UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

" TEORIA, METODOLOGÍA Y CONSIDERACIONES PARA UN DISEÑO ÓPTIMO DE REDES INFORMATICAS "

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÓN
PRESENTA:

OSCAR DANIEL ISLAS RUBALCABA

ASESOR: Ing. Norma Raquel Soto Arredondo

MEXICO , 2008

AGRADECIMIENTOS

A mis padres Blanca y Salvador por haber fomentando los valores y educarme con buenos principios, y la confianza que me brindaron para concluir este objetivo.

A mi Esposa Georgina por su compresión, apoyo, la dicha de tenerla a mi lado y principalmente por su amor.

A mis hermanas Diana y Marlene por su apoyo y amor que me dan día con día.

A mi tía Beatriz, a mi abuela Ángela y a mi tío Fernando que por la gracia de Dios ya no están con nosotros, los llevo dentro de mi corazón y les agradezco toda su ayuda incondicional.

A mis primos, tíos y abuelos por su comprensión.

A mis amigos por aceptarme y compartir parte de su vida conmigo.

Gracias a Dios por haberme dado mi Familia, que es la que le da sentido a mi vida.

Gracias a todos y cada uno de ellos por ser parte de mi historia.

Índice

- Introducción -

Uno de los aspectos más importantes en el camino hacia el éxito, radican en el manejo de la información (al menos en la actualidad). Incluso, se ha llegado a afirmar:

"Quien maneja la información, maneja el poder"

Se puede decir que una red tiene su origen en la necesidad de compartir los diversos recursos informáticos, entre distintos sectores, usuarios u organizaciones. La red permite el suministro de diversos servicios desde y a cualquier punto o puesto de trabajo.

Servicios importantes, tales como: consulta de bases remotas ubicadas en computadoras a miles de kilómetros; la transferencia "instantánea" de documentos, videoconferencia en tiempo real; correo electrónico; y tantos otros, ya coexisten con otros servicios tradicionales como la telefonía y el fax.

Las redes de computadoras han tenido un auge extraordinario en los últimos años y han permitido, entre otras cosas:

- Intercambiar información a grandes distancias.
- Compartir información entre diferentes usuarios a través del correo electrónico
- Crear grupos de discusión a distancia sobre diversos temas
- Tener acceso a bibliotecas electrónicas en lugares distantes
- Utilizar facilidades de cómputo en áreas de geográficas diferentes
- Crear sistemas de procesamiento distribuido de transacciones

Estos beneficios se derivan de la utilización de las redes y han sido posibles gracias a los avances logrados en el área de comunicación de datos

Las redes computacionales que operan en la actualidad están formadas por una jerarquía de redes de área amplia, redes metropolitanas y redes locales interconectadas entre sí.

Las redes que operan en áreas geográficas reducidas tales como un departamento, un edificio o una corporación son redes de área local. Algunas de estas redes están interconectadas entre sí formando redes metropolitanas y estas a su vez se interconectan a las redes de área amplia para permitir la comunicación entre puntos muy distantes geográficamente hablando. También se tienen redes de área local conectadas directamente a redes de área amplia.

Una red local aislada proporciona algunos beneficios; sin embargo, para poder explotar el potencial que proporcionan las redes computacionales, será necesario que esta red se interconecte con otras redes locales y con redes de área amplia.

Las redes de computadoras están hechas con enlaces de comunicaciones que transportan datos (sistema de comunicación), entre dispositivos conectados a la red.
Los enlaces (canales de comunicación) se pueden realizar con cables, fibras ópticas o cualquier otro medio de comunicación.

De esta manera, se puede clasificar a las redes de computadoras en:

- Redes Locales: Conocidas como LAN (Local Area Networks), son usadas para comunicar un conjunto de computadoras en un área geográfica pequeña, generalmente un edificio o un conjunto de edificios cercanos o en un campus.

- Redes Metropolitanas: También conocidas como MAN (Metropolitan Area Networks), cubren por lo general un área geográfica restringida a las dimensiones de una ciudad. Usualmente se componen de la interconexión de varias redes locales y utilizan alguna facilidad pública de comunicación de datos.

- Redes de Area Amplia: Las redes de área amplia, también denominadas WAN (Wide Area Networks), son las primeras redes de comunicación de datos que se utilizaron. Estas redes cubren áreas geográficas muy grandes, del tamaño de un país o incluso del mundo entero, como es el caso de la red Internet.

Por otro lado, y tomando en cuenta lo anterior, a través del tiempo y desde su nacimiento, se han buscado mejoras para las comunicaciones a través de redes cada vez más especializadas. Este no es un trabajo sencillo, pero alguien tiene que hacerlo.

Los especialistas en redes son personas que han trabajado mucho tiempo en el uso y manejo de redes, que tienen experiencia en la implantación y mantenimiento de éstas y, por tanto, tienen la capacidad y el conocimiento para ir paso a paso con un mínimo de errores.

La experiencia no se adquiere de la nada y, por ello, he tratado de manejar una visión completa y lo más general posible sobre lo que es el diseño eficiente de redes informáticas, su uso, manejo y los conceptos elementales necesarios.

Cabe mencionar que el diseño de redes debe adaptarse a las necesidades de usuario; es decir, tiende a ser diferente en cada caso y para cada organización.

- Capítulo I: Conceptos básicos -

1.1 Introducción

Una red, propiamente dicha, no se reduce exclusivamente al ámbito informático y tampoco a la era de las computadoras. Se define como red a cualquier medio que permita unir dos o más elementos para interactuar entre sí.

Se puede decir que el hombre hace uso de las redes desde el momento en que adoptó la idea de fijar caminos para unir distintos asentamientos, lo que hoy se ve transformado en rutas y autopistas.

Trasladado a las computadoras, se establece como red al medio que permite comunicar dos o más equipos para el intercambio de datos y recursos.

Actualmente, la tecnología digital permite que diferentes sectores se fusionen en uno solo (telecomunicaciones, datos, radio y televisión, por ejemplo). Esta circunstancia, que recibe el nombre de convergencia, está ocurriendo a escala global y está cambiando drásticamente la forma en que se comunican tanto las personas como los dispositivos.

En el espacio central de este proceso, y formando la red troncal, haciendo posible la convergencia, están las redes IP.

Los servicios y los dispositivos integrados de los consumidores para propósitos como:

- Telefonía
- Entretenimiento
- Seguridad personal
- Informática personal

Estos se están desarrollando constantemente; están siendo diseñados y convergen hacia un estándar de comunicación que es independiente de la conexión física subyacente.

La red de cable, por ejemplo, que fue diseñada primero para la transmisión de televisión al consumidor, puede ahora también usarse para enviar mensajes de correo electrónico, navegar por Internet e incluso para monitorizar una cámara de red enviando imágenes en directo desde otro continente. Además, estas características están también disponibles a través de otras redes físicas, como:

- La red telefónica
- La red de telefonía móvil
- La red de satélites
- Las redes informáticas.

1.2 Redes informáticas

Una red es un conjunto de computadoras interconectadas entre sí, que pueden comunicarse compartiendo datos y/o recursos, sin importar la localización física de los distintos dispositivos.

A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas, etcétera.

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites. Cada dispositivo activo conectado a la red se denomina nodo.

1.3 Evolución de las redes informáticas

En 1884, gracias a Samuel Morse, se crea la primera red telegráfica en Estados Unidos.

En 1878, se crea la primera red de telefonía local en New Heaven, Estados Unidos, a partir del invento de Alexander Gram. Bell.

En 1898, Marconi da inicio a inventos tan revolucionarios como la radio.

La evolución se detiene y no es hasta 1950 que aparece la red de microondas, predecesora de las redes satelitales de 1960.

En 1969, se da el primer paso para la gran revolución informática, cuando nace ARPANET del departamento de defensa de los Estados Unidos. Se unen cuatro universidades, poniendo así en actividad los primeros cuatro nodos de Internet.

A mediados de los años setenta´s, diversos fabricantes desarrollaron sus propios sistemas de redes locales.

En 1980, Xerox en cooperación con Digital Equipment Corporation e Intel, desarrolla y publica las especificaciones del primer sistema comercial de la red, denominado Ethernet.

En 1982, aparecen los ordenadores personales.

En 1986, IBM introduce la red Token Ring.

También en los años ochenta´s, el Internet se traslada a las computadoras personales, con servicios BBS para líneas telefónicas.

Ya acercándose el final de los noventa´s, Internet se masifica y da lugar a lo que hoy conocemos a través de avances como la banda ancha.

En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa o de una organización, puede constituir una clara ventaja competitiva.

La reducción de costes de periféricos y/o la facilidad para compartir y transmitir información son los puntos clave en que se apoya la creciente utilización de redes.

En la figura 1.1 se muestra un aspecto de las primeras redes telegráficas.

Figura 1.1 Aspecto del edificio de una de las primeras redes telegráficas del mundo

1.4 Objetivos de las redes

El principal propósito de armar una red consiste en que todas las computadoras que forman parte de ella, se encuentren en condiciones de compartir su información y sus recursos con las demás.

De esta manera, se estaría ahorrando dinero, debido a que si se colocara un dispositivo cualquiera a una de ellas, todas las computadoras de la red podrían utilizarlo.

Los recursos que se pueden compartir en una red son:

- Procesador y memoria RAM, al ejecutar aplicaciones de otras computadoras.
- Unidades de disco duro
- Unidades de disco flexible
- Unidades de CD-ROM/DVD-ROM
- Impresoras
- Fax
- Módem
- Conexión a Internet

También es posible compartir la información almacenada en las computadoras conectadas a la red, como son:

- Ejecución remota de programas de aplicación
- Bases de datos
- Documentos en general
    1. Archivos de texto
    2. Archivos de imagen
    3. Archivos de sonido
    4. Archivos de video
- Directorios o carpetas

Como ventaja adicional, la instalación de una red ofrece una interfaz de comunicación a todos sus usuarios. Esto se logra por medio de la utilización del correo electrónico, el Chat y la video conferencia. Esto se muestra en la figura 1.2

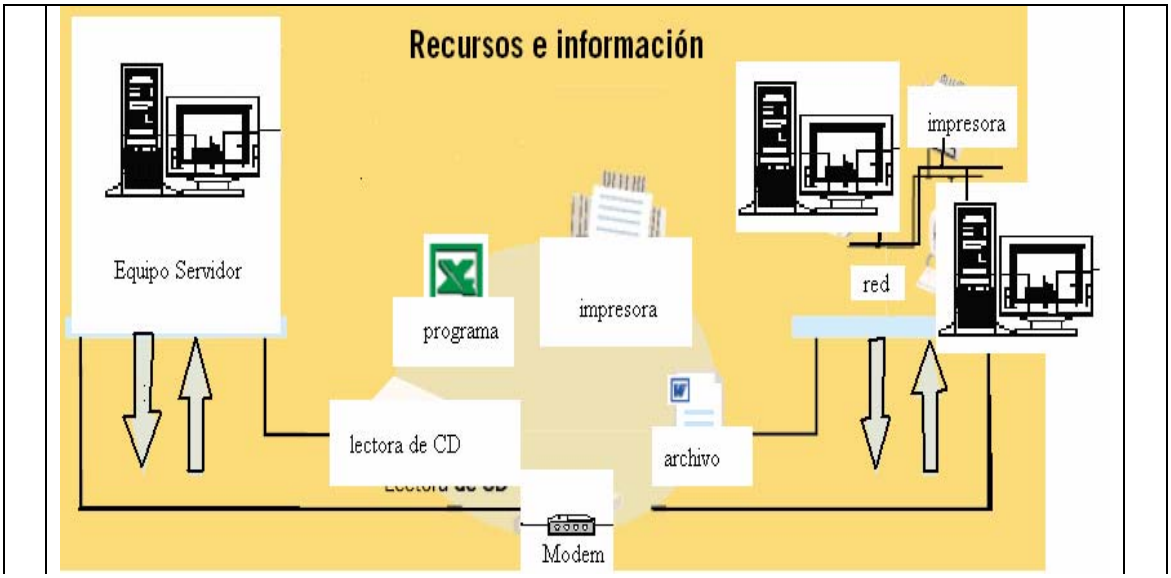


Figura 1.2 Compartición de recursos en red

1.5 Componentes de una red

Básicamente, una red se compone de:

- Un servidor
- Estaciones de trabajo
- Un sistema operativo de red
- Recursos a compartir
- Hardware de red

El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de información.

La estación de trabajo es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas de la veces, esta computadora ejecuta su propio sistema operativo y, ya dentro, se añade el ambiente de la red.

El sistema operativo de red es el sistema (software) que se encarga de administrar y controlar en forma general la red. Para esto, tiene que ser un sistema operativo multiusuario.

Al hablar de los recursos a compartir, se está refiriendo a todos aquellos dispositivos de hardware que tienen un alto costo y que son de alta tecnología. En estos casos, los más comunes son las impresoras en sus diferentes tipos.

El hardware de red implica a aquellos dispositivos que se utilizan para interconectar a los componentes de la red; es este caso, serían básicamente las tarjetas de red y el cableado entre servidores y estaciones de trabajo; asimismo, los cables para conectar los periféricos.

La figura 1.3 muestra de manera esquemática la estructura de una red.

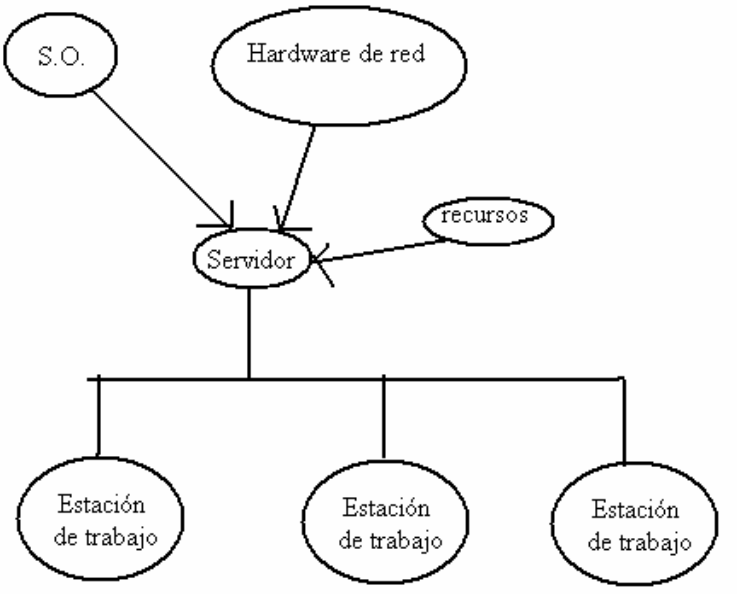


Figura 1.3 Esquema de una red

1.6 Tipos de redes

En un principio, la definición de red de computadoras abarcaba todas las posibilidades de conexión.

Actualmente, este concepto incluye muchas variantes, dadas las distintas posibilidades que nos brinda la tecnología para llegar al mismo objetivo: la comunicación entre computadoras y periféricos.

El criterio más común de clasificación de redes es dependiendo del territorio que abarca la red; y esto es:

- Red de área local
- Red de área amplia

Por otro lado, éstas pueden comunicarse por medio de conectores y líneas físicas, lo que se conoce como redes cableadas; o sin cables, lo que se llama redes inalámbricas.

1.6.1 Red de área local

Se denomina red de área local (LAN por sus siglas en inglés) a aquellas redes que tienen cerca sus computadoras: en la misma habitación, en diferentes pisos de un edificio o en edificios muy cercanos.

Las redes de área local proveen una excelente velocidad de transferencia, que va desde los 10 hasta los 1000 Mbps. Esto se debe a la corta distancia existente entre las computadoras, lo cual evita las interferencias. Un ejemplo de una red LAN se ve en la figura 1.4

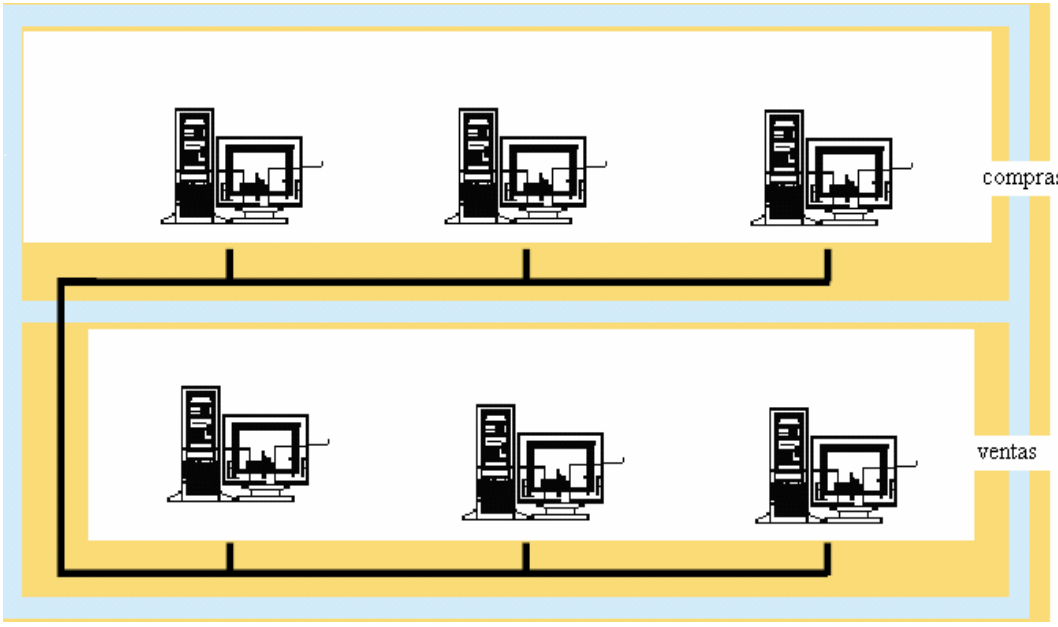


Figura 1.4 Ejemplo típico de una red LAN

En estas redes, la interferencia es directamente proporcional a la distancia entre el emisor y el receptor y también a la velocidad de transmisión; por consiguiente, al aumentar la distancia o la velocidad de transmisión, también aumenta la interferencia.

Las LAN´s se pueden dar el lujo de transmitir a altas velocidades a costa de distancias cortas. Las transmisiones de datos, en este caso, tienen una tasa de error muy baja.

El cableado que interconecta las computadoras de la red tiene uso privado; por ende, no se comparte. Esto significa que es utilizado sólo por las máquinas que conforman la red LAN.

Un caso particular de este tipo de red son aquellas redes LAN que están compuestas por varias redes LAN, a manera de subredes, que se interconectan mediante puentes o ruteadores. A este tipo de red se le denomina intranet.

1.6.2 Red de área extensa

Las redes de área amplia (WAN, por sus siglas en inglés) tienen las computadoras situadas en lugares distantes, como: diferentes ciudades, provincias, regiones, países, continentes o, simplemente, edificios muy lejanos dentro de una misma zona. Esta característica las hace más vulnerables a interferencias, lo cual disminuye la velocidad de transferencia a 30 Mbps.
Generalmente, utilizan una línea telefónica para conectarse entre sí, aprovechando la infraestructura lograda por Internet. No obstante, las empresas de mayor envergadura unen las computadoras que forman parte de su red, mediante una conexión satelital para conectar a ordenadores situados muy distantemente entre ellos.

La figura 1.5 muestra un ejemplo de red WAN.

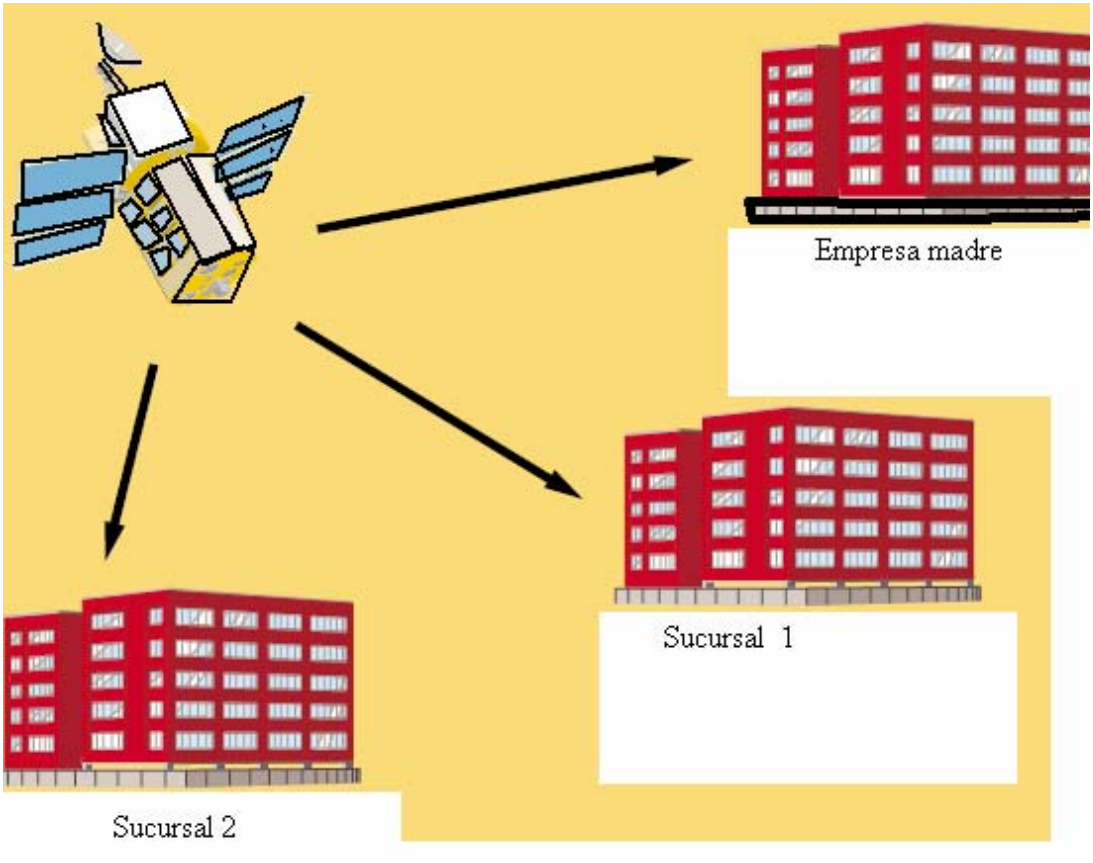


Figura 1.5 Ejemplo típico de una red WAN

Estas redes tienen menor velocidad en las comunicaciones porque tienen mayores problemas de interferencias. La razón es que las WAN pueden lograr distancias grandes, pero deben sacrificar la velocidad de transmisión a medidas muy reducidas.

En la actualidad, las velocidades de transmisión superan los 30 Kbps y pueden llegar a varios Mbps; todo ello depende de la tecnología usada al momento de realizar la instalación de la red.

Las WAN usan habitualmente las líneas telefónicas y los servicios de conexión con el proveedor de Internet para intercomunicar sus computadoras. Por otro lado, no tienen límite respecto de la cantidad de usuarios.

Cabe mencionar que la red WAN más grande del mundo no es de uso exclusivo de una sola empresa y es conocida por todo el mundo; se le conoce como Internet y, en su interior, contiene numerosísimas redes de tipo WAN y LAN; además de usuarios individuales que gozan de sus servicios. Esto se plasma en la figura 1.6

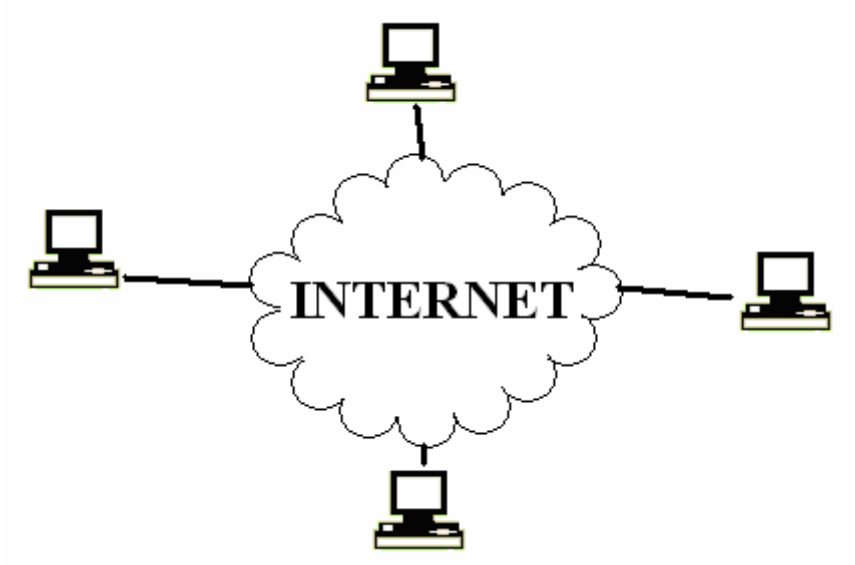


Figura 1.6 Vista de Internet

1.6.3 Red cliente-servidor

Con la llegada de las computadoras personales (que procesan información mediante su propia Unidad Central de Procesamiento de datos, almacenan datos en forma permanente mediante el disco duro, y almacenan información en forma provisoria por medio de la memoria RAM), se comenzó a utilizar otro tipo de redes descentralizadas llamadas cliente-servidor.

Esto significa que cada computadora personal (PC) integrante de la red es capaz de almacenar y procesar datos por su cuenta, sumado a lo que hagan las demás. En consecuencia, se elimina la idea de una PC central que hace el trabajo de todas las demás.

1.6.3.1 Ventajas de las redes cliente-servidor

En el caso de la red cliente-servidor, las computadoras tienen grandes puntos a su favor; entre las que destacan:

- Son de costo muy accesible debido a su difusión masiva.
- Tienen la capacidad de almacenar y procesar información por sí solas.
- Su difusión y aceptación a nivel mundial hizo que miles de fabricantes de hardware depositaran investigaciones, ideas, inventos, y crearan estándares que han permitido desarrollar su tecnología a un ritmo sin precedentes. Este avance tecnológico ha mejorado la calidad, variedad, velocidad de procesamiento y capacidad de almacenamiento de las computadoras personales, y cada día el mundo se sorprende más de ello.

- Disponen de una variedad muy grande de dispositivos accesorios que se pueden conectar; por ejemplo:
    1. Impresoras
    2. CD-ROM
    3. Escáneres
    4. Cámaras digitales
    5. Videocámaras
    6. Módems

  Incluso, ya hay varias firmas de electrodomésticos que están proyectando incorporar interfaces en sus productos para poder conectarlos a las computadoras personales y manipular su funcionamiento a través de Internet.

- Existe una inmensa variedad de aplicaciones de software que, además, son accesibles desde el punto de vista económico, pues entran en la categoría del software denominado "enlatado"; es decir, son creadas una vez para luego ser usadas y adaptadas en miles de sistemas de computadoras diferentes.

