Renovación de la red LAN del Ministerio de Justicia

Borja López Montilla

Jefe del Área de Comunicaciones y Seguridad

División de Informática y Tecnologías de la Información.
Subsecretaría

versión 1.0

Marzo 2010

Índice

1. Introducción

La dirección de las áreas de infraestructura (aquellas que gestionan las comunicaciones y la seguridad, principalmente) exige un ejercicio constante de equilibrio y distribución de prioridades, entre lo urgente y lo realmente crucial y estratégico.

Las incidencias del día a día, así como la puesta en marcha de servicios urgentes e inaplazables, son susceptibles de convertir la gestión de un área de comunicaciones en un continuo *triaje*[1], que haga olvidar el largo plazo y cometer errores que luego sea muy difícil corregir. La no inusual carencia de recursos técnicos, económicos y de gestión, unida a lo anterior, podría desembocar en crecimientos de las redes internas de las organizaciones, donde se ponen parches sobre parches, sin planificación.

La División de Informática y Tecnologías de la Información (DITI) del Ministerio de Justicia se encarga de la gestión integral de los servicios y sistemas informáticos y de comunicaciones de los servicios centrales del Departamento. Fue creada en el año 2004, con el objeto de atender las variadas necesidades informáticas de las distintas unidades del Ministerio. La nueva unidad se puso a trabajar de inmediato en la resolución de las urgentes necesidades que condicionaron su creación. Con evidente éxito, además, pues en los cuatro años siguientes, las TIC conocieron un grado de implantación y desarrollo, ignoto hasta entonces en los servicios centrales del Ministerio.

Ese crecimiento tan asombroso, fue posible en primer lugar gracias al entusiasmo y duro trabajo del personal de la unidad en estos años; y en segundo lugar, gracias a la dotación económica que se asignó a la unidad, reconociendo lo urgente y necesario de los trabajos que tenía ante ella.

Como no podía ser de otra manera, y como es inevitable que pase en las nuevas organizaciones, ese desarrollo vertiginoso no siempre pudo ser acompañado de la planificación y el análisis que se requieren para que los sistemas informáticos y de comunicaciones sean escalables, y tengan el rendimiento y la seguridad adecuadas.

En el verano de 2008, resultó evidente que la red local de comunicaciones del Ministerio no estaba diseñada para soportar el creciente número de usuarios y de servicios que ya hacían uso de ella. Los cortes en el servicio se sucedían diariamente, pudiéndose hacer poco por solucionarlos.

En otoño de 2008 comienza a formarse la nueva área de comunicaciones de la DITI, que recoge el testigo dejado por la anterior y su convencimiento de que había que replantearse toda la estructura de red del Ministerio desde el principio.

A lo largo del presente documento se recogerán los trabajos realizados desde finales de 2008 con el fin de renovar la infraestructura de red del Ministerio de Justicia y prepararla no sólo para las demandas de sus usuarios y servicios actuales sino también para las que se presenten en el futuro.

2. El origen del problema

La razón de fondo de los problemas que presentaba la red, era que, para facilitar la puesta en marcha de servicios y equipos de usuario, se había utilizado una única red privada virtual (VLAN), con un rango de direccionamiento único. Se había conectado, a un mismo switch, ordenadores y servidores, que compartían de este modo un mismo rango de direccionamiento y una misma VLAN. Según surgía la necesidad de conectar nuevos equipos y servidores, se añadían nuevos switches, enlazados entre sí.

La VLAN utilizada era la número 1. La desventaja de esta elección, radicaba en que los equipos de comunicaciones utilizaban la propia VLAN 1 para el tráfico de negociación de diversos protocolos de transporte como el VTP, el CDP, el PaGP, el LACP, y parte del STP, entre otros[2]. Al mezclarse tráfico de negociación con tráfico de datos, se disparaba el riesgo de que un pico de los datos aumentase las latencias y con ello provocase el fallo de los diversos protocolos de negociación, desencadenando una sucesión de errores en cascada que acabasen derrumbando la red. Este problema era de especial importancia en las sedes de la calle San Bernardo, 45 y San Bernardo, 62 (unidas entre sí mediante fibra óptica, a través de la cual se extendía la VLAN 1) ya que en las mismas se concentraba el mayor número de usuarios y la práctica totalidad de los servidores a cargo de la DITI, con lo que la presión sobre la VLAN 1 era significativamente mayor que en otras sedes del Ministerio, donde el número de usuarios era mucho menor, y no existían servidores conectados a la misma.

