

Titulo: Conmutación en alta velocidad en redes LAN.

Autor: Roberto Valtueña Rincón.

Resumen del trabajo:

En este documento se muestra la renovación tecnológica que la Gerencia Informática de la Seguridad Social ha realizado en los grandes centros de gestión a los que da soporte, dotándolos de sistemas de conmutación en alta velocidad que permitan abordar los nuevos desarrollos corporativos en Sistemas de Información y la integración de nuevos tipos de datos como la voz y el vídeo interactivo.

El documento incluye una descripción de la tecnología incorporada a las redes locales actuales, si como un detalle de la evolución de las redes locales en el entorno de la GISS.

Biografía del autor:

Funcionario del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado, es Ingeniero Superior de Telecomunicaciones y Master en Dirección de Sistemas y Tecnologías de la Información por la Universidad Politécnica de Madrid.

Desde 1993 trabaja en la Gerencia Informática de la Seguridad Social, dentro del Centro de Comunicaciones. Como responsable del servicio de redes locales ha estado a cargo de la implantación del Proyecto SILUETA, para la dotación de redes LAN en todas las oficinas de la Seguridad Social.

Anteriormente trabajo en Telefónica I+D en temas de planificación de redes de telecomunicaciones y redes ópticas de acceso, habiendo colaborado en el proyecto BAF (Broadband Access Facilities) dentro del programa RACE II.

Título: Conmutación en alta velocidad en redes LAN.

El papel fundamental que juegan hoy en día las redes locales en la actividad de las organizaciones y los nuevos flujos de datos - imágenes, voz y vídeo- obligan a proporcionar infraestructuras con altos niveles de disponibilidad y rendimiento. Las demandas de las organizaciones no se limitan a disponer de mayor ancho de banda y una gran tolerancia a fallos, se requiere una optimización de los recursos y una administración que permita adecuar los medios disponibles a las diferentes aplicaciones.

En este documento se muestra la renovación tecnológica que la Gerencia Informática de la Seguridad Social ha realizado en los grandes centros de gestión a los que da soporte, dotándolos de la infraestructura necesaria para abordar los nuevos desarrollos corporativos en Sistemas de Información y la integración de nuevos tipos de datos.

Artículo:

La revolución que los Sistemas de Información han experimentado en los últimos años esta provocando una convergencia de todas las fuentes de información, cada día más numerosas, en un único punto: el ordenador personal. El concepto de terminal de datos, empleado para el acceso y la manipulación de la información corporativa, esta siendo reemplazado por el terminal multimedia e interactivo, que permite al usuario utilizar de manera integrada todo tipo de comunicaciones dentro de su organización. Tras de los datos llegaron a los terminales las imágenes, el vídeo y el audio, y ahora surgen nuevos canales de comunicación que incluyen la interactividad como son la telefonía y la videoconferencia. Todo este fenómeno esta generando la necesidad de disponer de redes cada vez más potentes, tanto en ancho de banda ofrecido, como en disponibilidad y rendimiento.

La Gerencia Informática de la Seguridad Social (GISS) abordó en 1993 la transformación del terminal de usuario, mas allá de los grandes centros de proceso de datos, con la sustitución en todas las oficinas de las Entidades Gestoras y Servicios Comunes de la Seguridad Social (TGSS, INSS e ISM) de su red de terminales de datos, por terminales gráficos conectados en red local y su posterior integración en una Intranet corporativa que hoy en día cuenta con más de 25.000 terminales y 1.200 centros de trabajo con sus redes locales interconectadas.

El modelo de red local implantado en por la GISS en los grandes centros de gestión (Direcciones Provinciales y Servicios Centrales) ha evolucionado en estos años debido a varios factores, que junto con el incremento de puestos de trabajo, están saturando las redes locales tradicionales:

- Incremento de la capacidad de proceso. Hoy en día, el salto que la tecnología ha provocado en el mundo de los PCs, ha puesto de manifiesto que dos estaciones de trabajo en la misma LAN pueden saturarla fácilmente.
- Evolución de los Sistemas Operativos. La multitarea permite a los usuarios de la red iniciar simultáneamente transacciones de red, y consecuentemente, aumentar la sus demandas sobre recursos de red (discos, impresoras, CD-ROM, etc.) elevando el tráfico generado.
- Aumento en la demanda de los servicios de Red. La filosofía cliente-servidor han impulsado una creciente demanda de capacidad de almacenamiento y proceso en los servidores, saturando las redes locales.