1.6.3.2 Componentes de las redes cliente- servidor

Los componentes básicos de una red de tipo cliente-servidor son:

- Cliente
- Servidor

Una computadora es un cliente cuando utiliza recursos e información de otras computadoras de la red. Los recursos pueden ser, entre otras:

- Unidades de disco
- Impresoras
- Módems

La información se refiere, por ejemplo, a:

- Archivos
- Carpetas
- Programas

Un ordenador es un servidor cuando tiene como única función el ofrecer sus recursos y su información a cualquier otra computadora de la red. Generalmente, es mucho más potente que el resto de las computadoras de la misma red.

Los clientes pueden realizar tareas totalmente independientes del servidor y usar los recursos de éste cuando realmente lo requieran.

La figura 1.7, muestra una forma de ejemplificar el tipo de red cliente-servidor

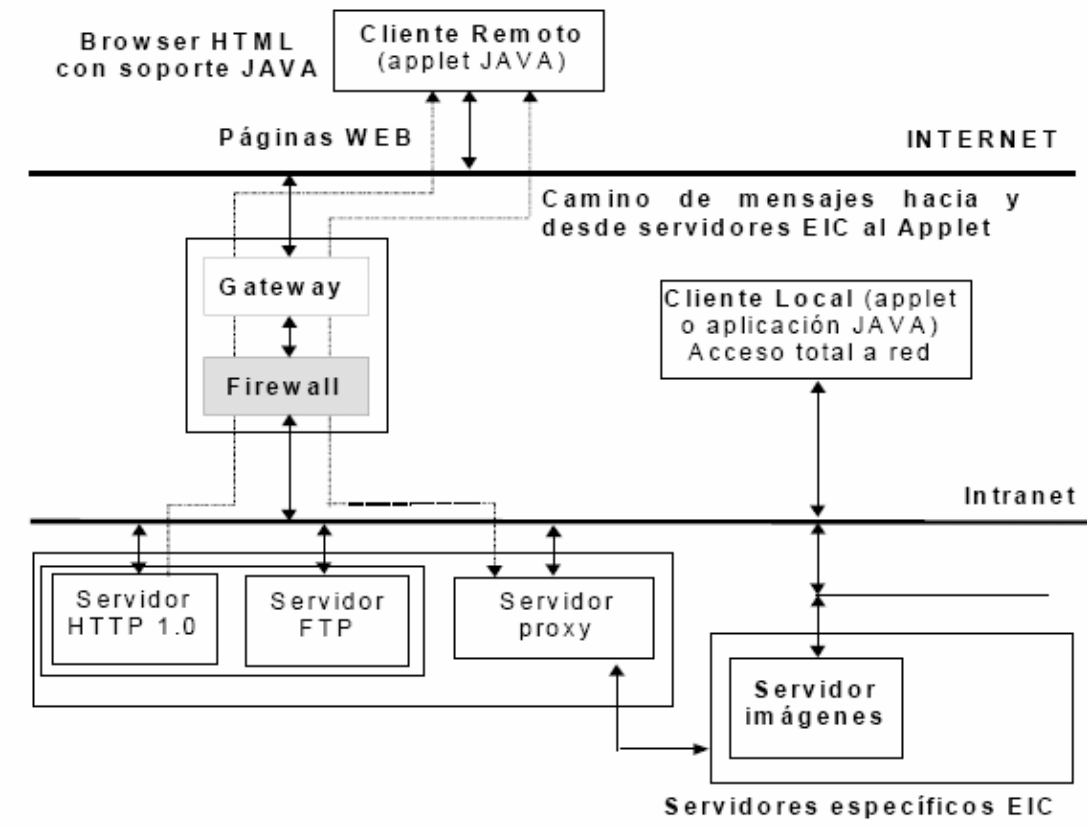


Figura 1.7 Vista clásica de una red cliente-servidor

1.6.3.3 Tamaño de una red cliente-servidor

El tamaño de una red cliente-servidor puede ir desde un solo cliente y un único servidor, hasta millones de clientes y miles de servidores, como es el caso de Internet.

Por supuesto, la cantidad de clientes es mayor que la cantidad de servidores.

Tanto los clientes como los servidores son computadoras que tienen la capacidad de procesar y almacenar información. No obstante, puede haber servidores que tengan mayores dimensiones que las computadoras convencionales; esto se debe a que están equipados con varios procesadores CPU y una gran cantidad de memoria RAM, además de varios discos duros. Todo ello determina que existan fabricantes que se especialicen en la fabricación de estos servidores de alta demanda.

1.6.4 Red inalámbrica

Las redes inalámbricas son aquellas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo, aunque su creación fue consecuencia de varios años de búsqueda.

Esta tecnología facilita el acceso a recursos en lugares donde se imposibilitaría el uso de cables, como zonas rurales poco accesibles.

Además, estas redes pueden ampliar una ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar sus computadoras a un hub o un switch por intermedio de cables. Estos usuarios podrían acceder a la red de su empresa o a la computadora de su casa en forma inalámbrica, sin configuraciones adicionales.

1.7 Ventajas del trabajo en red

Las ventajas de trabajar vía red, son muy numerosas. Podemos enumerar las más importantes de la siguiente forma:

- Disminución del costo de hardware
- Disminución del costo de software
- Intercambio de información
- Backups o copias de seguridad
- Espacio de almacenamiento
- Actualizaciones
- Administración y comunicación de los empleados
- Seguridad

La disminución del costo de hardware es posible debido a que se comparten los recursos de hardware. En consecuencia, no es necesario comprar dispositivos para cada una de las computadoras de la red, sino que basta uno solo y éste puede ser utilizado por cada una de los ordenadores conectados.

La disminución del costo de software es gracias a que es más económico adquirir un conjunto de licencias para cada máquina de la red, que comprar el programa para cada computadora en particular.

Con la implementación de una red, se evita el intercambio de información entre computadoras por medio de disquetes, CD u otros soportes de almacenamiento que pueden dañarse o perderse. De esta manera, el intercambio se produce en forma rápida y segura.
Se puede realizar una sola copia de seguridad de todo el contenido de la red, con lo cual se logra mayor velocidad en su armado y se evitan los backups fragmentados de cada máquina.

Se disminuye la aparición de archivos duplicados en varias máquinas, ya que una computadora central posee una versión actualizada de los mismos.

Las redes aportan velocidad al evitar actualizar la información contenida en todas las computadoras. Éste es un proceso automático del trabajo en red y no función de cada ordenador particular.

Con una red, se puede administrar, controlar y auditar a todos los empleados que trabajan con una computadora. Además, todos los empleados interconectados pueden comunicarse entre sí gracias a elementos como:

- El Chat
- El correo electrónico
- La videoconferencia

También, mediante una red es posible verificar y controlar los accesos no autorizados, intrusiones e intencionalidad de destruir información. Es posible centralizar la seguridad mediante el empleo de usuarios y contraseñas.

Si la red no se encuentra instalada y administrada adecuadamente, usuarios malintencionados (internos y/o externos a la red) podrían poner en riesgo la integridad de la información. Es aquí en donde toma especial protagonismo el Administrador de la red, que es la persona encargada de evitar estas acciones.

1.8 Desventajas del trabajo en red

Como todo en este mundo, también las redes tiene desventajas, tales como:

- Inversión inicial
- Capacitación del personal
- Clima laboral

Para implementar una red es necesaria una inversión de recursos, tales como tiempo, dinero y esfuerzo a fin de diseñarla; esto incluye compra, configuración e instalación de hardware y software.

También es necesario invertir en la capacitación del personal. Cabe mencionar que al instalar una red, puede producirse una merma en la productividad, mientras los empleados logren aprender el funcionamiento básico de ella.

Suele suceder que el aprendizaje de una nueva tecnología provoque problemas de adaptación del personal y genere cierto malestar en aquello sectores hostiles al cambio.

1.9 Topologías de red

Se le conoce como topología de una red al patrón de conexión entre sus nodos; es decir, a la forma en que están interconectados los distintos nodos que la forman.

1.9.1 Criterios de elección de topología

Los criterios a tomar en cuenta a la hora de elegir una topología en particular, en general, buscan que eviten el coste de encaminamiento (necesidad de elegir los caminos más simples entre el nodo y los demás), dejando en segundo plano factores como: la renta mínima, el coste mínimo, entre otras.

Otro criterio determinante en este caso, es la tolerancia a fallos o la facilidad de localización de éstos.

También hay que tener en cuenta la facilidad de instalación y reconfiguración de la red.

En otras palabras, se pueden observar dos aspectos al momento de considerar una topología:

- La topología física, que es la disposición real de las máquinas, dispositivos y cableado en la red.

- La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes son: broadcast (Ethernet), y transmisión de tokens (Token ring).

1.9.2 Objetivos de una topología

El objetivo fundamental de la topología es buscar la forma más económica y eficaz de conectar los diferentes elementos de una red para:

- Facilitar la fiabilidad del sistema,
- Evitar los tiempos de espera en la transmisión de datos,
- Permitir un mejor control de la red y
- Permitir, de forma eficiente, el aumento de las estaciones de trabajo

1.9.3 Topologías más usuales

Por sus características, las topologías son usadas en mayor o menor medida, siempre buscando la plena satisfacción del usuario.

Recordemos que la finalidad de una red informática es la de satisfacer los requerimientos de manejo y control de información por parte del usuario, de la mejor manera posible.

Las topologías más utilizadas son:

- Topología de bus lineal

- Topología de estrella
- Topología de anillo

Hablando de redes inalámbricas, se tienen dos topologías básicas:

- Topología ad-hoc
- Topología infraestructura

1.9.3.1 Topología de bus lineal

En este tipo de configuración, las terminales están conectadas a un único canal de comunicación.

Esta topología permite que todas las terminales reciban la información que se transmite; una terminal se encarga de transmitir y las terminales restantes reciben (escuchan) la información.

Básicamente, consiste en un cable con un controlador en cada extremo, del que se cuelgan todos los elementos de una red; esto es, todos los nodos de que consta la red están conectados a este cable, el cual recibe el nombre de “Backbone Cable”.

Tanto Ethernet como Local Talk pueden utilizar esta topología.

El bus es pasivo, esto es, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

La forma de representar una configuración de bus se observa en la figura 1.8

Figura 1.8 Topología de bus

1.9.3.2 Topología de estrella

En esta topología, las estaciones están conectadas directamente al servidor y todas las comunicaciones se han de hacer necesariamente a través de él.

Esto es, los datos fluyen desde el emisor y hasta el controlador, el cual realiza todas las funciones de la red, además de tomar la función de amplificador.

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

La representación de esta topología se observa en la figura 1.9

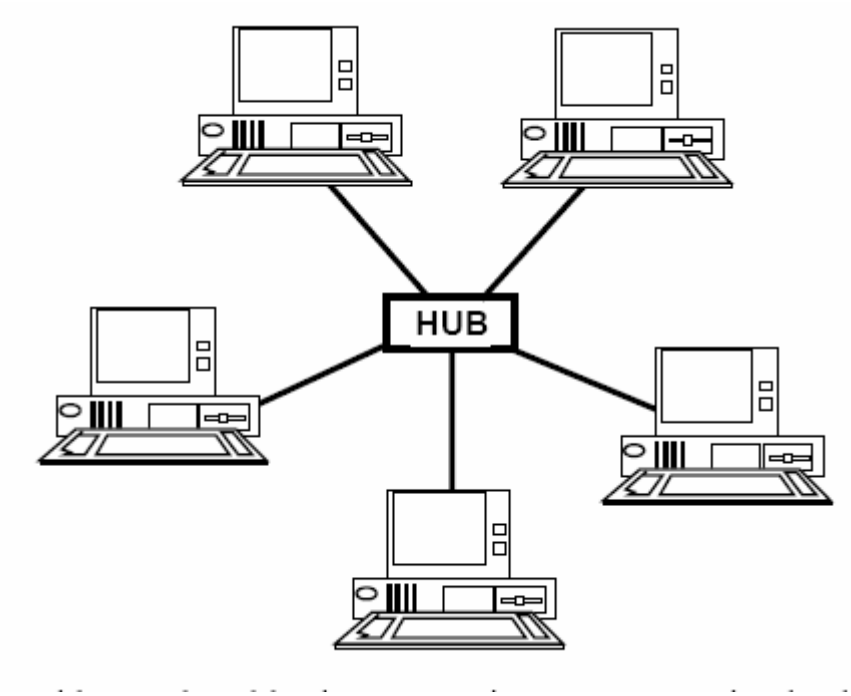


Figura 1.9 Topología en estrella

1.9.3.2.1 Configuración en estrella extendida

La configuración en estrella extendida es una variante de la topología de estrella, y también es llamada topología de malla o trama.

En esta topología se busca tener una conexión física entre todos los ordenadores de la red, utilizando conexiones punto a punto, lo que permitirá que cualquier ordenador se comunique con otros de forma paralela si fuera necesario.

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

La esquematización de esta topología se observa en la figura 1.10

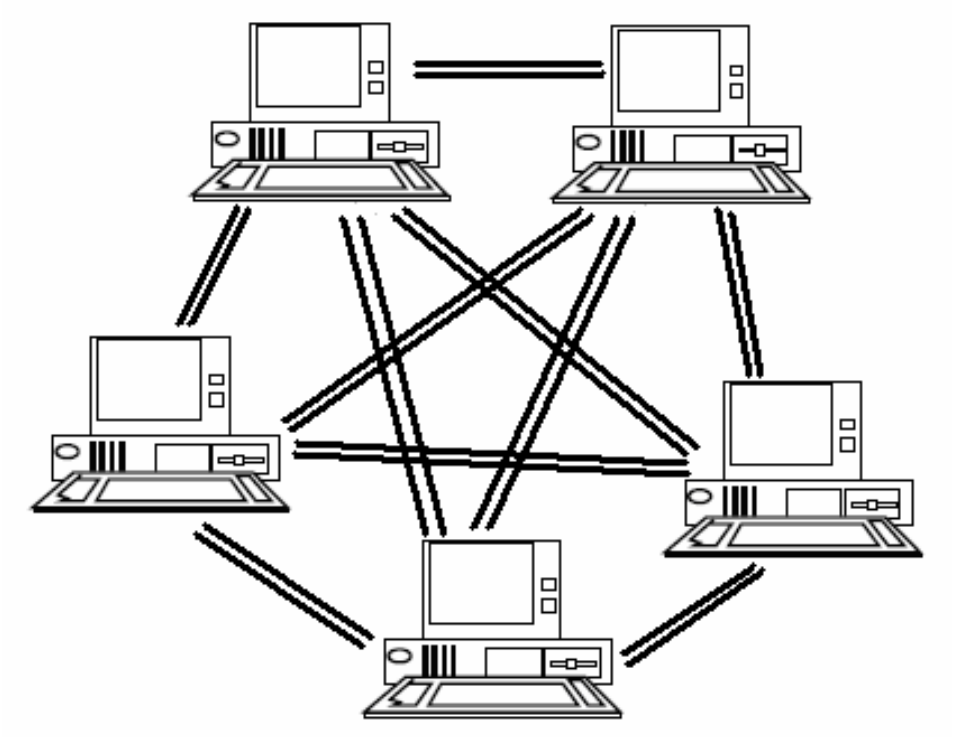


Figura 1.10 Configuración de estrella extendida

1.9.3.2.2 Configuración en árbol

En esta topología los nodos están conectados en forma de árbol. Desde una visión topológica, esta conexión es semejante a una serie de redes interconectadas.

Como la topología de estrella extendida, la configuración en árbol es una variante de la topología de estrella.

Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

Su esquematización se marca en la figura 1.11

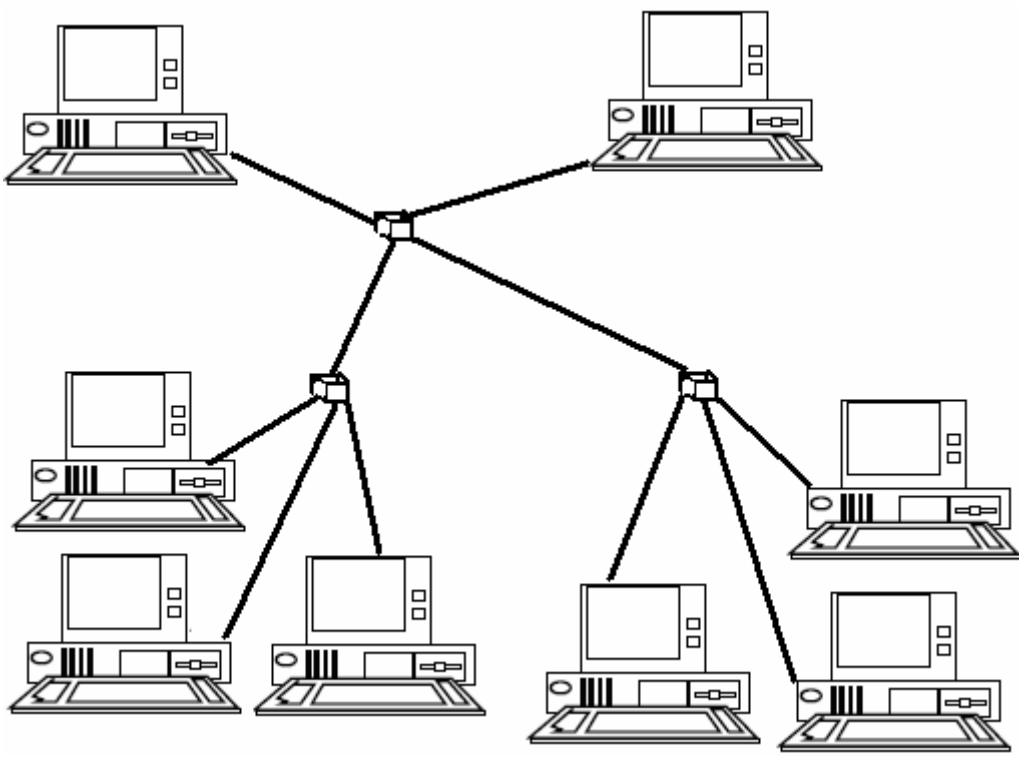


Figura 1.11 Configuración de árbol

1.9.3.3 Topología de anillo

En esta topología, las terminales se conectan formando un anillo. Es decir, cada una está conectada a la siguiente y la última está conectada a la primera

Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo.

La desventaja de la configuración de anillo, es que si se rompe una conexión, se cae la red completa.

Su esquema se muestra en la figura 1.12

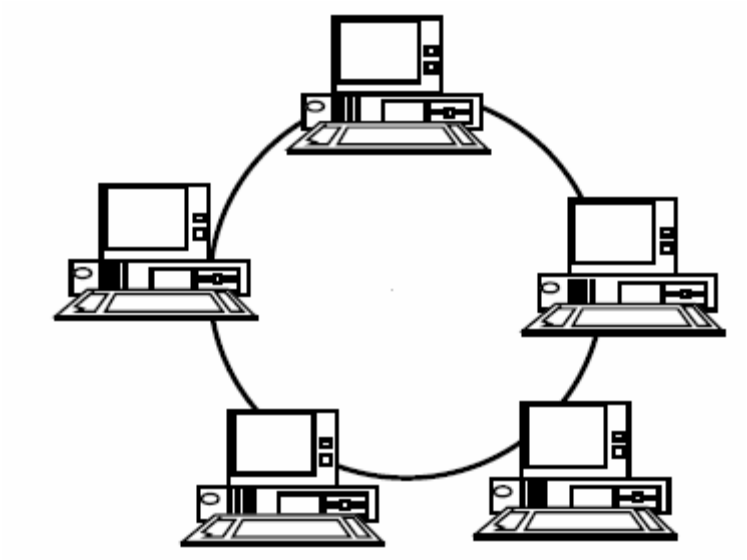


Figura 1.12 Topología de anillo

1.9.3.5 Topologías híbridas

De acuerdo con las necesidades de los usuarios, las topologías más usuales, vistas anteriormente, se pueden combinar para formar una configuración mixta.

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

La finalidad de crear estas complejas topologías es incrementar la eficiencia y confiabilidad de la red en uso.

Estas combinaciones, se pueden observar en la figura 1.13:

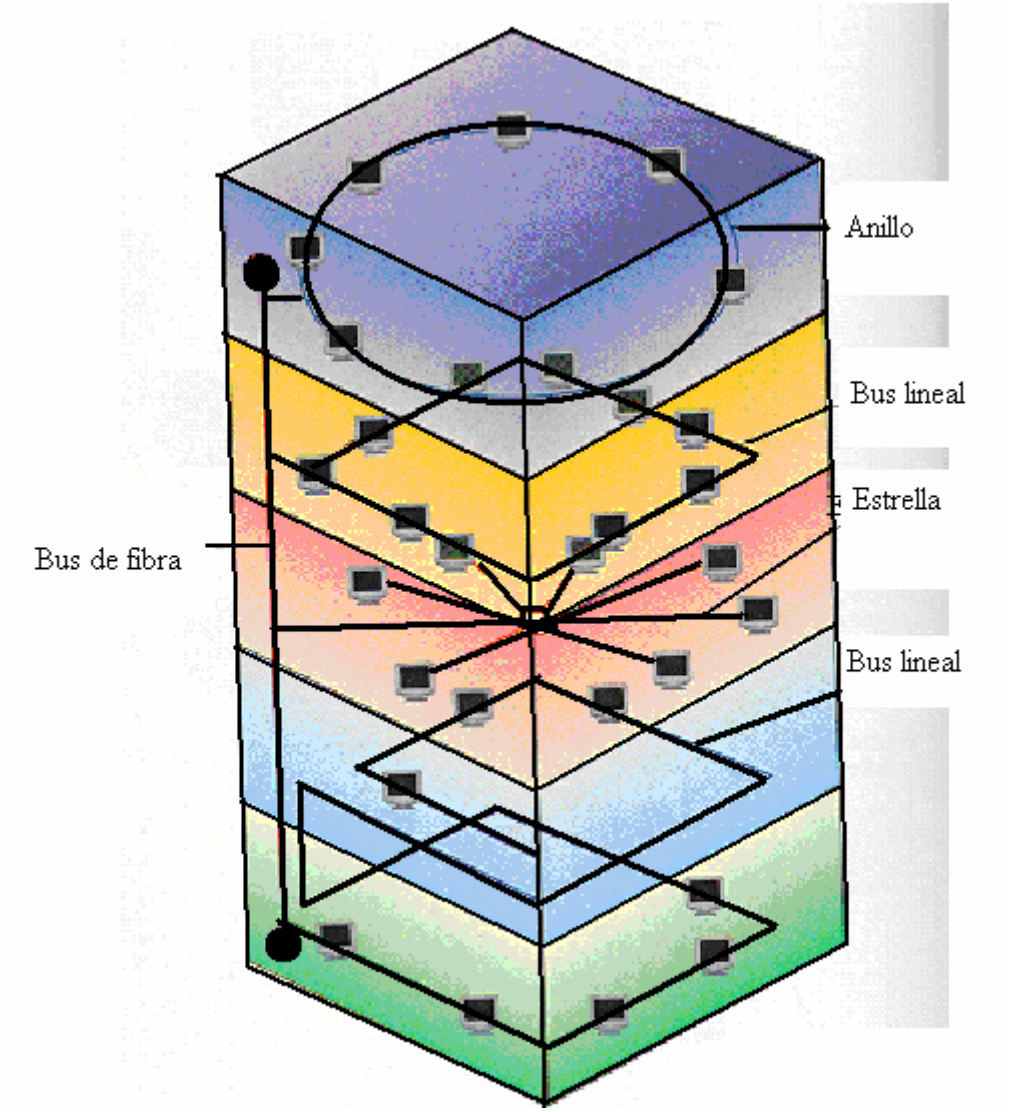


Figura 1.13 Topologías híbridas

1.9.3.5.1 Anillo en estrella

Esta configuración se utiliza con la finalidad de facilitar la administración de la red.

Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo. Esto se observa en la figura 1.14

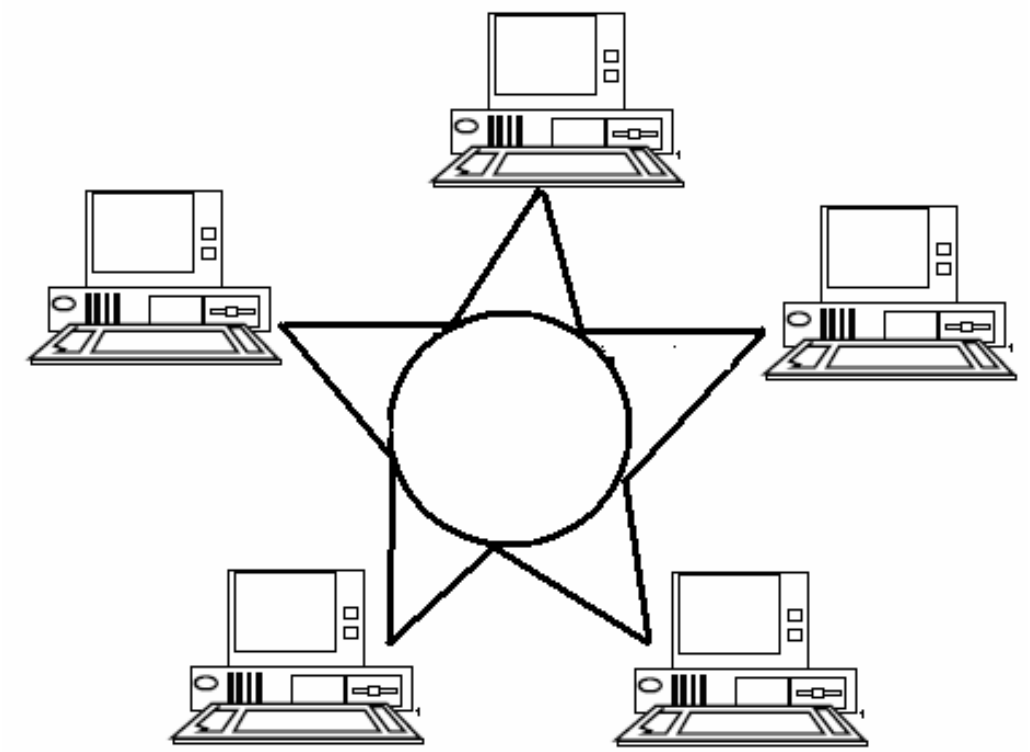


Figura 1.14 Configuración de anillo en estrella

1.9.3.5.2 Bus en estrella

Como en la topología de anillo en estrella, la finalidad de ésta configuración es facilitar la administración de la red

En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Esquemáticamente se podría observar como en la figura 1.15:

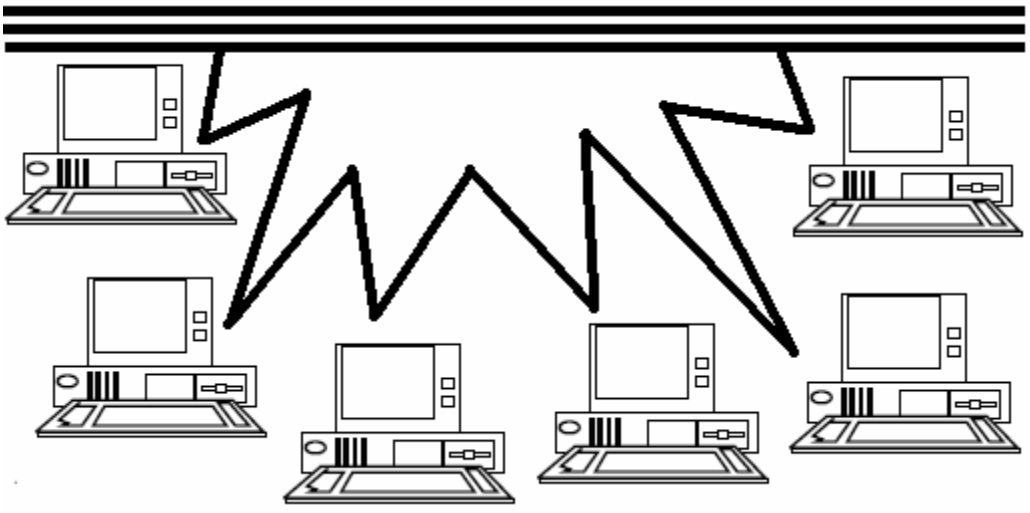


Figura 1.15 Configuración de bus en estrella

1.9.3.5.3 Estrella jerárquica

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formas una red jerárquica.

