

XXVI REUNION DE SISTEMATIZACION DE BANCOS CENTRALES AMERICANOS E IBERICOS

La Habana, Cuba, 26 al 30 de octubre de 1998

Proyecto de Interconexión del Banco Central de Cuba

Autor: Ing. Ronny Córdova Díaz

Banco Central de Cuba

Indice

Introducción

Presentación del problema

- Problemas fundamentales a resolver

Solución Propuesta

- Aspectos claves

Selección del equipamiento para las redes locales

Conclusiones

Anexo1

Anexo2

Introducción

El sistema bancario cubano se encuentra en un proceso de automatización que tuvo sus comienzos en 1995. Como parte de este proceso el Banco Central de Cuba (BCC) instaló redes locales en sus diferentes oficinas con el objetivo de realizar el trabajo de la forma más eficiente posible, sacando provecho de las ventajas que brindan los sistemas de computación y el trabajo en redes.

En la actualidad el BCC cuenta con más de 300 computadoras distribuidas en seis edificios. En el momento de instalación de las redes existía un proyecto según el cual en un plazo aproximado de dos años el BCC se mudaría a un nuevo edificio. Por esto se decide instalar redes a 10 Mbps basadas en hubs a modo de experimento y como una vía para ir entrenando a los usuarios en el trabajo en redes. El cableado se hizo usando cable UTP Categoría 5 y topología estrella.

Por diversos motivos la reconstrucción del nuevo edificio del BCC no ha podido ser terminada y se piensa en un plazo de al menos 4 años para su culminación. Por otra parte, las aplicaciones de los usuarios que en un inicio se limitaban al procesamiento local de información se han ido transformando en aplicaciones más intensas en lo referente a la utilización del ancho de banda, lo cual unido a las nuevas aplicaciones basadas en Web y multimedia hacen prever una posible congestión de la red si se continúan utilizando los actuales dispositivos de interconexión.

Teniendo en cuenta esto se toma la decisión de interconectar los diferentes edificios y migrar las redes existentes a 100 Mbps haciendo uso de switches como una vía para aumentar la disponibilidad del ancho de banda.

Presentación del problema

Como se mencionó anteriormente las diferentes redes del BCC están basadas en hubs a 10 Mbps como dispositivos de interconexión. La figura 1 muestra el esquema básico utilizado.

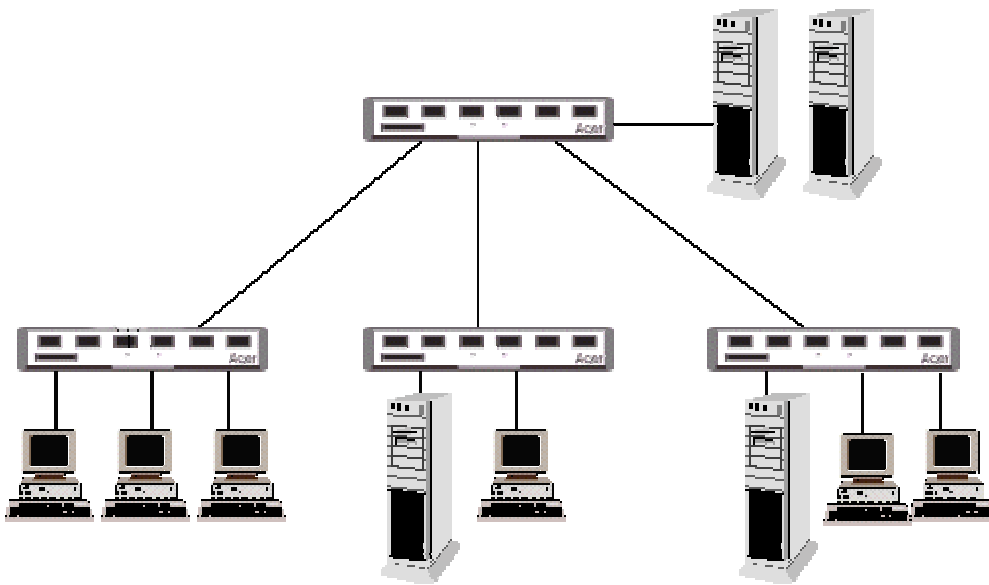


Figura 1: Diagrama general de las redes locales actuales del BCC.

