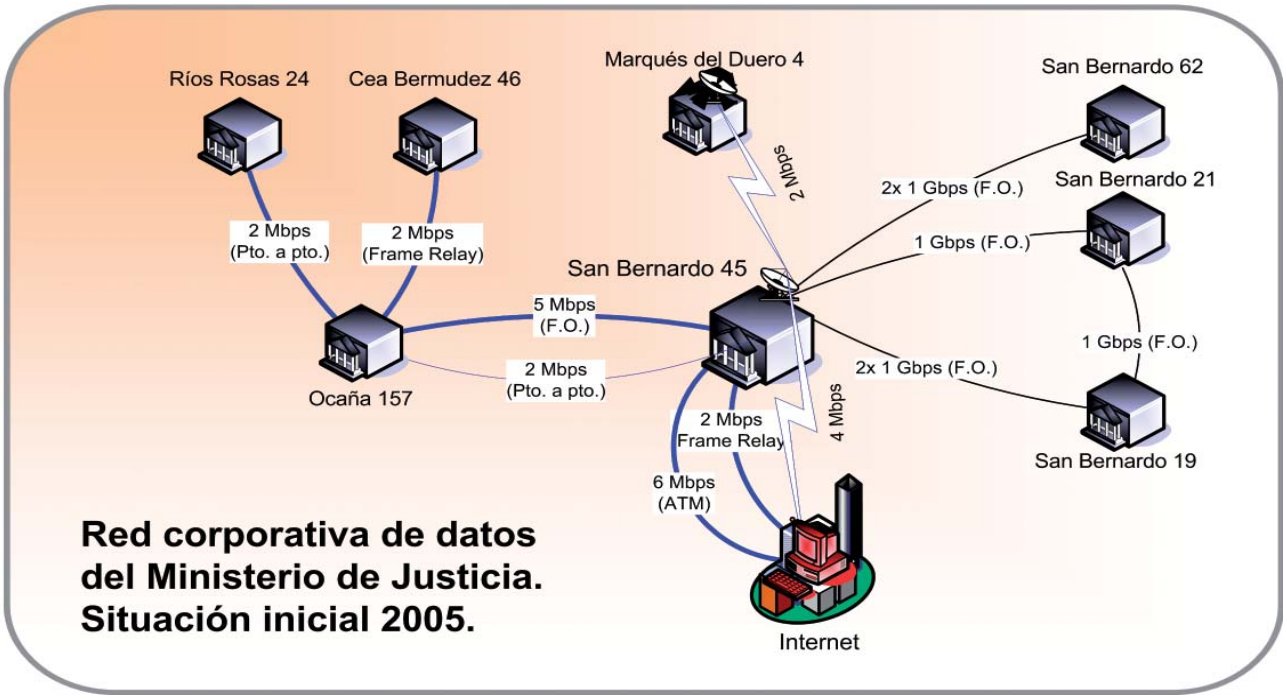
Introducción de mecanismos de enrutamiento dinámico

Como ya se ha comentado, en la red corporativa de datos del Ministerio a principios del 2005 se utilizaba exclusivamente enrutamiento estático. El hecho de no disponer de mecanismos dinámicos dificulta la gestión de la red y supone un serio inconveniente a la hora de planificar el crecimiento ordenado de la misma. Por este motivo, y teniendo en cuenta que el equipamiento existente permitía la puesta en servicio de estos mecanismos, se decidió priorizar este proyecto antes de acometer rediseños de la arquitectura física y lógica.

Como paso preliminar, se realizó el estudio de diversos protocolos dentro del grupo de los denominados IGP (Interior Gateway Protocols): RIPv2, OSPFv2 e EIGRP. Una vez consideradas las ventajas e inconvenientes de cada protocolo, se eligió el protocolo OSPF, por ser un protocolo estandarizado que, a cambio de una cierta complejidad de configuración, facilitaría el crecimiento futuro de la red.

La implantación del protocolo se llevó a cabo en el plazo de unas tres semanas, siendo totalmente trans-

Figura 2. Red corporativa de datos (MAN) a comienzos del año 2005



parente para los usuarios de la red corporativa. El proyecto finalizó en octubre de 2005.