Todos estos aspectos han motivado la necesidad de analizar con detenimiento los modelos de red empleados y buscar en el mercado nuevas tecnologías que permitan mantener el grado de servicio ofrecido a los usuarios.

El modelo de red elegido por la GISS en 1994, para la implantación del proyecto SILUETA en todas las oficinas de la Seguridad Social, ha demostrado su capacidad de adaptación a esta revolución tecnológica y de los Sistemas de Información, gracias a tres factores estratégicos:

1. Redes locales Ethernet. En una organización fuertemente ligada a los Sistemas de Información IBM, con una infraestructura de terminales 3270 conectados a unidades de control, la opción de Token Ring disponía en 1994 de numerosas ventajas que convencieron a grandes organizaciones: integración natural apoyada por IBM, mayor velocidad (16 Mbit/s) y rendimiento en red, reducción de riesgo de impacto, etc. No obstante, la mayor estandarización y el menor coste de implantación, han promovido que el mercado convierta a Ethernet en el líder indiscutible de los entornos de red.
2. Red de transporte TCP/IP. La red SILNET II de la Seguridad Social permite disponer de una red homogénea TCP/IP con capacidad para integrar los servicios necesarios para transportar múltiples tipos de datos (incluida la voz) e incorpora ya mecanismos de seguridad y Clase de Servicio en sus enlaces WAN.

3. **Sistemas de Cableado Estructurado.** El cableado de edificios se realizó mediante cable sin apantallar (UTP) que cumpliera las especificaciones de la categoría 5 de ATT (en la actualidad enlaces clase D), para todo tipo de terminales. Esta filosofía ha permitido asegurar la integración de los actuales sistemas Fast Ethernet (100Mbit/s).

Esta situación de las redes ha permitido incorporar de forma natural las nuevas tecnologías y seguir ofreciendo a los usuarios un servicio de alta calidad

Nuevas Tecnologías

Las tecnologías que la GISS ha incorporado en su modelo de red han sido:

1.-Commutación de nivel 2 y nivel 3.

Ethernet es una tecnología half-duplex que ofrece una velocidad de 10Mbit/s, pero que cuenta con los problemas derivados del control de acceso al medio: la pérdida de eficiencia que suponen las colisiones. Cuando ocurre una colisión, los dos equipos entran en una fase de recuperación y retransmiten más tarde, esperando un tiempo aleatorio. Cuantos más equipos se añaden a los segmentos de red Ethernet, más frecuentemente deben esperar antes de iniciar la transmisión, y más frecuentemente se producen colisiones debido a que más equipos intentan transmitir. Este hecho hace que el rendimiento obtenido (throughput) se reduzca a medida que los usuarios transmiten datos más a menudo y durante períodos de tiempo mayores.

Un conmutador Ethernet (Nivel 2) aumenta el ancho de banda disponible, separando los dominios de colisiones y enviando el tráfico de forma selectiva a los respectivos segmentos, lo que permite considerarlo un puente (bridge) multipuerto. Su modo de funcionamiento implica la independencia respecto del protocolo empleado en la red (IP, IPX, ...) y se basa exclusivamente en direcciones MAC (Media Access Control).

Además, si los equipos se conectan a los puertos de los conmutadores, desaparece el concepto de medio compartido y es posible tratar la emisión y recepción de datos de forma simultánea, disponiendo de un acceso full-duplex, y saltando la barrera del modelo half-duplex de Ethernet. Esto permite ofrecer un ancho de banda agregado de 20Mbit/s a los puestos de trabajo.

Cuando el acceso de las estaciones se realiza en IP a otros segmentos de red, los conmutadores de Nivel 2 no aportan una

solución y es necesario recurrir a los router, encargados de dirigir y encaminar el tráfico entre subredes. Sin embargo, los router no aportaban la velocidad ni el rendimiento demandado. Para solucionar este inconveniente, la industria introduce la conmutación de Nivel 3 que no es otra cosa que la funcionalidad de routing junto al alto rendimiento propio de la conmutación de Nivel 2.

