UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE REDES LAN REDUNDANTES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JAIME LUIS PARDO ALTUNA

PROMOCIÓN
1989-II
LIMA-PERU
2003

Dedico este trabajo a:
Mis padres por su apoyo incondicional,
Mi Esposa e hijas por su comprensión y paciencia.

DISEÑO DE REDES LAN REDUNDANTES

SUMARIO

El presente trabajo pretende presentar las pautas para el diseño de redes de alta confiabilidad y disponibilidad para mantener las redes de las empresas siempre operativas de acuerdo a las exigencias de productividad requeridas en el mercado competitivo de hoy.

En el capítulo I se hace una breve descripción de los componentes de una red LAN.

El capítulo II nos permite revisar los principales tecnologías usadas en la redes LAN, las cuales son estándares usados por la gran mayoría de fabricantes y nos ayudaran a tener las herramientas para el diseño de las redes.

El capítulo III se visualiza algunos ejemplos y pautas para diseñar redes en edificios o campus de acuerdo a las exigencias actuales de diseño.

El capítulo IV se refiere a identificar cuales son los componentes mas críticos de una red, el no funcionamiento de estos hará que la red deje trabajar y brindar servicio a los usuarios de la misma.

El capítulo V nos muestra cuales son los componentes que tienen redundancia en los equipos principales de una red, las mismas que han sido tomados en cuenta por la gran parte de los fabricantes de equipos de comunicaciones.

En el capítulo VI se dan las pautas para el diseño de redes redundantes.

Por último en el capítulo VII se dan ejemplos de costos para implementar redes alta confiabilidad y disponibilidad.

ÍNDICE

PRÓLOGO

A través de los tiempos, el manejo adecuado y oportuno de la información le ha permitido al ser humano tomar decisiones para satisfacer sus necesidades, con el uso de las computadoras surgió la necesidad de compartir información dando origen a las redes LAN que conocemos hoy en día. Estas redes han ido evolucionando a través de las últimas décadas siendo una de las partes más importantes en la productividad de las empresas debido a la gran demanda de aplicaciones, servicios ofrecidos y manejo de información entre los usuarios de una compañía. En este sentido el uso y acceso a los datos a través de las redes LAN se han vuelto de gran importancia para mejorar la productividad de las Empresas.

Este trabajo pretende darnos las pautas para el diseño de redes LAN que sean de alta disponibilidad a través del reforzamiento y redundancia de los elementos críticos de la Red.

CAPÍTULO I

DEFINICIÓN DE LOS COMPONENTES DE UNA RED LAN

1.1. INTRODUCCIÓN

Las redes LAN (Local Area Network) surgieron como necesidad para compartir información entre usuarios de computadoras, en este capítulo describiremos los diferentes componentes que la integran así como sus topologías y protocolos utilizados.

1.2. COMPONENTES DE LA RED LAN

La red LAN es un sistema de transmisión de información con el objetivo de compartir recursos con los que trabaja un ordenador normalmente, es decir, archivos, directorios, impresoras, plotters, escáneres, etc.

La palabra local se refiere a que el conjunto de ordenadores se encuentra próximo geográficamente hablando es decir, que se encuentra en el espacio físico de un mismo centro.

En general una red local está caracterizada por una distancia corta entre ordenadores, un medio de comunicación entre éstos, una velocidad de conexión elevada, la utilización de cables de conexión simples (como los coaxiales o los telefónicos). Cuentan con la facilidad de su instalación, de su administración y de su bajo precio. En la mayoría de los casos una red se usa para compartir entre varios ordenadores una unidad de almacenamiento enorme o en general cualquier dispositivo periférico del que hagan uso varias personas de un mismo grupo de trabajo, de esta forma no es necesario comprar ese periférico para cada ordenador, por ejemplo una impresora láser. Además constituye un valor añadido a la hora de compartir la información y distribuir tareas tal como se muestra en la figura 1.1.

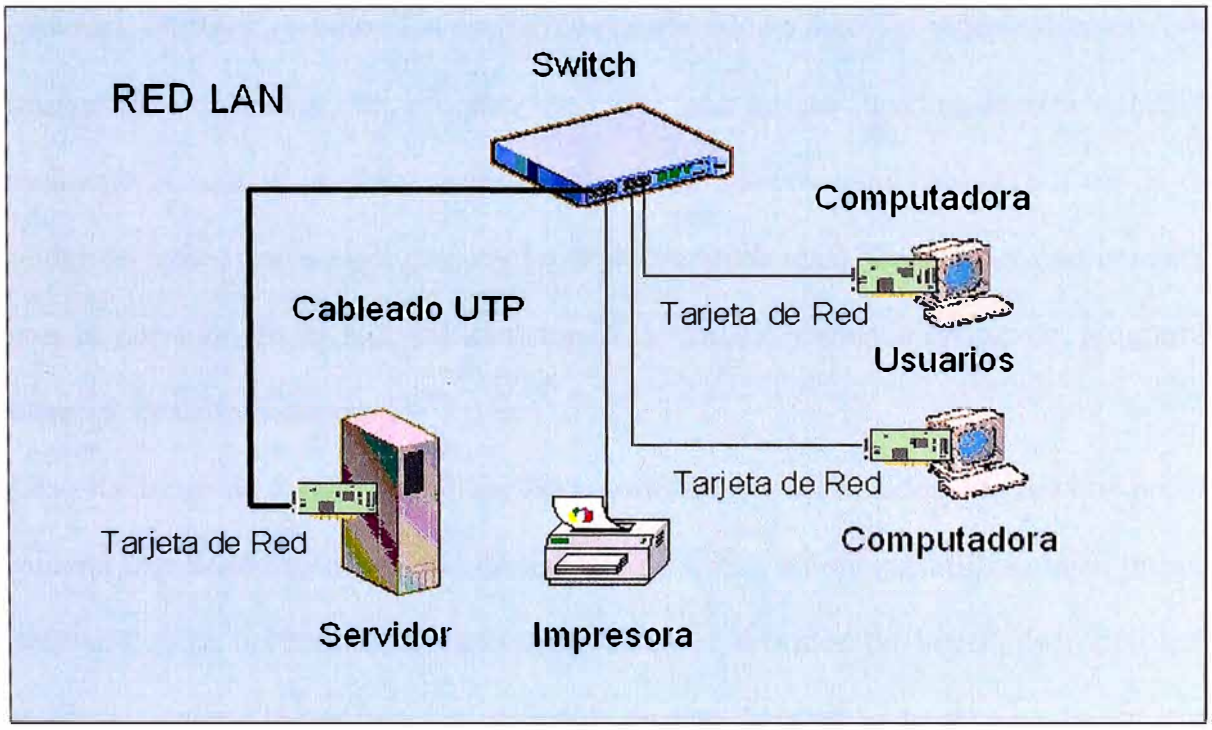

Figura 1.1 - Componentes de la red LAN

1.3. DESCRIPCION DE LOS COMPONENTES DE LA RED LAN

A continuación se hace una descripción de los principales componentes que integran una red LAN:

NODO:

Nodo es un término que se emplea en al ámbito de los grandes ordenadores (mainframes) y que en realidad a lo que se refiere es al principio, al final, o a la intersección de un enlace de comunicaciones, no a un dispositivo específico.

ESTACION DE TRABAJO:

El término estación de trabajo describe cualquier microordenador, ordenador personal, terminal, y todos los periféricos conectados a éstos, o independientes (una impresora, un módem, un escáner, etc.) con una tarjeta interfaz de red instalada mediante la cual se puede acceder al servidor a través de los cables (o a través de ondas de radio, como es el caso de las redes inalámbricas). Para poder comunicarse con el servidor de la red, las estaciones de trabajo deben ejecutar un programa especial de comunicaciones.

Las estaciones de trabajo suelen ser microordenadores conectados a la red que por la general mantienen su capacidad de trabajar de forma autónoma utilizando su propio software, pero normalmente están conectadas al servidor de la red de modo que pueden acceder a la información contenida en éste. Para poder hacer esto, la estación de trabajo necesita un interfaz especial que se conecta a una de las ranuras de expansión de la estación, y al que se conecta un cable que lo enlaza con el servidor.

SERVIDOR DE UNA RED LAN:

Hemos visto que una red local interconecta ordenadores, comparte dispositivos, pero para compartir eficientemente periféricos tales como discos duros o impresoras, es necesario configurar uno o más ordenadores como "gestores". Un gestor (también llamado servidor) es un ordenador que comparte sus periféricos con otros ordenadores. Un servidor de discos permite compartir zonas del disco. Un servidor de impresión es un ordenador que pueden utilizar todos los usuarios, y que se encarga de volcar el contenido de archivos en una impresora.

SERVIDOR DE DISCO (DISK SERVER):

Al principio las redes utilizaban un servidor de disco donde se almacenaba la información que iban a compartir las distintas estaciones de trabajo de la red. Para éstos el servidor es simplemente otra unidad de disco duro donde almacenar archivos. En el caso de un PC funcionando bajo Windows la unidad asignada del servidor de archivos es como un disco normal del que se mantiene una tabla de asignación de ficheros (FAT o file allocation table) propia para poder saber exactamente donde se encuentra un determinado archivo.

Lo de "propia" significa que el servidor de archivos contiene varias particiones, cada una de ellas asignada a un usuario. Esto se hace para que cuando el PC necesite leer un archivo, lea la FAT de la partición que le ha sido asignada y busque en ella el archivo que necesita. Una vez modificado lo graba en el disco grabando la FAT en la partición asignada. De no ser así, podría darse el caso de que varios usuarios accediesen a grabar la FAT, que en cada caso sería distinta, produciéndose un complicado galimatías indescifrable y se perderían todos los datos.

Algunas particiones pueden definirse como públicas, pero normalmente suelen definirse como de sólo lectura de modo que no puedan modificarse. Todas las estaciones pueden acceder a esta información pero no pueden cambiarla. Un ejemplo de partición pública podría ser una base de datos de consulta.

Hay dos tipos de servidores de disco: dedicados y no dedicados. Normalmente los servidores dedicados no disponen de monitor, ni teclado; para lo único que sirven es para dar servicio a las solicitudes de otros ordenadores de la red. Los servidores no dedicados son ordenadores normales que tienen conectado un disco duro o impresora, y que al igual que los dedicados dan servicio a la red, con la diferencia de que se puede utilizar como un ordenador normal mientras actúa de servidor.

SERVIDOR DE ARCHIVOS (FILE SERVER):

Un servidor de archivos es mucho más eficiente y sofisticado que un gestor de disco. Contiene software especial que procesa comandos antes de que el sistema operativo los reciba. El servidor de archivos contiene su propia FAT. Cuando una estación de trabajo pide un determinado archivo, el servidor de archivos ya sabe donde está el archivo y lo envía directamente a la memoria de la estación de trabajo. En este caso para la estación de trabajo el servidor de archivos no es otra unidad de disco más, como sucede con el servidor de disco. Es mucho más eficiente porque no necesita enviar una copia de la FAT a la estación que pide un archivo, y además no es necesario seccionar la unidad de disco.

El servidor de archivos se encarga de que en un momento dado, sólo hay un usuario utilizando un archivo determinado. Los usuarios pueden trabajar como si tuvieran un

disco de gran capacidad conectado a su ordenador. Cualquiera puede tener acceso a los archivos, a no ser que se establezcan claves de acceso.

Los servidores de archivos pueden ser de cuatro tipos: centralizados, distribuidos, dedicados y no dedicados.

SERVIDORES DE ARCHIVOS CENTRALIZADOS Y DISTRIBUIDOS:

Para la mayoría de las redes un único servidor de archivos es más que suficiente. Este tipo de servidor se conoce con el nombre de servidor central. Funciona de manera muy similar como lo hace un miniordenador; una unidad se encarga de dar servicio a cada estación de trabajo.

Por razones de eficiencia en ocasiones es conveniente instalar más de un servidor para dar servicio a departamentos distintos. Estos servidores se conocen con el nombre de servidores distribuidos. Esta es una solución más eficiente porque se reducen los tiempos de acceso y además si uno de ellos queda fuera de servicio, la red puede seguir funcionando.

SERVIDORES DE ARCHIVOS DEDICADOS Y NO DEDICADOS:

Un servidor de archivos dedicado es un microordenador con disco duro que se utiliza exclusivamente como servidor de archivos. Dedicando toda su capacidad de memoria, procesamiento y recursos a dar servicio a las estaciones de trabajo se consigue un aumento de la velocidad y eficiencia de la red. Un servidor no dedicado es aquél que se usa, además de para funciones de servicio de archivos, como estación de trabajo. Esto implica que la RAM debe estar dividida de forma que puedan ejecutarse programas en la máquina. Cuanto más rápido sea el microprocesador, más

rápido puede el servidor realizar sus tareas lo que a su vez implica un costo más elevado.

SERVIDORES DE ARCHIVOS DE UNA RED PUNTO A PUNTO:

En una red punto a punto los usuarios deciden qué recursos de su ordenador desean compartir con el resto de los usuarios de la red.

Un usuario puede utilizar su unidad de disco duro como servidor de archivos para otros usuarios de la red. Una red de este tipo puede constar de varias estaciones de trabajo que hacen funciones de servidor de archivos no dedicado cuyos propietarios han decidido compartir con el resto de los usuarios de la red. Esta filosofía es aplicable así mismo a las impresoras y otros dispositivos.

SERVIDOR DE IMPRESIÓN:

Al igual que un servidor de archivos permite compartir un disco duro, un servidor de impresión hace lo mismo, sólo que en esta ocasión lo que se comparten son las ımpresoras.

Cada uno de los ordenadores tiene conectada una impresora. Estas impresoras son suficientes para la mayoría de los trabajos, pero cuando es necesario hacer copias de mayor calidad, los usuarios utilizan la impresora láser conectada al servidor de impresión. El servidor de impresión puede tener varios tipos de impresoras, según las necesidades.

Para poder compartir ımpresoras, el servidor de impresión debe disponer del software adecuado y por lo general contiene lo que se conoce como un spooler de impresión, que es un buffer donde se almacenan los trabajos que cada estación

manda a imprimir. Los trabajos se van poniendo en cola y se imprimen de forma secuencial en orden de llegada. Hay spoolers de impresión con funciones para cambiar el orden de impresión de los trabajos y para indicar la hora en la que se quiere imprimir un determinado trabajo. Por ejemplo, los trabajos que requieren muchísimo tiempo de impresión se ponen en el spooler de impresión para que se impriman fuera de las horas de trabajo.

SERVIDOR DE COMUNICACIONES:

Los servidores de comunicaciones están diseñados para liberar a la red de las tares relativas a la transmisión de información. El servidor de comunicaciones funciona igual que una centralita telefónica, haciendo las mismas funciones que un sistema PABX (centralita automática privada). Por medio del servidor de comunicaciones una estación puede llamar a una red externa o cualquier otro sistema, buscar cierta información y enviarla a la estación que la ha solicitado. El servidor de comunicaciones se puede utilizar también para conectar dispositivos incompatibles a una red.

A pesar de que un servidor de comunicaciones efectúa las funciones de un módem, en particular proporcionando acceso a redes telefónicas de larga distancia, hay bastantes diferencias entre ellos. La mayoría de los módems están conectados a una sola estación y sólo los puede utilizar esa estación. Los servidores de comunicaciones pueden responder a varias solicitudes a la vez. Además el servidor de comunicaciones ofrece más funciones, tales como multiplexación y conmutación, detección de errores, y además es mucho más fiable.

Es de destacar que para redes de unos 12 equipos y con las nuevas tecnologías se puede perfectamente compartir un módem como un periférico más, usando un software específico y diseñado para tal fin, algo muy común hoy día. De esta forma el servidor de comunicaciones no sería necesario, ya que el módem compartido haría todo el trabajo.

1.4. TOPOLOGÍAS DE UNA RED

Nuestro objetivo es conseguir que todos los componentes de la red formen un todo y trabajen sin ningún problema de incompatibilidad, por ello si escogemos componentes hardware del mismo fabricante no tendremos ningún problema. Sin embargo, eso no siempre es posible y por ello existen estándares de software o más conocidos como protocolos, ellos son los que permiten la comunicación entre las distintas redes.

La red local está formada por cables que conectan los ordenadores entre sí y a la forma en que se distribuyen el cableado y los componentes de la red se le llama topología. Existen varias topologías básicas: bus, estrella, anillo y árbol.

TOPOLOGÍA EN BUS:

Existe un solo enlace de comunicaciones que se llama bus al cual están conectados todos los equipos de la red, tal como se muestra en la figura 1.2.

Como el bus es un medio de acceso compartido, sólo un dispositivo de todos los que están conectados al bus puede transmitir en un mismo momento. La comunicación se efectúa troceando la información para evitar que una estación transmita constantemente y las demás no puedan hacerlo.

En los extremos del cable existen unas piezas que se llaman terminadores, que indican el final o principio de la red.

Las conexiones entre la tarjeta de red y el bus se efectúan mediante un conector en forma de T, llamado derivador.

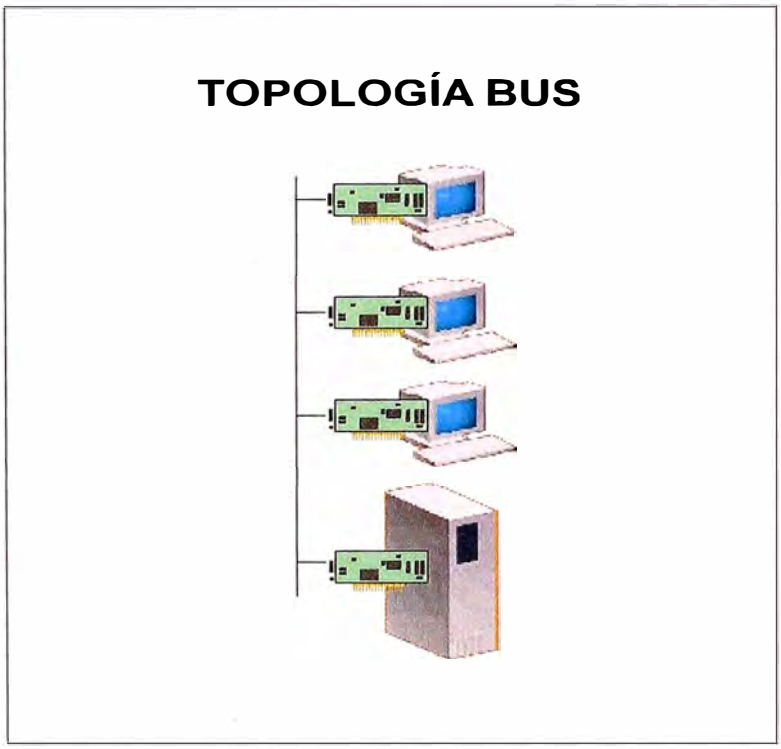

Figura 1.2 – Topología bus

TOPOLOGÍA EN ESTRELLA:

Los enlaces en la red se disponen de forma radial partiendo de un dispositivo central. Este dispositivo radial se conoce como concentrador/Switch. Cada rama de la estrella conecta al dispositivo central con otro periférico. El Switch actúa como central de comunicaciones entre los dispositivos periféricos como se muestra en la figura 1.3.

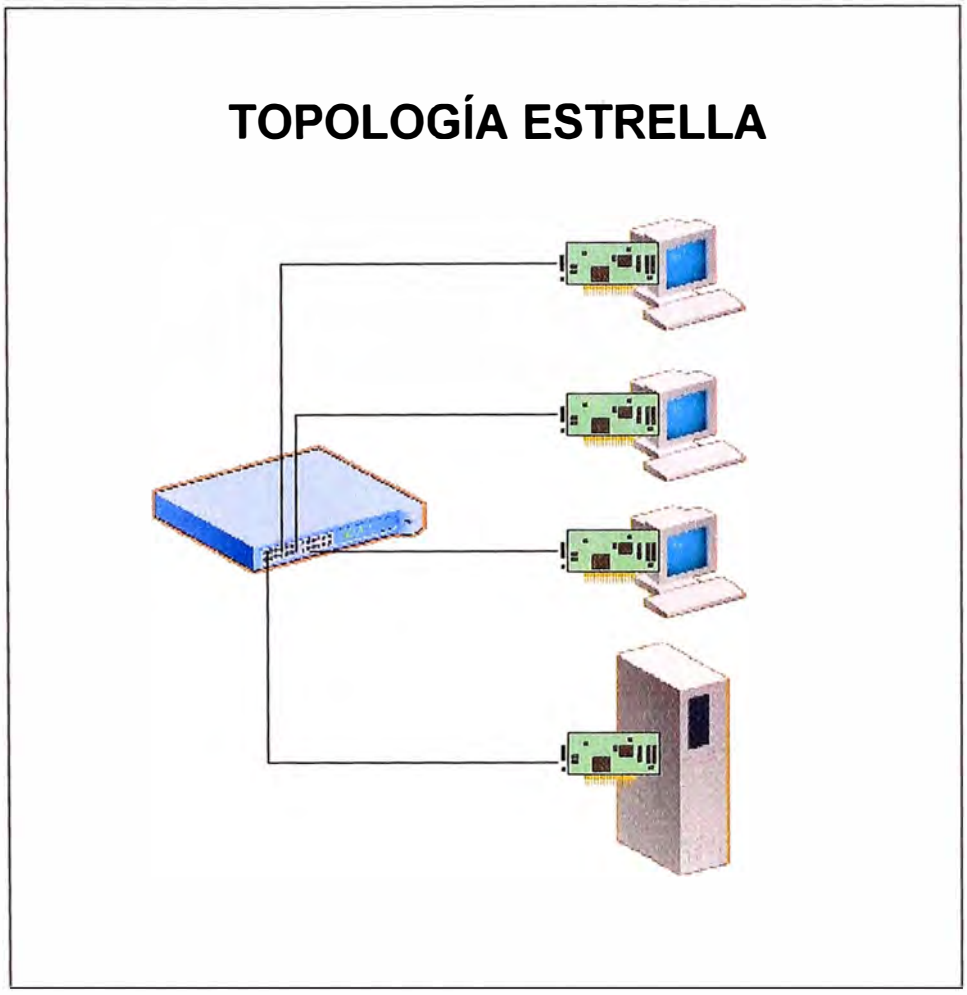

Figura 1.3 – Topología estrella

TOPOLOGÍA EN ANILLO:

Los computadoras se distribuyen alrededor de un anillo formado por el medio de transmisión como se muestra en la figura 1.4. Este anillo está formado por un pequeño repartidor llamado MAU o unidad de acceso a múltiples estaciones.

A diferencia de la topología en bus, en la que la información que un dispositivo dejada en el medio era recibido por todos los integrantes de la red, ahora viaja a su equipo adyacente y si no es para él se lo pasa al siguiente.

