UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CRITERIOS PARA DISEÑO DE REDES LOCALES

T E S I S
QUE PARA OBTENER EL TÍTULO DE:

ING. MECÁNICO ELECTRICISTA
(ÁREA ELÉCTRICA - ELECTRÓNICA)

P R E S E N T A:

J. ENRIQUE FRANCIA CAMPOS

DIRECTOR DE TESIS: ING. MARIO IBARRA PEREYRA

Ciudad Universitaria 1998

AGRADECIMIENTOS

A Dios.

Por guiar mi vida a un camino lleno de éxitos y darme la fortaleza necesaria para enfrentar todos los retos.

A mis padres.

Por el amor y confianza con que siempre me apoyaron, y sobre todo por haberme dado lo más precioso, la vida misma.

A mi esposa.

Por su amor y comprensión que siempre me ha brindado, y sin lugar a dudas por su apoyo incondicional ofrecido.

A mis hermanos.

Arturo y Miguel, por su cariño con que siempre me aconsejaron, así como por su buen ejemplo.

Al Ing. Mario Ibarra.

Por su apoyo desinteresado para la realización de esta tesis.

Criterios Para Diseño de Redes Locales.

Índice

CAPÍTULO 1
Introducción

La presente tesis tiene los siguientes objetivos:

1. Exponer un panorama de la tecnología de punta reinante en las Redes de Área Local (LANs), Redes de Área Metropolitana (MANs) y Redes de Área Amplia (WANs).

2. Indicar las mejores opciones de aplicación de cada uno de los componentes de las tecnologías de LAN, MAN y WAN, así como las diferencias entre tecnologías similares, con la finalidad de obtener el mejor aprovechamiento de ellas.

Lo anterior se expondrá sin la intervención de fórmulas y/o algoritmos, sino simplemente apelando a la experiencia en este campo. No con ello se pretende minimizar la literatura que hace fuerte uso de las matemáticas, puesto que es indiscutible su valía, sin embargo en muchos de los casos el uso de las mismas no es tan práctico, como se pretende presentar aquí, que pese a no basarse totalmente en detalles matemáticos, sí lo hace en forma técnica y práctica.

Con el resultado de esta exposición se pretende incrementar el nivel técnico de aplicación en el campo de las Redes de Área Local, Redes de Área Metropolitana y Redes de Área Amplia, todas ellas áreas de tecnología de punta que permiten a los grandes corporativos mejorar la plataforma de cómputo que a su vez apoye la oportuna toma de decisiones y el incremento de velocidad en las consultas en áreas corporativas que así lo requieran.

Para poder cubrir lo anteriormente expuesto es necesario tocar los puntos medulares de diferentes temas, por lo que a continuación se presenta una breve introducción a cada uno de los capítulos que se incluyen en esta tesis. Se empezará por el capítulo 2.

Capítulo 2. Introducción a redes locales, donde se tratará el tema en sus conceptos básicos, el inicio de las redes locales en la historia de la informática y los componentes de las redes locales.

Capítulo 3. Se indican los pasos a seguir para implantar una red local; es decir, para implementar una red local, es necesario conocer la problemática que se desea resolver al implementar un sistema de este tipo, así como el obtener la información pertinente que permita llevar a buen término un proyecto que involucre redes locales.

Capítulo 4. Con la información obtenida anteriormente, se debe de elegir la arquitectura que más se apegue a resolver nuestras necesidades. Por tal motivo en este capítulo se indicará el área de aplicación de las arquitecturas más importantes en el ramo de las redes locales, así como las características de estas arquitecturas.

Capítulo 5. Teniendo claros los requerimientos que se desean cubrir, y la arquitectura adecuada, es necesario determinar el tipo de cableado con el que se deben realizar las conexiones entre los diferentes equipos, por lo que en este capítulo se determinarán las condiciones en que aplican los diferentes tipos de cableado.

Capítulo 6. Sin importar el tipo de cable, topología, arquitectura o tamaño de red, existen diversas tecnologías que permiten mejorar el comportamiento de la misma, en este capítulo abordaremos este tema, con la finalidad de que los servicios que provee una red y su calidad sean como los necesitamos.

Capítulo 7. Con los puntos vistos en los capítulos anteriores se puede implementar una red local, sin embargo lo más común es que al tener redes locales en diferentes lugares, éstas se deseen interconectar, por lo que se convierte en una necesidad el determinar como realizar estos enlaces, tanto en una misma localidad (MAN), como entre localidades (WAN).

Capítulo 8. Existen gran cantidad de aplicaciones y servicios que se pueden proveer en las redes locales para apoyar el desempeño adecuado de funciones del personal que hace uso de estas tecnologías, por lo que dependiendo de las necesidades de cada usuario y las aplicaciones a utilizar, se determinarán los tipos de estación de trabajo y servidor a utilizar.

Capítulo 9. Al haber determinado lo anterior es necesario indicar las diferencias, ventajas y desventajas entre los dos sistemas operativos de redes locales (NOS, Network Operating System), más populares, que existen en México.

Capítulo 10. Al tener una LAN, MAN o WAN, se requiere una infraestructura de administración de todos los recursos que pueden ser accesados por los usuarios, por lo que se incluye una serie de recomendaciones que deben tomarse en cuenta para implementar una plataforma de este tipo.

Capítulo 11. Para terminar, se incluyen puntos adicionales que se deben considerar, para que un proyecto de esta magnitud pueda llevarse a buen fin.

Capítulo 12. Conclusiones de los temas expuestos.

Capítulo 13. Glosario de términos.

CAPÍTULO 2
Introducción a Redes Locales

Temas del capítulo.

2.1 Definición de red local.

2.2 Antecedentes de las redes locales.

2.3 Ventajas de las redes locales en los corporativos.

2.4 Mitos de las redes locales.

2.5 Componentes de las redes locales.

2.1 Definición de red local.

El concepto de Red Local, LAN (Local Area Network), se ha venido aplicando desde mediados de la década de los años 70's, con la conectividad entre equipos mainframes, sin embargo el mayor auge de las LANs, se empieza a tener en esta década de los 90's, con la popularización de la computación, los sistemas de comunicación y su normatividad, apoyado todo esto con la participación creciente de los fabricantes de equipos y componentes de cómputo, mismos que ponen al alcance de las empresas la tecnología adecuada para implementar grandes y versátiles sistemas de cómputo.

Con la finalidad de poder profundizar en el tema se presenta la siguiente definición:

Red Local.- Intercomunicación de computadoras mediante puertos de comunicación (tarjetas de red local), que permitan accesar y compartir información, datos (nómina, contabilidad, documentos, etc.), software

comercial (Windows, Word, Lotus, etc.), desarrollos hechos "en casa", periféricos (impresoras, modems, etc.), servicios (Internet, e-mail, etc.) y espacio en disco duro de uno o más equipos, en un ambiente de cómputo homogéneo, ubicado en un mismo recinto.

Anteriormente las redes locales se delimitaban por el cableado, sin embargo hoy en día existen tecnologías en las que un mismo cable (fibra óptica) soporta distancias de hasta 50 Km; así mismo existen redes locales inalámbricas, por lo que delimitar la distancia de la red local basándose en el cable, ya no es totalmente cierto, debido a que por un lado 50 Km no se puede considerar local, ni solo asumiendo que todas las redes locales utilizan cableado. Por lo que al día de hoy se considera local cuando la red abarca una misma oficina o edificio.

En el momento que se utiliza algún dispositivo que permita alcanzar grandes distancias, se deja de llamar red local, y dependiendo su cobertura se denomina MAN (Metropolitan Area Network) considerándose en una misma ciudad, o WAN (Wide Area Network) con cobertura nacional o internacional, y si existen dos o más ambientes operativos enlazados se denomina GAN (Global Area Network) no importando su alcance.

Es importante indicar que al hablar de red local no implica que se conforme solo de equipo de cómputo personal, ya que también puede ser formada por minicomputadoras o mainframes.

2.2 Antecedentes de las redes locales.

Las redes locales de microcomputadoras tienen su origen en la década de los 80´s propiciado principalmente por los siguientes puntos:

- El gran auge de las PCs o microcomputadoras.
- El "boom" de la comercialización (y piratería) de paquetería como herramientas de apoyo para realizar a las funciones personales.
- El alto costo de los equipos periféricos y dispositivos de almacenamiento masivo.

Estos tres puntos se dan en una forma desmedida en una misma corporación, llegando al extremo que hasta en un mismo departamento se pueden encontrar dos o más procesadores de texto, hojas de cálculo, bases de datos, etc., de diferente fabricante, pero que desgraciadamente los datos e información generados con estas herramientas no pueden ser transportables entre sí, y no solo eso sino que al tener la necesidad de intercambiar información se vuelve ridículo el tener que enviarla en listados, y por otro lado si se desea imprimir la información requerida era necesario trasladarse o hacer una gran cola de espera para hacer uso de una impresora, pero en el peor de los casos sería necesario cargar la impresora hasta el lugar en donde se tenga un PC con el software requerido y hacer una nueva espera para ocupar esa PC. Este ejemplo parece sin lugar a dudas extremista y por supuesto no ocurrió en todos los corporativos, pero si se presentó, y en algunos casos aun hoy en día es verídico, sobre todo en países y corporaciones tecnológicamente atrasados.

Un punto muy importante es que el "boom" de las PC se debe a que es más fácil trabajar en ambiente PC que en un ambiente Unix o IBM, lo que origina que la gente se incline por la utilización de estos equipos.

Por tales motivos se vislumbra la necesidad de interconectar microcomputadoras para compartir recursos tanto de software como de hardware, dando origen a las redes locales.

2.3 Ventajas de las redes locales en los corporativos.

Al nacer las redes locales sé tenia como principales objetivos el compartir hardware y software, mismos que definitivamente se consiguieron, sin embargo, al lograr estos objetivos, se alcanzan otros beneficios que traen las redes locales a las corporaciones, mismos que se derivan de la estandarización tanto de software como de hardware. A continuación se presentan las ventajas de este rubro:
Beneficios de la estandarización de software y hardware.

Información al alcance de todos.

La información que posea el corporativo o institución podrá ser consultada o utilizada fácilmente por cualquier persona, sin tener que realizar mayor esfuerzo, permitiendo con esto que la información fluya fácilmente, pero a la vez en forma segura y controlada.

Abatir inversión de hardware y software.

Dado que tanto el software como el hardware que se adquiera será compartido por diversos usuarios, y teniendo estos recursos se incrementa la productividad, el precio del producto con relación a la utilización que se le dé será realmente favorable para las corporaciones.

Automatizar procesos.

El tener un ambiente de cómputo homogéneo permite que los procesos cotidianos y muchas veces engorrosos puedan ser automatizados y ejecutados por microcomputadoras, permitiendo que los usuarios tengan más tiempo libre para realizar sus funciones y no perderse en los pequeños detalles que tanto tiempo quitan, y no solo tiempo, sino

que en casos especiales algún evento puede ser disparador de un proceso, lo que permite llegar a tener procesos automáticos.

Mayor poder de negociación con fabricantes de software y hardware.

Al realizar compras millonarias de software o hardware con un mismo fabricante, los precios de los productos bajan drásticamente. Y no solamente se habla de negociación en el rubro de dinero, sino también el poder tener productos *Beta* para su conocimiento y evaluación, línea directa de soporte con el fabricante, primicia en la obtención de productos liberados, atención y soporte directos del fabricante o mediante proveedores autorizados, etc. Para el caso de software es más sencillo obtener la actualización de productos cuando se habla de toda una empresa, que si hablamos de varios productos similares de diferentes marcas; además el tener un solo producto de la misma especie en el servidor de archivos permitirá mejorar el aprovechamiento de espacio en disco y administrar más fácilmente los recursos disponibles.

Sobre lo que a hardware se refiere, algunos de los fabricantes más importantes (Hewlett Packard, IBM, Digital, Compaq) han estado empezando a introducir a sus divisiones financieras en el mercado mexicano, entre otras razones por el estado de la economía nacional, pudiendo ofrecer servicios de financiamiento para la adquisición de equipo de cómputo o renta del mismo.

Aunque esto parecería que no es novedoso dado que tanto el financiamiento como la renta de equipo se puede llevar a cabo con instituciones financieras, como arrendadoras o bancos, la ventaja que se ofrece es que las tasas de interés son más atractivas, siendo tan buenas las condiciones que incluso algunos bancos están tomando estas

opciones. Entre algunas de las razones por las que realizar un contrato de este tipo con una arrendadora es más caro que con un fabricante, es que las arrendadoras al final de los periodos de contrato, se quedan con los activos y tienen un segundo problema, que dichas instituciones no se dedican a comercializar equipo de cómputo, situación que no ocurre en el caso de cuando los fabricantes de cómputo ofrecen sus servicios de arrendamiento de equipo, pudiendo colocar este equipo en mercados secundarios.

Por otro lado y sin abundar mucho sobre el tema, también resulta que al ofrecer opciones de financiamiento o renta de equipo se ofrece la posibilidad de afectar en forma diferente los estados financieros de los clientes, en un caso (financiamiento) se hacen de activos, y en el otro (renta) se contabiliza como un gasto, situaciones que fiscalmente pueden covenirle a las empresas.

Reducir gastos en capacitación y soporte técnico.

Esta reducción se debe a que al tener que capacitar sobre un solo producto, las capacitaciones son más sencillas, baratas, homogéneas y con el enfoque que desea la empresa. También el proporcionar soporte técnico sobre una gama reducida (en variedad) de software y hardware permite a los corporativos desarrollar verdaderos expertos en cada campo o área de acción que desee.

Por otro lado, al contar con herramientas de productividad de un mismo fabricante, provoca que los usuarios tengan un mayor conocimiento sobre las dichas herramientas, ya que los productos de un mismo fabricante se manejan de una forma muy similar, y esto también propicia la

desaparición de las pequeñas elites de, principalmente, el área de sistemas.

Crear sistemas de cómputo fáciles de reproducir.

Al diseñar un nuevo sistema de cómputo, este será fácilmente reproducible, debido a que los ambientes de operación son similares y compatibles. Lo que provoca que el índice de fallas en los nuevos sistemas sea menor.

Control de software existente.

Esto permitirá reducir drásticamente los actos de piratería, dado que al tener que realizar los trabajos con una misma herramienta, no es necesario contar con productos diversos de un mismo tipo, además de que existe un administrador de LAN, mismo que es responsable, entre otras cosas, de evitar la piratería de software.

Crear una mejor imagen corporativa.

Hoy en día la imagen que proporciona un corporativo es muy importante; sobre todo si hablamos de que la imagen es uno de los puntos con que, un corporativo, impulsa y vende sus productos o servicios. El decir que tal o cual corporativo posee tecnología IBM, o cualquier otra de reconocido prestigio, le permite ser identificado por el alto grado de tecnología que posee, y no solo eso, sino que dicha tecnología la pone al servicio de sus clientes.

2.4 Mitos de las redes locales.

Las redes locales, por su gran popularidad, y en muchos casos, la falta de información adecuada, han creado en torno a ellas una gran cantidad de conceptos erróneos, o parcialmente verdaderos. Esto provocado por el hecho de que existe una gran cantidad de personas de sistemas que se han desarrollado en el ambiente de mainframes, y consideran que una PC es fácilmente configurable en una red local, ya que consideran que las redes locales solo son PCs. Sin embargo para que una red local funcione adecuadamente es necesario más cosas que simplemente saber de PCs. A continuación se mostrarán las consideraciones erróneas más comúnmente atribuidas a las redes locales.

- Las redes locales solo servirán para tener un disco duro más en donde tener mucha información o una gran cantidad de espacio.

  Esto no es cierto, ya que con las redes locales se puede compartir tanto recursos de software como de hardware, e incluso servicios. Esta misma compartición de recursos provoca reducción de gastos.

- Al tener una red local solo es necesario adquirir un software y/o una licencia para poder hacer uso del mismo.

  Debido a que los recursos de software son compartidos, se piensa que solo se compra una licencia y hacen uso dos o más personas simultáneamente del mismo software, sin embargo es necesario adquirir las licencias por cada máquina en que se instale un mismo software. En algunos casos, en donde un mismo equipo es utilizado por dos o más

usuarios, por ejemplo Lotus Notes, se requiere una licencia por cada usuario. Anteriormente esto se hacia de una manera distinta, puesto que solo se tenía que adquirir licencias de software por uso concurrente del mismo, lo que se ejemplificaba con el hecho de contar con una licencia de conducir sin importar en qué automóvil que se manejara; de cualquier forma solo se podía manejar uno a la vez; ahora el concepto ha cambiado y se requiere contar con una licencia por usuario y por equipo; es decir, si un usuario utiliza una computadora en su casa y otra en la oficina, requiere doble licencia; por lo que ahora esta nueva forma de licenciamiento equivale a que todos los vehículos deben contar con tarjeta de circulación, sin importa si este circula o no.

- Cualquier PC puede formar parte de la red local.

  Teóricamente esto es bien posible; sin embargo, para que una PC forme parte de una red local es necesario que cuente con ciertas características mínimas de operación, como son: memoria, sistema operativo, espacio en slots disponibles, interrupciones y segmentos de memoria disponibles, arquitectura interna de la PC, tipo de microprocesador y en casos muy contados que prácticamente ya no se dan, el tipo de monitor que utiliza. Por lo que no cualquier PC puede formar parte de una red local.

  Esto cada vez aplica menos; sin embargo existe una buena cantidad de equipos que no pueden incorporarse a red aún "cumpliendo" con las especificaciones; por ejemplo, un equipo puede contar con la memoria RAM requerida, sin embargo el manejo de misma puede provocar que no

exista memoria contigua suficiente para abrir una aplicación o para cargar un drive.

- Dado que se trata solamente de PCs, cualquier persona puede hacerse cargo de una red local.

  Posiblemente este sea uno de los errores más comunes con los que se encuentra uno, ya que debido a que las PCs son equipos muy populares, y relativamente fáciles de utilizar, se cree que una red local es fácilmente administrable y controlable; sin embargo existe una gran variedad de problemas técnicos a los que se enfrenta un responsable de estas plataformas, siendo necesario contar con los servicios de una persona de buen nivel que permita, al menos, poder seguir instrucciones telefónicamente de personal capacitado, ya sea proveedor, fabricante o consultor, y por supuesto aplicar las instrucciones o conceptos generales, sin tener que llegar al grado de explicar el detalle, o explicar el detalle del las causas del problema sin tener que exponer paso a paso las acciones a tomar.

  Lo anterior aunque parece fácil, no lo es; se requiere tener un grado de conocimiento de redes locales, sistemas operativos tanto de red local como propios del equipo, protocolos, estándares, comunicaciones, cableados, arquitectura de equipos, software, reglas de diseño, etc.

2.5 Componentes de las redes locales.

Para que una red local pueda ser implementada es necesario contar con diversos componentes, todos importantes, sin alguno de estos componentes, no

es posible implementar una red local, con la excepción del cable y los conectores, caso especial que comentaremos más adelante.

Existen tres grupos de componentes en las redes locales, estos son: físicos, lógicos y estratégicos, mismos que se desglosan a continuación:

Componentes físicos.

- Cables y conectores.
- Tarjetas de red.
- Repetidores.
- Estaciones de trabajo.
- Servidores.
- Periféricos.

Componentes lógicos.

- Sistema operativo de red.
- Software.
- Configuración.
- Soporte técnico.

Componentes estratégicos.

- Diseño.
- Capacitación.
- Plan de contingencia.
- Respaldo de información.
- Administración de red.

- Herramientas de soporte y administración.
- Conectividad.

Componentes físicos.

A continuación se describen los componentes físicos de las redes locales:

- Cables y conectores.

El cable se utiliza para enlazar los diferentes equipos en una LAN, aunque en la actualidad ya se producen tarjetas de red inalámbricas. El cable sigue considerándose como la mejor opción en la mayoría de los casos; sin embargo es conveniente tener presente que el cable no es el único medio para realizar estos enlaces. El tipo de cable que se emplee depende tanto de la topología como de la arquitectura que se utilice, y los conectores dependen directamente del tipo de cable. A continuación se listan los tipos de cable utilizados en las redes locales.

Tipos de cable utilizados en las redes locales.

- ✓ *Cable coaxial.* Este tipo de cable se recomienda para ser implementado como enlace de redes locales en un mismo edificio o entre edificios, es decir, para formar un back bone. Al utilizar este tipo de cable como back bone no se puede tener cableados estructurados.
- ✓ *Cable UTP (Unshielded Twisted Pair).* El cable UTP es el que se conoce como tipo telefónico, sin embargo posee características muy particulares, por ejemplo el número de trenzados que debe de tener por metro, el calibre, código de colores, la frecuencia soportada, etc. Este tipo de cable es recomendado para enlazar equipos a una red local en un mismo piso o local. El cable UTP se mide por su calidad, misma que

se identifica por un concepto denominado Nivel o Categoría, donde el Nivel mínimo a utilizar en una red local es el Nivel 3. Conforme mayor sea el número mejor calidad tiene el cable. En caso de requerir mayores velocidades, por ejemplo las que utiliza Fast Ethernet o 100VG, se requiere un cable nivel 5.

- ✓ *Cable STP (Shielded Twisted Pair).* Este tipo de cable es utilizado básicamente por IBM en token ring, sin embargo puede ser utilizado, en algunos casos para soportar mayor distancia. Normalmente se utiliza en interiores.
- ✓ *Fibra óptica.* Este tipo de medio es utilizado principalmente en tres situaciones: alcanzar grandes distancias, para evitar interferencias electromagnéticas, o para alcanzar altas velocidades en la transmisión de datos.

- Tarjetas de red local.

Las tarjetas de red local (NIC Network Interface Card), son un puerto de comunicación, que se inserta dentro de la PC, utilizado para poder enlazarse a la red local. Existen básicamente cinco tipos de tarjetas con cinco variantes, ARCNet, Ethernet, Fast Ethernet, 100VG AnyLAN y Token Ring en buses Microcanal , ISA, EISA, PCI y PCMCIA. Las tarjetas de LAN más utilizadas son Ethernet y Token Ring.

- Repetidores de señal.

Los repetidores de señal son básicamente cajas negras que se encargan de regenerar la señal, amplificarla y retransmitirla por todos sus puertos, con la finalidad de que dos o más equipos puedan formar parte de una red local.

Tanto los repetidores como las tarjetas de red, deben ser de la misma arquitectura; es decir, si se requiere arquitectura Ethernet, ambos componentes deberán ser de dicha arquitectura.

- Estaciones de trabajo.

Este término es utilizado para definir la PC conectada a una red local, mediante la cual los usuarios pueden hacer uso de los beneficios de esta plataforma; algunos autores también les llaman nodos o terminales inteligentes; sin embargo un nodo también puede ser un servidor, por lo que aquí se llamará estación de trabajo. Existen diversos tipos de estaciones de trabajo conectadas a redes locales, estas pueden ser desde LapTops, enlazadas mediante lo que se pudiera llamar "tarjetas de red externas", computadoras Macintosh y PC con diferente configuración, pudiendo estar todos estos equipos compartiendo información de un mismo servidor.

- Servidores.

Existen diversos tipos de servidores dependiendo su aplicación. Los servidores son equipos dedicados a cumplir una función en específico, y que además se encargan de controlar, administrar y compartir los recursos inherentes a ellos. A continuación se presentan los servidores más comunes:

Servidor de archivos.

Este es el tipo de servidor es el más conocido; en él se basa el funcionamiento de una LAN. Pueden existir redes locales sin otro tipo de servidores, pero no sin servidores de archivos. Estos servidores contienen lo siguiente:

- Sistema operativo de LAN.
- Software y/o paquetería comercial.
- Archivos de la organización y de usuarios.

Servidor de impresión.

Este servidor como su nombre lo indica, controla las colas de impresión. Los servidores de Impresoras están poco a poco desapareciendo, sobre todo con la aparición en el mercado de componentes que permiten conectar las impresoras a la LAN como si fueran nodos; es decir se compra una tarjeta de red para impresora. Esto permite colocar las impresoras donde uno desee, sin tener que dedicar un PC, o compartir la PC con la función de estación de trabajo y servidor de Impresora, ambas opciones poco prácticas, ya que en el primer caso se desperdicia un equipo, y en el segundo los equipos, al estar imprimiendo, se "alentan", lo que le impide al usuario trabajar normalmente.

Servidor de base de datos.

Su máxima virtud es el manejo de bases de datos, optimizando el proceso de búsqueda y envío del dato solicitado por cualquier estación de trabajo o proceso que hubiera realizado el llamado (query).

Servidor de comunicaciones.

Estos serán los servidores más populares dentro de poco tiempo, ya que la comunicación es el punto más importante en cualquier empresa, no importando el tamaño de la misma. De estos equipos existen diferentes "versiones", definiremos cada uno de ellos:

- ✓ *Servidor de correo electrónico.* Este equipo se dedica a transmitir y recibir la correspondencia electrónica entre usuarios de distintas localidades. En la mayoría de los casos este equipo posee una configuración básica, es decir, una microcomputadora XT o una AT puede realizar esta función, todo dependiendo del software que realice este trabajo.
- ✓ *Servidor de fax.* Este equipo se dedica a transmitir y recibir la faxes, no importando si el fax proviene de un equipo similar o de un fax tradicional. El servidor de fax no es un substituto del fax tradicional, sino un complemento, ya que si se desea mandar el fax de un folleto o cualquier documento, este tendrá que estar capturado como un archivo para poder ser enviado. En algunos casos es posible tener en un mismo equipo los servicios de fax y correo electrónico, todo dependerá de los productos.
- ✓ *Servidor de bridge.* Algunos fabricantes de software han implementado la función de bridge en una microcomputadora. Sin embargo dado que el diseño de una microcomputadora es de propósito general, el grado de desempeño que tienen estos equipos contra un bridge implementado en una caja negra es mucho menor. En el capítulo 6 se explica la función de un bridge.
- ✓ *Servidor de router.* Es el mismo caso que el anterior solo que con funciones de ruteo. En el capítulo 6 se explica la función de un router.
- ✓ *Servidor de gateway.* Este es una de las implementaciones más complicadas que existe; todo depende del software que realice la tarea de gateway. Se considera que en un futuro los servidores de gateway tenderán a desaparecer, debido principalmente a que todos los fabricantes están impulsando lo que se llama sistemas abiertos, lo que

permitirá en un futuro interoperar diferentes ambientes sin necesidad de un gateway como tal. En el capítulo 6 se explica la función de un gateway.

- Periféricos.

El periférico más común es la impresora, pero no es único, existen otros como son: modems, graficadores, sistemas de respaldo, discos ópticos, etc.; todos ellos deben de traer drives adecuados para el sistema operativo de red que se utilice.

Componentes Lógicos.

A continuación se presentan los componentes lógicos de las redes locales:

- Sistema operativo de red local.

El sistema operativo de red local, Network Operating System (NOS), es el software que permite administrar, controlar y compartir los recursos existentes en una red local. Se considera el alma de una red local. Del NOS dependen las facilidades de comunicación que se tengan, los protocolos a utilizar, la transparencia de operabilidad con otros ambientes, la seguridad en la LAN, etc.

- Software, comercial o desarrollado en casa.

Los desarrollos de software o paquetería comercial son las herramientas de productividad con las que labora diariamente un usuario, entre algunos paquetes, como concepto, se mencionan los más comunes: hoja de cálculo, procesador de texto, diseño gráfico, bases de datos, software de comunicaciones, ambiente gráfico, utilerías, detectores y erradicadores de virus, etc. Sobre el

software hecho en casa, también conocido como desarrollo propietario, los más comunes son: nómina, contabilidad, almacén, etc.

Es importante que estos paquetes sean versión LAN, ya que no todos tienen esta cualidad y por lo tanto no funcionan en esta plataforma, o si lo hacen no son capaces de ser compartidos.

Así mismo existe software que únicamente funciona bajo un sistema operativo de red en específico, por lo que en caso de migración o actualización del sistema operativo, existen una gran posibilidad de que dicho software no funcione.

- Configuración.

Es muy importante contar con una plataforma de red que posea una configuración adecuada a las necesidades de dicha institución, y sobre todo que siga los estándares y diseños implementados previamente, y por supuesto que todo se encuentre documentado, ya que al momento de sufrir algún problema o realizar un cambio, lo primero que se necesita conocer es la configuración que guarda el sistema.

- Soporte técnico.

Todos los sistemas por buenos y completos que estos sean requieren en algún momento dado de soporte técnico, ya sea que este sea proporcionado por la misma institución o que se proporcione por un tercero. Lo que en verdad se estaría creando es un seguro, que por lo pronto se considera un gasto, pero en el momento que se utiliza es una inversión. Un jugador importante en el soporte técnico es el administrador de la red.

El administrador de la red local es la persona encargada de administrar y coordinar todo lo relacionado con la LAN; sus funciones van desde dar de alta usuarios, asignar seguridad tanto de archivos, directorios, colas de impresión como de usuarios, instalación de paquetería, compartición de recursos, ingreso de nuevos equipos a LAN, configuraciones y reconfiguraciones del NOS, servidores y estaciones de trabajo, apoyo a usuarios, mantenimientos preventivos y correctivos, hasta coordinar el cableado de nuevas estaciones de trabajo. Debe tener buenos conocimientos del NOS y de la paquetería utilizada, configuración de impresoras, etc.

Como se puede apreciar la responsabilidad de un administrador de LAN es muy fuerte, ya que prácticamente es quien proporciona los "primeros auxilios" a una LAN en el caso de que se presente cualquier situación inesperada.

Componentes estratégicos.

Estos componentes llevan a cabo la definición macro de lo que será la plataforma de la red local, así como sus alcances. A continuación se describen los componentes estratégicos de las redes locales:

- Diseño.

El diseño es probablemente uno de los puntos que mayor diversidad puede tener, ya que abarca desde las cuestiones técnicas hasta administrativas. Por la parte técnica existen diseños de cableado, disposición de equipos, segmentación de tráfico, grupos de usuarios, protocolos, etc.
Hablando del segmento administrativo, se tiene: procedimientos, compromisos, políticas, alcances, etc.

Sin un diseño adecuado, la mejor tecnología tiene altas probabilidades de ser mal aplicada, iniciando desde una compra errónea.

- Capacitación.

Muchas personas, principalmente con formación técnica desdeñan este punto, ya que piensan que la práctica es la forma en que las personas aprenden más; sin embargo debemos pensar que el grueso de las personas que utilizan estos equipos tienen una formación administrativa.

A fin de cuentas, la forma en que se mide si una inversión ha sido rentable o no, es mediante la adecuada utilización de las herramientas, mismas que si no son conocidas por los usuarios no tendrán ningún éxito.

- Plan de Contingencia.

Si la operación de una plataforma de red local es una herramienta de trabajo, debemos hacernos la pregunta ¿Qué implicaría si ésta dejara de funcionar? Normalmente, esta pregunta pocas veces la hacemos, pero es sumamente importante tenerla en cuenta, ya que si no existe una alternativa de operación, estaremos expuestos a perder dinero.

Existen sistemas sencillos que permiten continuar la operación por algunos minutos, en el caso de interrupciones de corriente eléctrica; sin embargo existen otros mas complicados que permiten continuar la operación en otras ciudades o países. Todo dependerá de las necesidades de cada corporativo.

A continuación se muestra una pequeña investigación económica de un sistema de respaldo de operación en caso de que el servidor de archivos Netware versión 4.1 deje de funcionar.

CONCEPTO	MONTOS	COMENTARIOS
Número de Usuarios	100	Que utilizan la red.
Sueldo promedio mensual	N$6,500.00	Por usuario.
Costo compañía	2.5 veces el sueldo	SAR, prestaciones, renta, luz, vigilancia, intereses, etc.
Sueldo promedio diario	N$81,250.00	De las 100 personas
Sueldo promedio hora	N$10,156.25	De las 100 personas
Costo cableado anual	N$70,000.00	De 100 nodos. Considerando una PC por usuario.
Costo cableado hora	N$36.46	De 100 nodos
Costo hardware anual	N$466,666.67	De 100 estaciones de trabajo
Costo hardware hora	N$243.06	De 100 estaciones de trabajo
Costo software anual	N$233,333.33	Paquetería comercial
Costo software hora	N$121.53	Paquetería comercial
Costo por Hora sin Servicio	N$10,557.29	Sueldo, cableado, HW y SW
Costo por Día sin Servicio	**N$84,458.33**	Considerando 8 horas

Se consideró depreciación de 3 años.

SISTEMA EN ESPEJO	PRECIO	COMENTARIOS
Un Servidor	N$75,000.00	HP, pentium a 100 MHz, 1 GB en DD, 16 MB RAM
Un Netware SFT III	N$29,962.00	Software para llevar a cabo el espejo
Dos Tarjetas SFT III	N$13,485.00	Enlace entre el servidor primario y el secundario
Instalación y Configuración	N$7,000.00	Servicio técnico.
Total sin descuento	N$125,447.00	Precios de lista
Total con descuento	**N$100,357.60**	Descuento de 20% aplicado por proveedores.

Como se puede apreciar, es más caro el sistema en espejo del servidor Netware 4.1, siempre y cuando solo se tenga el sistema fuera de operación un día; sin embargo ¿qué pasa con los costos ocultos?, mismos que incluso pueden ser más importantes que los considerados en el ejercicio anterior; entre estos costos ocultos se pueden encontrar: costo de oportunidad, pérdida de información, tiempo de recuperación del sistema, etc. Se calcula que las pérdidas por tener una red local fuera de operación pueden incrementarse entre 5 y 50 veces si se tomaran en cuenta esos y otros factores. Uno de los casos más críticos lo representaría una sucursal bancaria o una casa de bolsa, donde el costo fácilmente podría alcanzar 30 o 40 veces el costo calculado anteriormente.

Viéndolo desde esta óptica un sistema de estos podría fácilmente pagarse con una "caída de red" de una hora.

De esta forma podemos ver que un buen sistema de contingencia puede ahorrar una gran cantidad de dinero.

- Respaldo de Información.

Los respaldos de información deberían incluirse en los planes de contingencia, y de hecho es un subinciso de este rubro; sin embargo es tan importante, que se incluye como punto adicional.

Existen diversos sistemas de respaldo de información, así como marcas y soluciones a este punto, pudiendo abarcar situaciones donde la red local no cuenta con comunicación a otras redes, y no permite respaldos remotos, o sistemas que permiten realizar respaldos automáticos fuera de horarios de trabajo. Así mismo existen sistemas que permiten ser monitoreados en forma remota y avisar a algún sistema en caso de falla en el respaldo.

- Administración de red.

La administración de la red incluye una gran cantidad de rubros entre ellos la administración remota, help desk, simulación de tráfico, etc. De tal forma que se convierte en una herramienta indispensable para los corporativos que cuentan con redes locales; inclusive las empresas más pequeñas cuentan con una persona que se designa administrador de la red local.

Algo muy importante que se debe definir en la administración de la red es el alcance que se desea implementar, ya que de esto dependerán las herramientas necesarias para llevarse a cabo.

En la administración se definen los procesos de diagnóstico, solución de fallas, el perfil del personal de soporte, horas y días de atención, metodología de soporte, etc.

- Herramientas de Soporte y Administración.

De la definición que se haga de la administración de redes se determinará las herramientas e infraestructura necesaria para poder llevar a cabo las tareas y funciones definidas en dicho rubro.

Las herramientas pueden ir desde las básicas que comprenden la utilización de la red, mismas que se encuentran incluidas en la mayoría de los sistemas operativos de red, hasta las más complicadas que permiten llevar a cabo sistemas de simulación en comunicaciones, pasando por los antivirus.

Respecto a las herramientas de soporte, un equipo de ingenieros sin las herramientas adecuadas es el equivalente a tener a un mecánico sin herramientas. Dependiendo del fabricante, modelo y características de la red, es el tipo y cantidad de herramienta que se deben tener.

- Conectividad.

Siendo la conectividad un punto tan importante, es indispensable definir los requerimientos actuales y futuros que permitan implementar una plataforma lo suficientemente flexible para ir adicionando los diversos servicios que se requieran, como el caso de multiplexores, anchos de banda, entidades a enlazar, etc. Incluso en este punto es donde se determinan los ambientes a enlazar.

CAPÍTULO 3
Pasos a Seguir Para Implantar una Red Local

Temas del capítulo.

3.1 Información requerida para diseñar una red local.

Para implantar una LAN es necesario seguir una secuencia de pasos que permitan llevar a buen fin un proyecto de esta naturaleza, por lo que a continuación se indicarán en detalle los pasos a seguir en un proceso de este tipo.