En estas redes coexisten como sistemas operativos Windows NT 4.0 y Novell 3.12. Existen algunos servidores centrales a los cuales tienen acceso todos los usuarios y otros distribuidos en los diferentes departamentos con acceso restringido.

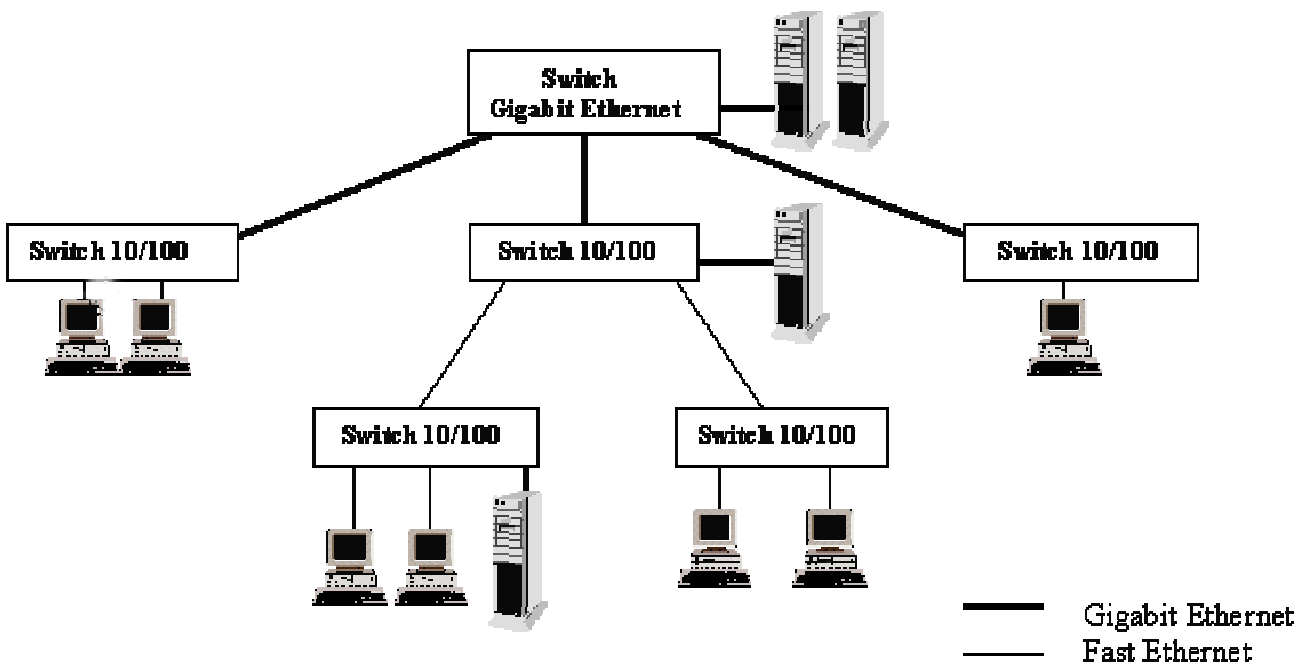
Problemas fundamentales a resolver:

- 1. Tiempo de respuesta lento:** Al usar hubs para realizar la interconexión se comparte el ancho de banda entre todos los usuarios por lo que las aplicaciones tienen que competir entre sí por el ancho de banda disponible. En estos momentos existen varias aplicaciones que son ampliamente usadas y que generan altos niveles de tráfico por lo que la red es generalmente lenta e impide el uso de nuevas aplicaciones. Entre las aplicaciones a introducir en un futuro inmediato se encuentran la educación a distancia basada en Web, los cursos multimedia y la videoconferencia, cada una de las cuales incrementan grandemente los niveles de tráfico.
- 2. Falta de conectividad entre las diferentes redes locales:** De las seis redes locales existentes sólo dos están conectadas mediante cable UTP y una tercera se conecta a las dos anteriores a través de líneas telefónicas

arrendadas, pero sólo con el objetivo de intercambiar mensajería. El resto de las redes no tiene conectividad alguna por lo que se dificulta la transferencia de información entre las diferentes direcciones.