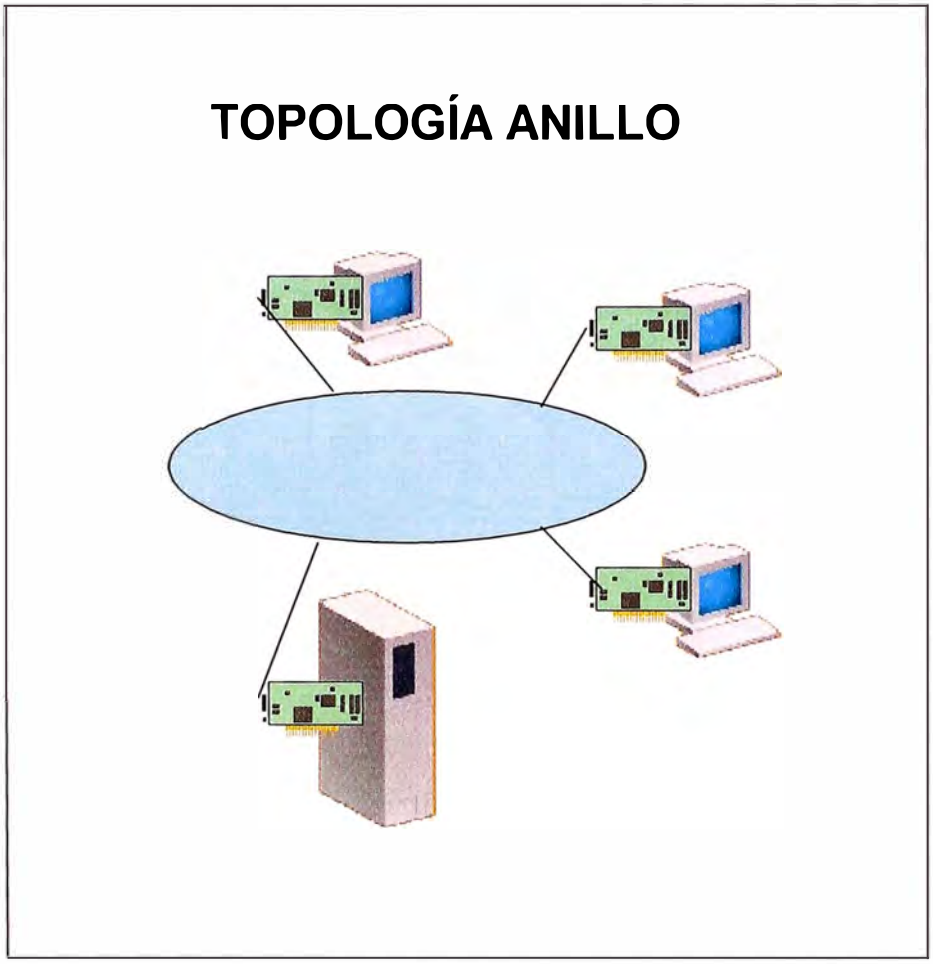

Figura 1.4 – Topología anillo

TOPOLOGÍA EN ARBOL:

Es la combinación de varias redes en estrella, estas redes en estrella se unen a su vez a un dispositivo central del cual se derivan todas las conexiones de los concentradores/switches o conexiones a servidores directamente tal como se muestra en la figura 1.5.

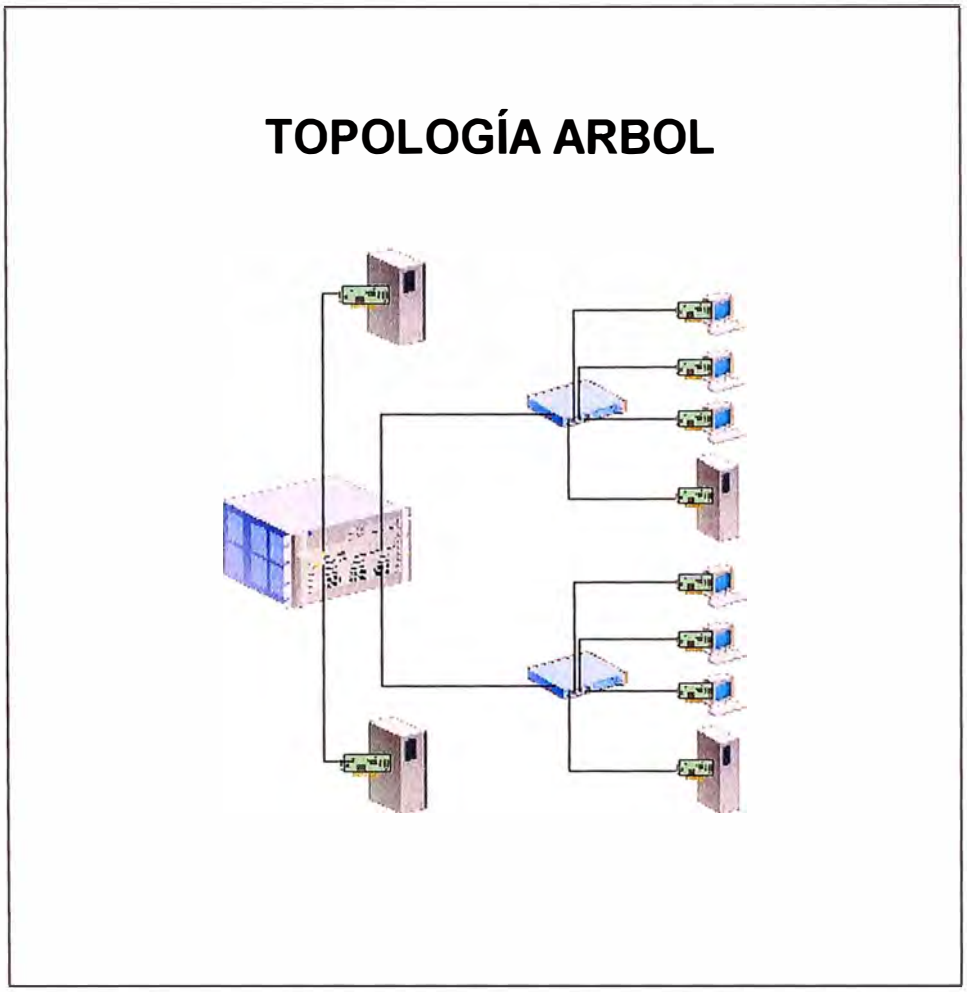

Figura 1.4 – Topología árbol

1.5. PRINCIPALES PROTOCOLOS DE RED

Conjuntos de normas que definen todos los aspectos que intervienen en una comunicación, por tanto definen el formato que van a tener los paquetes de información y las órdenes que un dispositivo va a aceptar.

NetBios: fabricado por Microsoft e IBM y se usa para redes de área local o de área metropolitana.

TCP/IP: siglas de Protocolo de Control de Transmisión/Protocolo Internet, fue desarrollado por el departamento de Defensa para su red de conmutaciones ARPA. Es muy empleado en máquinas UNIX y en redes de área extensa por sus facilidades de enrutamiento.

Tiene la ventaja de tener compatibilidad con todos los sistemas operativos, tecnología capaz de conectar sistemas con protocolos distintos entre sí, por ejemplo Ftp o Telnet, es el protocolo que se usa en Internet.

IPX/SPX: siglas de Intercambio de Paquetes entre Redes/Intercambio de Paquetes Secuencial. Fue definido por la compañía Novell como soporte de sus redes de área local, es plenamente enrutable.

Apple Talk: es la contribución de la compañía Apple a los protocolos, sólo se emplea en este tipo de ordenadores.

Todos los protocolos anteriormente mencionados los soporta Windows NT, Novell soporta su protocolo IPX/SPX.

1.6. TIPOS DE REDES DE ÁREA LOCAL

Ethernet: topología de Bus con cable coaxial grueso o delgado o bien con par trenzado. Velocidad: 10 Mbps.

Token ring: combina la topología en estrella y en anillo y opera en un ancho de banda de 4 o 16 Mbps.

ArcNet: usa una topología en bus o en estrella y generalmente opera a 2,5 Mbps, ArcNet Plus opera a 20 Mbps.

1.7. DISPOSITIVOS DE CONEXIÓN O CABLEADO

CABLE COAXIAL

Consiste en un cable conductor interno cilíndrico separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Esto se recubre por otra capa aislante que es la funda del cable como se muestra en la figura 1.5. Este medio físico, es más caro que el par trenzado, pero se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar mas estaciones.

Se suele utilizar para televisión, telefonía a larga distancia, LAN, conexión de periféricos a corta distancia, etc. Se utiliza para transmitir señales analógicas o digitales. Sus inconvenientes principales son: atenuación, ruido térmico, ruido de ínter modulación. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

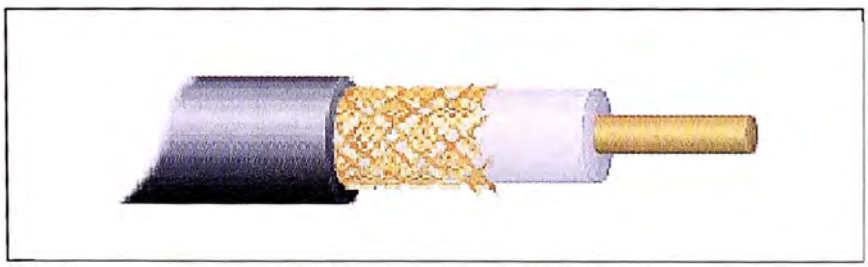

Figura 1.5 – Cable coaxial

CABLE PAR TRENZADO (UTP)

Se trata de dos hilos de cobre aislados y trenzados entre si y envueltos por una cubierta protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no) como se muestra en la figura 1.6. Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer.

Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. Está dividido en categorías por el EIA/TIA

Categoría 1: Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbps.

Categoría 2: Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbps.

Categoría 3: Velocidad de transmisión de 10 Mbps. Con este tipo de cables se implementa las redes Ethernet 10baset.

Categoría 4: La velocidad de transmisión llega a 16 Mbps.

Categoría 5: Puede transmitir datos hasta 100 Mbps. Tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de cambiar el cableado. Además, resulta fácil de combinar con otros tipos de cables para la extensión de redes.

Existen dos tipos de pares trenzados, los *apantallados o STP* y los *sin apantallar o UTP*. Los pares sin apantallar son los más baratos aunque menos resistentes a interferencias. A velocidades de transmisión bajas, los pares apantallados son menos susceptibles a interferencias, aunque son más caros y más difíciles de instalar.

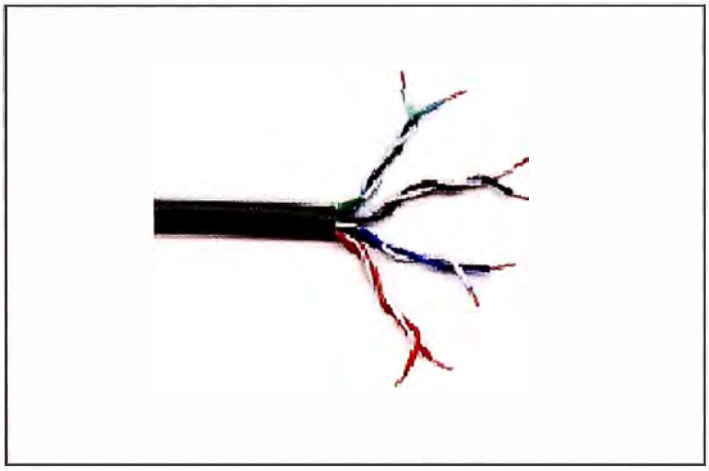

Figura 1.6 – Cable par trenzado

CABLE DE FIBRA ÓPTICA

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de esto está la cubierta, constituida de material plástico o similar, que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc. Como se muestra en la figura 1.7. Sus beneficios frente a cables coaxiales y pares trenzados son:

- Permite mayor ancho de banda.

- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.

Su rango de frecuencias es todo el espectro visible y parte del infrarrojo. El método de transmisión es el siguiente: los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo. Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino. A este tipo de propagación se le llama *multimodo*. Si se reduce el radio del núcleo, el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo, el rayo axial, y a este método de transmisión se le llama *monomodo*.

Los inconvenientes del modo multimodo es que debido a que dependiendo al ángulo de incidencia de los rayos, estos tomarán caminos diferentes y tardarán más o menos tiempo en llegar al destino, con lo que se puede producir una distorsión (rayos que salen antes pueden llegar después). Debido a esto, se limita la velocidad de transmisión posible.

Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama *multimodo de índice gradual*. Los emisores de luz utilizados son: LED (de bajo costo, con utilización en un amplio rango de temperaturas y con larga vida media) e ILD (más caro, pero más eficaz y permite una mayor velocidad de transmisión).

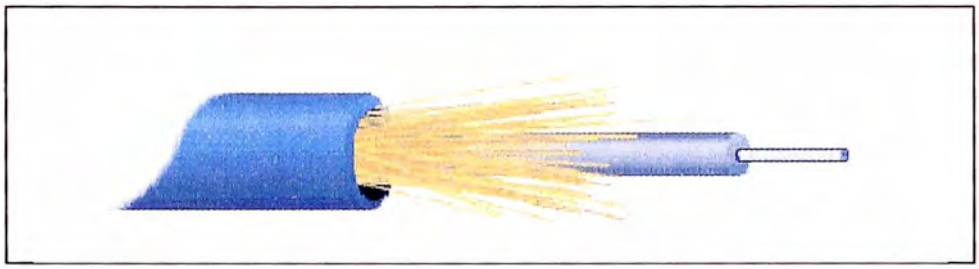

Figura 1.7 – Cable de fibra óptica

CAPÍTULO II

TECNOLOGÍAS EN REDES LAN

2.1 GIGABIT ETHERNET

Gigabit Ethernet es la tecnología de transmitir data a la velocidad de 1000Mbps esta tecnología provee un gran uso del ancho de Banda y es compatible con la tecnología 10/100 Ethernet la cual es la tecnología mas desarrollada y difundida a nivel mundial. Actualmente Gigabit Ethernet provee el mejor costo/rendimiento que otras tecnologías del mercado.

Ethernet es un estándar en redes basadas en paquetes conmutados que soportan velocidades de 10, 100 y 1000 Mbps.

- **IEEE 802.3** 10BASE-T Ethernet sobre cable UTP
- **IEEE 802.3u** 100BASE-T Fast Ethernet sobre UTP o cable de fibra óptica.
- **IEEE 802.3ab** 1000BASE-TX Gigabit Ethernet sobre cable UTP Categoría 5.
- **IEEE 802.3z** Gigabit Ethernet 1000BASE-SX y 1000BASE-LX sobre cable de fibra óptica multimodo y monomodo.

Las tres velocidades de Ethernet usan el mismo formato de trama IEEE 802.3, operación full-duplex y métodos de control de flujo.

En la figura 2.1 se muestran los elementos funcionales de Gigabit Ethernet

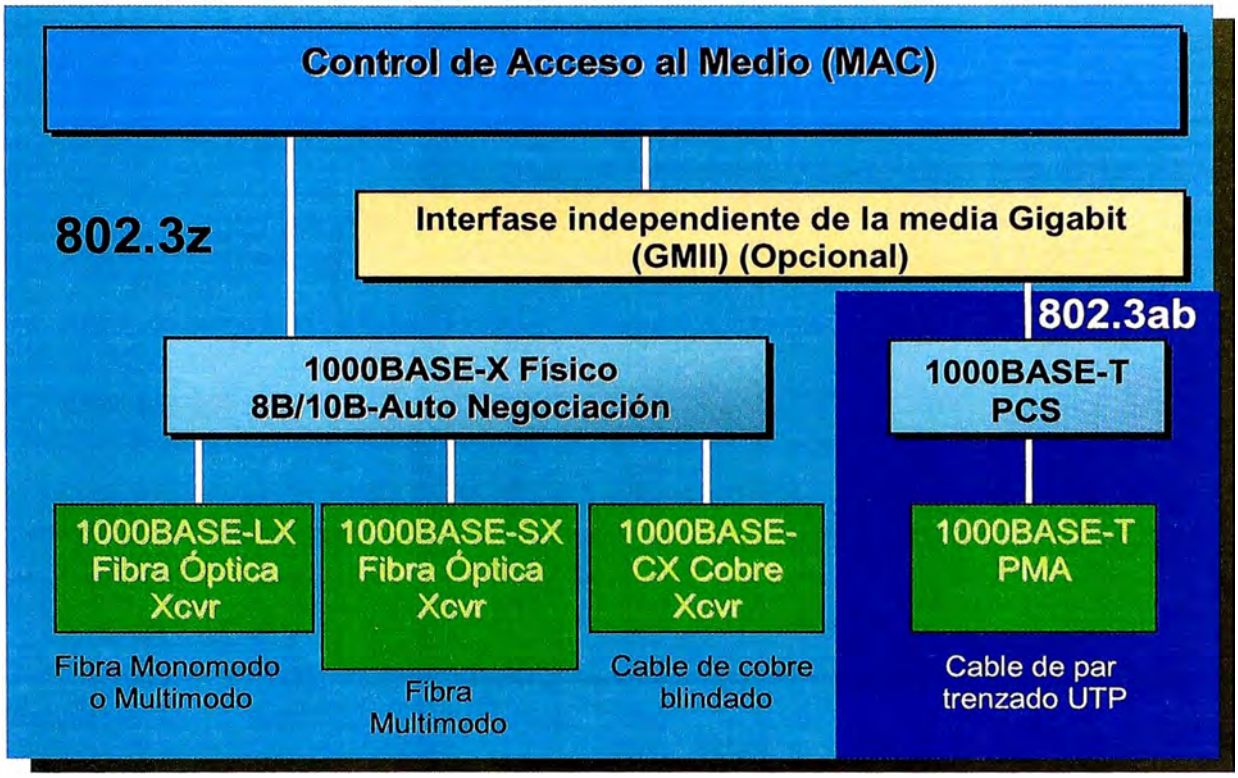

Figura 2.1 – Gigabit Ethernet

A continuación en la tabla 2.2 se muestra una tabla comparativa entre las velocidades de Ethernet, Fast Ethernet y Gigabit Ethernet en los diferentes medios usados en el cableado estructurado.

MEDIO DE TRANSMISIÓN	GIGABIT ETHERNET	FAST ETHERNET	ETHERNET
Velocidad	1000 Mbps	100 Mbps	10 Mbps
Categoría 5 UTP	100 m.	100 m.	100 m.
Fibra Monomodo	5 Km.	20 Km.	25 Km.
Fibra Multimodo	220-550 m.	412 m (half duplex) 2 Km. (full duplex)	2 Km.

Tabla 2.1 – Cuadro comparativo de velocidades Ethernet

En la figura 2.2 se muestra el uso de la Tecnología Gigabit Ethernet en el cableado estructurado para diferentes tipos de ambientes.

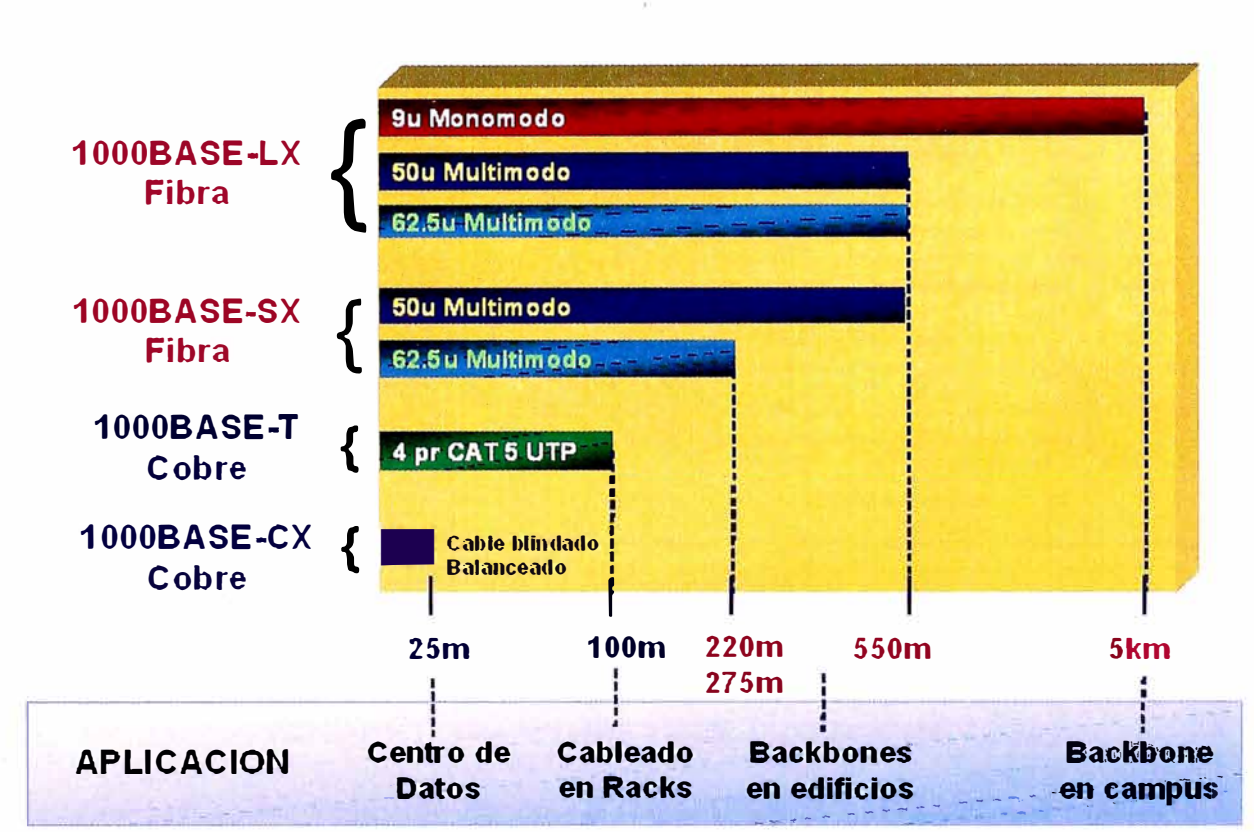

Figura 2.2 – Tecnología Gigabit Ethernet

2.2 ENLACES RESILENTES

Consiste en conectar equipos con dos enlaces, uno primario y el otro secundario este último se activa si en enlace primario falla, esta tecnología ofrece redundancia en caso de fallas, en la figura 2.3 se muestra la operación de este tipo de enlaces.