Piloto de LAN multiservicio

A finales del año 2005 se inició el proyecto de puesta en servicio de una nueva sede del Ministerio. Simultáneamente, se estaba realizando la preparación de los pliegos técnicos del mencionado concurso de comunicaciones. Por este motivo, se tomó la decisión de dotar a esta sede de una red multiservicio (telefonía IP + datos + aplicaciones). De esta manera, se podrían validar en la práctica una serie de soluciones técnicas antes de incluirlas en los pliegos técnicos, así como calibrar el impacto en los usuarios del Ministerio frente al cambio tecnológico a telefonía IP.

Se estudiaron las soluciones de tres fabricantes líderes en el sector: Avaya, Cisco y Nortel. La red corporativa de datos estaba compuesta en su mayoría por equipamiento de Cisco, y la red de voz, por equipamiento de Nortel: era razonable incluir a estos dos fabricantes en el análisis. Avaya fue seleccionada por tratarse de otro líder en el mercado.

Internamente se elaboró una propuesta técnica basada en las soluciones de Cisco, y en paralelo, se solicitaron propuestas adicionales a diversos integradores, con el fin de poder realizar la mejor elección posible.

La solución elaborada internamente resultó finalmente elegida, ya que aportaba ventajas técnicas:

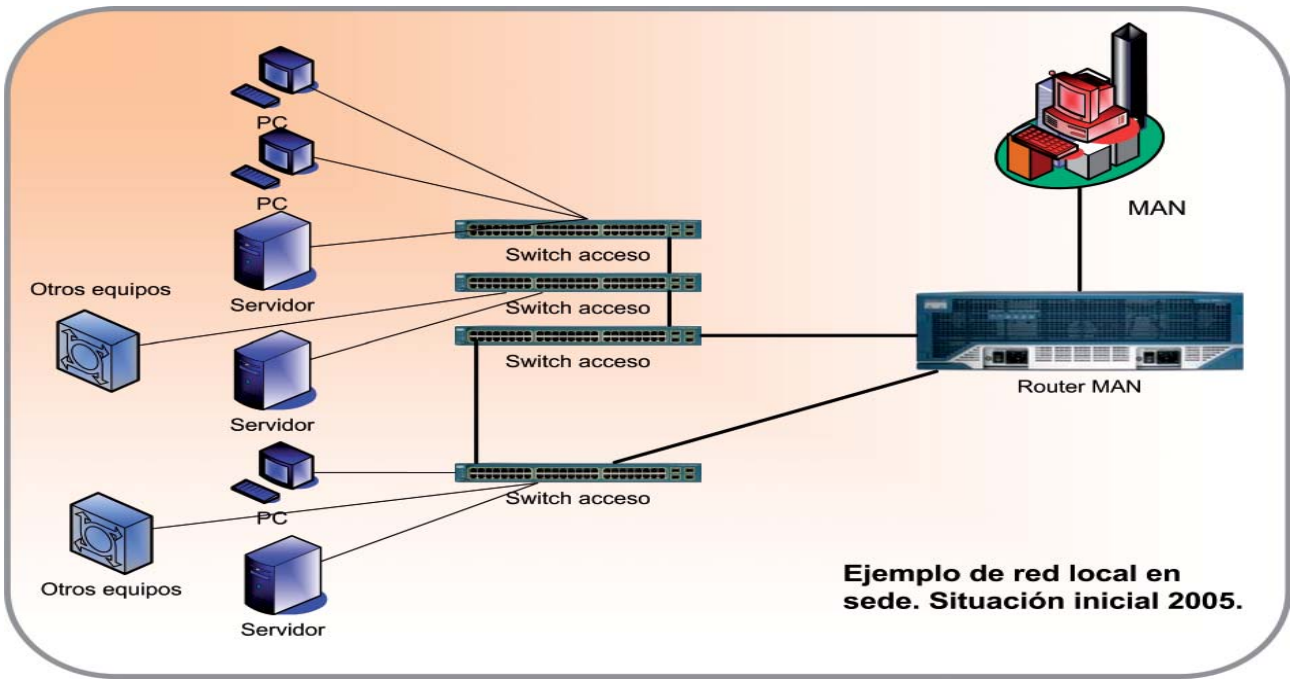
* Alto grado de redundancia: En todos los elementos clave de la red, para lograr la mayor disponibilidad posible.

* Completitud: Se incluían todos los elementos y diseños necesarios para evaluar la solución, cosa que no ocurría con otras propuestas.