- 3. Dificil administración y gestión de red:** La falta de vinculación entre las redes genera a su vez nuevos problemas. La administración de la red se torna compleja, debiendo desplazarse el personal técnico de una red a otra para diagnosticar los problemas y realizar tareas administrativas, a la vez que los dispositivos de interconexión usados no son compatibles SNMP por lo que resulta muy difícil la gestión de la red.
- 4. Proporcionar una conexión a Internet segura:** Un aspecto importante en la red del BCC es su conectividad con Internet, por lo que representa en cuanto al volumen de información disponible y por los problemas de seguridad que introduce al ser una red pública de alcance mundial. Muchas de las direcciones del BCC trabajan con información de tipo confidencial por lo que es necesario utilizar un sistema de seguridad que proporcione un acceso confiable.

Solución propuesta



En la siguiente figura se muestra el nuevo diseño basado en switches y Gigabit Ethernet.

Aspectos claves:

- 1. Uso de switches como dispositivos de interconexión en las redes locales:** Para solucionar los problemas anteriores y soportar las aplicaciones actuales y futuras se propone la utilización de switches para proporcionar ancho de banda dedicado a los usuarios. Los switches deben ser autonegociantes 10/100 Mbps de forma que se pueda realizar la migración de la red de la forma más rápida posible y de forma transparente a los usuarios. Se debe señalar que una buena parte de los usuarios poseen tarjetas de red autonegociantes 10/100 Mbps lo cual permite introducir los switches sin necesidad de realizar muchos cambios en el hardware de los usuarios. Además los switches deben poseer puertos Gigabit Ethernet para realizar la conexión de los servidores centrales. De esta forma se eliminan los posibles cuellos de botella que se crearían si dispusieran del mismo ancho de banda que los usuarios.