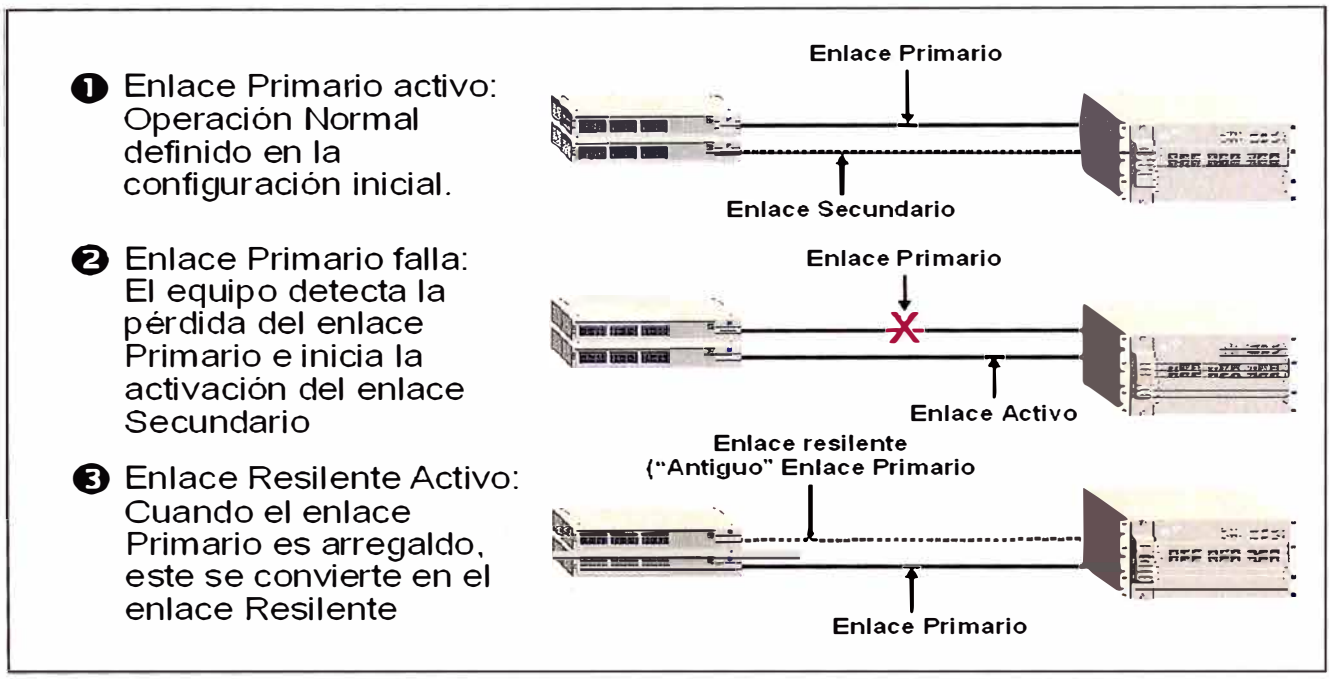

Figura 2.3 – Enlaces Resilentes

2.3 ARBOL EXTENDIDO (SPANNING TREE PROTOCOL - STP)

El árbol extendido (Protocolo Spanning Tree - IEEE 802.1D) crea una topología de red lógica libre de bucles poniendo los enlaces redundantes en modo de bloqueo, creando un único camino entre dos estaciones finales tal como se muestra en la figura 2.4

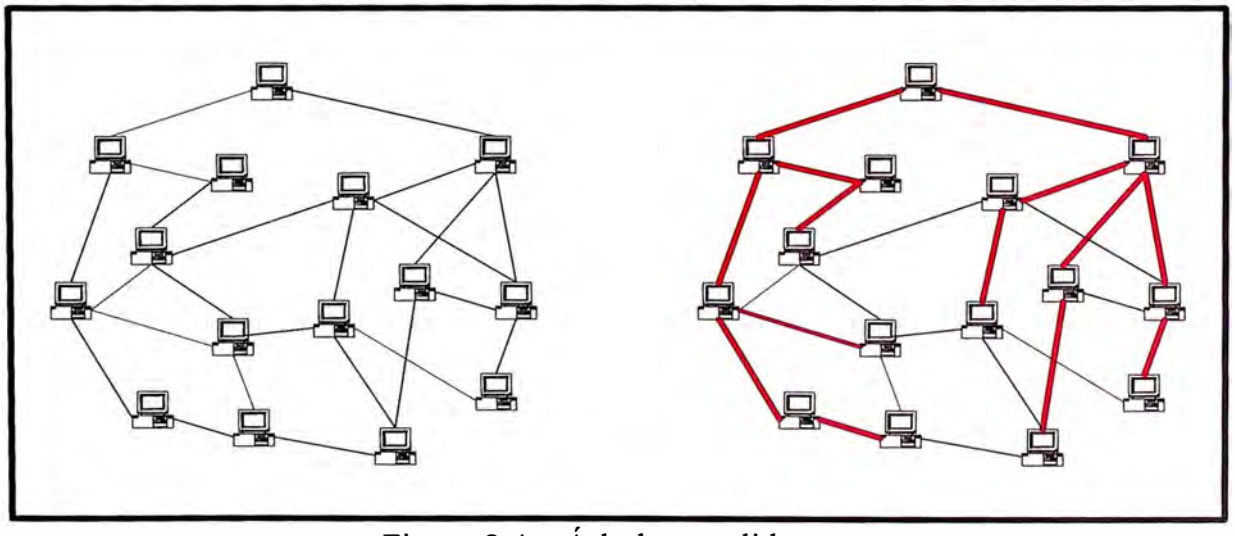

Figura 2.4 – Árbol extendido

El árbol extendido presenta algunos beneficios que podemos mencionar a continuación:

- Permite la creación de grandes y complejas redes.
- Garantiza que los paquetes llegaran en el orden en que fueron transmitidos.
- Elimina la duplicación de paquetes.
- Elimina el problema de aprendizaje evitando el tráfico broadcast.
- Provee tolerancia a fallas mediante reconfiguración automática.
- Opera transparentemente entre las estaciones finales.
- Provee interoperabilidad entre diferentes fabricantes.

2.4 ARBOL EXTENDIDO MEJORADO (RAPID SPANNING TREE PROTOCOL - RSTP)

Esta característica del árbol extendido mejorado (Rapid Spanning Tree Protocol IEEE 802.1W) da un camino para configurar rutas redundantes aunque mantiene un solo camino entre dos dispositivos. El RSTP monitorea el estatus de todas las rutas, si una ruta activa se cae, el RSTP activa el camino redundante y luego reconfigura la topología de la red. El árbol extendido mejorado (Rapid Spanning Tree Protocol - RSTP) es una mejora del Spanning Tree Protocol. A continuación en la Tabla 2.2 se muestra un cuadro comparativo entre las diferentes tipos de enlaces.

2.5 ENLACES AGREGADOS (TRUNKING)

Es el estándar 802.ad (Trunking) permite aumentar el ancho de Banda mediante enlaces activos paralelos punto a punto entres switches o Switch con servidor. Estos enlaces permiten aumentar la velocidad y redundancia de conexiones entre equipos

sin cambiar o reemplazar hardware o cableado existente. En la figura 2.5 se muestra los enlaces agregados entre dos switches.

ENLACE AGREGADO	ARBOL EXTENDIDO (SPANNING TREE)	ARBOL EXTENDIDO MEJORADO (RAPID SPANNING TREE)
El usuario configura cada Switch separadamente	El usuario habilita/deshabilita STP en cada bridge	El usuario deshabilita RSTP en cada bridge
Configuración Manual	Configuración Automática	Configuración Automática
En 5 segundos se reestablece la conexión del enlace resilente	Hasta 30 segundos de retardo en caso de falla de enlace	En 5 segundo reestablece la conexión de la red

Tabla 2.2 – Tabla comparativa entre enlaces

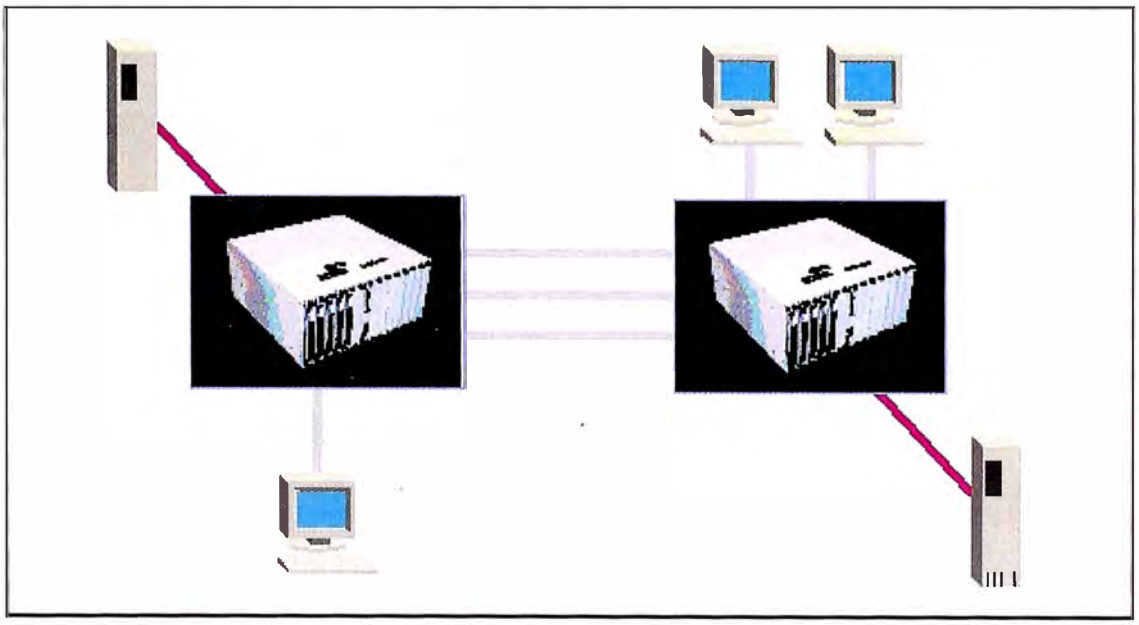

Figura 2.5 – Enlaces agregados

2.6 VLAN (REDES VIRTUALES)

Las VLANs son dominios de broadcast, las VLANs pueden ser vistas como un grupo de estaciones de trabajo definidas lógicamente en múltiples segmentos de la red LAN y se comunican entre ellas como si estuvieran en el mismo segmento LAN como se

muestra en la figura 2.6. Las VLANs no se pueden comunicar entre si a menos que se tenga un router o un Switch de capa 3 para realizar el encaminamiento entre ellas.

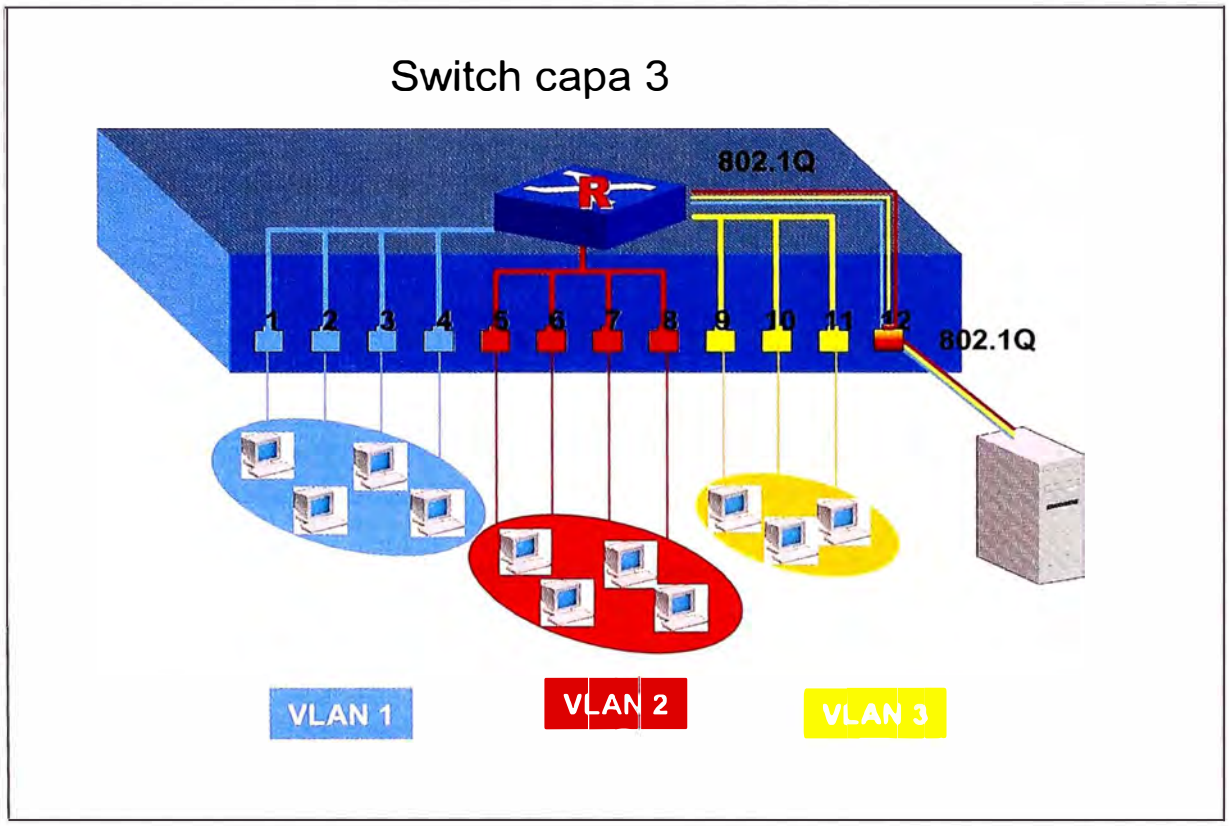

Figura 2.6 – Redes virtuales

2.7 PROTOCOLO DE ENRUTAMIENTO DE INFORMACION (RIP)

Es un protocolo de enrutamiento basado en vectores distancia, se utiliza el número de saltos como métrica para la selección de rutas y el número máximo de saltos permitido es 15. El protocolo RIP difunde sus actualizaciones de enrutamiento por medio de la tabla de enrutamiento completa cada 30 segundos por defecto.

RIP-1 requiere que se use una sola máscara de red para cada número de red de clase principal que es enunciado. La máscara en una mascara de subred de longitud fija.

RIP-2 permite mascaras de subred de longitud variable (VLSM) en la interconexión.

(El estándar RIP-2 permite actualizaciones desencadenadas a diferencia del RIP-1).

2.8 PROTOCOLO PRIMERO LA RUTA MÁS CORTA (OSPF)

El grupo de trabajo OSPF del IETF diseño el protocolo primero la ruta más corta (Open Shortest Path First, OSPF) a finales de los 80. Se diseño para cubrir las necesidades de las redes IP, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2, la implementación más actualizada, aparece especificado en la RFC 1583. OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes direccionados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas. Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es un protocolo de enrutamiento por estado de enlace. A diferencia de RIP e IGRP que publican sus rutas sólo a routers vecinos, los routers OSPF envían Publicaciones del estado de enlace (Link-State Advertisment, LSA) a todos los routers pertenecientes a la misma área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo SPF para calcular la ruta más corta a cada nodo.

Para determinar que interfaces reciben las publicaciones de estado de enlace, los routers ejecutan el protocolo OSPF Hello. Los routers vecinos intercambian mensajes Hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers. Cuando se detecta un router vecino, se intercambia información de topología OSPF. Cuando los routers están sincronizados, se dice que han formado una adyacencia. Las LSA se envían y reciben sólo en adyacencias. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF. La capa de transporte OSPF define un proceso fiable de publicación, acuse de recibo y petición para garantizar que la información de la LSA se distribuye adecuadamente a todos los routers de un área. Existen cuatro tipos de LSA. Los tipos más comunes son los que publican información sobre los enlaces de red conectados de un router y los que publican las redes disponibles fuera de las áreas OSPF.

La métrica de enrutamiento de OSPF se calcula como la suma de los OSPF a lo largo de la ruta hasta alcanzar una red. El coste OSPF de un enlace se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario.

La configuración del proceso de enrutamiento OSPF consiste en dos pasos: posibilitar que el router ejecute el protocolo OSPF e identificar las direcciones e interfaces de la red que deben incluirse en las actualizaciones de enrutamiento y las áreas a las que pertenecen las interfaces.

En la tabla 2.3 se muestra un comparativo entre RIP-1, RIP2 y OSPF

Característica	RIP-1	RIP-2	OSPF
Velocidad de convergencia	Lento	Más rápido que RIP-1	Rápido
Método de transmisión	Direccionamiento Broadcast	Direccionamiento Multicast	Direccionamiento Multicast
Tipo de métrica	Cuenta de saltos	Cuenta de saltos	Costo de ruta (velocidad de enlace)
Limitación de distancia	15 saltos	128 saltos	Saltos ilimitados
Intervalo de actualización	Periodicidad de actualización (30 segundos)	Periodicidad de actualización (30 segundos)	Actualización por Triggers (Eventos)
Uso de ancho de Banda	Toda la tabla	Toda la tabla	Solo cambios
Complejidad del protocolo	Baja (tipo de paquetes simples)	Baja (tipo de paquetes simples)	Alta (tipo de paquetes múltiples)
Vía de enrutamiento	Vía simple de enrutamiento	Vía simple de enrutamiento	Vías múltiples de enrutamiento
Soporte a múltiples Áreas	NO	NO	SI
Soporte VLSM	NO	SI	SI
Escalabilidad	Limitada	Mejorada	Excelente

Tabla 2.3 – Tabla de protocolos

2.9 PROTOCOLO MULTICAST IP

Multicast IP es de gran ayuda para enviar un flujo de datos a un grupo determinado de usuarios en una red. Una aplicación común de soporte multicast es cuando se tiene un servidor de video. Cuando el servidor de video envía un flujo de datos de video a una red conmutada que soporte protocolos multicast, es que el Switch no solo envía el flujo de video a los usuarios suscritos al multicast si no que permite la mejor utilización del ancho de banda de la red, tal como se muestra en la figura 2.7.

El multicast IP trabaja bien con los servicios QoS en redes permitiendo que los flujos multicast sean priorizados de acuerdo a las políticas de la empresa. Dentro de las características del multicast IP podemos mencionar:

- Habilita envío simultáneo de información a varios receptores de la mejor manera.
- Reduce la carga en la fuente, debido a que este no produce múltiples copias de la misma data.
- Hace uso eficiente del ancho de banda de acuerdo aunque aumente la cantidad de usuarios de la red.
- Da un gran soporte a aplicaciones multimedia en tiempo real.

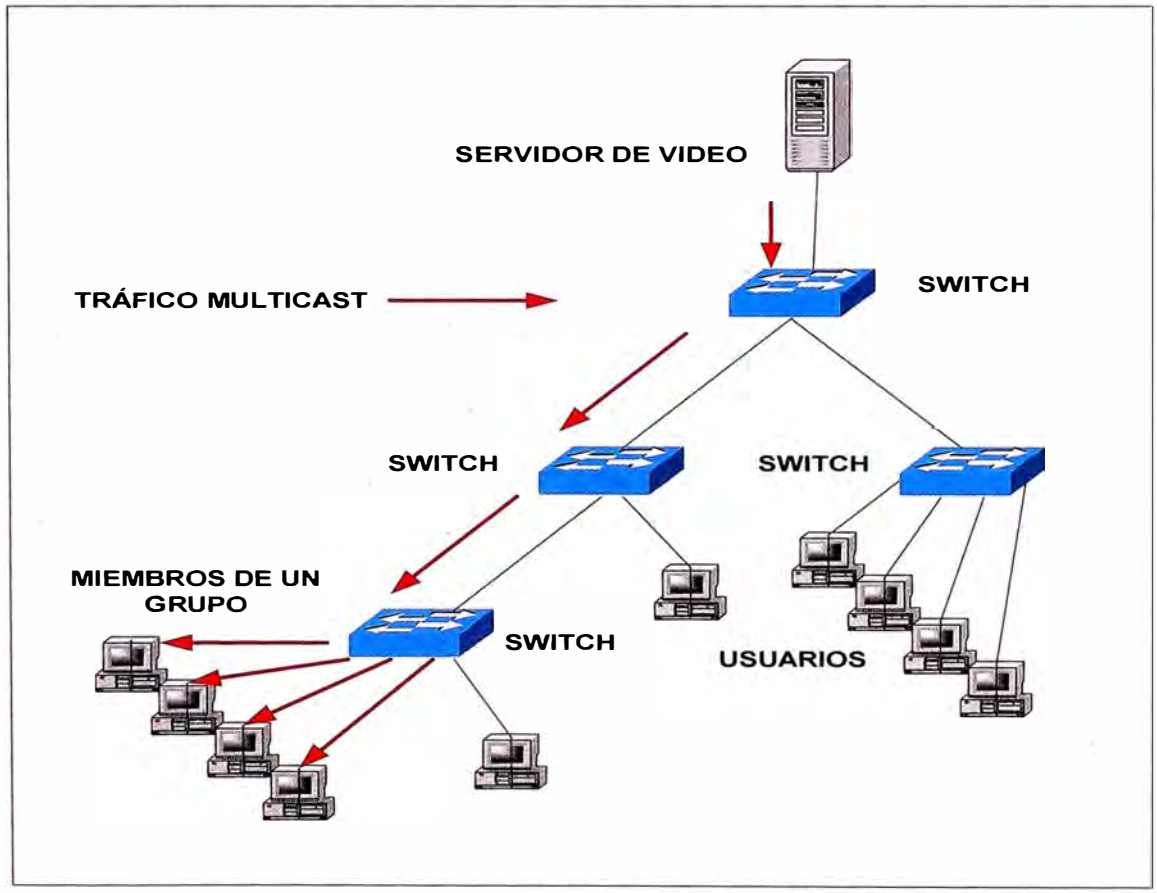

Figura 2.7 – Protocolo multicast IP

2.10 PROTOCOLO DE ENRUTAMIENTO RAPIDO EN ESPERA (HSRP - HOT STANDBY ROUTING PROTOCOL)

En la figura 2.8, los switches de distribución (Switches C y D) proveen conexiones de rutas redundantes a los switches de core. Con el protocolo HSRP (Hot Standby Routing Protocol) configurado en cada Switch, Switches C y D pueden ser configurados respectivamente como ruta primaria al core para la VLANs normal y alternativa y como ruta secundaria para la VLAN normal y alternativa. En este sentido, cada Switch de distribución juega un rol consistente en ambas capas 2 y 3.

HSRP crea una interfase de router virtual que puede ser compartida por dos o más routers. Esta interfase consiste de una dirección virtual MAC seleccionada de un grupo de direcciones reservada por los dispositivos del fabricante y una dirección IP virtual. HSRP es configurado por cada VLAN y los miembros de cada VLAN son configurados con la interfase virtual HSRP como puerto de salida por defecto. Cada uno de los routers participantes en la interfase virtual es asignado con una prioridad que es determinado por el router principal. En cada VLAN el router HSRP envía mensajes multicast periódicos "Hello" que incluyen la prioridad del router que envía. En el evento que el router principal falle, el router secundario detecta los mensajes "Hello" perdidos, determinando que el router secundario tiene ahora la máxima prioridad y comienza el proceso de direccionamiento de tráfico a la interfase virtual.

HSRP tiene una característica la cual le permite al router HSRP de máxima prioridad enviar el estatus a las interfases del Switch de core. Cuando la búsqueda de interfases está habilitada y cuando un componente no esta disponible durante la búsqueda, la prioridad del HSRP del router es automáticamente disminuida. Por ejemplo, si un Switch router HSRP (tal como el Switch en la figura 2.8) pierde todas sus interfases

al core, la disminución de la prioridad puede ser configurada para que se mantenga el estatus del router activo para las VLANs normales. Tan pronto como el Switch D se convierte en el router HSRP activo para la VLANs normales (al igual que las alternativas) el tráfico de la VLAN normal fluye directamente al Switch D sin necesidad de pasar a través del Switch C. La extensión de búsqueda al HSRP provee al ingeniero de red con la habilidad predeterminada de cómo la red puede ser configurada en los eventos de fallas. Este puede ayudar a que la consistencia de los servicios pueda ser mantenida y optimizada mientras la redundancia esta siendo restaurada.