A nivel 3, este esquema se basaba en un único rango de direccionamiento (máscara 255.255.248.0, ocho clases C) que lo abarcaba todo, mezclando usuarios con servidores, eliminando la posibilidad de aplicar políticas personalizadas de seguridad a unos y otros.

Por otro lado, era difícil mantener tanto las salas de datos del Ministerio, como los armarios de comunicaciones, pues los cableados no habían sido diseñados de manera sistemática.

En cuanto al equipamiento de comunicaciones en sí, era de buena calidad, pero estaba próximo a alcanzar el fin de su vida útil.

Por todo lo anterior, la red comenzó a fallar cada vez con más frecuencia y gravedad. El diagnóstico de los problemas era difícil y complejo. A comienzos del 2009, cuando aún no se

había empezado a desplegar la solución que se detallará en los apartados siguientes, el 60% del tráfico que travesaba la VLAN 1, era tráfico de broadcast, y los switches estaban sobrecargados: con frecuencia se saturaban sus tablas de memoria, pasando a funcionar en modo hub, degradando considerablemente el rendimiento global de la red.

3. El diseño de la solución

A comienzos del año 2009, el área de comunicaciones comenzó a diseñar un plan para dotar al Ministerio de Justicia de una nueva red de comunicaciones, que solucionara los problemas arriba detallados, y que hiciera posible un escenario fiable, en el que las aplicaciones y servicios se prestasen con las garantías de rendimiento, disponibilidad y seguridad requeridas por las organizaciones modernas. Este plan constaba de las siguientes fases:

- Sanear las salas de datos del Ministerio y muy especialmente el cableado de los armarios de comunicaciones.
- Sustituir el equipamiento de comunicaciones por otro nuevo, mucho más potente y mejor dimensionado.
- Rediseñar la topología de interconexión de este equipamiento, de manera que se asegurase la tolerancia a errores del diseño y su escalabilidad futura.
- Desplegar un nuevo esquema de capa 2 del protocolo de comunicaciones, que permitiese migrar a todos los usuarios y servidores, de la VLAN 1, a otras VLANs, más adecuadas y correctamente dimensionadas.
- En paralelo con la migración de equipos a las nuevas VLAN, se rediseñó el esquema de capa 3 del protocolo de comunicaciones, creando redes especializadas para los distintos tipos de equipos.

4. Saneamiento y recableado de los armarios

El primer paso hacia la reestructuración de la topología de redes del Ministerio de Justicia era la propia reorganización de los armarios.

Se planificó el saneamiento de cada una de las salas de datos y armarios del Ministerio.

Cada una de estas actuaciones comprendía las siguientes tareas:

- Inventariado de cada uno de los cables del armario.
- Valoración de los equipos conectados.
- Movimiento, en ventanas programadas, de los equipos y servidores importantes a armarios que no fueran a ser recableados.