3.1 Información requerida para diseñar una red local.

Para poder diseñar adecuadamente una LAN es necesario contar con cierta información, misma que permitirá realizar una buena propuesta técnica que permita cubrir los puntos requeridos. Por supuesto, todos los proyectos son diferentes, sin embargo se intentará cubrir los puntos generales; por lo tanto, lo que aquí se presenta es la información mínima requerida para llevar a cabo la implantación de una LAN.

La información que debe ser obtenida es la siguiente:

1. Objetivos a cubrir por el proyecto.
2. Puntos que deben ser cubiertos por la propuesta esperada. Es decir, puntos que por fuerza se deben cubrir.

3. Puntos deseados a ser cubiertos por la propuesta esperada. Es decir, puntos que de ser posible se puedan cubrir.
4. Misión y objetivo de la entidad. Esto con la finalidad de poder en un momento dado proporcionar una mejor opción o algún valor agregado a la plataforma de LAN, independientemente de involucrarse más a fondo con la entidad.
5. Organigrama. Indicar perspectivas de crecimiento en personal. El objetivo de solicitar esta información es poder crear grupos de trabajo mediante el sistema operativo de la red local así como saber quien debe disponer de la información y en casos extremos quienes son los indicados para acceder tal o cual información.
6. Indicar responsable del proyecto, puesto, funciones que desempeña, forma de localizarlo y de ser posible, experiencia en este tipo de proyectos. Es importante saber a quien nos podemos dirigir para aclarar puntos o hacer consultas.
7. Localización geográfica de la entidad y perspectivas de cambio, conectividad a otra LAN y crecimiento.
8. Mapa a detalle del local, indicando ubicación de equipos existentes y futuros (PC, impresoras, modems, etc.). Es conveniente que se incluyan los lugares de juntas, demostraciones y/o exposiciones que existan en la empresa, ya que son lugares donde en un futuro pueden requerirse conexiones virtuales. Se deberá indicar la ubicación del Servidor y características del lugar, como seguridad de acceso, temperatura, etc.
9. Diagrama de flujo a detalle de los procesos de información que se llevan a cabo. Se deberá indicar: entradas de información (área o departamento de procedencia), procesos (quien y como se realiza) y salidas de información (área o departamento destino). Esto permitirá en un momento dado automatizar algún proceso y proporcionar algún valor agregado al proyecto.

10. Identificación de funciones y procesos clave así como de cargas de trabajo (relacionado al punto anterior).
11. Tiempos de cada uno de los procesos desarrollados (relacionado al punto anterior). Permitirá en un futuro hacer una evaluación del proyecto.
12. Software y aplicaciones que se emplean en el desempeño de procesos, funciones y proyectos (en caso de aplicaciones desarrolladas en casa indicar el lenguaje de programación). Indicar nombre, versión, número de serie, en qué procesos, funciones o proyectos es usado, así como la frecuencia y dependencia que se tiene del mismo. También se deberá indicar si se requerirá en un futuro de algún software o aplicación adicional. Esto permitirá conocer las adecuaciones que se deben hacer a los sistemas, o en su caso hacer nuevos sistemas. Esta información permitirá hacer una buena estructura de directorios en el servidor de archivos. En estos casos es muy importante conocer si el software a utilizar opera exclusivamente bajo algún ambiente y/o condición especial.
13. Equipos con que se cuenta y características, indicando equipo actual y futuro.
    - PC. marca, modelo, microprocesador, velocidad, memoria RAM, tipo de monitor, unidades de almacenamiento, tarjeta(s) interna(s) adicional (es) indicando configuración, arquitectura interna, etc.
    - Impresora. Marca, modelo, tipo de impresión, memoria, conexión serie, paralelo o ambas, uso que se le da (textos, gráficas, etc.), etc.
    - Plotter. Marca, modelo, tipo de impresión, memoria, conexión serie, paralelo o ambas, etc.

- Modem. Marca, modelo, velocidades soportadas, indicar si son internos (tarjeta) o externos, en caso de ser internos indicar configuración interna, compatibilidad con Hayes, tipo de recomendación CCITT, y configuración que posee actualmente, etc.

Para todos los casos es conveniente conocer el uso que se le da a cada equipo, configuración actual, persona o personas que lo utilizan y de ser posible, tiempo de utilización.

14. Como se indicaba en el capítulo anterior, punto 2.4, es necesario contar con licencias de uso simultáneo de software; por lo que es conveniente saber si existe algún contrato corporativo de licencias con algún fabricante de software, ya que esto permitirá tener la actualización de software, de versión stand alone a versión red, a precios muy razonables.
15. Necesidades de conectividad a otros ambientes o con otras entidades indicando ubicación física, ambiente a interconectar y configuración del mismo. Para este caso se requiere conocer la infraestructura de comunicaciones con que se cuenta, indicando marca, modelo, versiones tanto de software como de hardware, ancho de banda disponible, si el canal es o no full duplex, etc.
16. Es necesario tener información sobre si se tiene regulación de corriente, fuentes ininterrumpidas de corriente, capacidad total, capacidad utilizada actual y capacidad libre que ofrecerá al momento de implantar la LAN. No solo es importante conocer si se tiene o no, sino que los equipos principales de la LAN deberían contarán con estos servicios.
17. Con la facilidad de poder realizar un cableado óptimo y de saber con qué infraestructura se cuenta, se deberá obtener información sobre ductos disponibles en el local o edificio. Se recomienda investigar sobre cercanía a

dichos conductos de: cables de corriente eléctrica, fuentes electromagnéticas, como generadores, motores, elevadores, etc. De ser posible obtener un mapa del tendido eléctrico.

18. Es conveniente saber qué tipo de muros, pisos y techos se tienen. En este punto es importante saber si es posible hacer algún tipo de adecuación al inmueble. Normalmente en todos los edificios ya se tiene algún tipo de cableado, telefónico o de otro tipo, por lo que es adecuado conocer por donde pasa y de ser posible como fue hecho y los problemas que se presentaron al realizar dichos cableados.

Estos son solo algunos de los puntos que se requiere conocer para poder implantar una LAN; por supuesto, es necesario tener en cuenta la infraestructura que ya se posee, la tendencia del mercado tecnológico, las preferencias del usuario, la capacitación con que cuenta, etc. Todo esto con la finalidad de poder realizar una propuesta que permita interoperar la base instalada de recursos con la propuesta misma. En algunos casos es conveniente sostener pláticas con las personas que de una u otra forma están involucradas en el proyecto, dado que muchas veces son estas personas quienes tienen más claros los requerimientos, problemática y hasta la solución. Como en todos los proyectos, mientras más información se tenga será mejor, ya que esto permitirá en un momento dado tener un punto de decisión.

Existen puntos adicionales que se deberán conocer al momento de seleccionar algún software o sistema operativo en especial; por ejemplo, en el caso de Netware 4.1 permite incluir datos del personal como dirección, teléfono, etc.; mismos que si bien no son indispensables, sí permiten llevar a cabo un proyecto con mas alcances, por ejemplo, apoyo a recursos humanos.

Por otro lado al trabajar en un proyecto como este, es recomendable que quede perfectamente delimitada la función y responsabilidades de cada una de las personas o entidades que intervienen en el proyecto; esto sin lugar a dudas deberá realizarse por escrito y con copia a los niveles superiores de los involucrados.

Al momento de implementar una red local se debe tener en cuenta que esta es un medio tecnológico para lograr un fin. El tener la red por si misma proporciona ventajas, pero puede ser que estas no sean aprovechadas por la entidad que la posea. Es muy importante entender que el cliente quiere servicios, no servidores, hubs, cableados, etc.

También es importante delimitar los alcances que se le pueden dar al proyecto, ya que es frecuente que quien desea implementar una red local esté influenciado, y aunque dicha entidad crea que necesita una red local, puede ser que esta no resuelva la problemática o que se adquiera una tecnología sumamente poderosa.

Es muy fácil llevar a cabo un proceso de reingeniería al implementar una red local, ya que muchos de los procesos se pueden automatizar, siendo muy conveniente automatizar un proceso eficaz, y no solo automatizar por automatizar.

Entre algunos de los procesos que en forma sencilla se pueden automatizar están los flujos de trabajo que utilizan mucho papel e interviene una gran cantidad de personas, ya que existen herramientas que permiten seguir una "línea de producción", permitiendo entre otras cosas:

- Evitar pérdida de tiempo en búsqueda de información (expedientes, firmas, etc.) para solucionar los problemas.
- Medición de tiempo de cada tarea en el proceso total.
- Detección de cuellos de botella.

- Seguridad de acceso a información.
- Reducción de espacio físico en cuanto a archiveros se refiere.
- Mejores tiempos de respuesta a clientes (internos o externos).

Haciendo uso de tecnologías de flujos de trabajo, se puede cambiar la filosofía de trabajo de la empresa, haciendo que los procesos y decisiones no dependan de la gente, sino de una metodología y de parámetros bien establecidos, eliminando la subjetividad que en un momento dado puede inducir una persona en la toma de decisiones.

CAPÍTULO 4
Arquitecturas de Red de Alta y Baja Velocidad

Temas del capítulo.

4.1 Diferencia entre arquitectura y topología.

4.2 Arquitecturas de baja velocidad. ARCNet, ethernet y token ring.

4.2.1 Criterios para elegir ARCNet. ¿Que hay de ARCNet Plus?

4.2.2 Criterios para elegir ethernet. ¿10BaseT, 10Base2, 10Base5, FOIRL?

4.2.3 Criterios para elegir token ring. ¿token ring a 4 o 16?

4.2.4 Tabla Comparativa de ARCNet, ethernet y token ring.

4.3 Arquitecturas de alta velocidad. 100VG, fast ethernet, FDDI y ATM.

4.3.1 Criterios para elegir 100VG.

4.3.2 Criterios para elegir fast ethernet.

4.3.3 Criterios para elegir FDDI. ¿FDDI o CDDI?

4.3.4 Criterios para elegir ATM. ¿25, 52, 155, 622 o 2,488 Mbps?

4.3.5 Tabla comparativa entre tecnologías de alta velocidad.

Cuando se va a implantar una LAN es necesario elegir entre diversas opciones del mercado. Se debe tener en cuenta que lo que finalmente se va a comprar es una tecnología, que por diversas causas tenderá a mejorar, y por el otro lado sabemos que no es posible adquirir algo muy grande, que no se use o que por el hecho de querer adquirir algo con mayor permanencia, la inversión también se diluya con el tiempo. También sabemos que podemos crecer en: volumen de información, número de usuarios simultáneos, aplicaciones, conectividad, servicios, etc.; por lo tanto es difícil elegir una opción tecnológica de

LAN que garantice permanencia, compatibilidad y apertura hacia nuevas tecnologías; sobre todo que es necesario elegir arquitectura, topología, velocidad, sistemas operativos, etc. Para ejemplificar un poco más esto, se puede afirmar que existen aproximadamente 60 versiones de ARCNet, 50 de Ethernet y 20 de Token Ring, adicionalmente existen aproximadamente 20 opciones de sistema operativo de red, por lo que la elección no es sencilla.

Para este capítulo abarcaremos el punto de elección de arquitectura de LAN.

4.1 Diferencia entre arquitectura y topología.

Antes de profundizar en el tema, es importante definir los términos arquitectura y topología, en cuanto a redes locales respecta.

Topología.

El término topología se refiere a la forma en que físicamente se interconectan los dispositivos en la red, considerando para esto la disposición de los elementos, determinándose por la forma del cableado. Existen diversas tipos, sin embargo las topologías principales en las redes locales son; estrella, bus y anillo. Existen otras topologías; sin embargo se consideran variantes de las mencionadas anteriormente.

En la figura 4.1 se presentan los tres tipos principales de topologías que rigen en las redes locales.

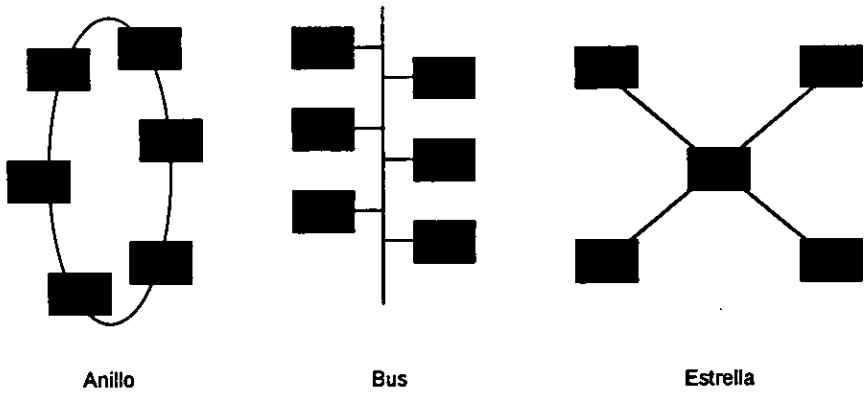


Fig. 4.1 Topologías principales en las redes locales

Arquitectura.

Se refiere a la tecnología que determina la velocidad, método de acceso y topología que tendrá la red local. Las principales arquitecturas presentes en las redes locales son: ethernet, ARCNet, token ring, 100VG, fast ethernet, FDDI y ATM. Las tres primeras son arquitecturas de baja velocidad y las cuatro restantes son consideradas de alta velocidad, aunque para el caso de ATM existe una variante a 25 Mbps, que de alguna manera se puede considerar de baja velocidad. En este tema se abundará mas adelante en este capítulo. El tipo de arquitectura indica el método de acceso al medio que se utilice.

4.2 Arquitecturas de baja velocidad. ARCNet, ethernet y token ring.

Existen diversos parámetros para elegir una LAN; entre los más importantes están: velocidad, método de acceso y distancia máxima de la red. Estas tres características se definen en la arquitectura de una red. En este

capítulo se analizarán estos tres puntos, partiendo de la velocidad de las arquitecturas.

Se consideran arquitecturas de baja velocidad aquellas tecnologías cuya velocidad no excede de 20 Mbps. Entre estas tecnologías se encuentran ARCNet, ethernet y token ring.

ARCNet, ethernet y token ring son las tres arquitecturas de LAN de baja velocidad más importantes que existen en el ámbito mundial.

De estas tres arquitecturas ARCNet y ethernet son los primeros modelos de LAN para microcomputadoras que se desarrollaron, apareciendo posteriormente token ring.

A continuación se presentan los aspectos más importantes de estas tres arquitecturas:

ARCNet.

ARCNet es un acrónimo de **A**ttached **R**esource **C**omputer **Net**work, desarrollado en 1977 por Datapoint Corp., con la finalidad de satisfacer sus necesidades internas de acceso a información de contabilidad en tiempo real.

La velocidad de ARCNet es de 2.5 Mbps, con un método de acceso al medio conocido como token passing, utilizando una modulación *baseband,* con una topología generalmente estrella, aunque también puede ser topología bus; sin embargo en forma lógica se considera que es topología anillo. Al conectar las PCs en una LAN ARCNet estas se numeran, manualmente, del 1 al 255, número que vendría haciendo las veces de dirección MAC, no debiendo existir números repetidos. ¿Cómo funciona esto? Al encender las PC en la LAN, la que posee el número más alto en ese momento genera un Token, mismo que será usado y posteriormente pasado a la PC o Servidor que posea el número más bajo; este

equipo utilizará el Token y lo cederá al equipo con el número que le siga en secuencia ascendente y así sucesivamente hasta llegar al último número y iniciar nuevamente, por lo que, como se puede apreciar, se tiene una lógica de anillo.

ARCNet es una arquitectura que tiene básicamente dos componentes, los repetidores activos y los repetidores pasivos; la diferencia entre ellos es la distancia que soportan: el primero soporta una distancia máxima de 1000 pies, y el segundo de 100 pies. Soporta cables de diversos tipos, inclusive en forma simultánea, como serían cable coaxial, UTP y fibra óptica.

La ventaja que posee ARCNet es su estabilidad, flexibilidad, alcance máximo y robustez a fallas. Su desventaja es que no pertenece a ningún estándar, es decir ARCNet como tal es un estándar de facto de la industria.

En la figura 4.2 se presenta un esquema de LAN bajo arquitectura ARCNet.

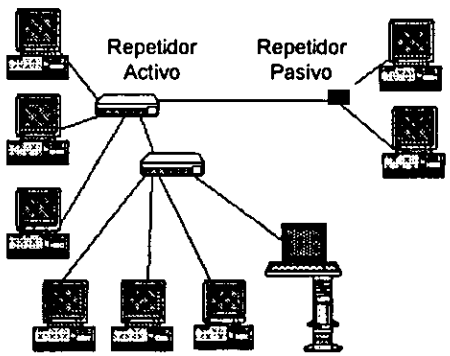


Fig. 4.2 Ejemplo de la topología ARCNet.

Ethernet.

Esta arquitectura de LAN es desarrollada por Xerox, Intel y DEC, con la finalidad de que DEC pudiera interconectar sus equipos de minicomputadoras, publicándose en 1980 las especificaciones para Ethernet, mismas que serían tomadas por el Comité IEEE 802 con algunos cambios, para generar la norma

IEEE 802.3. Ethernet es la arquitectura de LAN que posee mayor base instalada en el ámbito mundial.

Ethernet como tal, se ha caracterizado por operar bajo la topología de bus; sin embargo en la actualidad ya lo hace también en estrella y en forma combinada con bus, aunque lógicamente sigue funcionando como bus. Ethernet puede implementarse con diferentes tipos de cables como son: coaxial delgado, coaxial grueso, UTP y fibra óptica.

La velocidad de transmisión es de 10 Mbps con una modulación *baseband* utilizando un método de acceso CSMA/CD (Carrier Sence Multiple Access with Collision Detection), método de acceso que se describe a continuación: cuando una PC desea hacer una comunicación con otro equipo lo hacer y levanta una bandera indicando que el medio de comunicación se encuentra ocupado; con esto, si otro equipo desea utilizar el canal de comunicaciones, no podrá hasta que el equipo que lo esté usando lo deje de hacer y la bandera se encuentre abajo.

El método de acceso que maneja permite que el canal de comunicaciones se utilice aleatoriamente; es decir utiliza el medio de comunicación la estación de trabajo que desee hacerlo, siempre y cuando el canal no esté ocupado.

Aunque ethernet pertenece a un estándar (802.3 de la IEEE), existen cuatro tipos de ethernet; 10Base2, 10Base5, 10BaseT y FOIRL (Fiber Optic Inter Repeater Link), todos con las características anteriormente mencionadas, a excepción del cable y por supuesto la distancia que soportan.

El primer número significa la velocidad de operación en mega bits por segundo (10 Mbps), la palabra indica el tipo de modulación que está utilizando (base band) y el último número la distancia en cientos de metros que posee o el tipo de cable que utiliza, UTP para cable trenzado tipo telefónico.

- Ethernet 10Base2.

Este tipo de ethernet utiliza cable coaxial delgado de 50 ohms (RG-58), cuya distancia máxima es de 185 metros de un segmento. El número máximo de equipos conectados a un segmento es de 30. Por equipos se entienden PC, servidores, work stations, minicomputadoras, mainframes, repetidores de señal (hubs), transceivers, bridges, lanswitches y routers. La distancia mínima entre equipos es de 50 cm. No puede haber ramificaciones en el cable. La topología que utiliza este estándar es bus. Requiere de un terminador de 50 ohms en cada extremo del cable.

- Ethernet 10Base5.

Este tipo de ethernet utiliza cable coaxial grueso de 50 ohms (RG-8), cuya distancia máxima es de 500 metros de un segmento; se considera un segmento a la distancia de cable que existe entre dos terminadores. Requiere de un terminador de 50 ohms en cada extremo del cable. Un terminador debe ir aterrizado. El número máximo de MAUs conectados a un segmento es de 100. Un MAU es el dispositivo que permite conectar los equipos al cable (comúnmente se le denomina "vampiro", por la forma que posee y de conectarse); por equipos se entienden PC, servidores, workstations, minicomputadoras, mainframes, repetidores de señal (hubs), transceivers, bridges, lanswitches y routers. La distancia mínima entre MAUs es de 2.5 m. No puede haber ramificaciones en el cable. Esta arquitectura utiliza una topología de bus.

Como puede verse en la figura 4.3 la arquitectura 10Base2 y la 10Base5, tienen representaciones similares.

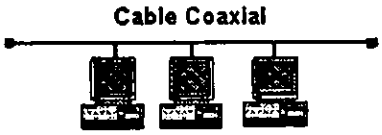


Fig. 4.3 Ejemplo de la topología de 10Base2 y 10Base5.

- Ethernet 10BaseT.

Aparece en el mercado en 1988-1989. Esta arquitectura utiliza cable tipo UTP (Unshielded Twisted Pair) de cuatro u ocho hilos con conector RJ-45 cuya distancia máxima es de 100 m. La idea de utilizar hilo tipo telefónico se debe a realizar cableados estructurados o inteligentes, concepto que se presenta en el capítulo siguiente. Es importante aclarar que el cable es tipo telefónico; sin embargo posee características específicas que impiden que cualquier tipo de cable telefónico pueda ser empleado; entre algunas de las características se encuentra el número de trenzados por metro (seis), el calibre del cable (22, 24 o 26 AWG), la atenuación, etc. Las características del cable se definen al indicar su nivel, que en este caso es nivel 3 o mayor. La topología de esta arquitectura es estrella. A diferencia de 10Base2 y 10Base5, requiere de un repetidor de señal. El número máximo de repetidores que puede cruzar una señal para llegar a su destino es de cuatro, por lo que la distancia máxima utilizando solo esta arquitectura es de 500m. Como se aprecia en la figura 4.4, el número máximo de nodos por segmento es de dos, donde en un extremo siempre se encuentra el repetidor (hub).

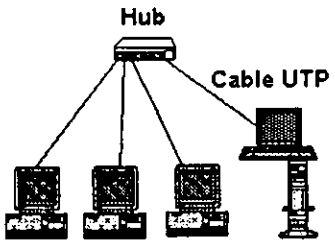


Fig. 4.4 Ejemplo de la topología de 10BaseT.

- Ethernet FOIRL.

Fiber Optic Inter Repeater Link (FOIRL) es una arquitectura que puede utilizar diversos tipos de fibra óptica (FO), unimodo y multimodo. La distancia máxima de un segmento de FO es de 1 Km; no puede haber más de seis segmentos de FO entre dos nodos, la suma de los segmentos de FO no debe exceder de 2 Km. Es compatible con 10BaseT, 10Base2 y 10Base5. La topología de esta arquitectura es estrella, al igual que 10BaseT.

En la figura 4.5 se presenta un esquema combinando las opciones de Ethernet.

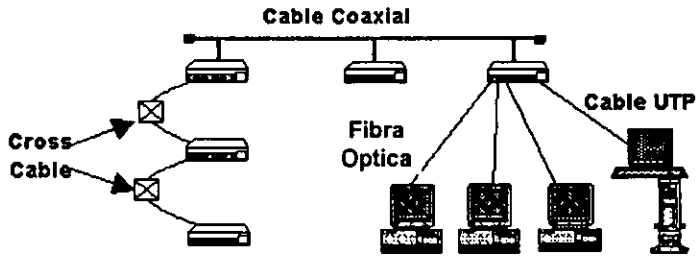


Fig. 4.5 Ejemplo de las diversas topologías de Ethernet combinadas.

Token Ring.

Esta arquitectura se desarrolló a principios de la década de los 80´s. Muchos creen que su creador fue IBM; sin embargo IBM adquirió los derechos para explotar la tecnología, y por supuesto la ha mejorado adicionándole un valor agregado. Token Ring es una arquitectura que se encuentra regida por el estándar IEEE 802.5. En el mercado mundial Token Ring es la segunda arquitectura con mayor base instalada. La topología tradicional que utiliza esta arquitectura es anillo; sin embargo ya existen implementaciones sin que exista un "cierre de anillo".

Así como ethernet ha desarrollado diversas variantes de su arquitectura, token ring también lo ha hecho. Originalmente la velocidad era de 4 Mbps; en la actualidad existe otro token ring a 16 Mbps. El método de acceso utilizado por esta arquitectura, al igual que ARCNet, es *token passing*; esto permite tener un acceso al medio en forma determinística.

El *token passing* es una señal que viaja por la LAN y la estación de trabajo que lo posee es quien puede hacer uso de los servicios de la LAN.

Teóricamente en token ring las estaciones se conectan unas con otras hasta formar un anillo, sin embargo en la práctica el anillo se forma entre los MAU o MSAU y de estos hacia los equipos la conexión se realiza en estrella. Los MAUs o MSAUs se conectan entre si mediante puerto destinados a este fin, denominados RI (Ring In) y RO (Ring Out).

Esta arquitectura es, posiblemente la que más tipos de cables puede utilizar, y al contrario de ethernet o ARCNet, no es posible indicar una distancia de operación, ya que esta depende del número de MAUs o MSAUs que se tengan, la distancia entre ellos, la distancia de los equipos a los MAUs o MSAUs, la velocidad de operación y el tipo de cable que se desee; con estos datos, la

aplicación de fórmulas y su correlación con unas tablas permiten indicar la distancia máxima de operación. En la figura 4.6 se muestra un ejemplo de esta arquitectura.

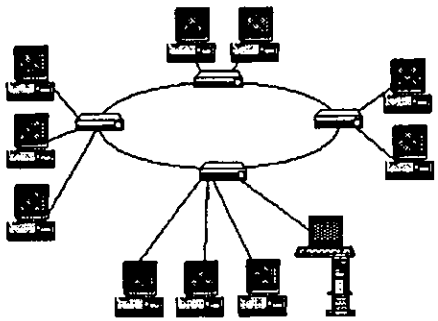


Fig. 4.6 Esquema de la Arquitectura Token Ring

4.2.1 Criterios para elegir ARCNet. ¿Que hay de ARCNet Plus?

ARCNet es una tecnología con varias desventajas debido a: su poca velocidad comparada con token ring o ethernet, la escasa cantidad de productos que existen en el mercado para comunicarse a otros ambientes de cómputo, la falta de un estándar que apoye esta tecnología, la carencia de una empresa que le dé un apoyo sustantivo y por otro lado el importante hecho de que Datapoint, creador de esta arquitectura adquiriera una compañía dedicada a la fabricación de tarjetas ethernet. Sin embargo, Datapoint afirma que para ARCNet no se ha dicho la última palabra, ya que ha invertido en el desarrollo de una nueva versión de ARCNet, denominada ARCNet Plus, con las ventajas de ARCNet, pero con velocidad de 20 Mbps y soporte a TCP/IP; sin embargo el mercado dice lo contrario, ya que ningún usuario considera que esta sea una arquitectura funcional.

En la segunda mitad de la década de los 80s ARCNet tuvo mucho auge en México, tanto por precio, como por compatibilidad, como por facilidad de uso; sin embargo en la actualidad esta tendencia está cambiando debido a los comentarios realizados en el párrafo anterior. En prácticamente ningún caso se recomendaría utilizar actualmente esta arquitectura, es una tecnología que se considera prácticamente muerta, por muchos factores, entre ellos, los mismos que en un principio le dieron tanto auge; compatibilidad, precio, seguridad en la inversión, facilidad de uso, precio, confianza de los usuarios, desarrollo de nuevos productos, etc. ya que todos estos factores se quedaron estancados y han sido superados por arquitecturas como ethernet y token ring. En el caso de que algún usuario de cualquier forma desee utilizar esta tecnología, se recomienda que solo lo haga bajo los siguientes criterios: que no se tenga necesidad de conectarse a otros ambientes, ni a otros lugares en forma remota, y que las aplicaciones sean típicas de una oficina muy pequeña; es decir, esta arquitectura solo podría ser recomendable para micro empresas, con bajísimo presupuesto, que poseen poco tráfico de información, que estén en un solo local y sus aplicaciones sean hojas de cálculo y procesadores de texto. Si se opta por esta tecnología es recomendable que el sistema operativo de red sea Netware ya que el mismo permite hacer en un momento dado conexión a arquitecturas ethernet o token ring en el mismo servidor, opción que Windows NT solo ofrece en versiones muy recientes. En realidad esta es una arquitectura en decadencia, y no se considera una opción adecuada versus los problemas que se pueden encontrar.

4.2.2 Criterios para elegir ethernet. ¿10BaseT, 10Base2, 10Base5?

Esta arquitectura se recomienda utilizar cuando:

1. No sea indispensable tener una secuencia de acceso a la LAN y sus servicios. Es decir que el acceso a LAN sea aleatorio, esto debido al tipo de método de acceso que maneja (CSMA/CD).
2. Si se desea tener conectividad con un ambiente diferente y que utilice la arquitectura de ethernet en forma nativa.
3. Si la inversión es un factor importante, ethernet es barato.
4. Si se desea tener flexibilidad en cuanto al diseño de la LAN.
5. Si se desea tener una gran cantidad de fabricantes que soporte esta arquitectura y sobre todo en México, asesores sobre esta tecnología.
6. Si el sistema operativo a utilizar es Unix, o alguna variante del mismo.

Por otro lado sabemos que existen diferentes tipos de ethernet, sin embargo la pregunta es ¿en los criterios de selección mencionados, cual de los tipos de ethernet se puede elegir?

El tipo de cable es uno de los principales parámetros que intervienen en esta decisión, ya que al día de hoy se utiliza el cableado estructurado, mismo que no incluye cable coaxial, por lo que en la parte horizontal (un mismo piso) se considera utilizar 10BaseT y el enlace entre pisos (back bone) con fibra óptica, y en el caso específico de ethernet, implica contar con FOIRL.

La ventaja que proporciona 10BaseT es que si uno de los equipos estando en la LAN presenta algún problema, el mismo no afecta a los demás componentes de la LAN. El único caso donde esto no necesariamente ocurre es cuando el cable se encuentra haciendo corto circuito, ya que este problema sí se refleja en toda la red.

En el caso de que se desee enlazar diversas LANs que se encuentren en un mismo edificio, se recomienda utilizar FOIRL, ya que este proporciona una mayor distancia. Lo que realmente se estaría haciendo sería formar un Back Bone, con esta arquitectura.

Adicionalmente FOIRL se recomienda en el caso de: requerir grandes distancias (máximo 2 Km entre dos bridges, lanswitches o routers, y 1 Km entre dos hubs), o en el caso de que se tengan fuentes electromagnéticas que alteren el tráfico de datos en los cables de cobre.

10Base2 se ha sido relegado para: redes muy pequeñas (5 nodos); cuando se desea cubrir pequeñas distancias y además no se utiliza una aplicación crítica en la misma. Este último punto es muy importante, ya que en el caso del cable coaxial, cuando se tiene problemas con el cable o sus componentes en cualquier punto de la red, esta deja de funcionar.

4.2.3 Criterios para elegir token ring. ¿Token ring a 4 o 16?

Como se podrá apreciar con las condiciones en donde aplica ethernet, es un poco difícil encuadrar a token ring; sin embargo esto es solo apariencia, ya que por supuesto los criterios de selección para esta arquitectura son distintos. Existe un campo de acción que se puede considerar exclusivo para token ring, por lo que, token ring se debe elegir cuando:

1. Se desee tener un acceso secuencial a los servicios de LAN. Es decir que forzosamente se deba tener un ordenamiento secuencial de acceso, como podría ser el caso del ensamblado de un producto.
2. Si se desea tener acceso a un equipo IBM o de cualquier otro fabricante, que nativamente considere a token ring como su opción de LAN.

3. Sea necesario contar con un sistema con redundancia en cableado. Este es el único sistema que presenta vías redundantes simultáneas, con sistema de respaldo (En ethernet se puede hacer pero no todos los fabricantes lo soportan, son opciones propietarias de algunos fabricantes).

Como sucede para el caso de ethernet, en token ring también se presentan opciones, solo que en este caso son solo dos; una es token ring a 4 Mbps y la otra token ring a 16 Mbps. Por un lado si tomamos la opción de 4 Mbps, que es la que más tiempo tiene en el mercado de las dos, y por lo tanto la que posee mayor número de pruebas realizadas, estaríamos invirtiendo en una tecnología que está siendo desplazada por la de 16 Mbps, y por otro lado a mayor velocidad menor distancia entre los dispositivos de la red, por lo que para tener una distribución similar en cuanto a distancias se refiere, la tecnología de 16 Mbps, requiere mayor número de componentes, y estos dos factores, la distancia y la mayor cantidad de dispositivos, hacen que el diseño de la red se complique.

La recomendación aquí, es que si se opta por utilizar la arquitectura de token ring, se adquiera una tarjeta de LAN que soporte ambas velocidades, opción muy común, y por otro lado se recomienda que se utilice la mayor velocidad que permita el cableado que se tenga; esto implicaría que todos los componentes de la LAN tendrían que estar a esa velocidad, ya que en caso de que un dispositivo estuviera a una velocidad menor, la red solo podría funcionar a la menor velocidad. Para el caso de que sea una LAN totalmente nueva y que no se tenga que enlazar a otras LANs se sugiere que el fabricante de las tarjetas sea 3Com o Bay Networks, mismos que han demostrado seriedad, representación en México y buena atención al mercado de token ring, incluso han desarrollado dispositivos para esta arquitectura.

Es adecuado considerar que mismo IBM ha empezado a sacar minicomputadoras y mainframes con posibilidad de conexión mediante ethernet, esto es importante debido a que anteriormente, los equipos de dicho fabricante solo contaban con la posibilidad de enlazarse a una arquitectura token ring. Además es conveniente tener en cuenta que en México muy pocos asesores pueden decir que proporcionan un soporte completo sobre esta arquitectura.

4.2.4 Tabla Comparativa entre ARCNet, ethernet y token ring.

Concepto	ARCNet	Ethernet	Token Ring
Estándar Seguido	Ninguno	802.3 IEEE	802.5 IEEE
Método de Acceso	Token Passing	CSMA/CD	Token Passing
Probabilidad de Acceso	Determinístico	Aleatorio	Determinístico
Velocidad	2.5 Mbps	10 Mbps	4/16 Mbps
Medio Físico	Coaxial, UTP, FO	Coaxial, UTP, FO	Coaxial, UTP, FO
Topología	Estrella y Bus	Estrella y Bus	Anillo y Estrella
Nombre Repetidor	Repetidor Activo	Hub	MAU o MSAU
Compatibilidad con Sistemas Operativos Estándar en Mercado	Si	Si	Si
Estabilidad en Mercado	Muy Poco Estable	Muy Estable	Estable
Conectividad a FDDI	No(solo si primero se convierte a Ethernet o Token Ring)	Si	Si
Distancia Máxima Entre Repetidores	2000 ft (600 m)	500 m	Varía
Aislamiento de Fallas	Si	Si	Si
Facilidad para Diseñar	Sencillo	Medio	Alto
Conexión a Bridges	No (tiene que convertirse a Ethernet o Token Ring)	Si	Si
Conexión a Routers	No (tiene que convertirse a Ethernet o Token Ring)	Si	Si
Soporta TCP/IP	No en forma nativa	Si	Si
Conexión simultánea a diversos tipos de cable.	Si	Si	Si

Mbps.- Mega Bits por Segundo (Mb/s)
UTP. - Cable trenzado sin blindaje.
FO.- Fibra Optica.
FDDI.- Fiber Distibuted Data Interface.
IEEE.- Instituto de Ingeniería Eléctrica y Electrónica.

4.3 Arquitecturas de alta velocidad. 100VG, fast ethernet, FDDI y ATM.

Hace algún tiempo solamente existía FDDI como arquitectura de LAN de alta velocidad; sin embargo, conforme se tienen aplicaciones mas demandantes de ancho de banda (videoconferencia, imágenes o multimedia), o negocios que por su giro requieren información inmediata, se han creado tecnologías acordes a estas necesidades.

Se considera alta velocidad a las tecnologías que operan por arriba de los 100 Mbps.

A continuación se expondrán las tecnologías que dominan al día de hoy las altas velocidades en las redes locales.

100VG.

En realidad el nombre completo de 100VG es 100VG AnyLan, sin embargo por el momento no es "Any Lan" (cualquier red), ya que solo tiene implementación para comunicarse a ethernet. Será "Any Lan" cuando tenga interfaz a token ring, ATM y FDDI, aunque por el momento se desconocen fechas para esto.

En un inicio se denominó 100BaseVG, aunque rápidamente cambió a como hoy se conoce: 100VG. VG significa Voice Grade, por utilizar un cable cuya característica es calidad de voz.