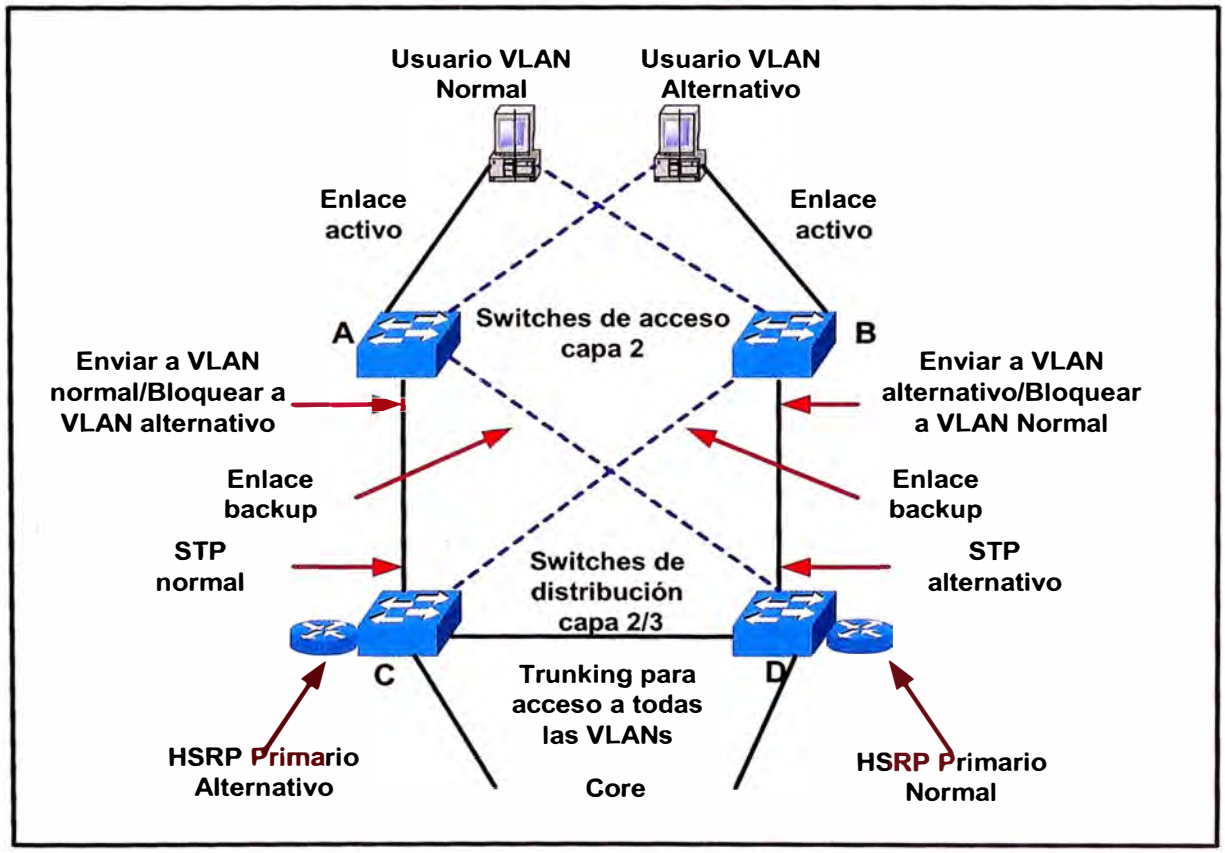

Figura 2.8 – Protocolo de enrutamiento rápido en espera

2.11 MONITOREO REMOTO (RMON)

Desarrollado por la IETF (Internet Engineering Task Force (IETF) en un Request For Comment (RFC) 1757 y provee el monitoreo y análisis de protocolos de la redes LAN en el nivel de enlace de datos. Para el monitoreo de la red las estaciones de trabajo o dispositivos de la red coleccionan datos localmente y son enviados a la estación de administración en intervalos regulares o cuando ocurre algún evento, este tipo de comunicación reduce la carga de tráfico en la red como se muestra en la figura 2.9.

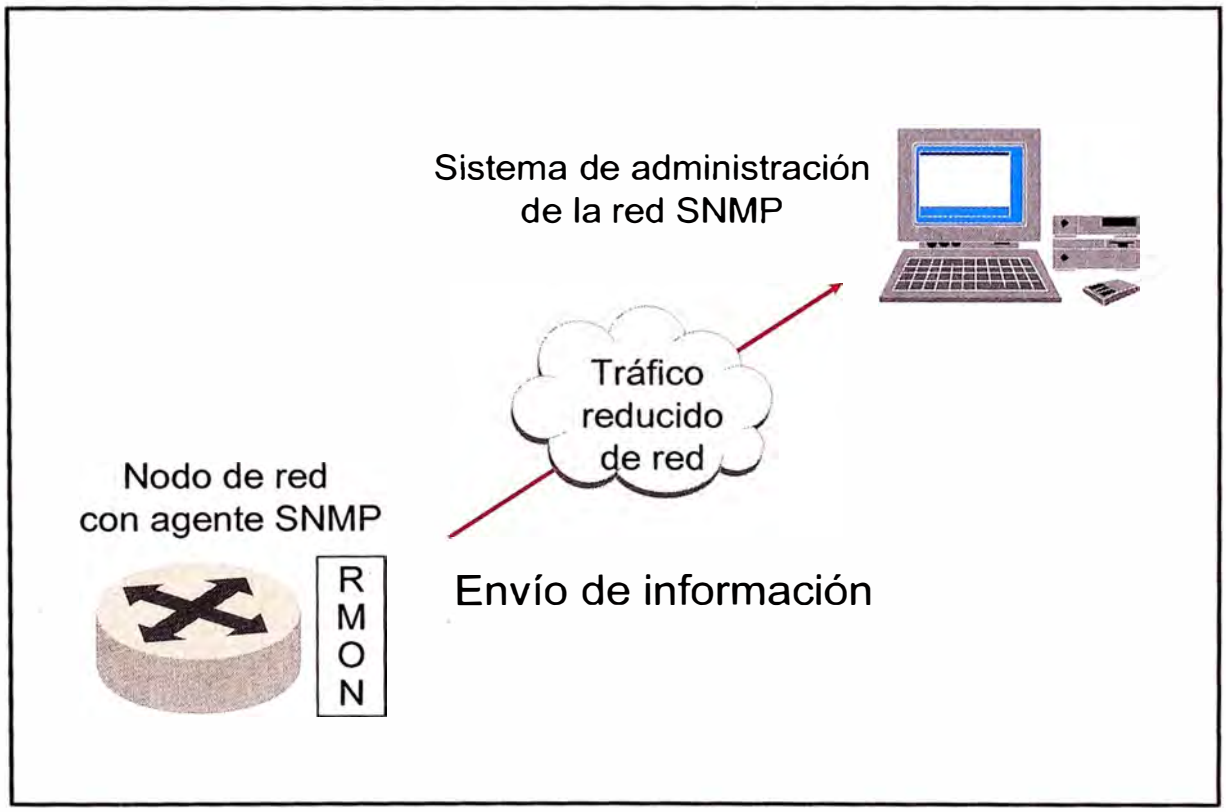

Figura 2.9 – Monitoreo remoto

CAPÍTULO III

DISEÑO DE REDES LAN

3.1 PRINCIPIOS DE DISEÑO DE REDES

El diseño de redes está basado en diversos conceptos que podemos resumirlos de la siguiente manera:

- **EXAMINAR PUNTOS DE FALLA:** Debe haber redundancia en las redes de tal manera que los puntos de falla sean aislados de cualquier segmento de la red. Existen dos aspectos de redundancia que necesitan ser considerados: Backup y balanceo de carga. En caso de evento de falla de la red debe existir una alternativa o ruta de backup. El balanceo de carga ocurre cuando dos o más caminos a un destino existen y pueden ser utilizados dependiendo de la carga de la red.
- **IDENTIFICAR EL TRAFICO DE LA APLICACIÓN Y PROTOCOLO DE RED:** Por ejemplo, el flujo de la data de una aplicación puede ser una interacción cliente/servidor y es crucial para ubicar eficientemente los recursos de la red saber el numero de clientes usando un servidor en particular o el numero de clientes en un segmento determinado.

- **ANALIZAR EL ANCHO DE BANDA DISPONIBLE:** Se debe tener en cuenta que en modelos jerárquicos los elementos o dispositivos de mayor jerarquía deben trabajar con enlaces de mayor velocidad puesto que tienen mayor tráfico de red y los elementos de menor jerarquía deben manejar el tráfico adecuado a sus necesidades de aplicaciones y acceso a los servicios de la red.
- **CONSTRUIR REDES USANDO MODELOS JERARQUICOS:** La jerarquía permite segmentos de red autónomos que pueden trabajar junto con otros segmentos de red. En la figura 3.1 muestra varios aspectos de un diseño de una red jerárquica. El diseño de una red jerárquica presenta tres niveles; core, distribución y acceso, cada uno de estos niveles presentan diferente funcionalidad.

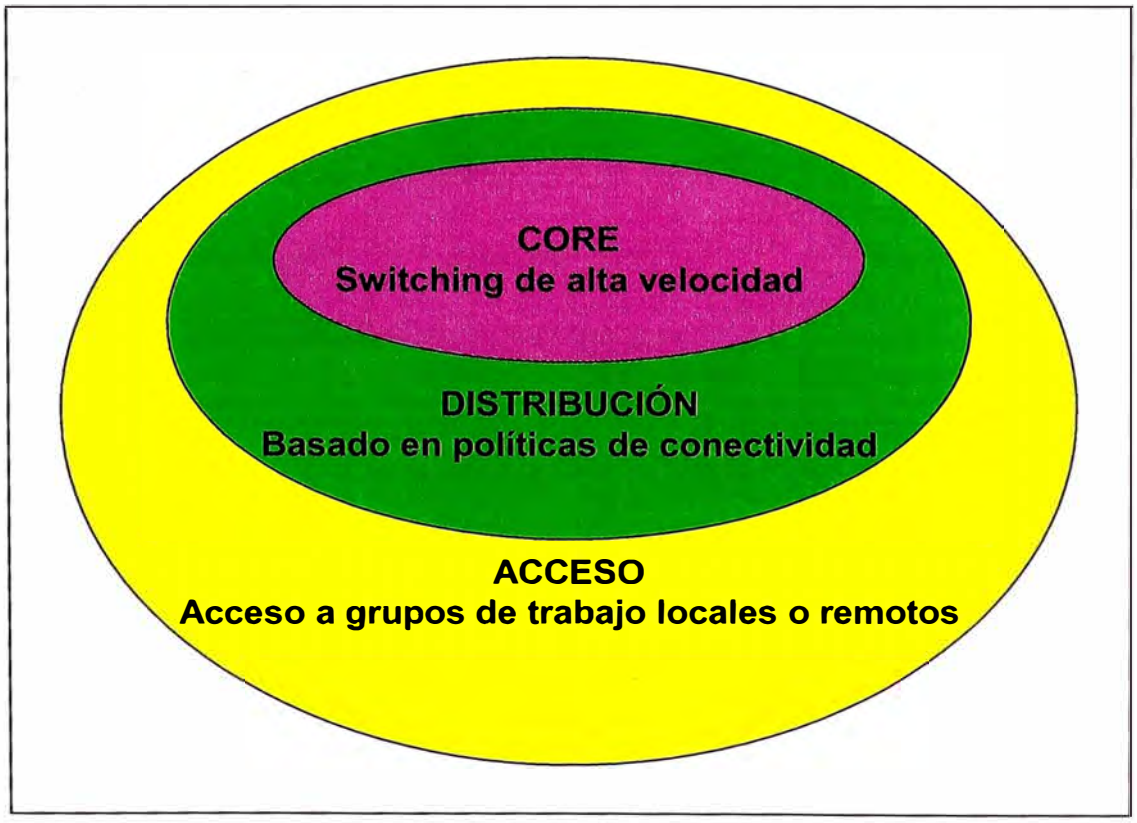

Figura 3.1 – Red jerárquica

3.2 NIVELES JERÁRQUICOS EN UNA RED

Para lograr un mejor diseño de redes se debe tener en cuenta los niveles jerárquicos de una red para lo cual se ha definido los siguientes niveles:

EL NIVEL CORE: Es un backbone conmutado de alta velocidad y debe ser diseñado para conmutar paquetes tan rápido como sea posible. En este nivel de la red no se debe configurar ninguna manipulación de paquetes, filtros que podrían bajar la velocidad de conmutación de paquetes.

EL NIVEL DISTRIBUCIÓN: Es el punto de demarcación entre los niveles de Acceso y Core, ayudando a definir y diferenciar el Core. El propósito de este nivel es proveer una definición de la frontera y es el lugar donde se puede manipular los paquetes de información. En un ambiente de campus, el nivel de distribución puede incluir varias funciones, tales como se menciona a continuación:

- Direcciones o agregación de Área.
- Acceso a grupo de trabajos o departamentos.
- Definición del dominio de Broadcast/Multicast.
- Enrutamiento de VLAN
- Seguridad

En ambientes que no son campus, el nivel de distribución puede ser un punto de redistribución entre los dominios de enrutamiento o la demarcación entre protocolos de enrutamiento estático o dinámico. También puede ser el punto al cual los sitios remotos accedan a la red Corporativa. El nivel de distribución puede resumirse como el nivel que provee conectividad basada en políticas.

EL NIVEL DE ACCESO: Este nivel es el punto en el cual los usuarios finales están permitidos de acceder a la red. Este nivel también puede usarse como lista de acceso o filtros para optimizar las necesidades de un particular conjunto de usuarios.

En un ambiento campus, las funciones del nivel de acceso pueden incluir los siguientes aspectos:

- Ancho de banda compartido.
- Ancho de banda conmutado.
- Filtro a nivel MAC.
- Microsegmentación.

En un ambiente no campus, el nivel de acceso puede dar acceso a sitios remotos a la red corporativa vía alguna tecnología WAN tales como Frame Relay, ISDN o líneas dedicadas. Algunas veces se piensa erróneamente que los tres niveles (Core, distribución y Acceso puede existir solas o en entidades físicas distintas, pero esto no tiene que ser el caso. Los niveles son definidos para tener un diseño de red optimizado y representan la funcionabilidad que debe existir en la red.

El inicio de cada nivel puede estar en distintos routers o switches, puede ser representado por una media física, puede ser combinado en un solo dispositivo o pueden ser omitidos todos juntos. El camino para implementar depende de las necesidades de diseño de la red, Sin embargo cabe notar que para que una red funcione óptimamente se debe mantener la jerarquía.

3.3 EJEMPLOS DE DISEÑO DE REDES

En el diseño de redes se debe tener en cuenta la cantidad de usuarios, el tipo de aplicaciones que se brindaran en la red y la ubicación de los equipos a integrar las

redes, a continuación se muestran algunos ejemplos típicos de implementación de redes.

REDES DE PISO: Como se muestra en la figura 3.2 estas redes están formadas por pocos usuarios y tienen un servidor donde comparten información, generalmente son redes diseñadas de un piso trabajan a velocidades de 10/100 Mbps, se puede decir que solo tienen el nivel de acceso a la red.

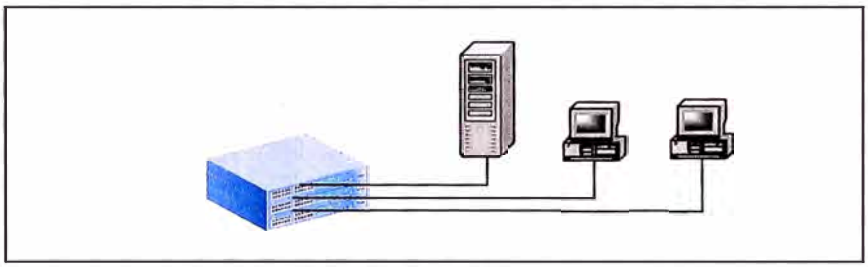

Figura 3.2 – Red de piso

REDES DE EDIFICIOS: Estas redes son mas complejas tienen redes de piso que están unidas a un Switch central de alta velocidad, este equipo central puede manejar velocidades de 100/1000Mbps y al cual se pueden conectar servidores directamente que comparten información entre las redes de piso, aquí se pueden implementar redes VLAN separando lógicamente los departamentos que manejan información similar y que necesitan están en el mismo dominio de broadcast. Esta es una red que tiene nivel de acceso y distribución como se muestra en la figura 3.3. Estas redes generalmente cuentan con un centro de cómputo donde se concentran los servidores, los equipos de comunicaciones y todos los servicios de gestión de la red.

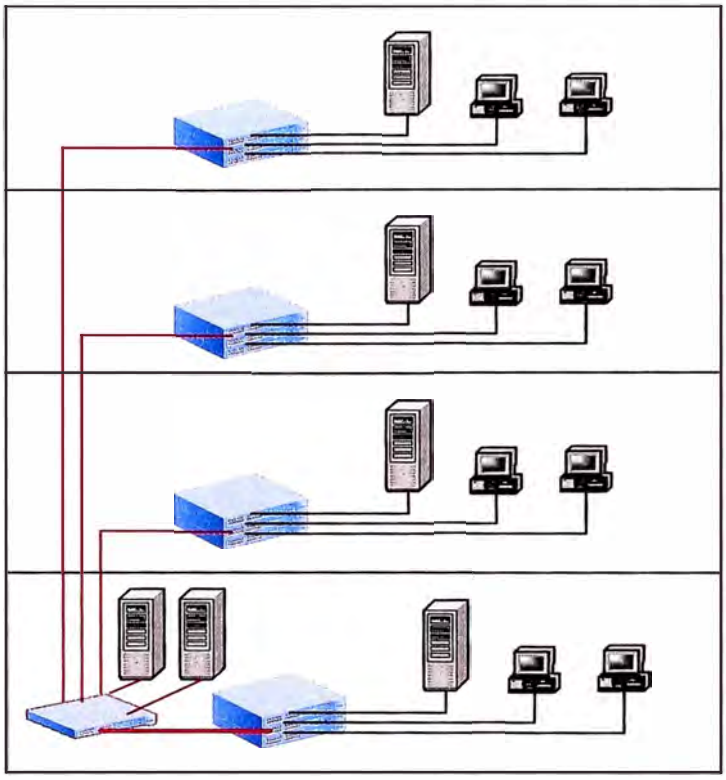

Figura 3.3 – Red de edificio

REDES DE CAMPUS: Esta es una red corporativa que une varios edificios distribuidos a través de un campus como se muestra en la figura 3.4. Cuentan con Centro de Computo Central, donde colapsan todas las redes de los edificios a una velocidad de 1Gbps, en este centro de computo central se conectan los servidores corporativos que brindan servicio a la red en su conjunto y están también conectados a altas velocidades 1Gbps.

Esta es una red que tiene los tres niveles; acceso, distribución y Core. Adicionalmente en estas redes se debe implementar la redundancia por la criticidad de los servicios con los que cuenta la red en su conjunto.

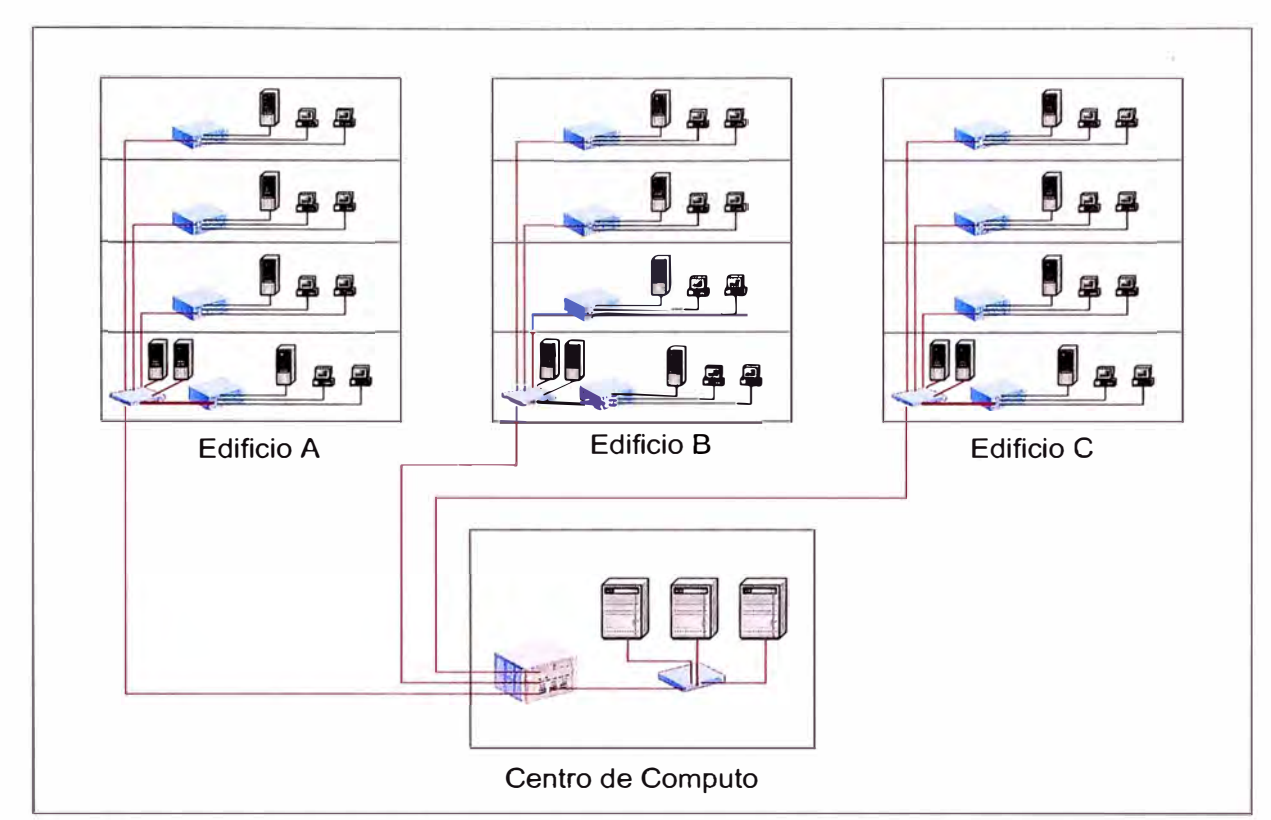

Figura 3.4 – Red de campus

CAPÍTULO IV

IDENTIFICACIÓN DE COMPONENTES CRÍTICOS DE LA RED LAN

4.1 TARJETA DE RED DEL USUARIO

En la identificación de componentes críticos de la red se puede identificar que uno de ellos es la tarjeta de red de la computadora del usuario como se muestra en la figura 4.1, en estos casos la mayoría de veces la tarjeta de red esta integrada a la computadora por lo que la falla de esta es cubierta por la garantía del equipo.