La conmutación de Nivel 3 pretende reducir los cuellos de botella generalmente asociados a los router convencionales, algo cada vez más importante a medida que los patrones de tráfico cambian el modelo 80/20 por el nuevo 20/80, forzando a la mayor parte del tráfico a cruzar los límites de la subred. El origen de este cambio reside en la desaparición paulatina de los servidores departamentales y la concentración de servidores en granjas o sistemas cluster de altas prestaciones, a los que todos los usuarios deben acceder desde sus respectivas subredes.

La GISS ha abordado hace tiempo la concentración de servidores en sistemas cluster de altas prestaciones y disponibilidad, agrupándolos en segmentos de red dedicados que permiten optimizar las políticas de gestión y control de acceso. Por este motivo se ha decidido incorporar en el proyecto equipos de conmutación de Nivel 2 y 3.

En cuanto al concepto de conmutación de Nivel 4, no se ha considerado explícitamente en el proyecto debido a la falta de una definición clara y un acuerdo en el mercado sobre dicho concepto, aunque la mayoría de equipos de gama media-alta, que disponen de conmutación de Nivel 3, ofrecen funcionalidades asociadas a la denominada conmutación de Nivel 4.

Básicamente, la conmutación de Nivel 4 es "una extensión del concepto de nivel 3", con la salvedad de que aplica a la conmutación de flujos de paquetes, identificados por características de transporte (puerto local y destino) - Nivel 4- además de las direcciones de red de origen y destino - Nivel 3-. El concepto se basa en que en una trama de Nivel 4 existe "un campo que describe la aplicación que se está transmitiendo en la trama" (por ejemplo FTP lleva el número 21), de forma que la conmutación se realiza a nivel 3 (entre usuarios) y a nivel 4 (aplicación), simultáneamente. De este modo, la comunicación de acceso al correo puede tratarse de forma distinta (mas prioridad, reserva de ancho de banda, es decir, con una calidad de servicio determinado) que una comunicación FTP con el mismo servidor.

2.- VLAN

Una red local virtual (Virtual LAN) es un grupo de servidores, puestos de trabajo o dispositivos de red, que constituyen un segmento de red Ethernet convencional (un mismo dominio de broadcast) sin tener que estar físicamente conectados al mismo Hub. Las VLAN se constituyen sin tener en cuenta su conexión física en la red, es decir, se trata de una asociación lógica de equipos, o dispositivos, pertenecientes a distintos conmutadores que se encuentran distribuidos por la red.

Los usuarios de una VLAN pueden estar distribuidos por una red de campus o en diversas localizaciones geográficas, conectados localmente a una electrónica de red, pero integrados en un "segmento ethernet privado". Las estrategias para determinar estas VLAN pueden ser muy diversas: se pueden realizar de acuerdo a sus departamentos jerárquicos o considerando sus equipos funcionales de trabajo. En general, el objetivo de las VLAN es conseguir una agrupación de dispositivos de tal forma que la mayor parte del tráfico sea local dentro de la VLAN. Mediante una política de VLANs se consiguen beneficios para la red como son: control del broadcast, aumento de la seguridad, mayor rendimiento y facilidades de gestión de red

La Figura I muestra una configuración típica redes locales conmutadas en la que se han definido varias VLANs.