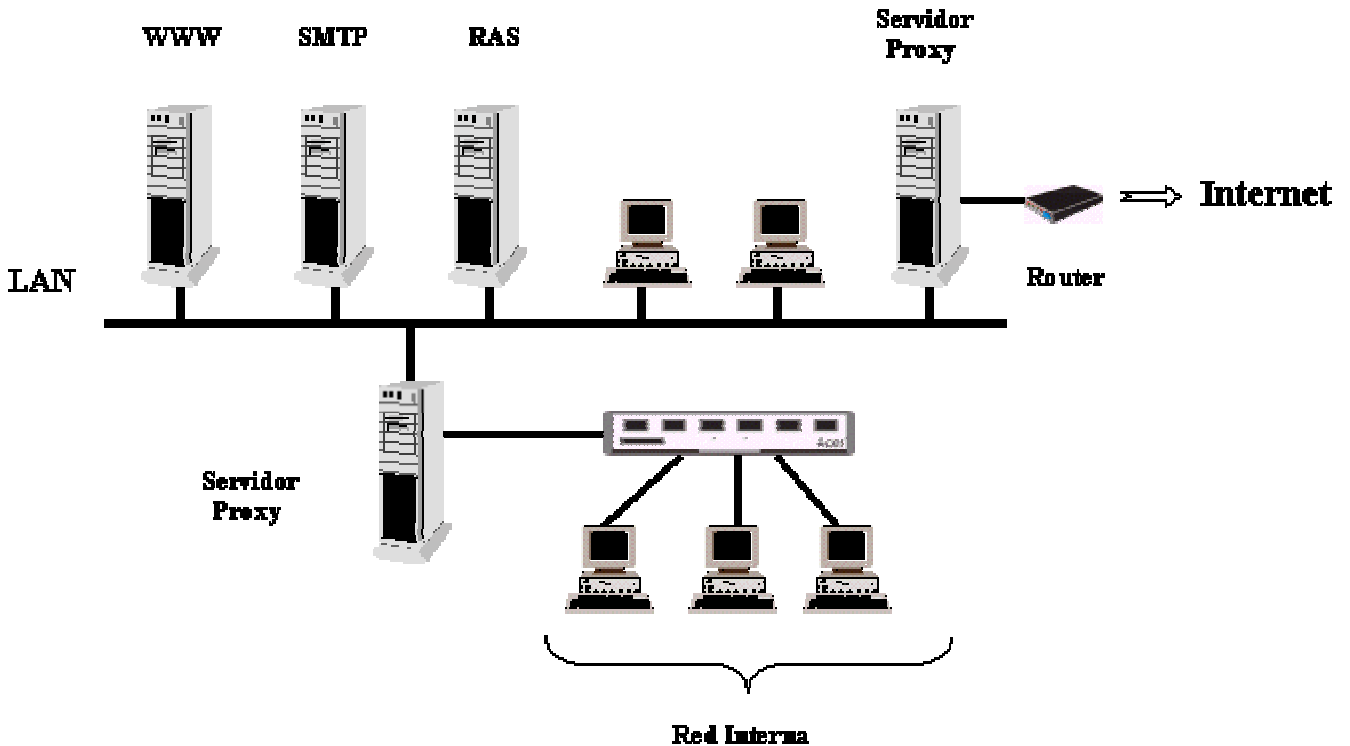
2. **Interconexión de las redes mediante fibra óptica:** se propone la utilización de fibra óptica debido a las distancias existentes entre edificios que imposibilitan la utilización de cable UTP. La aplicación de esta tecnología a las comunicaciones se ha incrementado como consecuencia de la creciente demanda de ancho de banda y el correspondiente descenso de los precios del cableado e instalación. Su uso permite alcanzar mayores distancias, ancho de banda, inmunidad ante las interferencias de tipo eléctrico y seguridad de los datos contra derivación no autorizada. Un switch Gigabit Ethernet proporcionaría ancho de banda suficiente para lograr un backbone de alta velocidad, teniendo en cuenta que los usuarios terminales contarán con conexiones a 100 Mbps dedicadas. El backbone trabajando en modo full dúplex representaría una velocidad de 2 gigabits.
3. **Uso de la tecnología de redes virtuales:** La introducción de redes virtuales es otro de los métodos a utilizar para controlar el tráfico de la red a la vez que ayuda a resolver problemas relacionados con la administración. Las VLANs permite que estaciones de trabajo y otros recursos, incluyendo impresoras y servidores de ficheros, sean organizados en dominios de broadcast lógicos. Si un broadcast es enviado dentro de la VLAN, el mismo llega a todos lo miembros de esa VLAN. Las VLANs representan una solución alternativa a los routers para la contención de broadcast, puesto que permite que los switches se encarguen de controlar este tipo de tráfico.

Algunos de los beneficios de implementar esta tecnología son: .