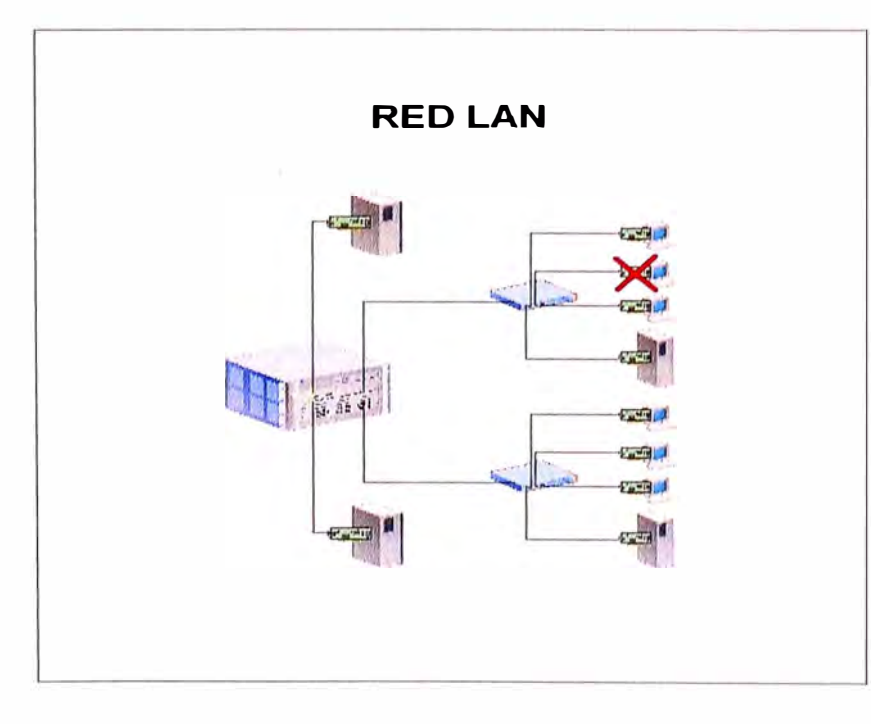

Figura 4.1 – Tarjeta de red del usuario

4.2 CABLEADO DE LA RED

El cableado estructurado es parte fundamental en la comunicación de redes LAN y es muy frecuente escuchar fallas en el mismo, muchas veces por falta de mantenimiento, es necesario que el cableado estructurado de una red deba estar certificado para garantizar el buen funcionamiento del mismo tanto en tramas de cableado de cobre UTP como cableado en fibra óptica.

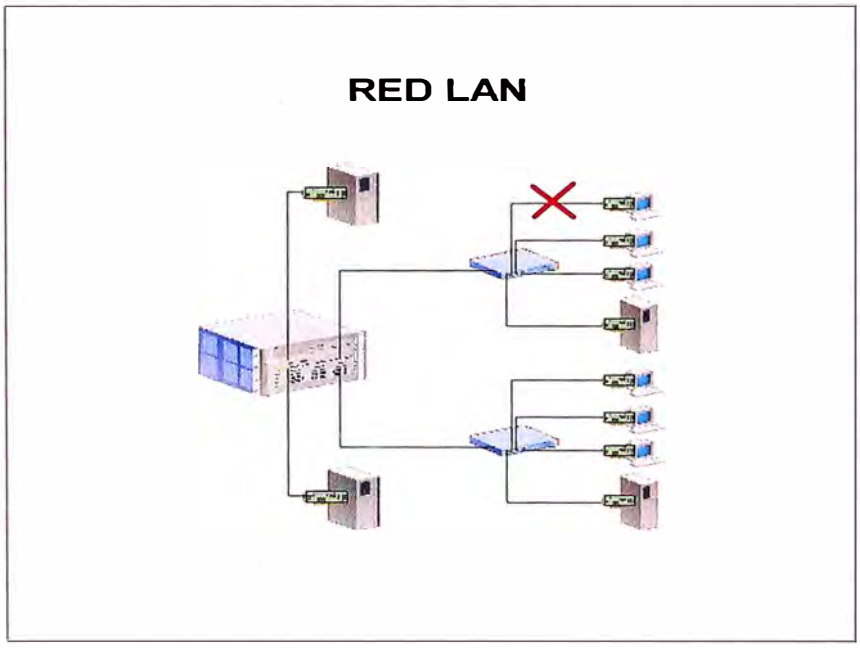

Figura 4.2 – Cableado de la red

4.3 SWITCH DE BORDE

Estos equipos son los que permiten la comunicación de los usuarios a la red por lo que la falla de este originaría que un segmento de la red deje de operar, en la mayoría de casos estos equipos dan acceso a los usuarios a una velocidad de 10/100 Mbps y se conectan al Backbone de la red a 1Gbps mediante conexión de fibra óptica como se muestra en la figura 4.3.

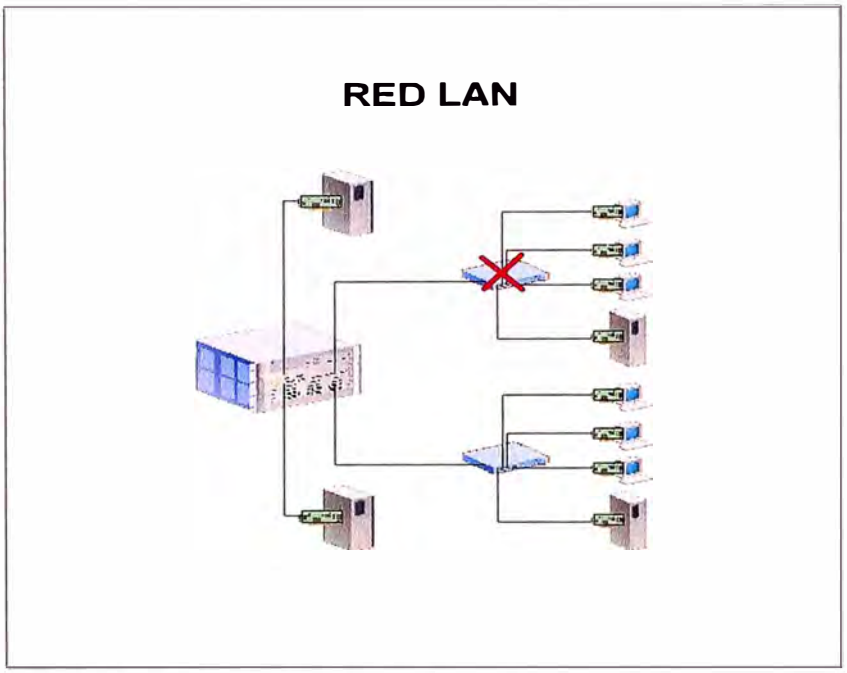

Figura 4.3 – Switch de borde

4.4 TARJETA DE RED DEL SERVIDOR

Los Servidores son unos de los componentes mas críticos de la red, puesto que en ellos se almacena información vital de las empresas, el no funcionamiento de la tarjeta de red del servidor inmediatamente origina caída del servicio a los usuarios que esta atendiendo, por eso es necesario que los servidores tengan enlaces resilentes de backup. Normalmente los servidores se conectan a la red a velocidades de 1Gbps ya sea en cobre UTP o fibra óptica según se muestra en la figura 4.4.

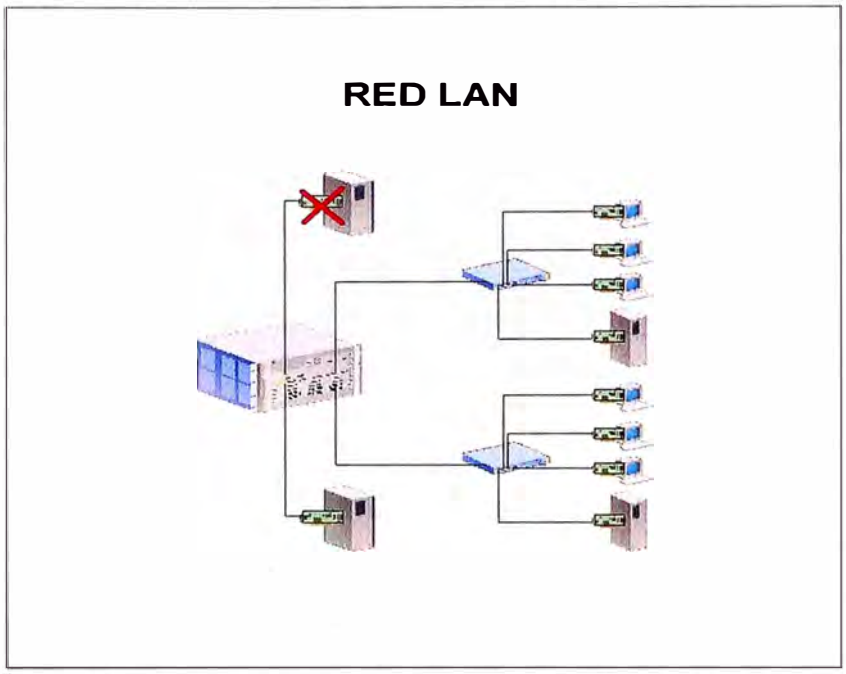

Figura 4.4 – Tarjeta de red del servidor

4.5 SWITCH CORPORATIVO

Este es el equipo neurálgico de la red debido a que todas las comunicaciones colapsan en el, según se muestra en la figura 4.5. A este equipo normalmente se conectan los switches de borde y los servidores a altas velocidades a 1Gbps. Estos equipos cuentan con elementos de redundancia tales como la fuente de poder, ventiladores, tarjeta procesadora principal, etc. Estos equipos permiten tener conexiones resilentes a los servidores y switches de borde para asegurar la continua operación de la red.

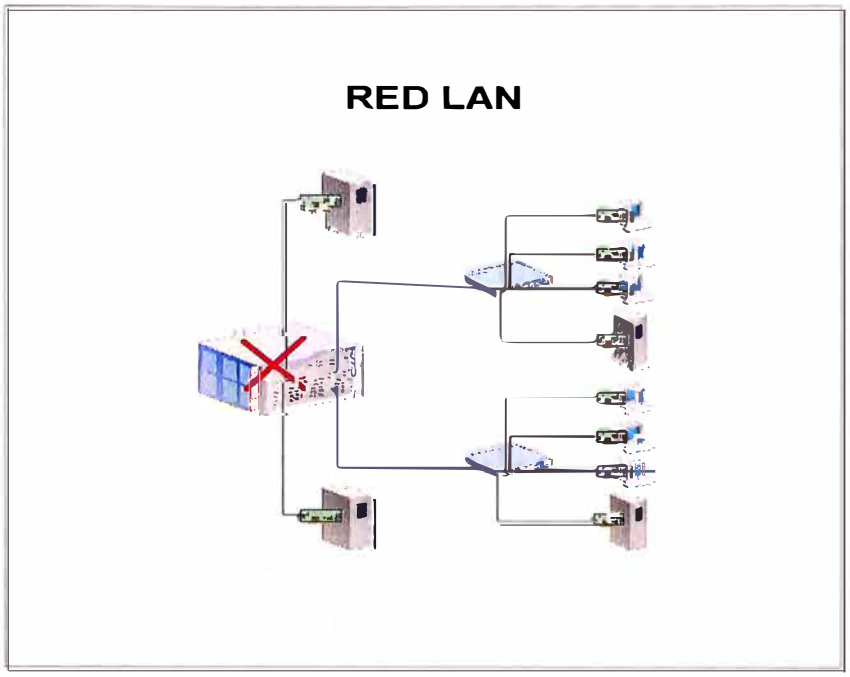

Figura 4.5 – Switch corporativo

CAPÍTULO V

DISPOSITIVOS TOLERANTES A FALLAS

5.1 INTRODUCCIÓN

En una red corporativa el equipo mas importante es el Switch de Core, por eso muchos fabricantes realizan sus mayores esfuerzos en diseñar equipos que soporten alta disponibilidad agregando componentes redundantes tales como la fuente de poder, los ventiladores, la tarjeta principal, etc., tal como se muestra en la figura 5.1. Dependiendo del grado de criticidad y política de las empresas están optan por diversos modelos de contingencia para mantener la operatividad de la red tales como:

- **OUTSOURCING DE EQUIPOS:** El modelo de outsourcing de los equipos de comunicaciones consiste en que el proveedor se encargue del mantenimiento preventivo y correctivo de los equipos asegurando ciertos tiempos de respuesta y tiempo de reparación.
- **EQUIPOS CON COMPONENTES REDUNDANTES:** Muchas empresas optan por comprar sus equipos de Core con elementos redundantes tales la fuentes de poder, ventiladores y tarjeta Switch fabric asegurando así la continuidad de los equipos. Cuando ocurre fallas en algún dispositivo redundante

este es automáticamente suplantado por el elemento redundante, posteriormente se programa una hora determinada para parar la red y realizar los cambios de los componentes deteriorados.

- **REDES REDUNDANTES:** Este es el caso cuando la no disponibilidad de la red produce mucha pérdida de dinero, en estos casos se diseñan equipos y enlaces redundantes de tal forma que se garantiza la operatividad de la red, así mismo los cambios de equipos fallados se pueden durante la operación normal de la red.

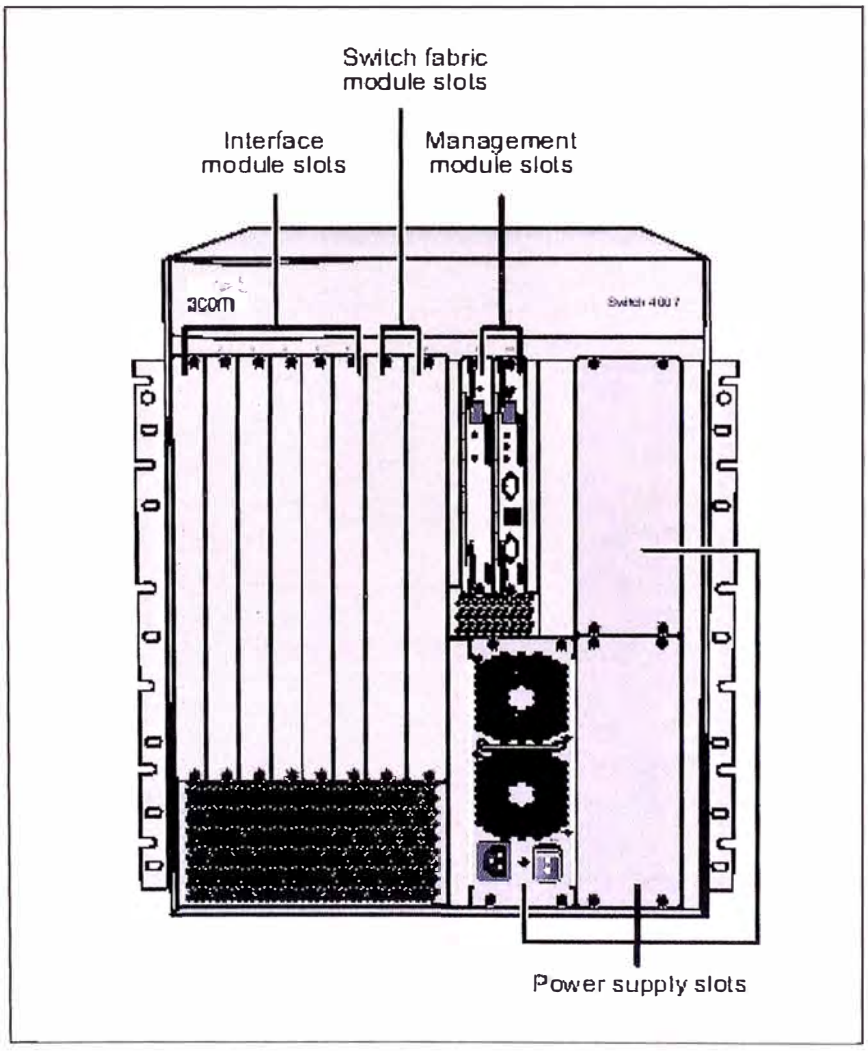

Figura 5.1 – Componentes de un switch

5.2 DISPOSITIVOS REDUNDANTES

5.2.1 FUENTE DE PODER

La mayoría de fabricantes que diseñan switches corporativos incluyen en sus equipos fuentes de poder de acuerdo a la cantidad de tarjetas que van ha soportar los equipos, adicionalmente se pueden agregar fuentes poder redundantes en caso de que la fuente de poder principal fallara o para balancear la carga del equipo. En la figura 5.2 se muestra un ejemplo de fuente de poder de un Switch de Core.

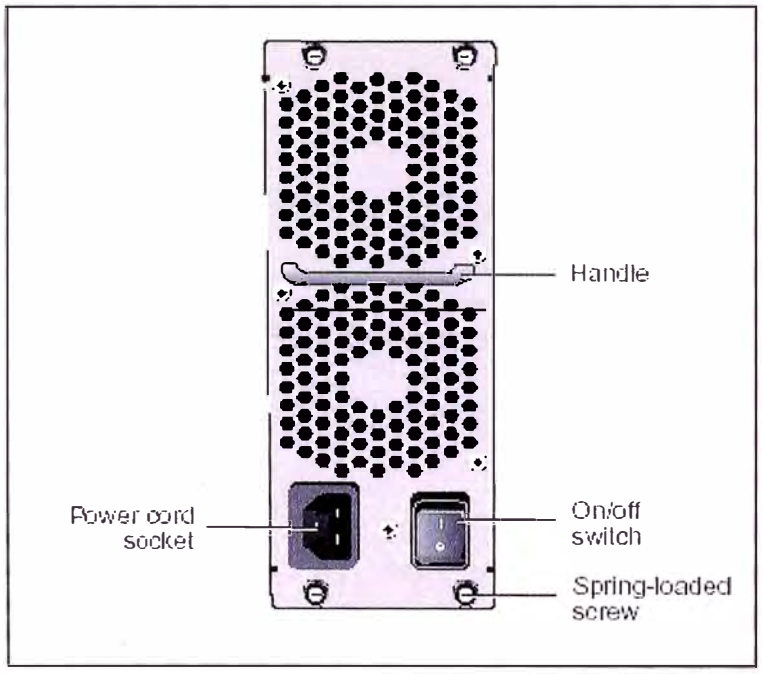

Figura 5.2 – Fuente de poder

5.2.2 VENTILADORES

Estos elementos son muy importantes por que permiten enfriar los componentes internos del equipo garantizando un tiempo de vida mayor de los mismos. Existen Fabricantes que diseñan el chasis de sus equipos para incluir ventiladores redundantes en el equipo tal como se muestra en la figura 5.3.

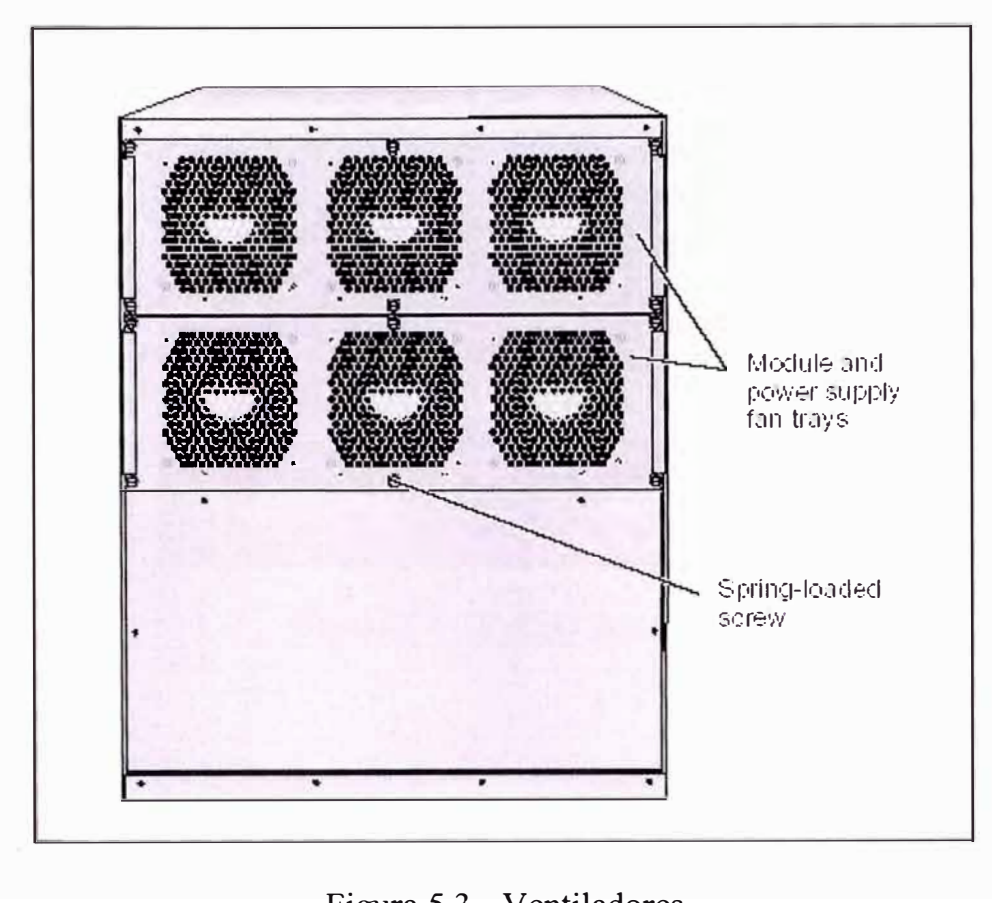

Figura 5.3 - Ventiladores

5.2.3 TARJETA PROCESADORA

Los equipos de chasis cuentan con dos ranuras exclusivas para colocar la tarjeta procesadora del Switch, en una de las ranuras se ubica la tarjeta procesadora principal y en la segunda ranura la tarjeta procesadora secundaria, esta última actúa como backup de la primera en caso de que esta falle. En la figura 5.4 se muestra un ejemplo de una tarjeta procesadora de un Switch de Core.