Se puede observar su configuración en la figura 1.16:

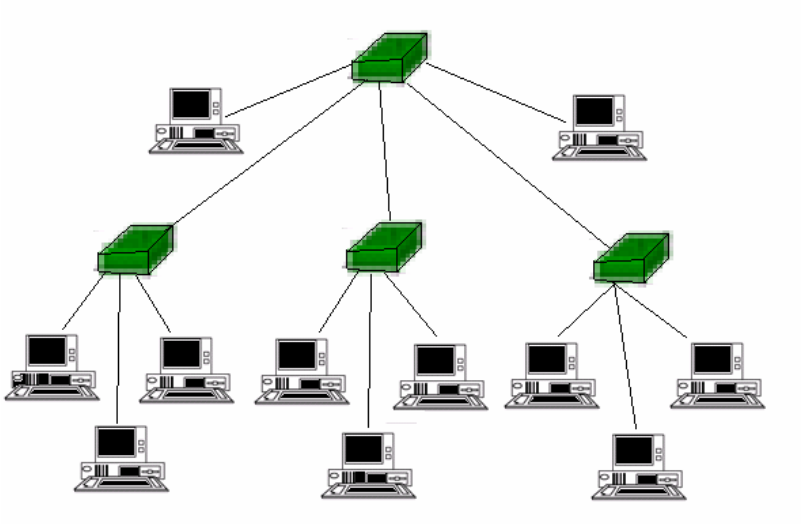


Figura 1.16 Configuración de estrella jerárquica

1.9.3.6 Topología Ad-Hoc

En una topología ad hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica

directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central.

Este tipo de topología es práctica en lugares en lo que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc podría ser un domicilio sin red con cable a una sala de conferencias, en donde los quipos se reúnan con regularidad para intercambiar ideas. En la figura 1.17 se muestra una red de este tipo.

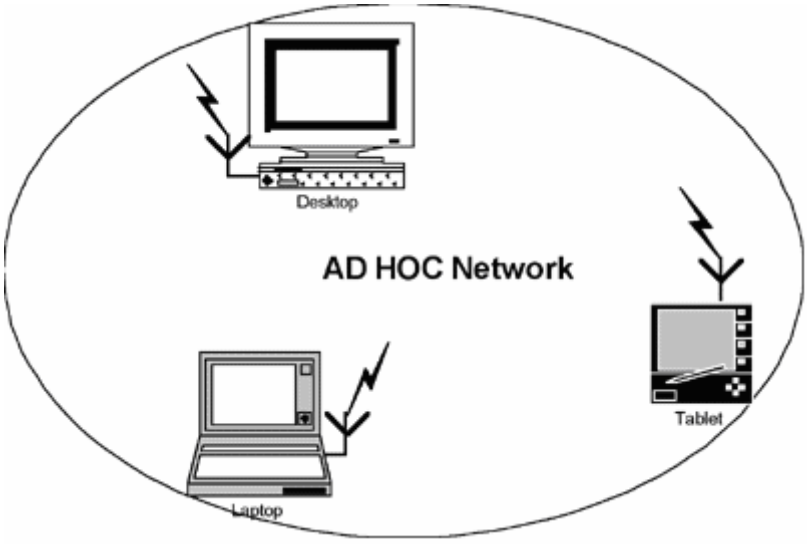


Figura 1.17 Vista clásica de una topología ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

1.9.3.7 Topología infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso.

El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto.

En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

La figura 1.18 muestra una configuración de infraestructura

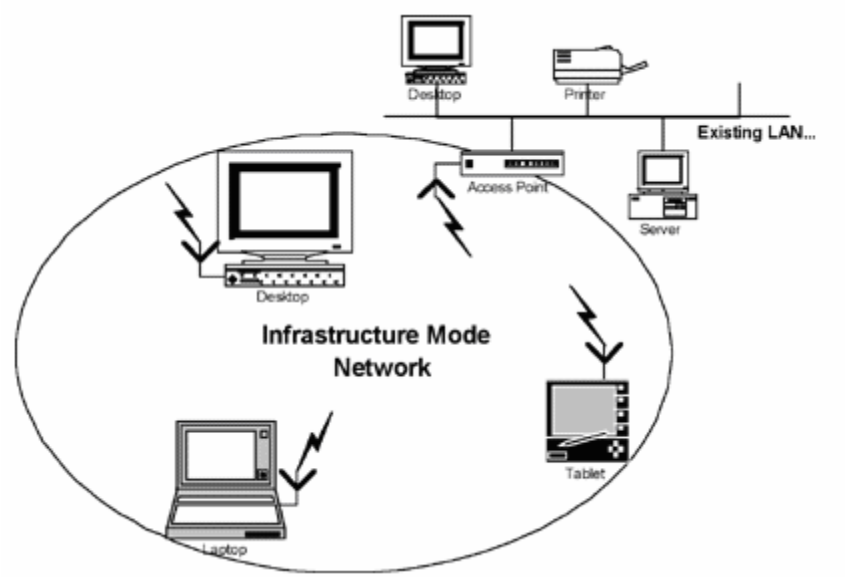


Figura 1.18 Vista clásica de una topología infraestructura

- Capítulo II: Análisis técnico de redes -

2.1 Introducción

La optimización en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la ciencia informática en la actualidad.

Es por ello que la aparición de las plataformas de interconexión de equipos de computación o redes informáticas resultan ser uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en una organización determinada.

2.2 Alcance de las redes

El alcance de una red hace referencia a su tamaño geográfico. El tamaño de una red puede variar desde unos pocos equipos de oficina hasta miles de equipos conectados a través de grandes distancias.

El alcance de una red hace referencia a:

- El número de equipos de la red
- La distancia existente entre los equipos

El alcance de una red está determinado por el tamaño de la organización y/o la distancia entre los usuarios de la red. También determina el diseño de la red y los componentes físicos utilizados en su construcción.

2.3 Análisis de conectividad

Los componentes básicos de la conectividad de una red incluyen: los cables adaptadores de la red y los dispositivos inalámbricos que conectan los equipos al resto de la red. Estos componentes permiten enviar datos a cada equipo de la red, permitiendo que los equipos se comuniquen entre sí.

Algunos de los componentes de conectividad más comunes son:

- Adaptadores de red
- Cables de red
- Dispositivos de comunicación inalámbricos

2.3.1 Adaptadores de red

Cada adaptador de red tiene una dirección exclusiva, denominada dirección de control de acceso al medio (MAC por sus siglas en ingles) incorporada en chips de la tarjeta.

Los adaptadores de red convierten los datos en señales eléctricas que pueden transmitirse a través de un cable. También, convierten las señales eléctricas en paquetes de datos que el sistema operativo puede entender.

Estos dispositivos constituyen la interfaz física entre el equipo y el cable de red. Los adaptadores de red, son también denominados tarjetas de red o NICs (Network Interface Card); se instalan en una ranura de expansión de cada estación de trabajo y servidor de la red. Una vez instalado el adaptador de red, el cable de red se conecta al puerto del adaptador para conectar físicamente el equipo a la red.

Los datos que pasan a través del cable hasta el adaptador de red se formatean en paquetes. Un paquete es un grupo lógico de información que incluye una cabecera, la cual contiene la información de la ubicación y los datos del usuario.

La cabecera contiene campos de dirección que incluyen información sobre el origen de los datos y su destino. El adaptador de red lee la dirección de destino para determinar si el paquete debe entregarse en ese equipo. Si es así, el adaptador de red pasa el paquete al sistema operativo para su proceso. En caso contrario, el adaptador de red rechaza el paquete.

Cada adaptador de red tiene una dirección exclusiva incorporada en los chips de la tarjeta. Esta dirección se denomina dirección física o dirección de control de acceso al medio (media access control, MAC).

Una de las vistas que tiene un adaptador de red, se muestra en la figura 2.1

Figura 2.1 Vista clásica del adaptador de red

2.3.1.1 Funciones del adaptador de red

El adaptador de red realiza las siguientes funciones:

- Recibe datos desde el sistema operativo del equipo y los convierte en señales eléctricas que se transmiten por el cable
- Recibe señales eléctricas del cable y las traduce en datos que el sistema operativo del equipo puede entender
- Determina si los datos recibidos del cable son para el equipo
- Controla el flujo de datos entre el equipo y el sistema de cable

2.3.1.2 Criterios del adaptador de red

Para garantizar la compatibilidad entre el equipo y la red, el adaptador de red debe cumplir los siguientes criterios:

- Ser apropiado en función del tipo de ranura de expansión del equipo
- Utilizar el tipo de conector de cable correcto para el cableado
- Estar soportado por el sistema operativo del equipo.

2.3.2 Cables de red

El cableado de red se refiere a los alambres que conectan los ordenadores individuales o grupos de computadoras y terminales a una red.

El cableado de red es utilizado, dentro de las redes, como un medio de transmisión bruto, el cual cumple con la función de trasladar datos (en forma de bits) de un lugar a otro.

Existen varios tipos de cables con los cuales se puede efectuar la transmisión de datos o de información. Dependiendo del cable utilizado, se maneja la topología de red y sus componentes.

Por supuesto, en las redes inalámbricas el concepto de cableado es inexistente. En su lugar, se utilizan ondas para el envío de información.

Los cables de red de uso común son:

- Cable coaxial
- Cable de par trenzado
- Fibra óptica

Asimismo, se puede hablar de una técnica de redes que recibe el nombre de cableado estructurado.

El cable de par trenzado es el más usual para las redes. El cable coaxial se utiliza cuando los datos viajan por largas distancias. Y, el cable de fibra óptica se usa cuando existe la necesidad de que la información viaje a la velocidad de la luz.

Al conectar equipos para formar una red, se utilizan cables que actúan como medio de transmisión de la red, lo que permite la comunicación entre los equipos conectados. Un cable que conecta dos equipos recibe el nombre de segmento.

Los cables se diferencian por sus capacidades y están clasificados en función de su capacidad para transmitir datos a diferentes velocidades, con diferentes índices de error.

2.3.2.1 Cable coaxial

El cable coaxial está formado por:

- Un núcleo de hilo de cobre rodeado de un aislamiento
- Una capa de metal trenzado
- Una cubierta exterior.

El núcleo de un cable coaxial transporta las señales eléctricas que forman los datos. Este hilo del núcleo puede ser sólido o hebrado.

Existen dos tipos de cable coaxial:

- Cable coaxial ThinNet (10Base2)
- Cable coaxial ThickNet (10Base5).

El cableado coaxial es una buena elección cuando se transmiten datos a través de largas distancias y para ofrecer un soporte fiable a mayores velocidades de transferencia cuando se utiliza equipamiento menos sofisticado. El cable coaxial debe tener terminaciones en cada extremo.

De acuerdo con el tipo de cable coaxial, se puede observar lo siguiente:

- El cable coaxial ThinNet puede transportar una señal en una distancia aproximada de 185 metros.

- El cable coaxial ThickNet puede transportar una señal en una distancia de 500 metros.

Ambos cables, ThinNet y ThickNet, utilizan un componente de conexión (conector BNC) para realizar las conexiones entre el cable y los equipos.

2.3.2.2 Cable par trenzado

El cable de par trenzado (10baseT) está formado por dos hebras aisladas de hilo de cobre trenzado entre sí. Existen dos tipos de cables de par trenzado:

- Par trenzado sin apantallar (unshielded twisted pair, UTP)
- Par trenzado apantallado (shielded twisted pair, STP).

Éstos son los cables que más se utilizan en redes y pueden transportar señales en distancias de 100 metros.

De acuerdo con el tipo de cable par trenzado, se pueden hacer las siguientes observaciones:

- El cable UTP es el tipo de cable de par trenzado más popular y también es el cable en una LAN más popular.

- El cable STP utiliza un tejido de funda de cobre trenzado que es más protector y de mejor calidad que la funda utilizada por UTP. STP también utiliza un envoltorio plateado alrededor de cada par de cables. Con ello, STP dispone de una excelente protección que protege a los datos transmitidos de interferencias exteriores, permitiendo que STP soporte índices de transmisión más altos a través de mayores distancias que UTP.

El cableado de par trenzado utiliza conectores Registered Jack 45 (RJ-45) para conectarse a un equipo. Son similares a los conectores Registered Jack 11 (RJ-11).

2.3.2.3 Cable de fibra óptica

El cable de fibra óptica utiliza fibras ópticas para transportar señales de datos digitales en forma de pulsos modulados de luz. Como el cable de fibra óptica no transporta impulsos eléctricos, la señal no puede ser intervenida y sus datos no pueden ser robados.

El cable de fibra óptica es adecuado para transmisiones de datos de gran velocidad y capacidad ya que la señal se transmite muy rápidamente y con muy poca interferencia.

Un inconveniente de este tipo de cable es que se rompe fácilmente si la instalación no se hace cuidadosamente. Por otro lado, es más difícil de cortar que otros cables y requiere un equipo especial para cortarlo.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

- Monomodo:. Permite la transmisión de señales con ancho de banda hasta 2 GHz.
- Multimodo de índice gradual:. Permite transmisiones hasta 500 MHz.
- Multimodo de índice escalonado: Permite transmisiones hasta 35 MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda.

Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas. Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad.

2.3.3 Dispositivos de comunicación inalámbrica

Los componentes inalámbricos se utilizan para la conexión a redes en distancias que hacen que el uso de adaptadores de red y opciones de cableado estándares sea técnica o económicamente imposible. Las redes inalámbricas están formadas por componentes inalámbricos que se comunican con redes de área local.

Excepto por el hecho de que no es un cable quién conecta los equipos, una red inalámbrica típica funciona casi igual que una red con cables: se instala en cada equipo un adaptador de red inalámbrico con un transceptor (un dispositivo que transmite y recibe señales analógicas y digitales). Los usuarios se comunican con la red igual que si estuvieran utilizando un equipo con cables.

Existen dos técnicas habituales para la transmisión inalámbrica en una red de área local:

- Transmisión por infrarrojos
- Transmisión de radio en banda estrecha.

2.3.3.1 Transmisión por infrarrojos

La transmisión por infrarrojos funciona utilizando un haz de luz infrarroja que transporta los datos entre dispositivos.

Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben; si hay algo que bloquee la señal infrarroja, puede impedir la comunicación. Estos sistemas deben generar señales muy potentes, ya que las señales de transmisión débiles son susceptibles de recibir interferencias de fuentes de luz, como ventanas.

2.3.3.2 Transmisión vía radio en banda estrecha

El usuario sintoniza el transmisor y el receptor a una determinada frecuencia. La radio en banda estrecha no requiere visibilidad directa porque utiliza ondas de radio.

Sin embargo, la transmisión vía radio en banda estrecha está sujeta a interferencias de paredes de acero e influencias de carga. La radio en banda estrecha utiliza un servicio de suscripción. Los usuarios pagan una cuota por la transmisión de radio.

2.4 Estructuras en redes

Como se ha hecho mención anteriormente, las redes suelen dividirse de muchas maneras; las más importantes son:

- De acuerdo con el territorio que abarcan
- De acuerdo a su tipo de conexión

La figura 2.2 muestra la clasificación de redes

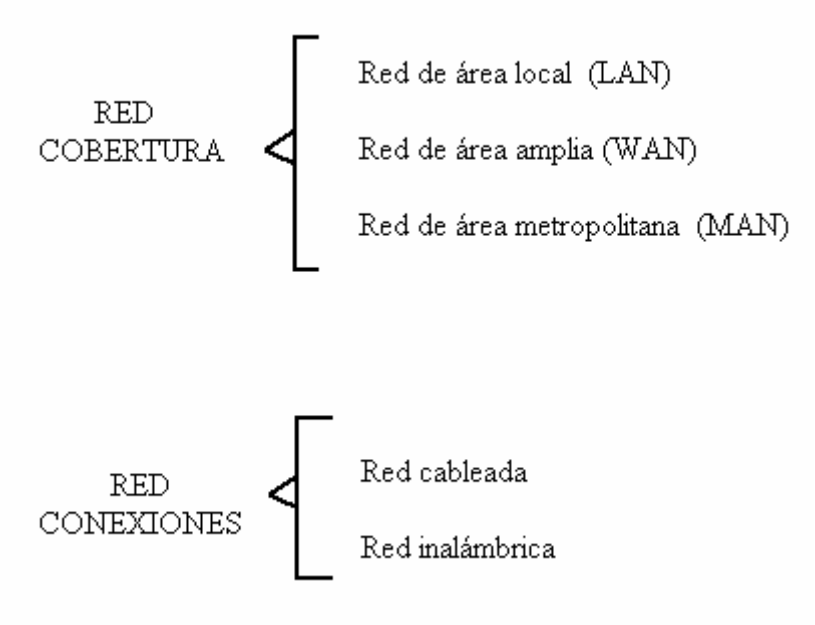


Figura 2.2 Criterios de clasificación de redes

2.4.1 Red de área local (LAN)

La definición más general de una red de área local es la de una red de comunicaciones utilizada por una sola organización a través de una distancia limitada, la cual permite a los usuarios compartir información y recursos.

La ubicación de las computadoras es un factor decisivo para determinar cuando una red es de área local o no. El ancho de banda, el medio de conexión, la capacidad y el número de ordenadores conectados a la red, son datos irrelevantes para el tipo de red que se maneja.

2.4.1.1 Características de una LAN

Los ordenadores conectados a una red local pueden ser grandes computadores o computadoras personales, con sus distintos tipos de periféricos. Aunque hay muchos tipos de redes locales; entre ellas existen características comunes a todas; como las siguientes:

- Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes locales están contenidas en una reducida área física.

- Una transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. El equipo de la red local puede transmitir datos a la velocidad máxima a la que pueden comunicarse las estaciones de la red, suele ser un MB por segundo.

- Una distancia entre estaciones, relativamente corta, entre unos metros y varios kilómetros.

- La posibilidad de uso de cables de conexión normales.

- Todos los dispositivos pueden comunicarse con el resto, y algunos de ellos pueden funcionar independientemente.

- Un sistema fiable, con un índice de errores muy bajo. Las redes locales disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.

- Flexibilidad, en donde el usuario administra y controla su propio sistema.

2.4.1.2 Componentes LAN

Los tipos básicos de dispositivos que pueden conectarse a una red local son:

- Las estaciones de trabajo
- Los servidores

Una estación de trabajo es un ordenador desde donde el usuario puede acceder a los recursos de la red.

Un servidor es un computador que permite a otros computadores que accedan a los recursos de que dispone.

Los servidores pueden ser:

- Dedicados
- No dedicados

Los servidores dedicados son aquellos que brindan un servicio específico dentro de una red; es decir, se especializa en una sola función.

En un servidor dedicado recae solamente una parte de la carga de trabajo de toda la red. Éste tiene variantes, tales como:

- De archivos
- De impresión
- De comunicación

Un servidor de archivos atiende los pedidos de acceso de los clientes a un medio de almacenamiento masivo. El acceso de los clientes a este medio de almacenamiento puede incluir las operaciones con archivos siguientes:

- Leer
- Escribir
- Copiar
- Modificar
- Crear
- Borrar
- Mover
- Ejecutar

En cada una de estas tareas, el servidor de archivos controla que el pedido de acceso del cliente al medio de almacenamiento masivo se corresponda con los permisos que haya definido el usuario administrador de la red para ese cliente en particular; de lo contrario, se negará el acceso.

El servidor de impresión administra los pedidos de impresión de los clientes. Para esto, recibe los archivos a imprimir (que pueden ser archivos; de texto, gráficos o imágenes), los almacena en una cola de espera y le da la orden a la impresora para que los vaya imprimiendo uno por uno, en la misma secuencia en que llegaron.

En este caso, la impresora se encuentra instalada en forma directa al puerto de impresión del servidor, mientras que los otros ordenadores (los clientes) acceden a esta a través de la red

El servidor de comunicaciones, también conocido como gateway, recibe los pedidos de transmisión de una red, los traduce y los entrega a su destino, que puede ser otra red, con un sistema operativo y/o protocolos diferentes.

La función de estos servidores es la de oficiar traductores entre dos redes distintas.

Por otro lado, el servidor no dedicado puede trabajar simultáneamente como servidor y como estación de trabajo.

De forma general, en una red, al nodo que pide un servicio o inicia una comunicación, se le denomina cliente. Al nodo que responde a la petición, se le denomina servidor.

Las formas de formar una red LAN se muestran en la figura 2.3.

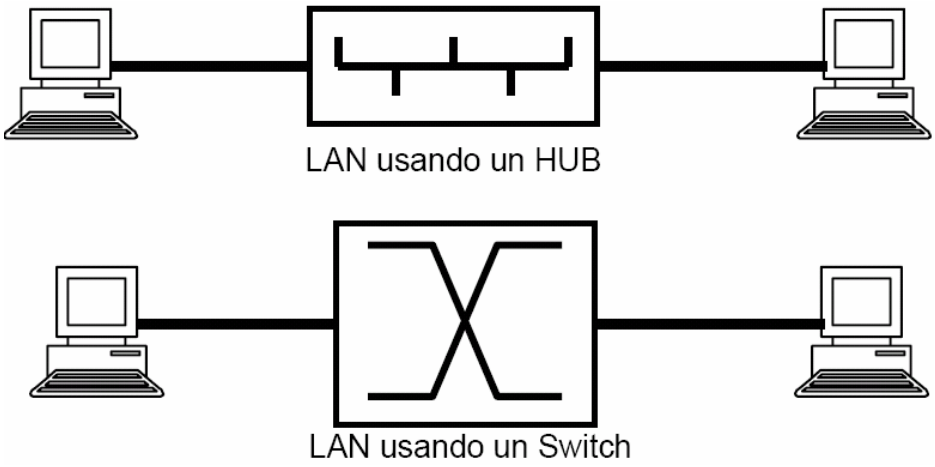


Figura 2.3 Conexiones de una red LAN

2.4.2 Red de área extensa (WAN)

Las redes de área o cobertura amplia (WAN, son todas aquellas redes que cubren una extensa área geográfica. Generalmente, son una serie de dispositivos de conmutación interconectados. Se desarrollaron por dos vías:

- Utilizando tecnología de conmutación de circuitos
- Utilizando tecnología de conmutación de paquetes

Cuando una red de área local crece y expande la cantidad de computadores y usuarios en diversas localidades o ubicaciones, se convierte en una red de área extensa.

Las maneras de realizar conexiones de una red WAN a través de redes LAN´s se muestran en la figura 2.4.

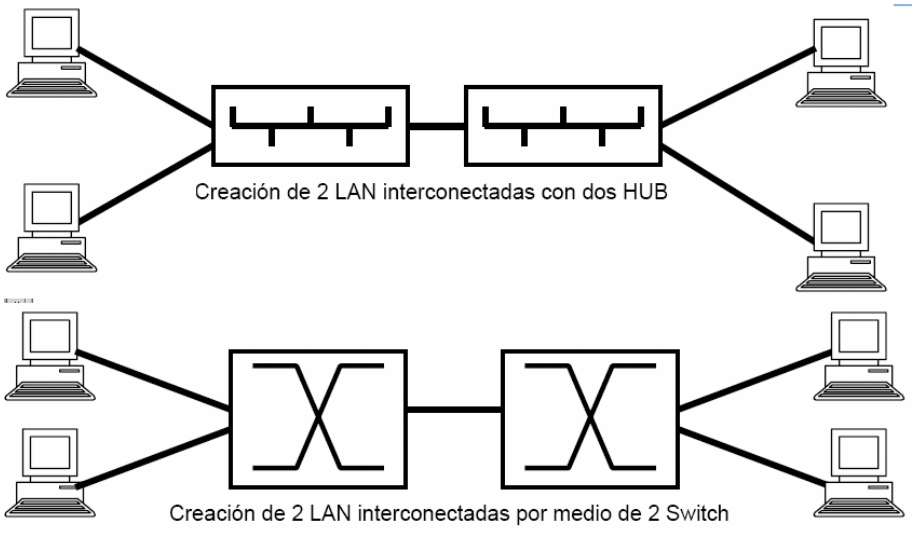


Figura 2.4 Conexión de Red WAN

Otra manera de formar redes WAN es conectando redes LAN a Internet, como se muestra en la figura 2.5.

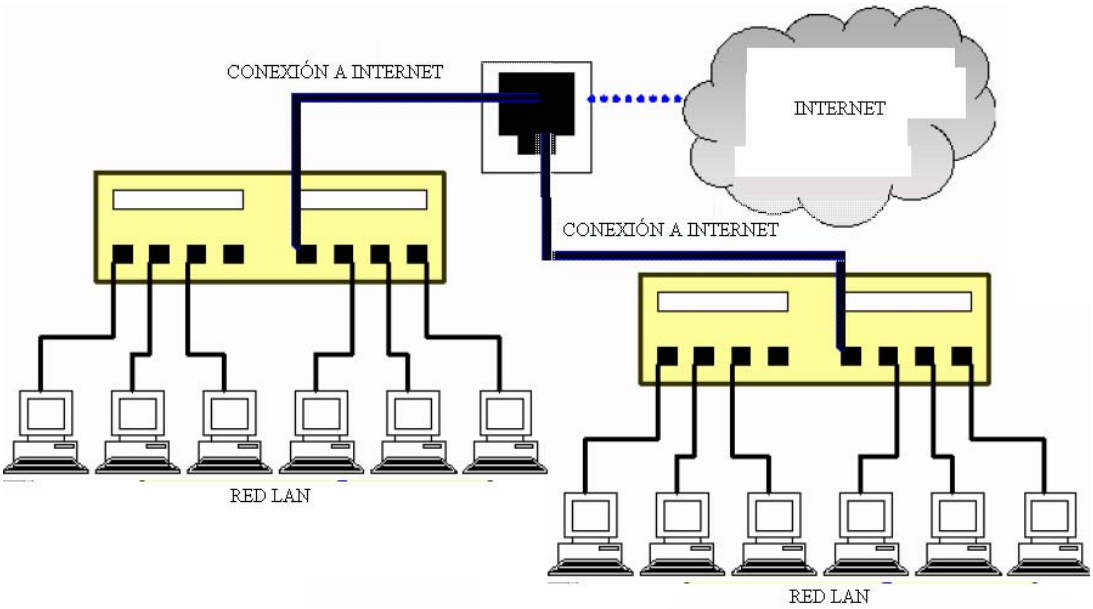


Figura 2.5 Conexión de red WAN a través de Internet

2.4.3 Red de área metropolitana (MAN)

Una red de área metropolitana (MAN) es una red que se expande por pueblos o ciudades, y se interconecta mediante diversas instalaciones públicas o privadas. Ejemplos de este tipo de red son: sistemas telefónicos o los suplidores de sistemas de comunicación por microondas o medios ópticos.