- Reducción de los costos de movimientos de usuarios: Se simplifica el proceso de adicionar, mover y cambiar usuarios. Usualmente implica personal para el movimiento de computadoras, reconfiguración según la nueva ubicación, cambios en las listas de accesos de los routers y la imposibilidad del usuario de acceder la red hasta que los cambios sean realizados. Las VLANs simplifican este proceso cambiando la relación entre los usuarios y la red. La pertenencia a una VLAN no está atada a la ubicación de las estaciones de trabajo en la red, permitiendo a los usuarios moverse y retener su dirección IP original.
 - Control de broadcast y tráfico multicast: el nivel de tráfico broadcast y multicast es uno de los factores que ponen límite al tamaño de las redes conmutadas. Normalmente los switches no filtran este tipo de tráfico sino que lo replican a todos los puertos, lo cual genera tráfico y consume ancho de banda. El tráfico broadcast de servidores y estaciones en una VLAN particular es replicado sólo a los puertos de los usuarios pertenecientes a esa VLAN.
 - Grupos de trabajos virtuales: miembros de un departamento pueden compartir la misma VLAN. Cuando alguno se mueve hacia una ubicación física diferente y permanece en el mismo departamento no necesita reconfiguración alguna. Contrariamente, un usuario no tiene que cambiar de ubicación para pertenecer a otro departamento, sino que se cambiaría su pertenencia a la VLAN.
 - Seguridad: permite mejorar la seguridad de la red sin recurrir a separar la conectividad física o hacer un uso más complejo de técnicas de firewall basadas en routers. Definiendo los accesos a los servicios de red usando VLANs se puede lograr un alto nivel en el control de la seguridad a la vez que se mantiene una infraestructura de red común.
 - Reducción de la necesidad de routers puesto que muchas de las funciones de los routers pueden ser mas efectivamente manejadas por VLANs, especialmente las relacionadas con el tráfico broadcast y multicast.
1. **Uso de dispositivos compatibles SNMP:** SNMP es un protocolo de administración de redes que permite a través de aplicaciones gráficas tener una visión del comportamiento de la red. Se puede obtener información acerca del estado de cada uno de los dispositivos en un momento dado, así como de cada uno de los puertos en los switches, permitiendo un monitoreo extremo a extremo. También se pueden obtener patrones del tráfico en la red lo cual es muy útil para el diagnóstico de problemas.
 2. **Utilización de Microsoft Proxy Server 2.0 para la protección de la red en la conexión a Internet:** El mismo es un servidor de caché con funciones de firewall incorporadas por lo que además de mejorar el

acceso a Internet y usar más eficientemente el ancho de banda proporciona un buen sistema de seguridad. A continuación explicaremos algunos detalles del esquema de seguridad adoptado y de la estructura de la red.

Figura 3: Esquema de conexión a Internet usando MS Proxy 2.0.



La característica fundamental de los servidores proxy es que actúan como intermediarios entre los usuarios e Internet. Los mismos procesan las solicitudes de los clientes y hacen la búsqueda de información en Internet, retornando los resultados al usuario que los solicitó. La asignación de direcciones IP se simplifica debido a que la única dirección válida es la que utiliza el servidor proxy. Las direcciones internas son enmascaradas brindando un mayor nivel de seguridad.

En el sistema implementado por el BCC se usa un primer servidor proxy el cual se conecta directamente a Internet a través de una línea arrendada de 64 Kbps. Detrás de este servidor se encuentran los servidores de correo, WWW y RAS y un segundo servidor proxy, que a través de un mecanismo de autenticación entre servidores proxy, brinda acceso a Internet a los usuarios de la red.

Esta configuración se adapta perfectamente a la implementación de dominios en Windows NT. Se crean dos dominios diferentes, uno para los usuarios internos y otro para ubicar los servidores que brindan servicios a Internet. Entre estos dos dominios existe una relación en la cual los usuarios de la red interna tienen acceso al dominio externo pero de este dominio no se tiene acceso al interno. Los usuarios de Internet para acceder los servicios de WWW, FTP, etc., que sean ofrecidos por el Banco Central, tienen que hacerlo a través del primer servidor proxy cumpliendo con las medidas de seguridad impuestas por este, sin concedérceles acceso a la red principal. Si ocurre alguna violación de la seguridad impuesta por el primer servidor proxy entonces el atacante debe burlar un segundo servidor por lo que la penetración de la red se hace más difícil.

Ventajas de usar Microsoft Proxy Server 2.0

- Permite extender el acceso a Internet a todos los usuarios en la red interna. Es compatible con la mayoría de los protocolos usados en Internet y soporta el uso de IPX/SPX y TCP/IP en la red interna. Entre las aplicaciones soportadas incluye HTTP, FTP, Telnet, Gopher, IRC, POP3, SMTP y NNTP.
- Acceso seguro: Previene el acceso no autorizado a la red interna y elimina la necesidad de conectar los clientes directamente a Internet. Técnicas de filtrado de paquetes y alertas proporcionan mayor seguridad. Se puede configurar el server para conceder acceso a Internet basado en usuarios, servicios o dominios IP.
- Caché distribuida: permite distribuir el contenido de caché entre múltiples servidores proxy haciendo un balance de carga a la vez que proporciona tolerancia a fallos. Puede ser implementado usando arreglos de servidores, servidores en cadenas o combinaciones de ambos.