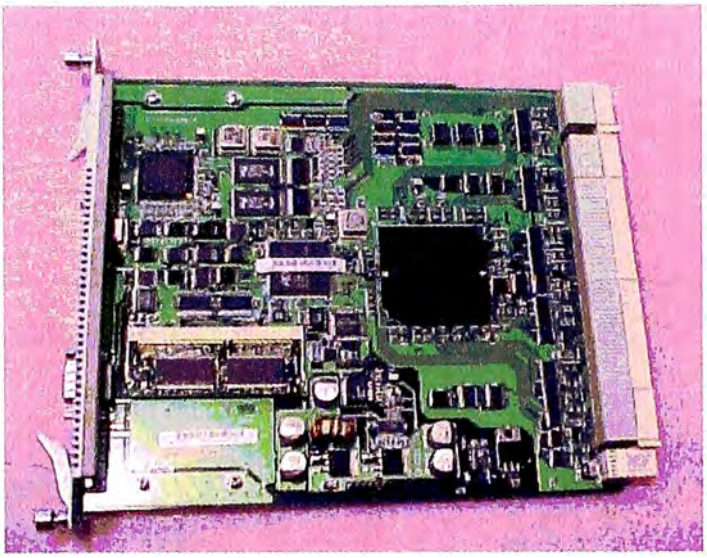

Figura 5.4 – Tarjeta principal

CAPÍTULO VI

DISEÑO DE UNA RED LAN REDUNDANTE

6.1 IMPORTANCIA DE LAS REDES DE ALTA DISPONIBILIDAD

La última década un número de desarrollos han aumentado la integración de las redes de cómputo con procesos básicos de negocios. Como beneficios de estas aplicaciones de redes, estas han sido reconocidas como parte de los procedimientos operacionales de los negocios y han ido cambiando gradualmente el punto de vista de los gerentes para optimizar el uso de sus aplicaciones. Donde el proceso revolucionario se ha ido desarrollando, las organizaciones han encontrado que sus procedimientos operacionales son severamente paralizados o descontinuados cuando la red se encuentra no disponible.

Mientras que las aplicaciones que trabajan en redes LAN se han convertido en indispensables o de misión critica en las organizaciones e industrias, estas aplicaciones se han convertido en la base de las empresas, dentro de las cuales podemos mencionar:

- El correo electrónico se ha convertido en el canal preferido en las comunicaciones internas y externas de las organizaciones. El correo electrónico

puede se fácilmente priorizado, mientras que el mensaje de voz no. El correo electrónico también permite que los mensajes alcancen una gran audiencia, produciendo un record de comunicaciones que soporta respuestas automáticas permitiendo adjuntar archivos multimedia. El correo electrónico, en conjunto con la telefonía proveen un alto sistema de comunicaciones redundantes.

- Los sistemas ERP (Enterprise Resource Planning) han sido desarrollados para automatizar cadenas de suministros de las grandes empresas en manufactura, distribución y servicios relacionados con las industrias. En estas organizaciones, la Base de Datos del ERP se han convertido en el repositorio más importante y es donde se almacena la información requerida para decisiones críticas del negocio. La tecnología de los ERP continua madurando y esta siendo personalizada para un gran numero de industrias y simplificada para uso de pequeños negocios.
- Una nueva generación de aplicaciones de negocios que trabaja en redes que están emergiendo, focalizando en aumentar la eficiencia de las unidades más importantes de las empresas tales como ventas, servicio a clientes, recursos humanos. El aumento de estas aplicaciones ha ocasionado el intercambio de información entre ellas y a través de los sistemas ERP demandando elementos de comunicaciones de alta velocidad.
- El Web browser y los motores de búsqueda se han convertido en la interfase universal de los usuarios para acceder a información crítica de negocios a través de Internet e Intranet. Redes de terminales dedicados y aplicaciones de emulaciones de terminal 3270 para acceder a aplicaciones mainframes están siendo retirados del mercado por el acceso a través de Web browser.

- El rápido crecimiento de Internet ha hecho que los sitios externos de Web un importante canal entre la comunicación del cliente y la distribución de productos. El sitio Web conduce automáticamente al comercio electrónico y entrega información de los productos, soporte a clientes, información al inversionista y materiales públicos y de mercadeo. El sitio Web externo es por si mismo una aplicación de misión critica aumentando la criticidad de la Intranet la cual depende del contenido diario y continuo seguimiento de los pedidos de los clientes.

En la medida que estas tendencias continúen en el futuro, cada vez será mas dramático los requerimientos de disponibilidad de la redes como convergencia del resultado de ofrecer multiservicios o redes convergentes. En el modelo multiservicio las redes de datos de hoy en día involucran una simple infraestructura de red basada principalmente en el protocolo IP y en la capacidad de soportar aplicaciones tradicionales mas un gran rango de demanda en tiempo real, aplicaciones y servicios de comunicaciones multimedia. Mas y mas servicios están siendo consolidados en una sola infraestructura, en consecuencia la disponibilidad de la red se ha vuelto mas critica para los empleados de la red siendo parte de la responsabilidad de su trabajo. Por ejemplo con correo electrónico y voz en la misma infraestructura son de misión crítica por lo que la red debe asegurar la disponibilidad de la operación de las aplicaciones a pesar que el correo electrónico no es una aplicación en tiempo real.

Entre los servicios de comunicaciones emergentes podemos señalar:

- El flujo de video en vivo es una aplicación en tiempo real, aplicación IP multicast que potencialmente esta revolucionando las comunicaciones corporativas

permitiendo a los ejecutivos participar en eventos corporativos sin la necesidad de viajar o interrumpir sus agendas de trabajo.

- Video en demanda o video playback, es una aplicación unicast de almacenamiento y envío que se aplica en entrenamiento a distancia u otros almacenamientos de contenidos, evitando la necesidad gastar costosos viajes o grabar cintas de video o CD-ROM.
- Conferencia multimedia es una aplicación unicast o multicast en tiempo real que aumentar la colaboración entre grupos de trabajo remotos.
- Voz sobre IP (VoIP), en la cual las señales de voz viajan digitalizadas y comprimidas por transmisión en redes sobre IP, ofreciendo la posibilidad de reemplazar las tradicionales PBX con servicios de telefonía LAN basados en muchas de las mismas tecnologías mencionadas como conferencia multimedia.

Es claro que a medida que las nuevas aplicaciones están siendo implementadas en las infraestructura de redes de las empresas, están demandan mayor ancho de banda y alta disponibilidad de la red debido a la gran cantidad de aplicaciones criticas que trabajan en esta infraestructura.

6.2 REDES BASADAS EN DISPOSITIVOS TOLERANTES A FALLAS

Una aproximación en la construcción de redes de alta disponibilidad es el uso extremo de dispositivos tolerantes a fallas a través de la red como se muestra en la figura 6.1. Para asegurar la alta disponibilidad extremo a extremo, cada dispositivo tolerante a fallas debe ser optimizado. Esto se asegura brindando backup redundantes en cada dispositivo de los equipo de comunicaciones, por ejemplo un Switch tolerante a fallas debe ser configurado con fuentes de poder redundantes,

ventiladores, Switch fabric y procesadores de Switch, además de aprovisionar enlaces redundantes vía interfaces físicas soportadas por los equipos.

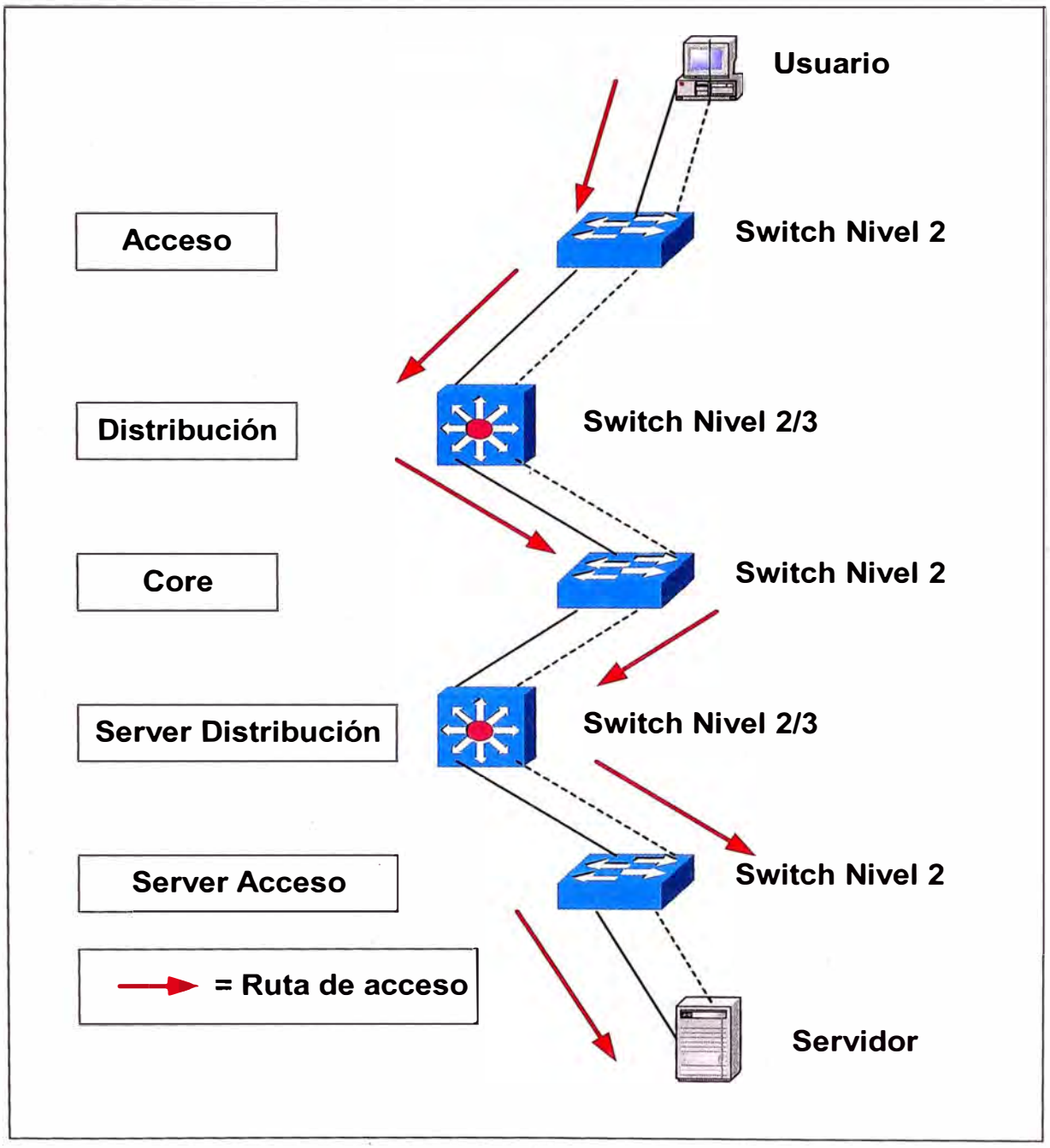

Figura 6.1 – Niveles de una red

Con el grado de redundancia interna, es posible calcular el nivel del dispositivo hasta en 10,000 horas de MTBF (Mean Time Between Failure – Tiempo promedio entre

fallas). Asumiendo que el MTTR (Mean Time to Repair – Tiempo promedio de reparación) es una hora, este MTBF puede corresponder teóricamente a un dispositivo de alta disponibilidad de 99.999%. Mientras que los cálculos teóricos del MTBF por hardware de dispositivo puede resultar en números impresionantes, tratar de tener redes de alta disponibilidad solo a través de dispositivos redundantes tiene algunos puntos en contra tales como.

- Redundancia masiva en cada dispositivo adiciona costo significativo a cada equipo, mientras que al mismo tiempo reduce la capacidad física de consumir ranuras que pueden servir como interfases de redes internas o para proveer servicios de red.
- Subsistemas redundantes con dispositivos son frecuentemente mantenidos en modo standby (en espera), donde estos no pueden contribuir adicionalmente al rendimiento de la red debido a que solo son activados cuando el componente primario falla.
- Focalizarse en dispositivos de hardware puede resultar en un número de otros mecanismos de fallas. Los elementos de redes no son dispositivos stand-alone (solos) pero son componentes de un sistema de red el cual tiene operaciones internas y niveles de interacción que son gobernados por software y parámetros de configuración. Cada componente del sistema de la red también reside en un ambiente físico que requiere energía eléctrica, control de temperatura y operadores humanos. Imperfecciones en cualquiera de estos aspectos de la red tiene una potencial causa de fallas que no pueden se controladas aisladamente.

En consecuencia si una red de producción esta diseñada con muchos dispositivos tolerantes a fallas pero con múltiples puntos de falla como se muestra en la figura

6.1, los aspectos mencionados anteriormente pueden ser puntos dominantes que causan que las redes dejen de funcionar. Cada falla que ocurre y que requiere intervención humana para diagnostico y reparación, resultan en un tiempo típico de caída o MTTR de 2 a 4 horas. Así con puntos simples de falla en el diseño de la red, el gasto económico de estos dispositivos redundantes produce pequeñas mejoras en términos de alta disponibilidad de toda la red.

6.3 REDES CON TOPOLOGÍAS REDUNDANTES

Otro camino de construir redes de alta disponibilidad es proveer redundancia en la topología de la red, con este diseño aproximado el campus de red mostrado en la figura 6.1 se puede modificar como se muestra en la figura 6.2. Esta nueva red de alta disponibilidad tiene un número de potenciales ventajas:

- Los elementos de la red proveen redundancia que no necesitan colocadas en los elementos primarios de la red. Esto reduce la probabilidad de problemas con el ambiente físico que pueda interrumpir el servicio.
- Problemas con software bucles/upgrades o cambios/errores de configuración pueden ser efectuados separadamente en las rutas primarias y secundarias sin interrumpir el servicio. Así el nivel de redundancia de la red puede también impactar en los mecanismos de fallas de los componentes que no son hardware.
- Con la redundancia provista por la red, cada dispositivo de la red no necesita ser configurado con tolerancia a fallas. La tolerancia a fallas de los dispositivos puede ser concentrado en los niveles de Core y Distribución de la red donde una falla de hardware puede afectar una gran cantidad de usuarios. Se puede decir

que la necesidad de adquirir dispositivos redundantes puede ser reemplazado por la adquisición de equipos adicionales para la redundancia.

- Con características de resilencia apropiada mas un cuidadoso diseño y configuración, la carga del tráfico entre los respectivos niveles de la topología de la red puede ser compartido entre los enlaces primarios y secundarios. Así el nivel de redundancia también puede agregar rendimiento y capacidad de la red lo cual ayudad a reducir el costo incremental de la red redundante.
- Redes redundantes pueden ser configurados automáticamente en caso de fallas pasando de los enlaces primarios a los secundarios sin intervención del operador. Durante la interrupción del servicio es igual al tiempo que toma la falla es decir pocos segundos.

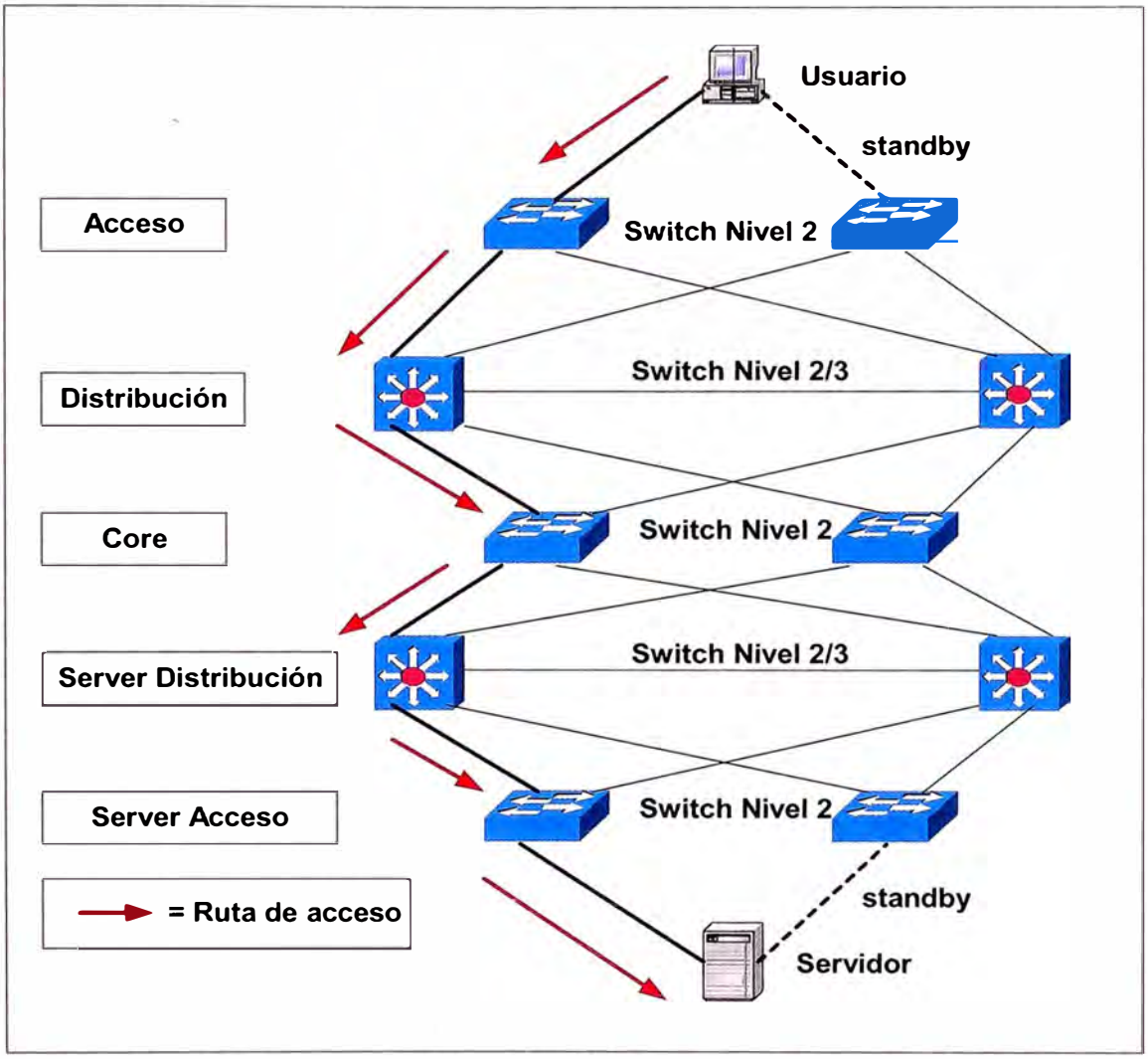

Figura 6.2 – Redes redundantes

6.4 TIEMPOS DE RESPUESTA EN REDES REDUNDANTES

Este es un ejemplo de pruebas realizadas en los laboratorios del Fabricante Cisco con la configuración de red que se muestra en la figura 6.3.

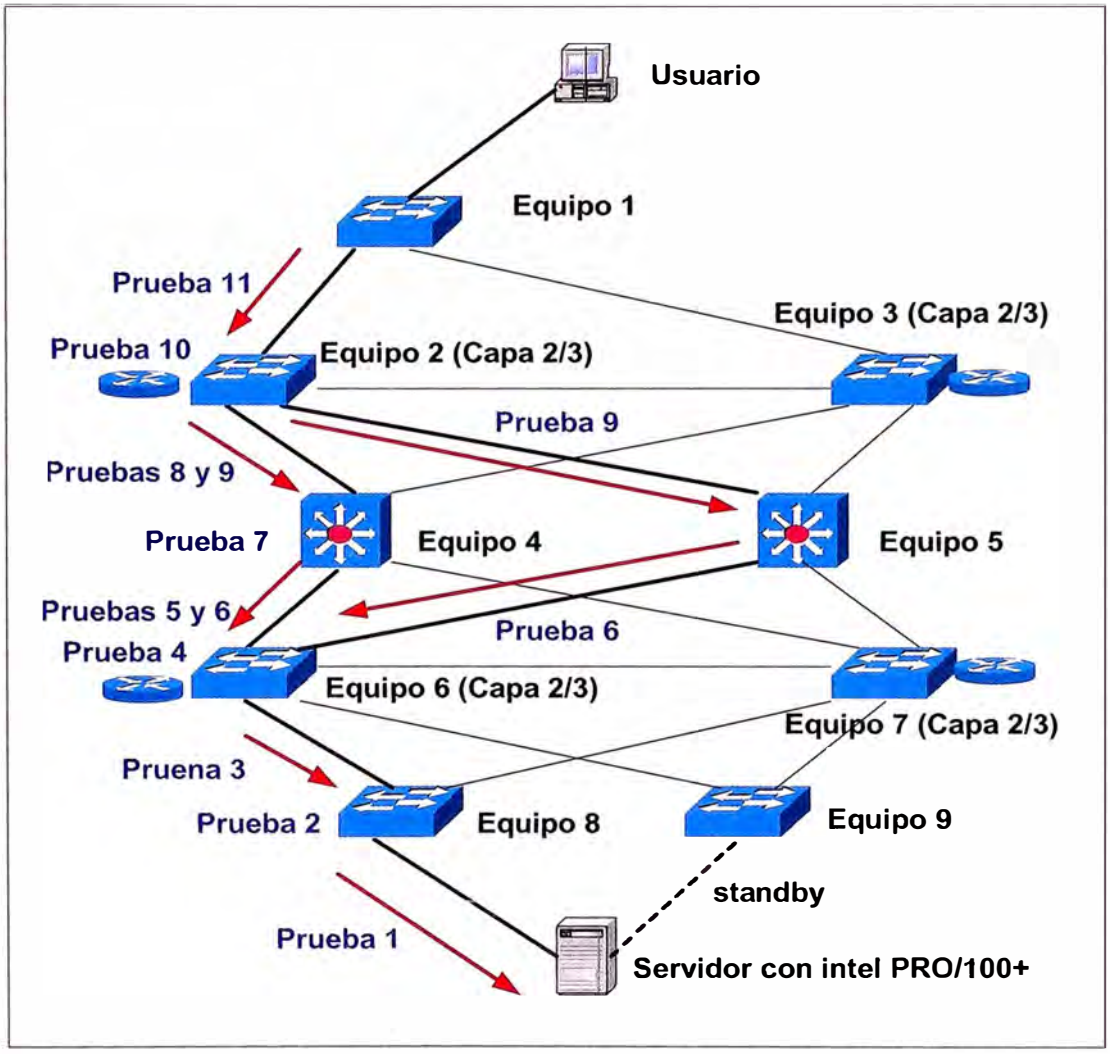

Figura 6.3 – Pruebas en una red redundante

El procedimiento de las pruebas fue el siguiente:

PRUEBA 1: FALLA DEL ENLACE DEL SERVIDOR

En esta prueba, el enlace primario del servidor al Switch de acceso (Equipo 8) fue removido causando falla en el enlace, haciendo que se active el enlace secundario del servidor al Switch de acceso (Equipo 9) según la figura 6.3. El servidor fue equipado con una tarjeta Ethernet dual intel PRO/100+ configurado en el modo AFT (Adapter Fault Tolerant). El tiempo de falla entre los puertos de la tarjeta intel PRO/100+ primaria y secundaria es determinado por el intervalo de polling (preguntar estado)

configurado en la tarjeta la cual fue configurada a 2 segundos para esta prueba. En enlace entre switches entre el Equipo 9 y Equipo 6 tuvo siempre un enlace activo para la VLAN del servidor es decir el Equipo 9 estuvo siempre disponible para enviar tráfico al servidor tan pronto como se activara el puerto de la tarjeta secundaria. El tiempo de falla observado en la red fue de 02 segundos.