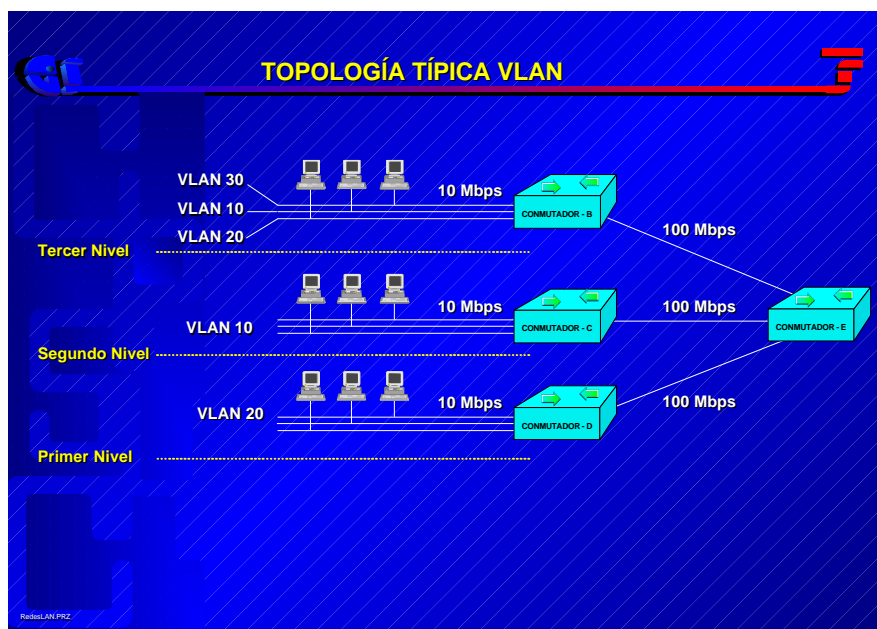


Figura I Topología típica VLAN

Los conmutadores de la figura se comunican entre ellos mediante protocolos de nivel 2 como IEEE 802.10 y el Inter-Switch Link (ISL), permitiendo que una VLAN exista a través de una variedad de equipos que las interconectan.

Requerimientos incluidos en el nuevo modelo de red local.

La nueva electrónica deberá, por tanto, incluir esta tecnología, pero además de ello existen otra serie de requerimientos básicos que también deben ser satisfechos:

- ♦ **Velocidad.** En la actualidad, cada vez son más necesarios los enlaces de 10 Mbps dedicados, e incluso 100 Mbps. En cuanto a los servidores, se hace necesario superar los 100 Mbps para poder atender la avalancha de peticiones en estas redes de alta velocidad.

En esta situación, abordar la inclusión de puertos Gigabit Ethernet es una extensión natural del networking Ethernet 10/100, que proporciona no sólo un ancho de banda incrementado sino también una continuidad en la tecnología empleada (Ethernet), que permite extender las mismas técnicas de administración y control dentro del backbone.

- ♦ **Alto rendimiento y alta disponibilidad.**

El rendimiento de una red depende de la velocidad de envío y de la cuota de pérdida de paquetes del conmutador. La latencia, congestión y bloqueo de cabeza de línea (HOL-Head Of Line) pueden perjudicar el rendimiento, obligando a prestar especial atención a aspectos relacionados con el tipo de matriz de conmutación, la velocidad de conmutación, posibilidad de escalado, la memoria asociada a cada buffer de puerto, el número de colas de calidad de servicio, las direcciones MAC que se mantienen activas en la tabla de consulta del puente, etc.

Mantener altos niveles de disponibilidad exige disponer de módulos y componentes reemplazables "en caliente" y redundantes. Aquellos componentes activos (sometidos a una mayor probabilidad de fallo) así como los que afectan de forma global al equipo, como ocurre con los módulos procesadores y los subsistemas de energía (fuentes de alimentación) deben incluirse en estas categorías.

- ♦ **Clases/Calidad de servicio.**

Clase de servicio (CoS) implica la priorización de tipos de tráfico claramente definidos en la red, permitiendo que, por ejemplo, el personal de atención al público

disponga siempre la respuesta más rápida de la red, con independencia de la aplicación que estén usando.

Mientras CoS implica simple priorización, Quality of Service (QoS) representa un mayor nivel de ancho de banda, así como ciertas garantías de que parámetros del tráfico como el jitter y la latencia van a mantenerse. Esta característica proviene del ámbito de las redes ATM, pero hoy en día están emergiendo protocolos y tecnologías de conmutación que permiten implementarlo en redes ethernet. En este sentido, las técnicas de control de admisión permitirán determinar los privilegios de acceso y ancho de banda antes de que el usuario o la aplicación utilicen la red. En este escenario el IETF (Internet Engineering Task Force) está definiendo dos técnicas, RSVP (Resource Reservation Protocol) y SBM (Subnet Bandwidth Manager).

◆ Gestión.