* Experiencia interna: El fabricante elegido era bien conocido tanto a nivel técnico (personal interno con formación y capacidad de gestión) como estratégico (soporte de marca y existencia de numerosos integradores capacitados para dar soporte a la solución).

El plazo de implantación de la solución fue muy reducido, en torno a seis semanas, debido a la inminente puesta en servicio de la sede (Marzo de 2006). El proyecto se completó con éxito en la fecha prevista, y permitió obtener conclusiones que fueron incorporadas a los pliegos técnicos del concurso de comunicaciones. »

Figura 3. Red local de una sede a comienzos del año 2005



Rediseño arquitectura física y lógica LAN

Otra de las necesidades de mejora detectadas era la referente a la propia arquitectura física y lógica de la LAN de cada una de las sedes del Ministerio, Tras evaluar diversas alternativas, y utilizando los conocimientos adquiridos durante el proyecto de LAN multiservicio, finalmente se decidió implantar un modelo físico de doble estrella redundante muy similar al de dicha sede, que constituía una arquitectura más robusta, fácil de gestionar, y que permitiría la implantación paulatina de nuevos servicios.

De esta manera, cada switch de usuario (capa de acceso) estaría conectado a dos dispositivos centrales (capa de distribución y core) que harían funciones de conmutación y enrutamiento. Igualmente, y con el fin de eliminar los puntos únicos de fallo, la conectividad de cada sede hacia la red corporativa, se llevaría a cabo de manera redundante.

Desde el punto de vista de la arquitectura lógica, se tomó la decisión de realizar la segmentación de la red, definiendo un conjunto de VLANs de propósito específico para: servidores, PCs de usuario en cada una de las sedes, equipos en cuarentena, máquinas de gestión, teléfonos IP, etc.

En la actualidad se ha implantado la nueva arquitectura física en tres de las sedes, mientras que el modelo lógico ya se encuentra implantado globalmente.