2.4.4 Red inalámbrica

Una red inalámbrica puede definirse como una red local que utiliza tecnología de radiofrecuencia para enlazar los equipos conectados a la red en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableados. Estos enlaces se implementan mediante tecnología basada en microondas o bien en infrarrojos.

La tecnología basada en microondas se puede considerar como la más desarrollada, dado que es donde se han conseguido los resultados más claros. La tecnología basada en infrarrojos, actualmente es la menos desarrollada, porque las distancias que cubren son cortas y aún existen una serie de problemas técnicos por resolver. A pesar de ello, presenta la ventaja frente a las microondas de que no existe el problema de la saturación del espectro de frecuencias, lo que la hace llamativa.

Las redes inalámbricas tienen las siguientes características particulares:

- Traspasan edificios, paredes, sin correr peligro
- Están listas para la acción en pocos minutos
- Permiten a sus usuarios trabajar en redes de equipos portátiles

La forma de visualizar las redes inalámbricas se observan en la figura 2.6.

Figura 2.6 Vista de redes inalámbricas

2.4.4.1 Condiciones de uso de redes inalámbricas

Hay ciertos casos en los que la utilización de una red convencional se vuelve imposible. Las empresas pueden tener sectores en edificios separados, y para compartir la información, el uso de redes cableadas no es la solución indicada, ya sea por la distancia entre ambas áreas o por inconvenientes tales como:

- Que el trayecto del cable esté cruzado por una ruta.
- Que en algunos edificios no se puedan realizar cableados adicionales.

Las redes inalámbricas aparecieron para solucionar estos inconvenientes. Existen, dentro de la tecnología inalámbrica, diversas vertientes aplicadas a las redes en general (principalmente hablan de de redes locales). Estas redes pueden subdividirse en:

- Industriales
- Empresariales
- Caseras o de hogar.

2.4.4.2 Redes inalámbricas industriales

Las redes inalámbricas industriales son, precisamente, las utilizadas en industrias que necesitan los datos en tiempo real de determinados sectores en los que la información solicitada se encuentra en constante movimiento físico (almacenamiento, stock, montaje), y la utilización de un terminal convencional con una red cableada impide que la información sea entregada de manera instantánea.

Para plantear el concepto aún más claramente, se puede tomar el ejemplo de un autoelevador, que apila la mercadería de los camiones que entran en los depósitos, y el operador debe llenar un formulario con la mercadería descargada y luego transcribir nuevamente la información del formulario en una computadora que agrega este nuevo stock.

En cambio, al utilizar una red inalámbrica, el operador puede contar en el mismo autoelevador con una computadora portátil que utiliza una placa de red wireless. Al llegar la mercadería, ingresa directamente la información en la computadora, y ésta figurará de inmediato en la base de datos del stock de la empresa.

Éste es un ejemplo básico de lo que se puede realizar, aunque hay más usos. Las redes industriales pueden trabajar desde cortas distancias hasta varios kilómetros, utilizando antenas especiales.

2.4.4.3 Redes inalámbricas empresariales

Las redes inalámbricas empresariales son las que se utilizan cuando se necesita enlazar las diferentes redes de la empresa, y éstas se encuentran separadas físicamente (en diferentes edificios, por ejemplo).

Este tipo de redes permiten a los ejecutivos desplazarse con sus equipos portátiles por todo el entorno de la compañía y trabajar en cualquier lugar, tal como lo harían desde su oficina. Estas redes son utilizadas por grandes empresas, corporaciones o universidades.

2.4.4.4 Redes inalámbricas para el hogar

Las redes inalámbricas de hogar son las más pequeñas y sencillas. Esto se debe a que la cantidad de equipos que comparten la información es menor y el volumen de ésta es ínfimo comparado con el de una red industrial.

Este tipo de red se utiliza en pequeñas y medianas industrias, o en hogares, donde, si bien la velocidad y el volumen de información son importantes, no tienen un carácter crítico.

2.5 Análisis de topologías

Como se ha mencionado anteriormente, una topología es la estructura de equipos, cables y demás componentes en una red. Es un mapa de la red física. El tipo de topología utilizada afecta al tipo y capacidades del hardware de red, su administración y las posibilidades de expansión futura.

La topología puede tomarse en cuenta de una manera física o de una manera lógica; por lo general, al hablar de una red, es necesario manejar ambas. En este sentido, se puede describir a ellas como sigue:

- La topología física describe cómo están conectados los componentes físicos de una red.
- La topología lógica describe el modo en que los datos de la red fluyen a través de componentes físicos.

Básicamente, se habla de cinco topologías:

- Bus
- Estrella
- Anillo
- Malla
- Híbrida

También, se habla de dos topologías básicas en redes inalámbricas:

- Ad-hoc
- infraestructura

2.5.1 Topología de bus

En la topología de bus, los equipos están conectados a un cable común compartido; es decir, todos los equipos de una red están unidos a un cable continuo, o segmento, que los conecta en línea recta.

En esta topología en línea recta, el paquete se transmite a todos los adaptadores de red en ese segmento.

Algunos puntos importantes para este tipo de conexión son:

- Los dos extremos del cable deben tener terminaciones.

- Todos los adaptadores de red reciben el paquete de datos.

- Debido a la forma de transmisión de las señales eléctricas a través de este cable, sus extremos deben estar terminados por dispositivos de hardware denominados terminadores, que actúan como límites de la señal y definen el segmento.

- Si se produce una rotura en cualquier parte del cable o si un extremo no está terminado, la señal balanceará hacia adelante y hacia atrás a través de la red y la comunicación se detendrá.

- El número de equipos presentes en un bus también afecta al rendimiento de la red. Cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus, y en consecuencia, la red irá más lenta.

- Debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho ruido. Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente. Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.

2.5.1.1 Características de la topología de bus

Las principales características de la topología de bus son:

- Consta de un único cable que se extiende de un ordenador al siguiente de un modo serie. Todas las estaciones están conectadas a un único canal

- Los extremos del cable se terminan con una resistencia denominada terminador, que además de indicar que no existen más ordenadores en el extremo conectados a la red, permiten cerrar el bus.

- Los dispositivos conectados en bus, disponen de un alto nivel de inteligencia; de lo contrario, deberán disponer de una unidad de interfaz que señale las direcciones de cada ordenador conectado.

- Puesto que las estaciones más cercanas a la estación emisora reciben una señal muy fuerte que las que se encuentran en los extremos, los transmisores y los receptores utilizados por la red deberán ser capaces de tolerar una amplia gama de señales. Por ello, es conveniente limitar la longitud de segmento del cable y el número de estaciones conectadas.

2.5.1.2 Ventajas de la topología de bus

En general, se pueden enumerar las siguientes ventajas de la topología de bus para la conexión de redes:

- Es muy simple y fácil de dar mantenimiento.
- Es muy fácil de instalar y mantener.
- Es relativamente más económica que cualquier otra, ya que requiere menos cableado a diferencia de las otras topologías.
- Es especialmente cómoda para una pequeña red y temporera.
- Es una topología adecuada para tráfico muy alto.
- Existe una interconexión total entre los equipos que integran la red.
- Es sencillo conectar nuevos dispositivos.
- Hay una gran facilidad de ampliación, y se pueden agregar fácilmente nuevas estaciones o ampliar la red añadiendo una nueva línea conectada mediante un repetidor.
- No existen elementos centrales de los que dependa toda la red, cuyo fallo dejaría sin operación a todas las estaciones.

2.5.1.3 Desventajas de la topología de bus

Entre las desventajas de la topología de bus para la conexión de redes, se pueden enumerar las siguientes:

- Algún fallo en una parte del cableado detendría el sistema, ya sea de manera parcial o total. Esto depende del lugar en que dicho fallo se produzca. Por otro lado, es muy difícil localizar las averías por la manera de conexión de la red; sin embargo, ya localizada la falla, es muy sencilla su reparación.
- Todos los nodos han de ser inteligentes, ya que han de manejar el medio de comunicación compartido.
- Debido a que la información recorre el bus bidireccionalmente hasta encontrar su destino, la posibilidad de que sea interceptada por usuarios no autorizados es superior a la existente en las otras topologías.
- El sistema no reparte equitativamente los recursos.

- La red es vulnerable a la atenuación, ya que pierde señal a través de la distancia del cable.

- La interfaz con el medio de transmisión ha de hacerse por medio de dispositivos inteligentes; de no ser así, se requiere de unidades de interfaz muy sofisticadas.

- La longitud del medio de transmisión no sobrepasa los dos mil metros, generalmente.

2.5.2 Topología de estrella

En la topología de estrella, los equipos están conectados a segmentos de cable que se extienden desde una ubicación central, o concentrador; esto es, los segmentos de cable de cada equipo en la red están conectados a un componente centralizado, o concentrador.

Un concentrador es un dispositivo que conecta varios equipos juntos. En una topología en estrella, las señales se transmiten desde el equipo, a través del concentrador, a todos los equipos de la red. A mayor escala, múltiples LAN´s pueden estar conectadas entre sí en una topología en estrella.

2.5.2.1 Ventajas de la topología de estrella

Las ventajas en el uso de la topología de estrella para la interconexión de redes se enumeran como sigue:

- Si uno de sus equipos falla, únicamente este equipo es incapaz de enviar o recibir datos. El resto de la red funciona normalmente.

- La detección y localización de averías es sencilla.

- Es posible conectar terminales no inteligentes, ya que el nodo central tiene capacidad de proceso.

- Es fácil de reconfigurar, añadir o remover una computadora de la red.

2.5.2.2 Desventajas de la topología en estrella

Básicamente, los inconvenientes de utilizar una topología de estrella son:

- Debido a que cada equipo está conectado a un concentrador, si éste falla, fallará toda la red. Además, en una topología en estrella, el ruido se crea en la red.

- Se necesitan longitudes grandes de cableado, ya que dos estaciones cercanas entre sí, pero distantes del nodo central, requieren, cada una, un cable que las una a éste.

- Poseen limitaciones en cuanto a expansión, dado que cada canal requiere una línea y una interfaz al nodo principal.

- La carga de la red es muy elevada en el nodo central, por lo que éste no se puede utilizar más que como servidor o controlador.

- No soporta cargas de tráfico elevadas por sobrecarga del nodo central.

- El cable viaja por separado del hub a cada computadora.

2.5.3 Topología de anillo

En una topología en anillo, los equipos están conectados con un cable de forma circular. A diferencia de la topología de bus, no hay extremos con terminaciones.

Las señales viajan alrededor del bucle en una dirección y pasan a través de cada equipo, que actúa como repetidor para amplificar la señal y enviarla al siguiente equipo.

A mayor escala, en una topología en anillo múltiples LANs pueden conectarse entre sí utilizando el cable coaxial ThickNet o el cable de fibra óptica.

2.5.3.1 Ventajas de la topología de anillo

Entre las ventajas que ofrece la topología de anillo para la conexión de redes, sobresalen las siguientes:

- Es posible realizar el enlace mediante fibra óptica, por sus características de unidireccionalidad, con las ventajas de su alta velocidad y fiabilidad.

- Cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo, conservando la potencia de la señal.

- Puede gestionar mejor entornos con mucho tráfico que las redes con bus.

- Además, hay mucho menos impacto del ruido en las topologías en anillo que en las otras.

2.5.3.2 Desventajas de la topología de anillo

Las desventajas de este tipo de topología son:

- Los equipos sólo pueden enviar los datos de uno en uno en un único Token Ring.
- Las topologías en anillo son normalmente más caras que las tecnologías de bus.
- La caída de un nodo supone la paralización de la red.
- Es difícil la localización de fallos.
- La reconfiguración de la red es complicada, puesto que el incluir un ordenador más en la red, implica variar el nodo anterior y posterior de varios nodos de la red.

2.5.3.3 Topología de anillo doble

La topología de anillo doble es una topología que consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí.

Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

Los equipos están conectados a un cable que forma un bucle alrededor de una ubicación central.

2.5.3.4 Paso de testigo

El método de transmisión de datos alrededor del anillo se denomina paso de testigo (token passing). Un testigo es una serie especial de bits que contiene información de control. La posesión del testigo permite a un dispositivo de red transmitir datos a la red. Cada red tiene un único testigo.

El equipo emisor retira el testigo del anillo y envía los datos solicitados alrededor del anillo. Cada equipo pasa los datos hasta que el paquete llega el equipo cuya dirección coincide con la de los datos. El equipo receptor envía un mensaje al equipo emisor indicando que se han recibido los datos. Tras la verificación, el equipo emisor crea un nuevo testigo y lo libera a la red.

2.5.4 Topología de malla

En una topología de malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el en lace conduce el tráfico únicamente entre los dos dispositivos que conecta.

Por lo tanto, una red en malla completamente conectada, necesita

$$\frac{n(n-1)}{2}$$

canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S).

A mayor escala, múltiples LANs pueden estar en estrella conectadas entre sí en una topología de malla utilizando red telefónica conmutada, un cable coaxial ThickNet o el cable de fibra óptica.

2.5.4.1 Ventajas de la topología de malla

Las ventajas que ofrece la topología de malla son:

- El uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminan do el problema que surge cuando los enlaces son compartidos por varios dispositivos.

- Una topología en malla es robusta, si un enlace falla, no inhabilita todo el sistema.

- Ofrece privacidad y seguridad. Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes.

- Los equipos de la red están conectados entre sí mediante un cable. Esta configuración proporciona rutas redundantes a través de la red de forma que si un cable falla, otro transporta el tráfico y la red sigue funcionando.

- Una de las ventajas de las topologías de malla es su capacidad de respaldo al proporcionar múltiples rutas a través de la red.

2.5.4.2 Desventajas de la topología de malla

Se puede decir que, debido a que las rutas redundantes requieren más cable del que se necesita en otras topologías, una topología de malla puede resultar cara.

2.5.5 Topología híbrida

Actualmente, las topologías híbridas son las más frecuentes y se derivan de las anteriores, conocidas como topologías puras.

En una topología híbrida, se combinan dos o más topologías para formar un diseño de red completo. Raras veces, se diseñan las redes utilizando un solo tipo de topología.

Por ejemplo, es posible que desee combinar una topología en estrella con una topología de bus para beneficiarse de las ventajas de ambas.

Resulta importante destacar que, en una topología híbrida, si un solo equipo falla, no afecta al resto de la red.

Normalmente, se utilizan dos tipos de topologías híbridas:

- Topología en estrella-bus
- Topología en estrella-anillo.

En una topología en estrella-bus, varias redes de topología en estrella están conectadas a una conexión en bus. Cuando una configuración en estrella está llena, podemos añadir una segunda en estrella y utilizar una conexión en bus para conectar las dos topologías en estrella.

En una topología en estrella-bus, si un equipo falla, no afectará al resto de la red. Sin embargo, si falla el componente central, o concentrador, que une todos los equipos en estrella, todos los equipos adjuntos al componente fallarán y serán incapaces de comunicarse.

En la topología en estrella-anillo, los equipos están conectados a un componente central al igual que en una red en estrella. Sin embargo, estos componentes están enlazados para formar una red en anillo.

Al igual que la topología en estrella-bus, si un equipo falla, no afecta al resto de la red. Utilizando el paso de testigo, cada equipo de la topología en estrella-anillo tiene las mismas oportunidades de comunicación. Esto permite un mayor tráfico de red entre segmentos que en una topología en estrella-bus.

2.5.6 Topología ad-hoc

Del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes.

Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación.

La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

2.5.7 Topología infraestructura

Dentro de esta topología, el portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles.

Este proceso se lleva a cabo mediante el control de las tramas de señalización que proceden de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras).

Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. En la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones.

Entre estas estaciones, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red.

Incluso si una estación no puede oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

2.6 Tecnología de redes

Utilizamos diferentes tecnologías de redes para la comunicación entre equipos redes. Se puede utilizar una combinación de tecnologías para obtener la mejor relación costo-beneficio y la máxima eficacia del diseño de la red.

Hay muchas tecnologías de redes disponibles, entre las que se encuentran:

- Ethernet
- Token ring
- Modo de transferencia asíncrona (asynchronous transfer mode, ATM)
- Interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface, FDDI)
- Frame relay.

Una de las principales diferencias entre estas tecnologías es el conjunto de reglas utilizada por cada una para insertar datos en el cable de red y para extraer datos del mismo. Este conjunto de reglas se denomina método de acceso.

Cuando los datos circulan por la red, los distintos métodos de acceso regulan el flujo del tráfico de red.

2.6.1 Ethernet

Ethernet es una popular tecnología LAN que utiliza el Acceso múltiple con portadora y detección de colisiones (Carrier Sense Múltiple Access with Collision Detection, CSMA/CD) entre estaciones con diversos tipos de cables.

Ethernet es pasivo, lo que significa que no requiere una fuente de alimentación propia, y por tanto no falla a menos que el cable se corte físicamente o su terminación sea incorrecta. Ethernet se conecta utilizando una topología de bus en la que el cable está terminado en ambos extremos.

Ethernet utiliza múltiples protocolos de comunicación y puede conectar entornos informáticos heterogéneos, incluyendo Netware, UNIX, Windows y Macintosh.

2.6.1.1 Métodos de acceso

El método de acceso a la red utilizado por Ethernet es el Acceso múltiple con portadora y detección de colisiones (Carrier Sense Múltiple Access with Collision Detection, CSMA/CD).

CSMA/CD es un conjunto de reglas que determina el modo de respuesta de los dispositivos de red cuando dos de ellos intentan enviar datos en la red simultáneamente. La transmisión de datos por múltiples equipos simultáneamente a través de la red produce una colisión.

Cada equipo de la red, incluyendo clientes y servidores, rastrea el cable en busca de tráfico de red. Únicamente cuando un equipo detecta que el cable está libre y que no hay tráfico envía los datos. Después de que el equipo haya transmitido los datos en el cable, ningún otro equipo puede transmitir datos hasta que los datos originales hayan llegado a su destino y el cable vuelva a estar libre. Tras detectar una colisión, un dispositivo espera un tiempo aleatorio y a continuación intenta retransmitir el mensaje.

Si el dispositivo detecta de nuevo una colisión, espera el doble antes de intentar retransmitir el mensaje.

2.6.1.2 Velocidad de transferencia

Ethernet estándar, denominada 10BaseT, soporta velocidades de transferencia de datos de 10 Mbps sobre una amplia variedad de cableado.

También están disponibles versiones de Ethernet de alta velocidad. Fast Ethernet (100BaseT) soporta velocidades de transferencia de datos de 100 Mbps y Gigabit Ethernet soporta velocidades de 1 Gbps (gigabit por segundo) o 1,000 Mbps.

2.6.2 Token ring

Las redes Token ring están implementadas en una topología en anillo. La topología física de una red Token Ring es la topología en estrella, en la que todos los equipos de la red están físicamente conectados a un concentrador o elemento central.

El anillo físico está cableado mediante un concentrador denominado unidad de acceso multiestación (multistation access unit, MSAU). La topología lógica representa la ruta del testigo entre equipos, que es similar a un anillo.

Importante El anillo lógico representa la ruta del testigo entre equipos. El anillo físico está cableado mediante un concentrador denominado unidad de acceso multiestación (multistation access unit, MSAU).

2.6.2.1 Método de acceso

El método de acceso utilizado en una red Token Ring es de paso de testigo. Un testigo es una serie especial de bits que viaja sobre una red Token Ring. Un equipo no puede transmitir salvo que tenga posesión del testigo; mientras que el testigo está en uso por un equipo, ningún otro puede transmitir datos.

Cuando el primer equipo de la red Token Ring se activa, la red genera un testigo. Éste viaja sobre el anillo por cada equipo hasta que uno toma el control del testigo. Cuando un equipo toma el control del testigo, envía una trama de datos a la red. La trama viaja por el anillo hasta que alcanza al equipo con la dirección que coincide con la dirección de destino de la trama. El equipo de destino copia la trama en su memoria y marca la trama en el campo de estado de la misma para indicar que la información ha sido recibida.

La trama continúa por el anillo hasta que llega al equipo emisor, en la que se reconoce como correcta. El equipo emisor elimina la trama del anillo y transmite un nuevo testigo de nuevo en el anillo.

2.6.2.1 Velocidad de transferencia

La velocidad de transferencia en una red Token Ring se encuentra entre 4 y 16 Mbps.

2.6.3 Modo de transferencia asíncrona (asynchronous transfer mode, ATM)

El modo de transferencia asíncrona (Asynchronous transfer mode, ATM) es una red de conmutación de paquetes que envía paquetes de longitud fija a través de LANs o WANs, en lugar de paquetes de longitud variable utilizados en otras tecnologías.

Los paquetes de longitud fija, o celdas, son paquetes de datos que contienen únicamente información básica de la ruta, permitiendo a los dispositivos de conmutación enrutar el paquete rápidamente. La comunicación tiene lugar sobre un sistema punto-a-punto que proporciona una ruta de datos virtual y permanente entre cada estación.

Utilizando ATM, podemos enviar datos desde una oficina principal a una ubicación remota. Los datos viajan desde una LAN sobre una línea digital a un conmutador ATM y dentro de la red ATM. Pasa a través de la red ATM y llega a otro conmutador ATM en la LAN de destino. Debido a su ancho de banda expandido, ATM puede utilizarse en entornos de:

- Voz, vídeo en tiempo real.
- Audio con calidad CD
- Datos de imágenes, como radiología en tiempo real.
- Transmisión de datos del orden de megabits.

2.6.3.1 Método de acceso

Una red ATM utiliza el método de acceso punto-a-punto, que transfiere paquetes de longitud fija de un equipo a otro mediante un equipo de conmutación ATM.

El resultado es una tecnología que transmite un paquete de datos pequeño y compacto a una gran velocidad.

2.6.3.2 Velocidad de transferencia

Velocidad de transferencia La velocidad de transferencia en una red ATM se encuentra entre 155 y 622 Mbps.

Es importante hacer mención de que la velocidad de transmisión de ATM permite transmitir voz, vídeo en tiempo real, audio con calidad CD, imágenes y transmisiones de datos del orden de megabits.

2.6.4 Interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface, FDDI)

Una red de Interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface, FDDI) proporciona conexiones de alta velocidad para varios tipos de redes. FDDI fue

diseñado para su uso con equipos que requieren velocidades mayores que los 10 Mbps disponibles de Ethernet o los 4 Mbps disponibles de Token Ring. Una red FDDI puede soportar varias LANs de baja capacidad que requieren un backbone de alta velocidad.

Una red FDDI está formada por dos flujos de datos similares que fluyen en direcciones opuestas por dos anillos. Existe un anillo primario y otro secundario. Si hay un problema con el anillo primario, como el fallo del anillo o una rotura del cable, el anillo se reconfigura a sí mismo transfiriendo datos al secundario, que continúa transmitiendo.

Cabe mencionar que FDDI proporciona un backbone de alta velocidad a las redes LAN o WAN existentes.

2.6.4.1 Método de acceso

El método de acceso utilizado en una red FDDI es el paso de testigo. Un equipo en una red FDDI puede transmitir tantos paquetes como pueda producir en un tiempo predeterminado antes de liberar el testigo. Tan pronto como un equipo haya finalizado la transmisión o después de un tiempo de transmisión predeterminado, el equipo libera el testigo.

Como un equipo libera el testigo cuando finaliza la transmisión, varios paquetes pueden circular por el anillo al mismo tiempo. Este método de paso de testigo es más eficiente que el de una red Token Ring, que permite únicamente la circulación de una trama a la vez.

Este método de paso de testigo también proporciona un mayor rendimiento de datos a la misma velocidad de transmisión.

2.6.4.2 Velocidad de transferencia

La velocidad de transferencia en una red FDDI se encuentra entre 155 y 622 Mbps.

2.6.5 Frame relay.

Frame relay es una red de conmutación de paquetes que envía paquetes de longitud variable sobre LANs o WANs. Los paquetes de longitud variable, o tramas, son paquetes de datos que contienen información de direccionamiento adicional y gestión de errores necesaria para su distribución.

La conmutación tiene lugar sobre una red que proporciona una ruta de datos permanente virtual entre cada estación. Este tipo de red utiliza enlaces digitales de área extensa o fibra óptica y ofrece un acceso rápido a la transferencia de datos en los que se paga únicamente por lo que se necesita.

La conmutación de paquetes es el método utilizado para enviar datos sobre una WAN dividiendo un paquete de datos de gran tamaño en piezas más pequeñas (paquetes). Estas piezas se envían mediante un conmutador de paquetes, que envía los paquetes individuales a través de la WAN utilizando la mejor ruta actualmente disponible.

Aunque estos paquetes pueden viajar por diferentes rutas, el equipo receptor puede ensamblar de nuevo las piezas en la trama de datos original.

Sin embargo, es posible establecer un circuito virtual permanente (permanent virtual circuit, PVC), que podría utilizar la misma ruta para todos los paquetes. Esto permite una transmisión a mayor velocidad que las redes Frame Relay convencionales y elimina la necesidad para el desensamblado y reensamblado de paquetes.

2.6.5.1 Método de acceso

Frame relay utiliza un método de acceso punto-a-punto, que transfiere paquetes de tamaño variable directamente de un equipo a otro, en lugar de entre varios equipos y periféricos.

2.6.5.2 Velocidad de transferencia

Frame relay permite una transferencia de datos que puede ser tan rápida como el proveedor pueda soportar a través de líneas digitales.

2.7 Métodos de acceso

La optimización en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la ciencia informática en nuestros días. Por ello, la aparición de las plataformas de interconexión de equipos de computación o de redes informáticas, son uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en cualquier organización.

Actualmente, el uso de las redes informáticas es uno de los avances mayormente aceptados por los consumidores informáticos a nivel mundial, esto se debe a las grandes ventajas que ofrecen.