El networking de alta velocidad supone serios retos para la gestión de red, ya que requiere que más información de gestión sea procesada más rápido. Entre las funcionalidades que deben estar disponibles destacan : gestión de dispositivos, VLANs, gestión de tráfico, instalación de software, seguimiento de cambios en la red y vistas de disponibilidad de los dispositivos.

La gestión debe poder realizarse dentro y fuera de banda (permitiendo disponer de acceso a equipos remotos vía módem o terminal dedicado). Los métodos de gestión dentro de banda (empleando la propia red local para acceder al equipo) se realizan a través de SNMP, cliente Telnet, BOOTP, TFTP (Trivial File Transfer Protocol) y el agente de monitorización remota RMON. El soporte de agentes SNMP y RMON son fundamentales para la integración de los equipos en plataformas de gestión centrales, que no suelen estar asociadas al mismo fabricante de los equipos.

Situación de partida.

La dotación de infraestructura para red de área local en una Dirección Provincial (ya sea de TGSS o del INSS) proviene de un modelo de red normalizado, que la GISS establece a partir del proyecto SILUETA. Este modelo de red, diseñado en 1994, se basa en segmentos de red Ethernet con velocidades de 10 Mbit/s y consta de los siguientes elementos:

1. Un equipo bastidor dotado de elementos redundantes, con capacidad para la conexión de 240 estaciones de trabajo a 10 Mbit/s. Este equipo dispone de 10 tarjetas (cada

- una con capacidad para 24 estaciones) que constituyen el segmento mínimo de red.
2. Las D.P. estructuran sus segmentos de red a partir de este equipo, contando con segmentos de 120 equipos (5 tarjetas por segmento).
 3. El sistema de cableado que conecta este equipo con las estaciones de trabajo cumple las especificaciones de categoría 5, permitiendo la ampliación de la velocidad a 100 Mbit/s.
 4. Los servicios de red se soportan en un servidor Novell que atiende la totalidad de usuarios de la D.P. Este servidor puede disponer de varias conexiones a los segmentos de 10 Mbit/s donde se encuentran los usuarios.

Esta situación representa el 90% de las instalaciones en D.P., ya que para aquellas de mayores dimensiones (Madrid, Barcelona, Sevilla, Valencia,..) cuentan con una configuración distinta. Con objeto de optimizar el acceso en aquellas redes de más de 200 usuarios, se añadieron en 1998 conmutadores de Nivel 2 y un segmento Ethernet a 100 Mbps no conmutado.