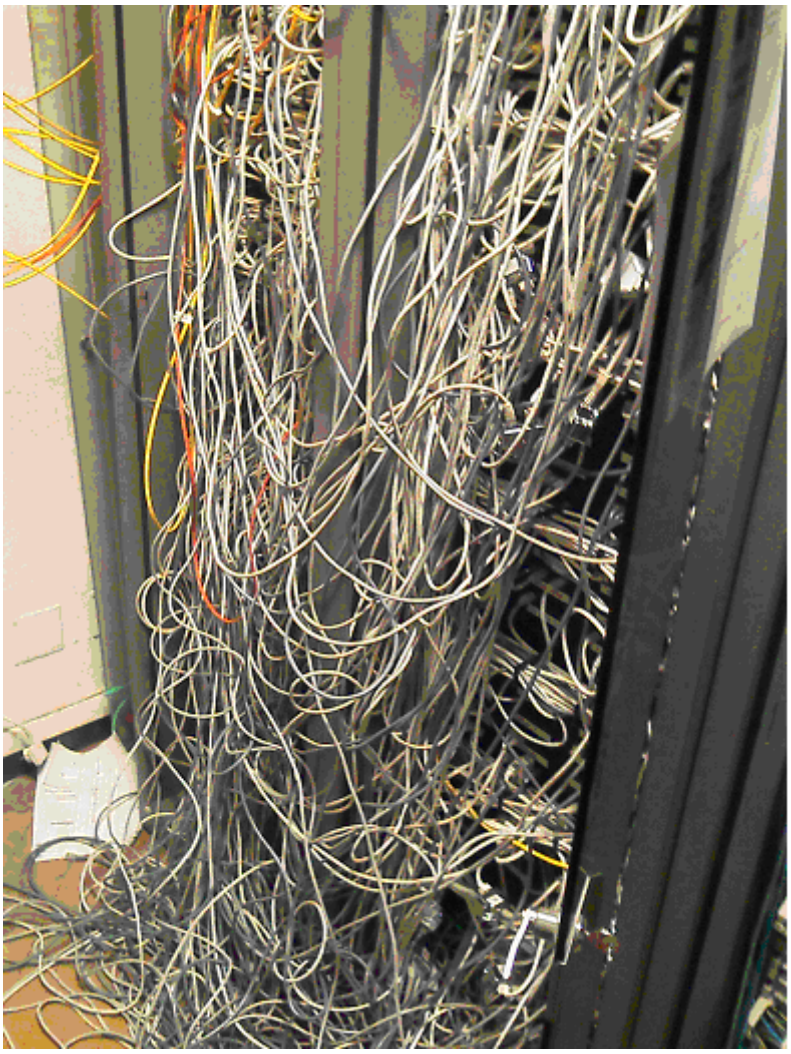

Ilustración 1: Los armarios de comunicaciones de una de las salas de datos antes del recableado.

Luego, en una ventana programada de fin de semana, se realizaba el recableado completo de cada armario:

- Retirada del cableado antiguo.
- Desmontaje de las regletas de parcheo antiguas.
- Desmontaje de los switches antiguos.
- Montaje de las nuevas regletas de parcheo en sus nuevas ubicaciones
- Reubicación de los switches en sus nuevas localizaciones.
- Reconexión con el cableado nuevo.

Los switches se intercalaron con las regletas de parcheo, de manera que las asignaciones no requiriesen latiguillos de red mayores de 30 cm. Además, para el hipotético caso de que alguno de los latiguillos no tuviese que conectarse al switch inmediatamente adyacente se incluyeron abundantes pasahilos. Esto permitió armarios mucho más limpios donde resulta inmediato saber a qué puerto de switch iba conactada cada una de las rosetas de usuario, reduciendo casi completamente el cableado entre armarios.