- Capítulo III: Especificaciones -

3.1 Introducción

Todo requiere de ser controlado y estandarizado de alguna manera; las redes informáticas no son la excepción.

De acuerdo con el tipo de red de que se trate, las normas son específicas; sin embargo, es necesario hacer mención de que todas las redes tienen un mismo objetivo: la comunicación entre usuarios; ya sea que esta se realice a diferentes distancias y distintos tiempos, o con dispositivos diversos.

3.2 Estándares de redes

Para los creadores de estándares el trabajo no termina, siempre están tratando de moldear estándares y normas a llevar a cabo. Sin embargo, una vez creados los estándares, son violados tan pronto como el proveedor agregue una nueva característica.

Cabe mencionar que, si un formato o lenguaje se usa extensamente y otros lo copian, se convierte en un estándar de hecho y puede pasar a ser usado tan ampliamente como aquellos estándares oficiales creados por las organizaciones autorizadas.

3.3 Organizaciones creadoras de estándares

Las organizaciones oficiales para la creación y difusión de estándares de redes son:

- ISO (Organización internacional de normas). Esta organización es la más reconocida a nivel mundial.

- IEEE (Instituto de Ingenieros Eléctricos y Electrónicos). Esta organización es la encargada de fijar los elementos físicos de una red (cables, conectores, etcétera). El comité que se ocupa de los estándares de computadoras a nivel mundial es la IEEE en su división 802, los cuales se dedican a lo referente del sistema de red. Están especificados los siguientes:

    1. IEEE 802.3. hace referencia a las redes tipo bus, en donde se deben evitar las colisiones de paquetes de información, por lo cual este estándar hace referencia al uso de CSMA/CD (acceso múltiple con detección de portadora con detección de colisión).

2. IEEE 802.4. Hace referencia al método de acceso Token, pero para una red con topología en anillo o la conocida como token bus.

3. IEEE 802.5. Ésta hace referencia al método de acceso token, para una red con topología en anillo, conocida como la token ring.

4. IEEE 802.3i Ethernet 10/100Base-T LAN. Estandariza los requerimientos de medios y distancias para redes de 10 Mbps.

5. IEEE 802.3u Ethernet 10/100Base-T LAN. Estandariza los requerimientos de medios y distancias para redes de 100 Mbps.

- EIA/TIA-568. Esta organización estandariza los requerimientos de sistema de cableado de telecomunicaciones de redes de edificios con servicios de voz, datos, imagen y video.

    1. EIA/TIA TSB-36. Se encarga de las especificaciones adicionales para cables UTP.

    2. EIA/TIA TSB-40. Se encarga de las especificaciones adicionales de transmisión para cables UTP.

    3. EIA/TIA-569. Estandariza las prácticas de diseño y construcción dentro y entre los edificios.

    4. EIA/TIA-606. Guía para la administración de la infraestructura de telecomunicaciones en edificios.

    5. EIA/TIA-607. Provee los estándares para aislar y aterrizar el equipo de telecomunicaciones y sus datos.

- ANSI X3T9.5 FDDI. Define los estándares para redes locales de 100 Mbps basadas en fibra óptica o UTP.

3.4 Estructuras de red en los estándares

Dentro de los estándares, se encuentran referencia a las siguientes estructuras de red:

- 10 base 5. Esto describe a una red tipo bus con cable coaxial grueso o RG8, banda base, que puede transmitir a 10 Mbps a una distancia máxima de 500 metros.

- 10 base 2. Se refiere a una red tipo bus con cable coaxial delgado RG58, banda base; y que puede transmitir a 10 Mbps a una distancia de 200 metros; a ésta se le conoce como chip Ethernet.

- 10 base T. Actualmente, este tipo de red es de las más usadas. Debido a su fácil estructuración y control central, en ésta se utiliza cable UTP y se puede transmitir a 10 Mbps a una distancia de 100 metros.

3.5 Ampliación de una red

Para satisfacer las necesidades de red, crecientes en una organización, se necesita no sólo ampliar el tamaño, sino mejorar el rendimiento de una red. Es necesario aclarar que no se puede hacer crecer una red simplemente añadiendo nuevos equipos y más cable.

Cada topología o arquitectura de red tiene sus límites. Sin embargo, se pueden instalar componentes para incrementar el tamaño de la red dentro de su entorno existente. Entre los componentes que permiten la ampliación de la red están:

- Repetidores y concentradores (hub´s). Los repetidores y concentradores retransmiten una señal eléctrica recibida en un punto de conexión (puerto) a todos los puertos para mantener la integridad de la señal.

- Puentes (bridge). Los puentes permiten que los datos puedan fluir entre redes LAN.

- Conmutadores (switch). Los conmutadores permiten el flujo de datos de alta velocidad a redes LAN.

- Enrutadores (router). Los enrutadores permiten el flujo de datos a través de LANs o WANs, dependiendo de la red de destino de los datos.

- Puertas de enlace (Gateway). Las puertas de enlace permiten el flujo de datos a través de LANs o WANs y funcionan de modo que equipos que utilizan diversos protocolos puedan comunicarse entre sí.

También se puede ampliar una red permitiendo a los usuarios la conexión a una red desde una ubicación remota. Para establecer una conexión remota, los tres componentes requeridos son:

- Un cliente de acceso remoto
- Un servidor de acceso remoto
- Conectividad física.

Microsoft Windows 2000 permite a clientes remotos conectarse a servidores de acceso remoto utilizando:

- Red pública telefónica conmutada (RTC).
- Red digital de servicios integrados (RDSI).
- X.25.
- Línea ADSL (Asymmetric Digital Subscriber Line).

3.5.1 Repetidores y concentradores

Podemos utilizar repetidores y concentradores para ampliar una red añadiendo dos o más segmentos de cableado. Estos dispositivos utilizados habitualmente son económicos y fáciles de instalar.

Los repetidores reciben señales y las retransmiten a su potencia y definición originales. Esto incrementa la longitud práctica de un cable (si un cable es muy largo, la señal se debilita y puede ser irreconocible).

Instalar un repetidor entre segmentos de cable permite a las señales llegar más lejos. Los repetidores no traducen o filtran las señales. Para que funcione un repetidor, ambos segmentos conectados al repetidor deben utilizar el mismo método de acceso.

Por ejemplo, un repetidor no puede traducir un paquete Ethernet a un paquete Token Ring. Los repetidores no actúan como filtros para restringir el flujo del tráfico problemático; sino que envían cada bit de datos desde un segmento de cable a otro, incluso si los datos están formados por paquetes malformados o no destinados a un equipo en otro segmento.

Cabe hacer mención de que los repetidores son una forma económica de extender la longitud de cableado sin tener una pérdida de datos.

Es recomendable el uso de repetidores para:

- Conectar dos o más segmentos con cable similar.
- Regenerar la señal para incrementar la distancia transmitida.
- Transmitir todo el tráfico en ambas direcciones.
- Conectar dos segmentos del modo más rentable posible.

Por otro lado, los concentradores o hub´s, permiten conectar varios equipos a un punto central sin pérdida de datos. Un concentrador transmite el paquete de datos a todos los equipos y segmentos que están conectados al mismo.

Los concentradores son dispositivos de conectividad que conectan equipos en una topología en estrella. Los concentradores contienen múltiples puertos para conectar los componentes de red.

Si utiliza un concentrador, una rotura de la red no afecta a la red completa; sólo el segmento y el equipo adjunto al segmento falla. Un único paquete de datos enviado a través de un concentrador fluye a todos los equipos conectados. Hay dos tipos de concentradores:

- Concentradores pasivos
- Concentradores activos

Los concentradores pasivos envían la señal entrante directamente a través de sus puertos sin ningún procesamiento de la señal. Estos concentradores son generalmente paneles de cableado.

Los concentradores activos, a veces denominados repetidores multipuerto, reciben las señales entrantes, procesan las señales y las retransmiten a sus potencias y definiciones originales a los equipos conectados o componentes.

El uso de un concentrador es recomendable para:

- Cambiar y expandir fácilmente los sistemas de cableado.
- Utilizar diferentes puertos con una variedad de tipos de cable.
- Permitir la monitorización central de la actividad y el tráfico de red.

3.5.2 Puentes y direcciones MAC

Un puente es un dispositivo que distribuye paquetes de datos en múltiples segmentos de red que utilizan el mismo protocolo de comunicaciones.

Un puente distribuye una señal a la vez. Si un paquete va destinado a un equipo dentro del mismo segmento que el emisor, el puente retiene el paquete dentro de ese segmento. Si el paquete va destinado a otro segmento, lo distribuye a ese segmento.

A medida que el tráfico cruza a través del puente, la información sobre las direcciones MAC de los equipos emisores se almacena en la memoria del puente. El puente usa esta información para construir una tabla basada en estas direcciones.

A medida que se envían más datos, el puente construye una tabla puente que identifica a cada equipo y su ubicación en los segmentos de red. Cuando el puente recibe un paquete, la dirección de origen se compara a la dirección de origen listada en la tabla. Si la dirección fuente no está presente en la tabla, se añade a la misma.

A continuación, el puente compara la dirección de destino con la dirección de destino listada en la tabla. Si reconoce la ubicación de la dirección de destino, reenvía el paquete a esta dirección. Si no reconoce la dirección de destino, reenvía el paquete a todos los segmentos.

El uso de un puente es para:

- Expandir la longitud de un segmento.
- Proporcionar un mayor número de equipos en la red.
- Reducir cuellos de botella de tráfico resultante de un excesivo número de equipos conectados.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo cada red más eficiente.
- Enlazar cables físicos de distinto tipo, como cable de par trenzado con cable coaxial en Ethernet.

3.5.3 Conmutadores

Los conmutadores son similares a los puentes, pero ofrecen una conexión de red más directa entre los equipos de origen y destino.

Cuando un conmutador recibe un paquete de datos, crea una conexión interna separada, o segmento, entre dos de sus puertos cualquiera y reenvía el paquete de datos al puerto apropiado del equipo de destino únicamente, basado en la información de la cabecera de cada paquete. Esto aísla la conexión de los demás puertos y da acceso a los equipos origen y destino a todo el ancho de banda de una red.

A diferencia de un concentrador, los conmutadores son comparables a un sistema telefónico con líneas privadas. En tal sistema, si una persona llama a cualquier otra, el operador o conmutador telefónico les conecta a una línea dedicada. Esto permite que tengan lugar más conversaciones a más en un momento dado.

Se utiliza un conmutador para:

- Enviar un paquete directamente del equipo origen al destino.
- Proporcionar una mayor velocidad de transmisión de datos.

3.5.4 Enrutadores o routers

Un enrutador es un dispositivo que actúa como un puente o conmutador, pero proporciona funcionalidad adicional. Al mover datos entre diferentes segmentos de red, los enrutadores examinan la cabecera del paquete para determinar la mejor ruta posible del paquete.

Un enrutador conoce el camino a todos los segmentos de la red accediendo a información almacenada en la tabla de rutas. Los enrutadores permiten a todos los usuarios de una red compartir una misma conexión a Internet o a una WAN.

Se recomienda usar un router para:

- Enviar paquetes directamente a un equipo de destino en otras redes o segmento. Los enrutadores usan una dirección de paquete más completa que los puentes. Los enrutadores garantizan que los paquetes viajen por las rutas más eficientes a sus destinos. Si un enlace entre dos enrutadores falla, el enrutador de origen puede determinar una ruta alternativa y mantener el tráfico en movimiento.

- Reducir la carga en la red. Los enrutadores leen sólo los paquetes de red direccionados y pasan la información sólo si la dirección de red es conocida. De este modo, no pasan información corrupta. Esta capacidad de controlar los datos que pasan a través del enrutador reduce la cantidad de tráfico entre redes y permite a los enrutadores utilizar estos enlaces más eficientemente que los puentes.

3.5.5 Puertas de enlace (Gateway)

Las puertas de enlace permiten la comunicación entre diferentes arquitecturas de red. Una puerta de enlace toma los datos de una red y los empaqueta de nuevo, de modo que cada red pueda entender los datos de red de la otra.

Una puerta de enlace es cómo un intérprete. Por ejemplo, si dos grupos de personas pueden físicamente hablar entre sí pero hablan idiomas diferentes, necesitan un intérprete para comunicarse. De modo similar, dos redes pueden tener una conexión física, pero necesitan una puerta de enlace para traducir la comunicación de red.

Use una puerta de enlace para enlazar dos sistemas que no utilizan:

- La misma arquitectura.
- Los mismos conjuntos de reglas de comunicación y regulaciones.
- Las mismas estructuras de formateo de datos.

3.6 Estándares de telecomunicaciones ANSI/TIA/EIA-568

El estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales, define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

La finalidad de este estándar es el permitir el diseño y la instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán.

La instalación de los sistemas de cableado durante el proceso de instalación y/o de remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

La norma ANSI/TIA/EIA-568-A publicada en Octubre de 1995 amplió el uso de Cable de Par Trenzado (UTP) y elementos de conexión para aplicaciones en Redes de Área Local (LAN) de alto rendimiento.

La edición de la ANSI/TIA/EIA-568-A integra los Boletines Técnicos de servicio TSB 36 y TSB 40A los cuales prolongan el uso de Cable de Par Trenzado (UTP) en un ancho de banda de hasta 100 MHz.

Además, la norma ANSI/TIA/EIA-568-A especifica los requisitos mínimos para cableado de telecomunicaciones dentro de edificios comerciales, incluyendo salidas y conectores, así como entre edificios de conjuntos arquitectónicos.

Los estándares más conocidos para su uso en redes informáticas son:

- IEEE 802.3 (estándar para Ethernet)
- IEEE 802.5 (estándar para Token Ring)
- IEEE 802.11 (estándar para redes inalámbricas Wi-Fi)
- IEEE 802.15 (estándar para bluetooth)

3.6.1 Uso del cable adecuado

El cable más utilizado es el UTP Categoría 5, es decir Cable de Par Trenzado el cual está compuesto de conductores de cobre aislados por plástico y trenzados en pares. Esos pares son después trenzados en grupos llamados unidades, y estas unidades son a su vez trenzadas hasta tener el cable terminado.

La razón de seleccionar este tipo de cable es que es uno de los más populares, tanto en precio como en rendimiento.

Los motivos más comunes de su uso son:

- No es muy costoso
- Es de fácil manipulación
- Disminuye el ruido de interferencia

Por supuesto, esto se aplica en una red en donde los usuarios se encuentran muy cercanos entre sí (no implica que estén juntos, sólo que no muy lejos).

3.6.2 Cable coaxial

En cuanto al cable coaxial, se suele utilizar para transmitir señales analógicas o digitales. Actualmente no tiene mucha demanda en redes; el área en donde más se utiliza es en televisiones por cable.

Hablando de cable coaxial en la interconexión de redes, se tienen las siguientes desventajas:

- Es mucho más costoso que el cable de par trenzado.
- Suele atenuar la señal.
- Tiene ruido térmico.
- Presente ruido de intermodulación.
- Para señales analógicas, se necesita un amplificador cada pocos kilómetros.
- Para señales digitales, se necesita un repetidor por cada kilómetro de la red.

A pesar de que el cable de fibra óptica esta remplazando hoy día los demás tipos de cables, en algunos sitios todavía no se cuenta con la tecnología necesaria para utilizar este tipo de cableado.

3.6.3 Cable de fibra óptica

El cable de fibra óptica es muy versátil y ofrece muchos beneficios; el pero que tiene es su alto costo.

3.7 Cableado estructurado

Un sistema de cableado estructurado es un diseño de arquitectura abierta ya que es independiente de la información que se trasmite a través de él.

3.7.1 Características del cableado estructurado

Entre las características del cableado estructurado, se pueden destacar las siguientes:

- Es confiable porque está diseñado con una topología de estrella, la que en caso de un daño o desconexión, éstas se limitan sólo a la parte o sección dañada, y no afecta al resto de la red. En los sistemas antiguos, basados en bus Ethernet, cuando se producía una caída, toda la red quedaba inoperante.

- Se gastan recursos en una sola estructura de cableado y no en varias (como en los edificios con cableado convencional)

- En casos de actualización o cambios en los sistemas empresariales, sólo se cambian los módulos TC y no todos los cables de la estructura del edificio.

- Se evita romper paredes para cambiar circuitos o cables; lo que, además, provocaría cierres temporales o incomodidades en el lugar de trabajo.

- Permite mover personal de un lugar a otro o agregar servicios a ser transportados por la red sin la necesidad de incurrir en altos costos de recableado. La única manera de lograr esto es tender los cables del edificio con más rosetas de conexión que las que serán usadas en un momento determinado.

3.7.2 Levantamiento de Información

Se le llama levantamiento de la información a:

- La determinación de la cantidad y ubicación física de las terminales (relevamiento y proyección a mediano plazo).

- La asignación de los puntos de concentración y "racks" (gabinetes con equipos que contienen la electrónica de la red).

- La instalación del cable adecuado y tomas RJ-45 para terminales en áreas de trabajo (subredes).

- La colocación del cable UTP (desde las tomas RJ-45 hasta los paneles de interconexión de los "racks")

- La configuración y realización de pruebas de certificación del cableado (verificación técnica con instrumentos).

- La conexión del sitio cableado el equipo de conectividad "switch/hub" para la subred.

- La comprobación y la realización de pruebas finales.

- La configuración de los equipos terminales y uso efectivo de la subred

3.8 Diseño de redes

El diseño de la red es el proceso anterior a su interconexión; en él, se ven las necesidades a cubrir por ella y las características que debe tener para ser fácil de utilizar por el usuario.

Este proceso puede ser dividido en:

- Diseño lógico
- Diseño físico

El diseño lógico define la arquitectura de la red, mientras el diseño físico establece el detalle de los componentes y configuraciones. Los diseños tienen que crearse en función de las necesidades tanto actuales como previsibles de la empresa, con el objetivo de obtener el mayor rendimiento de la red y retorno de la inversión posibles. Esto es todavía más importante en redes multimarca.

Con frecuencia se cae en el error de no valorar adecuadamente el diseño cuando es uno de los servicios más estratégicos: resulta paradójico querer ahorrarse un poco de dinero en el diseño para después perder cantidades muy importantes en falta de rendimiento y velocidad de la red y, en consecuencia, productividad por parte de los usuarios, o en costes de comunicaciones.

3.9 Normativa de Canalizaciones

La normativa de canalización se utiliza para proteger los cables de agresiones físicas y, en algunos casos, de interferencias electromagnéticas. Estas son:

- Canaleta. Se utiliza para instalaciones vistas o industriales. Permiten un fácil acceso a los cables. Es metálica si protege de interferencias, para uso industrial o falsos suelos; es de PVC si no protege de interferencias. En este caso resulta más barata la canaleta de PVC que la metálica.

- Tubos corrugados. Para falsos techos, falso suelo o empotrados. Por su estructura permiten mucha flexibilidad para seguir las formas del edificio. Dos niveles de grosor del plástico: plástica si no protege de interferencias; metálicas si protegen de interferencias. Los tubos metálicos llevan capas internas de película metálica. En este sentido, es más barato el tubo plástico.

- Tubo rígido. Se utiliza en cuartos de máquinas, garajes, etcétera. No tiene la flexibilidad del corrugado. Normalmente es de PVC.

- Rejillas metálicas. Se utilizan en falsos suelos y algunas veces en falsos techos. No cubren el cable pero se puede sujetar mediante bridas, tienen forma de U y son económicas.

- Otras. Existen otras canalizaciones a veces adaptadas al entorno y otras forman parte de la arquitectura del edificio.

3.10 Estimación de tiempo y costos

Se adjunta en el siguiente anexo, un listado detallado con los materiales y precios en el mercado local para elaboración el cableado estructurado.

Una vez concluido el cableado de la subred el sitio se encontraría listo para ser integrado a la red. Sólo restaría el disponer del equipo de conectividad correspondiente a esa subred "Hub de 8 o 16 puertos en 10 o 100 Mb/s" colocado en el "Rack"

Tabla de costos		
Descripción	**Destino**	**Precio Estimado**
Concentrador de 8 puertos	Red de Área Local	220.000
15 metros de cable UTP Categoría 5	------	30.000
8 conectores RJ45	--------	4.000
Mano de obra	--------	200.000

3.11 Tecnologías

Se utilizan diferentes tecnologías de redes para la comunicación entre equipos de redes de área local (LAN´s) y de redes de cobertura amplia (WAN´s). Sin embargo, se puede utilizar una combinación de tecnologías para obtener la mejor relación costo-beneficio y la máxima eficiencia del diseño de la red

Hay muchas tecnologías de redes disponibles, entre las cuales podemos escoger las más idóneas para la red en particular, cuidando obtener las ventajas o cualidades de cada una de ellas.

3.12 Conectividad en acceso remoto

Windows Server y otros sistemas operativos de características de servidores, permiten a los usuarios conectarse a una red desde una ubicación remota utilizando una diversidad de hardware, como módems. Un módem permite a un equipo comunicarse a través de líneas telefónicas.

El cliente de acceso remoto se conecta al servidor de acceso remoto, que actúa de enrutador o de puerta de enlace, para el cliente a la red remota. Una línea telefónica proporciona habitualmente la conectividad física entre el cliente y el servidor. El servidor de acceso remoto ejecuta la característica de enrutamiento y acceso remoto de para soportar conexiones remotas y proporcionar interoperabilidad con otras soluciones de acceso remoto.

Los dos tipos de conectividad de acceso remoto proporcionados en Windows 2000/3 Server son:

- El acceso telefónico a redes
- La red privada virtual (VPN).

3.12.1 Acceso telefónico a redes

Windows 2000/3 Server proporciona un acceso remoto telefónico a los usuarios que realizan llamadas a intranets empresariales.

El equipo de acceso telefónico instalado en un servidor de acceso remoto ejecutando Windows 2000/3 responde peticiones de conexión entrantes desde clientes de acceso telefónico remotos.

El equipo de acceso telefónico responde la llamada, verifica la identidad del llamador y transfiere los datos entre el cliente remoto y la intranet corporativa.

3.12.2 Red privada virtual (VPN)

Una red privada virtual (virtual private network, VPN) utiliza tecnología de cifrado para proporcionar seguridad y otras características disponibles únicamente en redes privadas.

Una VPN permite establecer una conexión remota segura a un servidor corporativo que está conectado tanto a la red de área local corporativa como a una red pública, como la Internet.

Desde la perspectiva de usuario, la VPN proporciona una conexión punto-a-punto entre el equipo del usuario y un servidor corporativo. La interconexión intermedia de redes es transparente al usuario, como si tuviera conexión directa.

3.12.3 Red pública telefónica conmutada RTC

La red pública telefónica conmutada (RTC) hace referencia al estándar telefónico internacional basado en utilizar líneas de cobre para transmitir datos de voz analógica. Este estándar fue diseñado para transportar únicamente las frecuencias mínimas necesarias para distinguir voces humanas.

Como la RTC no fue diseñada para transmisiones de datos, existen límites a la velocidad máxima de transmisión de una conexión RTC. Además, la comunicación analógica es susceptible de incluir ruido de línea que causa una reducción de la velocidad de transmisión de datos.

La principal ventaja de la RTC es su disponibilidad a nivel mundial y el bajo coste del hardware debido a la producción masiva.

El equipo de acceso telefónico a redes está formado por un módem analógico para el cliente de acceso remoto y otro para el servidor de acceso remoto. Un módem analógico es un dispositivo que permite a un equipo transmitir información a través de una línea telefónica estándar. Como un equipo es digital y una línea de teléfono es analógica, se necesitan módems analógicos para convertir la señal digital a analógica, y viceversa.

Para organizaciones de mayor tamaño, el servidor de acceso remoto está adjunto a un banco de módems que contiene cientos de módems. Con módems analógicos tanto en el servidor de acceso remoto como en el cliente de acceso remoto, la máxima velocidad de transferencia binaria soportada por conexiones PSTN es de 56.000 bits por segundo, o 56 kilobits por segundo.

3.13 Red digital de servicios integrados (RDSI – ISDN)

La red digital de servicios integrados (RDSI) es un estándar de comunicaciones internacional para enviar voz, vídeo y datos a través de líneas telefónicas digitales y líneas telefónicas estándares. RDSI tiene la capacidad de ofrecer dos conexiones simultáneamente a través de un único par de línea telefónica. Las dos conexiones pueden ser cualquier combinación de datos, voz, vídeo o fax.

La misma línea utiliza un servicio de subscriptor RDSI, que se denomina Interfaz de Acceso Básico (Basic Rate Interface, BRI). BRI tiene dos canales, denominados canales B, a 64 Kbps cada uno, que transportan los datos, y un canal de datos a 16 Kbps para información de control. Los dos canales B pueden combinarse para formar una única conexión a 128 Kbps.

El otro servicio de velocidad de transmisión RDSI, el Interfaz de Acceso Primario (Primary Rate Interface, PRI), tiene 23 canales B y un canal D a 64 Kbps y utiliza más pares de líneas. PRI es mucho más caro que BRI y no es el habitualmente escogido por usuarios de acceso remoto individuales. En la mayoría de casos, BRI es el preferido cuando se utiliza RDSI para el acceso remoto.

3.13.1 Transmisión digital

RDSI es una transmisión digital, a diferencia de la transmisión analógica de RTC. Las líneas RDSI deben ser utilizadas tanto en el servidor como en el sitio remoto.

Además, se debe instalar un módem RDSI tanto en el servidor como en el cliente remoto.

3.13.2 Ampliación sobre el intercambio telefónico local

RDSI no es simplemente una conexión punto-a-punto. Las redes RDSI se amplían desde el intercambio telefónico local al usuario remoto e incluyen todas las telecomunicaciones y equipo de conmutación que subyace entre ellos.

El equipo de acceso remoto telefónico a redes está formado por un módem RDSI tanto para el cliente como el servidor de acceso remoto. RDSI ofrece una comunicación más rápida que RTC, comunicándose a velocidades superiores a 64 Kbps.

3.13.3 X.25

En una red X.25, los datos se transmiten utilizando conmutación de paquetes. X.25 utiliza un equipo de comunicaciones de datos para crear una red universal y detallada de nodos de reenvío de paquetes que envían un paquete X.25 a su dirección designada.

X.25 (PAD) Los clientes de acceso telefónico a redes pueden acceder directamente a una red X.25 utilizando un ensamblador/desensamblador de paquetes X.25 (packet assembler/disassembler, PAD).

Un PAD permite el uso de terminales y conexiones de módems sin necesidad de hardware y conectividad de clientes costosa para hablar directamente a X.25.

Los PADs de acceso remoto son una elección práctica para los clientes de acceso remoto porque no requieren insertar una línea X.25 en la parte posterior del equipo. El único requisito para un PAD de acceso remoto es el número telefónico del servicio de PAD para el operador.