Esta tecnología tiene la facilidad de utilizar tres tipos cable, UTP, fibra óptica y STP. Para el caso de UTP el cable puede ser nivel 3, 4 o 5, utilizando cuatro pares en cualquier caso. Hace uso de dos cables cuando utiliza STP o fibra óptica.

100VG tiene la facultad de utilizar cables de 25 pares mediante el uso de conectores Telco de 50 pines.

El creador de 100VG es Hewlett Packard, y el estándar que utiliza es 802.12 de la IEEE. La topología que usa es estrella. El método de acceso que utiliza se denomina "Demanda por Prioridad".

Este método de acceso es una simplificación del esquema de CSMA/CD utilizado en ethernet a 10 Mbps. Al eliminar la colisión de paquetes se simplifica la operación de la red y elimina la sobrecarga por colisiones y recuperación de paquetes.

Con demanda por prioridad, un nodo solicita permiso del hub para transmitir un paquete sobre la red. Si la red está en espera, el hub confirma la petición y la estación inicia la transmisión de su paquete. Conforme el paquete llega al hub, el hub decodifica la dirección destino y en forma automática direcciona el paquete entrante al puerto destino. Si más de una petición es recibida al mismo tiempo, el hub confirma cada petición a su turno, hasta que todas las peticiones se han confirmado.

Como los paquetes de información se direccionan únicamente a su puerto destino, ninguna otra estación en la red verá el paquete de información, su fuente o su destino. Esto proporciona un nivel de privacia a nivel enlace o seguridad que no se obtiene actualmente con redes como ethernet, token ring, FDDI o fast ethernet.

Adicionalmente, ya que el hub sirve de árbitro para las peticiones individuales de transmisión de paquetes, éste puede coordinar peticiones con distintas prioridades, confirmando peticiones de paquetes de alto nivel antes de peticiones con prioridad normales. Al conocer el número de aplicaciones que transmiten en alta prioridad, a estas aplicaciones se les puede asegurar un mínimo de espera antes de que su paquete sea transmitido a su destino. Esto proporciona en forma efectiva un ancho de banda garantizado para estas aplicaciones, sin importar el tráfico de la red.

Fast Ethernet.

Uno de los creadores de esta tecnología es 3Com, y el estándar fue aprobado en junio de 1995, por lo que es un estándar realmente nuevo. El estándar que posee esta tecnología es 802.3u de la IEEE; como se puede observar es una variante de ethernet, solo que a 100 Mbps.

A fast ethernet también se le conoce como 100BaseT, aunque en realidad está mal empleado el término, ya que la T tradicionalmente se utiliza para indicar cableado UTP. Esta tecnología también permite utilizar fibra óptica, motivo por el que aquí se denominará como fast ethernet.

La topología que utiliza esta arquitectura es estrella.

Fast Ethernet ha sido creado a partir de diversas propuestas tecnológicas, mismas que solucionan la problemática presentada por cableados UTP y de fibra óptica. Estas tecnologías son 100Base-FX (fibra óptica), 100Base-TX (UTP categoría 5 y STP) y 100Base-T4 (UTP categoría 3, 4, y 5), mismas que pueden ser combinadas en una misma red.

100Base-TX utiliza dos pares y 100Base-T4 hace uso de cuatro pares. Estas tecnologías no permiten utilizar cables de 25 pares con conector Telco.

Esta tecnología ha sido diseñada para ser la evolución más natural de ethernet a 10 Mbps, ya que también utiliza el mismo método de acceso (CSMA/CD); en otras palabras fast ethernet es el mismo ethernet pero 10 veces mas rápido.

FDDI.

Al igual que la mayoría de las tecnologías, FDDI ha tenido ramificaciones, como CDDI, e incluso el mismo fast ethernet, en el estándar 100BaseTX, fue diseñado a partir de FDDI.

Por sus características se recomienda para ser utilizada en el Back Bone, o en aplicaciones de misión crítica debido a la redundancia que presenta.

Fiber Distributed Data Interface (FDDI) es una arquitectura de red que además de tener cobertura local, también se podría considerar de campus.

FDDI es un sistema de transmisión de datos sobre conductores de fibra óptica. El uso de fibra óptica en lugar de conductores de cobre proporciona ciertas ventajas, como es la cantidad de información que puede transportar y la inmunidad que ofrece a interferencias; esto último debido a que la fibra óptica transporta señales de luz, y la luz no se ve afectada por interferencias de radio frecuencia (RFI) o de campos electromagnéticos.

FDDI transmite información a 100 Mbps sobre fibra óptica con una topología de anillo doble, con una distancia entre dos equipos de 2 Km y con una cobertura total de 100 Km, mediante un protocolo de acceso al medio denominado token passing. FDDI aunque similar a token ring (IEEE 802.5), presenta mayor velocidad para pasar de un equipo a otro y además posee una codificación más eficiente.

Si algún equipo se desea conectar al anillo doble de fibra óptica es necesario hacerlo mediante una conexión DAS (Dual Attach Station), y si el equipo se desea conectar a FDDI pero sin la redundancia que presenta el anillo doble, entonces lo hace a través de una conexión SAS (Single Attach Station).

FDDI pertenece al estándar X3T9.5 de ANSI (American National Standards Institute), mismo que fue publicado en 1987. La figura 4.7 muestra un diagrama de la arquitectura FDDI.

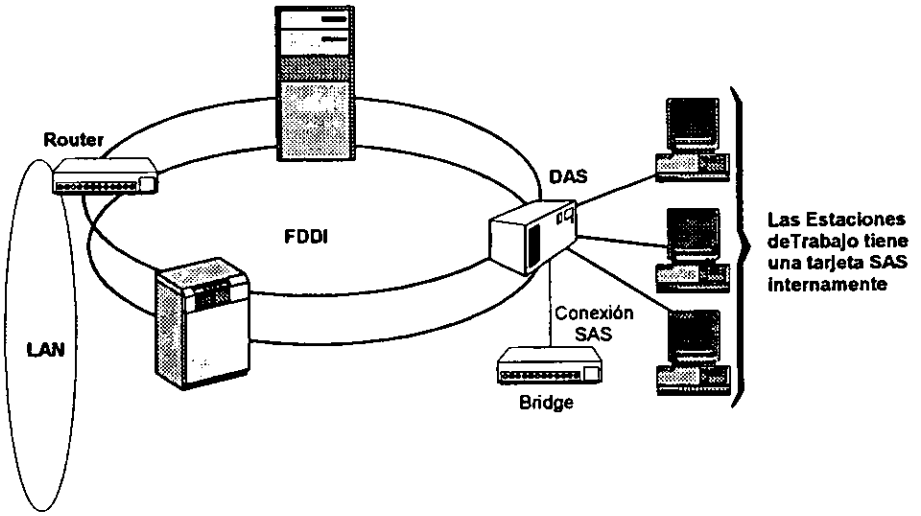


Fig. 4.7 Esquema de FDDI

Por otro lado CDDI (Copper Distributed Data Interface) es la misma implementación de FDDI solo que sobre cobre, pudiendo ser UTP o STP. Esta variante se basa en el estándar de ANSI denominado Twisted Pair Physical Medium Dependent (TPPMD).

ATM.

ATM basó su desarrollo en los trabajos que realizó el Grupo de Estudio XVIII de International Telecommunication Union Telecomminication Standardization Sector (ITU-T) desarrollando primeramente Broadband Integrated Services Digital Network (BISDN) para la transmisión a alta velocidad de voz, vídeo y datos en redes públicas.

El Forum de ATM se fundó a finales de 1991 bajo la promoción de Adaptive, Corp., Cisco Systems Inc., Northern Telecom Ltd. y Sprint Corp. Este Forum tiene 606 miembros, de los cuales 179 son miembros principales (que

pagan por este privilegio $10,000 USD al año), todos divididos en nueve grupos de trabajo.

ATM es una tecnología combinada de alta velocidad de switching y multiplexing, cuyos beneficios conjuntos son retardo de transmisión constante y capacidad garantizada, así como la flexibilidad y eficiencia para tráfico intermitente. Esta tecnología permite transmitir diferentes tipos de tráfico en forma simultánea, incluyendo voz, vídeo y datos.

ATM cuenta con topología en estrella y su operación puede describirse en forma lógica en tres planos; usuario, administración y control. El plano del usuario coordina la interfaz entre los protocolos utilizados como podría ser IP; El plano de administración coordina lo niveles del stack de ATM; y por último, el plano de control coordina la señalización, así como el establecimiento y rompimiento de los enlaces virtuales.

Al igual que las tecnologías anteriormente descritas esta también presenta sus variantes en cuanto a velocidad se refiere. Estas velocidades varían desde 25 Mbps pasando por 52 Mbps y 155 Mbps hasta 622 Mbps, planeándose a futuro una velocidad de 2.488 Gbps.

4.3.1 Criterios para elegir 100VG.

Esta tecnología es una excelente opción cuando se presentan las siguientes situaciones:

1. Se requiera alta velocidad.
2. El local sea de amplias dimensiones.
3. Se tenga necesidades de seguridad en la información.

4.3.2 Criterios para elegir fast ethernet.

Las situaciones en las que se recomienda la utilización de esta tecnología son:

1. Se requiera alta velocidad.
2. No se requiera cubrir un área muy extensa.
3. Se disponga de poco presupuesto, pero con grandes necesidades de alta velocidad.

4.3.3 Criterios para elegir FDDI. ¿FDDI o CDDI?

Por el hecho de que FDDI utiliza fibra óptica doble, posee características de alto rendimiento y seguridad en la transmisión de los datos, y debido a la distancia y velocidad que soporta se clasifica como una tecnología de enlace entre diversos puntos apoyando el desarrollo de MANs. Las características de esta tecnología permiten que se catalogue como una arquitectura de enlace entre grupos de usuarios, procesos distribuidos, procesamiento de imágenes y conectividad entre edificios.

El uso de fibra óptica evita que exista generación de emisiones eléctricas que puedan ser detectadas a distancia, por lo que esta tecnología presenta características de seguridad muy especiales, principalmente para gobiernos, bancos o instituciones que requieran una seguridad de este nivel.

4.3.4 Criterios para elegir ATM. ¿25, 52, 155, 622 o 2,488 Mbps?

ATM (Asynchronous Transfer Mode) se considera la tecnología del futuro tanto para redes de área local (LAN) como para redes de área amplia (WAN), y aunque la tecnología ya se encuentra disponible, aunque solo para LAN, en este

momento el estándar para esta tecnología no se encuentra terminado. Según el Forum de ATM, la definición final del estándar se llevaría a cabo a finales de 1997, lo que implica que si dicha tecnología se adquiere al día de hoy, y este plazo no se cumpliera seguramente los productos adquiridos serán incompatibles con el estándar. Si por alguna causa se adquiere esta tecnología aún sin tener el estándar terminado se recomienda llegar a un acuerdo con el fabricante, de actualización al estándar final sin costo o al menor costo posible. Esta situación no es nueva, ya que cuando FDDI se encontraba en una situación similar, UB (fabricante de esta tecnología) comercializó diversos sistemas FDDI, mismos que tuvieron que ser desechados totalmente al momento de salir el estándar final, ya que una gran cantidad de aplicaciones especiales para aprovechar FDDI, no eran soportadas por esta tecnología de UB.

Se recomienda tener esta tecnología en observación debido a qué, por los alcances que tendrá, será la mejor tecnología de redes (LAN, MAN y WAN) a partir del año 2005. Inclusive quienes mayor provecho obtendrán de esta tecnología son los llamados "carriers", que son compañías de comunicaciones que se encargan de proveer servicios de transporte para datos, vídeo y voz, creando redes públicas de datos. Por supuesto los "carriers" no serán los únicos que exploten esta tecnología, ya que aquellos corporativos o entidades que requieran de un transporte de información sumamente rápido, confiable y que garantice una inversión redituable a largo plazo serán usuarios ideales de esta tecnología.

Al día de hoy esta tecnología se recomienda utilizar como back bone de edificios grandes, o para enlace entre edificios. Las bajas velocidades prácticamente no se usan. Las velocidades que mayor demanda han tenido son la de 155 y de 622 Mbps, debido a la relación costo beneficio que presentan.

4.3.5 Tabla comparativa entre tecnologías de alta velocidad.

Para poder comparar ATM con las demás tecnologías, es importante comentar que la comparación directa debería de ser más contra: X.25, Frame Relay y Switched Multimegabit Data Service (SMDS); sin embargo, por el momento se considera una tecnología más orientada a LAN en campus, que a MAN o WAN, y que por otro lado ATM es considerada una tecnología de switcheo de paquetes. El hecho de haberse incluido en este capítulo fue para no dejar fuera la tecnología que se considera la panacea de las arquitecturas de redes, por lo que en la tabla que se presenta a continuación no se incluirá dicha comparación.

CARACTERÍSTICA	Fast Ethernet	100VG	FDDI/CDDI
Topología física	estrella	estrella	anillo
Topología lógica	bus	estrella	anillo
Método de Acceso	CSMA/CD	Demanda por Prioridad	Token Passing
Velocidad	100 Mbps	100 Mbps	100 Mbps
Rendimiento esperado	60%	90%	98%
Estándar	IEEE 802.3u	IEEE 802.12	ANSI X3T9.5
Cable soportado	UTP 3, 4 y 5. STP. Fibra Óptica	UTP 3, 4 y 5. STP. Fibra Óptica	UTP 5. STP. Fibra Óptica.
Precio	X	1.2X	3X
Distancia máxima entre dos PCs usando UTP.	205 m	500 m	200 m
Distancia máxima entre dos PCs usando FO.	309 m	2,000 m	2,000 m
Convivencia directa con Ethernet a 10 Mbps.	Si	Si	Si
Convivencia directa con Token Ring a 4 y 16 Mbps.	Si	Si	Si
Convivencia directa con FDDI.	Si	No	----------
Convivencia directa con ATM.	Si	No	Si
Cascadeo múltiple sin uso de bridges o routers	No	Si	Si
Soporte a multimedia garantizando ancho de banda	No	Si	Si
Existe Routers que soporten la tecnología.	Si	No	Si
Utilización Principal.	Escritorio	Escritorio	Back Bone
Soportado por Novell.	Si	Si	Si
Soportado por Windows NT.	Si	Si	Si
Soportado por Unix.	Si	Si	Si

CAPÍTULO 5
Diferencias Entre los Tipos de Cableado

Temas del capítulo.

5.1 Cableado tradicional.

5.2 Cableado estructurado.

En cualquier tipo de red o sistema existe la posibilidad de que fallen los componentes. Sin embargo uno de los puntos más vulnerable a las fallas en una LAN es el cableado. Se considera que las fallas en el cableado de una LAN originan del 50% al 70% de los problemas que se presentan, entre los que se encuentran; la suspensión de las comunicaciones y los errores binarios; esto sin lugar a dudas habla por si mismo del punto primordial a cuidar; por supuesto sin dejar a un lado ninguno de los demás componentes que forman una LAN. La pregunta entonces es ¿debo mejorar la calidad del cable? ¿su diseño? o ¿capacitar al personal que instala?. Por supuesto todo esto hará que disminuyan los problemas en un cableado; sin embargo ha aparecido en el mercado de LANs una tecnología, denominada cableado estructurado. Para explicar este concepto adecuadamente, se expondrá en primer lugar en que consiste el cableado tradicional.

5.1 Cableado tradicional.

En el inicio de las redes locales y hasta hace relativamente poco tiempo, seis años, solo se utilizaba cable coaxial para enlazar los equipos que conformaban una LAN; esto debido principalmente a que esta tecnología había

sido desarrollada con estas normas; por ejemplo ethernet, con su cable coaxial delgado (RG-58) o grueso (RG-8), token ring con sus diversos tipos de cables blindados y por supuesto ARCNet con su cable coaxial (RG-62). Cableados que si bien cubrían las necesidades de comunicación no proporcionaban ventajas adicionales.

Este tipo de cableado presenta la gran ventaja de proporcionar una buena distancia, debido a la malla o mallas que protegen la integridad de los datos, y que además es relativamente fácil de conseguir e instalar.

Sin embargo ofrece más desventajas que ventajas; las desventajas principales son:

- Cualquier crecimiento por pequeño que sea implica cableado adicional.

  Este punto, y seguramente varios otros, se explican sabiendo que este tipo de cableado se lleva a cabo de punta a punta, por lo que si se requiere de un nuevo servicio, es necesario, hacer un nuevo cableado del servicio correspondiente.
- No existen sistemas de administración adecuados.

  El cableado tradicional no tuvo un apoyo adecuado en cuanto a la administración se refiere, ya que cuando se empezaron a introducir al mercado los productos de administración de cableado, se empezaba a promover el cableado estructurado. Es importante mencionar que aún cuando se hubieran tenido con anticipación los productos de administración, el cableado tradicional de cualquier manera no hubiera sobrevivido.
- No presenta segmentación a problemas.

  En tecnologías como ethernet con 10Base2 o 10Base5, cuando se produce un problema en el cableado, se detiene la operación total de la red, lo que hace que las fallas sean generales, no particulares.

- La detección de problemas es difícil.

  Apoyándose en el punto anterior, cuando un cableado de este tipo falla, es difícil conocer la ubicación del problema.

- La modificación de ubicación del mobiliario, implica recableado total.

  Debido a que el cableado se instala punta a punta, cualquier modificación en su trayectoria origina un cambio total, teniendo que llevar a cabo una nueva instalación de cable, siendo difícil la utilización parcial del cableado anterior o actual.

Adicionalmente se tiene un problema de administración y mantenimiento de este tipo de sistemas, ya que no existe fácil acceso a los elementos para obtener una organización adecuada del cableado. Es importante comentar que el sistema de cableado tradicional se lleva a cabo de punta a punta, sin contar con subsistemas de administración y mantenimiento como en el caso del tendido telefónico, que por su estructura es un sistema modular y muy flexible.

A lo anterior es conveniente agregar que un cable coaxial RG-58 ocupa 2.5 veces mas que el espacio ocupado por un cable UTP, lo que hace que se requiera mas espacio disponible para instalarlo. En el caso del cable RG-8, este ocupa el mismo espacio que un cable de 25 pares UTP, lo que implica tener 6 servicios de datos en lugar de uno. Un punto importante es que la administración de un cableado coaxial hace que se requiera una gran cantidad de espacio. Así mismo existen configuraciones de cables que cuentan con 25 pares y ocupan el espacio equivalente de cuatro cables coaxiales RG-58; es decir, con el cable de 25 pares se podría dar servicio a 6 conexiones de red (se utilizan 4 por conexión), mientras que en el caso del cable coaxial, en el mismo espacio, solo se proporcionarían servicio a cuatro. Lo que hace que se tengan 50% más de servicios con una configuración de este tipo (25 pares) con respecto al cable

coaxial, en espacios similares. Posiblemente en un solo tendido no se alcance a notar la diferencia, pero ¿qué pasa con el tendido de una red de tamaño estándar, que en México se considera de alrededor de 50 nodos? En realidad no se podría llevar a cabo la instalación del cableado utilizando el coaxial por la gran cantidad de espacio que utiliza.

El precio de un cable coaxial es aproximadamente 25% mas alto que el del cable UTP; sin embargo es importante hacer notar que si bien el cable coaxial es mas caro, la cantidad de elementos que se involucran en un cableado estructurado incrementa cuatro o cinco veces el costo de un cableado estructurado con respecto a un cableado tradicional; esto sin considerar, para el caso de ethernet 10BaseT, el costo de los hubs, mismos que no se requieren cuando se utiliza un cableado tradicional.

5.2 Cableado estructurado.

Este término se empieza a emplear en el campo de las redes locales al momento que el cableado denominado UTP, hace acto de presencia en esta tecnología. El cableado estructurado tiene su principal fuerza en el dicho que dice "divide y vencerás"; esto debido a que al tener un cableado del tipo tradicional como es el coaxial, las fallas que se originaban en este tipo de cable afectaban a todos los componentes de la LAN, hablando primordialmente de ethernet, estándar que impulsó inicialmente este concepto, con la aparición de la arquitectura denominada 10BaseT.

El cableado estructurado consiste en realizar la implementación y administración conjunta de señales de vídeo, voz, datos y control sobre un mismo cableado y desde un mismo punto. Este tipo de cableado presenta las siguientes ventajas:

- Realizar conjuntamente la labor del cableado de vídeo, voz, datos y señales de control. Cuando se implementa en un edificio una solución que abarque las cuatro señales anteriormente mencionadas, se habla de edificios inteligentes, donde incluso las señales de emergencia, temperatura, vigilancia, etc. se administran desde un punto común, y bajo un mismo esquema de cableado. Es conveniente aclarar que para redes locales pequeñas, una implementación de este tipo es más costosa que una bajo el cableado tradicional, debido a que se requiere hacer demasiados cambios y adecuaciones para implementarse. El hecho de que el cable UTP sea más barato que el cable coaxial, no quiere decir que un cableado de LAN con cable UTP sea más barato; esto debido a que requiere, por ejemplo para ethernet, invertir en repetidores, mismos que no son utilizados para una implementación con cable coaxial y por otro lado, si se desea hacer la implementación para token ring, será necesario muchas veces utilizar más componentes para conseguir mayor distancia. Como se puede apreciar, en ambos casos una implementación así es más costosa, pero a la vez más segura, confiable y fácil de administrar, puntos que sin lugar a dudas hacen que la inversión en un cableado estructurado sea por demás rentable.
- Detección sencilla de fallas. El tener una infraestructura segmentada, como en este caso, hace que la detección y corrección de fallas sea mucho más fácil y rápida. Esta tecnología debido a sus características de administración y flexibilidad también requiere de mayor número de componentes, lo que a su vez implica mayores costos.
- Realizar cambios físicos sin grandes esfuerzos. Es común que en una oficina se realicen reubicaciones de personal; sin embargo, al ser realizadas no se requieren cambios drásticos en las instalaciones debido a que el sistema es

modular, lo que permite aprovechar el 80% del cableado existente al llevar a cabo una reubicación. Por otro lado en el peor de los casos, si es necesario instalar a alguna persona en un lugar en que no exista ninguna de estas conexiones, será relativamente sencillo llevar a cabo la instalación tanto de la línea telefónica como de la línea de conexión a la LAN. Cuando se diseña con cableado estructurado se previene crecimientos en número de servicios, siendo estos crecimientos calculados basándose en el espacio del local.

- Capacitación del personal. En las grandes corporaciones, que es a donde va dirigida esta tecnología, cuentan normalmente con personal técnico en telefonía, y dado que la implementación es muy similar, es fácil conseguir y capacitar personal que realice el trabajo de cableado. Esto no quiere decir que cualquier persona con conocimientos de telefonía puede realizar un cableado de este tipo; simplemente que les será más fácil adquirir los conocimientos necesarios para realizar esta labor.

Así como el cableado tradicional tiene bien definido su campo de acción, también lo tiene el cableado estructurado, basándose en criterios que son en la mayoría de los casos mutuamente excluyentes, por lo que la selección del cableado es muy sencilla.

El ambiente ideal donde se recomienda el cableado estructurado es para ser implementado principalmente, en edificios nuevos, dado que en estos casos se contempla el cableado de datos en los diseños del edificio, pudiendo ser canaletas o escalerillas para este tipo de cableado. Cuando se requiere un cableado estructurado en edificios viejos, normalmente es necesario una inversión un poco mayor, debido a que no es común encontrar la infraestructura necesaria para su implementación.

Es importante tener en cuenta que debido al hecho de que las líneas telefónicas puedan utilizar este tipo de cableado no significa que las

comunicaciones de LAN puedan implementarse sobre líneas telefónicas existentes; esto debido principalmente a que se requiere un cable UTP con características especiales. Este último comentario va dirigido a las implementaciones que deseen realizarse en edificios viejos con cableados telefónicos que deseen aprovecharse. Es importante remarcar el hecho de que el cable utilizado en este tipo de implementaciones ha sido mal llamado cable telefónico, por el hecho de basarse en esta tecnología y además de tener similitud de cableado; sin embargo posee características especiales que lo hacen diferente de un cable telefónico común.

En segundo lugar el cableado estructurado se recomienda para LANs grandes, o en su defecto que requieran de gran seguridad en el cableado.

Los puntos anteriores no implican que no se puedan conjuntar ambos tipos de cableados; sin embargo el concepto original, de realizar un solo cableado, se distorsionaría, y en el mejor de los casos solo estriamos utilizando parcialmente el concepto.

Se recomienda que si se va a realizar un cableado totalmente estructurado se tenga en cuenta lo siguiente:

- Lugares de acceso al cableado mayores que los telefónicos, debido a que en estos lugares es necesario instalar equipo de LAN, como son repetidores, algunas veces bridges o lanswitches y con menor frecuencia routers; estos tres últimos equipos serán discutidos en el capítulo 6.
- Es adecuado que se tenga acceso al cableado en cada piso. Esto con la finalidad de que cualquier adición, modificación o corrección sea sencilla.
- El nivel del cable recomendado al día de hoy es nivel 5, ya que soporta altas velocidades, soportando arquitecturas como ethernet, fast ethernet, token ring, FDDI (CDDI) y 100VG ¿y porqué no? estar preparados por si en un futuro existe una tecnología más rápida. Los principales fabricantes de este tipo de

tecnología ofrecen una garantía de 15 años sobre los cableados que ofrecen, esto habla bien de la confianza que se tiene.

- El acceso a los paneles de cableado se encuentre totalmente restringido, debido principalmente a que en ellos se encontrará la columna vertebral de nuestras comunicaciones.
- Al realizar un esquema de este tipo, es por demás importante seguir el código de colores que se ha establecido para esta tecnología. Esto es vital dado que más de una persona estará involucrada en una comunicación de este tipo.
- Es conveniente que quien realice el diseño de un cableado estructurado posea conocimientos tanto de telefonía como de redes locales, debido a que será el responsable del funcionamiento adecuado de ambos tipos de comunicaciones. El diseñar la trayectoria del cableado, no implica que se esté diseñado una LAN, ya que para realizar un diseño de LAN se requiere conocer las reglas de diseño de la arquitectura que se trate, así como conocer cierta información que permita implementar una LAN con un desempeño adecuado.
- Por supuesto, se deberán de respetar las normas para efectuar cableados estructurados.

  Los principales fabricantes de sistemas de cableado estructurado han desarrollado sobre la base de estos estándares sus propios estándares. Los principales fabricantes que producen sistemas de cableado estructurado son: AT&T (ahora Lucent Technologies) y Northern Telecom.

Al utilizar el concepto de cableado estructurado y llevar a cabo una implementación de este tipo se debe recordar que finalmente se deberá hacer una separación entre las señales de vídeo, voz y control de las señales de LAN,

misma que puede realizarse en el panel de distribución, en el lugar en donde se requieran estos servicios. Algunos fabricantes sacaron al mercado tarjetas de red incorporando conexiones de voz y datos, realizando la separación internamente, con lo que el teléfono en lugar de conectarse a la pared, se conecta directamente a la tarjeta de LAN instalada en la microcomputadora. Estas tarjetas presentan dos conectores: uno para la conexión del cableado de voz y datos y uno para el teléfono. No se requiere que la PC se encuentre encendida para que funcione el teléfono. Al día de hoy existen pocas tarjetas de este tipo; sin embargo esto demuestra el auge que el cableado estructurado ha despertado en el mundo de las redes locales.

CAPÍTULO 6
Cómo mejorar el desempeño de una LAN

Temas del capítulo

6.1. Introducción a bridges locales.
6.2. ¿Cuándo aplica un bridge local?
6.3. Introducción a lanswitches.
6.4. ¿Cuándo aplica un lanswitch?
6.5. Diferencias entre lanswitches y bridges locales.
6.6. Información necesaria para mejorar el desempeño de una LAN.

Existen muchas formas de mejorar el desempeño de una LAN, algunas de ellas triviales, como: incrementar la velocidad en la LAN, contar con mejores tarjetas de red, poner un servidor con mayores capacidades, instalar otro servidor para dividir tareas, etc. o utilizando otras técnicas mas complicadas como mejorar el tráfico en red, eficientar los protocolos, etc. Sin embargo para poder incrementar el desempeño de una LAN se requiere antes que nada conocer el estado de la misma; esto con la finalidad de que las acciones que se tomen sean enfocadas a resolver el problema real, no sus efectos, ya que existe una gran variedad de problemas en una red que demeritan su desempeño.

En este capítulo se hablará de como mejorar el desempeño de una LAN sobre la base del tráfico de la misma.

Existen básicamente dos dispositivos que se utilizan en estos casos: los bridges locales y los lanswitches. Ambos dispositivos operan en las dos primeras capas del nivel de OSI, es decir, son independientes de los protocolos superiores.

Tanto bridges locales como lanswitches segmentan tráfico y ayudan a mejoran el desempeño de una LAN. Ambos segmentan el tráfico basándose en las direcciones MAC de los nodos.

6.1 Introducción a bridges locales.

La operación básica de los bridges locales y remotos es exactamente la misma: segmentar tráfico y conectar LANs entre sí. La diferencia entre bridges locales y remotos estriba en que los bridges locales no tienen puertos de WAN, solo de LAN, y los bridges remotos tienen tanto puertos de LAN como de WAN.

Un bridge es un dispositivo que opera sobre la base de las direcciones MAC de cada dispositivo conectado en la red, y con estas direcciones crea, por cada puerto una tabla de direcciones, lo que le permite conocer la ubicación de todos los dispositivos en la LAN, así como la ruta que debe seguir el flujo de información para que dos dispositivos puedan entablar comunicación; también permite restringir el paso de información de una LAN a otra en forma selectiva o global, haciendo con esto segmentación de tráfico y evita tráfico "basura", entendiéndose por tráfico basura la propagación de frames (paquetes de información) más allá de la estación destino. Al evitar el tráfico basura se proporciona mayor estabilidad y funcionalidad a un conjunto de LANs, no importando si estas están conectadas local o remotamente. Los bridges también se utilizan para extender el alcance de LAN.

Existen cuatro tipos de bridges, dependiendo de su operación:

Sobre estos cuatro tipos de bridges que se explican a continuación no existe diferencia para cuando se habla de bridges locales o remotos.

- Transparent bridge.
- Translating bridge.
- Encapsulating bridge.
- Source routing bridges.

- Transparent bridge.

Este tipo de bridge fue el que primeramente hizo su aparición en el mercado. Su función es interconectar LANs con arquitectura similar; por ejemplo dos ethernet o dos token ring (no existen bridges para ARCNet). En la figura 6.1 se muestra este concepto.

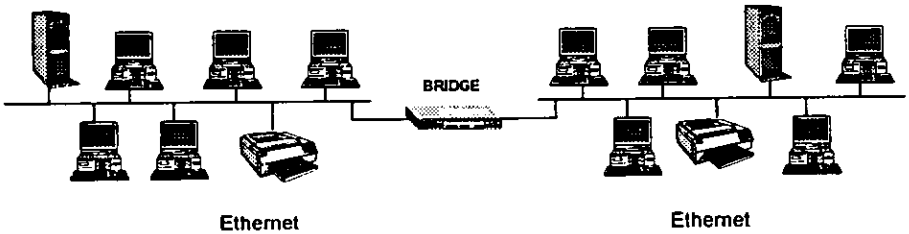


Fig. 6.1 Transparent bridge.

- Translating bridge.

Los bridges que se encuentran bajo este tipo presentan la característica de conectar LANs de arquitectura diferente; por ejemplo una ethernet y una token ring (no existe comunicación a ARCNet). En la figura 6.2 se muestra un esquema de este concepto.

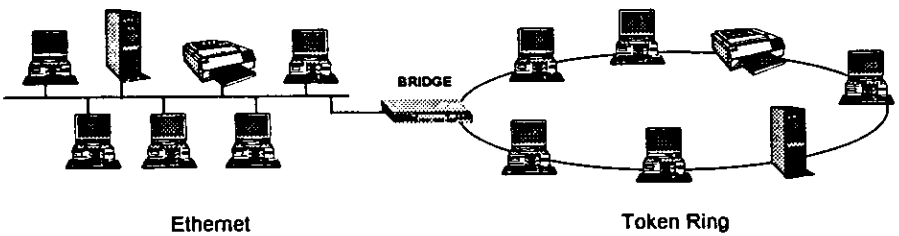


Fig. 6.2 Translating bridge

- Encapsulating bridge

Este tipo de bridge se asocia generalmente a un back bone, ya que su función es la de interconectar LANs a través de una arquitectura diferente; por ejemplo, comunicar dos LANs ethernet por medio de una arquitectura FDDI. En el caso de ARCNet solo se puede implementar si se utiliza el sistema operativo de red Netware. En la figura 6.3 se muestra un esquema de esta tecnología.

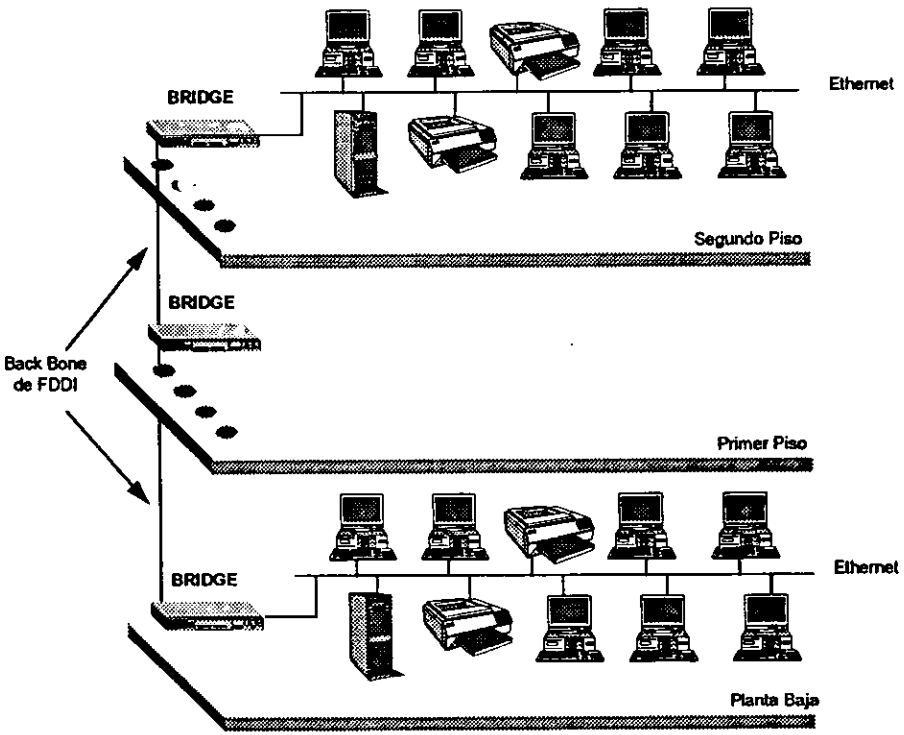


Fig. 6.3 Encapsulating bridge

- Source routing bridges

Esta técnica fue creada por IBM para enviar frames entre diferentes LANs token ring, e incorporada a los bridges ethernet. Este tipo de bridges lleva a cabo la siguiente operación: al realizar una comunicación entre dos PCs o servidores que se encuentran en LANs diferentes, mismas que están conectadas mediante bridges en forma redundante, el frame de búsqueda enviado por el equipo fuente, puede encontrar varios caminos para encontrar al equipo destino; sin embargo uno de estos caminos será el más rápido; en ese momento se realiza una conexión por la ruta más rápida y las demás rutas son ignoradas al momento de continuar la transmisión. Lo que realmente hacen los bridges es mantener en sus tablas de direcciones la ruta optima de comunicación entre LANs.

6.2 ¿Cuando aplica un bridge local?

Al día de hoy son pocas las situaciones en donde se recomendaría hacer uso de un bridge local; sobre todo debido a que equipos que posean la funcionalidad de bridges como única opción son muy pocos. Los routers, de los que se hablará en el próximo capítulo, cuentan con una opción para ser configurados como bridges locales o remotos, dependiendo principalmente de los puertos del router.

La única situación donde se recomendaría utilizar un bridge es que ya se tenga un router y que este se configure como bridge para no tener que invertir; es decir, solo por aprovechar una infraestructura que ya exista; sin embargo sí se requiere de cinco o más bridges, aún pudiendo configurar routers como bridges, se recomienda revisar el diseño de la LAN, ya que difícilmente se requiere tal

cantidad de bridges, y en caso de ser verdaderamente necesario, posiblemente la tecnología de bridging no sea la mejor solución.