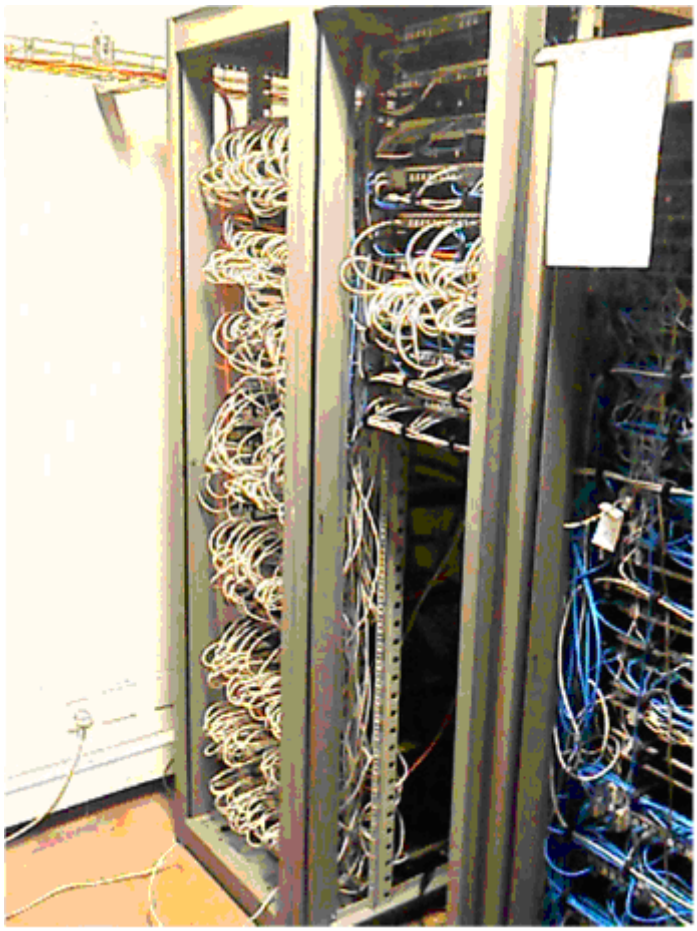

Ilustración 2: Los mismos armarios, tras el recableado.

Los resultados, según se deduce de las figuras 1 y 2, son evidentes. Este proceso se realizó en las 14 salas de datos del Ministerio a lo largo del 2009.

5. Renovación de los equipos de red

Una vez que los armarios de una sala quedaban saneados y ya se podía operar fácilmente con ellos, se procedía a sustituir los switches antiguos (Cisco-3500XL) por otros más potentes (Cisco-3750G-48PS, Cisco-3750E-24TD-E, Cisco-3750E-24TD-S y Cisco-3560-G) durante ventanas de corte programadas a última hora de la tarde, fuera del horario laboral.

6. Cambio de la topología

Al renovar los equipos, se iba aprovechando para ir cambiando la topología de cada una de las salas.

La importancia y complejidad de esta fase fue especialmente señalada en las sedes del Ministerio de Justicia de la calle San Bernardo, al ser donde se concentraba la mayor parte de los servidores y usuarios y donde se producía el problema con la VLAN 1 antes reseñado. En la estructura primitiva de estas sedes, las regletas de rosetas de usuario se parcheaban a switches, denominados *de acceso*, y éstos se conectaban directamente al núcleo de conmutación formado por dos equipos Cisco 4500 en alta disponibilidad, a través de switches de acceso de cabecera del stack. La conexión de estos switches de cabecera con el núcleo no estaba redundada, por lo que cada switch sólo conectaba con uno de los nodos del núcleo. Como todos los switches estaban en la VLAN 1, el núcleo ejercía de plataforma de conmutación entre los equipos de dicha VLAN, y a la vez les ofrecía la puerta de enlace de nivel 3 necesaria para salir hacia otras redes. Esto hacía que el núcleo sufriese el ruido habitual del nivel 2, por lo que su rendimiento y capacidad de crecimiento se veía seriamente disminuido.

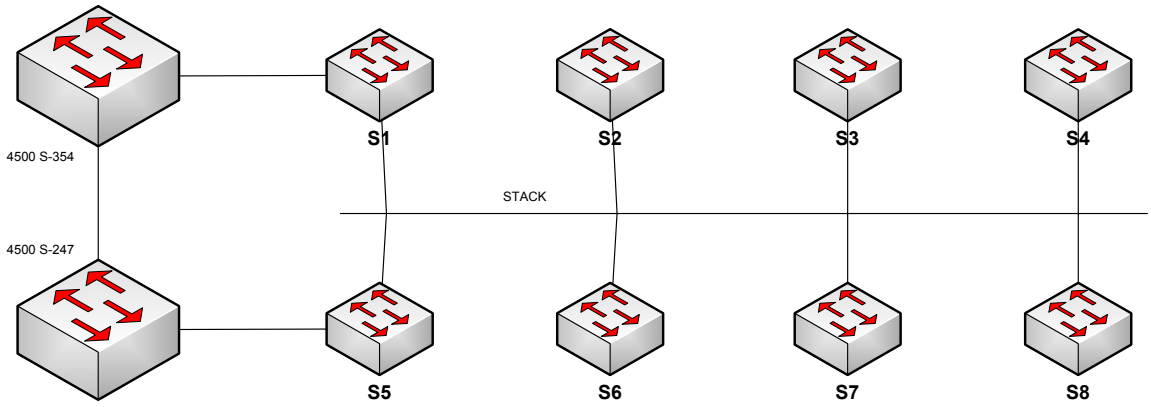

Ilustración 3: Topología de una de las salas del Ministerio antes del cambio.