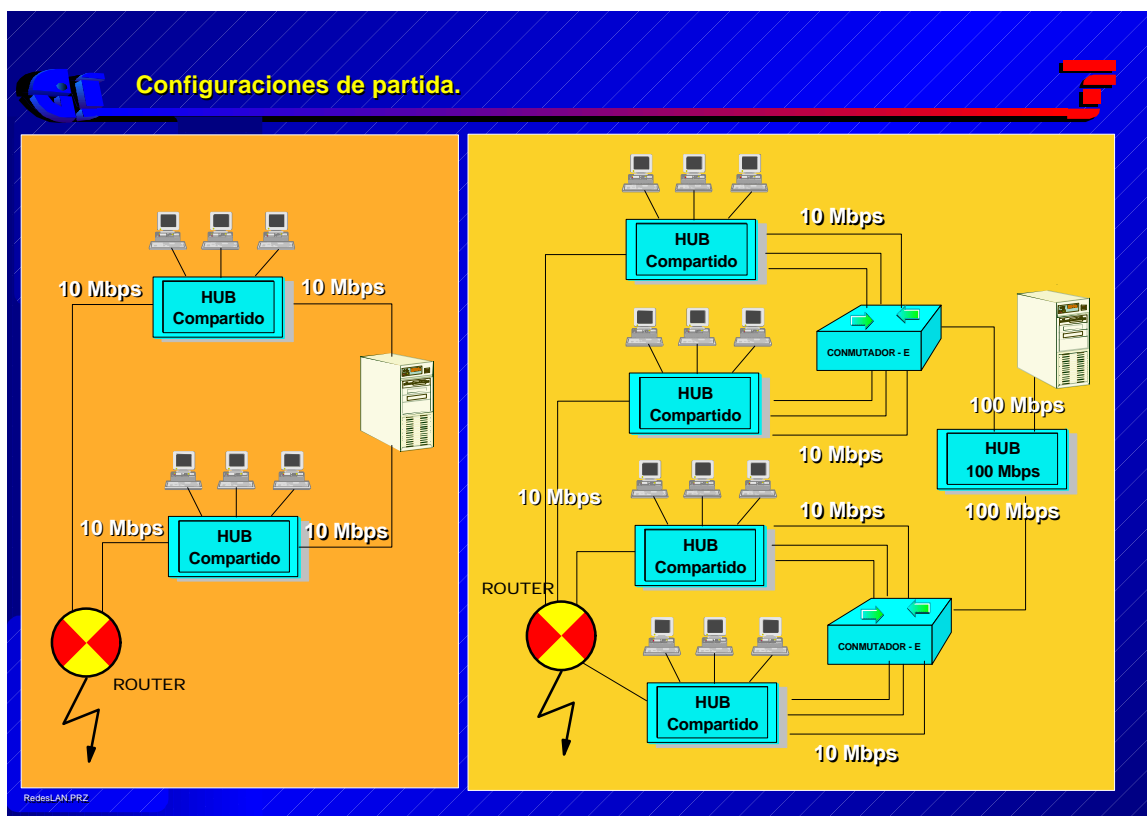


Figura II. Configuraciones de partida.

Como se muestra en la figura, el sistema se basa en tres equipos de sobremesa: dos equipos conmutadores y un Hub a 100 Mbps, por los siguientes motivos:

- a) Dado que los equipos no poseen un elevado rendimiento (debido a la capacidad de proceso y buffer asociados a los puertos) se consigue un balanceo de carga de los usuarios que acceden a los servidores.
- b) Se consigue una configuración que es capaz de soportar la avería de cualquiera de sus elementos. Los conmutadores disponen del 50% de sus puertos libres, permitiendo agrupar las conexiones de usuarios, y pueden interconectarse para recoger las conexiones de los servidores, si falla el Hub a 100Mbps.

Esta configuración permite aumentar el ancho de banda ofrecido a las estaciones de trabajo, pero mantiene a todas las estaciones dentro del mismo dominio de broadcast, al no permitir la creación de VLAN. Además hace necesario mantener múltiples conexiones en los routers, dado que los conmutadores solo consideran el Nivel 2.

Modelo de red local.

El modelo base que se ha establecido en la GISS para dotar de una nueva infraestructura de red de área local a todos los grandes centros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social se ha diseñado de modo que no sea necesaria una renovación inicial de toda la electrónica instalada, y permita una implantación en fases sucesivas. De este modo, se consigue cubrir los objetivos propuestos con un coste de inversión inicial inferior, y aprovechar, cuando se aborde la renovación total, la reducción de costes que ha de producirse en los próximos años. Las dos fases de implantación establecidas son:

- a) Una fase inicial, en la que el 50% de los puestos de trabajo se integran de forma directa en equipos conmutadores 10/100 Mbps, mientras que el resto permanece en segmentos ethernet.
- b) Una fase final, en la que se da cobertura al 100% de los dispositivos de red.