6.3 Introducción a lanswitches.

Los lanswitches son los dispositivos que al día de hoy empiezan a substituir a los bridges en lo que a configuración local se refiere. Estos equipos en la actualidad no presentan opciones de comunicación remota, contando solo con puertos de LAN. Los lanswitches son dispositivos que al igual que los bridges, operan en la capa dos de OSI, y su operación se basa en las direcciones origen y destino que se encuentran en el frame; sin embargo a diferencia de los bridges, los lanswitches no esperan a capturar la totalidad del frame para poder leer estas direcciones, simplemente leen las direcciones, que se encuentran al principio de cada frame y deciden. Debido que no esperan a capturar el frame completo, el proceso de decisión es mucho más rápido que el de un bridge. Adicionalmente a tomar las decisiones con mayor rapidez, llevan a cabo conexiones de equipos en forma paralela. En la figura 6.4 se muestra este concepto.

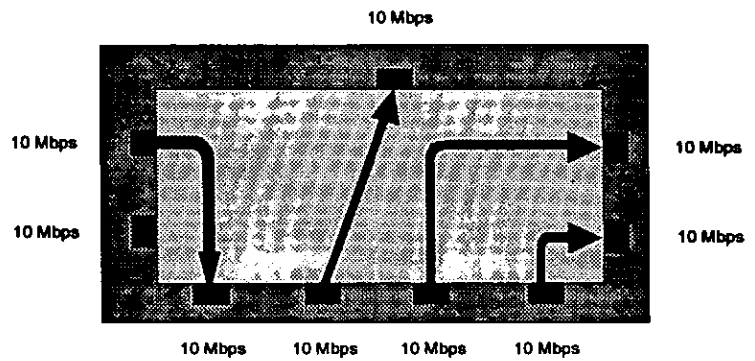


Fig. 6.4 Operación básica de un lanswitch.

6.4 ¿Cuando aplica un lanswitch?

Los lanswitches tiene su principal aplicación en redes locales grandes, ya que permiten segmentar el tráfico y por ende mejorar el desempeño de la red.

El término "red local grande" es muy subjetivo, por lo que se hará un dimensionamiento que permita tener un mejor panorama sobre lo que se considera una LAN grande.

Existen básicamente dos parámetros para determinar el tamaño de una LAN: la cantidad de usuarios y el tráfico.

Una LAN se puede considerar grande cuando:

- Se tiene una gran cantidad de usuarios, 100 o más.
- La utilización de la red es muy alta, mayor al 25%.
- Cuenta con cuatro o más servidores.
- Si se cuenta con enlaces remotos (cinco o más usuarios).

Los elementos que intervienen directamente en el tamaño de una LAN son servidores y estaciones de trabajo, por lo que a estos equipos nos enfocaremos.

Es muy común que los servidores y estaciones de trabajo de alto desempeño se conecten directamente a un puerto del lanswitch, dedicando con esto un ancho de banda exclusivo para dichos dispositivos, y los demás puertos se comparten con los demás equipos conectados en red.

Estos dispositivos permiten dedicar un canal, por ejemplo de 10 Mbps en el caso de ethernet, a un solo equipo o servicio, lo que hace que se pueda mejorar el tráfico en los equipos requeridos. Por ejèmplo se puede tener conectado un puerto dedicado para cada servidor, y conectar a grupos de 15 usuarios a otros

puertos, lo que hace que se tengan redes grandes funcionando con un desempeño similar a redes pequeñas.

Una ventaja adicional del switch es la seguridad, ya que solo los equipos que se encuentren conectados a los puertos que se comunican entre sí podrán ver la información que se transmita; los otros puertos no se enteran de lo que está sucediendo.

En la figura 6.5 se muestra un esquema sencillo utilizando un lanswitch en una LAN, misma que cuenta con tres departamentos. En realidad lo que se estaría teniendo es: seis redes locales, tres de ellas siendo grupos de trabajo, y las otras tres formadas, cada una, por un solo usuario. Este esquema se podría visualizar bajo la arquitectura de ethernet 10BaseT. La ventaja en este esquema es que cada director tendrían un canal de comunicación dedicado, lo que resultaría en un mejor tiempo de respuesta, y por otro lado se tendría un canal de comunicación dedicado para cada grupo de usuarios.

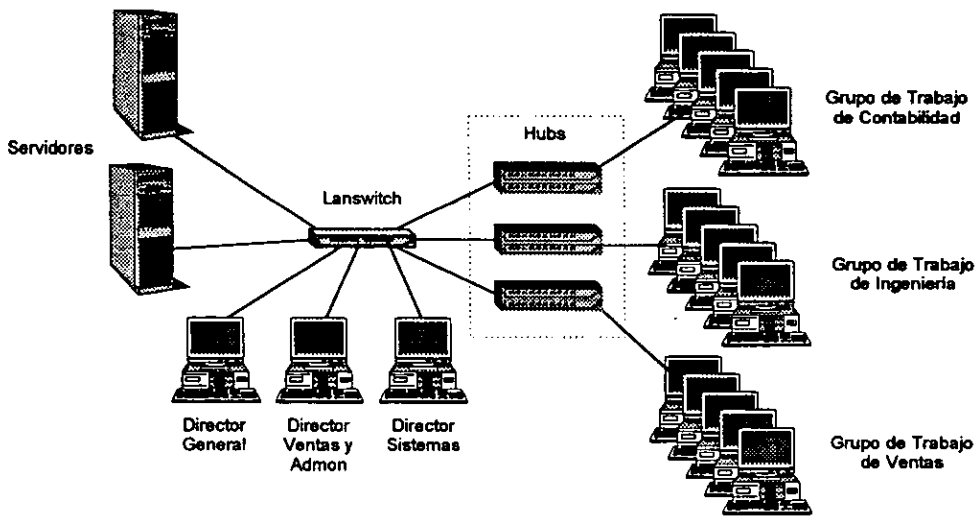


Fig. 6.5 LAN ethernet implementada con lanswitch

Una gran ventaja de esta tecnología es que posee una buena variedad de interfaces para con prácticamente todas las arquitecturas de LAN, principalmente con respecto a las de alta velocidad como: fast ethernet, FDDI, ATM y 100VG. El solo hecho de contar con un lanswitch garantiza un incremento en el desempeño de una LAN, y si adicionalmente esta misma tecnología permite tener combinación de arquitecturas, el desempeño de cualquier LAN se verá ampliamente favorecido, sobre todo con la opción de alta velocidad.

En el esquema anterior (figura 6.5) se puede detectar un cuello de botella en los servidores; siendo estos el único punto en común de toda la LAN; este problema se podría evitar si los servidores tuvieran tarjetas de red de alta velocidad; esto con la finalidad de que ya que estos atienden los requerimientos de todos los usuarios conectados en LAN, tuvieran un excelente tiempo de repuesta. En la figura 6.6 se muestra esta modificación.

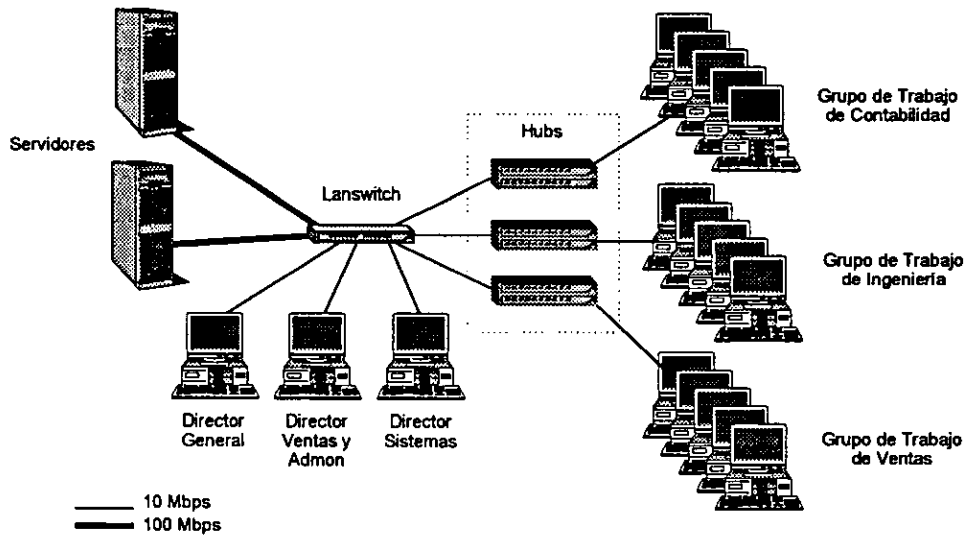


Fig. 6.6 Lanswitch con puertos a 10 Mbps y 100 Mbps.

Los esquemas anteriores muestran solamente un lanswitch, pero ¿qué pasa cuando se tiene un edificio con varias redes locales interconectadas entre sí y se desea incrementar el desempeño de la LAN en su conjunto?

En la figura 6.7 se presenta un caso típico de uso de lanswitches en un edificio que tiene varias redes locales y diferentes arquitecturas de red. En este caso se pueden observar la forma en que se puede solucionar el hecho de contar con diferentes arquitecturas interconectadas entre sí, haciendo uso de un cableado estructurado. En este esquema existe un equipo en común, que dependiendo de sus características podría en un momento dado convertirse en "cuello de botella". Este equipo es el lanswitch al que se comunican todos los pisos. Un equipo que haga esta función deberá tener un backplane de alta velocidad, lo que implicaría que tendría un sistema de comunicación de alta velocidad entre todas las tarjetas que maneja, donde típicamente esta velocidad superaría 1 Gbps. A este concepto se le denomina Back Bone Colapsado, es decir, el medio de comunicación entre pisos se realiza dentro de un dispositivo. Anteriormente este tipo de conceptos solo se encontraba en routers muy grandes; sin embargo, al día de hoy se encuentra en dispositivos como lanswitches.

Por otro lado el back bone colapsado no solamente se utiliza como punto de comunicación entre diferentes pisos, sino también en el caso que se tengan diferentes arquitecturas en un mismo local, o piso, como sucede en el piso 3 de la figura 6.7. Lo que permite que la comunicación entre estas distintas arquitecturas se lleve a cabo de una manera más eficiente, ya que por un lado segmenta el tráfico entre las mismas, y por otro, las comunica a grandes velocidades.

En este mismo esquema se puede apreciar que la comunicación que se lleva entre los pisos del edificio se resuelve con un mismo dispositivo; sin embargo, también es factible resolver la comunicación a otros edificios que se encuentren dentro de un mismo complejo de oficinas. En la figura 6.7 se presenta el esquema anteriormente comentado.

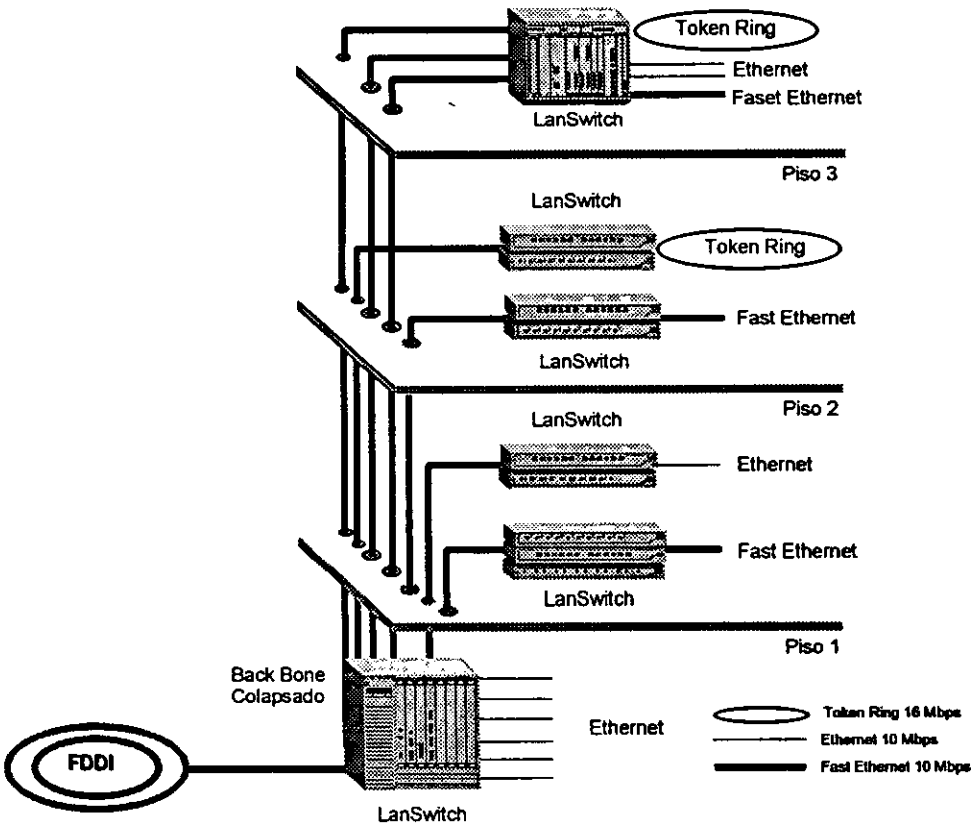


Fig. 6.7 Lanswitches interconectando diversas LANs

6.5 Diferencias entre lanswitches y bridges locales.

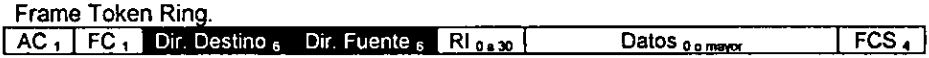
La diferencia entre bridges y lanswitches es realmente mínima; de hecho no es sencillo explicar tan sutil diferencia, ya que incluso sus funciones son iguales. En realidad se puede encontrar una diferencia, que es la que hace que los bridges empiecen a desaparecer del mercado: esta diferencia es la velocidad en cuanto a la decisión de direccionamiento de los frames.

Los lanswiches son más rápidos que los bridges, ya que los lanswitches, al contrario de los bridges, no requieren capturar todo el frame para conocer la dirección destino, haciendo que la tarea de decisión se lleve menos tiempo.

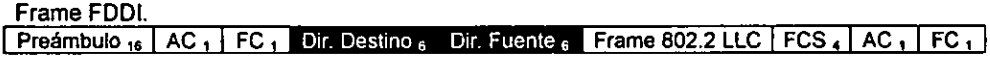
Es importante mencionar que los frames, sin importar la arquitectura de que se trate siempre tienen formatos muy parecidos. A continuación se muestra el formato de diferentes frames, con la finalidad de mostrar la ubicación de las direcciones fuente y destino.

Frame Ethernet.

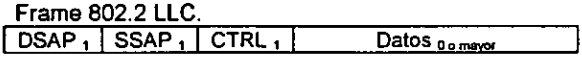
Frame Token Ring.



Frame FDDI.



Frame 802.2 LLC.



AC. Access Control
CTRL. Control.
DSAP. Destintion Service Access Point.
FC. Frame Control.
FCS. Frame Check Sequence
RI. Routing Information.
SSAP. Source Service Access Point.
El número en cada campo indica el tamaño en bytes.

Como se puede apreciar, existe una gran diferencia entre leer todo un frame para tomar una decisión, o solo leer las direcciones destino y origen para hacerlo.

6.6 Información necesaria para mejorar el desempeño de una LAN.

Se sabe que con solo colocar lanswitches se mejora el desempeño de una LAN, pero existe una gran interrogante que se debe resolver, ¿cómo formar los grupos de trabajo? Estos se pueden implementar de muchas formas, entre algunas de ellas: por función, tráfico generado, aplicaciones que accesan, horario de trabajo, jerarquía, etc.

En realidad cualquiera de estas premisas para formar los grupos de trabajo garantizaría tener un mejor desempeño en la LAN, pero el problema es determinar cual es la mejor selección para formar estos grupos de trabajo. No existe una regla general para todos los casos, dada la enorme cantidad de variantes por cada caso; sin embargo sí se puede decir que la mejor forma de diseñar será basándose en el tráfico generado por cada usuario. Esto es sumamente complicado, ya que requiere de una gran cantidad de herramientas de administración y monitoreo que permitan conocer el tráfico generado por cada usuario en un ciclo de trabajo (normalmente un mes).

En general, para mejorar el desempeño de una LAN es necesario conocer cierta información; sin la misma, cualquier medida que se tome no necesariamente resolverá el problema. En los párrafos posteriores se lista la información requerida para mejorar el desempeño de una red.

Diagrama de la red a detalle que indique:

- Tipo de cable.
- Longitud de cada segmento de cable.

- Estaciones de trabajo.
- Servidores.
- Periféricos.
- Hubs.
- Bridges.
- Lanswitches.
- Routers.
- Gateways.

Por cada dispositivo se deberá contar con su configuración correspondiente en cuanto a hardware y software.

Adicionalmente se deberá contar con la siguiente información:

- Grupos de trabajo de usuarios.
- Aplicaciones y/o servicios a que accesa cada grupo de trabajo o usuario.
- Ubicación de los servicios y/o aplicaciones (servidores).
- Frecuencia de uso de las aplicaciones y/o servicios.
- Determinar la importancia de cada aplicación y/o servicio en el desempeño de la labor de cada grupo de trabajo o usuario.
- Usuarios remotos y locales.

Si se tienen usuarios remotos accesando la LAN, se deberá conocer:

- Localidades remotas.
- Ancho de banda por cada enlace.
- Medio utilizado.
- Protocolos de ruteo y ruteables utilizados (se explica en el siguiente capítulo).
- Diagrama de comunicación.

La parte más importante, la cual haría la diferencia entre mejorar el desempeño de un LAN e implementar el mejor desempeño de una LAN, se basa en el conocimiento del tráfico que cada usuario genera. Por lo que se deberá de

contar con las herramientas pertinentes para llevar a cabo estas mediciones. Estas herramientas podrán detectar entre otras cosas:

- Usuarios más demandantes.
- Fallas en cable.
- Horas pico.
- Errores en los frames.
- Tráfico en red.

Con toda esta información se determinan los grupos de trabajo que conformarán la LAN. Estos grupos de trabajo deberán garantizar un tiempo de respuesta de acuerdo a las necesidades que se tengan. En algunos casos muy críticos se deberá considerar conectar diversos equipos en forma directa a un puerto del lanswitch, como en el caso de vídeo o multimedia, por ejemplo.

La idea básica es agrupar a los usuarios de acuerdo a:

- Aplicaciones comunes utilizadas.
- Servicios comunes utilizados.
- Baja utilización del canal de transmisión.

Lo anterior deberá garantizar que los grupos de usuarios creados tengan tiempos de respuesta de acuerdo a sus necesidades.

Difícilmente en el primer intento de rediseño de una LAN se obtendrá el mejor desempeño posible; de hecho se deberá dejar que los sistemas se estabilicen durante un tiempo razonable, que bien podría variar de tres a cinco meses, y realizar un nuevo monitoreo, para realizar los ajustes correspondientes. Con el tiempo se podrán realizar ciertos cambios sin necesidad de llevar a cabo todos los procesos de monitoreo, ya que la experiencia ayudará en gran medida.

Es común que exista movimiento de personal en los corporativos, lo que implica cambiar usuarios de un grupo de trabajo a otro, lo que a su vez hace necesario interactuar con el cableado. Al día de hoy existen diversos fabricantes que ofrecen productos que permiten hacer cambios virtuales entre grupos de trabajo. Para mayor información al respecto consultar el capítulo 10.

CAPÍTULO 7
Diseño de MAN o WAN ¿Cuándo se Utilizan Bridges, Routers o Gateways?

Temas del capítulo:

7.1 Introducción a bridges remotos.

7.2 Introducción a routers.

7.3 Introducción a gateways.

7.4 Diferencias entre bridges, routers y gateways.

7.5 Información necesaria para diseñar una MAN o una WAN.

Lo más común es que en una corporación, al empezar a tener auge las instalaciones de las LANs, se empiece a tener la necesidad de interconectarlas entre sí; esto por supuesto es un proceso natural de crecimiento y aunque prácticamente solo se aplica a los grandes corporativos, no quiere decir que no pueda ser implementado para corporativos medianos con grandes necesidades de comunicación entre equipos de cómputo.

Si las LANs se encuentran distribuidas en una misma ciudad, el enlace entre ellas se denomina MAN (Metropolitan Area Network), y si las LANs se encuentran en ciudades diferentes, o se requiere enlazar MANs se denomina WAN (Wide Area Network). Como se podrá ver, esto parece ser solo cuestión de cobertura geográfica; sin embargo al hablar de MAN o WAN, también se está hablando de un mismo ambiente de cómputo; es decir, un mismo protocolo y/o un mismo sistema operativo de LAN. Para el caso de que se desee realizar la interoperabilidad entre ambientes de sistemas diversos, a la red se le denomina

GAN (Global Area Network), concepto que engloba el máximo nivel de interoperabilidad que puede existir en un sistema de cómputo; es decir, hacer convivir protocolos, sistemas operativos y hasta fabricantes diversos, todos operando entre sí bajo un mismo esquema, como una sola máquina. Por facilidad (o desconocimiento) se ha adoptado el término de WAN, como el de mayor alcance; incluso el término de GAN no es conocido. En esta tesis se adoptará la terminología general (WAN en lugar de GAN); sin embargo, sí es adecuado saber que existe algo más.

Por supuesto, la idea de cualquier corporativo es contar con una WAN; sin embargo, para realizar esto, primero es necesario poseer una plataforma de LAN y MAN con orientación a los sistemas abiertos; por tal motivo, en este capítulo se plantearán las mejores opciones que existen actualmente para implementar una plataforma de MAN y WAN.

En primer lugar se expondrán conceptos previos para proporcionar un mejor panorama sobre estos tópicos.

Básicamente se tiene tres tipos de comunicación.

- Comunicación en tiempo real.
- Comunicación store and forward (guardar y enviar).
- Comunicación en batch.

Estos tipos de comunicación dependen directamente del tiempo y de la facilidad de interactuar o no con los sistemas remotos.

El primer tipo es la comunicación que se realiza inmediatamente y se encuentra establecida, normalmente, todo el tiempo; en ella se pueden consultar bases de datos, acceder archivos o ejecutar paquetería en forma interactiva.

El segundo tipo es la que se utiliza por ejemplo en el correo electrónico. La forma de operar de esta comunicación, consiste en intercambiar información entre dos o más entidades de la misma forma en que se realiza con el correo que todos

conocemos, pero este se efectúa en forma electrónica desde una computadora. Este tipo de comunicación garantiza el envío y recepción de información o mensajes en forma correcta y en el menor tiempo posible; sin embargo nunca podremos tener una comunicación "en vivo" con nuestro destinatario, como en el caso de la comunicación en tiempo real.

En el caso de la comunicación en batch se debe cumplir una condición, por ejemplo el tiempo, que sirva de disparador para que se ejecute una acción definida previamente; este disparador puede ser totalmente automático, o que el personal sea el encargado de ejecutar la acción al momento de que se cumpla la condición.

En el ámbito de las redes, la comunicación más utilizada es en tiempo real; sin embargo, esto no quiere decir que los otros dos tipos de comunicación no se utilicen. De hecho los tres tipos de comunicación se llevan a cabo; sin embargo al crear una plataforma de WAN, se deberá estar pensado en una comunicación en tiempo real, ya que esta representa el máximo nivel de comunicación.

Si se resuelve el problema de contar con una comunicación en tiempo real, se podrán realizar los otro tipos de comunicación, por lo que será la comunicación en tiempo real el problema a resolver con los dispositivos que se discutan.

Entre los problemas más comunes que enfrentamos para interconectar LANs, al formar una MAN o crear una WAN se pueden mencionar los siguientes:

- Numerosas topologías y algunas veces híbridas.
- Diversidad de protocolos. Incluyendo protocolos no ruteables.
- Variedad en tipos de interfaz.
- Diferentes medios de transmisión.
- Necesidad de flexibilidad en crecimiento.
- Baja velocidad de transmisión disponible baja. Menor o igual a 64 Kbps.

La idea fundamental que se debe perseguir al realizar un proyecto de enlace de redes es poder accesar toda la información que se desee, así como compartir todos los servicios disponibles, sin importar donde se encuentren estos; debiendo ser la plataforma de comunicaciones totalmente transparente para el usuario. Se sabe finalmente que no todos los usuarios utilizarán la totalidad de los servicios, sin embargo debido a que finalmente esto es una posibilidad, y desde luego el peor caso, deberá estar considerada la conectividad total. Con las tecnologías actuales el usuario ya no deberá conocer la ubicación física y lógica de los recursos que se deseen accesar; por lo que lo único que deberá tener es los derechos para efectuarlo. Se debe estar consciente como usuario, que la velocidad de acceso y ejecución de archivos o paquetería será menor que la velocidad de respuesta a la que se encuentra acostumbrado; ya que, al día de hoy, los anchos de banda de las comunicaciones remotas son menores a los anchos de banda de las comunicaciones locales. Normalmente se habla de Megabits por segundo versus decenas de Kilobits por segundo.

Para realizar comunicaciones entre dos o más redes locales remotas existen básicamente dos elementos, bridges y routers (en este caso quedan excluidos los repetidores y lanswitches debido a que su solución es local, no permitiendo conectividad remota). Para el caso de ambientes diferentes se utiliza un gateway. Estos conceptos se discutirán a continuación.

7.1 Introducción a bridges remotos.

Los bridges presentan un grado de "inteligencia" mayor que los repetidores; sin embargo no utilizan protocolos de red adicionales para el transporte de un paquete de información de una LAN a otra, debido a que los

bridges trabajan en forma independiente a protocolos de alto nivel, como podrían ser IPX, TCP/IP, etc.

Para que los bridges interconectados entre sí puedan tener redundancia a fallas, utilizan un protocolo llamado Spanning Tree Protocol (STP), mismo que permite que uno de los bridges funcione como enlace principal y el otro como de respaldo.

Existen bridges locales y remotos. Los bridges locales se utilizan para mejorar el desempeño de una LAN, y los bridges remotos se pueden utilizar para crear MANs y WANs.

Para conexiones remotas los bridges se conectan, por medio de líneas telefónicas analógicas y digitales, aunque es importante tener cuidado de no utilizar enlaces ISDN, ya que en México este tipo de comunicación no existe. Como características generales, dependiendo de la marca, manejan: Ethernet, Token Ring, RS-232, V.35, RS-449 y actúan en las dos primeras capas del modelo OSI. Ver figura 7.1.

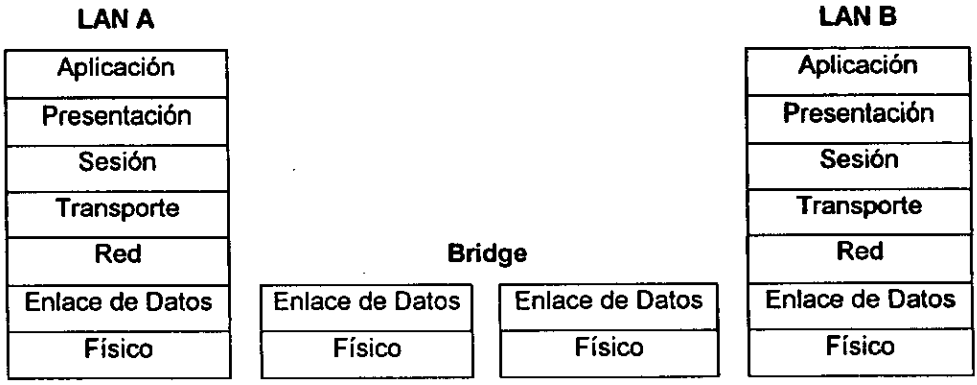


Fig. 7.1 Representación de un bridge en el modelo OSI.

Ventajas de los bridges.

- Fáciles de instalar, no requieren configuraciones complicadas y su presencia es transparente para los usuarios. Todos los bridges salen de fábrica con una configuración universal de operación, permitiendo con esto instalar y conectar (plug and play) inmediatamente, con excepción de la velocidad, ya que no poseen reloj interno. La señal de reloj en un enlace remoto la debe de proveer otro dispositivo.
- Debido a que son independientes de los protocolos superiores permiten conectar LANs con ambientes operativos diferentes.
- Son una verdadera solución para mejorar el rendimiento de LANs a un precio relativamente bajo.

Desventajas de los bridges.

- Los bridges no pueden tomar ventaja de tener múltiples rutas lógicas entre diversos puntos, ya que solo utilizan una de ellas.
- En casos de que se tengan diversos bridges interconectados en forma redundante pueden presentarse graves problemas de retraso de tiempo de respuesta.
- En esquemas de conexión con configuraciones implementadas indebidamente es posible que se genere gran cantidad tráfico; a este problema se le llama "storm broadcast". Este problema se puede generar si un puerto de algún bridge se daña, problema nada fácil de detectar y corregir.

7.2 Introducción a routers.

Los routers (en español, ruteadores) son equipos con mayor "inteligencia" que los repetidores, bridges y lanswitches, pero también son más difíciles de configurar así como de dejarlos funcionando en forma óptima; sin embargo el servicio que proporcionan es mucho más flexible. Los ruteadores están hechos para tener gran flexibilidad de comunicación y tener diferentes protocolos funcionando. Enlazando LANs tanto remotas como locales, permite hacer balanceo de cargas de trabajo, algo que no permiten los bridges. Sin embargo como características generales, soportan, dependiendo de la marca: token ring, ethernet, FDDI, TCP/IP, X.25, frame relay, XNS, IPX/SPX, SNMP, RS-232, V.35, RS-422, velocidades de 9,600 a 2.048 Mbps en diferentes medios (satélite, microondas, fibra óptica etc.) y por si fuese poco, pueden manejar varios protocolos, velocidades e interfaces funcionando simultáneamente.

Los routers pueden, seleccionar la méjor ruta entre dos puntos, en base a costo de línea, velocidad de línea, tráfico en línea, etc. Como se puede ver es un producto que pudiese considerarse muy sofisticado. Su funcionamiento abarca los tres primeros niveles de modelo OSI. Ver figura 7.2

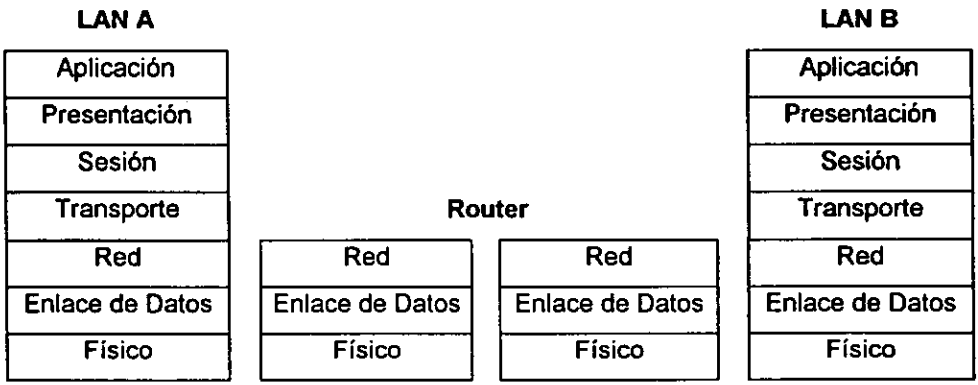


Fig. 7.2 Representación de un router en el modelo OSI.

Protocolos de ruteo.

Los ruteadores para conocer la ruta entre un origen y un destino cuentan con información que se comunican entre sí. Esta información se transmite mediante protocolos denominados protocolos de ruteo. Los ruteadores en general poseen básicamente dos protocolos de ruteo para encontrar la mejor ruta entre dos dispositivos; estos protocolos son RIP y OSPF mismos que están implementados como software en los routers. Existe un fabricante que posee un protocolo propietario denominado IGRP; dicho fabricante es Cisco Systems. IGRP es considerado uno de los mejores en el medio; sin embargo solo se incluye en los productos de Cisco. Existen otros protocolos de ruteo; sin embargo son muy poco utilizados dentro de un mismo corporativo; estos son: EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) y OSI Routing.

Por su importancia y difusión para los protocolos de ruteo en un corporativo se abordarán solo los tres principales; RIP, OSPF e IGRP.

- Routing Information Protocol (RIP).

RIP es un protocolo de ruteo desarrollado para el protocolo XNS (de Xerox) y utilizado también por protocolos como IPX y TCP/IP.

Este protocolo funciona propagando cada router las direcciones que posee en cada uno de sus puertos a través de los demás routers conectados, permitiendo con esto que todos los routers conectados entre sí, conozcan la ruta para llegar a algún servidor o dispositivo, es decir envían mensajes de broadcast para mantener actualizadas las rutas entre equipos.

Este método funciona adecuadamente en interconexiones de LANs relativamente pequeñas o medianas (5 a 10 routers); sin embargo en plataformas más grandes difícilmente RIP provee un sistema estable de comunicación, debido

a que cada 30 segundo todos los routers intercambian información de sus rutas (tablas de direcciones), por lo que se genera un tráfico intenso entre ruteadores, provocando un overhead cuando los usuarios de la plataforma desea utilizar los canales de comunicación.

RIP permite como máximo 16 ruteadores en cascada, es decir un mensaje no puede atravesar mas de 16 ruteadores para llegar a su destino.

RIP es un protocolo de vector de distancia; esto significa que utiliza un algoritmo que hace que el router decida únicamente basándose en el número de ruteadores que debe pasar para que un paquete llegue a su destino. RIP no considera ninguna otra característica, como congestión, velocidad de la línea, costo, etc., al momento de elegir la ruta.

- Open Shortes Path First (OSPF).

Este protocolo de ruteo lo que hace es encontrar la ruta lógica más corta entre dos equipos a comunicarse; es decir, entre una nube de comunicaciones con routers y enlaces redundantes se tienen varios caminos para enlazar dos equipos, y OSPF permite encontrar la ruta de comunicación entre equipos donde exista la menor cantidad de routers tomando en cuenta el costo de la línea. El costo de la línea es un valor arbitrario que se configura; sin embargo se recomienda que para asignar este costo se tomen en cuenta, el ancho de banda, el costo de la línea, tipo de enlace, o cualquier otro criterio que se considere pertinente. A diferencia de RIP, OSPF actualiza tablas de direcciones cada 30 minutos, y en caso de que exista alguna alteración en las rutas antes de ese cambio masivo de direcciones, actualiza solo la ruta que se modificó.

Este protocolo se recomienda cuando se tiene TCP/IP (IPX no funciona) y se requiere conectar una gran cantidad de lugares; por ejemplo, diez o más

routers interconectados, o en su defecto cuando se tenga una menor cantidad de routers pero se desee tener optimizado el tráfico en la WAN.

- Interior Gateway Routing Protocol. (IGRP).

Este protocolo fue desarrollado por Cisco Systems en la mitad de los años 80s. A diferencia de OSPF y RIP, la tabla de direcciones de IGRP se actualiza cada 90 segundos. Tiene la gran ventaja de poder utilizar múltiples rutas para hacer llegar una comunicación. Se considera que es una de las mejores opciones que existen en cuanto a protocolos de ruteo; sin embargo se debe tener en cuenta que es una implementación propietaria.

El desempeño que tienen los ruteadores de Cisco con sus propios protocolos es superior comparado al que tiene cuando se utiliza OSPF o RIP.

En este caso, aunque IGRP es propietario, es el mismo caso que con IPX o Netbeui, que son protocolos desarrollados por Novell y Microsoft respectivamente, no queriendo con esto afirmar que por el hecho de ser propietario es malo.

IGRP utiliza una combinación de factores para decidir la mejor ruta. Estos factores son; tiempo de retardo de la interred, ancho de banda, confiabilidad y carga de las rutas factibles de ser utilizadas. Se le puede asignar el peso a estas variables de acuerdo a un criterio definido expresamente para el ambiente bajo el que funcionarán los ruteadores, o en su defecto utilizar los valores de dafault que posee este protocolo.

Para la asignación del peso se tienen diferentes rangos dependiendo del factor; por ejemplo: para confiabilidad y carga se tiene un rango de 1 a 255, para ancho de banda se toman rangos de 1,200 bps a 10 Gbps, y el tiempo de retardo se pueden tomar valores de 1 a 24.

IGRP permite utilizar dos líneas con un mismo ancho de banda, viendo ambas líneas como una sola.

Tanto OSPF como IGRP solo pueden manejar IP, lo que hace que ambientes con Netware tengan que cambiar su protocolo IPX a IP. Existe una variante de IGRP denominada Enhance IGRP, misma que sí tiene la capacidad de utilizar IPX al igual que IP.