A esta situación se le dio solución mediante una **estructura en tres capas**[3] que asegurase que el núcleo se viese libre de todo el tráfico de capa 2 posible, quedando únicamente como núcleo de enrutamiento de alto rendimiento. Para ello se introdujo una capa intermedia denominada *capa de distribución*. Esta capa, formada por switches multinivel, se sitúa entre el *núcleo* y los switches de acceso, presentándoles a los equipos conectados a estos últimos su respectiva puerta de enlace. Los switches de distribución se conectan al núcleo a través de la capa 3 (dicho de otro modo: mediante *routing*). De este modo, aunque los switches de acceso siguen funcionando exclusivamente a nivel 2, esta capa se acaba en los switches de distribución por lo que el núcleo permanece a salvo de las anomalías típicas de la capa 2,

las cuales quedan limitadas a afectar a un único switch en vez de a la red entera. La capa de distribución realiza también enrutamiento entre las redes, para las cuales hace de puerta de enlace, por lo que gran parte del tráfico de nivel 3 ni siquiera necesita ser remitido al núcleo. Cualquier tipo de filtrado desde la capa de acceso se realizaría en la de distribución para procurar que el núcleo tuviese la configuración más sencilla posible y por tanto de mayor rendimiento.

La estructura en tres capas no es algo nuevo en el mundo de las redes, pero es difícil verla en infraestructuras que no sean de reciente implantación, dadas las dificultades que entraña adaptar una red heredada a este tipo de topología (¡el contenido de esta comunicación es el perfecto ejemplo de dichas dificultades!).

Además de su estabilidad, esta estructura permite un alto grado de escalabilidad ya que hace posibles distribuciones en árbol de los switches, por lo que el núcleo puede servir a muchos más switches (de usuarios o servidores) que en el caso tradicional de distribuciones en estrella de switches de acceso directamente conectados al núcleo.

Los switches de acceso, además de concentrar la capa 2 en ellos, sirven para fragmentarla en VLANs de tamaño adecuado. En vez de tener una VLAN gigantesca como antes, cada uno de los switches de acceso sitúa a los usuarios conectados a él en una VLAN diferente a las del resto de los switches de acceso. De esta manera, los dominios de broadcast se reducen muchísimo con el consiguiente aumento del rendimiento y la estabilidad.

Cada una de las VLANs anteriores tiene una correspondencia a nivel 3 con un rango de direccionamiento diferenciado para cada una de ellas. El servidor de DHCP se encarga de asignarle el mismo rango de direccionamiento a cada uno de los equipos conectados a una VLAN concreta. Esto permite racionalizar el uso de direcciones IP y agiliza tremendamente la atención de incidencias, ya que sabiendo la dirección IP de un equipo se puede saber la VLAN en la que se encuentra, de ahí hay una correspondencia inmediata a su switch. Luego es fácil averiguar su MAC en la tabla de ARP del switch de distribución, con lo que se puede conocer el puerto del switch de acceso donde se encuentra y con un mero examen visual del armario se puede ver la roseta donde se conecta el equipo (gracias al saneamiento realizado en el cableado de los armarios). Todo este proceso no dura más de tres minutos.

Los rangos concedidos por el servidor de DHCP a cada uno de los switches están acotados a máscaras 26 (64 direcciones), de manera que haya 1 dirección por puerto de switch de acceso (cada uno de los cuales cuenta con 48 puertos) y una pequeña reserva de direcciones para el caso de que se utilizasen miniswitches en alguno de los puertos. De todos modos, procuramos evitar en lo posible el uso de miniswitches, reservándolos exclusivamente para emergencias y para situaciones provisionales. Esto es así porque los

miniswitches suelen ser un elemento que a la larga acaba *ensuciando* las redes, permitiendo que proliferen zonas fuera del control y la gestión de las áreas de comunicaciones.