Es necesario señalar que el sistema de caché ha presentado algunos problemas en su implementación en el BCC. Debido a los problemas con la velocidad de acceso a Internet, en ocasiones la información no llega completa y al ser almacenada en el caché del proxy posteriores intentos de obtener la información correcta se ven frustrados al ser servidos de la información errónea almacenada.

Funciones de Firewall

- Filtrado de paquetes dinámico: soporta filtrado de paquetes de entrada y de salida determinando de forma dinámica cual paquete puede pasar a la red interna. Esta característica abre los puertos automáticamente manteniéndolos abiertos sólo el tiempo que dure la comunicación, lo cual minimiza el número de puertos expuestos en cualquier dirección.
- Alerta y registro de eventos: suministra notificaciones casi inmediatas si la red se encuentra bajo ataque de forma que pueda ser tomada una acción. Permite mantener un registro completo de los eventos de seguridad.
- Publicación Web: en conjunto con Internet Information Server permite la publicación de información en Internet sin mayores riesgos de comprometer la seguridad, permitiendo la ubicación de los servidores Web detrás del servidor proxy.

Selección del equipamiento para las redes locales

Basado en los aspectos analizados anteriormente se realizó la selección del equipamiento. Se tomaron en cuenta productos de 3Com, Accton y RADLAN, siendo seleccionado el switch Apollo Pro de RADLAN.

El modelo específico es el Apollo Pro 2401, un switch de nivel 3 con 24 puertos autonegociantes 10/100 Mbps y un puerto Gigabit Ethernet. El mismo soporta enrutamiento de paquetes IP e IPX con dos métodos de enrutamiento: paquete por paquete (el método de los routers tradicionales) y "cut-through" (enruta el primero y conmuta los siguientes), posee un sistema de firewall por puerto para aumentar la seguridad del sistema y soporta la tecnología de redes virtuales. Además puede ser apilado y es compatible SNMP permitiendo el monitoreo extremo a extremo.

En una primera etapa se realizará la migración a 100 Mbps y posteriormente la interconexión de las diferentes LANs a través de un backbone de fibra óptica usando el switch Enterprise-5000, el cual posee 8 puertos Gigabit Ethernet.

Conclusiones

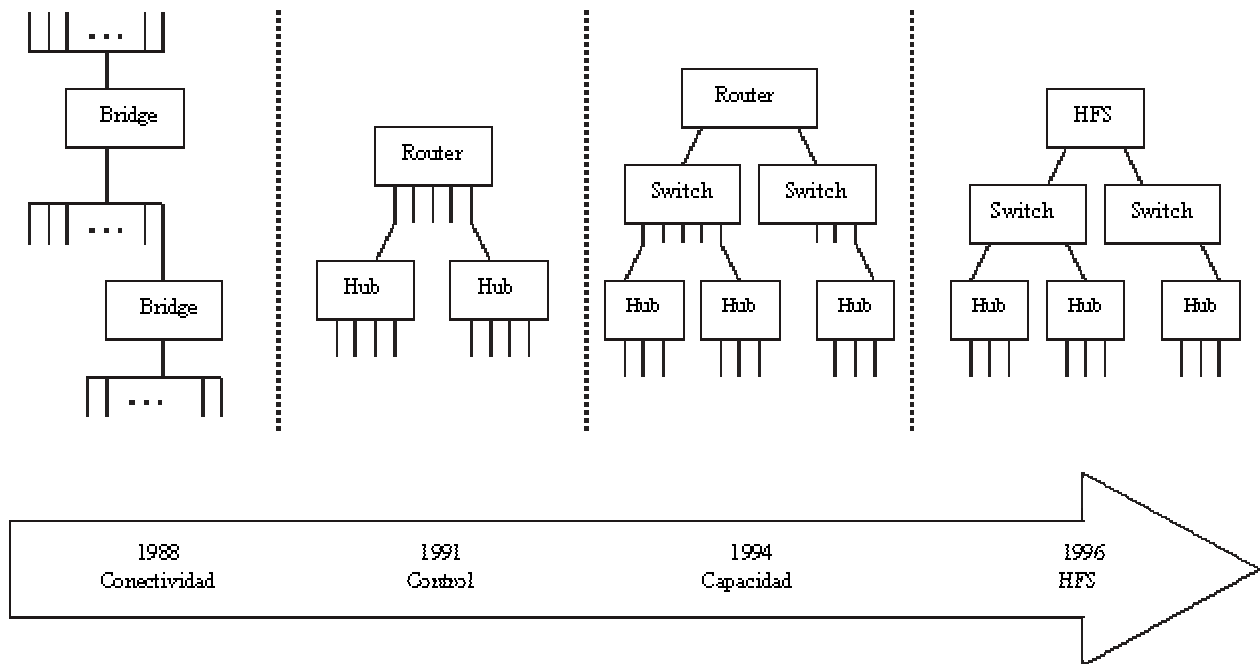
Las redes actuales necesitan mayor disponibilidad de ancho de banda para soportar la amplia gama de aplicaciones basadas en Web y tecnología multimedia que cada vez ganan más aceptación. Estas aplicaciones producen un nivel de tráfico en la red que puede llevar a la congestión si no se cuenta con los dispositivos de interconexión adecuados. La utilización de switches para la implementación de redes conmutadas y la introducción de las redes virtuales parecen ser la solución a estos problemas. Las mismas brindan soluciones para el control del tráfico en la red y hacen más fácil la administración. En particular la utilización de switches debe tenerse en cuenta como una vía de migración hacia tecnologías de altas velocidades y para aumentar el rendimiento de las redes.