Ventajas de los routers para interconectar redes locales.

- Debido a la gran cantidad de opciones que presentan para su configuración, permiten un diseño de acuerdo a las diversas necesidades que se tengan, haciendo que sean equipos muy versátiles.
- Una vez instalados son equipos realmente sencillos de operar y mantener, especialmente cuando se tiene la opción de protocolos fáciles de actualizar.
- Con los routers sí se aprovecha el tener diversas rutas entre equipos, elevando con esto el nivel de aprovechamiento de los recursos y esto permite mayor velocidad en la comunicación entre equipos.
- Cuando un bridge o el segmento de la red donde se encuentra algún bridge falla, el tiempo de reconfiguración de los bridges involucrados en el sistema es mucho mayor que cuando un router o su sistema falla, ya que los routers están diseñados para tomar decisiones en forma autónoma; en cambio los bridges tienen que esperar que el que se denomina "root" reasigne las nuevas direcciones.

Desventajas de los routers para interconectar redes locales.

- Pueden requerir en un momento dado mucho tiempo para su configuración, debido a que la misma no es sencilla, por la gran cantidad de opciones que presenta.
- Al contrario que los bridges, los routers son dependientes de los protocolos de nivel superior, como de IPX, IP, X.25, etc. lo que complica la configuración. Por cada protocolo que se utilice se debe realizar un diseño. Esto dificulta tanto la puesta en marcha como su operación.
- Debido a que los routers son equipos más complejos que los bridges, son más caros. La diferencia en precios entre un dispositivo que solo tenga funciones de bridge versus el router más sencillo es de un 100%. Aunque al día de hoy es difícil encontrar dispositivos que solo tengan la funcionalidad de bridges, en general los routers tienen opción de ser configurados como bridges.

7.3 Introducción a gateways.

Entender el concepto de gateway es relativamente sencillo, lo realmente difícil es implementar, evaluar, administrar y soportar un sistema de este tipo. Un gateway es un sistema que permite comunicar ambientes operativos diferentes, facilitando con esto la integración de plataformas diversas en una misma compañía. Un ejemplo clásico de esto es encontrarse en un mismo escritorio terminales conectadas a diferentes equipos y adicionalmente una PC, ¿porqué no mejor utilizar las características superiores de una PC? ya que esta realiza funciones diversas, como emulación de terminal, transferencia de archivos, procesos cooperativos o procesos distribuidos.

En palabras llanas, un gateway es un traductor de idiomas (protocolos), que permite que dos personas (ambientes operativos) se comuniquen entre sí; esto por supuesto hace que un gateway sea el más inteligente de los equipos de comunicación y por lo tanto también es el más lento de ellos, pero a su vez realiza funciones más complicadas.

Los gateway, estrictamente operan en los siete niveles de OSI, sin embargo los niveles en que trabajan dependen del grado de conectividad que se desee, y la compatibilidad entre los ambientes a intercomunicar. La figura 7.3 muestra el esquema comentado.

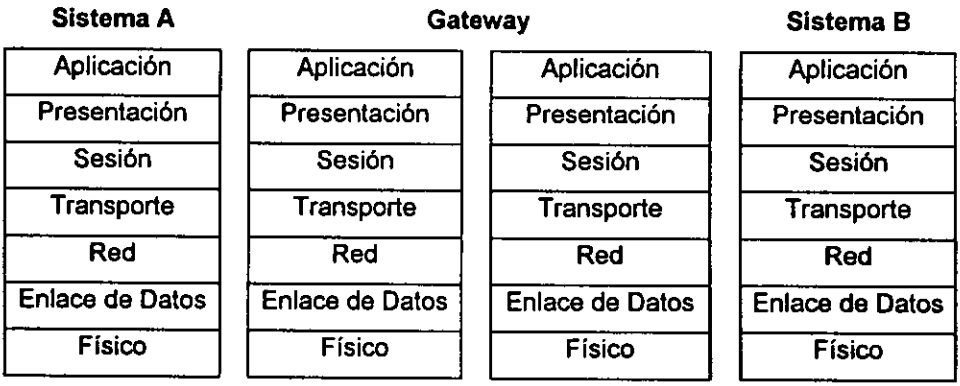


Fig. 7.3 Representación de un gateway en el modelo OSI.

7.4 Diferencias entre bridges, routers y gateways.

Debido a que tanto gateways, routers y bridges permiten interconectar equipos, es adecuado marcar perfectamente las diferencias entre ellos, así como la aplicación que se le debe de dar a cada uno.

Debido a que las características que presentan y la labor que desempeñan los bridges, routers y gateways son diferentes; incluso funcionan en diferentes

niveles del modelo OSI; debido a esto se debe hacer una agrupación en dos grandes rubros:

- Aquellos equipos que comunican ambientes similares sin llegar a proporcionar servicios de comunicación elevados.
- Aquellos equipos que permitan que ambientes diferentes interactúen entre sí.

Al primer rubro corresponderían los bridges y routers y al segundo los gateways. Esta división se hace para poder realizar una comparación de equipos similares y con características comparables, ya que debido a su función no es posible comparar un gateway contra un bridge o un router; sin embargo, sí es posible realizar una comparación entre un bridge y un router.

Diferencias entre bridges y routers.

- Detección y corrección de errores. Los bridges al actuar sobre la segunda capa de OSI presentan un nivel de corrección menor al de los routers. Sabemos que en cualquier tipo de enlace siempre existirán errores, por lo que es adecuado tener en mente que los routers presentan un mayor grado de confiabilidad en este rubro, aunque también son más lentos.
- Tolerancia a fallas. La mayoría de los bridges no presentan tolerancia a fallas en contraste con los routers que sí presentan cierto nivel de tolerancia a fallas. Sabemos que las comunicaciones en las líneas telefónicas, microondas, vía satélite o cualquier otra no están exentas de fallas, por lo que tener recuperación automática de enlaces después de una "caída" es muy importante, y los pocos modelos de bridges que tienen esta opción, son más lentos que los routers.

- Tiempos de retardo. Dado que los bridges tienen una tecnología menos sofisticada presentan tiempos de retardo menores que los routers al enviar paquetes de información. Esto se debe a que si se manda un archivo de una LAN a otra mediante routers estos toman el frame empaquetado en el protocolo que se está usando, lo empaquetan en otro protocolo (en caso de ser necesario), eligen una ruta de acuerdo a los parámetros de configuración y lo envían al router destino donde se realiza la operación contraria dejando el frame en su protocolo original o en el mismo dependiendo de si se llega a un sistema similar o uno diferente. Lo que un bridge haría en el mismo caso sería tomar el frame ver a donde va y enviarlo a otro bridge que lo toma, haciendo que las tareas que realiza un bridge sean menos complejas y por lo tanto es más rápido.
- Tamaño de frame. Los routers fragmentan los frames para acoplarlos al tamaño usado por el protocolo de comunicación. Al llegar al router destino reensamblan el frame para que llegue en su forma original o lo pueden dejar con ese nuevo tamaño o a otro dependiendo del protocolo que exista en el otro extremo. Los bridges no necesariamente necesitan fragmentar los frames y operan más eficientemente cuando no es necesario realizar esta operación dado que trabajan con el protocolo original de las LAN emisora y destino.
- Seguridad de acceso. Los routers presentan un nivel de seguridad de acceso a la WAN mayor que los bridges.
- Costo. Los routers son un poco más caros que los bridges.
- Balanceo de cargas. Esto se refiere a que si se está conectado a dos puntos por diferentes vías, ambas vías puedan utilizarse simultáneamente. Esto para el caso de bridges no es posible, ya que aunque pueden disponer de varias rutas, solo una de ellas se encuentra activa, y hasta que no deja de funcionar

esta vía de comunicación, la otra vía no empieza a funcionar. En el caso de los routers, estos sí pueden hacer uso simultáneo de ambas vías, o más.

Aplicaciones para bridges y routers

Tratando de resumir un poco sobre todo lo anterior diremos que:

Los bridges remotos tienen una mejor aplicación, en comparación con los routers, cuando:

- El ambiente de operación es pequeño, no mayor a dos lugares a conectar.
- El ambiente operativo sea el mismo.
- Las redes en cada uno de los puntos a conectar no sean mayores a cinco usuarios.
- El tráfico sea muy bajo.
- No se tenga enlace corporativo a Internet.
- No se tengan usuarios remotos con acceso dial up.

El porqué de esto se debe básicamente a dos puntos:

1. Presentan una posibilidad de interconexión relativamente barata de dos puertos.
2. Ofrecen un método más o menos sencillo de ampliar la extensión de una LAN, así como de controlar tráfico, acceso y fallas.

Los routers presentan un mejor uso cuando el ambiente de operación es muy grande en cuanto a distribución, variedad de equipos, protocolos, sistemas operativos, etc. A continuación se expondrán los puntos que apoyan lo anteriormente descrito:

- Permiten múltiples protocolos simultáneos por un mismo puerto.
- Cambian de ruta cuando existe una falla en la ruta principal.

- Permiten topología redundante en los enlaces, con la finalidad de que los enlaces sean inteligentes y no necesariamente punto a punto.
- Permiten tener un crecimiento a futuro sin grandes cambios ni inversiones.
- Existen varios modelos que integran hubs o modem en espera de llamada.

Algo que se tiene que tomar en cuenta, es que todos los routers incluyen opciones para funcionar como bridges, por lo que puede ser que se configuren en un inicio de una forma, y posteriormente al crecer las necesidades, se cambie su configuración y operen como routers. Esto proporciona una gran flexibilidad y seguridad en la inversión. Lo que se debe tener en cuenta es que los cambios implican un gran esfuerzo, y es mejor desde un inicio hacer un buen diseño que, en caso de crecimientos, implique cambios mínimos.

Por otro lado, en el caso de los gateways existe una gran cantidad de ellos; prácticamente tantos como ambientes diferentes combinados contra ambientes diferentes, por poner solo una muestra, se tienen gateways para:

LAN con Netware a AS/400 de IBM.

LAN con Netware a VAX de DEC.

LAN con Netware a HP-9000 de Hewlett Packard.

LAN con Netware a RS6000 de IBM.

LAN con Netware a 3090 de IBM.

LAN con Netware a A17 de Unisys.

LAN con Windows NT a AS/400 de IBM.

LAN con Windows NT a VAX de DEC.

LAN con Windows NT a HP-9000 de Hewlett Packard.

LAN con Windows NT a RS6000 de IBM.

LAN con Windows NT a 3090 de IBM.

Por supuesto, esto es solo una pequeñísima muestra de la cantidad de ambientes combinados que puede existir, cuya solución se lleva a cabo mediante un gateway.

En la figura 7.4 se muestra un esquema donde se presentan los bridges, routers y gateways mediante el modelo OSI de ISO.

MODELO *OSI* DE *ISO*

Modelo OSI	Equipo de Interconexión			Modelo OSI
LAN o Ambiente A	Bridge	Router	Gateway	LAN o Ambiente B
Aplicación				Aplicación
Presentación				Presentación
Sesión				Sesión
Transporte				Transporte
Red				Red
Enlace de Datos				Enlace de Datos
Físico				Físico

Fig. 7.4 Comparativo de bridges, routers y gateways en el modelo OSI.

7.5 Información necesaria para diseñar una MAN o una WAN.

Para poder implementar una plataforma de "red de redes", es decir, una MAN o una WAN se requiere contar con información que permita realizar un buen análisis y así determinar perfectamente los equipos o la combinación de ellos que se necesiten. Por supuesto, es necesario conocer el objetivo del proyecto, así como las necesidades que se desea cubrir, y también es necesario realizar preguntas adicionales como podrían ser:

1. ¿Equipos y recursos con que se cuenta?

2. ¿Cuál es el tamaño promedio de los paquetes de información que se desea transmitir sobre la plataforma?
3. ¿Qué porcentaje de los paquetes son pequeños, medianos o grandes?
4. ¿Número de usuarios que utilizarán cada uno de los enlaces?
5. ¿Recursos disponibles para realizar los enlaces?
6. ¿Capacidad de los equipos existentes para soportar el número de usuarios que los accederán simultáneamente?
7. ¿Cuál es el protocolo predominante en los ambientes a enlazar?
8. ¿Aplicaciones de gran importancia?
9. ¿Qué protocolos soportan los multiplexores y switches?
10. ¿Sobre las líneas se transmite voz y datos?
11. ¿Los equipos poseen compresión de datos?

Además de las respuestas a las interrogantes anteriores es necesario conocer:

- Infraestructura de comunicaciones.
- Ambientes a comunicar.
- Plataforma de LANs existente.
- Requerimientos en volumen de información.
- Crecimientos.

A continuación se describen los rubros de cada uno de estos incisos:

Infraestructura de comunicaciones.

Se requiere conocer la infraestructura de comunicaciones con que se cuenta para así saber las ventajas o limitaciones que se pueden tener.

Entre los puntos a conocer están:

- Velocidad del canal de comunicaciones.
- Full duplex o half duplex.
- Canal de comunicaciones dedicado o no dedicado.
- Radiofrecuencia, líneas telefónicas analógicas, microondas, satélite o RDI.
- Características del CSU/DSU a utilizar.
- Interfaz disponible para realizar los enlaces.
- Ubicación geográfica en donde se debe o puede accesar a la plataforma de comunicaciones.

Ambientes a comunicar.

En el caso de que existieran minicomputadoras o mainframes conectados a la plataforma se requiere conocer:

- Marca, modelo, configuración y ubicación de los equipos.
- Sistema operativo que utilice y versión.
- Protocolo(s) que utilice actualmente.
- Protocolo(s) que pueda utilizar adicionalmente al que se utiliza normalmente.
- Aplicaciones que se utilicen actualmente.
- Lugares importantes que requieran redundancia en comunicación. En este punto se debe conocer adicionalmente al lugar, el ambiente que se desea tener respaldado. Este punto aplica a cualquier ambiente de cómputo, incluso LANs y PC stand alone.
- Direcciones que utilicen los equipos. Al tener diversos equipos, estos requieren de direcciones, como IP, que se deben conocer; así mismo,

se deberá conocer si existe alguna política para la asignación de las mismas.

- Nivel de comunicación que se desea tener hacia ese equipo, como puede ser emulación de terminal, transferencia de archivos, procesos distribuidos o procesos cooperativos.

Plataforma de LANs existente.

Normalmente al planear una plataforma de estas características, ya se cuenta con una base instalada de LANs; sobre ella es necesario conocer:

- Arquitectura(s).
- Topología(s).
- Sistema(s) operativo(s) de LAN (versión).
- Sistema(s) operativo(s) en los equipos conectados a las LANs (versión).
- Marca, modelo, configuración y ubicación de los equipos conectados a las LANs. Es importante conocer microprocesador y memoria de los equipos. No es necesario que se tenga la información a detalle de cada uno de los equipos, sino que se especifique en general y del grueso de los equipos y para el caso de equipos asignados a personal importante es necesario conocerlo a detalle.
- Aplicaciones que se utilicen, tanto desarrollos caseros como comerciales (indicar versiones). Es importante especificar los recursos que utilizan las aplicaciones, principalmente de memoria.
- En todos los casos al tener una LAN, esta posee una dirección y/o nombre, características que deben conocerse.

Requerimientos en volumen de información.

Cuando se planea implementar una plataforma de este tipo se requiere conocer la cantidad de información que se va a transportar de un lugar a otro; para esto se requiere:

- Tipo de operaciones que se desean realizar en forma remota y entre qué lugares y ambientes
- Número de usuarios concurrentes que harán uso de las comunicaciones y a qué lugares y ambientes.
- Volumen de información a transmitir entre los diferentes puntos.
- Horarios requeridos para realizar esta transferencia o consulta.

Crecimientos.

Debido a la magnitud del proyecto es necesario conocer algunos puntos importantes, como son:

- Necesidades futuras de conectividad a otro(s) ambiente(s).
- Crecimiento en número de equipos a conectar a la plataforma.
- Enlaces futuros a otras entidades geográficas.
- Ubicación geográfica de todos los lugares a enlazar.
- Ubicación del personal a cargo del proyecto.
- ¿Existe alguna plataforma que pueda ser cambiada?
- Experiencia del personal para llevar a cabo el proyecto, sobre todo por las posibles modificaciones que se requieran en los equipos existentes.
- Presupuesto destinado al proyecto.

Existen procedimientos que permitirán conocer algunos puntos, como son las herramientas de análisis y monitoreo de señales; sin embargo, si no se tiene la experiencia suficiente, realmente será difícil interpretar los datos que se obtengan por este tipo de medios; por otro lado, es recomendable hacer un análisis previo a la plataforma que se tenga con la finalidad de conocer su estado y así, al realizar el proyecto, saber si algún tipo de problemas ya se presentaba con anterioridad o es consecuencia de equipos nuevos en la plataforma.

Por supuesto, lo anterior es lo mínimo de información que se debe conocer para poder elegir adecuadamente la plataforma de equipos que permitan implementar una plataforma de MAN o WAN. Sin embargo entre más información se tenga será mejor.

CAPÍTULO 8
Como Determinar Servidores y Estaciones de Trabajo a Utilizar

Temas del capítulo

8.1 Características del servidor.

8.2 Características de las estaciones de trabajo.

Para llevar a cabo la implementación de una LAN se deben seleccionar diversos elementos. En capítulos anteriores se habló de arquitecturas, cableados y comunicaciones; sin embargo, esto realmente es solo una pequeña parte de los componentes que se deben tener en cuenta. No existe un componente más importante que otro; realmente todos son muy importantes, y la adecuada elección de cada uno de ellos permitirá que un proyecto de este tipo sea todo un éxito.

La adecuada selección de los servidores donde residirán las aplicaciones e información, permitirá que los tiempos de respuesta y de tráfico en los canales de comunicación hacia las estaciones de trabajo u otros servidores sean aceptables; esto incluye tiempos de lectura, escritura, búsqueda, envío de información, impresión, etc. Por tales motivos la buena elección tanto de servidores como de estaciones de trabajo permitirá que la LAN en su conjunto tenga un desempeño adecuado de las funciones que se le asignen.

8.1 Características del servidor.

Como se comentaba en el capítulo 2, sección 2.5 (componentes de las redes locales), existen diversos tipos de servidores. En este capítulo se hablará de como seleccionar un servidor de archivos y con qué características debe contar. Es adecuado recordar que un servidor de archivos posee mayor capacidad que una estación de trabajo; es decir, mayor velocidad, mayor capacidad en disco duro, más memoria y un microprocesador de mayor tamaño.

Para poder delimitar los requisitos para adquirir un servidor de archivos, es necesario conocer lo que un equipo de estos contiene normalmente. A continuación se enlistarán los diversos elementos que guarda un servidor de archivos:

- Sistema Operativo de LAN (Netware, Windows NT, Vines, etc.).
- Paquetería comercial (Windows, PC Tools, Lotus, Word, Power Point, etc.). En este punto se incluyen las herramientas de desarrollo (Dbase IV, C++, Java, etc.).
- Desarrollos caseros o realizados por terceros (nómina, contabilidad, etc.).
- Datos.
- Información.

Adicionalmente, el servidor de archivos posee en forma general, la configuración de colas de impresión, derechos y restricciones de cada usuario, configuración de arranque del servidor, configuración de ingreso al servidor, etc. Aunque estas configuraciones en realidad ocupan tan poco espacio que se podría despreciar.

Por supuesto, lo anterior es muy importante, pero para poder determinar las características del servidor de archivos es necesario conocer también lo siguiente:

- Número total de usuarios de LAN.
- Número de usuarios concurrentes (simultáneos) que utilizarán la LAN.
- Número de usuarios remotos, y tiempo promedio de conexión.
- Aplicaciones que utilizan los usuarios (locales y remotos).
- Aplicaciones comerciales que se instalarán en el servidor de archivos, indicando el espacio en disco duro que ocupa cada aplicación.
- Desarrollos caseros o realizados por terceros. Indicar el espacio que ocupan al instalarse.
- Tipo de archivos que se almacenarán (texto, imagen, etc.) y quién hará trabajos con ellos, y de ser posible indicar el tamaño promedio de cada uno de los archivos a utilizar.
- Tipo de respaldo de información deseado.
- Si utilizará el concepto de cliente/servidor, peer to peer o híbrido (estos conceptos se verán en el capítulo siguiente).

La información recabada permitirá determinar las características del servidor de archivos en cuanto a los siguientes puntos:

- Capacidad del disco duro.
- Memoria RAM.
- Velocidad de reloj del microprocesador.
- Tipo de microprocesador.
- Tarjeta de red.

Capacidad del disco duro.

Se considera que por cada usuario que se tenga dado de alta en la LAN deben existir, al menos, de 3 a 4 MB de espacio en disco. Si se tiene correo electrónico, mínimo agregar 500 Kb para cada usuario. En caso de que los usuarios no tengan archivos en el servidor, se les deberá asignar al menos 1 MB, para poder imprimir; este espacio podría variar dependiendo del tamaño de las impresiones, sin embargo 1 MB es un espacio con el que se podría empezar y ajustar posteriormente.

De las aplicaciones que se instalen en el servidor, si son bajo ambiente Windows se calcula que cada una ocupa aproximadamente entre 40 y 120 MB en disco duro; si son aplicaciones modo caracter se considera de 5 a 80 MB de espacio en disco duro; para el caso de utilerías se consideran de 2 a 10 MB de espacio en disco duro.

Para información y datos se recomienda tener 1 GB; sin embargo si se utilizan bases de datos de considerable tamaño se podrían manejar varios GB. Es importante indicar que dependiendo de la base de datos que se utilice, se deberá de considerar el tamaño de las herramientas de desarrollo, los runtimes, y el espacio que por si mismo ocupa la aplicación, adicionalmente a los datos.

Por otro lado los sistemas operativos de LAN requieren para su instalación y configuración de espacio en disco; este varía dependiendo del sistema que se trate y de la configuración que se le dé; sin embargo, para casos prácticos se deberá considerar 200 MB para el sistema operativo.

Por supuesto, la mejor forma de medir el espacio requerido es consultando las hojas técnicas de cada aplicación, donde se consignan los requisitos de operación.

Es importante considerar que independientemente del espacio que ocupe cada aplicación, se requiere espacio adicional para operar, independientemente del crecimiento que se tenga previsto.

Memoria RAM.

Es muy común oír que si se tiene más memoria RAM, se solucionan los problemas de procesamiento de información; esto en parte es verdad, pero existe una cierta cantidad de memoria qué, o ya no es aprovechada por el servidor de archivos o si la aprovecha ya no se nota ninguna ventaja; por lo que es necesario calcular la memoria ideal. Para calcular la cantidad de memoria RAM se considera en primer lugar el tipo de sistema operativo que se utilice; por ejemplo, para el caso de Netware se requiere mínimo de 12 MB, y para el caso de Windows NT deben de ser 16 MB; con esta cantidad de memoria funciona el servidor de archivos; sin embargo, es muy importante considerar que quienes informan de las características mínimas de operación es el mismo fabricante, y que esta información es muy comercial, por lo que para que uno de esos sistemas realmente pueda operar se requieren 4 MB de memoria adicional; sin considerar otros puntos, como el número de usuarios y las aplicaciones. En la práctica se ha encontrado que todo depende de la carga de trabajo que tenga el servidor de archivos. Existen dos tipos de cargas de trabajos: una que es la cantidad de usuarios simultáneos que generan tráfico, y la otra es la cantidad de tráfico generado por usuarios, es decir, el tráfico generado por 20 usuarios con cargas de trabajo normal puede ser superado por 5 usuarios con altas cargas de trabajo.

La práctica indica que si existen entre 25 y 30 usuarios simultáneos con aplicaciones como procesador de textos u hojas de cálculo, se recomienda que para Netware se tengan 20 MB en RAM y para Windows NT 24 MB en RAM. Por

supuesto que si se tienen más usuarios o con tráfico mayor se deberá incrementar a razón de 1 MB por cada 5 usuarios. No se recomienda tener LANs lógicas mayores de 50 usuarios; esto se refiere a que si en un servidor de archivos se instala una tarjeta de LAN, se tendrá una LAN lógica, si se tienen dos tarjeta de LAN se tendrán dos LAN lógicas, etc. Dependiendo la arquitectura que se esté utilizando se considera como límite superior una LAN de 50 usuarios. Con el auge que está teniendo Internet, empiezan a existir productos que para instalarse en los servidores Intel requieren de 128 MB en RAM.

Para el caso de sistemas RISC, se requiere más memoria que para CISC (Intel). Normalmente se inicia con 32 MB en RAM; sin embargo, dependiendo de las aplicaciones y productos que se desee tener, pudiera requerirse 128 MB en RAM y en casos especiales 256 MB o más.

Incluso en aplicaciones similares, se requiere el doble de memoria en RISC que en CISC; como es el caso de Internet, en donde una misma aplicación de Netscape para ambos ambientes requiere el doble de memoria en RISC que en CISC.

Velocidad de reloj del microprocesador.

Para este punto es necesario tener en cuenta el tamaño de la LAN. Un servidor de archivos puede empezar a funcionar desde los 50 MHz para LANs realmente muy pequeñas (menos de 10 usuarios o muy poco tráfico), 133 MHz para LANs medianas (de 10 a 20 usuarios) y de 166 MHz en adelante para LANs de mayor tamaño; por supuesto, como en el punto anterior, esto depende de la cantidad de tráfico que exista en la LAN.

La recomendación en este punto es con respecto a las nuevas versiones de microprocesadores, que pueden ser actualizados sin tener que cambiar más

dispositivos; esta opción se presenta prácticamente solo en microcomputadoras que utilicen microprocesador 80486; es decir, si se tiene una microcomputadora con uno de estos microprocesadores a 25 MHz, el mismo puede ser actualizado a versión de 33 MHz o más, con solo cambiar el microprocesador, y esto permitirá que el equipo que se tenga pueda ser actualizado fácilmente, proporcionando un crecimiento acorde a las necesidades que se tengan.

Para redes locales corporativas, se recomienda que la velocidad mínima sea de 133 MHz, ya que estas redes fácilmente pueden crecer en número de usuarios, o incorporar aplicaciones muy demandantes.

Tipo de microprocesador.

Mucho se ha hablado de que el software no aprovecha todas las ventajas que presenta un microprocesador, y esto en parte es cierto; sin embargo, esto no quiere decir que debido a que no existe un Netware 5, no es recomendable utilizar un servidor de archivos con un microprocesador pentium.

Sabemos por experiencia que en este campo el hardware se ha desarrollado más rápido que el software, por lo que es normal que el software no pueda aprovechar al máximo todas las ventajas que ofrece el hardware, aunque no por esto significa que lo desperdicie.

Debido a la competencia de los sistemas operativos de red, los fabricantes de NOS anuncian que sus sistemas operan con el menor procesador posible, pero esto no quiere decir que opere al 100%; en realidad se podría decir que solo "levanta" con esos requerimientos.

Por supuesto, todo depende de las necesidades y de las características propias de cada proyecto, pero en general es posible utilizar un microprocesador 80486; sin embargo, también es adecuado tomar en cuenta la tendencia que han

estado siguiendo los fabricantes de microcomputadoras y de sistemas operativos. Por un lado la tendencia de los fabricantes, en cuanto a microcomputadoras se refiere, es no producir o producir cada vez menos los modelos de microcomputadoras con microprocesadores 80486, como es el caso de HP, mismo que ya no fabrica computadoras, y mucho menos servidores con este microprocesador. Si se pretende utilizar un microprocesador 80486 en el servidor, se recomienda que sea un microprocesador completo, no el recortado, principalmente porque el modelo recortado presenta algunos problemas para la instalación de algunas tarjetas de LAN y con algunos dispositivos adicionales, como discos duros y dispositivos de respaldo principalmente, aunque no quedan excluidas impresoras, modems, etc.

Así mismo algunos fabricantes de hardware han desarrollado líneas de productos especiales para redes; por lo que se recomienda utilizar uno de estos servidores.

Como sugerencias adicionales, es recomendable adquirir servidores de archivos de fabricantes con reconocido nivel de atención a usuarios y con representación directa en México, ya que muchas veces se adquiere equipo que es de menor precio, pero al momento de solicitar soporte o asesoría es prácticamente imposible recibir apoyo.. Por otro lado si se desea adquirir algún dispositivo de alguna otra marca, como algún disco duro o algún sistema de respaldo, seguramente se requiera un drive, mismo que por lo general quien lo provee es el fabricante del servidor de archivos, o el fabricante del dispositivo, por lo que no se deberá esperar a que el fabricante del NOS lo proporcione.

Con respecto a los servidores RISC, existen diversas versiones; para este caso se deberá recurrir al fabricante para que determine el tamaño del servidor; incluso el mismo fabricante de la aplicación que se desee tener, deberá proponer el hardware adecuado para la aplicación.

Es recomendable que para el caso de RISC se soliciten referencias de clientes que utilicen dicho producto, operando bajo las mismas condiciones propuestas. De hecho esto aplica incluso para CISC, aunque para dicho caso es más sencillo determinar las características del servidor.

Al día de hoy también se requiere que el servidor cuente con otro tipo de características, como es que cuente con CD y cinta de respaldo.

Para elegir dispositivo de respaldo, se deberá consultar con el fabricante del NOS para que recomiende alguno, ya que existen algunos dispositivos que podrían llegar a no ser compatibles con el sistema operativo de red.

Tarjeta de Red.

Este dispositivo al ser el puerto de comunicaciones hacia la red, en caso de no elegirse adecuadamente, puede en un momento dado ser un "cuello de botella". Claro que la tarjeta de red depende del diseño de la red; sin embargo, un tipo de tarjeta, por ejemplo Ethernet, tiene diferentes tecnologías, por lo que se deberá no solo elegir la arquitectura adecuada, sino la tecnología correcta. Los servidores requieren de tarjetas rápidas, por lo que se recomienda utilizar, al menos, tarjetas de 32 bits (EISA) para el caso de ethernet o token ring, o tarjetas de arquitecturas de alta velocidad como Fast Ethernet, 100VG, ATM o FDDI en cualquiera de sus versiones. Es importante tener cuidado, debido a que si se adquieren los hubs para ethernet, y una tarjeta, por ejemplo FDDI para el servidor, se deberá asegurar que el hub de ethernet cuente con al menos un puerto FDDI, ya que en caso contrario este servidor no se podrá incorporar a la LAN.

Se han visto casos en que se tienen servidores muy poderosos, y que por no seleccionar una tarjeta de red adecuada, el comportamiento de la red equivaldría a contar con un servidor de la mitad del tamaño.

8.2 Características de las estaciones de trabajo.

Las estaciones de trabajo son los equipos por medio de los cuales hacemos uso de los recursos que ofrece una plataforma de LAN, es decir, estos elementos son la puerta de entrada a la LAN.

Con estos equipos sucede algo similar que con los servidores de archivos, ya que se tiene la idea de que entre más grande en cuanto a configuración, más ventajas se van a tener; esto es totalmente cierto; sin embargo, no es necesario contar con la configuración más poderosa para que dicho equipo satisfaga las necesidades para las que fue adquirido, por lo que se debe hacer un pequeño análisis para determinar la configuración adecuada.

Para poder elegir adecuadamente el equipo que se necesita, el procedimiento es el siguiente:

1. Se detallan todas y cada una de las funciones-necesidades a cubrir por la persona o personas que harán uso del equipo.
2. Al tener claras las funciones-necesidades se elige el software que las solucione.
3. Y por último se detalla el equipo (hardware) que soporta a ese software que a su vez soluciona o cubre las funciones-necesidades de la persona o personas que harán uso de ese equipo.

En pocas palabras, lo que se hace es tipificar las funciones-necesidades de las personas para así tener diferentes configuraciones de equipo que satisfaga esas necesidades. Por ejemplo, las funciones-necesidades de una secretaria, en cuanto a recursos de cómputo, son menores que las de un desarrollador de software, ya que por lo general un desarrollador requiere normalmente de un microprocesador pentium o mayor, y por supuesto una secretaria no requiere de tanto poder de procesamiento, dado que una de sus principales funciones es realizar documentos en procesadores de texto y la velocidad que requieren realmente no es crítica para el desempeño de sus funciones.

Al igual que en el caso del servidor de archivos, es necesario considerar la estación de trabajo sobre la base de ciertos parámetros, mismos que se verán a continuación:

- Tipo de microprocesador y velocidad.
- Memoria en RAM.
- Capacidad del disco duro.
- Tipo de monitor.
- Unidades de disco flexible.

Tipo de microprocesador y velocidad.

Un punto importante es que existen fabricantes que ya sacaron del mercado modelos de microcomputadoras con microprocesadores 80486.

Por otro lado, es por demás adecuado tener en cuenta que todas las nuevas aplicaciones son para ambiente gráfico; esto no es solo porque este ambiente sea agradable a la vista, sino porque se realizó un estudio entre los usuarios de equipos Macintosh (posee ambiente 100 % gráfico) y usuarios con

aplicaciones DOS, y se encontró que los usuarios MAC dominaban más paquetes que los de DOS, y esto principalmente debido a que el ambiente gráfico posee estándares de operación, no importando si es una hoja de cálculo, procesador de texto, generador de imágenes, etc. Todos estos paquetes presentan necesidades comunes, como imprimir, abrir archivos, guardar archivos, etc., utilerías que se encuentran y usan de la misma manera en el ambiente gráfico; caso totalmente contrario a lo que ocurre en aplicaciones que funcionan bajo el ambiente DOS, inclusive productos diferentes de un mismo fabricante se manejan de forma totalmente diferente; todo lo anterior hace que los usuarios de ambientes gráficos, como MAC, manejen de dos a tres veces más paquetes que los usuarios que utilizan ambiente DOS. Adicionalmente el ambiente gráfico permite tener interacción entre software de diversos fabricantes y entre diversas aplicaciones en una forma totalmente transparente. Y por si lo anterior fuera poco, el ambiente gráfico independiza las aplicaciones del hardware, sobre todo ahora con Windows 95, que reconoce prácticamente cualquier dispositivo conectado a la computadora.

Todas estas ventajas que provee el ambiente gráfico, hacen que el ambiente operativo al que están enfocados todos los esfuerzos de los fabricantes de software sea Windows. Esto repercute directamente en que los equipos que soportan a este tipo de software requieran de mayor procesamiento y memoria principalmente. Por otro lado, el mercado de microcomputadoras, sobre todo en México, es relativamente nuevo, por lo que está a punto de empezar a utilizarse en forma masiva no solo en los corporativos, donde ya desde hace algunos años se encuentra bien posicionada la tecnología, sino en el negocio pequeño e incluso el hogar, donde ahora con la revolución que está causando Internet, la tendencia es que sea tan popular como tener una televisión; por lo que se puede decir que es ahora cuando se debe pensar en romper con los esquemas

anteriores, para entrar a la era de la interoperabilidad de sistemas y ambientes de una forma fácil y transparente para el usuario final, y por supuesto esto requiere que los equipos que se adquieran sean relativamente grandes (mínimo 80486). Esto no quiere decir que los equipos 80386, se depositen en la basura; simplemente que se les dé otras funciones, como correo electrónico, fax, correo de voz, etc. , o que se asigne a personal que no requiere este ambiente; por ejemplo la captura de información no requiere de este ambiente, o en algunos tipos de consulta de información tampoco se requiere; inclusive existen algunos gateways que no requieren mayor capacidad de procesamiento que la que ofrece una 80386. Los equipos AT y XT ya no tienen cabida en este ambiente.

En forma práctica, al día de hoy es factible adquirir una PC 80486 (80386 en el peor de los casos) que opere a una velocidad de reloj de 66 MHz, y se tendrá un equipo que realice al menos funciones básicas, como ingresar a Internet o trabajar en un documento en un procesador de texto.

Memoria en RAM.

Para calcular la memoria que se requiere tener en RAM, primero se debe conocer las aplicaciones que se van a utilizar, ya que de ello dependerá la cantidad de RAM que se requiera. Como se comentaba anteriormente, la tendencia de los fabricantes de software es hacia ambientes gráficos; por lo que sí se desea trabajar bajo este ambiente, se requerirá un poco más de memoria RAM. Al día de hoy los equipos XT o AT no se pueden utilizar en un ambiente de red local, incluso prácticamente ya no sirven para nada.

Para estaciones de trabajo en ambiente gráfico se requiere tener mínimo 8 MB en RAM; recomendable 12 MB, y 16 en el caso de tener acceso a Internet.