PRUEBA 2: FALLA DEL SWITCH DE ACCESO PRIMARIO (EQUIPO 8)

En esta prueba, la falla del Equipo 8 fue simulada removiendo el conector de la fuente de poder del Switch. El proceso de falla es idéntico al de la prueba 1 y el tiempo observado de falla de la red fue de 02 segundos. Aunque este no fue probado, el mismo comportamiento de la falla y tiempo de recobro fue esperado al igual que en el caso de la falla de la interfase del modulo del puerto del Switch o la falla del puerto primario de la tarjeta dual del servidor.

PRUEBA 3: FALLA DEL ENLACE PRIMARIO DEL SWITCH DE ACCESO

En esta prueba, el enlace entre el Switch de acceso (Equipo 8) y el Switch de distribución (Equipo 6) fue removido para simular esta falla. Con esta falla, la ruta bloqueada entre el Equipo 8 y el Equipo 7 debió activarse, con el tráfico entre el Equipo 7 y el Equipo 6 a través del enlace entre switches.

Con el enlace habilitado en los switches de acceso, la ruta del Equipo 8 al Equipo 7 había sido preseleccionado por el protocolo spanning tree siendo la ruta secundaria y cuando la falla ocurrió el enlace secundario se activo tan pronto como se detecto en rompimiento de la conectividad del enlace primario. El tiempo de falla observado en

la red fue de 02 segundos. Con la operación normal del spanning tree y los valores de los parámetros por defecto, esta falla podría haber tomado hasta 30 segundos.

PRUEBA 4: FALLA DEL SWITCH DE DISTRIBUCIÓN

La falla del Switch de Capa 2/3 (Equipo 6) fue simulada, removiendo su conexión eléctrica. En este escenario varias fallas ocurren separadamente antes de que el servicio se recobrado: El tráfico que fluye a través del Equipo 8 es recibido a través de la activación del enlace hacia el Equipo 7 al igual que en la prueba 3, spanning tree para la VLAN del servidor tiene que reconverger, el RSM (Route Switch Module) del Equipo 7 tiene que convertirse en el router activo HSRP (Hot Standby Routing Protocol) para la VLAN del servidor, así el OSPF activa la ruta de capa 3 desde el Equipo 7 al Switch de Core (Equipo 4). En la configuración de demostración de la red de la figura 6.3, los tiempos del protocolo HSRP han sido configurados a menos de 01 segundo, el intervalo de "Hello" del OSPF (Para ver estado del enlace) a 01 segundo y el intervalo de "dead" (Comando que avisa la no actividad de un enlace) a 03 segundos. Con esta configuración se observó que el tiempo de recobro de la red fue de 9 a 10 segundos incluyendo todas las actividades de fallas mencionadas anteriormente.

PRUEBA 5: FALLA DEL ENLACE DEL SWITCH DE DISTRIBUCIÓN AL SWITCH DE CORE

En esta prueba, la capa 3 del enlace entre el Switch de distribución (Equipo 6) y el Switch de Core (Equipo 4) fue removido para simular esta falla. Anteriormente a esta falla la capa 3 del Switch de Core había sido configurado para balanceo de carga

entre los dos enlaces que salen del equipo 2 hacia los switches de Core (Equipo 4 y 5) Desde que el balanceo de carga fue configurado, todo el tráfico del usuario al servidor fluye a través del enlace fallido de capa 3. Con el balanceo de carga configurado, el tráfico puede inmediatamente continuar a través del Core vía el Equipo 5. En la resolución del tiempo medido en este mecanismo empleado se observó que el tiempo de recobro fue instantáneo (o segundos).

PRUEBA 6: FALLA DE AMBOS ENLACES DEL SWITCH DE DISTRIBUCIÓN AL SWITCH DE CORE

Ambos enlace del Switch de Core (Equipo 6) fueron simultáneamente removidos. En esta escenario de falla el Equipo 6 retiene una ruta al Core vía su enlace de capa 2 al Equipo 7. Así podría ser posible para el Equipo 6 mantener el router primario HSRP para la VLAN del servidor, pero esto involucrar un salto de ruta extra debido a que el tráfico podría fluir directamente al Equipo 7 y luego al Core. La característica del HSRP ha sido configurada para que la prioridad de la ruta del Equipo 6 se disminuida en el evento de falla de los enlaces al Core. La disminución de la prioridad ha sido escogida como un camino si y solo si un enlace falla (como en la prueba 5), el Equipo 6 podría mantener el HSRP primario, pero si ambos enlaces fallan, la prioridad del Equipo 6 podría disminuir de prioridad al router HSRP secundario (el RSM del Equipo 7). Con el Equipo 7 asumiendo el rol de router primario al Core, el tiempo total de falla es determinado por los tiempos de los HSRP que están en espera y los tiempos del OSPF como en la prueba 4. El tiempo de falla observado para la prueba fue de 6 a 8 segundos.

PRUEBA 7: FALLA DEL SWITCH DE CORE

En esta prueba simula la falla del Switch de Core (Equipo 4). El mecanismo de falla y los resultados son esencialmente los mismos de la prueba 5.

PRUEBA ADICIONALES

Fallas adicionales fueron simuladas del lado del usuario hacia el Switch Core, distribución y acceso como se indica en la figura 6.3 con las pruebas del 8 al 11. La descripción y resultados de estas pruebas son las mismas que corresponden a la pruebas realizadas del lado del servidor al Switch de Core, distribución y acceso, por lo que no fueron repetidas aquí. El resultado de todas las pruebas se resumen en la tabla 6.1.

PRUEBA	MECANISMO DE FALLA	TIEMPO DE RECUPERACIÓN
1	Enlace del servidor	2 segundos
2	Switch de acceso (Equipo 8)	2 segundos
3	Enlace de subida al Switch de acceso	2 segundos
4	Switch de distribución (Equipo 6)	9-10 segundos
5	Enlace de subida del Switch Core	0 segundos
6	Ambos enlaces de subida del Switch Core	6-8 segundos
7	Switch Core (Equipo 4)	0 segundos
8	Enlace de subido al Switch Core	0 segundos
9	Ambos enlaces de subida al Switch Core	6-8 segundos
10	Switch de distribución (Equipo 2)	9-10 segundos
11	Enlace de subida del Switch de acceso	2 segundos

Tabla 6.1 – Tabla de tiempos de recuperación

6.5 EJEMPLOS DE DISEÑOS DE REDES REDUNDANTES

A continuación se mostrará algunos ejemplos de redes redundantes sugeridos por algunos fabricantes de equipos de comunicaciones.

RED REDUNDANTE CISCO: En la figura 6.4 se muestra un diseño con equipos CISCO para una red de campus que esta integrada por 03 edificios y en cada uno de estos edificios se encuentran los switches de acceso y distribución con enlaces redundantes por otro lado tenemos los switches de Core que integran la comunicación de los edificios y por último los servidores corporativos agrupados con switches de distribución con enlaces redundantes.

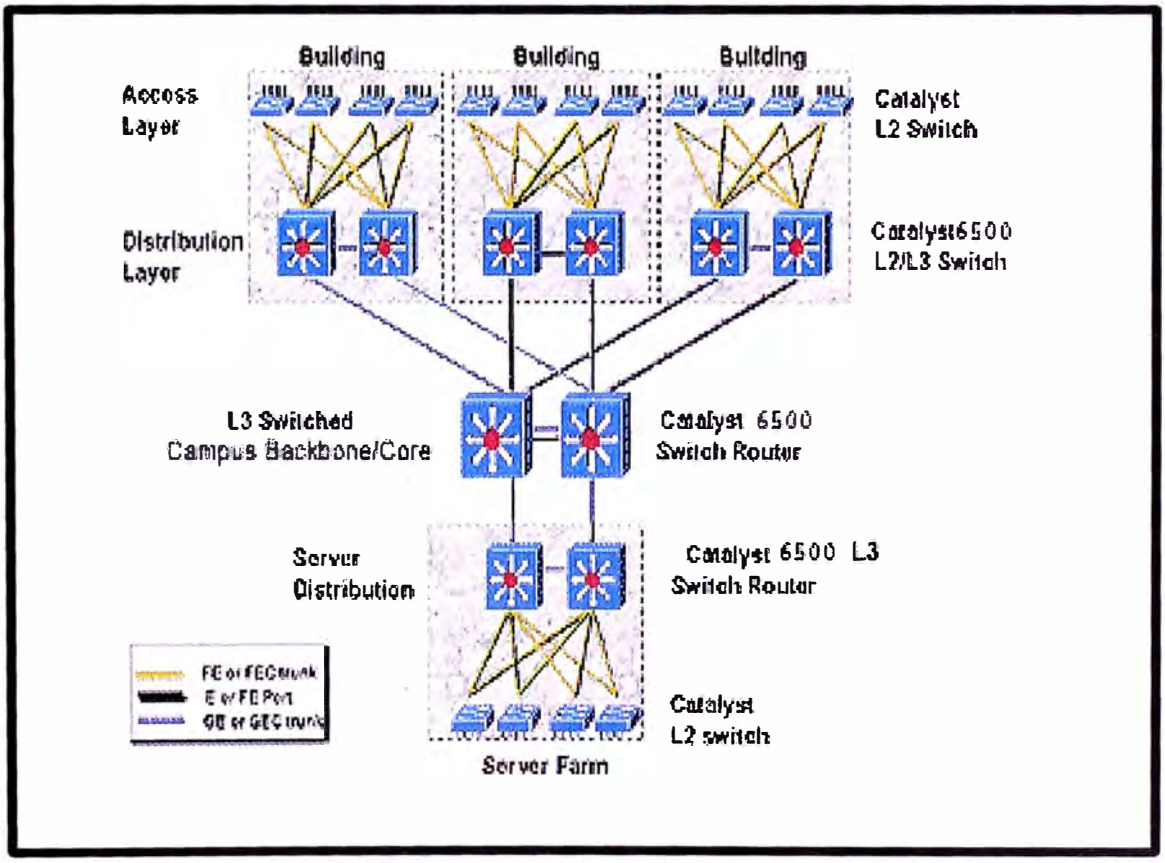

Figura 6.4 – Red redundante Cisco

RED REDUNDANTE 3COM: En la figura 6.5 se muestra un diseño con equipos 3Com para una red que está integrada por 04 grupos de trabajo unidos con switches de grupo con enlaces redundantes a los switches de Core. Estos switches de Core se encuentran conectados con enlaces redundantes y se conectan con los servidores también con enlaces redundantes.

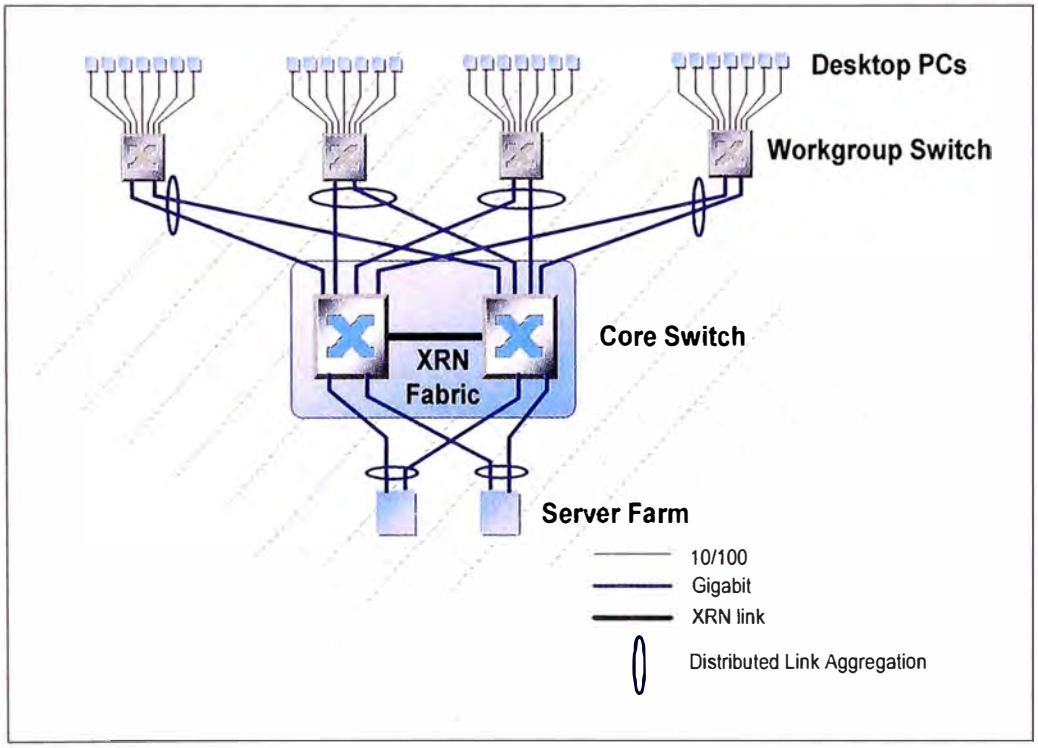

Figura 6.5 – Red redundante 3Com

CAPÍTULO VII

COSTOS DE UNA RED REDUNDANTE

7.1 EJEMPLO DE UNA RED DE CAMPUS

Se tiene una red de campus conformada por 03 edificios y 01 centro de computo dispersos en un radio de 0.5 Km. La cantidad de usuarios están distribuidos de acuerdo a la tabla 7.1, 7.2, 7.3 y 7.4 que se muestra a continuación:

EDIFICIO A	
Piso	Cantidad de usuarios
5	54
4	65
3	57
2	70
Piso	Cantidad de Servidores
1	2

Tabla 7.1 – Usuarios del edificio A

EDIFICIO B	
Piso	Cantidad de usuarios
3	71
2	66
Piso	Cantidad de Servidores
1	1

Tabla 7.2 – Usuarios del edificio B

EDIFICIO C	
Piso	Cantidad de usuarios
4	56
3	64
2	68
Piso	Cantidad de Servidores
1	2

Tabla 7.3 – Usuario del edificio C

CENTRO DE COMPUTO	
Piso	Cantidad de Servidores
1	5

Tabla 7.4 – Usuarios del centro de computo

Los tres edificios A, B y C se conectan al centro de computo a través de fibra óptica (cada enlace con 6 pares de fibra), todos los edificios están cableado con cable UTP categoría 6 en cobre (soporta velocidades de 10/100/1000 Mbps), en el centro de computo se encuentran 05 servidores con aplicaciones corporativos con tarjetas internas de 1Gbps con conexión en fibra, todos los usuarios de la red tienen tarjetas de red internas de 10/100 Mbps y los servidores de archivos de cada edificio tienen también tarjetas de red internas de 100/1000 Mbps.

7.2 DISEÑO DE LA RED

Para el ejemplo anterior se realizará el diseño con equipos de marca 3Com de acuerdo al siguiente detalle:

Como se observa todos los pisos tienen el siguiente rango de usuarios:

48 usuarios < número de usuarios de cualquier piso < 72 usuarios

Por lo tanto se utilizará 03 switches de 24 puertos en cada piso, estos switches estarán formando una pila (stack) de 72 puertos, adicionalmente se está agregando dos tarjetas de 1Gbps en cobre para se colocados en 02 de los switches de la pila para conectarse al Backbone haciendo un enlace trunking de 2Gbps. El modelo de Switch que reúne estos requisitos es el SS3 Switch 4400 SE 24 ports. Como se muestra en la figura 7.1.

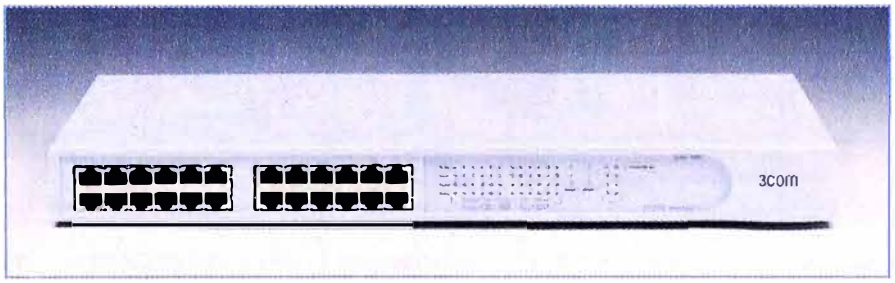

Figura 7.1 Switch de acceso

Como Switch de distribución de cada edificio se utilizará el SS3 Switch 4950 el cual viene con 12 puertos 10/100/1000 Mbps en cobre y 6 puertos 1000 BaseSX en fibra, como se muestra en la figura 7.2. Los puertos de cobre servirán para conectar las pilas de switches de cada piso y los puertos de fibra para conectarse al Switch de Core del centro de computo.

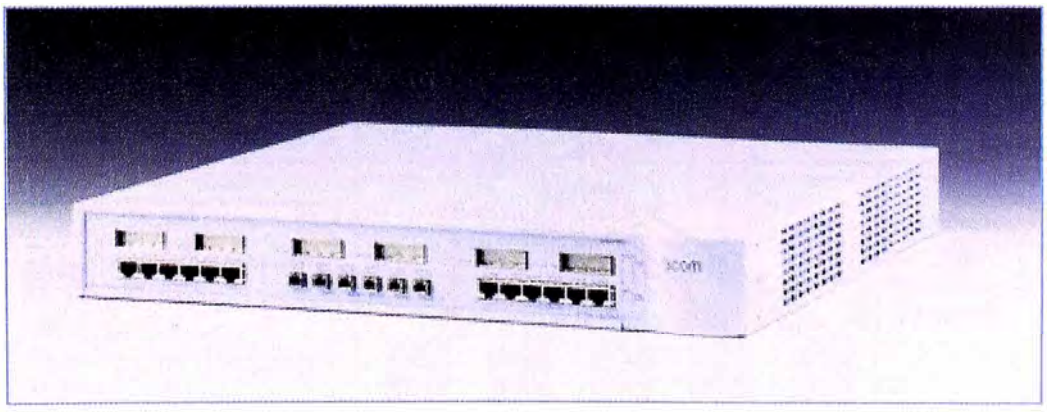

Figura 7.2 – Switch de distribución

Como Switch de core se utilizará el Switch 3Com 4007R Layer 2 Starter Kit que viene con 18 puertos de fibra a 1Gbps, como se muestra en la figura 7.3.

Figura 7.3 – Switch de core

Por lo tanto el diagrama total de la solución es como se muestra en la figura 7.4

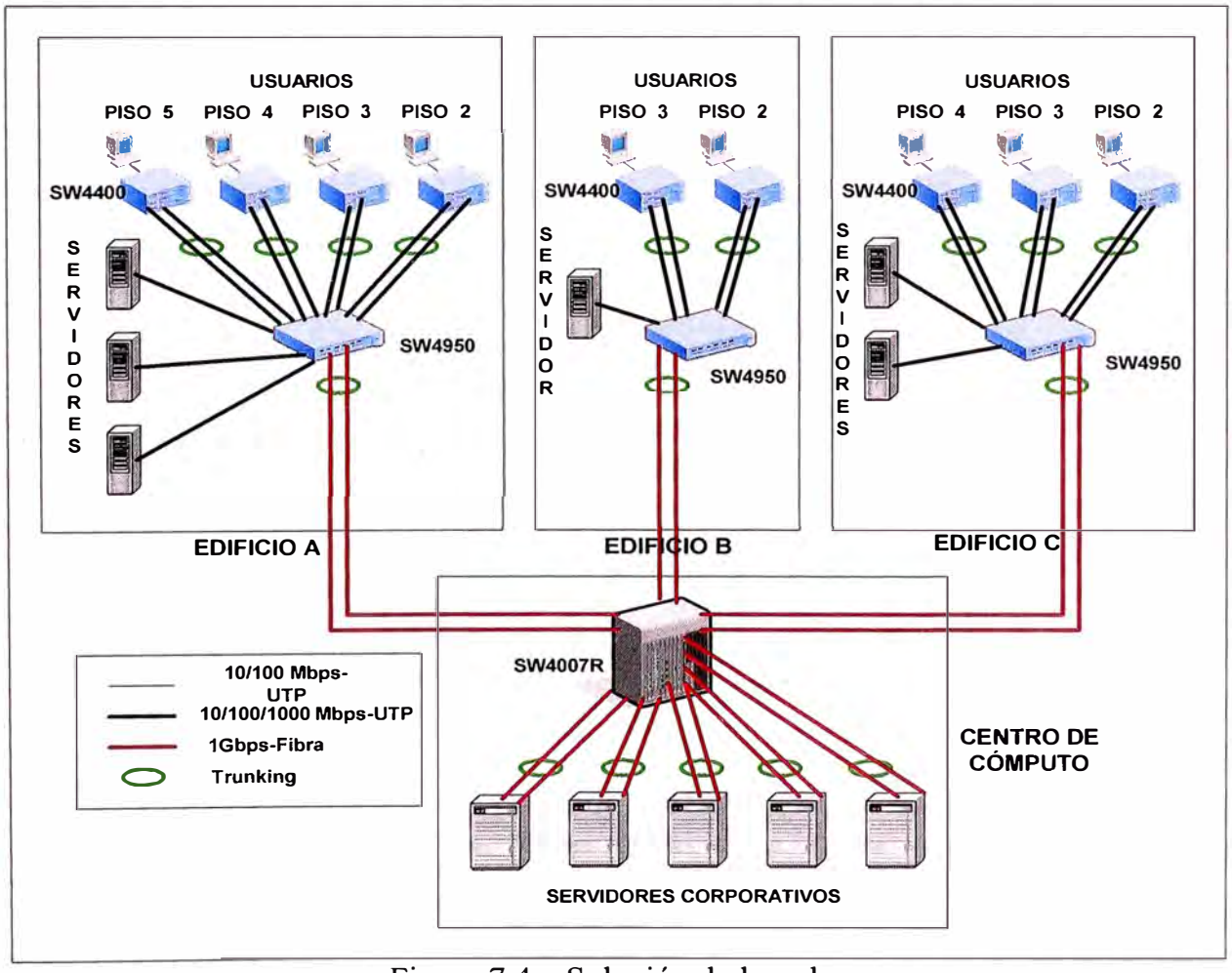

Figura 7.4 – Solución de la red

Adicionalmente se muestra la tabla 7.5 con la estructura de costos para la solución anteriormente planteada.

EDIFICIO A				
ITEM	**DESCRIPCIÓN**	**CANT.**	**COSTO UNITARIO US $**	**COSTO TOTAL US $**
01	SS3 Switch 4400 SE 24 ports	12	1,245.00	14,940.00
02	SS3 Switch 4400 1000BaseT module	08	395.00	3,160.00
03	SS3 Switch 4400 Stacking kit	08	445.00	3,560.00
04	SS3 Switch 4950	01	13,995.00	13,995.00
EDIFICIO B				
01	SS3 Switch 4400 SE 24 ports	06	1,245.00	7,470.00
02	SS3 Switch 4400 1000BaseT module	04	395.00	1,580.00
03	SS3 Switch 4400 Stacking kit	04	445.00	1,780.00
04	SS3 Switch 4950	01	13,995.00	13,995.00
EDIFICIO C				
01	SS3 Switch 4400 SE 24 ports	09	1,245.00	11,205.00
02	SS3 Switch 4400 1000BaseT module	06	395.00	2,370.00
03	SS3 Switch 4400 Stacking kit	06	445.00	2,670.00
04	SS3 Switch 4950	01	13,995.00	13,995.00
CENTRO DE CÓMPUTO				
01	4007R Layer 2 Starter Kit	01	33,995.00	33,995.00
			TOTAL US $	124,715.00

Tabla 7.5 – Costos de la solución

Estos precios no incluyen el IGV y están expresados en Dólares Americanos.