El servicio de enrutamiento y acceso remoto proporciona acceso a la red X.25 en alguna de las dos configuraciones mostradas en la siguiente tabla:

3.14 Línea de subscripción digital asimétrica o asíncrona (ADSL)

La línea de subscriptor digital asimétrica (Asymmetric digital subscriber line, ADSL) es una tecnología que permite enviar mayor cantidad de datos sobre líneas telefónicas de cobre existentes. ADSL lo consigue utilizando la porción del ancho de banda de la línea telefónica no utilizado por la voz, permitiendo la transmisión simultánea de voz y datos.

Los usuarios de acceso remoto telefónico a redes reciben mucha más información que envían. La naturaleza asimétrica de la conexión ADSL encaja bien con la mayoría de usos de negocio remoto e Internet. En la recepción de datos, ADSL soporta velocidades de transferencia desde 1,5 a 9 Mbps.

En el envío de datos, ADSL soporta velocidad de transferencia de 16 a 640 Kbps. Aunque ADSL proporciona mayores velocidades de transmisión de datos que las conexiones PSTN y RDSI, el equipo cliente puede recibir datos a una mayor velocidad que enviar datos.

3.14.1 Interfaz LAN o interfaz de acceso telefónico a redes

El equipo ADSL puede aparecer a Windows 2000 tanto como un interfaz LAN como un interfaz de acceso telefónico a redes. Cuando un adaptador ADSL aparece como un interfaz LAN, la conexión ADSL opera del mismo modo que una conexión LAN a Internet.

Cuando un adaptador ADSL aparece como un interfaz de acceso telefónico a redes, ADSL proporciona una conexión física y los paquetes individuales se envían utilizando el modo de transferencia asíncrona (ATM). Se instala un adaptador ATM con un puerto ADSL tanto en el cliente como en el servidor de acceso remoto.

Es importante resaltar que la línea de subscriptor digital asimétrica (Asymmetric digital subscriber line, ADSL) es una tecnología que permite enviar mayor cantidad de datos sobre líneas telefónicas de cobre existentes.

En la recepción de datos, ADSL soporta velocidades de transferencia desde 1,5 a 9 Mbps. En el envío de datos, ADSL soporta velocidad de transferencia de 16 a 640 Kbps. Cuando un adaptador ADSL aparece como un interfaz LAN, la conexión ADSL opera del mismo modo que una conexión LAN a Internet.

3.14.2 Conexiones

Según el tipo de red que se elija, se requiere seguir ciertas especificaciones. Las tablas siguientes muestran las recomendaciones básicas según la normatividad:

Directa	
Normativa 568-A (recomendada)	
Conector 1	Conector 2
1 – Blanco Verde	1 – Blanco Verde
2 – Verde	2 – Verde
3 – Blanco Naranja	3 – Blanco Naranja
4 – Azul	4 – Azul
5 – Blanco Azul	5 – Blanco Azul
6 – Naranja	6 – Naranja
7 – Blanco Marrón	7 – Blanco Marrón
8 – Marrón	8 – Marrón

Directa	
Normativa 568-A (recomendada)	
Conector 1	Conector 2
1 – Blanco Naranja	1 – Blanco Naranja
2 – Naranja	2 – Naranja
3 – Blanco Verde	3 – Blanco Verde
4 – Azul	4 – Azul
5 – Blanco Azul	5 – Blanco Azul
6 – Verde	6 – Verde
7 – Blanco Marrón	7 – Blanco Marrón
8 – Marrón	8 – Marrón

Cableado cruzado	
Conector 1	Conector 2
1 – Blanco Naranja	1 – Blanco Verde
2 – Naranja	2 – Verde
3 – Blanco Verde	3 – Blanco Naranja
4 – Azul	4 – Azul
5 – Blanco Azul	5 – Blanco Azul
6 – Verde	6 – Naranja
7 – Blanco Marrón	7 – Blanco Marrón
8 – Marrón	8 – Marrón

Como ilustración, se tiene la figura 3.1

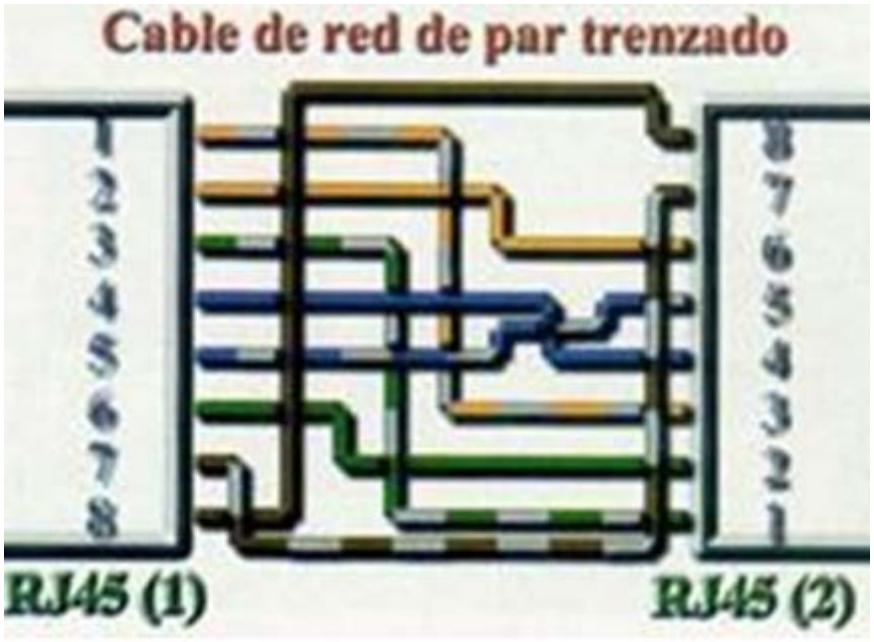


Figura 3.1 Cable de red de par trenzado

Visto a manera de esquema, se muestra la figura 3.2

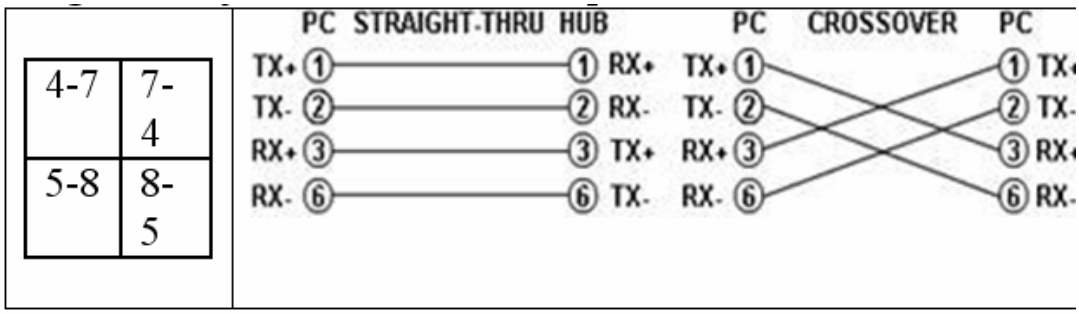


Figura 3.2 Esquema de conexión en par trenzado

Según la tarjeta, el cable cruzado puede ser:

- Cable de conexión directa: conecta un PC/Panel al Hub/Switch
- Cable consola: conecta un PC al Router-Cable Consola
- Cable de conexión cruzada: Conecta nodo a nodo (PC con PC, hub con hub, hub con switch)

Lo anterior se muestra en la figura 3.3

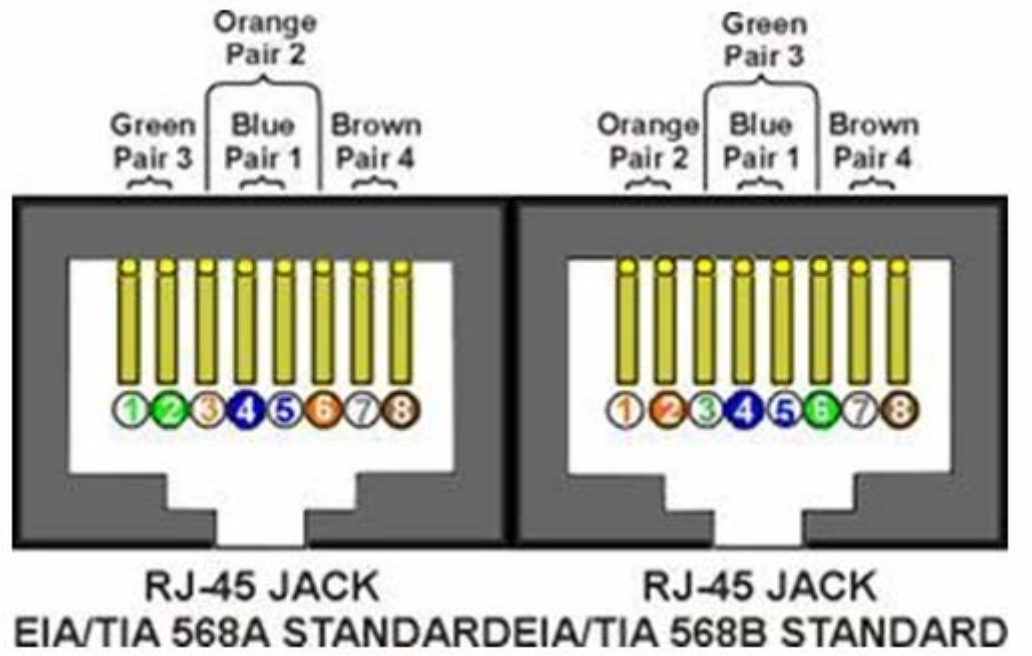


Figura 3.3 Cables de par trenzado

3.14.3 Cable UTP

El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores un poco más anchos.

Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

Los cables de par trenzado pueden ser de dos tipos:

- UTP (Unshielded Twisted Pair, par trenzado no apantallado)
- STP (Shielded Twisted Pair, par trenzado apantallado)

3.14.4 Categorías y parámetros

Las categorías de cables, que son tomadas en cuenta en los estándares de redes son:

- Categoría 1: Descrito en el estándar EIA/TIA 568B. Cable de par trenzado sin apantallar, se adapta para los servicios de voz, pero no a los datos.

- Categoría 2: Cable de par trenzado sin apantallar, este cable tiene cuatro pares trenzados y está certificado para transmisión de 4 mbps.

- Categoría 3: Cable de par trenzado que soporta velocidades de transmisión hasta de 10 mbps de ethernet 10Base-T, Este cable tiene cuatro pares.

- Categoría 4: Cable par trenzado certificado para velocidades de hasta16 mbps. Este cable tiene cuatro pares.

- Categoría 5: Es un cable de cobre par trenzado de cuatro hilos de 100 OHMIOS. La transmisión de este cable puede se a 100 mbps para soportar las nuevas tecnologías como ATM (Asynchronous Transfer Mode).

Existen varias opciones para el estándar 802,3 que se diferencian por velocidad, tipo de cable y distancia de transmisión:

- 10Base-T: Cable de par trenzado con una longitud aproximada de 500 mts, a una velocidad de 10 mbps.

- 1Base-5: Cable de par trenzado con una longitud extrema de 500 mts, a una velocidad de 1 mbps.

- 100Base-T: (Ethernet Rápida) Cable de par trenzado, nuevo estándar que soporta velocidades de 100 mbps que utiliza el método de acceso CSMA/CD.

Los parámetros eléctricos que se miden son:

- Atenuación en función de la frecuencia (db)

- Impedancia característica del cable (Ohms)
- Acoplamiento del punto mas cercano (NEXT- db)
- Relación entre Atenuación y Crostalk (ACR- db)
- Capacitancia (pf/m)
- Resistencia en DC (Ohms/m)
- Velocidad de propagación nominal (% en relación C)

3.14.5 Tipos de cableado y dispositivos normalizados

Se tienen contemplados, para la conexión de redes, los siguientes cableados:

- Cableado horizontal.
- Cableado vertical.

Se denomina cableado horizontal al conjunto de cables y conectores que van desde el armario de distribución hasta las rosetas del puesto de trabajo. Desde la roseta de cada uno de las áreas de trabajo irá un cable a un lugar común de centralización llamado panel de parcheo.

En un sistema de cableado estructurado, el cableado vertical es el cable extendido desde el armario de cableado de cada planta al equipo principal alojado en el sótano o primera planta del edificio. En contraste, el cableado horizontal es el que va de un armario de cableado de telecomunicación a cada estación de trabajo en una planta de un edificio

Los dispositivos básicos son:

- Concentrador o Hub.
- Paneles de parcheo (Patch Panel).
- Conector RJ-45.

Un hub es un dispositivo que no solamente realiza multiplexación a un puerto de salida, pero el cual tiene un procesador programado o programable que realizará la conmutación y enrutamiento a algunos puertos de salida a la vez que maneja comprensión de datos, conversión de códigos, control de errores y funciones de protocolo.

Un hub o concentrador es el punto central desde el cual parten los cables de par trenzado hasta las distintos puestos de la red, siguiendo una topología de estrella. Se

caracterizan por el número de puertos y las velocidades que soportan. Por ejemplo, son habituales los hubs 10/100 de 8 puertos.

Los Paneles de parcheo (Patch Panel) son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos.

Un Patch-Panel posee una determinada cantidad de puertos (RJ-45 End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas (o dientes - mencionados con anterioridad).

Patch cord (o latiguillos). Los latiguillos son los cables que nos van a permitir conectar entre el panel de parcheo y los concentradores. También se les llama latiguillos a los cables que van a servir para conectar cada uno de los PCs de la red a sus correspondientes rosetas de conexión.

En estos conectores es donde se ponchan las cerdas de los cables provenientes de los cajetines u otros Patch-Panels.

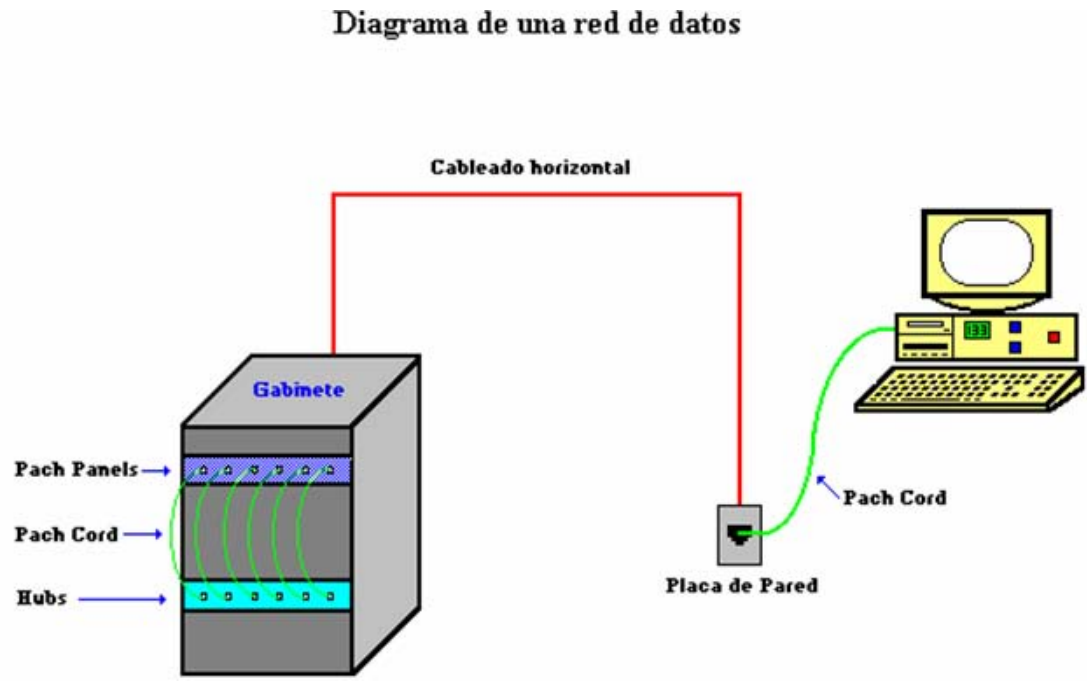
La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera. Para ponchar las cerdas de un cable Twisted Pair en el Patch-Panel se usa una ponchadora al igual que en los cajetines.

Un conector RJ-45 se utiliza con el cable UTP. Está compuesto de 8 vías con 8 "muelas" que a la hora de grimpar el conector pincharán el cable y harán posible la transmisión de datos. Por eso será muy importante que todas las muelas queden al ras del conector.

Los pares usados según la norma son:

- ATM 155Mbps usa los pares 2 y 4 (pins 1-2, 7-8)
- Ethernet 10Base - T4 usa los pares 2 y 3 (pins 1-2, 3-6)
- Ethernet 100Base-T4 usa los pares 2 y 3 (4T+) (pins 1-2, 3-6)
- Ethernet 100Base-T8 usa los pares 1,2,3 y 4 (pins 4-5, 1-2, 3-6, 7-8)

El diagrama general de una red de datos, así como su certificación, se muestra en la figura 3.4



Modelo típico de una Certificación TIA CAT 5 de Canal:

ITH NETWORK Sumario de Pruebas: PASA
LUGAR: COMPUTER KUEHNE NAGEL ID. Cable: DATOS 1
OPERADOR: ING HERNAN HERNANDEZ Fecha/Hora: 16/03/1998 11:24:01
NVP: 69,0% UMBRAL DE ANOMALIA DE FALLO: 15% Estánd. Pruebas: TIA Cat 5 Channel
FLUKE DSP-100 N/S: 6780047 Tipo de Cable: UTP 100 Ohm Cat 5
PASO LIBRE: 8,3 dB Versión de Estándares: 5.3
Versión de Software: 5.3

Mapa de Cableado PASA Result. TERM. RJ45: 1 2 3 4 5 6 7 8 B
| | | | | | | |
TERM. RJ45: 1 2 3 4 5 6 7 8

Par	1,2 3,6 4,5 7,8
Impedancia (ohmios), Límite 80-120	102 107 104 109
Longitud (m), Límite 100,0	20,1 19,4 19,4 19,0
Tiempo de Prop. (ns)	97 94 94 92
Diferencia Retardo (ns), Límite 50	5 2 2 0
Resistencia (ohmios)	3,9 3,7 3,7 3,7
Atenuación (dB)	4,3 4,2 4,4 4,1
Límite (dB)	24,5 24,5 24,5 24,5
Margen (dB)	20,2 20,3 20,1 20,4
Frecuencia (MHz)	100,0 100,0 99,9 100,0

Pares	1,2-3,6 1,2-4,5 1,2-7,8 3,6-4,5 3,6-7,8 4,5-7,8
NEXT (dB)	49,2 56,3 46,2 45,3 40,3 39,7
Límite (dB)	28,6 47,3 30,7 33,4 27,4 27,1
Margen (dB)	20,6 9,0 15,5 11,9 12,9 12,6
Frecuencia (MHz)	82,7 6,4 62,5 43,1 96,6 100,0
NEXT del Remoto (dB)	54,0 35,4 40,8 44,8 41,9 38,4
Límite (dB)	33,4 27,1 29,0 33,4 27,4 27,1
Margen (dB)	20,6 8,3 11,8 11,4 14,5 11,3
Frecuencia (MHz)	42,9 99,6 77,4 43,1 96,2 100,0

Figura 3.4 Diagrama y certificación de una red de datos

De la figura anterior se puede describir lo siguiente:

- El primer parámetro que vemos es el mapeado del cable, el cual indica que está correctamente conectado.

- La impedancia del cable puede variar en un 20%; para la categoría 5 mejorada muchos fabricantes están confeccionando los cables con los pares pegados y, aunque la mano de obra se encarece, esto mejora mucho otros parámetros a los cuales la impedancia del cable les afecta.

- La longitud está establecida en 100 metros; esto no significa que las redes actuales a 10 ó 100 Mhz no funcionen con una longitud mayor, pero hay que recordar que cada día, como afirmamos al principio de nuestro artículo, las velocidades aumentan y a mayor longitud mayor atenuación de la señal y otros efectos.

- Tiempo de propagación. Este es el tiempo que la señal demora en llegar al extremo distante; como se podrá observar el par que tiene mayor longitud tiene mayor tiempo de propagación.

- Diferencia de retardo. El límite está fijado en 50 ns., esto no es más que la diferencia que existe entre el límite de retardo y el valor medido de retardo; este parámetro es muy importante, debido a que si estamos trabajando con velocidades de propagación full duplex, o a través de los 4 pares, los receptores pueden tener información errónea, ralentizando la red.

- La resistencia. Este parámetro está referido a una medición con frecuencia 0 Hz.

- Atenuación. Para este parámetro es muy significativa la longitud del cable, el instrumento va haciendo un barrido de frecuencias, en el cual se detecta a qué frecuencia es dónde se encuentra la mayor pérdida; como se puede observar en el Modelo a 99.9 Mhz se detecta en el par 4-5 una pérdida de 4.4 dB, siendo el límite 24.5 dB; hay que destacar que estamos haciendo una medición sobre un cable de 20 metros, con lo cual los márgenes resultan muy favorables.

- Next cercano y Next remoto. Existen equipos en el mercado que sólo arrojan mediciones sobre el next cercano y no hacen la prueba del next remoto, siendo tan importante en un sentido como en el otro.

- El next es un efecto físico e indeseable, donde la señal en un par se induce en el otro, originando un ruido en el par y cambiando en muchos casos el valor de la información; para esto lo que se hace es inyectar señal en un par, y medir qué cantidad de esa señal se induce en un segundo par; el equipo genera un barrido de frecuencias, donde se puede observar a que se produce la peor situación, para mejorar este efecto, se fabrican los pares con un paso de trenzado diferente para evitar el acoplamiento. Se concluye que, cuanto mayor sea la diferencia entre la señal deseada y la indeseada, mejor.

Finalmente, en el informe de certificación anterior, se puede observar una categoría 5 a 100 Mhz; Existe una certificación más avanzada (o mejorada), conocida como "Powersum".

3.14.6 Powersum

Como pudimos apreciar anteriormente, para medir el next el equipo inyecta una señal en un par y observa qué ocurre en un segundo par.

En PowerSum, lo que se hace es inyectar tres señales en 3 pares y observa qué sucede en un cuarto par; la prueba es mucho más rigurosa que la anterior, con lo cual la calidad de los materiales y la profesionalidad del instalador juegan un papel de suma importancia. Esta prueba se observa en la figura 3.5

ITH NETWORK Sumario de Pruebas: PASA
LUGAR: VALCOM ID. Cable: DATOS 11
OPERADOR: ING HERNAN HERNANDEZ Fecha/Hora: 23/06/1998 12:58:32
NVP: 69,0% UMBRAL DE ANOMALIA DE FALLO: 15% Estánd. Pruebas: Power Sum Cat 5 Channel
FLUKE DSP-100 N/S: 6780047 Tipo de Cable: UTP 100 Ohm Cat 5
PASO LIBRE: 8,2 dB Versión de Estándares: 5.3
Versión de Software: 5.3

Mapa de Cableado PASA Result. TERM. RJ45: 1 2 3 4 5 6 7 8 B
| | | | | | | |
TERM. RJ45: 1 2 3 4 5 6 7 8

Par 1,2 3,6 4,5 7,8

Impedancia (ohmios), Límite 80-120 106 107 108 109

Longitud (m), Límite 100,0 22,1 22,1 21,5 21,3
Tiempo de Prop. (ns) 107 107 104 103
Diferencia Retardo (ns), Límite 50 4 4 1 0

Resistencia (ohmios) 4,4 4,4 4,4 4,4

Atenuación (dB) 4,9 5,0 4,9 4,7
Límite (dB) 24,5 24,5 24,5 24,5
Margen (dB) 19,6 19,5 19,6 19,8
Frecuencia (MHz) 100,0 100,0 99,7 100,0

PSNEXT (dB) 42,4 38,3 36,5 42,1
Límite (dB) 34,0 27,9 28,0 33,9
Margen (dB) 8,4 10,4 8,5 8,2
Frecuencia (MHz) 40,0 90,5 89,8 40,1

PSNEXT del Remoto (dB) 39,9 37,4 52,0 52,8
Límite (dB) 31,6 27,9 43,5 43,3
Margen (dB) 8,3 9,5 8,5 9,5
Frecuencia (MHz) 55,2 90,5 10,8 11,1

Figura 3.5 Certificación Powersum

- Capítulo IV: Visión de eficiencia y seguridad –

4.1 Introducción

A finales del siglo XX, las redes informáticas se han constituido como una de las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización.

Actualmente, la informática se encuentra subsumida en la gestión integral de la empresa; por ende, las normas y estándares propiamente informáticos deben estar sometidos a los generales de la misma.

En consecuencia, las organizaciones informáticas forman parte de lo denominado "management" o gestión de la empresa.

Cabe aclarar que la informática no gestiona propiamente a la empresa, sino que ayuda a la toma de decisiones sin decidir por sí misma.

Por lo tanto, debido a su importancia en el funcionamiento de la empresa, existe la auditoria informática, que trata de evaluar la eficiencia y eficacia de los sistemas.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz sistema de información. Cabe hacer énfasis en que, para la realización de una auditoria informática eficaz, se debe entender a la empresa en su más amplio sentido.

4.2 Antecedentes

La teoría de las redes informáticas no es algo reciente.

La necesidad de compartir recursos e intercambiar información fue una inquietud permanente desde los primeros tiempos de la informática. Los comienzos de las redes de datos se remontan a los años sesenta´s, en los cuales perseguían exclusivamente fines militares o de defensa. Paulatinamente se fueron adoptando para fines comerciales.

Obviamente en esa época no existían las PCs , por lo cual los entornos de trabajo resultaban centralizados y lo común para cualquier red era que el procesamiento quedara delegado a una única computadora central o mainframe Los usuarios accedieran a la misma mediante terminales "bobas" consistentes en sólo un monitor y un teclado.

Los tiempos han cambiado y ya prácticamente todos los usuarios acceden a los recursos desde PCs. Sin embargo, la teoría, los principios básicos, los protocolos han mantenido vigencia y si bien es cierto, se va produciendo obsolescencia de parte de ellos, es muy conveniente partir de los principios y de la teoría básica. Resulta dificultoso comprender las redes actuales si no se conocen los fundamentos de la teoría de redes.

Resulta algo bueno el tomar un punto de partida en este sentido, así que tomaré como base el X.25; un sistema tradicional, que trabaja sobre redes analógicas, es decir líneas telefónicas dedicadas. Hoy en día tiene pocas aplicaciones, como ser cajeros automáticos, validación de tarjetas de crédito, etc; pero su robustez, seguridad y confiabilidad han hecho mantenerlo como un estándar para las redes públicas y privadas durante una gran cantidad de años.

Además sus principios, su teoría de funcionamiento aporta conceptos sumamente importantes que nos ayudarán a comprender los siguientes.

Frame Relay es una mejora de X.25. Se trata de un sistema mucho más simple y eficiente, el cual tiene plena vigencia hoy en día en redes de área amplia. Trabaja sobre enlaces digitales generalmente punto a punto.

Posteriormente veremos las tecnologías LAN y por último culminaremos con el de mayor auge en nuestros días, base indispensable del funcionamiento de Internet: TCP/IP.