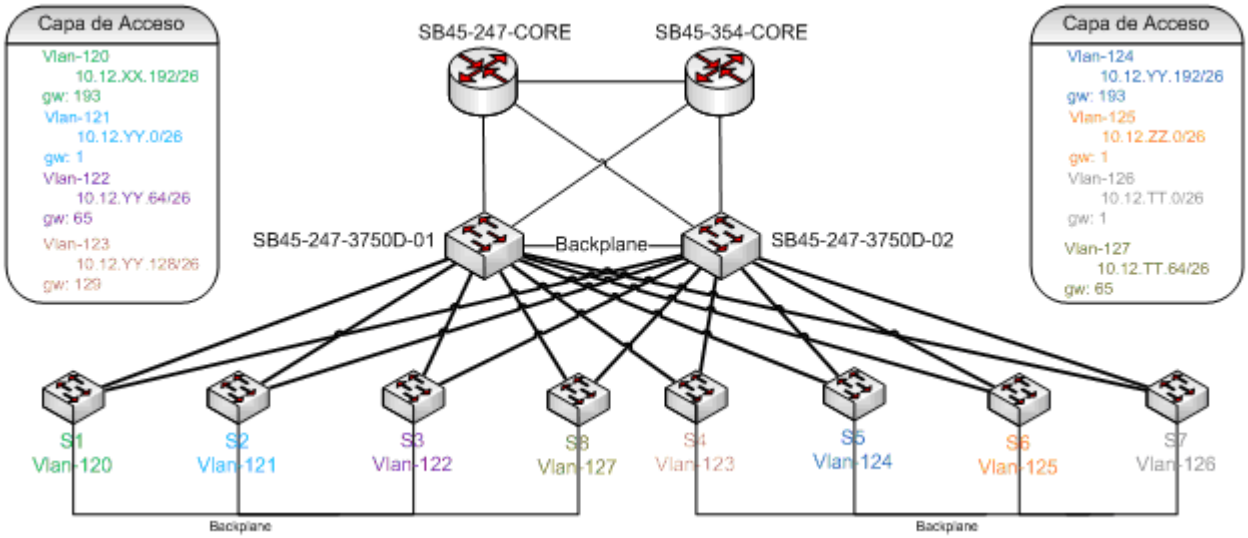

Ilustración 4: Topología de la misma sala después de los cambios.

Como se puede ver en la ilustración anterior, se redundaron todos los enlaces ascendentes, de manera que el servicio de cualquier switch fuese capaz de sobrevivir a la caída de cualquiera de sus enlaces. Además, y para aumentar aún más la tolerancia a errores, todos los switches de una misma capa se unieron entre sí mediante cables de stack, de manera que, en caso de caída de los dos enlaces ascendentes de un mismo switch, éste pudiera salir por los de sus compañeros de stack.

En la práctica, renovar la infraestructura de red y adaptarla a esta topología supuso la configuración e integración de 66 switches, distribuidos entre 24 armarios de comunicaciones en 14 salas de comunicaciones de 7 sedes y, por supuesto, fue un proceso muy largo realizado poco a poco en intervenciones nocturnas durante todo el año 2009.

7. Resultados

Habiendo finalizado en su práctica totalidad las tareas descritas en esta comunicación, los resultados no pueden ser más satisfactorios: la red está estable, los usuarios no experimentan cortes, el rendimiento es muy alto y la estructura ha ganado resistencia frente a fallos. Quedan aún muchas cosas por mejorar, pero gracias a lo que ya se ha hecho la infraestructura de red del Ministerio de Justicia se ha convertido en una base estable sobre la que situar servicios de alta calidad tanto para los ciudadanos como para el personal de las distintas unidades del Ministerio.

Anexo I: Referencias

[1] http://es.wikipedia.org/wiki/Triaje

[2] http://www.ciscopress.com/articles/article.asp?p=358549

[3] http://en.wikipedia.org/wiki/Cisco%27s_3_Layered_Model