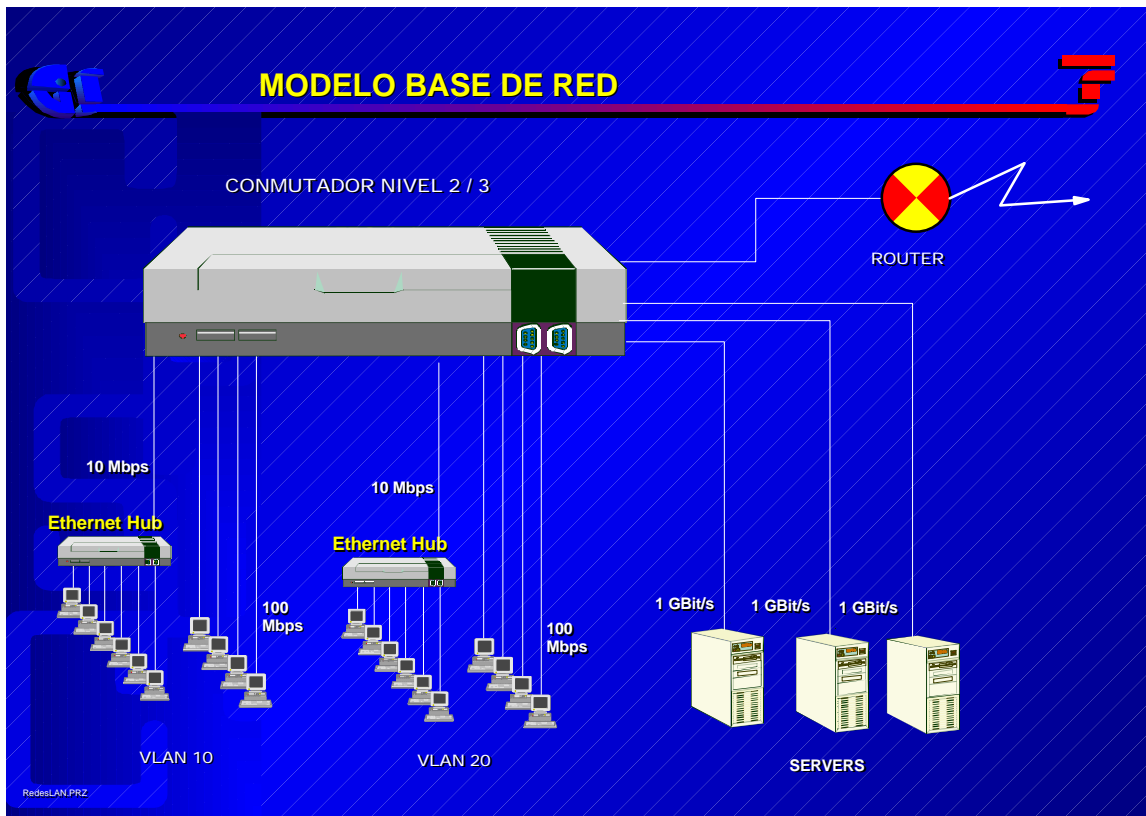


Figura III. Modelo base de red.

La configuración básica de la red de área local propuesta en el modelo constará, tal y como se muestra en la figura III, de los siguientes elementos:

- Un segmento de alta velocidad, que constituirá el troncal de la red (back-bone), trabajando a 1 Gbit/s conmutado, y en el que se ubicarán los equipos servidores (Ficheros, Aplicaciones, Sistemas Documentales, etc.)
- Varios segmentos de red (VLANs), que se corresponderían con los actuales segmentos IP que tienen las Direcciones Provinciales. Estos segmentos estarán formados, en la fase inicial, por:
 1. - Estaciones de trabajo conectadas a 100 Mbit/s. Estos equipos corresponderán a aquellos usuarios que requieren trabajar con sistemas documentales o aplicaciones que manejan grandes volúmenes de datos.
 2. - Segmentos Ethernet compuestos por una tarjeta de 24 puertos con que cuenta el bastidor actualmente instalado. Estos segmentos permiten mantener equipos conectados a 10 Mbit/s, pero mejorando el acceso actual, debido a que los 10 Mbit/s disponibles pasan

a estar compartidos por un máximo de 23 usuarios (una puerta se dedica a la conexión con el conmutador), en lugar de los 120 usuarios con que cuentan los segmentos actuales.

- Los segmentos VLAN, dispondrán de una conexión con el router instalado en la D.P. para permitir su acceso hacia los sistemas instalados en la GISS. Además, dicho router, deberá permitir el Back-up de las funciones de encaminamiento con el sistema conmutador de nivel 3 (IP), de modo que se garantiza una alta disponibilidad del sistema.

Con esta configuración de partida, y contando con equipos bastidores de distinta capacidad, se pretende disponer de un sistema que permita llegar a una situación final en la que todas las estaciones de trabajo dispongan de conexiones a 100Mbit/s Full-Duplex (200 Mbit/s), en el momento en que las necesidades de los usuarios así lo requieran.