4.2 Conceptos elementales de redes

Recopilando un poco, es necesario recordar algunos conceptos como:

- Red. Es un conjunto de computadoras o terminales conectados mediante una o más vías de transmisión y con determinadas reglas para comunicarse.

- Host. Aunque en general este término suele relacionarse con Servidores, en un sentido amplio llamaremos HOST a cualquier equipo que se conecta a una red.

- Protocolo. Conjunto de comandos establecido por convención que deben conocer tanto emisor como receptor para poder establecer una comunicación en un red de datos. Constituyen el software de la red.

- DTE. Data Terminal Equipement es el equipo terminal de datos, la computadora o terminal que es el extremo final de la red.

- DCE. Data Communication Equipement es el equipo de comunicación. Generalmente un modem u algún otro dispositivo que establece el enlace físico y lógico con la red.

- Internet. aunque todos sabemos lo que es Internet, aquí lo utilizaremos también en otro sentido. Una Internet es un conjunto de dos o más redes que se interconectan mediante los medios adecuados.

4.3 Redes orientadas según objetivos

Las redes pueden ser orientadas de acuerdo a las necesidades y recursos propios de cada organización; en este sentido, las redes pueden ser:

- Orientadas a la conexión
- No orientadas a la conexión

Se dice que una red es Orientada a la Conexión cuando se establece un único camino para la transferencia de la información. Los datos viajarán uno tras otro por dicho camino. No hay más de un camino simultáneamente.

Estas redes requieren obligatoriamente de 3 fases:

- Establecimiento
- Transferencia
- Desconexión

Son el caso de X.25 , Frame Relay, ATM y TCP.

Las redes No Orientadas a la Conexión (connectionless) no utilizan un único camino, sino que los datos se fraccionan y toman por distintas vías simultáneamente para llegar a destino. Se la conoce también como Servicio de Datagramas y los casos típicos son IP y UDP.

4.4 Circuitos virtuales

Las redes Orientadas a la Conexión pueden constituir 2 tipos de circuitos o caminos para establecer la comunicación:

- Circuitos Virtuales Conmutados (SVC´s) establecen un camino de comunicación a través de la red que no es siempre el mismo. La conexión se establece por un camino al necesitar intercambiar datos y se libera al finalizar. Al establecerse una nueva conexión el camino a través de la red puede ser diferente. X.25 trabaja de esta forma.

- Circuitos Virtuales Permanentes (PVC´s) son similares a una línea punto a punto, están siempre fijos y no alternan entre caminos diferentes. La conexión se establece por única vez por un único medio físico al contratar el servicio y se mantiene inalterable hasta la baja del mismo. Frame Relay suele trabajar de esta forma aunque soporta también conmutados.

4.5 Conmutación en redes

Las redes pueden conmutar circuitos , como es el caso de la red telefónica o conmutar paquetes, que son una subdivisión lógica de la información.
Casi todas las tecnologías actuales : X.25 , Frame Relay , ATM , TCP/IP son de conmutación de paquetes.

4.6 Modelo OSI

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Como se ha mencionado, el modelo OSI es el plan a seguir en el manejo e interconexión de redes.

Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema.

A cada capa se le asigna una función bien específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento.

Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo - y de hecho, normalmente no lo hacen- pero de todas formas se recomienda siempre tener en cuenta el modelo OSI como referencia, ya que conocimiento del mismo posibilita la correcta comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

Las 7 capas son las siguientes:

7	APLICACIÓN
6	PRESENTACIÓN
5	SESIÓN
4	TRANSPORTE
3	RED
2	ENLACE
1	FÍSICA

El modelo OSI

Este modelo puede explicarse de la siguiente manera:

- CAPA 1 : Physical (Física): Define las reglas para transmitir el flujo de bits por el medio físico.
- CAPA 2 : Data Link (Enlace) : Organiza los bits en grupos lógicos denominado tramas o frames . Proporciona además control de flujo y control de errores.
- CAPA 3 : Network (Red) : Proporciona la posibilidad de rutear la info agrupada en paquetes.
- CAPA 4 : Transport (Transporte): Realiza el control de extremo a extremo de la comunicación, proporcionando control de flujo y control de errores. Esta capa es asociada frecuentemente con el concepto de confiabilidad.
- CAPA 5 : Session (Sesión): conexión y mantenimiento del enlace
- CAPA 6 : Presentation (Presentación): frecuentemente forma parte del sistema operativo y se encarga de dar formato los datos.
- CAPA 7 : Aplication (Aplicación) : Servicios para el usuario como ser e-mail, servicios de archivos e impresión, emulación de Terminal, login , etcétera.

Es importante aclarar con respecto a esta última que no cualquier aplicación que corra dentro de una PC encuadra en la capa Aplicación del modelo OSI, sino solamente las aplicaciones a los efectos del trabajo en red.

4.7 Software de red

El Software de una red lo constituyen los protocolos de comunicaciones. Es el conjunto de instrucciones que deben conocer ambos extremos de un enlace para poder establecer una comunicación.

Ejemplos de protocolos son :

- X.25
- Frame Relay
- ATM
- IP
- Apple Talk

Los mismos pueden también ser estratificados en las distintas capas del modelo OSI. Existen por lo tanto protocolos de capa 2, capa 3, capa 4 y así sucesivamente.

Pero los mismos no actúan en forma independiente. La relación entre ellos es lo que le da la verdadera dinámica al modelo OSI.

Los protocolos de distintas capas se suelen agrupar para su estudio en los llamados "stacks" (pilas) de protocolos. La idea sería que cualquier stack cumpla con todas las funciones definidas por el modelo OSI, aunque la correspondencia no deba ser necesariamente capa a capa. Por ejemplo un conjunto o "suite" de protocolos que forma un stack es TCP/IP.

El mismo cumple todas las funciones del modelo OSI pero su distribución no es la misma. TCP/IP está formado sólo por cuatro capas y algunas de ellas equivalen a más de una del modelo OSI.

Del mismo modo se pueden hacer otras agrupaciones siempre respetando la estructura del modelo OSI.

Existen multitud de recomendaciones que nos posibilitan armar conjuntos de protocolos que contituyan esquemas armónicamente funcionales.

Por ejemplo la recomendación del ITU-T (ex CCITT) para el protocolo de nivel de Red X.25, es que esté montado sobre LAPB a nivel de Enlace y EIA-232 ó V.24 a nivel Físico.

4.8 Seguridad en redes

La seguridad en las redes informáticas se ha convertido, a lo largo del tiempo, en un factor decisivo en todas las organizaciones.

En todas las áreas, por muy sencillas que sean, la seguridad es muy importante; aún así, la pérdida de información y de recursos, sigue siendo un problema muy común.

Partiendo del hecho de que no existe un sistema 100% seguro y de que las principales personas de quien se deben cuidar las organizaciones es de sus propios empleados, la seguridad en informática parece ser un cerco difícil de vencer.

Un primer paso para mejorar la seguridad informática y minimizar los riesgos, suele ser la implantación de políticas, acrecentar las restricciones para la mayoría de los usuarios, entre otras acciones como la actualización del software a utilizar, la capacitación del personal a cargo, etcétera.

4.8.1 Métodos

Un procedimiento muy básico pero funcional dentro de la seguridad en las redes informáticas se basa en la combinación de dos líneas de actuación muy claras:

- Establecimiento de políticas de seguridad
- Generación de auditorias

4.8.2 Inclusión de Políticas

En primer lugar, es recomendable establecer una política de seguridad que alcance a todo el sistema.

Debe plasmarse en un documento escrito donde se contemple la asignación de responsabilidades y refrendado al más alto nivel de dirección posible, lo que implicará a toda la estructura en su cumplimiento.

Se debe hacer un control riguroso de aplicación del mismo, pero también de su difusión para tener la certeza de que todos los afectados conocen su contenido.

Para su implantación es necesaria una adecuada generación de medios humanos y materiales específicos.

Y algo importantísimo: es fundamental la concienciación del personal afectado por las medidas a adoptar.

4.8.3 Aplicación de la política de seguridad

Los criterios implantados por la política de seguridad deben seguirse siempre, desde que el sistema es simple o sencillo hasta cuando su crecimiento lo transforma en uno complejo.

El mejor procedimiento es la escalabilidad, permitiendo de esta manera validar las políticas llevadas hasta el momento, afinando y optimizando las futuras.

4.8.4 Responsabilidades de la política de seguridad

De una manera genérica, la responsabilidad de implantación de la política de seguridad afecta a todos los usuarios del sistema de información, tanto los normales como los privilegiados, donde habría que englobar a:

- ✓ Administradores de sistemas
- ✓ Administradores de bases de datos y
- ✓ Responsables de comunicaciones.

De manera específica, debe existir un responsable de seguridad, con dedicación exclusiva caso de tratarse de sistemas de información importantes.

Para poder ejercer su labor, esta persona responsable debe contar con un equipo de seguridad que permita desarrollar la política determinada por escrito.

Es positivo establecer un equipo de supervisión compuesto por los usuarios privilegiados señalados anteriormente y el equipo de seguridad.

4.8.5 Bases para una política de seguridad

De manera recomendada y recomendable, las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible de ataque).
- Establecer niveles de prioridad e importancia sobre esta información.
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla
- Implementar respuesta a incidentes y recuperación para disminuir el impacto

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional (firewalls, autenticación, \ antivirus, controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros), y no únicamente tecnología.

Un esquema de seguridad empresarial contempla la seguridad física y lógica de una compañía. La primera se refiere a la protección contra robo o daño al personal, equipo e instalaciones de la empresa; y la segunda está relacionada con el tema que hoy nos ocupa: la protección a la información, a través de una arquitectura de seguridad eficiente.

Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos para generar una cultura de seguridad dentro de la organización.

4.8.6 Generación de auditorias

Por otro lado, se hace necesaria la generación de auditorias periódicas, tanto de tipo interno como externo.

Las auditorias internas provienen de la propia estructura de seguridad del sistema. Las auditorias externas las realizarían personal de una empresa o contratados a tal efecto y no siempre los mismos.

El objeto de las últimas es la revisión del sistema por parte de elementos que no se encuentren "viciados" por la rutina o el conocimiento del funcionamiento del sistema, extremo que se da con el personal propio.

4.8.7 Riesgos y recomendaciones en redes

La conexión a la red es la base del Internet. Es prácticamente imposible obtener todos los beneficios de la computación sin tener una conexión a la red.

Desafortunadamente, la conexión a la red también conlleva que, todas las amenazas que existen dentro de ella, estén conectadas a su computadora. Esto puede crear vulnerabilidades:

- ✓ Ataques de los hackers
- ✓ Acceso no autorizado
- ✓ Robo de información
- ✓ Ataques con programas malignos
- ✓ Daños legales.

Para bajar el riesgo de las conexiones de red, se recomienda lo siguiente:

1. Desactive los archivos compartidos en su Windows. En Windows 98 vaya a "Inicio/ Configuración/ Panel de control", busque "Compartir archivos e impresoras" y seleccione el botón "desactivar". Si debe habilitar los compartidos, asegúrese de utilizar una contraseña y sólo comparta los directorios indispensables.

2. Instale un cortafuegos personal, como el “Zone Alarm”, para proteger su computadora de los intentos de intrusión y los troyanos.

3. Evite el uso de programas de red inseguros tales como ICQ, AIM o IRC para tratar información confidencial. El contenido de esa comunicación puede ser visto por terceras personas, y utilizarlo para atacar su sistema o entregarle virus.

4. Considere utilizar sistemas operativos más seguros tales como Windows NT, 2000 o el nuevo Windows XP.

4.9 Visión a futuro

Las redes informáticas siguen evolucionando y adaptándose a las necesidades crecientes de los usuarios.

En muchos momentos de la historia, se pensó que toda la evolución se había llevado a cabo y que nada más se podría agregar ni inventar… estaban equivocados.

Si bien la tecnología va cambiando, lo hace a la par de los requerimientos, mismos que van cambiando en el transcurso del tiempo.

Seguramente, se seguirán creando redes cada día más eficientes y confiables, también de fácil uso para los usuarios e incrementando la seguridad en ellos.

Como se sabe, las redes funcionan desde una computadora hasta niveles mundiales de la transferencia de la información, como se observa en la figura 4.1

Figura 4.1 Enlace de redes informáticas a nivel global

La evolución en redes se encuentra marcada por el tamaño y los dispositivos que abarca. La evolución del modelo de interconexiones abiertas se puede ver como en la figura 4.2

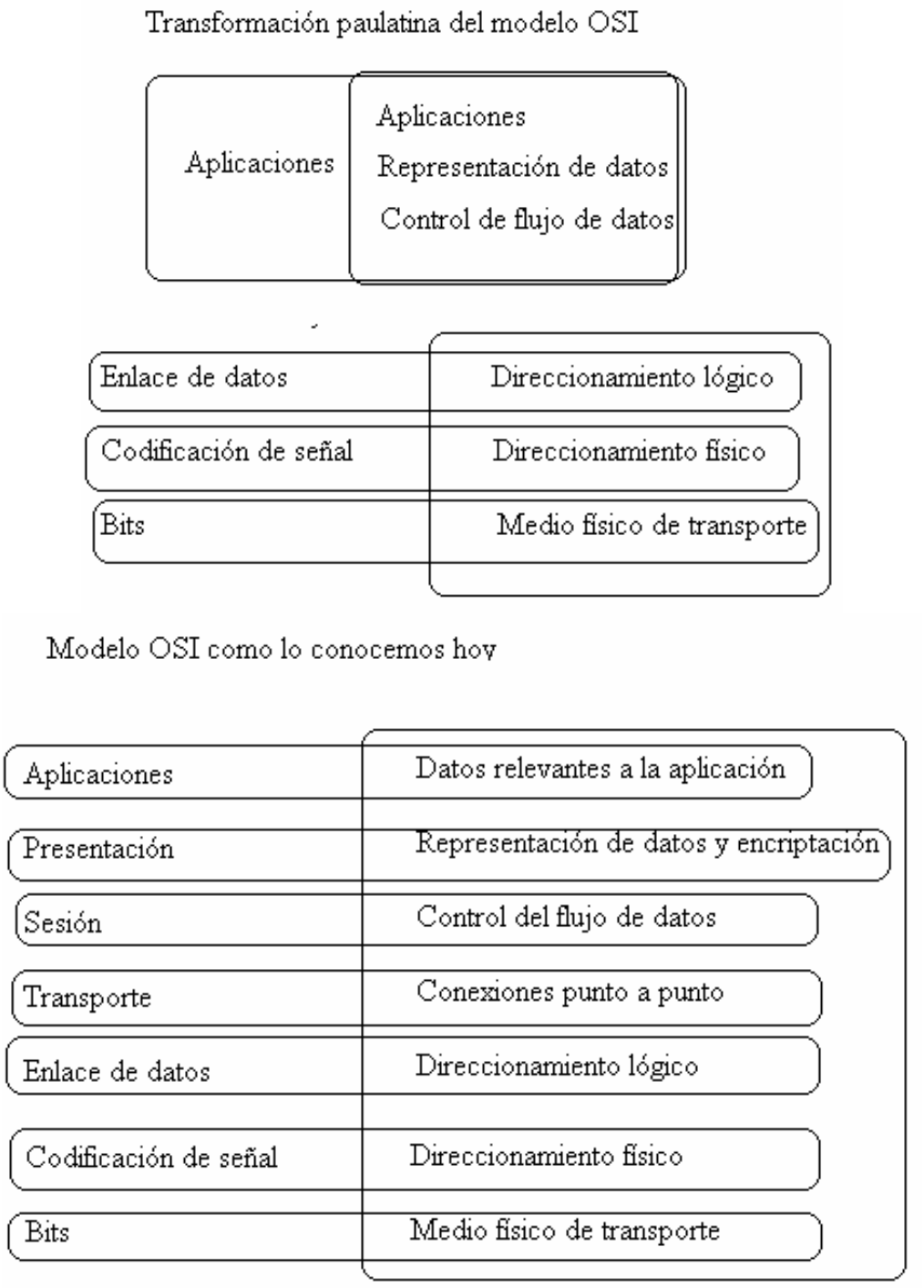


Figura 4.2 Modelo de interconexión de sistemas abiertos

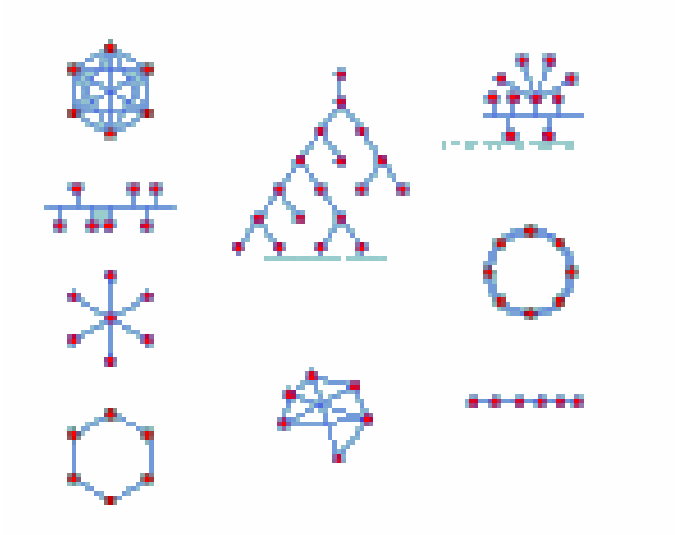
4.9.1 Nuevas tendencias en topologías de redes

Las redes informáticas de la actualidad, proveen un alto nivel de confiabilidad; garantizan ancho de banda y hacen posible la omnipresencia de la información.

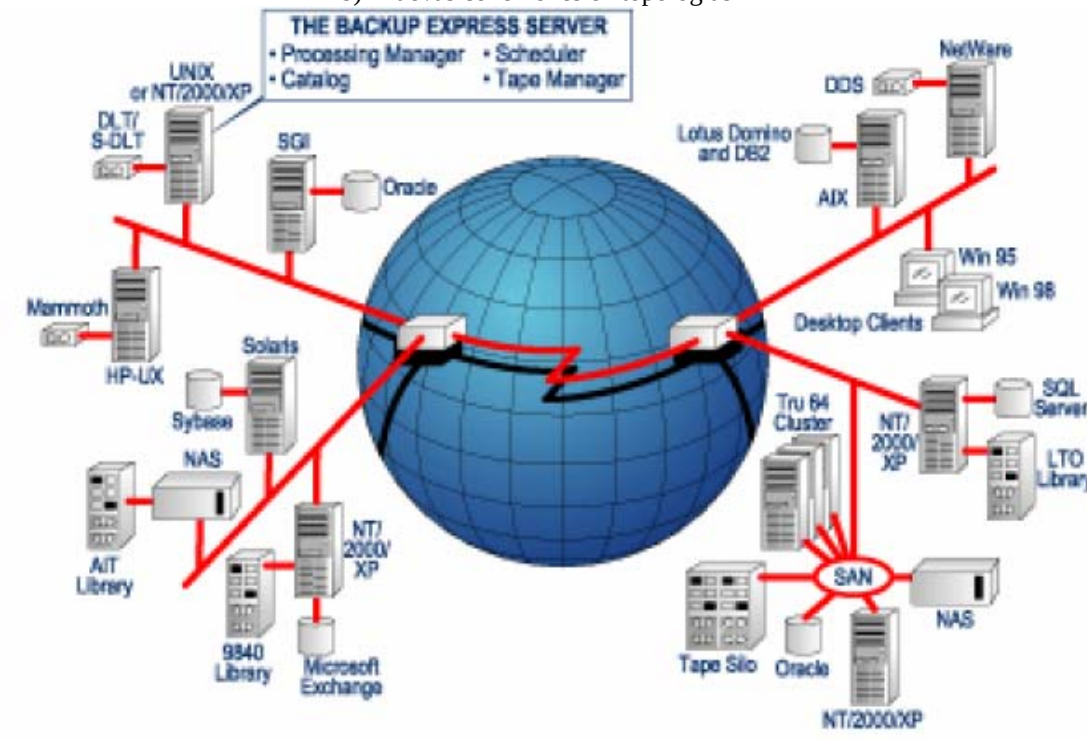
Solamente a través de topologías nuevas e híbridas, la redundancia y eficiencia necesaria puede lograrse.

Lo anterior se muestra gráficamente en la figura 4.3

a) Topologías de redes establecidas



b) Nuevas conexiones en topologías



c) Visiones a futuro

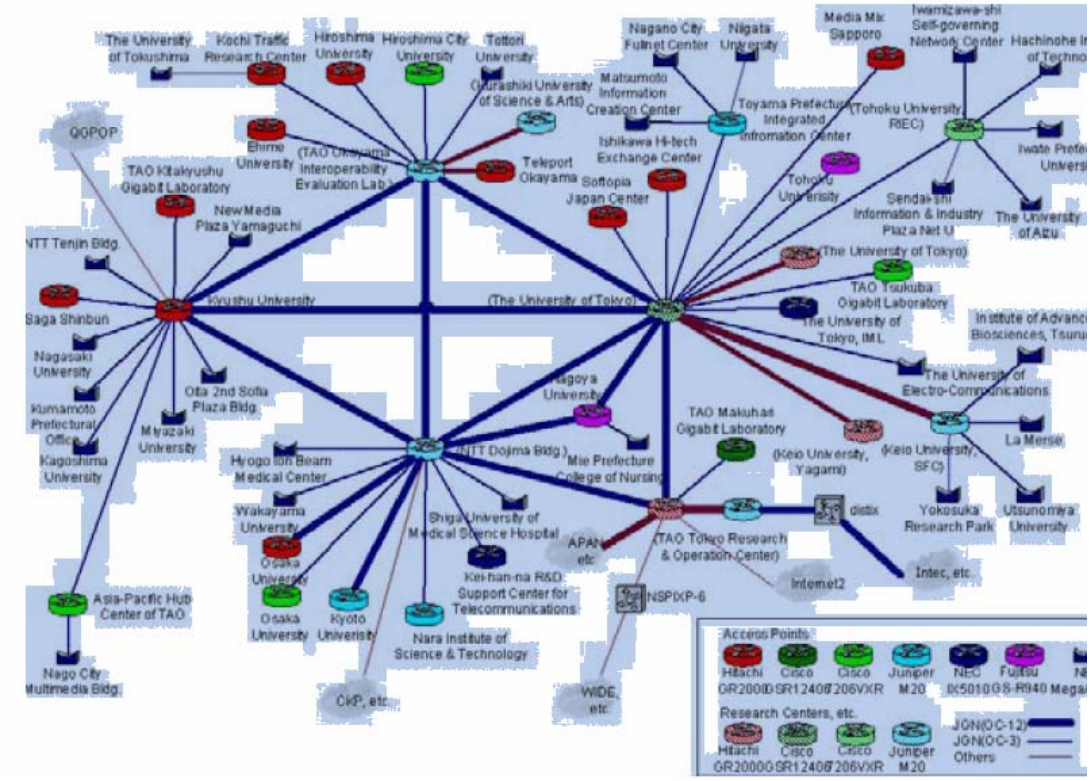


Figura 4.3 Nuevas tendencias en redes

4.9.2 Tendencias de diseño e implementación de redes

En el futuro de las redes informáticas se tienen proyectos muy ambiciosos y, por ende, las características a cubrir cambian adaptándose a las nuevas necesidades.

Entre las características que se pueden listar son:

- Maximizar el flujo de datos
- Los cambios y evolución en las implementaciones de aplicaciones clientes y servicios serán la norma y no la excepción
- La infraestructura debe ser dinámica y diseñada para ser extendida y no monolítica

Lo anterior se enmarca en la figura 4.4

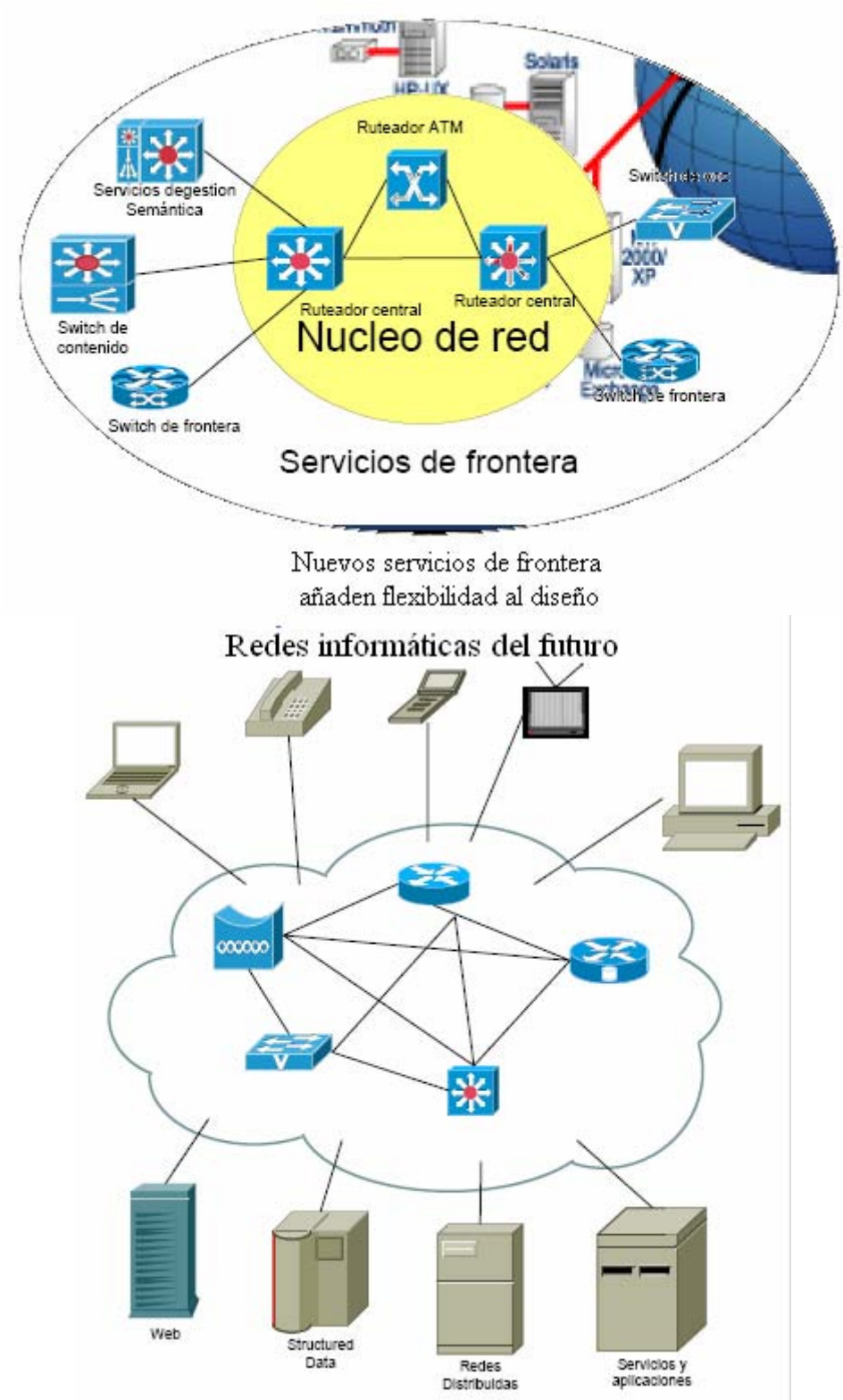


Figura 4.4 Nuevas características de redes

4.9.3 Arquitectura de redes de alto desempeño

La arquitectura de redes de alto desempeño surge cuando la Ethernet de 10 Gb no es suficiente.