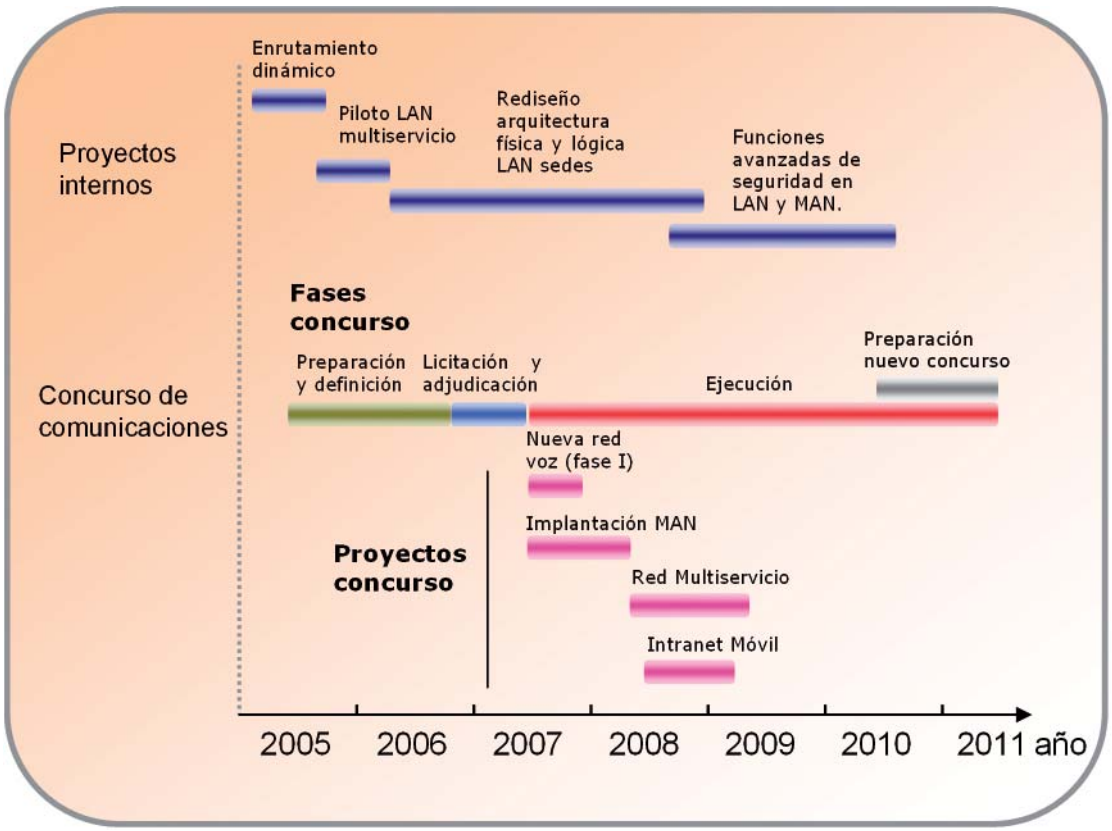
Funciones avanzadas de seguridad

Otros proyectos actualmente en estudio están relacionados con la mejora del nivel de seguridad en la red corporativa, tanto a nivel de LAN como de MAN. En particular, se han detectado dos necesidades, que serán afrontadas en función de los recursos disponibles:

* Control de admisión en red (NAC): En la actualidad, no se dispone de mecanismos que permitan autenticar los diversos dispositivos que se conectan a la red, con el consiguiente riesgo de sufrir ataques internos debido a máquinas que se conectan sin seguir unas mínimas precauciones de seguridad.

* Encriptación de flujos de tráfico extremo a extremo: Dado que la infraestructura de la MAN ha evolucionado (en el marco del contrato de comunicaciones en ejecución) hacia un servicio de transporte sobre la red MPLS de un operador, resulta prioritario el disponer de mecanismos que permitan securizar, de manera selectiva, la transmisión de flujos de información entre las diversas sedes.

Figura 4. Proyectos previstos para el periodo 2005-2011



Estos proyectos son sólo una muestra dentro del establecimiento de una política global de seguridad informática del Ministerio, que deberá contar con el impulso y apoyo del estamento directivo de la organización si se quiere lograr el éxito.

El concurso de comunicaciones

La decisión de lanzar el concurso público de comunicaciones viene motivada por dos grupos de factores. Por un lado, de índole económica, ya que se estaban pagando precios demasiado elevados por los servicios de comunicaciones, herencia de una situación en la que existía un único operador dominante. Por otro lado, existían argumentos técnicos: una vez expuestas las necesidades del Ministerio se deseaba recabar las propuestas técnicas de los diferentes operadores y suministradores acerca de las soluciones técnicas que se podían ofertar.

El pliego del concurso se estructuró en base a ocho lotes. Cuatro lotes deberían prestar servicio a la red corporativa de voz y datos del Ministerio, mientras que los otros cuatro deberían hacer lo mismo con la red corporativa de la Administración de Justicia.

Los cuatro lotes del Ministerio quedaron definidos como sigue:

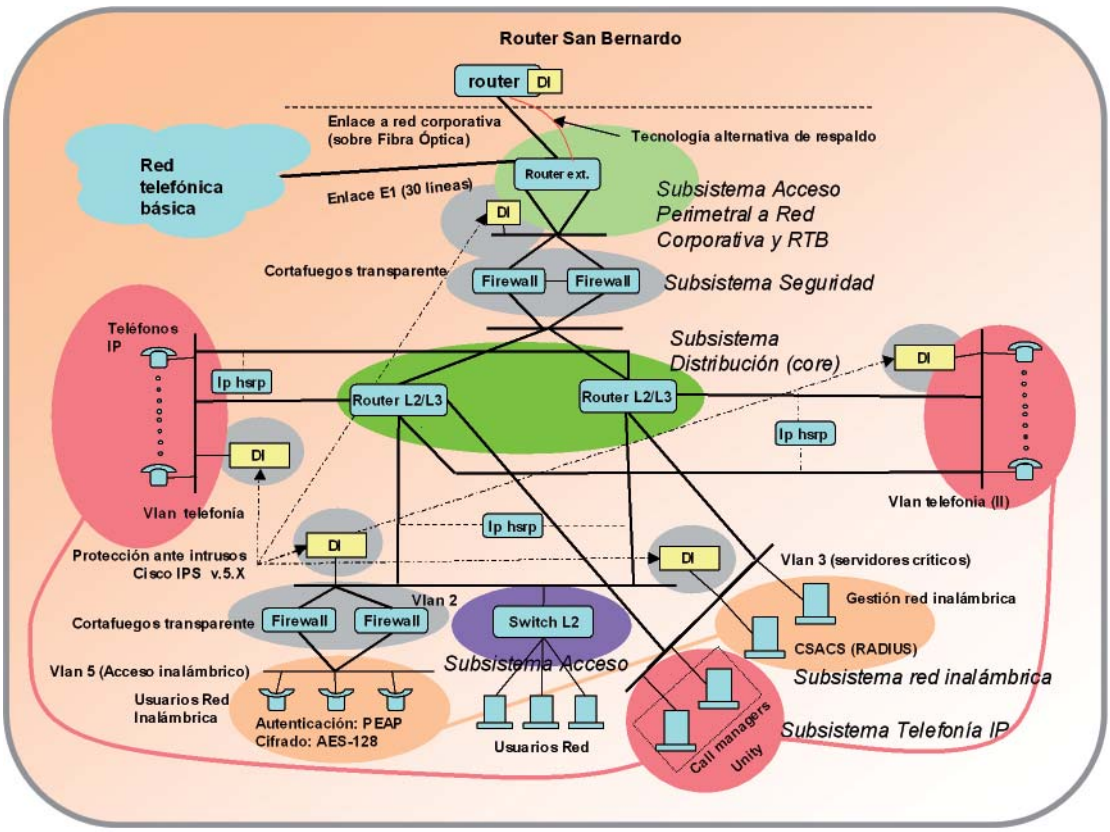
* Lote 1: Red MAN entre sedes y servicio de Internet. Servicios de telefonía fija.
* Lote 2: Servicios de telefonía móvil (voz y datos).
* Lote 3: Redundancia para MAN y acceso a Internet.
* Lote 4: Servicios de gestión y control de los lotes 1,2 y 3.

Tras el proceso de licitación, finalmente el adjudicatario de los lotes 1,2 y 3 resultó ser el grupo *Orange Business Services (France Telecom S.A.)*.

La solución técnica ofertada tiene una serie de puntos destacados:

* Se trata de una red de Telefonía IP basada en tecnología Cisco. Existe un nodo central ubicado en las instalaciones del operador. En este nodo »

Figura 5. Vista lógica LAN multiservicio



se ubican los equipos que realizan las funciones de: control y gestión del sistema de telefonía IP (Cisco Call Manager), gateways o pasarelas hacia las redes públicas de voz, etc. En el caso de un fallo en los elementos de este nodo central, existe una solución de redundancia que permite garantizar la continuidad en el servicio de voz. Esta solución está compuesta por un conjunto de gateways ubicados en las sedes y un segundo cluster de Call Managers físicamente ubicado en una de las sedes del Ministerio. Si tuviera lugar un fallo simultáneo de ambos clusters, entraría en marcha un tercer mecanismo de supervivencia que permitiría garantizar el servicio de manera parcial, utilizando para ello la infraestructura local de cada sede (mediante la función SRST).