Anexo 1

Evolución de las redes

La complejidad de las redes ha aumentado ampliamente desde las primeras redes basadas en puentes (bridges), hasta las redes jerárquicas usando routers y hubs. En años recientes los switches han sido añadidos para resolver los requerimientos de ancho de banda.

Figura 4: Desarrollo de los dispositivos de interconexión de redes.



A principio de los 90 se comenzó a sustituir los puentes con routers multipuerto para segmentar las redes a nivel 3 y contener el tráfico de broadcasts. En esta configuración los segmentos y los dominios de broadcast se relacionan 1:1 y cada segmento contenía entre 30 y 100 usuarios. Con la introducción de los switches se dividieron las redes en menores segmentos incrementando el ancho de banda por segmento y los dominios de broadcast abarcaron múltiples segmentos conmutados soportando 500 ó más usuarios por dominio. El desarrollo de los switches continuó dividiendo la red en mas segmentos con menos usuarios por segmentos.

Conjuntamente con la aceptación de los switches de nivel 2, otros dos factores se fueron desarrollando: la migración de los servidores distribuidos a servidores centrales con el objetivo de aumentar su seguridad y protección contra fallos y el desarrollo de las intranets y comunicaciones cliente/servidor basadas en la tecnología Web. Estos factores comenzaron a mover datos fuera de las subredes locales, por lo que las limitaciones de los routers se evidenciaron cada vez más. La clásica relación entre el tráfico local y remoto se invirtió y pasó a ser de 20:80.

En los últimos años la necesidad de ancho de banda ha aumentado rápidamente. La proliferación de broadcasts y multicast unido con el déficit en la capacidad de la red, han creado problemas significativos. Cuando la demanda excede la capacidad del ancho de banda se producen pérdidas de paquetes reduciendo la eficiencia y confiabilidad de la red. Muchos switches convencionales, a pesar de incrementar la capacidad, no proporcionan contención de broadcasts. Como resultado los usuarios de la red sufren de congestión, inadecuado acceso a los servidores y tiempos de respuesta lentos.

Para enfrentar estos problemas surgen los llamados "High Function Switches", diseñados sobre la base de circuitos integrados específicos de aplicación (ASIC) y arquitectura RISC.

Algunas de sus funciones claves son: escalabilidad, control de tráfico, tolerancia a fallos, administración extremo a extremo, tecnología de nivel 2 y 3, implementación de VLANs, servicio multicast y control de broadcast.