Para aquellas D.P. de mayores dimensiones, se ha considerado la necesidad de establecer una configuración redundante, basada en dos equipos gemelos, que se conectan entre sí mediante conexiones en fibra óptica y permiten distribuir la carga. Dichos equipos deberán trabajar en balanceo de carga, y permitirán mantener el acceso a los servidores y el acceso a la GISS para el resto de usuarios del sistema, ante la pérdida total de uno de ellos. (Figura IV)

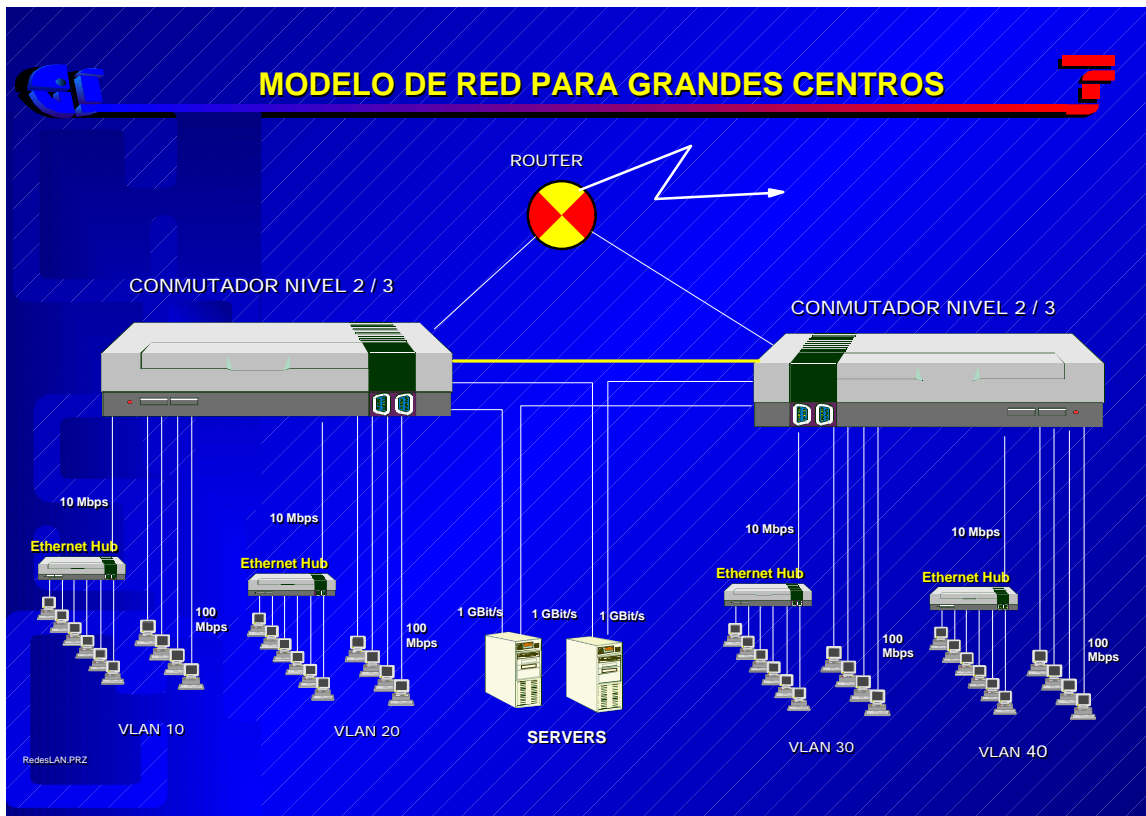


Figura IV: Modelo de red para grandes centros.

Conclusiones.

La Gerencia de Informática de la Seguridad Social ha abordado la renovación de la infraestructura de comunicaciones en red de área local para los grandes centros de gestión de la Seguridad Social, para dotarlos de la infraestructura necesaria para abordar con éxito los nuevos retos del Siglo XXI.

Se trata de dotar a los centros de redes de gran ancho de banda y disponibilidad, que incluyan técnicas de reserva y control del ancho de banda, así como los nuevos mecanismos de calidad de servicio (QoS), que aseguren el ancho de banda necesario para el tráfico crítico y sensible a los retardos. De este modo, no sólo se han incorporado mecanismos para optimizar y garantizar el acceso a los Sistemas de Información actuales, sino que se ha incorporado la tecnología que permitirá añadir los canales de comunicación que han de incorporarse en estos años a los puestos de trabajo: voz y vídeo interactivo.