7.3 DISEÑO DE LA RED REDUNDANTE

Para el ejemplo anterior para tener una red redundante se debe agregar un Switch 4950 adicional en cada edificio así como las tarjetas de red Gigabit adicional para cada servidor. En el centro de computo se debe agregar un equipo Switch de Core 4007R y adicionalmente se ha adicionado 02 switches 4900 de 12 puertos 1000BaseSx de fibra para manejar la redundancia con los servidores corporativos,

adicionalmente se debe añadir 1 tarjeta de 1Gbps de fibra para cada servidor corporativo, en la figura 7.5 se muestra el equipo de distribución para los servidores que es el SS3 Switch 4900 SX.

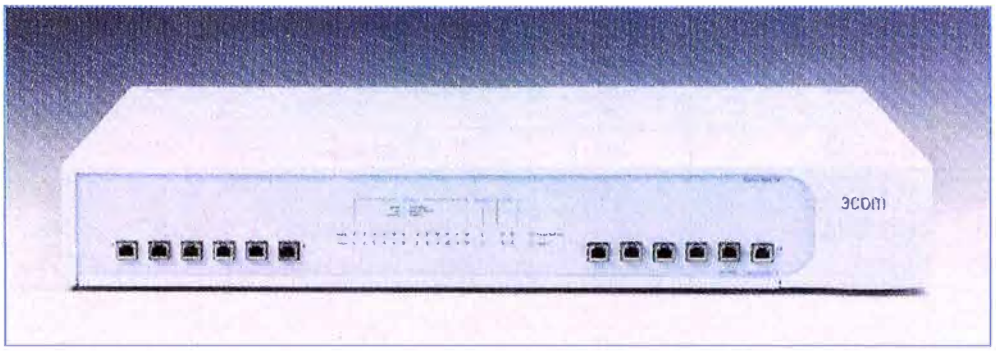

Figura 7.5 – Switch de acceso a servidores

Por lo tanto el nuevo diseño de la red será como se muestra en la figura 7.6.

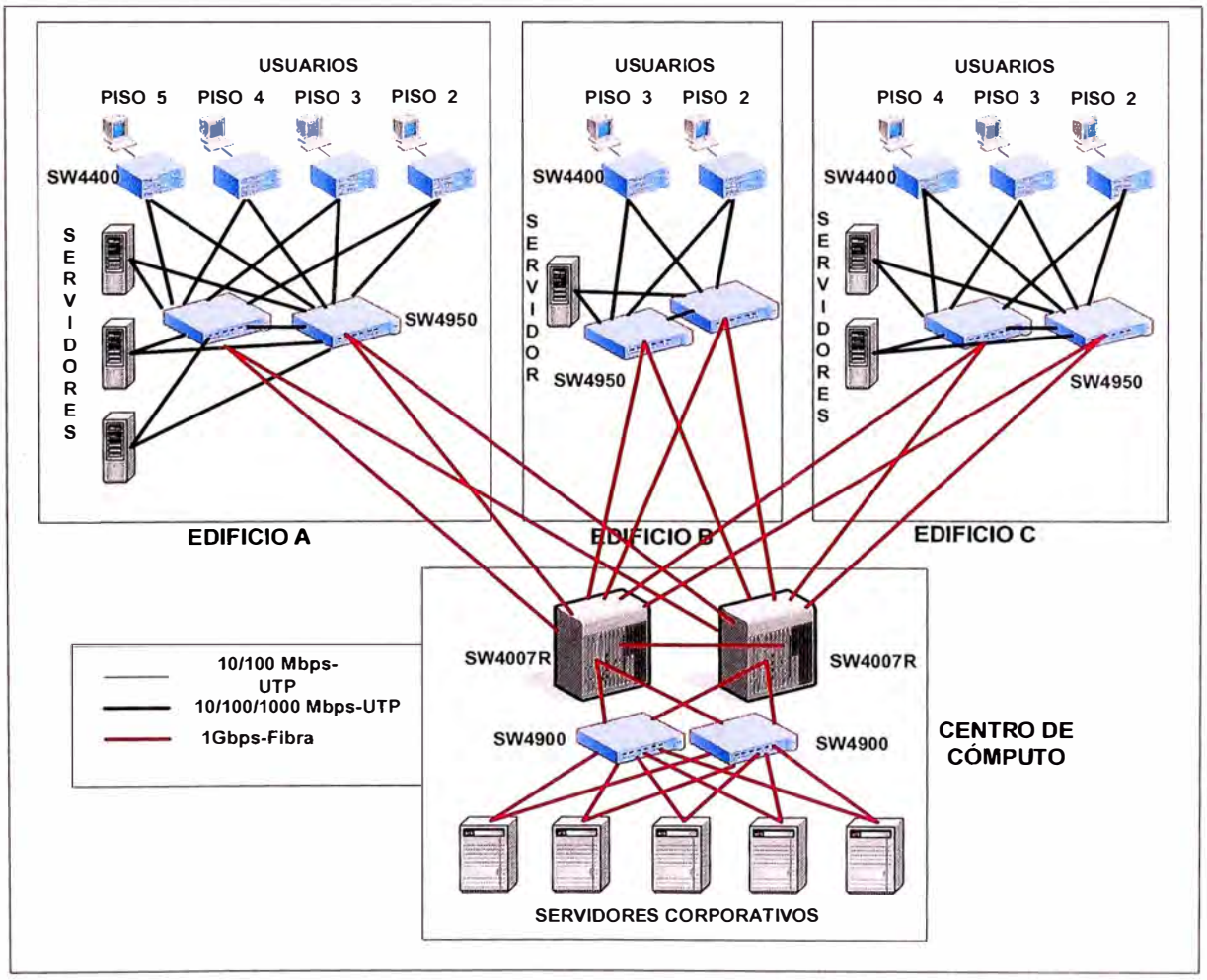

Figura 7.6 – Solución de la red con redundancia

Finalmente la nueva estructura de costos se muestra en la tabla 7.6.

EDIFICIO A				
ITEM	**DESCRIPCIÓN**	**CANT.**	**COSTO UNITARIO US $**	**COSTO TOTAL US $**
01	SS3 Switch 4400 SE 24 ports	12	1,245.00	14,940.00
02	SS3 Switch 4400 1000BaseT module	08	395.00	3,160.00
03	SS3 Switch 4400 Stacking kit	08	445.00	3,560.00
04	SS3 Switch 4950	02	13,995.00	27,990.00
05	3Com Gigabit Copper Server NIC 710025 (0.5MB)	03	295.00	885.00
EDIFICIO B				
01	SS3 Switch 4400 SE 24 ports	06	1,245.00	7,470.00
02	SS3 Switch 4400 1000BaseT module	04	395.00	1,580.00
03	SS3 Switch 4400 Stacking kit	04	445.00	1,780.00
04	SS3 Switch 4950	02	13,995.00	27,990.00
05	3Com Gigabit Copper Server NIC 710025 (0.5MB)	01	295.00	295.00
EDIFICIO C				
01	SS3 Switch 4400 SE 24 ports	09	1,245.00	11,205.00
02	SS3 Switch 4400 1000BaseT module	06	395.00	2,370.00
03	SS3 Switch 4400 Stacking kit	06	445.00	2,670.00
04	SS3 Switch 4950	02	13,995.00	27,990.00
05	3Com Gigabit Copper Server NIC 710025 (0.5MB)	02	295.00	590.00
CENTRO DE CÓMPUTO				
01	4007R Layer 2 Starter Kit	02	33,995.00	67,990.00
02	SS3 Switch 4900 SX	02	7,200.00	14,400.00
03	3Com Gigabit Fiber-SX Server NIC 710011 (0.5MB)	05	995.00	4,975.00
			TOTAL US $	221,840.00

Tabla 7.6 – Costos de la solución redundante

CONCLUSIONES

1. La implementación de las redes redundantes aplican para empresas con una gran cantidad de usuarios y que cuenten con aplicaciones críticas donde tener la red fuera de servicio implica grandes pérdidas de dinero.

2. El diseño y la implementación de una red redundante en una empresa debe ser parte del plan de contingencia de la misma donde además se debe tener en cuenta la redundancia en los servidores y aplicaciones críticas de la empresa (Cluster).

3. Los grandes fabricantes de equipos de comunicaciones no solo tienen equipos con dispositivos tolerantes a fallas si no también cuentan con equipos que soportan tecnología para implementar redes redundantes.

4. La implementación de redes con equipos que cuentan con múltiples dispositivos tolerantes a fallas hace mas compleja la administración, por eso las redes redundantes a pesar de incrementar los costos de implementación inicial, tiene

beneficios tales como la de balancear carga de la red, mejorar el rendimiento de la misma y los mas importante es que los procesos en caso de fallas son automáticos y no requieren de intervención del operador.

5. En el proceso de implementación y durante todo el funcionamiento de la red es necesario tener una consola de administración para monitorear los equipos de la red y tomar medidas preactivas en caso de fallas, así mismo esta administración nos permitirá optimizar los enlaces de la red.

6. Para tener un proceso exitoso durante y después de la implementación de una red redundante es necesario que departamento encargado de las comunicaciones sean entrenados adecuadamente y formen parte del proceso de implementación.

GLOSARIO

10Base-T

Nombre técnico para las redes de par trenzado.

802.3

Estándar IEEE para Ethernet.

Algoritmo

Procedimiento matemático o lógico para realizar un cálculo o para resolver un problema. Sucesión de operaciones elementales, perfectamente especificadas y ordenadas, que sirven para hacer algo preciso.

Ancho de banda (Bandwidth)

Define la cantidad de información que puede ser transmitida en un periodo de tiempo determinado a través de una Red. Es la diferencia entre la frecuencia más alta y la más baja de un canal de transmisión (en hertz, Hz). Margen de frecuencias capaz de transmitirse por una red de telecomunicaciones.

ANSI (American National Standards Institute)

El Instituto Nacional Norteamericano de Normalización es la organización responsable de aprobar las normas de los EEUU en muchas áreas, ordenadores y comunicaciones, y es miembro de ISO.

Árbol

Estructura de representación de la información que consiste en un único registro "padre" del que dependen cero o más registros "hijos" que, a su vez, pueden dar origen a nuevos subárboles.

ASCII.

American Standard Code for Information Interchange. Código estándar americano para intercambio de la información. Esquema normalizado de codificación de caracteres introducido en 1.963 y muy utilizado en muchas máquinas. Sistema de codificación de caracteres alfanuméricos en 7 bits para la operación interna del computador y su comunicación con los periféricos. Este sistema, promovido por el ANSI (American National Standard Institute), es ampliamente utilizado por ordenadores personales, estaciones de trabajo y miniordenadores.

Backbone

Red principal de una red de comunicaciones.

Base de datos.

(Data base) Conjunto de datos no redundantes, almacenados en un soporte informático, organizados de forma independiente de su utilización y accesibles simultáneamente por distintos usuarios y aplicaciones. La diferencia de una BD respecto a otro sistema de almacenamiento de datos es que estos se almacenan en la

BD de forma que cumplen tres requisitos básicos: no redundancia, independencia y concurrencia.

BIOS

(Basic Input Output System) Conjunto de rutinas básicas que se almacenan en memoria ROM. Este sistema incluye rutinas para el teclado, la pantalla, los puertos paralelos y serie y para servicios internos como hora y fecha. Acepta solicitudes desde las unidades de los dispositivos en el sistema operacional, así como desde los programas de aplicaciones.

Bit

Binary Digit. Dígito binario. Unidad mínima de información con la que trabajan los ordenadores. Es un dígito del sistema binario que puede tener el valor 0 o 1.

bps

(bits por segundo) Medida de velocidad de transmisión de datos.

Bridge

Puente. Unidad Funcional que interconecta dos redes de área local que utilizan el mismo protocolo de control de enlace lógico pero distintos protocolos de control de acceso al medio dentro del nivel 2 de OSI.

Broadcast

Es un sistema de entrega de paquetes que entrega una copia de un paquete dato a todos los equipos de una red Ethernet.

Buffer

Segmento reservado de memoria que se usa para almacenar datos mientras se procesan. Conjunto de registros conectados en paralelo que actúan como memoria

intermedia para almacenar datos temporalmente para compensar y adaptar diferencias de velocidad entre emisor y receptor.

Bus

Conjunto de líneas que transportan información binaria entre el procesador, la memoria y las unidades periféricas.

Byte

Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

Canal

Denominación general para una vía de transmisión lógica o física.

CCITT

Comité Consultivo Internacional de Telegrafía y Telefonía. Antiguo órgano competente de la Unión Internacional de Telecomunicaciones de las Naciones Unidas en asuntos de telefonía, telegrafía y datos, que coordinaba los Sistemas telefónicos y de comunicación de datos de todo el mundo. Con frecuencia, sus recomendaciones técnicas se convierten en normas reconocidas internacionalmente. Ha sido sustituido por la UIT-T (Unión Internacional de Telecomunicaciones - Telemática, ITU-T: Internacional Telecommunicacion Union - Telematics).

Cliente/Servidor

Arquitectura de sistemas de información en la que los procesos de una aplicación se dividen en componentes que se pueden ejecutar en máquinas diferentes. Modo de funcionamiento de una aplicación en la que se diferencian dos tipos de procesos y su soporte se asigna a plataformas diferentes.

Codificación

Transformación de un mensaje en forma codificada, es decir, especificación para la asignación unívoca de los caracteres de un repertorio (alfabeto, juego de caracteres) a los de otro repertorio. || Conversión de un valor analógico en una señal digital según un código prefijado.

Controlador

(Driver) Conjunto de programas, dispositivo electrónico (o ambos) que controla el intercambio de información entre el ordenador y un periférico.

Copia de seguridad

(Backup) Replicación periódica y almacenamiento externo (usualmente en discos y/o cintas) de datos y programas en previsión de posibles contingencias. Reproducción de los datos actuales guardados en un soporte informático, para tenerlos disponibles en caso de que un desastre del sistema impida recuperar los datos con los que se está trabajando.

CPU

(Central Processing Unit) Unidad Central de Proceso. Parte principal del ordenador que incluye la unidad aritmético-lógica (ALU) y la unidad de control (UC).

CSMA/CD

(Carrier Sense Multiple Access with Collision Detection) Protocolo de comunicaciones para una red de área local que utiliza una estructura en bus. Define los niveles físico y de enlace del modelo OSI para el método de acceso a la red por el cual una estación obtiene el uso del medio físico para enviar un mensaje a través de la red. La especificación de este protocolo se describe en las normas IEEE 802.3 e ISO 8802.3, ambas basadas en el estándar Ethernet.

Datagrama IP

Unidad básica de información que pasa a través de Internet.

Dúplex

Circuito o canal bidireccional que puede transmitir la información simultáneamente en ambas direcciones.

Dominio

Estructura jerárquica que organiza las máquinas de Internet de forma que sea fácil recordar su nombre.

EIA/TIA

(Electronic Industry Association / Telecommunication Industry Association) Asociación de la industria electrónica / Asociación de la industria de telecomunicaciones.

Encapsulación

Permite la conexión de varias redes informáticas entre sí para formar una sola red de nivel más alto. Cuando se utiliza encapsulación, se define un nuevo nivel de protocolo; esto proporciona una semántica uniforme para servicios tales como conmutación de paquetes, correo electrónico, etc.

Estándar

Conjunto de reglas y regulaciones acordado por una organización oficial de estándares (estándar de jure) o por aceptación general en el mercado (estándar de facto).

Ethernet

Red de área local ISO 8023 que transmite a 10 Mbits/s y pueden conectarse en total hasta 1024 nodos. Conjunto de especificaciones que definen el funcionamiento de redes locales CSMA/CD.

Encriptado

Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.

Enlace

(Link) Apuntador de hipertexto que sirve para saltar a otra página Web, a otro servidor, o a otro servicio (correo, FTP) cuando se navega por Internet.

Frame

Encuadre, bloque, secuencia, trama

Firewall

El "cortafuegos" es una medida de seguridad que se coloca entre una Red local e Internet, que filtra los paquetes que entran y salen hacia Internet desde una red local.

Frecuencia

El número de ciclos por segundo de una onda. Se mide en Hertzios (Hz), que indican el número de cambios por segundo.

FTP

(File Transfer Protocol) Protocolo para la Transferencia de

Ficheros.

Gateway

Puerta de acceso, pasarela. Unidad de interfuncionamiento. Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos

propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red RAL, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

Host

En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red.

Hub

Equipo para diversos tipos de cables y para diversas formas de acceso que sirve de plataforma integradora para distintas clases de cables y de arquitectura.

IEEE

(Institute of Electrical and Electronics Engineers) Instituto de Ingeniería Eléctricos y Electrónicos. Organismo normalizador de métodos de acceso y control para redes de área local. Es miembro de ANSI e ISO.

IP

(Internet Protocol) Protocolo Internet. Protocolo sin conexión (connectionless) encargado de controlar la información por la red. Permite la integración de otras subredes.

IRTF

(Internet Research Task Force) Es un grupo de gente que trabaja para resolver problemas relacionados con TCP/IP y conexiones a Internet.

ISO

(Internacional Organization for Standarization) Un grupo internacional que confecciona borradores, discusiones, propuestas y especificaciones de estándares para protocolos de redes.

Kbps

Kilobits por segundo. Medida de velocidad de transmisión.

KiloByte

(KB) Unidad de medida de memoria. Equivalencia: 1 KByte = 10 Bytes = 1.024 Bytes.

LAN

(Local Area Network) Red de área local.

LLC

(Logical Link Control). Control de enlace lógico. Protocolo de nivel de enlace del modelo OSI definido para redes de área local.

MAC

(Medium Access Control) Protocolo de control de acceso al medio empleado para la propagación de las señales eléctricas. Define el subnivel inferior de la capa 2 del modelo OSI (nivel de enlace).

MAN

Metropolitan Area Network. Red de Area Metropolitana. Red de comunicaciones que cubre un área geográfica como una ciudad o un suburbio.

Mbps

Megabits por segundo. Medida de velocidad de transmisión. 1Mbps = 10 bps (bits por segundo).

MegaByte

(MB) Unidad de medida de memoria que equivale a 1.024 KB.

Memoria caché

Memoria intermedia de acceso aleatoria muy rápida entre la unidad central de proceso y la memoria principal que almacena los datos o instrucciones extraídos más frecuente y recientemente de la memoria principal.

Multicast

Técnica que permite copias de un paquete simple se pasado a través un conjunto de equipos seleccionados.

NetBios

(Network Basic Input Output System) Es una interfase estándar para redes de computadoras IBM.

OSI

(Open Systems Interconnection) Interconexión de Sistemas Abiertos. Estándar ISO para comunicaciones a nivel mundial que define una estructura con el fin de implementar protocolos en 7 estratos o capas. El control se transfiere de un estrato al siguiente comenzando en el estrato de aplicación en una estación, llegando hasta el estrato inferior, por el canal hasta la próxima estación y subiendo nuevamente la jerarquía. Las 7 capas o estratos son: Físico, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación. El OSI requiere una enorme cooperación para que sea un estándar universal como el sistema telefónico.

OSPF

(Open Shortest Match First) Protocolo de enrutamiento diseñado por la IETF.

Paquete

Secuencia de dígitos binarios, incluyendo datos y señales de control, que se transmite y conmuta como un todo.

PC

(Personal Computer) Ordenador Personal. Ordenador generalmente monousuario y monotarea, que utiliza como CPU un microprocesador. Tradicionalmente asociado a los ordenadores de uso personal o doméstico.

PCI

(Peripheral Component Interconnect) Bus de 32 bits de longitud de palabra de datos para los ordenadores personales. Protocolo. Conjunto formal de convenciones que gobiernan el formato y control de datos. Conjunto de procedimientos o reglas para establecer y controlar transmisiones desde un dispositivo o proceso fuente a un dispositivo o proceso objeto.

Protocolo de comunicaciones

Reglas preestablecidas para efectuar la conexión electrónica entre dos sistemas de comunicación. Puede haber diferentes tipos, que establecen desde las normas para las tensiones eléctricas en los extremos de los contactos metálicos hasta reglas lógicas de alto nivel, como la organización de los datos a trasmitir, su modo de identificación, codificación, etc. Conjunto de reglas y convenios que posibilitan la transmisión de información a través de una red de telecomunicaciones. Conjunto de reglas semánticas y sintácticas que rigen el comportamiento de las unidades funcionales en las comunicaciones.

Puerto

(Port) Conector de la placa base para instalar elementos externos.

RFC

(Request for comments) Es el nombre de una serie de notas que contiene ideas, medidas, técnicas y observaciones que son propuestas y aceptadas para los protocolos estándar TCP/IP.

Router

Enrutador, encaminador de paquetes hacia su destino por la ruta óptima.

Router

(Direccionador) Dispositivo que se encarga de dirigir el tráfico en una red. La información pasa de nuestro ordenador a un router, y luego de router a router, hasta que el destino está en la misma red local que el último.

Servidor

Ordenador que ofrece sus prestaciones a varios ordenadores clientes conectados a una red.

TCP/IP

(Transmission Control Protocol/Internet Protocol) Protocolo de Control de Transmisión/Protocolo Interredes. Protocolo para el control de la transmisión orientado a la conexión (connection-oriented) TCP, establecido sobre el protocolo Internet (IP). Su amplia extensión permite reconocerla como una norma de facto aunque no es una norma internacional. Mientras que TCP es un protocolo de transporte (nivel cuatro de OSI), el IP es un protocolo de red. Son un conjunto de normas (nivel tres de OSI) para LANs definidas en Estados Unidos para los organismos de defensa para la DARPA (Defense Advanced Research Projects Agency), donde está definida la forma en que deben comunicarse los ordenadores, las redes entre sí y el encaminamiento del tráfico de la red.

UTP

(Unshielded Twisted Pair) Par trenzado no apantallado.

WAN

(Wide Area Network) Red de área extensa.

BIBLIOGRAFÍA

1. Rolf McClellan "Network-level Redundancy/Resilience for High-Availability Campus LANs", 1999.
2. Geoff Haviland "Designing High-Perfomance Campus Intranet with Multilayer Switching", 1998.
3. Cisco White Paper "Gigabit Campus Network Design-Principles and Architecture", 1999.
4. 3Com White Paper "Introduction to XRN: A new Direction for Enterprise Networking", 2002.
5. Presentación de 3Com "Enterprise Strategy Focus on the LAN Core", 2000.
6. Documento 3Com "Switch 4007R Getting Started Guide", 2002.
7. Carta Anuncio de Cisco "Cisco 7500 Series", 1997.
8. Presentación de 3Com "Switch 4007: Technical Training", 2001.
9. Presentación de 3Com "3Com LAN Switching Solutions", 2001
10. 3Com University "Gigabit Ethernet Technology: Overview", 2001