En el caso de estaciones de trabajo que utilicen OS/2, se requiere mínimo 6 MB en RAM; recomendable 12 MB en RAM; esto por requerimientos del sistema operativo.

Si se va a utilizar un microprocesador pentium, se recomienda que el equipo cuente al menos con 12 MB en RAM, ya que de otra forma se desperdiciaría poder de procesamiento.

En caso de utilizar Windows 95, se recomienda tener mínimo 16 MB en RAM, ya que de otra forma el sistema sería demasiado lento. Si una pentium con 16 MB en RAM está lenta, pudiera ser que tuviera menos de 25 MB de espacio libre en disco duro.

Capacidad del disco duro.

Al igual que las características anteriores, el disco duro va de acuerdo a las funciones-necesidades del usuario de dicho equipo. Lo normal es tener, en su mayoría, estaciones de trabajo sin disco duro; aunque existen casos en que sí es indispensable, por ejemplo para administradores de LAN, desarrolladores, o personal que requiera demasiada confidencialidad de la información que maneja; es decir, personas que por sus funciones-necesidades justifiquen un dispositivo de este tipo.

Los discos duros recomendables para los usuarios que así lo ameriten, de preferencia, deben ser de entre 500 MB y 1 GB; un disco fuera de este rango es o demasiado pequeño o demasiado grande.

Tipo de monitor.

Como en los casos anteriores, este elemento depende de las funciones-necesidades del usuario; sin embargo, debido principalmente al ambiente gráfico, se recomienda que los monitores sean a color y de alta resolución (mínimo VGA); esto no quiere decir que monitores de menor resolución y/o monocromáticos no funcionen; por otro lado, el tener un monitor a color no es un lujo, dado que proporciona menor esfuerzo a la lectura o creación de documentos; además de que al tener un ambiente más agradable la productividad de cada individuo aumenta considerablemente.

Así mismo existen funciones-necesidades que requieren de gráficas; por ejemplo el monitoreo de una LAN, que para presentar los resultados en gráficas es prácticamente indispensable contar con un monitor a color, con una resolución de por lo menos de Super VGA; otro ejemplo es la creación de presentaciones a miembros de alto rango en la corporación, manejo de estadísticas, etc.

Adicionalmente existen aplicaciones que funcionan con requerimientos mínimos de monitores.

Se pueden tener prácticamente cualquier tipo de monitor, pero es necesario tener muy presente el efecto negativo que puede tener sobre una persona el hecho de estar trabajando con un monitor de baja resolución y monocromático.

Unidades de disco flexible.

Como en todos los casos en que se requiere seleccionar un dispositivo, es necesario conocer el detalle de las funciones-necesidades que se desean cubrir para, en base a eso, determinar las características del dispositivo.

De hace algunos años a la fecha se ha estado promoviendo el uso, en la red, de microcomputadoras sin disco duro y sin disco flexible, es decir, se utiliza una microcomputadora con un microprocesador de tamaño razonablemente grande, una buena cantidad de memoria y un monitor a color de buena resolución, pero a un costo menor, ya que no posee unidad de disco flexible ni disco duro. Estos equipos se utilizan principalmente para personas cuyas funciones-necesidades no requieran de estos dispositivos. Adicionalmente a que resulta que el equipo es más barato, se encuentra otra ventaja que es la seguridad. Esto permite que no cualquier persona pueda extraer información, ni introducir discos flexibles que pudieran en un momento dado estar contaminados con algún tipo de virus, y adicionalmente a esto, sabemos que el hecho de que un equipo tenga menos dispositivos, hace que la posibilidad de que ese equipo sufra algún desperfecto disminuye considerablemente; y más aun, teniendo en cuenta que estos dispositivos, al ser mecánicos, presentan un mayor grado de factibilidad de sufrir algún desperfecto.

Por otro lado así como se propone que algunas microcomputadoras no cuenten con discos flexibles, también se recomienda que exista por lo menos un equipo con dos unidades de disco flexible, una de 3.5 " y otra de 5 1/4"; otro equipo con dos unidades de 3.5" y uno más con dos unidades de 5 /14"; en todos los casos se recomienda que sean unidades de alta densidad, ya que sabemos, siempre existe algún motivo por el cual se requiera de ambos.

Incluso ahora con la tecnología de CD, es recomendable que al menos una computadora dentro de la red local cuente con un dispositivo de CD-ROM.

Por supuesto, no en todos los proyectos se requiere tener esto; sin embargo, en LANs corporativas sí se recomienda. Es conveniente tener en cuenta que los discos de 5 1/4" tienden a desaparecer, por lo que será conveniente adecuarnos lo antes posible a esta tendencia.

CAPÍTULO 9
Sistemas Operativos de Red. ¿Netware o Windows NT?

Temas del capítulo.

9.1 Introducción a sistemas operativos de red.

Cliente / Servidor.

Peer to peer.

9.2 Productividad del negocio y personal.

9.3 Mercado mexicano.

9.4 Compañías (Microsoft y Novell).

9.5 Productos (Windows NT y Netware).

9.1 Introducción a sistemas operativos de red.

Dentro de los elementos que componen una LAN, se puede decir que básicamente son dos los elementos físicos que determinan el funcionamiento de la misma: uno de estos puntos se refiere a la arquitectura de la LAN y el otro al sistema operativo. En este capítulo se desarrollará el punto de los sistemas operativos de LAN, basándose en los dos con mayor incidencia en el mercado mexicano. Por un lado se tiene el Netware de Novell y por el otro Windows NT de Microsoft. Esto no quiere decir que sean los únicos, ya que existen otros como

VINES de Banyan Systems, POWERLan de Performance Technology y LANtastic de Artisoft; sin embargo, sí se puede considerar que los dos primeros son los de mayor penetración en México.

Aunque en este capítulo se presenta una comparación entre Netware y Windows NT, se expondrán los puntos básicos del porqué no se incluye, a detalle, el comparativo versus Unix.

Los sistemas operativos de redes locales se basan en dos filosofías de operación, una de ellas denominada Cliente/Servidor y la otra Peer to Peer (o de igual a igual); ambas filosofías podrían por si mismas ser un tema de tesis; por tal razón se expondrán en una forma muy sencilla los principios en que se basan estas filosofías para posteriormente entrar de lleno al tema que nos atañe.

- Cliente/Servidor.

La filosofía cliente/servidor se inicia conjuntamente con el desarrollo de la arquitectura Ethernet, en Palo Alto, California. La idea principal fue, desarrollar aplicaciones prototipo en computadoras personales conectadas a una LAN; a estos programas se les denominaron "clientes", ya que hacían requisiciones y obtenían resultados de programas "servidores" que corrían en la computadora central de la LAN. La palabra cliente se utilizó para diferenciar a los programas de los usuarios (humanos); así el término cliente/servidor se inició y ahora se utiliza para designar aplicaciones de software basadas en dos o más programas que

corren cooperativamente en diferentes computadoras conectadas por medio de una LAN.

En esta filosofía, los procesos se llevan a cabo en forma distribuida, lo que se conoce como procesos cooperativos. Al implementar una plataforma de LAN existe una entidad que se encarga de administrar, controlar, compartir y proporcionar todos los servicios que una LAN permite a las entidades que así lo soliciten; es decir, existe una entidad primaria o maestra (servidor) que se encarga de proporcionar todos los servicios que le sean solicitados por las entidades secundarias o clientes.

Esto, a simple vista, parece la definición de un esquema Unix, o en forma genérica, de un ambiente de minicomputación o de mainframe; sin embargo, la diferencia estriba en que en el ambiente de redes locales, los clientes poseen "inteligencia", es decir, microprocesador, mismo que es utilizado de la siguiente forma: supongamos que tenemos una LAN, y uno de los clientes desea utilizar un procesador de textos, con lo que el cliente solicita, al servidor, hacer uso del mismo; entonces el servidor hará una copia del procesador de texto que posee en disco duro y la enviará al cliente, en donde residirá la copia en memoria, con lo que el cliente se encargará de hacer todo el trabajo en cuanto no sea requerido un acceso al servidor. En este caso el servidor de archivos es un equipo relativamente grande y las estaciones de trabajo de menor capacidad que el servidor de archivos.

El llamado paradigma cliente/servidor, en el que se afirma que las microcomputadoras desplazarán a las minicomputadoras y mainframes es

totalmente falso, ya que cada vez se observa la necesidad de poseer servidores más poderosos debido a las aplicaciones que actualmente así lo están requiriendo. Podemos ver que hacer dos años un servidor 80486 era considerado adecuado para el 80% de las aplicaciones que se requería tener en operación en una LAN; ahora vemos que servidores con microprocesador 80486 empiezan a ser pequeños, y se empieza a requerir Pentium o WorkStation para algunos casos, y para otros ya se está necesitando equipos más poderosos; todo debido a las aplicaciones que cada vez requieren de mayor velocidad y capacidad de procesamiento; esto lo único que nos muestra es que el paradigma basado en microcomputadoras no se llevará a cabo; sin embargo sí el basado en plataformas de LAN heterogéneas en cuanto a los tipos de equipos de cómputo.

- Peer to Peer.

En la filosofía Peer to Peer, de igual a igual o punto a punto como también se le conoce, se tiene que todas las entidades que se encuentran conectadas a la plataforma de LAN son simultáneamente clientes y servidores, es decir todos los equipos conectados permiten en un momento dado compartir con otros usuarios/equipos los recursos con los que cuentan, adicionalmente a utilizar los propios.

Para este caso, debido a que todos los equipos son servidores, requieren que cada equipo se encuentre en un rango de capacidad entre mediana y grande; esto se refiere a microprocesador y memoria, ya que al compartir los recursos con

otros equipos, el proceso que se esté llevando a cabo en ese equipo en forma local y remota tomará más tiempo, por lo que se recomienda que estos equipos posean microprocesador pentium a 133 MHz con 16 MB o más en RAM.

Peer to Peer es una tecnología que de alguna forma es barata, ya que no requiere un servidor dedicado a llevar a cabo estas funciones; por otro lado requiere que cada usuario sea responsable de su propio "servidor", lo que implica que los usuarios tengan un nivel de conocimientos mucho más elevado, debido a que ahora deberán administrar tantos servidores, como equipos conectados se tenga la red local.

Aunque tanto Microsoft como Novell cuentan con productos que abarcan ambas filosofías de operación, en este capítulo solo se expondrá lo referente al ambiente Cliente/Servidor.

9.2 Productividad del Negocio y Personal.

La mayoría de las redes locales en México tienen, ya sea, Netware, Windows NT o Unix. La pregunta es ¿cuando elegir uno u otro?

La experiencia dice que si es necesario que las aplicaciones de un negocio se encuentren en redes locales, se haga en ambiente Unix, y si se desea implementar soluciones departamentales o de productividad personal, se lleve a cabo en un ambiente ya sea de Netware o Windows NT. Esto significa que por lo general se deberá contar con al menos dos servidores, uno donde residan las

aplicaciones mismas del negocio, y otro, donde se cuente con las herramientas de productividad personal.

El mayor poder del ambiente transaccional en las redes locales, se encuentra en los sistemas Unix. Siendo Netware o Windows NT, una solución para ambientes mas enfocados a la productividad personal, no del negocio de un corporativo. La influencia de esta tendencia la marcan dos puntos, el sistema operativo y el microprocesador; ya que por un lado, tanto Unix como RISC han probado ser más confiables que con CISC y Netware o Windows NT; y aunque Windows NT tiene una solución en equipos Digital que cuenta con procesador RISC, Microsoft no ha promocionado suficientemente esta solución, al parecer mas por Digital (DEC) que por Microsoft mismo.

Esto parece muy simple, y expuesto así, incluso parece no contar con un análisis previo; sin embargo este análisis lo marca la experiencia y el desempeño que se ha demostrado a lo largo del tiempo.

Otra razón que refuerza lo anterior es que existen pocos productos terminados que se adapten 100% a la forma de trabajo de una empresa, por lo que las compañías prefieren desarrollar su propio sistema, para ser totalmente compatible con la filosofía y modo de trabajo de cada una.

¿Bajo qué sistema operativo se cuenta con la mayor versatilidad para desarrollar y a su vez que cuente con gran poderío de procesamiento? A esta pregunta cualquiera de los fabricantes respondería que su sistema operativo es el mejor; sin embargo, se ha demostrado que para un desarrollador es mucho más versátil y eficiente hacer una aplicación en ambiente Unix, mismo que ha

demostrado que su capacidad de procesamiento es superior en condiciones similares, a las de Netware o Windows NT.

Para muchos, la versatilidad y facilidad en la creación de una aplicación serán más importantes; por lo que seguramente elegirían Windows NT por la gran cantidad de herramientas de desarrollo que Microsoft tiene; sin embargo, cuando es necesario sacrificar facilidad de desarrollo para mejorar la velocidad de procesamiento, la experiencia dice que se utilice Unix.

En este caso lo más importante es la eficiencia, donde típicamente se mide por el tiempo de respuesta, aunque esto es muy subjetivo, ya que también se requiere: integridad, oportunidad, validez y disponibilidad. Los grandes corporativos, por la cantidad de transacciones que manejan, requieren tiempos de respuesta excelentes, y debido a sus requerimientos utilizan mainframes; sin embargo, para empresas de menor tamaño, donde el tiempo de respuesta también es importante, pero se cuenta con menores recursos, tanto informáticos como financieros, la solución podría implementarse en una PC con sistema operativo Netware o Windows NT.

Así mismo, la información del negocio, que poseen los corporativos normalmente es del tipo transaccional, por lo que el ambiente Unix resulta con mayores ventajas, e incluso en ese ambiente se cuenta con mayor experiencia por parte de los fabricantes y proveedores de servicios.

Por otro lado, existe una gran cantidad de información que si bien es importante para la operación de un negocio, no se puede catalogar como primordial, aunque si necesaria. Esta información es la que normalmente poseen

los usuarios y les permite desarrollar su labor. A este tipo de información la denominaremos departamental o de productividad personal.

Para este caso, tanto Netware como Windows NT, han demostrado contar con la mejor solución del mercado. ¿Porqué? Muy sencillo, debido a que el 80% del software se ha desarrollado para este segmento, y a que los usuarios prefieren herramientas fáciles de utilizar, bajo ambientes sencillos de operación como Windows, sin dejar de lado la plataforma Macintosh; sobre todo que el grueso de los usuarios no es de formación técnica, y la idea fundamental es que los usuarios se enfoquen a sus tareas principales, y que la tecnología solo sea una herramienta de trabajo.

9.3 Mercados y estrategia comercial.

Desde el punto de vista anterior, existen dos nichos de mercado: uno enfocado a la productividad del negocio y otro a la productividad personal o departamental. ¿Pero qué pasa con el tamaño de las compañías?. En realidad el comportamiento anterior, respecto a la productividad del negocio o personal, se lleva a cabo con más claridad en las instituciones de mayor tamaño, ya que en la pequeña y mediana empresa es más difícil segmentar por tipo de producto, sobre todo debido a que la diferencia ente ellos es tan sutil, que cuando las cargas de trabajo no son muy demandantes y no existe una gran cantidad de servidores

conectados ente sí, la diferencia entre estos sistemas es realmente mínima, y la elección es mas por preferencias.

Según la experiencia del personal de Novell y Microsoft, para que se aprecie una diferencia real entre Netware y Windows NT, se debería tener un laboratorio de al menos 70 servidores interconectados entre sí, incluyendo aplicaciones, generadores de tráfico, benchmarks y equipo para análisis de tráfico. Como se puede apreciar llevar a cabo un comparativo de esta forma sería realmente complicado, tanto desde el punto de vista técnico, como económico.

Para poder hacer un análisis con mayor detalle, se tomaran dos segmentos de mercado: los grandes corporativos (es decir los primeros 100 de Expansión) y la empresa mediana y pequeña (del 101 al 500 de Expansión). Por lo que a continuación solo se hablará de Netware y Windows NT, siendo que Unix cuenta con un "nicho especial", sin importar el tamaño de la empresa, según lo planteado en párrafos anteriores.

Hasta fines de 1994, el rey absoluto del mercado mexicano en cuanto a los sistemas operativos se refiere en los grandes corporativos, era Netware de Novell. La cantidad de productos instalados era sin lugar a dudas el orgullo de Novell. Al día de hoy los grandes corporativos prefieren Windows NT de Microsoft. La gran pregunta es ¿Qué sucedió en el mercado mexicano que hiciera que la balanza fuera más equilibrada?

Novell se ha esforzado en demostrar que su producto es realmente bueno, pero se le olvidó crear una estrategia comercial adecuada. En realidad siempre creyó que por tener un excelente producto, los clientes seguirían comprando sin

importar la atención, ni el precio. Por ejemplo, el esquema de licencias corporativas de Novell, no ofrecía ventaja alguna a quien lo adquiría. Este esquema de licencia consiste en comprometerse a adquirir cierta cantidad de software al año, por lo que el único que ganaba era Novell; incluso el precio era prácticamente el mismo que si las licencias se adquirían sin el contrato.

Otro punto muy importante, y que sin lugar a dudas influye mucho, es que la venta de productos tanto de Novell como de Microsoft, se lleva a cabo por medio de distribuidores, mismos que compran a mayoristas. Por si mismo esto no es importante; sin embargo, resulta que los distribuidores de software obtienen mayores ingresos al comercializar un producto de Microsoft que de Novell, por lo que resulta más atractivo, para el canal de distribución, promocionar los productos de Microsoft, que de Novell.

Por otro lado Microsoft, mas que ser una empresa desarrolladora de software es una empresa de publicidad que casualmente promueve software. Esto ha hecho que los anuncios de Microsoft detengan ventas de productos de la competencia, debido a las promesas que lleva a cabo.

Microsoft se ha caracterizado por tener al cliente contento antes que ofrecer un producto excelente; esto no quiere decir que los productos sean malos, simplemente que en un principio ofrece productos que solo cumplen con las características mínimas indispensables solicitadas por los usuarios, y a través del tiempo fortalece sus productos en base a promesas que siempre ha cumplido, normalmente no en las fechas anunciadas, pero si con las características y beneficios prometidos.

El esquema de licencias corporativas que ofrece Microsoft es mas apegado a las necesidades del cliente y sobre todo, algo muy importante: la lógica, que resulta mucho más fácil de comercializar por parte de los proveedores, y de entender por parte de los clientes. Microsoft incluye garantía de actualización de software, las veces que sea necesario, en caso de que exista una nueva versión en el lapso de un año, pagando por anticipado una renta mínima, también ofrece este esquema de licencias, dos años antes que Novell y cuando Novell lo saca al mercado no tiene ni la experiencia, ni las condiciones ni ventajas que ofrece Microsoft.

Por otro lado, ¿Qué sucede en el mercado de las empresas medianas y pequeñas? En este segmento sin lugar a dudas Novell sigue siendo quien más base instalada tiene, la pregunta es ¿por qué? La razón principal es que Novell tiene mucho tiempo en el mercado mexicano, lo que ha permitido que mucha gente lo conozca suficientemente bien como para poder sugerirlo como solución y soportarlo técnicamente.

En el caso de Windows NT, es un producto relativamente nuevo, la capacitación es cara y quien proporciona servicios para este segmento del mercado difícilmente conoce esta tecnología tan a detalle como en el caso de Netware. Quienes sí tienen el conocimiento adecuado sobre Windows NT son los grandes distribuidores, mismos que por su estructura están enfocados al mercado de los grandes corporativos.

Claro que Microsoft ya se dio cuenta de esto y ahora quiere desarrollar a distribuidores que puedan atender en forma adecuada al mercado de pequeña y mediana empresa.

9.4 Compañías (Microsoft y Novell).

Las compañías y el trato que se recibe de ellas son un factor sumamente importante, siendo este un gran diferenciador, para elegir entre estos dos sistemas operativos de red.

Novell cuenta con una oficina de representación de ventas, careciendo de personal técnico suficiente para soportar el producto. De hecho la definición en México es que el personal está para promocionar el producto y demostrarlo, no para soportarlo, por lo que en realidad Novell no apoya técnicamente al usuario, como este lo desea, después de que el producto se ha vendido.

Novell no cuenta con recursos que permitan llevar a cabo el liderazgo del proyecto sin descuidar otros clientes. Careciendo en México de un departamento de servicios profesionales que se involucre en la problemática del cliente, esta labor la deja al distribuidor. Incluso en el caso de que el cliente solicite la asistencia de un técnico bajo contrato, Novell carece de infraestructura para hacerlo, apoyándose para esto en la capacidad de los distribuidores.

En el caso de Microsoft, este tiene una gran ventaja: el tiempo que tiene en México es mayor que el de Novell; por lo que incluso, adicionalmente a contar con

más personal, cuenta con un departamento de servicios profesionales. Lo que permite apoyar al cliente desde las pruebas del producto hasta el soporte posterior; inclusive cuenta con un help desk, apoyando inmediatamente a sus clientes.

9.5 Productos (Windows NT y Netware).

En Estados Unidos, principalmente, se ha tratado de encontrar cual es el mejor producto por medio de evaluaciones entre Windows NT y Netware; sin embargo esto no ha hecho que exista un acuerdo unánime al respecto.

Por lo anterior difícilmente se podría realizar una comparación de productos y en base a eso determinar cual es el mejor. Y aunque sí se presentará una comparación de productos al final de este capítulo, en esta sección se analizarán Netware y Windows NT desde el punto de vista "lo que se espera de ellos en un futuro y sus estrategias", ya que al día de hoy los decisores de las empresas se inclinan mas por comprar infraestructura que puedan aprovechar a futuro, que un producto que al día de hoy resuelva. Esta forma de verlo es como levantar un edificio; si los cimientos están bien, se podrá construir con confianza.

Por otro lado, el elegir a un ganador sería tan difícil como decidir si X automóvil es el mejor vehículo de transporte. Para poder decir esto deberíamos elegir un marco de comparación, como tipo de terreno, normas de seguridad del lugar, leyes de cada lugar, etc. Lo mismo sucede con estos sistemas; sin

embargo, el determinar un marco de acción de cada uno de ellos es sumamente complicado debido a que las diferencias son tan sutiles que el fijar un marco de referencia para cada uno de ellos resultaría prácticamente imposible.

También debe reconocerse que mucha de la selección que hace el personal de sistemas es en base a preferencias y a conocimiento del producto.

Es importante mencionar que tanto Novell como Microsoft han hecho con esta "guerra de los sistemas operativos de red", que el usuario sea quien en realidad gane, ya que mientras ambas compañías se esfuerzan por demostrar cual es el mejor producto, los corporativos obtienen mayores beneficios.

El hacer una evaluación que deje satisfecho a todos, es sumamente complicado, ya que "cada quien habla como le va en la fiesta". Sobre todo habiendo visto que en ambientes similares con clientes distintos, un mismo producto se comporta distinto, incluso siendo un mismo ingeniero el encargado de realizar la instalación y configuración del sistema.

Ambos sistemas operativos han evolucionado, y por supuesto esta evolución ha afectado y se ha visto afectada por el mismo ambiente informático, que crean tanto usuarios como fabricantes. Así mismo se ha visto una clara tendencia en esta evolución, misma que podríamos resumir con los siguientes puntos:

- La mayoría de los corporativos se inclinan por Windows NT de Microsoft.
- Novell evolucionó su Netware 3.x a 4.x tomando conceptos importantes del ambiente Unix, e incluso tomando algunos conceptos de Windows NT.

- Unix se ha posicionado fuertemente como el ambiente ideal para las aplicaciones de negocios.
- Novell ha perdido participación de mercado, aunque no lo quiera admitir.
- Todos los fabricantes de software cuentan con soluciones para Windows, incluso Novell.
- El líder indiscutible en software y sistemas operativos de escritorio es Microsoft.
- La base instalada más grande de sistemas operativos de red es de Novell.
- Los visionarios apuestan a que los sistemas operativos de red más fuertes en la primer década del siglo 21 serán Unix y Windows NT, sobre todo por el desarrollo que ambos ambientes tienen para la red de redes, Internet.

Si el mejor sistema operativo con que cuenta Novell es Netware 4.x, ¿por qué muy pocos corporativos han realizado el cambio de Netware 3.x a 4.x?
Algo que no ha ayudado mucho a Novell en los grandes corporativos es la forma de migrar de Netware 3.x a Netware 4.x, debido a que es tan difícil como si se tratara de marcas distintas. Sobre todo debido a que los drives de software que utiliza Netware 3.x, no funcionan adecuadamente para Netware 4.x. Esto significa que en una migración se tienen problemas de entrada en la tarjeta de red y el CD-ROM. Si se cuenta con equipo para respaldo, este también tendrá problemas, y en caso de que se tengan aplicaciones que interactúen con Btrieve, también tendrán problemas; así mismo, si se cuenta con aplicaciones que estén hechas exclusivamente para la versión 3, también tendrán problemas.

Para que un corporativo esté seguro de que la migración no tendrá problemas con su base instalada actual, se deberá llevar a cabo un prototipo en laboratorio, donde se tendrá que invertir poco más de 40,000.00 dólares en productos (hubs, routers, cableado, unidades de respaldo de información, servidores, tarjetas de red y cuanto se tenga en el corporativo para realizar una simulación), y de tres a cuatro meses de pruebas con personal altamente capacitado.

Seguramente existen muchos usuarios que prefieren no llevar a cabo estas pruebas; sin embargo, si consideramos que el 10% de las redes que existen al día de hoy en un corporativo son de operación o misión crítica; es decir, que estas redes se utilizan para atender clientes, o llevan procesos que no se pueden detener, el no realizar pruebas con estas redes podría acarrear problemas muy graves para el corporativo.

Esto visto desde un punto de vista crítico significa que Novell inició por un camino equivocado y que al día de hoy, que intenta corregir el camino se encuentra con que lo más difícil es salvar los obstáculos que el mismo Novell impuso; en caso contrario las actualizaciones de software no serían verdaderas migraciones, ya que incluso algunos drives de impresoras dejan de funcionar en este ambiente. Según Novell existen cerca de 50 correcciones (parches) para Netware 4.x.

Netware de Novell.

Antes de iniciar el análisis a detalle de las características de este sistema operativo, se aclarará que el fabricante de este sistema operativo es Novell, y el nombre del producto es Netware, esto sencillamente debido a que erróneamente se dice, por ejemplo, "mi LAN es Novell", siendo que Novell no solo fabrica sistemas operativos para redes locales, también posee una extensa gama de productos adicionales, principalmente gateways o sistemas que permitan comunicación a otros ambientes o protocolos y también posee sistemas que permiten implementar el protocolo TCP/IP en redes de microcomputadoras que no tenga sistema operativo de red dedicado, e incluso cuenta con productos para crear un Web Site. Es el equivalente a decir que tenemos un vehículo Ford, sin embargo esto no nos dice prácticamente mucho, ya que sabemos que existe desde una versión austera de un coche de cuatro cilindros, hasta un coche de super lujo, por supuesto pasando por toda la gama de accesorios y motores, etc., por lo que el decir que "se tiene una LAN Novell" es un error de conceptos, aunque sin lugar a dudas aceptado por muchos.

El sistema operativo de Novell, Netware, posee dos protocolos básicos IPX/SPX (Internetwork Packet Exchange/Sequence Packet Exchange) mismos que se desarrollaron a partir del protocolo XNS de Xerox, por Ray Norda, Judith Clarke, Craig Burton y un grupo de desarrolladores de una compañía llamada Superset en Utah.

Estos protocolos son excelentes para ambientes departamentales, con tráfico no muy intenso; sin embargo, cuando el tráfico es alto, y existen enlaces remotos, se convierten en protocolos poco prácticos, debido a que no fueron creados para trabajar bajo estas características.

Windows NT de Microsoft.

Microsoft creó Windows NT a partir de su LanManager, cuya última versión fue la 2.2; a su vez el LanManager de Microsoft basa su concepción en LanServer de IBM y 3+Open de 3Com.

En realidad Windows NT sigue siendo el mismo LanManager; lo que sucede es que Microsoft le cambia el nombre a Windows NT aprovechando la enorme popularidad de Windows para escritorio; una estrategia que sin lugar a dudas ha redituado grandes ganancias, y todo por una estrategia comercial.

De hecho LanServer en su momento, era una licencia de Microsoft para utilizar este software, al igual que el caso de 3+Open. Así mismo el LanServer siempre era una versión anterior al LanManager, es decir, si LanManager era la versión 2.1, LanServer era el equivalente de la versión 2.0.

El protocolo principal de Windows NT se denomina NetBEUI, que es una versión mejorada de NetBios. NetBEUI es un protocolo cuya característica principal es que no puede ser ruteado, por lo que en caso de requerir enlace entre redes locales vía ruteadores se requiere agregar o cambiar a TCP/IP, mismo que también soporta.

En lo que a protocolos concierne, Windows NT hace más transparente el uso de varios de ellos en forma simultánea, incluso del mismo IPX, ya que Windows NT presenta una característica con la que permite acceder simultáneamente a un servidor Windows NT y a otro servidor Netware, proceso que no permite Netware; sin embargo, esto es totalmente comercial, ya que quien posee la mayor base instalada de sistemas operativos de redes locales es Netware, y a quien le interesa conectarse a lo que ya existe es a Windows NT, no a Netware.

Comparación entre Netware y Windows NT.

Como se puede apreciar en párrafos anteriores, la diferencia entre Windows NT y Netware es realmente poca; entonces ¿Cual de los dos se debe elegir?

La decisión no puede ser por comparación, ya que dependiendo la situación, la experiencia previa, el gusto, las necesidades, la plataforma actual, etc. será el sistema operativo que se elija.

Es importante indicar que para empresas medianas que tengan alrededor de 20 sistemas operativos de red interconectados, y no se estén utilizando bases de datos para llevar el negocio de la empresa, no existirá una gran diferencia. En lugares en donde se tenga dos o tres sistemas operativos de red, donde el sistema no dependa de tiempo de respuesta, la diferencia de sistemas operativos no es muy visible ni medible.

La pregunta original ¿Cual de los dos sistemas operativos se debe elegir?, sigue en pie; sin embargo la respuesta es ahora más sencilla, el mejor es aquel sistema operativo que cubra la mayoría de mis necesidades y que lo que no llegue a cubrir se pueda realizar por un tercer producto. Por lo que la pregunta cambia a otro punto, que nos lleva a la aplicación, no al sistema operativo, y entonces la pregunta es: ¿La aplicación seleccionada en qué NOS opera mejor? por supuesto es necesario contemplar la plataforma actual para complementar el entorno y poder elegir adecuadamente.

Con la finalidad de apreciar a detalle las diferencias entre estos sistemas operativos de LAN se presenta a continuación un cuadro comparativo entre ambos:

Las siguientes páginas le ofrecen un listado comparativo detallado entre los sistemas operativos Windows NT Server 4 y NetWare 4.1. Este cuadro comparativo está basado en la información publicada por Novell así como en la implantación actual de sus productos. La simbología utilizada en cada línea es:

✓Significa que esta característica está incluida en el producto (con excepción de las específicamente marcadas).

Es importante hacer notar que dentro de lo incluido en la tabla, algunas de las características, sí son posibles de realizar; sin embargo, esto se logra con soluciones de terceros, es decir, el producto o el fabricante, no cuentan, por sí mismos con la solución.

Tabla Comparativa Entre Windows NT y Netware.

	Windows NT Server 4.0	*NetWare 4.1*
Arquitectura:		
Sistema operativo multi-usuario	✓	✓
Procesadores– Intel	✓	✓
Procesadores– RISC	MIPS, DEC Alpha AXP, PowerPC	
Multiprocesadores simétricos	✓arriba de 32 Procesadores	
Multiprocesamiento asimétrico		
RAM mínimo	16 MB	8 MB
RAM máximo	4 GB	4 GB
Máximo de usuarios conectados	ilimitado	1000
Sistema operativo de 32-bits	✓	✓
Búsqueda dinámica de servicios	✓	✓
Protección de memoria para aplicaciones	✓	
Alertas para auditoría	✓	✓
Subsistemas protegidos	✓	
Sistemas de archivo instalables	✓	✓
Soporte NIC - Al Cliente:		
Soporte Ethernet de 16 bits	✓	✓
Soporte Ethernet de 32 bits	✓	✓
Soporte Token Ring de 16 bits	✓	✓
Soporte Token Ring de 32 bits	✓	✓
Soporte NDIS	✓	✓
Soporte ODI	✓	✓
Soporte de drivers de terceros	✓	✓
Soporte NIC - Al Servidor:		
Soporte Ethernet de 16 bits	✓	✓
Soporte Ethernet 32 bits	✓	✓
Soporte Token Ring de 16 bits	✓	✓
Soporte Token Ring de 32 bits	✓	✓
Soporte NDIS	✓	
Soporte ODI		✓
Soporte de drivers de Terceros	✓	✓
Múltiples adaptadores de Red	✓	✓
Soporte de otro hardware:		
CD-ROM	✓	✓
Adaptadores SCSI	✓	✓
Plotters	✓	✓
Scanners	✓	
Transportes:		
IPX	✓	✓
IPX Dial-in	✓	✓
"Packet Burst"	✓	✓
LIP	✓	✓
AppleTalk	✓	✓ (costo extra)
NetBEUI	✓	
TCP/IP (tunneling)		✓ (para 500 usuarios)
TCP/IP (nativo)	✓	
OSI	✓ (en Win32 SDK)	
DLC	✓	✓
Internal routing	✓Solo RAS	✓

	Windows NT Server 4.0	NetWare 4.1
Sistema de archivos:		
Número máximo de archivos protegidos	ilimitados	100K
Número máximo de archivos abiertos	ilimitados	100K
Tamaño máximo de archivos	17 billones de GB	4 GB
Compresión de archivos	✓	✓
Sistema de transacción basada en archivos	✓	✓
Soporte de archivos DOS	✓	✓
Soporte de archivos Mac	✓	✓
Soporte de archivos OS/2	✓	✓
Soporte de NFS	✓ de Terceros	✓con costo extra
Volúmenes distribuidos	✓	✓
Almacenaje total en disco	408 millones TB	32 TB
Volumen máximo en el servidor	25	64
Tamaño máximo de la partición	17,000 TB	medida del drive
Tamaño máximo del volumen	17,000 TB	32 TB
Largo máximo de nombre de archivos	255	255
Optimización de Rendimiento:		
Cache dinámico	✓ 1GB por proceso	(cache estático)
Elevator seeking	✓	✓
Memoria cache de lectura adelantada	✓	✓
Escritura en background	✓	✓
Búsquedas en overlapped	✓	✓
Búsquedas en split	✓	✓
Directory hashing	✓	✓
Directory caching	✓	✓
File caching	✓	✓
Memoria Virtual	✓	
Memoria Retornable	✓	✓
Data scattering		✓
Seguridad:		
Diseñada en el nivel de seguridad C2	✓ Libro Rojo ✓ Libro Naranja	✓ Libro Rojo Libro Naranja N/D
Login único a la red	✓	✓
Logon único de seguridad	✓	✓
Restricción mínima del largo del password	✓	✓
Password encriptado	✓	✓
Packet signing (secure authentication)	✓	✓
Password aging	✓	✓
Password histórico	✓	✓
Account lockout	✓	✓
Login restringido a estaciones de trabajo específicas	✓	✓
Login de cliente reemplazable	✓	✓
Límite en el número de conexiones concurrentes de un mismo usuario		✓
Login restringido por hora y día	✓	✓
Fecha de caducidad de cuenta	✓	✓
Desconexión en tiempo de acceso vencido	✓	✓
Derechos de administración configurable	✓	✓
Auditoria de seguridad centralizada	✓	
Alertas en eventos de seguridad	✓	
Auditoria en el sistema de archivos	✓	✓

	Windows NT Server 4.0	NetWare 4.1
Derechos de Archivos y Directorios:		
Lectura	✓	✓
Escritura	✓	✓
Ejecución	✓	✓
Borrado	✓	✓
Cambio en permisos (Grant)	✓	✓
Propiedad	✓	✓
Ultimo directorio	✓	✓
Creación de archivos en directorios	✓	✓
Derechos del usuario:		
Respaldo de archivos y directorios	✓	✓
Restauración de archivos y directorios	✓	✓
Shutdown local del sistema	✓	✓
Forzar el shutdown remoto	✓	✓
Carga y descarga de drivers de los dispositivos	✓	✓
Manejo de bitácoras de auditoría y seguridad	✓	
Toma de propiedad en archivos y otros objetos	✓	✓
Auditoria de Seguridad:		
Auditoria de seguridad en transacciones de usuarios	✓	✓
Auditoria de seguridad de transacciones de archivos	✓	✓
Auditoria en transacciones de administrador	✓	✓
Auditoria en estadísticas de creación de archivos	✓	✓
Auditoria en estadísticas de volumen	✓	✓
Filtros de bitácoras de auditoria	✓	✓
Auditoria de cambios y políticas de seguridad	✓	
Auditoría para apagar o reiniciar el sistema	✓	✓
Servidor No dedicado	✓	con add-in de OS/2
Impresión:		
Puerto de impresión remoto a la estación de trabajo	✓	✓
Servicios de impresión peer		
Asignación de prioridades de impresión queue	✓	✓
Múltiples quedes en una sola impresora	✓	✓
Múltiples quedes en múltiples impresoras	✓	✓
Múltiples impresoras en un queue	✓	✓
Soporte PostScript	✓	✓
Capacidad máxima para compartir impresoras por servidor	ilimitada	255
Manejo remoto de queue	✓	✓
Soporte de múltiples formas		✓
Soporte de impresora conectadas directamente	✓	✓
Informa al usuario el fin del trabajo de impresión	✓	✓
Notifica al operador problemas de impresión	✓	✓

	Windows NT Server 4.0	*NetWare 4.1*
Alertas de impresión:		
Papel agotado	✓	✓
Solicitud de impresión eliminada	✓	✓
Solicitud de impresión completa	✓	✓
Impresora fuera de línea	✓	✓
Papel atascado	✓	✓
Requiere una forma específica		✓
Reporte de error de configuración en usuarios específicos		✓
Administración de la Red:		
Utilerías de comandos en línea	✓	✓
Utilerías GUI	✓	✓
Administración remota, rendimiento y monitoreo de eventos	✓	✓
Administración asíncrona remota	✓	✓
Instalación Remota	✓	✓
Actualización Remota	✓	✓
Servicios correctivos remotos	✓	✓
Sesión de seguridad remota	✓	✓
Módem con regreso de llamada remota	✓ con costo extra	✓con costo extra
Soporte DHCP para TCP/IP	✓	
Soporte WINS para TCP/IP	✓	
Monitoreo del Rendimiento:		
Porcentaje en uso del CPU	✓	✓
Uso total de los privilegios sobre el CPU	✓	
Total del uso del CPU	✓	
Vista de la lógica del uso de disco	✓	✓
Vista física del uso de disco	✓	✓
Vista del uso de cache	✓	✓
Vista de paquetes/bytes enviados	✓	✓
Vista de fallas por segundo	✓	
Vista del número de procesos activos	✓	✓
Vista del número de "threads" activos	✓	
Vista del tiempo-procesador por proceso	✓	
Vista del tiempo del procesador por "thread"	✓	
Estadísticas extensas de rendimiento	✓	
Delegación de responsabilidades de administración:		
Operación contable	✓	✓
Operación de respaldo	✓	✓
Administración de directorios	✓	✓
Administrador de empresa	✓	✓
Operador de impresión	✓	✓
Operador de réplica	✓	
Operador del servidor	✓	✓
Mensajes de Alerta:		
El volumen se está saturando	✓	✓
El volumen está saturado	✓	✓
Error la bitácora está saturada	✓	✓
Conexiones agotadas	✓	✓
Memoria disponible para los recursos agotada	Alerta de memoria virtual baja	✓
Utilización de disco fuera de límites	✓	✓

	Windows NT Server 4.0	*NetWare 4.1*
Tolerancia a fallas:		
El sistema recupera el archivo de bitácora	✓	
Estructura de directorios redundante	✓	✓
Verificación de directorios durante el encendido	✓	✓
Verificación leer antes de escribir	✓	✓
Reparación urgente (Hot fix)	✓	✓
Recuperación/undelete	✓ (solo FAT)	✓
Soporte UPS	✓	✓
Duplicado de discos	✓	✓
Disco espejo	✓	✓
Software RAID 5	✓	✓
Servidor Espejo		✓
Dynamic volume sets	✓	
Respaldo:		
Respaldo/recuperación del disco del servidor con seguridad	✓	✓
Respaldo en línea para archivos de cuenta	✓	
Utilerías de respaldo incluidas	✓	
Respaldo de estaciones de trabajo (Windows for Workgroups, Windows NT Workstation)	✓	✓ TSR
Servicio de réplica automática de archivos	✓	
Agenda de trabajo del Servidor	✓	

Con la finalidad de ofrecer diferentes puntos de vista con respecto a estos dos productos, se presentan a continuación dos comparaciones efectuadas por compañías ajenas tanto a Novell como a Microsoft.