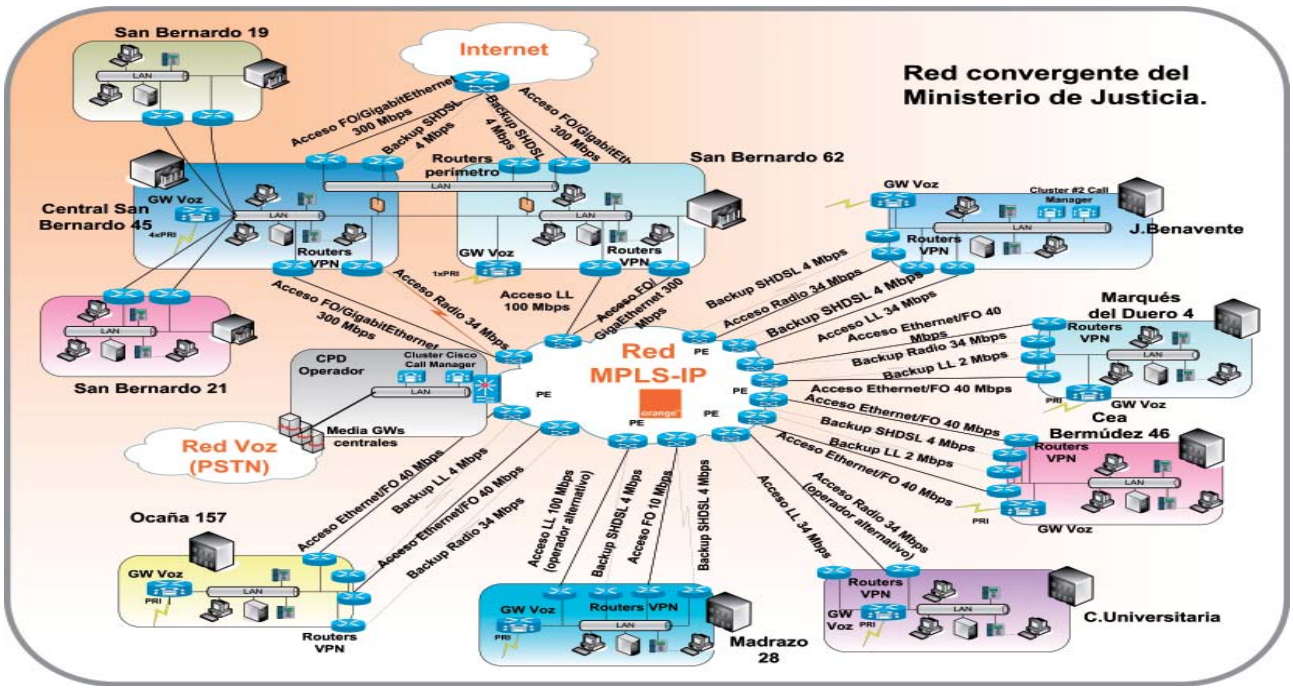
* La conectividad entre sedes se realiza a través del backbone MPLS del operador, existiendo diversas tecnologías de acceso a dicho backbone.

* El acceso de cada sede a la red MPLS se realiza de manera redundante en equipos y líneas, de manera que cada sede dispone de cuatro líneas distintas. Igualmente, se diversifica en todo lo posible la gama de tecnologías de conexión, utilizando las siguientes: fibra óptica propia o de operador alternativo (COLT), radioenlaces punto a punto propios o de operador alternativo (ONO), líneas SHDSL y circuitos punto a punto de operador alternativo (Telefónica).

* Existe redundancia en el extremo del operador, ya que la conectividad de las líneas de una misma sede está diversificada entre dos nodos distintos de la red.

* Las cuatro sedes ubicadas en la C/San Bernardo en Madrid están dotadas de una solución de acceso diversificado y dual. Esta solución dota de accesos independientes – tanto a Internet como a la red MPLS – a las dos sedes de esta zona en las que se ubican el CPD principal y el de respaldo del Ministerio.

Figura 6. Nueva red integrada de voz y datos



En el momento de escribir este artículo, se ha finalizado el despliegue de la nueva MAN sobre MPLS, así como los accesos redundantes a Internet. Igualmente, se encuentra en funcionamiento la solución de Telefonía IP que se desarrolló como parte del piloto de LAN multiservicio (una sede con 350 usuarios). En la siguiente fase de despliegue, se acometerá la migración paulatina del resto de sedes a la solución de telefonía IP global.

Conclusiones

En este artículo se ha presentado la evolución tecnológica de las redes del Ministerio de Justicia desde principios del año 2005. Partiendo de una situación inicial con redes de voz y datos "ad hoc" que tradicionalmente habían tenido un crecimiento no planificado, siempre en base a las necesidades de cada momento, se han expuesto los diversos proyectos que están haciendo posible el evolucionar desde esa situación inicial a una situación mucho más adecuada a las necesidades de una organización como el Ministerio de Justicia. Esta evolución viene marcada por tres ejes principales:

* Reducción de costes.
* Mejora de los niveles de servicio.
* Aumento del número de servicios ofrecidos por la red corporativa.

Una vez completado el proceso de cambio tecnológico, el Ministerio dispondrá de una única red sobre la que se prestarán, de manera integrada, los servicios de comunicaciones de telefonía fija, datos y telefonía móvil del Ministerio.

Adicionalmente, se habrán realizado las tareas necesarias para garantizar que esta red tenga los elevados niveles de disponibilidad y calidad de servicio que den respuesta a los exigentes requisitos de comunicaciones de una organización como el Ministerio de Justicia.

Luis Rodríguez Vega es Jefe de Área de Comunicaciones de la División de Informática y Tecnologías de la Información del Ministerio de Justicia