Anexo 2

Uso de switches como dispositivos de interconexión

Los switches son dispositivos diseñados para incrementar el rendimiento de las redes, facilitando la segmentación. Son capaces de tomar decisiones inteligentes acerca de hacia donde debe ser enviado un paquete y mantienen la comunicación entre dos usuarios apartada del resto de los usuarios de la red. Debido a que los switches pueden ser implementados sin cambiar adaptadores, cableado, hubs, etc., la inversión que se ha hecho en una red puede ser preservada, a la vez que son transparentes a los usuarios.

En esencia, un switch es un puente multipuerto de baja demora que crea segmentos separados. Son utilizados para proporcionar ancho de banda dedicado a cada usuario o servidor en redes Ethernet y Token Ring, y para la transición a tecnologías de alta velocidad, tales como Fast Ethernet, Gigabit o ATM.

Los Switches pueden ser usados para:

- Interconectar elementos de un sistema distribuido.
- Proporcionar conexiones de alta velocidad al backbone de la red y a los servidores.
- Aumentar el ancho de banda adicionando más puertos conmutados.

Por todas estas razones, los switches han emergido como la mejor solución para incrementar el ancho de banda, los niveles de eficiencia y reducir los costos.

Switches de nivel 3

El término nivel 3 se refiere a la forma en que la tecnología de redes es separada en 7 niveles en el modelo de referencia OSI.

En el primero de los niveles se encuentra el nivel físico, donde se definen las especificaciones para la conexión mecánica y eléctrica entre los dispositivos. Encima de este nivel se encuentra el nivel de enlace o nivel 2 en el cual operan usualmente los switches. En este nivel cada paquete de información contiene la dirección física de su destino y el switch usa esta dirección para dirigir los datos a la red correcta independientemente del protocolo usado.

En el nivel 2 no hay nada relacionado con subredes o máscaras de dirección. Esta información es definida en el nivel 3, también conocido como nivel de red, en el cual se añade la información relacionada con el protocolo que se esté usando. Es en este nivel que operan los routers.

El término router es usualmente asociado con bajo rendimiento, puesto que su operación fundamental es compleja y siempre será de menor eficiencia que un switch. El proceso de mover paquetes de un puerto a otro sobre un router es mucho más complejo que el mismo proceso en un switch.

Cuando un paquete es recibido por un router todos los campos de información MAC son eliminados puesto que no se utilizan en la lógica de enrutamiento. El router debe identificar que protocolo contiene el paquete. Cada protocolo de nivel 3 tiene un formato único y sus propias reglas de enrutamiento. Una vez identificado el protocolo se determina el destino a través de tablas de enrutamiento y se pueden aplicar listas de acceso u otras reglas al paquete. Cuando se completa toda la operación interna el router construye un nuevo paquete a nivel MAC y realiza la entrega. Este proceso debe ser repetido para cada paquete enviado a cualquier interfaz del router.

Los switches de nivel 3 combinan la velocidad de conmutación de un switch de nivel 2 con las capacidades de enrutamiento de nivel 3. Toda la comunicación es hecha a nivel 2 basada en direcciones MAC. Un switch de nivel 3 se comunica con un router WAN usando protocolos de enrutamiento estándar como RIP y OSPF.

Los dispositivos de nivel 3 permiten aplicar mecanismos para alterar el encaminamiento normal de un paquete. Ejemplos comunes incluyen seguridad y balance de carga. Nuevas características incluyen QoS (Quality of Service), una forma de asignar ancho de banda y controlar las demoras en la propagación, en adición a CoS (Class of Service), un método para la priorización de varios tipos de tráfico. QoS y CoS no sólo son un medio de posibilitar las nuevas aplicaciones multimedia, sino que aseguran el tiempo de respuesta de la red para aplicaciones críticas tales como telemedicina. Estas características implementadas por dispositivos de red inteligentes, como los switches de nivel 3, permiten la integración de voz, video y datos sobre la misma infraestructura, un proceso llamado convergencia.