Comparación Según Windows Magazine

Opción	NetWare 4.1	NTServer 4.0
32 bit Multitask OS	Si	Si
Capacidad	4Gb RAM 32Tb disco	4Gb RAM 408millonesTB
Max conexiones por Servidor	1000	10,000+
Max impresoras por Servidor	256	ilimitado
Soporte SMP	Si	Si
Servidores Redundantes	SFT-III	No
Encripción	RSA	DES
Login	Red	Dominio
X.500	Si	No
MHS	Si	No
Mover	Drag & Drop	Borra/Recrea
Administración por teléfono (dial-up)	Si	Si
Distribución de Software	Agregado	Agregado
Dynamic Device Management	Si	Limitado
Storage Managment	Si	Limitado
Prioridad Tiempo-Real	No	Si
Soporte ODI	Cliente y Servidor	Solo Cliente
OLTP	Tuxedo	Terceros
Actualización Remota	Si	Limitada (Vía SMS, con operador)
Consola de Administrador	DOS, Windows, OS/2, Mac	Windows, Windows NT, Windows 95
Requerimientos Mínimos	386 6Mb	386 16Mb
Tolerancia a Fallas en disco	Espejo, Duplexing, RAID, SFT-III	Espejo, Duplexing, RAID,
Compresión en disco	Si	Si
Tamaño máximo de bloque	64Kb	4Kb
File Recovery luego de borrado	Limitado	Terceros

Comparación Según PCWeek Labs

Opción	NetWare 4.10	Windows NT 4.0 Server
DESEMPEÑO		
Archivos e Impresión	Excelente	Bueno
Servidor/Aplicaciones	Buena	Excelente
Escalabilidad	Buena	Excelente
Ajuste	Excelente	Regular
INSTALACION		
Cliente	Buena	Buena
Distribución	Regular	Regular
Instalación del NOS	Buena	Excelente
Facilidad de actualización del NOS	Excelente	Buena
SOPORTE DE CLIENTE		
Recursos requeridos	Buena	Buena
Acceso Remoto	Excelente	Excelente
ADMINISTRACION		
Admon. Remota	Excelente	Buena
Alertas y alarmas	Buena	Excelente
Scripting a tiempos	Excelente	Buena
Control dispositivos	Regular	Buena
SEGURIDAD		
Seguridad	Excelente	Excelente
ADMINISTRACION EN CORPORATIVOS		
Integración a WAN	Buena	Buena
Servicio Directorios	Excelente	Buena
Protocolos	Excelente	Excelente
Integración a Mensajería	Buena	Excelente
Escalabilidad	Buena	Buena

Esta última tabla cuenta con una evaluación muy subjetiva; sin embargo, se presenta con la finalidad de contar con la mayor cantidad de información posible, para que quien decida elegir un sistema operativo sobre la base de esta tesis, tenga la mayor información posible.

CAPÍTULO 10

Administración de la Red Local.

Temas del capítulo.

10.1 Funciones del administrador de una red local.

10.2 Información que debe poseer el administrador de la red local.

10.3 Herramientas que debe poseer el administrador de la red local.

10.4 Administración total de sistemas.

La administración de las redes locales (LANs) es, aunque no lo parezca, el punto fino de la operación de las mismas. Mediante una buena administración y planeación se podrá, por ejemplo, garantizar la fácil localización y corrección de posibles fallas en el sistema, lo que permitirá tener una mayor continuidad en la operación de la LAN que estemos administrando.

Al tener cualquier tipo de falla en nuestra LAN puede ocurrir que se detengan por minutos, horas o días las funciones de nuestra oficina, ocasionando pérdidas realmente cuantiosas. En Estados Unidos existen antecedentes de casas de bolsa que paralizaron sus operaciones bursátiles debido a fallas en su LAN, por lo que las pérdidas que esto ocasionó fueron realmente cuantiosas.

El carecer de una buena administración es el equivalente, valga la comparación, a tener un automóvil y no saber que necesita aceite, agua, gasolina,

etc.; es decir; lo utilizaremos, pero al primer problema que se presente no se sabrá qué hacer; esto por supuesto acarreará muchos gastos y pérdidas de tiempo, y no solo eso sino que para corregir cualquier problema se requiere de los servicios de un consultor sobre LANs, provocando con esto estar sujetos a los conocimientos de este tipo de personas o proveedores de este servicio.

La función de administrar una LAN generalmente requiere una sola persona. En caso de tener una LAN muy grande o una MAN (Metropolitan Area Network) o una WAN (Wide Area Network) se necesitará un grupo de personas que realicen las funciones de administración. El administrador de LAN es en quien recae la responsabilidad de solucionar todos los problemas que puedan ocurrir en una LAN. Por lo anterior, concluimos que no puede existir una red sin administrador.

Por supuesto, existen herramientas de administración especializadas para cada ambiente, y aunque estas herramientas son de mucha ayuda, no lo hacen absolutamente todo; se requiere de una persona o de un grupo de personas que sean los responsables de interpretar la información y de tomar decisiones con respecto a esta plataforma de comunicaciones, por lo que se deberá contar con la administración de una LAN como una función, ya que al tener una o varias LANs, quien garantiza su funcionamiento es quien posee dicha función de administración.

En el proceso de implantación de una LAN es necesario obtener cierto tipo de información, así como efectuar ciertas tareas importantes que garanticen que la implantación que se efectúe será adecuada.

Como pasos iniciales para mantener esta plataforma funcionando, se encuentran ciertas tareas, mismas que permitirán hacernos la vida más fácil en caso de que surjan fallas posteriores a la instalación; algo nada raro, ya que sabemos que las fallas ocurrirán no importando que tanto hagamos para no tenerlas; sin embargo, si estamos prevenidos para cuando llegue el momento de enfrentarnos a algún problema, el mismo será resuelto con mayor rapidez.

Las tareas a realizar son las siguientes:

- Designar al administrador de la LAN y sus funciones.
- Hacer el diagrama de ubicación de componentes de la LAN.
- Realizar la definición de nombres de usuarios.
- Estructurar adecuadamente los directorios del servidor.
- Asignar privilegios y restricciones a usuarios.
- Definir utilerías de administración.
- Generar documentación.
- Elegir las herramientas del administrador.

A continuación se desarrollará cada uno de los puntos anteriores, mencionándose puntos adicionales que apoyen los conceptos anotados anteriormente.

10.1 Funciones del administrador de una red local.

Es muy importante designar desde un principio y de manera formal a la persona que se hará cargo de la administración, monitoreo y control de la LAN. No debe hacerse de manera informal. Nuestro candidato a administrador deberá estar consciente y perfectamente enterado del trabajo que desarrollará en esta nueva actividad. Es recomendable que sea voluntario pero si no es así, de cualquier manera habrá que elegir uno, y no solo de nombre, sino realmente deberá cumplir con su papel, ya que es un trabajo que por momentos parecerá que no termina. La actividad del administrador de LAN le "robará", en un inicio, aproximadamente 50 % de su tiempo o más; sin embargo, conforme los usuarios y él mismo se especialicen en esta nueva herramienta, solo le quitará a lo mucho una hora diaria (en caso de tener todo perfectamente organizado y de que cuente con las herramientas de administración adecuadas), habiendo días que no realice actividades de administración; sin embargo, el hecho de que solo al principio requiera de mayor tiempo no quiere decir que si se le proporciona capacitación, la misma será aprovechada solo en un inicio, sino que al tomar mayor experiencia sobre este asunto requerirá cada vez de menor tiempo.

Se recomienda que quien efectúe toda la instalación y configuración del sistema operativo en el servidor de archivos sea el administrador; por supuesto con la supervisión adecuada y evidentemente que para poder realizar esto, se deberá previamente haber tenido una capacitación formal.

A continuación se definirán en forma general las funciones que debe cubrir un administrador de LAN:

El administrador de LAN se encargará de planear, programar, organizar, integrar, implementar, mantener, verificar y adecuar los recursos y elementos que conformen la LAN a su cargo; hablando en general de: software, hardware, información y usuarios. En pocas palabras es el encargado de todo lo que se involucre con la LAN a su cargo.

Es por demás adecuado que sea una persona que posea experiencia en todo lo relacionado a software y hardware en el ambiente elegido, y que posea conocimientos sobre comunicaciones, ya que lo que hará finalmente será mantener en funcionamiento canales de comunicación entre los usuarios. El hecho que una LAN involucre PCs, no quiere decir que sea una labor fácil, ya que al adentrarse en este mundo se verá la necesidad de tener conocimientos a detalle, al menos de los conceptos, del funcionamiento de PCs y periféricos, sin excluir por supuesto al software.

Como se podrá observar, en el administrador de la LAN recae toda la responsabilidad de la operación y buen funcionamiento de una plataforma de este tipo.

Algunos de los puntos que deberán llevarse a cabo al implementar una red local son:

- Etiquetado de cables.

Aun teniendo los diagramas de cableado, es muy recomendable tener etiquetado cada extremo de cable, ya que al momento de llegar físicamente a ver los cables, el diagrama ya no ayudará lo que nosotros quisiéramos.

Es conveniente tener una etiqueta código, es decir, la forma en que se identificará cada extremo de cable. Puede haber diferentes formas de identificar los extremos; por ejemplo, con colores o números iguales en un mismo cable, o indicando el nombre de la persona, estación de trabajo o componente que se encuentre en el otro extremo; aquí lo importante es identificar cada cable, no importando como se realice; sin embargo, lo que sí es importante es que al elegir el código a utilizar, este se dé a conocer, y se utilice como estándar en la organización.

Se debe elegir un buen material para las etiquetas, ya que si estas se llegan a desprender se empezará a tener problemas; por tal motivo no se recomienda utilizar etiquetas de papel. Existen etiquetas de cartón, plástico y metal. En el caso de las etiquetas de cartón se recomiendan las que cuentan con arillo metálico, ya que este proporciona una protección. Las etiquetas de plástico tienen la característica de poder escribir sobre estas solo con plumón. Para las etiquetas de metal es necesario contar con una pequeña máquina para el

grabado. Las etiquetas de cartón normalmente se fijan al cable por medio de un cordón por lo que resultan poco seguras, situación que se pueda agravar si por cuestiones de aseo se moja el cartón. Las etiquetas de metal son muy seguras, aunque un poco difíciles de colocar, sin contar con que es necesario cargar con el rotulador. En el caso de las etiquetas de plástico, estas son muy fáciles de colocar y muy seguras, ya que si se utiliza el plumón adecuado, resultan indelebles.

Cuando el cable recorre distancias considerables, se recomienda que se encuentre identificado en toda su trayectoria, sobre todo en los registros, ya que si existe alguna falla, estas etiquetas serán la única forma sencilla en que se pueda identificar el cable.

Existe una buena cantidad de elementos que los fabricantes de cableado han desarrollado para la identificación adecuada de los cables, por lo que se recomienda que estos elementos sean utilizados. Entre algunos de los elementos de identificación se encuentran los propios del cableado estructurado, en donde se indica el tipo de servicio (voz, datos o vídeo) que el cable provee.

Al momento que se detecte que alguna etiqueta se ha desprendido, será necesario remplazarla inmediatamente, ya que con el transcurso del tiempo empezaremos a tener más de un cable sin etiqueta, y será un poco tardado determinar a donde va dicho cable. Aunque esto no parezca muy importante, si lo es, ya que el verificar el cableado de una LAN que abarque 4 pisos y aproximadamente 70 nodos, se llevarán, dos personas, de cuatro a cinco días, sin corregir fallas, solo haciendo una detección de las mismas y levantando un diagrama de como se encuentra el cableado, y por supuesto este trabajo lo deberá realizar personal muy capacitado. Esto realmente nos da una pauta de la importancia que posee la información que podamos tener sobre un cableado de LAN.

- Respaldo de información.

Como todos los discos duros, el que se encuentra en el servidor puede llegar a dañarse o llenarse; por tal motivo es recomendable tener un buen sistema de respaldo de información, mismo que, en muchos casos, nos podrá sacar de apuros, si es que se llega a perder información del disco duro. Por otro lado si la información no se pierde, llegará el momento de que el disco duro se llene y no se pueda seguir trabajando en él, por lo que si se tiene un sistema de respaldo histórico se podrá ir borrando del servidor la información más vieja o la que menos se consulta. Para poder determinar esto último existen utilerías de los sistemas operativos de LAN que permiten saber qué información no ha sido accedida desde tal o cual fecha, permitiéndonos con esto determinar los archivos a respaldar o de plano, los que se decida borrar.

El sistema de respaldo nos permitirá resguardar información que sea útil pero que no necesitemos accesar constantemente; por ejemplo, el presupuesto del año anterior, cartas de entrega de equipo, la planeación del año anterior, etc. Si se desea tener una gran cantidad información (mayor a 2 Gbytes) en línea, se puede conectar un equipo llamado *mass storage*, mismo que, dependiendo del modelo y fabricante puede almacenar hasta 600 Gbytes en discos compactos.

Los respaldos de información se pueden programar cada semana, cada quincena, cada mes o como se requiera, dependiendo de la importancia de la información generada o de la cantidad de la misma.

Existen diversos sistemas de respaldo, desde el más común como es el disco flexible o hasta el más complejo como el disco óptico, pasando por los respaldos en cintas magnéticas.

Existen sistemas de respaldo muy sofisticados, que se basan en un concepto denominado HSI (herarquical storage information), concepto que

permite guardar la información en diversos medios dependiendo de su utilización; es decir, se coloca en el disco duro del servidor la información que tiene no más de tres meses, en disco óptico la que tiene de tres meses a un año y en cinta la que tiene un año o más.

- Planeación de mantenimientos preventivos.

Sabemos que todos los equipos deberán ser limpiados periódicamente, y no solo limpiados sino incluso acondicionados adecuadamente, como el caso de las cabezas de las impresoras que deben estar a una distancia adecuada del papel. Para todo esto es adecuado contar con los servicios de una empresa que le proporcione mantenimiento preventivo, y de ser posible correctivo, a los equipos. El servicio que se contrate debe abarcar algo más que la limpieza del teclado y de las cabezas de los discos flexibles, como es el limpiar cada CPU internamente, verificación de cableado, etc.

Es por demás conveniente revisar con un detector de virus los discos flexibles que utilicen los técnicos que proporcionen el servicio de mantenimiento, ya que los discos flexibles que se utilizan, son usados en muchísimos otros equipos que probablemente no pertenezcan a su empresa, y que tienen una gran posibilidad de estar infectados por algún virus.

La fecha programada para dar mantenimiento a los equipos deberá ser dada a conocer a todos los usuarios con al menos dos semanas de anticipación, ya que esto permitirá que se planeen las actividades y se aproveche el tiempo en funciones que no requieran el uso de la microcomputadora, impresora o incluso de la LAN. No se debe excluir al servidor de estos mantenimientos.

- Componentes de respaldo.

El hecho que sepamos detectar problemas, no implica que los podamos solucionar, ya que muchas veces no contamos con la pieza o el equipo de repuesto apropiado. Se debe contar con NICs, repetidores, MAUs, concentradores, bridges, routers, cable, conectores, terminadores, etc. Este equipo permitirá continuar con la operación de su LAN si alguno de los componentes llegara a fallar.

La mejor forma de negociar esto es solicitando al proveedor de este equipo que podamos tener en nuestras oficinas un stock de equipo, mismo que podrá se facturado al momento que lo utilicemos y la garantía del equipo substituido esté vencida. Por supuesto para poder hacer esto se deberá haber adquirido una gran cantidad de equipo, ya que de otra manera el proveedor seguramente se negará a esta petición.

- Bitácora de fallas y soluciones.

En el caso de que surjan fallas en la LAN, se deberá documentar el problema tanto como sea posible. Esto ayudará a entender en detalle el problema. Se deberá anotar hora, fecha, configuración del equipo respecto a software y hardware y qué es lo que se estaba haciendo cuando sucedió el problema. Cuando se encuentra la solución se deberá adicionar la misma al planteamiento del problema, indicando paso a paso las acciones que se deben seguir para llegar a la solución. Lo anterior permitirá, posteriormente, solucionar fallas similares y hasta intercambiar experiencias con otros usuarios de LANs.

Esta bitácora de fallas permitirá llevar estadísticas de fallas por equipo, lo que le dará una pauta para el equipo o piezas de respaldo que deberá tener.

Adicionalmente se recomienda formar una biblioteca de manuales de cada componente de la LAN y adicionar a cada uno de estos manuales las referencias de problemas que se han presentado.

- Verifique que las NICs tengan números de nodo únicos.

No importando qué arquitectura posea una LAN, cada tarjeta de LAN debe poseer un número, llamado dirección MAC; misma dirección que debe ser diferente a todas las demás, sin importar el tamaño de la LAN. Para garantizar esto, los fabricantes se han puesto de acuerdo para la numeración que deben asignar a sus NICs (direcciones universalmente administradas); sin embargo, los fabricantes permiten que los usuarios tengan la facilidad de cambiar esta dirección (direcciones localmente administradas), por lo que se recomienda que estos números jamás sean cambiados, ya que si esto sucede, se deberá garantizar que ninguna dirección esté repetida, ya que en caso de que esto suceda, la LAN dejará de funcionar. Es conveniente que después de instalar la LAN, se verifique la dirección MAC de cada nodo. El software de monitoreo que se utiliza para la administración de LANs, al reportar los errores o problemas que detecta, los documenta de acuerdo a la dirección MAC del dispositivo que esté involucrado, por lo que se recomienda que se documente la dirección MAC que posee cada tarjeta de LAN instalada en cada equipo, inclusive los repetidores, bridges y routers poseen dirección MAC, así como dispositivos para impresión, como el LANPort, o cualquiera que sea equivalente, es decir, cualquier dispositivo conectado a la LAN posee una dirección MAC que permite identificarlo dentro de la misma, por lo que todos los equipos deberán documentarse.

10.2 Información que debe poseer el administrador de la red local.

El hecho de contar con un buen administrador de LAN es una ventaja; aunque no lo es todo, ya que adicionalmente es necesario contar con una perfecta organización en la información referente a la LAN, que permita desarrollar esta función y contar con información actualizada y a la mano, todo con la finalidad de permitir efectuar sin obstáculos mayores la función de administración.

La información que deberá poseer quien desempeñe el cargo de administrador de LAN es la siguiente:

- Diagrama de ubicación de los componentes de la LAN.

Es indispensable contar con diagramas que indiquen la localización exacta de los diversos componentes que conforman nuestra LAN, como podrían ser: estaciones de trabajo, servidor, MAUs, routers, transceivers, repetidores, gateways, data base server, server de comunicaciones, concentradores, terminadores, cableado, etc. Esto permitirá localizar fácilmente fallas de cableado, substitución de algún componente o aislar zonas de falla.

Se recomienda que este mapa posea un 100% de veracidad, ya que la mayoría de las veces este punto se efectúa, pero al paso del tiempo se desactualiza y se posee un esquema totalmente erróneo, pudiéndose dar el caso de que la persona encargada de esta LAN esté de vacaciones o en el peor de los

casos ya no labore en la empresa, por lo que difícilmente se podrá obtener esta información si no se tiene actualizada, principalmente lo referente a cableado.

- Definición de usuarios.

Es importante realizar una lista de los usuarios que tendrán acceso a la LAN; esto permitirá hacer grupos de usuarios que tengan necesidades similares de acceso, derechos o una configuración en especial; por ejemplo, se puede crear un grupo llamado *administración*, este grupo tendrá acceso a cierto tipo de software e información como podría ser nómina, contabilidad, etc., y otro grupo llamado *desarrollo*, que tendrá acceso a compiladores, utilerías de desarrollo, etc., y no solo ayudará para la asignación de derechos en cuanto a software, sino para permitir el uso de periféricos, o de asignar horarios de trabajo. El realizar grupos de trabajo nos ahorrará tiempo en la asignación de restricciones y derechos en el sistema operativo y mejorará el control que tengamos sobre los usuarios y recursos de la LAN.

El administrador de la red Local, al hacer uso de los recursos de la LAN deberá separar perfectamente sus funciones de administrador y de usuario del sistema, ya que él mismo es usuario y administrador. Esta recomendación se debe a que el sistema operativo asigna a cada archivo creado o copiado un propietario, y si el administrador es propietario de todos los archivos se perderá control sobre el servidor; inclusive podrá llegar el caso de no saber si los archivos pertenecen al sistema operativo o son de la persona que ejerce la función de

administración. Otra razón de peso es que en un momento de descuido, el administrador, al no tener restricciones sobre archivos y directorios pudiera borrar información importante. Por tales motivos es recomendable que el administrador de LAN tenga dos nombres de usuario para acceso a la LAN, uno llamado, por ejemplo ADMIN y otro su propio nombre de usuario, uno para cada función que se encuentre desempeñando. Incluso es adecuado que se tenga un usuario con derechos similares al ADMIN, pero que su clave de acceso (password) este bajo llave, esto debido a que es relativamente frecuente que se pierdan la clave del ADMIN.

¿Con qué nombre o identificador se debe reconoce a los usuarios en una LAN? Existen diferentes formas de hacerlo, desde las más sencillas, como asignarle un número a cada usuario (que realmente no nos ayudará mucho), hasta la identificación más significativa, como el asignar ocho letras de su apellido paterno o algo similar que permita identificar fácilmente a nuestros usuarios. Existe por supuesto quien prefiere asignar nombres genéricos debido al alto índice de rotación que pudiera tener entre sus empleados; aunque si hablamos de corporativos e instituciones en donde el personal permanece un tiempo considerable, es por demás conveniente que los usuarios se den de alta de acuerdo a su nombre. Esto adicionalmente permitirá tener mayor control sobre los archivos que se encuentren en el servidor, así como el diseño, en caso de llegarse a tener, de correo electrónico o Internet.

- Estructura de directorios.

Una buena estructura de directorios permitirá tener un tiempo menor de acceso a las aplicaciones. La idea principal de la organización de discos duros es crear una estructura de directorios de acuerdo a funciones o estructuras de la entidad que haga uso del servidor de archivos.

Existen diversas formas de organizar un directorio; sin embargo, la más común consiste en tomar las funciones más significativas que se realicen entre los usuarios de la oficina u organización; por ejemplo, administración, ventas, almacén, etc., o de acuerdo a la organización jerárquica que posea la empresa. Se deberá tener en cuenta que la organización será de tal forma, que cualquier usuario pueda encontrar rápidamente los archivos y/o directorios que se encuentren en el servidor de archivos. De hecho se puede uno apoyar en los grupos de trabajo creados anteriormente para efectuar la estructura de directorios, permitiendo con esto tener la estructura lógica realizada con el sistema operativo de LAN igual a la estructura de directorios del disco duro del servidor de archivos; aunque eso no es todo ya que también se deberá contemplar el software que se utilizará, así como directorios de información.

Al efectuar una estructura de directorios es recomendable considerar cuatro áreas de trabajo; una de ellas se implementa automáticamente, misma que corresponde al área de sistema operativo, con lo que quedan tres áreas por definir, estas son:

1. Area de trabajo de usuarios.

2. Aplicaciones comerciales y caseras.

3. Información y datos.

A continuación se explicará únicamente la función del área de trabajo de usuarios, ya que los puntos dos y tres se explican por si mismos.

1. Area de trabajo de usuarios.

En el desarrollo de proyectos o funciones se recomienda que la información se encuentre bajo un responsable, concentrando así en la cuenta de una persona toda la documentación inconclusa, y al terminar el proyecto o documento, dicha información podrá pasar a un área común de consulta, donde cualquier usuario (con derechos) podrá accederla sin ningún problema. Es decir, se considera que esta área asignada a usuarios es un área transitoria, donde los archivos que ahí se encuentran no están terminados. Si esta área no se crea, se podría dar el caso de tener una cantidad considerable de información y datos importantes, que nadie podrá acceder, o en el peor de los casos, ni siquiera se conocerá su existencia.

Si cada usuario tiene su propia área de trabajo, se podrá tener mayor control sobre la información contenida en el servidor, evitando con esto tener documentación repetida y/o basura. Es recomendable asignar un espacio en el disco duro del servidor, y que este espacio no sea aumentado, ya que de lo

contrario significará que existe documentación, que podría ser importante, sin compartir con otros usuarios.

A continuación se muestra una propuesta de estructura de directorios, que por supuesto puede variar dependiendo de las necesidades de cada usuario.

```
RAIZ/
USUARIOS/
        ADMON/
                CORTEGA
                CTINOCO
                LFERRER

        DESARROL\
                AALVAREZ
                JPEREZ
                PLOPEZ

        VENTAS\
                ANAVA
                CLANDA
                LSILVA

APLICA/
        WINDOWS/
                DESIGNER
                EXCEL
                PRESMANA
                WINWORD

        NOWINDOW/
                WORKS
                WORD5
                LOTUS
                HG
                FLANCE

        UTILERIAS/
                PCTOOL
                NORTON
                SLEUTH
                DVIRUS

INFORMA/
        NOMINA
        CONTABIL
        FORMAS
        CARTAS
        GRAFICAS
        ESTADIST
```

Los únicos que podrán acceder estas áreas de usuarios sin restricciones son el administrador de la LAN y el usuario propietario del área.

El directorio de APLICA servirá como un depósito común de aplicaciones; las mismas podrán ser accedidas por los usuarios que así lo requieran; pero nadie tendrá derecho a escribir o borrar en esta área.

Los usuarios al generar algún nuevo producto, terminar una evaluación, acabar una presentación, etc. deberán depositarla en el directorio INFORMA en el subdirectorio que corresponda. Este directorio (INFORMA) deberá poder ser accedido por los usuarios que hagan uso de esta información, pero con derechos solamente de lectura, con la finalidad de que no puedan borrar, solo consultar.

Una forma rudimentaria pero efectiva de ver si se tiene una buena estructura de directorios, es que podamos ver en una sola pantalla, toda la información contenida en un directorio o subdirectorio al ejecutar un DIR.

- Asignación de derechos y restricciones a usuarios.

Para asignar derechos y restricciones a usuarios no es necesario tener una buena estructura de directorios, ya que se podría considerar que una se efectúa en forma lógica y otra en forma física; sin embargo, si estas dos estructuras son similares, se podrá tener una mejor organización en la LAN; pero, aun con esto, cabe aclarar que la asignación de derechos y restricciones se efectúa directamente en el sistema operativo de LAN, y es independiente de la estructura de directorios que se tenga. Por ejemplo, los usuarios que pertenezcan al grupo

de ADMON, podrán tener derecho tanto a hojas de cálculo, como al directorio INFORMA/NOMINA, pero los usuarios que pertenezcan al grupo DESARROL (desarrolladores) no tendrán nada que consultar en la nómina o contabilidad del negocio. Como se puede apreciar la asignación de derechos y restricciones se realiza sobre la estructura de directorios que se tenga; adicionalmente se poder realizar esto sobre periféricos e incluso sobre horario de acceso al servidor.

10.3 Herramientas que debe poseer el administrador de la red local.

Para poder desarrollar la función de administración de LANs es adecuado contar con herramientas que permitan apoyar dicha función, ya que existe una gran variedad de eventos que ocurren a nivel de software, y por supuesto de hardware, que no es posible detectar fácilmente. Normalmente estos eventos suceden entre las capas dos a cinco del modelo OSI, por lo que es necesario contar con equipo que permita detectar las anomalías que ahí se presenten. Claro esto no quiere decir que no exista otro tipo de problemas, como direcciones duplicadas, cables en mal estado, cuellos de botella, generación de tráfico excesivo por diversos usuarios, discos duros del servidor a punto de fallar, tarjetas de red con errores intermitentes, etc.

Es importante mencionar que estas herramientas no solo sirven para detectar fallas, sino incluso para realizar reconfiguración de sistemas.

Utilerías de administración.

Existen en el mercado diversas herramientas, tanto de software como de hardware, que apoyarán significativamente la detección de problemas generados en la LAN; las más importantes en el mercado son: NetView de IBM, Open View de Hewlett Packard y Sun NetManager de SUN. De estas tres plataformas la más completa es la que posee Open View, ya que solo Hewlett Packard cuenta con aproximadamente 150 productos que apoyan estas funciones, y adicionalmente existe una gran cantidad de terceros fabricantes que tienen productos para esta plataforma.

Con estas herramientas podemos monitorear diversos aspecto, tanto a nivel LAN como WAN, como son: tráfico, frames recibidos, frames enviados, quién genera el tráfico, qué aplicaciones se están utilizando y por quién, monitoreo de señales satelitales, monitoreo de estaciones terrenas, etc.

Es importante saber qué tipos de errores de software se están generando y qué tan frecuente es este tipo de errores; a estos errores se les conoce como "soft errors" y su frecuencia es uno de los indicadores que se pueden tomar para determinar la magnitud del problema.

Al adquirir un monitoreador de nuestra LAN es conveniente entender todos y cada uno de los conceptos de medición que se están usando, dado que si nos dice que "X" cosa tiene "N" errores no sabremos si eso es bueno o malo, y en caso de que sea malo, qué tanto lo es, y por supuesto se deberá conocer a detalle la arquitectura que se tenga, debido a que los errores y conceptos que

maneja cada herramienta de monitoreo varían dependiendo la arquitectura que se tenga.

Adicionalmente existe equipo que permite verificar en una forma por demás sencilla la condición de un cable; esto es muy importante sobre todo por la cantidad de problemas que se generan a partir de cables en mal estado.

Otro punto importante y por demás conveniente, es adquirir un detector, protector y limpiador de virus, dado que en una LAN es factible que se propague este tipo de problemas. Es necesario asegurarse de que el antivirus elegido sea versión LAN y compatible con el sistema operativo de LAN que se esté utilizando. Mucha de la gente contamina accidentalmente sus estaciones de trabajo por no tener un buen detector de virus y sobre todo, por pensar que a ellos jamás les ocurrirá, por lo que el antivirus elegido deberá estar instalado en cada una de las estaciones de trabajo, y se deberá activar al momento de encender el equipo. Sin embargo esto no es todo, ya que adicionalmente se deberá contar con dos o tres detectores de virus de diferente fabricante, ya que en la mayoría de los casos uno solo no es suficiente. Vale la pena renovar constantemente esta herramienta, ya que cualquier antivirus de hoy no detectará los virus que se desarrollen mañana.

Por último es conveniente adquirir herramienta como: pinzas, cautín soldadura, desarmadores, cúter, etc. Esto le permitirá reemplazar NICs (Network Interface Card), cables o conectores de una forma rápida y sencilla, sin tener que esperar a que quien realizó el cableado repare las fallas. Por supuesto que si las fallas no son considerables o no son urgentes se podrá uno esperar a que llegue la gente de cableados; sin embargo el 90% de las veces es urgente, y para eso

es necesario estar preparado. Si es posible se debe contar también con un multímetro, lo que nos permitirá detectar continuidad en cables, verificar condiciones de corriente, etc.; esto será algo similar a un botiquín de primeros auxilios para la LAN.

10.4 Administración Total de Sistemas.

Cuando se tiene redes de misión crítica, o una gran cantidad de redes interconectadas, se recomienda hacer uso del concepto que denominaré Administración Total de Sistemas. Este concepto abarca los siguientes puntos:

- Help Desk.
- Monitoreo de Redes y Sistemas.
- Control de Redes y Sistemas.
- Simulación de Eventos en Redes y Sistemas.

Help Desk.

Este concepto tiene un objetivo básico: "solucionar la problemática lo más rápido posible, ya sea vía telefónica o en forma personal"; esto mismo requiere darle seguimiento a los problemas, desde la notificación del evento vía telefónica, correo electrónico o fax, hasta la conclusión del mismo.

El Help Desk debe tener personal técnico de planta atendiendo los requerimientos de los usuarios, mismo que se encarga primordialmente de diagnosticar y de ser posible solucionar telefónicamente la problemática que se presente y de asignar la solicitud al personal adecuado.

Debe haber un procedimiento de atención, scripts de bienvenida, scripts de preguntas de acuerdo a la problemática y procedimientos de escalación para cuando el problema no se puede resolver telefónicamente, para de esta manera contar con la mayor cantidad de información posible antes de asistir a solucionar el problema, y ser más efectivos en las visitas.

Se recomienda tener un conmutador que permita tener estadísticas de llamadas, para de esta forma conocer el tiempo de espera en la línea antes de recibir apoyo técnico. Este conmutador deberá permitir realizar monitoreo silencioso de llamadas, para verificar la atención del personal técnico hacia los usuarios del servicio, y poder retroalimentar al personal del help desk.

El Help Desk deberá contar con los siguientes elementos:

- Base de datos de reportes levantados.
- Manuales y documentos técnicos.
- Librerías electrónicas en discos ópticos (CDs)
- Equipo para replica de situaciones.
- Fax y correo electrónico.
- Acceso a Internet.

La base de datos permite entre otras cosas obtener estadísticas sobre; tiempo de atención de reportes, tiempo de solución de los mismos, equipos que más fallan, componente que más falla, usuarios con mayor demanda, días y horas pico de solicitud de atención, bitácora de soluciones, etc.

Las estadísticas permitirán tomar medidas como contratación adicional de ingenieros, evaluación de los ingenieros, asignación de ingenieros adicionales en horas pico, compra de refacciones y equipo de respaldo, capacitación hacia algún usuario o ingeniero, prevención de fallas en equipos, etc.

La lógica indica que el personal que se encuentre en el help desk deberá tener un perfil técnico; sin embargo, la experiencia indica que mas que contar con un técnico, deberá ser un administrador con buenos conocimientos técnicos, ya que esta labor no solo implica el tomar una reporte y diagnosticar adecuadamente el origen del problema, sino saber manejar a clientes o usuarios difíciles, coordinar personal, apoyar telefónicamente al personal técnico, investigar información, proporcionar seguimiento a reportes, generación de estadísticas, etc., tareas que si bien requieren de conocimiento técnico, el lado administrativo es el importante.

Monitoreo de redes y sistemas.

La función principal que se debe desarrollar en este rubro es obtener información de lo que está sucediendo en la red y sus dispositivos. Existe al día

de hoy una gran cantidad de software y hardware que permite apoyar este tipo de funciones. Entre los beneficios que se pueden tener se encuentran los siguientes:

- Análisis de tráfico en red (LAN y WAN).
- Análisis de protocolos en red (LAN y WAN).
- Mapa automático de todos los elementos conectados a la red (LAN y WAN).
- Volumen de información entre equipos en tiempo real.
- Estadísticas de colisiones, errores, reintentos de acceso, etc.
- Monitoreo de servidores (Intel o RISC), en cuanto a memoria, procesos, disco, etc. Algunos productos permiten monitorear hasta 256 eventos.
- Monitoreo de dispositivos, como: PCs, impresoras, UPS, unidades de respaldo, modems, repetidores, bridges, routers o lanswitches.

El monitoreo de redes implica tanto software como hardware, dependiendo del equipo que se tenga, ya que existe software que puede instalarse en ciertos equipos.

Control de redes y sistemas.

La función principal es llevar a cabo acciones en forma remota sobre los dispositivos que conforman la red, entre las que se encuentran:

- Levantamiento de inventario en forma electrónica de software y hardware.

- Aviso a localizadores personales (pagers) y/o a la base de datos para errores críticos en LAN o WAN. (líneas caídas, servidores caídos, exceso de colisiones, etc.).
- Asignación de filtros para acceso a redes.
- Administración global de correo electrónico.
- Ejecución de tareas en forma automática. (respaldo de información, borrado de archivos basura, etc.).
- Control de licencias de software.
- Reconfiguración de estaciones de trabajo en forma remota.
- Reconfiguración de servidores en forma remota, utilizando comunicación alterna a la WAN, o la misma WAN.
- Distribución, instalación y configuración de software en servidores y estaciones de trabajo en forma remota y automática.
- Control de sistemas operativos en servidores remotos, utilizando comunicación alterna a la WAN.
- Administración, control, utilización y configuración remota de elementos de red, como modems, impresoras y estaciones de trabajo.
- Manejo de redes virtuales.

El manejo de redes virtuales es un sistema que permite tener usuarios de diversas redes, formando una sola, por supuesto, en forma virtual. Esto es posible gracias a una combinación de productos de hardware y software. Al día de hoy existen muy pocos fabricantes que cuentan con esta tecnología. Con esta tecnología el usuario de una red física, puede pertenecer lógicamente a otra.

Simulación de eventos.

Una pregunta típica que se hace un administrador de red es ¿Cómo se comportará la red si se conectan N usuarios adicionales?, En caso de contar con las herramientas adecuadas, es posible responder este tipo de preguntas, con una confiabilidad del 90%.

Han salido al mercado herramientas de software que permiten llevar a cabo simulación de una gran cantidad de situaciones. Entre las situaciones que al día de hoy podemos simular se encuentran, tráfico en red, conexión de ruteadores y bridges, incluyendo sistemas operativos de red, aplicaciones típicas, etc.

Es factible armar una red en el simulador, que tenga incluso diferentes versiones de sistemas operativos de red, varios hubs de diversos fabricantes, ruteadores, líneas de comunicación con un ancho de banda predeterminado, varias redes interconectadas con N número de estaciones de trabajo, y observar el rendimiento que se puede tener, los tiempos de respuesta, etc.

Contar con una herramienta de este tipo equivale sin lugar a dudas a poseer una "bola de cristal" que nos evitará grandes dolores de cabeza.

También existen herramientas de software que contienen una opción denominada ¿Qué pasaría si . . .?, mismo que permite realizar diversos supuestos, y obtener un resultado sin tener que realizar cambios en la red.

Entre esta gama de productos existen algunos que permiten fijar criterios de desempeño de una red, y si nuestra red rebasa alguno o varios de dichos

parámetros, se lanza una alarma. Esto con la finalidad de tener nuestra red funcionando bajo un esquema deseado.

Como se puede observar, existe una gran cantidad de herramientas que permiten tener un Administración Total de Sistemas. Se calcula que al día de hoy existen cerca de 5,000 productos que tienen esta capacidad.

CAPÍTULO 11
Puntos Adicionales a Considerar al Implantar Redes Locales.

Temas del capítulo.

Los puntos tocados en el capítulo anterior permitirán ejercer la función de administración de LANs adecuadamente; sin embargo, para completar el esquema de administración, se deberán cubrir diversos aspectos que son complementarios, y que permitirán al administrador, tener control sobre todos los puntos que involucran a una red local de microcomputadoras, como son las condiciones eléctricas en el local, temperatura, seguridad de acceso, etc.

11.1 Condiciones del local.

En cuanto a las condiciones del local, se deben verificar básicamente dos puntos: las condiciones eléctricas y el clima. Existen otros puntos, que si bien no son de menor importancia, no son estrictamente necesarios, por lo que no se tocarán en esta tesis, como son: iluminación, ubicación de equipos, ergonomía, seguridad de acceso, detección de humo, sistemas extinción de incendios, etc.

- Verificación de las condiciones eléctricas.

Este punto normalmente no es tomado muy en cuenta por el usuario de una LAN, y no por eso deja de ser un punto importantísimo para el buen funcionamiento de todos los equipos, y no solo del funcionamiento, sino de la garantía que posean, ya que al descomponerse un equipo por cuestiones como sobrecargas de corriente o voltaje, se pierde la garantía del mismo. Posiblemente si hablamos de un solo equipo, esto no represente un gran problema; pero si hablamos de un volumen de equipos, sí es significativo, ya que el poseer un año de garantía sobre equipos, es considerado, en términos económicos, equivalente de un punto porcentual del valor del equipo nuevo. Si consideramos que cuando cualquier institución o corporativo compra equipo, su decisión entre una marca y otra puede ser de un punto porcentual en el costo de los equipos, resulta que la garantía es realmente importante. Por supuesto, aquí no trataremos sobre los descuentos para la compra de equipos, simplemente es una pequeña muestra de lo que una garantía representa para cualquier institución.

Lo que se debe hacer es verificar las condiciones eléctricas del local donde se instalará la LAN, verificar polaridades y por supuesto que exista tierra física, ya que los equipos de cómputo utilizan neutro, positivo y tierra física.

Este acondicionamiento consiste no solo en tomas de corriente para tres clavijas, sino que se encuentre en las condiciones eléctricas adecuadas, es decir, que la diferencia de voltaje entre el neutro y la tierra física sea cuando más de 1.5 volts y que la línea se encuentre regulada.

Por supuesto que el esquema ideal es que todos los equipos se encuentren conectados a corriente regulada y a No Breakes; sin embargo, esto es sumamente costoso, por lo que se recomienda que al menos el servidor, una estación de trabajo y una impresora se encuentren conectados a No Breakes o

UPS. Lo que sí es importante es que al menos el servidor se encuentre totalmente protegido contra cualquier problema que se presente en las líneas eléctricas.

Existen algunos fabricantes de UPS que incluyen en sus equipos la posibilidad de comunicación entre el UPS y el servidor, pudiendo hacer que el servidor se "dé de baja" en forma automática al recibir aviso del UPS. Este aviso se realiza cuando existe X tiempo en el que el UPS no ha recibido alimentación eléctrica, mandando una señal al servidor para que este en forma automática y normal se "dé de baja", permitiendo que todos los archivos se cierren y guarden sin sufrir sin daño.

Dependiendo de la marca y modelo, las condiciones de operación eléctrica de las microcomputadoras se basan en fuentes de poder autoreguladas en un rango de operación de 90 a 132 V en AC para una frecuencia entre 47 y 63 Hz.

Si en capítulos anteriores se mencionó que el mayor porcentaje (50% a 70%) de los problemas presentados en una LAN se originan por cableado. Se puede afirmar sin lugar a dudas, que de los problemas presentados en una LAN, del 20% al 30% son originados por condiciones eléctricas inapropiadas de alimentación a los equipos.

- Otras condiciones.

En lo que respecta al local, este deberá cumplir con las condiciones de humedad y temperatura que se indican en los equipos; aunque definitivamente sabemos que en general, en los lugares en donde la gente se encuentre cómoda, se puede considerar como un lugar apropiado para las microcomputadoras.

Dependiendo de la marca y modelo se tienen en general los siguientes rangos de operación dependientes del medio:

Condiciones Ambientales	Valores
Temperatura	5 a 40 grados centígrados
Humedad	15% a 80% dentro del rango de temperatura
Altitud	4.6 Km

La temperatura y humedad inciden directamente en el funcionamiento del disco duro, por lo que en ciudades cerca de la costa, es muy recomendable contar con sites de cómputo con condiciones adecuadas de clima y eléctricas.

Se deberá tomar en cuenta que si se está en una oficina alfombrada, esta deberá ser de tipo antiestático; y en caso de que se cuente con un laboratorio, el mismo no esté alfombrado, ya que incluso el caminar con tarjetas de vídeo, red, etc., en alfombra, puede ocasionar que estas se dañen.

11.2 Capacitación.

- Capacitar a un segundo administrador de LAN.

Es muy conveniente que sean dos las personas que puedan resolver los problemas de una LAN, ya que si existe solo un administrador del sistema, este algún día tendrá que: asistir a un curso, faltar por enfermedad, salir de vacaciones o simplemente renunciar, y los usuarios se quedarán desamparados ante cualquier suceso imprevisto que se presente en la LAN. No se deberá esperar a que pase mucho tiempo para designar a un segundo administrador. Si es posible, la capacitación se deberá efectuar simultáneamente al administrador primario. Ambos administradores deberán conocer a detalle todo lo referente a la administración de la LAN; ninguno deberá conocer más a detalle la LAN que el otro; sin embargo, sí se deberá indicar quien lleva la batuta de la administración.

Se recomienda que existan dos administradores de LAN por cada servidor; sin embargo, si el número de servidores fuera muy alto se podría pensar en un esquema en que existiera un administrador por servidor, y un substituto por cada X adicionales.

- Capacitación a usuarios.

Quienes finalmente aprovecharán los recursos de una LAN son los propios usuarios, por lo que se deberá planear una capacitación para todos ellos, ya que por ejemplo, si desean imprimir un documento, acceder algún tipo de información o utilizar algún recurso en la LAN, ellos mismos podrán hacerlo si se encuentran capacitados. El 95% de las veces un usuario que conozca los comandos y utilerías del sistema operativo resolverá sus propios problemas. Un curso de este tipo toma aproximadamente un día y medio.

Mientras los usuarios tengan más conocimientos sobre la LAN, más provecho podrán obtener de este recurso, pudiendo adicionalmente, ellos mismos resolver sus propios problemas. La idea no es que no exista un administrador de LAN, simplemente que el administrador solo intervenga cuando el problema realmente lo amerite, ya que muchas veces los usuarios ni siquiera conocen los comandos básicos de DOS, o la lógica que se debe de tener para hacer tal o cual cosa dentro de la LAN, y desean que todo se realice automáticamente; por supuesto que muchos trabajos repetitivos pueden ser totalmente automatizados; sin embargo, para eso se requieren desarrollos, o en el mejor de los casos macros, todo por supuesto con la finalidad de ahorrarse tiempo para poder realizar más cosas, no con la finalidad de no hacer nada.

- Mantener actualizado al administrador de LAN en nuevas tecnologías y productos.

Existen básicamente dos métodos para mantenerse actualizados: uno es mediante cursos o seminarios, y el otro es mediante lectura; ninguno de ellos es excluyente del otro; sin embargo, puede ser uno más caro que el otro, y adicionalmente cada uno tiene sus ventajas y desventajas. En el caso de los cursos, es necesario esperar a que alguien aprenda el concepto o el producto del que queremos aprender, y que lo exponga; esto por supuesto trae como consecuencia un pequeño retraso en la obtención de la información, sobre todo si no estamos muy en contacto con los organizadores de los eventos; así mismo, el tomar cursos tiene la ventaja de que podemos preguntar al expositor sobre cuestiones relacionadas al tema que está exponiendo, pudiendo obtener una gran cantidad de información si se hacen las preguntas adecuadas. Por otro lado los cursos que se podrían considerar importantes se proporcionan ya sea totalmente en inglés, o cuando menos el material. Si esperamos a que el curso se imparta totalmente en nuestro idioma sucederá lo mismo que con las publicaciones.

Para el caso de las revistas, se tiene la gran ventaja de primero conocer los nuevos conceptos que se manejan en el medio, y posteriormente iremos viendo productos que hagan uso de los mismos; con esto iremos viendo la polémica, y los comentarios que se vierten sobre tal o cual tecnología o producto. La gran desventaja es que para tener una buena información deberemos de leer más de tres artículos en revistas relacionadas al tema, para así formarnos una mejor opinión con respecto al concepto o tecnología que nos interese. Por otro lado deberán elegirse adecuadamente las revistas a leer, ya que algunas son muy tendenciosas. El número adecuado de revistas a leer mensualmente es de entre 5 y 10. Adicionalmente es conveniente contar con uno o dos proveedores de

tecnología que compartan la información de primera mano, ya que es la mejor forma de conocer la tecnología, a bajo costo.

Existe otra forma de actualizarse: asistiendo a exposiciones; sin embargo, por si solas las exposiciones no ayudarán en mucho, ya que por ejemplo; en las que se realizan en México, quienes atienden al público generalmente son agentes de ventas, y no personal técnico de buen nivel que nos pudiera ofrecer mayor información, por lo que en la mayoría de los casos la información será incompleta o incorrecta. En el caso de las exposiciones en el extranjero es común que quien atiende al público es gente bien capacitada, sin embargo asistir a exposiciones fuera del país es sumamente caro.

No importando la forma de actualización que se elija, esta deberá llevarse a cabo.

El mantenerse actualizado en lo que respecta a nuevas tecnologías, tendencias de las mismas o sobre nuevos productos, permitirá al administrador de LAN solucionar algunos de los problemas que se le presentan, o encontrar soluciones a situaciones que se pensaba que no podrían mejorarse; tal es el caso de las tarjetas de red inalámbricas, o compartición de impresoras sin estar conectadas a una microcomputadora o al servidor, o impresión a través del cableado eléctrico; por supuesto los anteriores son ejemplos de tecnologías ya disponibles en el mercado de cómputo.

- Mantener informados a los usuarios.

EL hecho de que el administrador resuelva los problemas que se presentan en una LAN, no significa que para el usuario esté resuelto el problema. Al usuario se le deberá avisar y enseñar el procedimiento a seguir para no caer en el mismo error; utilizar todos lo recursos, o acceso a nuevos productos que se instalen en

LAN, ya que muchas veces los usuarios no hacen tal o cual función o actividad porque no saben que se puede hacer, o cómo se puede usar.

Se puede utilizar la misma LAN para emitir boletines informativos; esto se puede hacer al entrar al servidor, de modo que lo primero que aparezca en la pantalla sea un pequeño boletín informativo, o mediante folletos; ya sea que se peguen en un pizarrón, en un lugar concurrido por todos, como la cafetería, o que se tenga un pequeño periódico que les llegue a todos los usuarios. Lo importante no es el cómo, sino que los usuarios tengan información oportuna para que utilicen en un 100% los recursos que ofrece la LAN.

- Conscientización a usuarios sobre uso de equipos.

Es por demás indispensable que los usuarios conozcan las normas mínimas para conservar los equipos en buen estado; es decir, que estén informados de asuntos como: la secuencia en que un equipo debe encenderse (CPU, monitor y periféricos); los cuidados que debe tener un equipo (no fumar, no comer ni beber cuando se esté utilizando un equipo, etc.); e incluso que el usuario conozca los puntos básicos que deben revisarse cuando se tienen fallas típicas en el uso de una LAN. El hecho de que los usuarios conserven los equipos en buen estado, y que ellos mismos solucionen los problemas sencillos que se originan en la LAN (cable desconectados, servidor apagado, etc.), hará que su nivel profesional se incremente, sean autosuficientes en problemas sencillos, y en caso de que laboren fuera de horas de trabajo puedan realizar su trabajo normalmente. Esto no quiere decir que se les estén pasando funciones de administración de LAN a los usuarios; simplemente que los mismos usuarios puedan hacer su propio trabajo sin contratiempos, y que no utilicen los servicios del administrador para problemas sencillos, ya que una buena cantidad de veces

los mismos usuarios pueden solucionar los problemas que presenten sus equipos. Todo lo anterior permitirá que el administrador de LAN tenga más tiempo para investigar sobre nuevos productos o tendencias informáticas que puedan incorporarse a la LAN, solucionar algún problema grave en otro equipo, desarrollar otra actividad, mejorar los sistemas actuales y por supuesto todo esto en beneficio de los usuarios, por lo que finalmente, los usuarios podrán hacer uso de más recursos y beneficios.

CAPÍTULO 12
Conclusiones

A través de esta tesis se han explicado los diferentes elementos que deben ser tomados en cuenta para llevar a cabo un proyecto de LAN. También se han expuesto diferencias entre tecnologías; así mismo se han expuesto ventajas y desventajas de productos en diferentes situaciones; sin embargo, ahora se explicarán los conceptos o tendencias básicas que deben tenerse en mente al desarrollar un proyecto que involucre las tecnologías aquí descritas.

Por supuesto no es fácil enumerar los puntos claves en las redes locales, ya que existen muchas variantes dependiendo de lo que finalmente se desee tener, adicionalmente a que se involucra una gran cantidad de elementos; sin embargo, siempre existen recomendaciones importantes, que si uno sigue, podrán invariablemente llevar proyectos de redes locales a buen fin.

Posiblemente el punto más importante sea el referente a los estándares, no importando que estos sean de facto; es decir, propuestos por la industria, como serían DOS, TCP/IP, Windows, IBM compatible, etc., o los que han sido totalmente avalados, depurados y aprobados por un comité internacional o nacional, como podrían ser las normas de ISO, IEEE, ANSI, CCITT, etc. El motivo de estar siempre dentro de uno o más estándares se puede resumir en lo siguiente: independizarse de las directrices de un fabricante, así como de su suerte comercial, y poder crecer fácilmente una plataforma con prácticamente cualquier tecnología, sin realizar cambios, o realmente mínimos, en lo que ya se tiene. Como se puede apreciar, esto permitirá hacer un buen uso de las inversiones que se tengan, lo que implica aprovechar las plataformas existentes; es decir solo adicionamos tecnologías, no cambiamos lo que ya se tiene; de esta

forma además de que se cuida el presupuesto, también se cuida la compatibilidad e interoperabilidad de sistemas y tecnologías.

Para poder llegar al punto anterior se deberá contar con personal especialista en cada una de las herramientas, productos y equipos que deseemos incorporar a la LAN. Por supuesto que no es fácil contar con gente que tenga el nivel adecuado para cada campo; sin embargo, se debe formar un equipo de muy alto nivel. Definitivamente esto dependerá de la magnitud de nuestro proyecto; por otro lado, si la idea es ser competitivos con otras empresas, principalmente las extranjeras, que dentro de relativamente poco tiempo estaremos compitiendo con ellas, deberemos pensar en grande, y si es así también deberemos contar con estos especialistas; es decir, que sean las propias empresas las que dicten sus tendencias, ya que son las mismas quienes conocen con mayor detalle la problemática a resolver, y no dejarse influenciar por empresas proveedoras de servicios de informática, ya que en muchas ocasiones las recomendaciones que estas hacen, son acordes a las relaciones comerciales que estas tienen o a la capacidad de sus asesores, y no a una verdadera solución integral a la problemática de la empresa. Por supuesto que esto no quiere decir que nunca le hagamos caso a un proveedor; simplemente que tengamos personal capacitado para verificar las características y/o ventajas que ofrecen los productos y/o servicios que dichos proveedores representan o proporcionan, ya que de otra forma se estará a expensas de lo que otros digan, quieran, conozcan o puedan vender.

Sabemos que en el ámbito de cómputo, aproximadamente cada 3 meses se tienen nuevos productos de hardware (PCs y periféricos), y cada aproximadamente 4 meses nuevos productos de software; sin embargo no es fácil estar haciendo cambios cada tres o cuatro meses, teniendo en cuenta que es molesto que ya que nos empecemos a familiarizar con algún producto, entonces

se tenga otra opción. La verdad es que deberemos tener una mente muy despierta para reconocer un pequeño avance tecnológico o adecuación de productos, de un gran avance tecnológico o nueva tecnología de punta. Es bueno revisar de vez en cuando los nuevos productos, pero no es posible comprarlos o hacer la evaluación con todos.

Sabemos que uno de los criterios con el que actualmente se mide el avance de un país o corporativo se basa en el tipo de comunicaciones que posea; por lo tanto es muy importante ir renovando la tecnología con que se cuenta; sobre todo en el ámbito de las comunicaciones, ya que de no ser así, se perderá liderazgo. Esto no quiere decir que se tenga que cambiar la plataforma de comunicaciones cada vez que sale al mercado un nuevo protocolo o mecanismo de comunicación; simplemente que se esté consiente de que estas tecnologías deberán irse renovando y ampliando. Se considera que en nuestro país, se podrá tener una gama impresionante de productos y servicios de comunicación (en todos los sentidos) a partir del año 1997; por supuesto, esto no se ha dado como se quisiera, aunque definitivamente se empieza a ver una mejora. Se dice que el as bajo la manga de Telmex, será la Red Digital de Servicios Integrados o RDSI (ISDN en inglés), que podrá, entre otras cosas abaratar enormemente el costo de las líneas de comunicación dedicadas; esto quiere decir que si ahora tenemos comunicaciones, a partir de 1998 las comunicaciones podrán ser mucho más eficientes.

La tecnología que involucra a las redes locales y a todo lo que les rodea, es una tecnología de punta, misma que es utilizada por los grandes corporativos para satisfacer sus necesidades de comunicación, información, procesamiento, automatización, etc.; es decir, son herramientas realmente productivas, que bien empleadas proporcionan ventajas sobre competidores, ya sea internos o externos. Por ejemplo, en Estados Unidos se calcula que existen en un corporativo del

tamaño de IBM alrededor de mil servidores enlazados, y en corporativos como instituciones bancarias este número varia de mil a cuatro mil servidores. Si tomamos el ejemplo como un signo de avance tecnológico y de ventaja competitiva podremos apreciar que lo han logrado; por lo que en México deberemos utilizar cada vez con mayor frecuencia la tecnología que permita proporcionar cualquier ventaja sobre cualquier competidor.

Al realizar un proyecto de esta naturaleza deberemos forzosamente trabajar con algún proveedor. Para hacer una buena elección, es recomendable preguntar al fabricante la mejor opción de los proveedores que lo representan, ya que los fabricantes no atienden por lo regular directamente, sino a través de asociados. De esta forma sabremos que quien nos esté prestando el servicio será la mejor opción que existe y que estará 100% apoyado por el fabricante para proporcionar el servicio. No solo se deberá buscar ventajas comerciales, sino también es adecuado saber la capacidad de la gente técnica, la cobertura que tienen, los servicios que puede proporcionar y qué valor agregado ofrece el proveedor y/o fabricante al adquirir un compromiso con él.

En resumen, la tecnología de redes locales está al alcance de cualquier corporativo que desee hacer uso de ella; sin embargo se deberá estar capacitado para usarla. El hecho de involucrar PCs, no quiere decir que sea algo sencillo, es una tecnología muy compleja, dado que involucra software, hardware, comunicaciones, circuitos, protocolos, estándares, configuraciones, microcomputadoras, minicomputadoras, mainframes, etc.; es decir, son campos que individualmente se han explotado mucho; aunque como un todo no se ha desarrollado tanto, y este conjunto de elementos cada vez tiene mayor auge, tanto en el ámbito nacional, como internacional.

Así mismo, es muy importante no perder de vista la tecnología que se está desarrollando para Internet, ya que muchos de los problemas que se tienen al día

de hoy en cuanto a búsqueda de información, capacitación y seguridad se están resolviendo con conceptos de Internet; sin embargo, sobre esto no se abunda debido a que la magnitud del tema, se presta para otra tesis.

Ahora que existen relativamente pocas opciones para poder solucionar la problemática que se vive hoy en día, es el momento de entrar en este campo, ya que después será cada vez más difícil, y este es el momento en que tanto nosotros como mexicanos y como profesionistas estamos en el mejor momento de desarrollarnos, y así ayudar al crecimiento que se espera tener en el país.

Como se podrá apreciar, esta tesis carece de un apéndice bibliográfico; esto debido a que se ha desarrollado en base a la experiencia que el autor posee sobre los temas aquí expuestos.

A través de esta tesis hemos podido observar las diversas tecnologías, productos, protocolos y opciones que existen al día de hoy para llevar a cabo un proyecto de red local, por lo que considero, que los dos objetivos planteados al inicio de esta tesis, se han cumplido adecuadamente, dichos objetivos fueron:

1. Exponer un panorama de la tecnología de punta reinante en las Redes de Área Local (LANs), Redes de Área Metropolitana (MANs) y Redes de Área Amplia (WANs).

2. Indicar las mejores opciones de aplicación de cada uno de los componentes de las tecnologías de LAN, MAN y WAN, así como las diferencias entre tecnologías similares, con la finalidad de obtener el mejor aprovechamiento de ellas.

En el desarrollo de esta tesis se ha vertido una gran cantidad de conocimiento y experiencia; sin embargo, desde mi punto de vista, el desarrollo de la misma me ha dejado algo muy importante, ya que ha implicado procesos

mentales muy interesantes, debido a que la tecnología no solo se debe conocer, sino también se debe poder explicar de una manera clara y sencilla, ya que no es lo mismo explicarse uno mismo el funcionamiento de las cosas, que explicarlo al lector.

Posiblemente al inicio de la tesis no se veía con muy buenos ojos el hecho de anticipar que no se iban a incluir fórmulas y/o procesos matemáticos en esta tesis, sin embargo, espero haber cambiado este concepto.

En otro orden de ideas, el campo de las redes locales, será la plataforma de todos los sistemas informáticos, ya que las tendencias nos dicen que no solo en las empresas se cuenta o contará con estas tecnologías, sino que incluso, se encontrará dentro de los mismos hogares, inclusive ya se acuñó un nuevo término, Home Area Network (HAN), lo que implica que ya se está pensando que esta tecnología también llegará a los hogares. La tecnología en el hogar se esta pensando no solo para interconectar computadoras, sino también para: controlar los sistemas de seguridad, el acceso a información (TV, radio, internet), así como el control de todos los dispositivos eléctricos y electrónicos que existan. Si hacemos cuentas, la cantidad de ingenieros necesarios para llevar a cabo un proyecto de esta magnitud y adicionalmente permitir la continuidad con la base instalada que crece día a día, hace que esta sea un área de la ingeniería muy importante, no solo desde el punto de vista personal, sino desde el punto de vista UNAM y sociedad.

CAPÍTULO 13
GLOSARIO

10Base2	Estándar IEEE 802.3 con cable coaxial delgado y topología bus.
10Base5	Estándar IEEE 802.3 con cable coaxial grueso y topología bus.
10BaseT	Estándar IEEE 802.3 con cable UTP y topología estrella.
802.3	Estándar desarrollado por IEEE para ethernet.
802.5	Estándar desarrollado por IEEE para token ring.
Ancho de banda	Rango de frecuencias asignadas a un canal de comunicaciones.
ANSI	American National Standards Institute. Institución que ayuda a definir estándares y que representa a Estados Unidos ante OSI.
ARCNet	Attached Resource Computer Network. Arquitectura creada por Datapoint. Transmite a 2.5 Mbps y utiliza un método de acceso al medio denominado token passing.
Arquitectura	Método que se utiliza para formar una LAN. Existen básicamente cuatro; Ethernet, Token Ring, ARCNet y FDDI.
ATM	Asynchronous Transfer Mode.
AUI	Attachment Unit Interface. Tipo de interfaz utilizado comúnmente en Ethernet.

BackBone	Se considera que es el enlace entre varias redes locales ubicadas en un mismo edificio. Este enlace puede efectuarse con cualquiera de las topologías, aunque normalmente se realiza mediante bus.
Batch	Método de procesamiento de datos en donde todas las acciones se agrupan para después ejecutarse en forma secuencial, siguiendo el mismo orden en que fueron indicadas.
Beta	Producto de software o hardware prácticamente terminado que aún puede presentar fallas y se encuentra bajo observación. Es el equivalente a un prototipo, pero en la industria de cómputo.
BNC	Bayonet Navy Connector. Conector de seguridad utilizando para cables coaxiales.
Boot remoto	Para acceder a un servidor de archivos es necesario ejecutar ciertos archivos. Cuando la estación de trabajo no posee unidades de almacenamiento, los archivos son ejecutados desde el servidor, y a este proceso se le llama Boot Remoto.
BPS	Abreviación de bits por segundo. Medida de velocidad de transmisión utilizada en el campo de las redes locales.
Bridge	Dispositivo de comunicación entre LANs, que trabaja en los dos primeros niveles del modelo OSI de ISO.
Canal	Es un camino físico o lógico por el cual se transmite información.

CCITT	Comité Consultivo Internacional de Telefonía y Telegrafía. Organización internacional iniciada en Francia que desarrollaba estándares y definía interfaces de comunicación.
Colisión	Término que se utiliza, cuando dos o más estaciones de trabajo intentan simultáneamente utilizar el mismo canal de transmisión.
Correo Electrónico	Es un sistema de correo basado en computadoras, ya sea que estas estén dentro de una LAN o fuera de ella, o una mezcla. Un software se encarga de enviar las comunicaciones (cartas) y de asegurar que lleguen a su destino. El correo electrónico se basa en estándares de MHS, X.400 o X.500, dependiendo de la plataforma en la que esté funcionando.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection. Es el método de acceso al medio (cable) que utiliza Ethernet.
DAS	Dual Attachment Station. Dispositivo utilizado en FDDI para conectar equipos directamente al anillo doble.
Emulación	Imitación que hace un equipo de otro. Normalmente se utiliza este término cuando una PC imita a una terminal que no posee microprocesador.
Estación de Trabajo	Conocida como PC. Se considera que es un equipo que se encuentra conectado a una LAN en donde un usuario puede accesar los recursos que se encuentren habilitados.

Ethernet	Arquitectura de LAN cuya velocidad es 10 Mbps, con protocolo CSMA/CD. Regida por el estándar IEEE 802.3. Permite utilizar topologías en bus y en estrella, independientes o combinadas.
Escalabilidad	Capacidad de utilizar el mismo software en computadoras de diferentes tamaños, desde computadoras personales hasta supercomputadoras.
Estándar de facto	Un estándar tan ampliamente utilizado que se convierte en un estándar no oficial de la industria.
FDDI	Arquitectura de red, utilizada principalmente para formar un backbone entre edificios. Su velocidad es de 100 Mbps, utiliza fibra óptica en una topología de anillo doble, con método de acceso token passing.
Frame	Bloque de datos organizado de una forma especial, siendo un conjunto indivisible.
GAN	Global Area Network. Enlace de equipos de cómputo que operan bajo ambientes de cómputo diferentes, sin importar su ubicación.
IEEE	Institute of Electrical and Electronic Engineers. Sociedad profesional de la industria electrónica comisionada por la ANSI para definir o especificar estándares.
Interconectividad	Posibilidad de realizar un enlace de equipos de cómputo dentro de los primeros tres niveles del modelo OSI.

Interfaz gráfica	Software que crea medios físicos o gráficos para que el usuario interactúe con un sistema de cómputo y el software de aplicación separado de la funcionalidad de un programa de aplicación.
Internet	Red mundial de computadoras conectadas entre sí mediante enlaces dedicados. Se inició como plataforma de comunicaciones en la defensa de los EUA. Actualmente incluye entre otros servicios: WWW, e-mail, gopher, etc. Siendo WWW el más solicitado.
Intranet	Incorporación de los servicios de WWW dentro de un corporativo. Estos servicios incluyen principalmente la fácil utilización de todos los recursos desde una misma interfaz gráfica.
Interoperabilidad	Intercambio de información entre equipos de cómputo dentro de los últimos cuatro niveles del modelo OSI.
ISO	International Standars Organization. Organización que coordina todas las actividades internacionales de estándares, incluyendo los estándares de OSI para redes de comunicación multivendedores.
LAN	Local Area Network. Ver Red Local.
MAN	Metropolitan Area Network. Enlace de Redes Locales en una misma ciudad, bajo un mismo ambiente operativo.
Nodo	Cualquier estación de trabajo, repetidor, bridge, router o dispositivo conectado a la LAN.
NOS	Network Operating System. Sistema operativo de Red Local.

OSI (modelo)	Especificación de componentes físicos y lógicos que intervienen en una comunicación dividido en siete niveles.
Página Web	Documento HTML que puede visualizarse con un navegador de internet. Existen páginas estáticas y dinámicas.
Portabilidad	Capacidad de utilizar el sistema operativo de software de aplicación en sistemas de cómputo de diferentes proveedores.
Protocolo	Conjunto de reglas que se establecen para comunicar dos entidades.
Red local	Enlace de computadoras ubicadas en una misma oficina o edificio con la finalidad de compartir recursos físicos y lógicos, utilizando un mismo ambiente operativo.
Ruteador	Dispositivo para interconectar LANs, pudiendo en forma dinámica encontrar rutas óptimas entre dos o más redes locales.
SAS	Single Attachment Station. Dispositivo utilizado en FDDI para conectar equipos sin estar en el anillo doble.
Sistemas abiertos.	Ambiente de cómputo en el cual el sistema operativo y el software de aplicación son portables e interoperables. En un sistema abierto, el hardware, sistemas operativos, aplicaciones e interfaces de usuario de diferentes proveedores pueden trabajar juntos en un ambiente integrado.

Sistema operativo.	Grupo de programas que administran los recursos de un sistema de cómputo. El sistema operativo se ocupa de aspectos como la memoria, procedimientos de entrada/salida, calendarización de procesos y de la administración de archivos y recursos.
STP	Shielded Twisted Pair. Par trenzado blindado utilizado en los cableados que requieren grandes distancias, y muy utilizado para arquitecturas token ring.
TCP/IP	Transport Control Protocol/Internet Protocol. Protocolo estándar de la industria creado en la defensa de los Estados Unidos con la finalidad de enlazar equipos de cómputo diferentes.
Topología	Forma física de enlazar equipos de cómputo. En el ámbito de las redes locales existen básicamente tres; estrella, bus y árbol, y combinaciones de ellas.
UTP	Unshielded Twisted Pair. Cable parecido al telefónico utilizado para enlazar equipos de cómputo.
WAN	Wide Area Network. Enlace de MANs o LANs entre diferentes ciudades, bajo un mismo ambiente operativo.