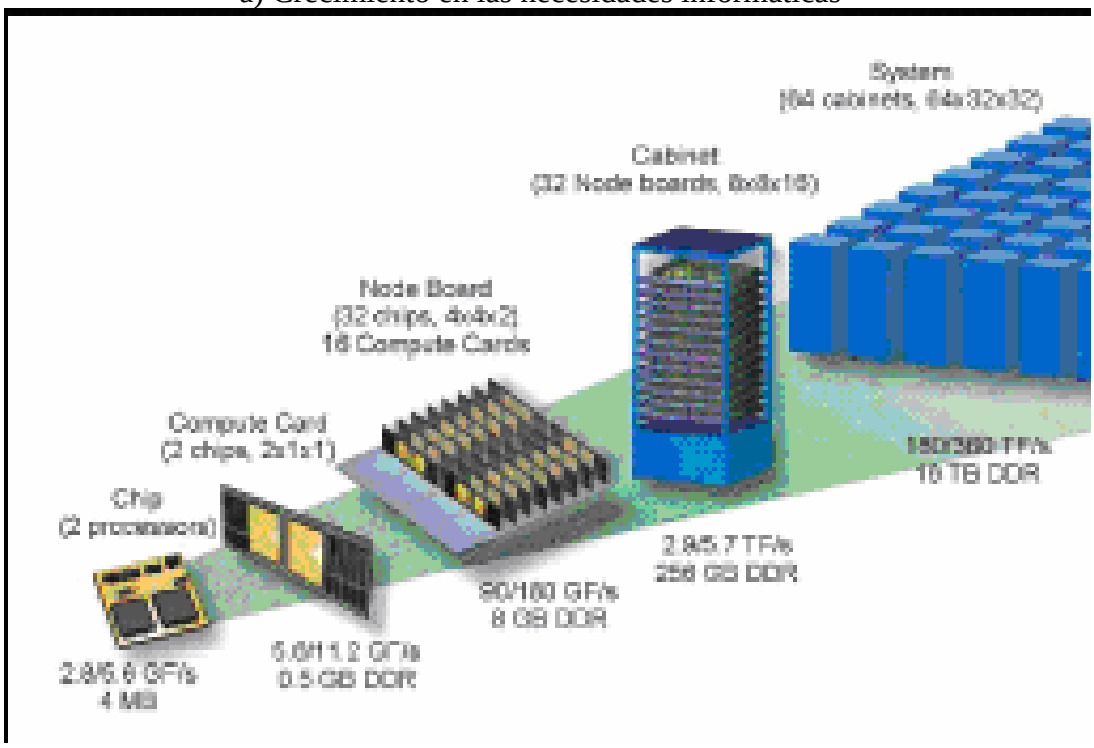
Es necesario hacer mención de que, con la continua caída del precio de la infraestructura, la cantidad de equipo disponible aumenta; asimismo, la necesidad de mantenerlo interconectado también aumenta.

Por otro lado, es necesario desarrollar nuevas técnicas y estándares de interconexión de dispositivos para satisfacer las necesidades crecientes.

La arquitectura de redes toroidales de transmisión múltiple, dicho como ejemplo, provee una alta capacidad con redundancia de canales interconstruida.

Lo anterior se puede ver en la figura 4.5

a) Crecimiento en las necesidades informáticas



b) Redes toroidales

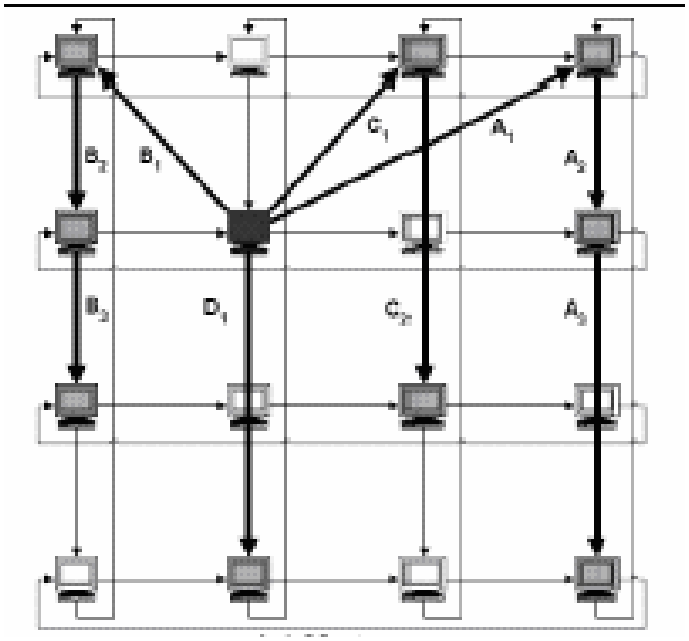


Figura 4.5 Redes de alto desempeño

4.9.4 Redes de aplicaciones distribuidas de gran escala

La implementación en masa de dispositivos de lógica avanzada, capaces de conectarse en red, afectará dramáticamente el flujo y volúmenes de tráfico.

Tradicionalmente, con algoritmos avanzados de negociación semántica de contenido, se puede reducir el tráfico a un volumen manejable.

Se prevé que, en el futuro, sistemas avanzados en la arquitectura orientada a servicios filtrará, sintetizará y agregará la información disponible haciéndola omnipresente.

- Conclusión-

A manera de conclusión, se puede decir que el diseño de redes informáticas no es una tarea sencilla, pero alguien tiene que hacerlo.

Si bien el diseño de redes debe adaptarse a las necesidades de los usuarios en particular, existen medidas a tomar en cuenta de manera general para todas las modalidades de redes, mismas que se recomienda respetar.

Para realizar un buen diseño de redes, las bases están asentadas y los ajustes van a cargo del diseñador de la red; asimismo, es importante tomar en cuenta el tamaño y el alcance de la organización dentro de este contexto.

También, una visión a futuro se hace necesaria, ya que las necesidades actuales de los usuarios se pueden ver modificadas a través del tiempo.

De esta forma y de acuerdo a los requerimientos, hay que tomar en cuenta diversos aspectos, tales como:

- El tipo de usuario de la red
- Las necesidades generales y particulares de la organización en específico.
- El tipo de manejo que se le va a dar a la red.
- La distancia entre las terminales.
- Tipo de terminales
- Ambiciones y/o proyectos a futuro
- Número de usuarios
- Etcétera.

Por supuesto, el software y el hardware son también importantes.

Con esta información, se puede determinar el tipo y la funcionalidad de la red; tomar decisiones en cuanto a:

- Topologías
- Tipo de cables de interconexión
- Tipo y número de dispositivos de red
- Etcétera

Conclusión

Actualmente, las topologías híbridas han tenido mucho más aceptación que las configuraciones sencillas; esto debido a que se combinan las ventajas de cada una de ellas; sin embargo, hay que tener cuidado en acrecentar el nivel de ventajas y no absorber todos los inconvenientes en cada caso.

También se ha puesto de moda la mezcla entre redes cableadas y redes inalámbricas; esto con la finalidad de incrementar el alcance de la red en tiempo y distancia.

Es importante resaltar que toda red informática requiere de la realización de pruebas de funcionamiento antes y después de su implantación, así como una continua revisión y actualización de hardware, software y demás aditamentos, según se requiera.

La seguridad es de suma importancia, sobre todo, cuando se realiza un manejo y/o transferencia de información, y hay que tener cuidado en ese aspecto que resulta fundamental para el manejo de redes.

Para terminar, diré que este proyecto fue creado de la manera más general posible a fin de dar un panorama más amplio en lo que a diseño de redes informáticas se refiere.

Espero que el presente trabajo pueda ser de utilidad.

- Glosario de términos -

2B +D	Codificación de lìnea 2B1Q. 2B+D.- Canales B, By D
802.11	Conjunto de estándares de red de área local inalámbrica definidos por el IEEE.
AC	Control de Acceso, (Access Control)
ACF	Campo de Control de Acceso, (Access Control Field).
ACCESS POINT	Punto de acceso. Dispositivo que normalmente se conecta a los dispositivos de cliente. Tiene un punto Ethernet y otro de energía; e incluye uno o dos antenas que transmiten y reciben señales RU.
ACCESO REMOTO	Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.
ACCESORIO WI FI	Es el accesorio adicional que usaremos para incoporar el estándar 802.11 a nuestro equipo (PDA, ordenador portátil o de sobremesa), en caso de no tener Wi-Fi integrado. Estos accesorios pueden encontrarse en formato de tarjetas PCMCIA (para portátil), PCI y USB (para ordenador de sobremesa) y esperamos que muy pronto en formato SD (Secure Digital) para nuestros PDAs Palm OS.
ACK	Acuse de Recibo, (Acknowledgement)
AD-HOC	(Punto a Punto). Modo de conexión en una red wireless que define que nuestro equipo (PDA, ordenador portátil o de sobremesa) se conectará directamente a otro equipo, en vez de hacerlo a un Punto de Acceso. Ad-Hoc es una forma barata de tener conexión a Internet en un segundo equipo (por ejemplo un PDA) sin necesidad de comprar un Punto de Acceso. Para este uso la configuración se dificulta ya que tenemos que configurar en el ordenador que tiene la conexión a Internet un programa *enrutador* o una conexión compartida.

ADM	Multiplexor Agregar-soltar
ADMINISTRADOR	Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local o de un servidor de red.
ADMINISTRACIÓN DE RED	Término que se usa para describir sistemas o acciones que ayudan a mantener Y caracterizar una red; o resolver problemas de la red.
ADCPM	Modulación adaptativa por código de pulso referencial
AMPLIFICADOR	Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido pre-amplificado y un amplificador lineal de salida de radio frecuencia (RF).
ANCHO DE BANDA	Rango de frecuencia necesaria para transportar una señal, medido en unidades de Hertz (HZ). Depende del esquema de modulación, velocidad de datos y cantidad de canales del espectro de radio.
ANSI	Acrónimo del Instituto Nacional de estándares de Estados Unidos. Una organización voluntaria compuesta de miembros corporativos, gubernamentales y de otros tipos, que coordina las actividades relacionadas con los estándares internacionales y de la Unión Americada relacionados, entre otras cosas, con las comunicaciones y las redes.
ANTENA	Dispositivo para transmitir o recibir una frecuencia de radio (RU); están diseñadas para frecuencia específicas y de manera relativamente estricta.
ARP	Protocolo de Resolución de Dirección, (Address Resolution Protocol).
ARPA	Agencia de Investigación de Proyectos Avanzados, (Advanced Research Projects Agency).

ARPANET	Red pionera de gran alcance fundada por ARPA (Advanced Research Projects Agency) después DARPA. Sirvió de 1969 a 1990 como base para las primeras investigaciones de red durante el desarrollo de Internet. ARPANET consiste en nodos individuales conmutadores de paquetes interconectados por líneas arrendadas.
ARQ	Requerimiento de Repetición Automático, (Automatic Repeat Request).
ASCII	Código estándar de Estados Unidos para el intercambio de información. Especifica un código de ocho bits para la representación de caracteres.
ATM	Model de Transferencia Asíncrono, (Asynchronous Trabsfer Mode).
ATENUACIÓN	Pérdida de energía en la señal de comunicación; sea por el diseño del equipo, manipulación del operador o transmisión a través de un medio.
AUTENTICACIÓN	Verificación de la identidad de una persona o proceso. Es abierta si se verifica a una persona; es de estación si lo que se verifica es un dispositivo.
BANDA BASE	Banda angosta, característica de una tecnología de red donde solamente se usa un portador de frecuencia.
BANDA DE PASO	Se le denomina a las frecuencias que un radio permite que pasen desde su entrada hasta su salida.
BIT	Es la unidad más pequeña de información que puede controlar una computadora. Es un dígito binario; es decir, un cero o un uno.
BLUETOOTH	Tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de diez). No está pensada para soportar redes de ordenadores, sino para comunicar un ordenador o un dispositivo con sus periféricos.

BPSK	Acrónimo de la modulación de fase por desplazamiento binario. Se trata de una técnica de modulación de frecuencia digital que se usa para transmitir información.
BRI	Interfaz de Tasa Básica, (Basic Rate Interface).
BRIDGE	Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar
BSS	Basic Service Set. Conjunto de servicios básicos. Es una modalidad de comunicación en las que se puede configurar las terminales de una red Wi Fi. También es conocido como modo infraestructura.
BYTE	Conjunto de ocho bits. Representa un carácter alfabético o numérico.
CCK	Complementary Code K-ying Salto de código complementario. Es una técnica de modulación utilizada en Wi Fi junto con las técnicas de espectro distribuido.
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía, (Committee Consultative Internacional for Telegraphy and Telephony).
CCS	Señalización de Canal Común, (Common Channel Signaling).
CDMA	Acceso Múltiple por División de Código, (Code Division Multiple Access).
CERTIFICADO	Una declaración firmada en forma digital de una entidad que establece que una clave pública en alguna entidad tiene algún valor en particular.
CIB	Bit Indicador de CRC 32, (CRC 32 Indicator Bit).
CIR	Tasa de Información Comprometida, (Commited Information Rate)

CLAVE	Se usa para abrir un texto cifrado. La clave se puede considerar en los mismos términos relativos que un cerrojo o una llave. Una sola clave puede generar una gran cantidad de versiones diferentes de texto cifrado desde el texto sencillo.
CLAVE DE ENCRIPTACIÓN	Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.
CLAVE DE REGISTRO	El registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiarán de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.
CNM	Gestión de Red de Cliente, (Customer Network Management).
COCF	Función de Convergencia Orientada a Conexiones, (Connection- Oriented Convergente Function).
COM	Continuación del Mensaje (Continuation of the Message).
CONMUTACIÓN DE PAQUETES	Método que consiste en dividir toda la información que sale de un ordenador para ser trasmitida por la red en bloque de determinada longitud (Paquetes) que contienen la información relacionada con el origen y destino del paquete así como el orden que ocupa dentro de la división realizada. Esto permite que cada paquete se mueva de forma independiente en la red y al llegar a su destino puedan ser reensamblados para construir nuevamente la información enviada.
CORTAFUEGOS	Firewall. Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc...

CPCS	Subcapa de Convergencia de Parte Común, (Common Part Convergente Sublayer).
CPCS-UU	Subcapa de Convergencia de Parte Común-Indicación Usuario a Usuario, (Common Part Convergente Sublayer-User to User Indication).
CRC	Verificación de Redundancia Cíclica (Cyclic Redundancy Check)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance. Acceso múltiple por detección de portadora con evitación de colisión. Es el sistema que emplea Wi Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión)
CSMA/CD	Acceso Múltiple por Detección de Portadora/Detección de Colisiones, (Carrier Sense Multiple Access/Co/lision Detect)
CSR	Tasa de Bit Constante, (Constant Bit Rate).
CSTA	Aplicaciones Telefónicas Soportadas por Ordenador, (Computer Supported Telephony Applications).
CSU	Unidad de Servicio de Canal, (Channel Service Unit).
DECT	Telecomunicaciones Digitales Europeas sin Cordón, (Digital European Cordless Telecommunications).
DESENCRIPTAR	Proceso de transformación de ciphertext - texto encriptado o cifrado - a plaintext. Es la acción inversa a encriptar.
DHCP:	Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente. Por defecto la mayoría de los routers ADSL y los Puntos de Acceso tienen DHCP activado.

DISPOSITIVO MÓVIL	Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras,...).
DIRECCIÓN MAC:	(MAC address - Media Access Control address) Es el código único de identificación que tienen todas las tarjetas de red. Nuestro accesorio Wi-Fi o nuestro PDA con Wi-Fi integrado, al ser un dispositivo de red, también tendrá una dirección MAC única. Las direcciones MAC son únicas (ningún dispositivo de red tiene dos direcciones MAC iguales) y permanentes (ya que vienen preestablecidas de fábrica y no pueden modificarse).
DLCI	Identificador de Conexión de Enlace de Datos, (Data Link Connecuonldenufie)·
DNA	Arquitectura Digital de Red, (Digital Network Architecture).
DNS	Sistema de Nombres de Dominio, (Domain Name System). DP.- Punto de Detección, (Detectionon Point).
DPDU	PDU de Capa de Enlace de Datos, (Data Link Layer PDU). DPSK.- PSK Differential, (Differential PSK).
DSI	Interpolación Digital de Voz, (Digital Speech Interpolation).
DSP	Parte Específica para el Dominio, (Domain Specific Part).
DSSS	Espectro Amplio mediante Secuencia Directa. A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos .Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.

DSU	Unidad de Datos de Servicio, (Data Service Unit).
DTE	Equipo Terminal de Datos, (Data Terminal Equipment).
DTI	Departamento de Comercio e Industria, (Department of Trade and Industry).
DTMF	Tono Dual, Múltiple Frecuencia, (Dual Tone Multiple Frecuency)
EC	Comisión Europea, (European Commission).
ECMA	Asociación de Fabricantes de Equipo de Cómputo Europea, (European Computer Manufacturers Association).
ECSA	Asociación de Normas Portadoras de Intercambio, (Exchange Carriers Standards Association).
EOM	Fin del Mensaje, (End of Message).
ESTÁNDAR	Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etcétera.
ETHERNET	Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.
ETSI	Instituto de Normas de Telecomunicaciones Europeas, (European Telecommunications Standard Institute).
FCC	Comisión Federal de Comunicaciones, (Federal Communicauons Commission).
FDDI	Interfaz de Datos Distribuida por Fibra, (Fiber Distribuited Data Interfaz).

FEC	Control de Errores hacia Adelante, (Forward Error Control).
FECN	Bit de Notificaciones Explícita de Congestionamiento hacia Adelante, (Forward Explicit Congestion Notification Bit).
FHSS	Espectro Amplio mediante Saltos de Frecuencia. Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar acabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este "Hopping Pattern". El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.
FIRMA ELECTRÓNICA	El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.
FIRMWARE	Software (programas o datos) escritos en la memoria de sólo lectura (ROM). El firmware es un combinación de software y hardware. ROMs, PROMs e EPROMs que tienen datos o programas grabados dentro son firmware.
FRF	Foro de Frame Relay, (Frame Relay Forum).
FTP	Protocolo de transferencia de archivos que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

GATEWAY	Puerta de enlace Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas
GSM	Grupo Especial Móvil, (Groupe Speciale Mobile)
GUI	Interfaz Gráfica de Usuario, (Graphical User Interface
HARDWARE (MAQUINARIA)	Componentes físicos de una computadora o de una red, a diferencia de los programas o elementos lógicos que los hacen funcionar.
HCS	Secuencia de Verificación de Encabezado, (Header Check Sequence).
HDCL	Control de Enlace de Datos de Alto Nivel, (High Level Data Link Control).
HDSL	Línea de Suscriptor Digital con Alta Tasa de Bits, (High Bit-Rate Digital Subscriber Line).
HOTSPOT	Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc...) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.
HTTP	Protocolo de Transferencia de Hipertexto, (Hyper Texte Transfer Protocol).
HUB	(concentrador) Dispositivo electrónico al que se conectan varios ordenadores, por lo general mediante un cable de par trenzado. Un concentrador simula en la red que interconecta a los ordenadores conectados.
ICF	Función de Convergencia Isócrona, (lsochronous Convergence Function).
ICI	Interfaz de Portadora de Intercambio, (lnterchange Carrier Interfaz).
ICIP	Protocolo ICI, (lCI Protocol).

IEEE	Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Es la sociedad que se encarga de los estándares de redes a nivel internacional.
IGMP	Internet Group Multicast Protocol. IKE.- Internet Key Exchange.
IMPDU	Unidad de Datos de Protocolo MAC Inicial, (Inicial MAC Protocol Data Unit).
INFRAESTRUCTURA	Modo de conexión en una red wireless que define que nuestro equipo (PDA, portátil u ordenador de sobremesa) se conectará a un Punto de Acceso. El modo de conexión debe de especificarse en la configuración de nuestro equipo o del accesorio Wi-Fi. Por defecto viene activado este modo.
INTEGRIDAD DE ARCHIVOS	Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).
INTERNET	Conjunto de redes y ruteadores que utiliza los protocolos TCP/IP para formar una sola red virtual cooperativa.
IP	Protocolo de Internet, (Internet Protocol).
IPv4	Protocolo de Internet Versión 4, (Internet protocol Version 4).
IPv6	Protocolo de Internet Versión 6, (Internet protocol Version 6)

IP ADDRESS	Dirección IP. Una dirección IP es una serie de números que identifica a nuestro equipo dentro de una red. Distinguimos entre IP pública (ej. 80.20.140.56), cuando es la dirección que nos identifica en Internet (por ejemplo la IP de tu router ADSL en Internet) e IP privada (ej. 192.168.0.2), que es la dirección que identifica a un equipo dentro de una red local (LAN). Si, por ejemplo, pensamos en una red local con un router ADSL, los PCs o equipos conectados a la red tendrán sólo IP privada, mientras que el router tendrá una IP pública (su identificación en Internet) y una IP privada (su identificación en la red local).
ISDN	Red Digital de Servicios Integrados, (Integrated Services Digital Network).
ISO	Organización Internacional de Normas, (Internacional Standards Organization).
ISP	Internet Service Provider.
ISUP	Parte de Usuario de ISDN, (ISDN User Part).
ITU	Unión Internacional de Telecomunicaciones, (Internacional Telecommunications Union).
LAN	Red de área local. Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topologia en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.
LAPB	Procedimiento de Acceso a Enlaces Balanceado, (Link Access Procedure Balanced).
LAPD	Procedimiento de Acceso a Enlaces para el Canal O, (Link Access Procedure for the D Channel).

LT	Terminación de Línea, (Line Termination).
MAC	Dirección de Control de Acceso a Medios. Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexademinal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.
MAN	Red de Área Metropolitana, (Metropolitan Area Network).
MBPS	Megabits por segundo. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.
MHz	Mega hertz. Unidad empleada para medir la "velocidad bruta" de los microprocesadores equivalente a un millón de hertzios.
MIB	Base de Información de Gestión, (Management Information Base)
MID	Identificador de Mensaje, (Message Identifier).
MMDS	Servicio de Distribución Multipunto Multicanal, (Multipoint Multichannel Distribution Service).
MODEM	Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).
MPLS	Mufti Protocol Laber Switching.
MSU	Unidad de Señal de Mensaje, (Message Signal Unit).

MTP	Parte Transferencia de Mensajes, (Message Transfer Part).
N-ISDN	ISDN de Banda Angosta, (Narrowband ISDN).
NAK	Acuse de Recibo Negativo, (Negative Acknowlegment)
NEI	Identificador de Entidad de Red, (Network Entity Identifier)
NIU	Unidad de Interfaz de Red, (Network Interface Unit). MNS.- Network Management System.
NNI	Interfaz Red-Nodo (Network-Node Interface). NNI.- Interfaz Red-Red, (Network-to-Network Interface). NOC.- Network Operations Center.
OSPF	Abrir Primero el Trayecto más Corto, (Open Shortest Path First).
PABX	Private Automatic Branch Exchange. PBX.- Private Branch Exchange.
PCI	Protocol Control Information.
PCM	Modulación por Código de Pulso, (Pulse Code Modulation)
PCMCIA	Personal Computer Memory Card Internal Associated
PHY	Capa Física, (Phisical Layer).
PPTP	Poin-to-Point Tunneling Protocol.
PRI	Interfaz de Tasa primaria, (Primary Rate Interface).
PROTOCOLO	Descripción formal de formatos de mensajes y reglas que dos o más ordenadores deben seguir para intercambiar mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de ordenador a ordenador o el intercambio entre programas de aplicación.
PSK	Modulación por Desplazamiento de Fase, (Phase Shift Key)
PSTN	Public Switched Telephone Network.

PT	Tipo de carga Útil, (Payload Type).
PTT	Protocolo para Telefonía y Telegrafía.
PUNTO DE ACCESO	Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.
PVC	Circuito Virtual Permanente, (Permanent Virtual Circuit)
PVN	Red Virtual Permanente, (Private Virtual Network).
QAM	Modulación de Amplitud y Cuadratura, (Quadrature Amplitude Modulation).
QoS	Calidad de Servico, (Quality of Service).
QPSK	Modulación de Cuadratura y Desplazamiento de Fase, (Quadrature Phase Shift Keyed).
ROUTER	Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.
ROAMING	En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad
RQ	Contador o Temporizador de Solicitudes, (Request Timer) .
SAP	Punto de Acceso al Servicio, (Service Access Point).
SAPI	Identificador de Punto de Acceso al Servicio, (Service Access Point Identifier) .
SDDI	Especificación de Par trenzado Blindado

SDH	Jerarquía Digital Síncrona, (Synchronous Digital Hierachy)
SER	Tasa de Errores de Bit (Bit Error Rate). BOOTP.- Bootstrap Protocol.
SERVIDORES DNS	DNS Server. Las páginas web también tienen su dirección IP pública y es a través de ésta dirección como en realidad nos conectamos a ellas. Pero claro, es más sencillo memorizar o escribir el nombre del dominio que su dirección IP. Para no memorizar la retahíla de números tenemos los servidores DNS. Un servidor DNS es un servidor en donde están almacenadas las correlaciones entre nombres de dominio y direcciones IP. Cada vez que cargamos una página web, nuestro equipo (PDA, portátil u ordenador de sobremesa) envía una petición al servidor DNS para saber la dirección IP de la página que queremos cargar, y es entonces cuando hace la conexión. Probablemente se esta familiarizado con eso de "servidor DNS primario" y "servidor DNS secundario". El primario es el "principal" y el secundario es el de emergencia que usará nuestro ordenador en caso de que el primario no funcione.
SIR	Tasa de Información Sostenida, (Sustained Information Rate).
SISTEMA OPERATIVO	Conjunto de programas o software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera eficiente.
SNMP	Protocolo Simple de Gestión de Redes, (Simple Network Management Protocol).
SOFTWARE	Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica de una computadora.
SONET	Red Óptica Síncrona, (Synchronous Optical Network).
SPVC	Circuito Virtual Semipermanente, (Semipermanent Virtual Circuit)

SQL	Standard Query Language.
SSID	Service Set Identification. Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso.
STDM	Multiplexor Estadístico por División en el Tiempo, (Statistical Time Division Multiplexer).
SUBNET ADDRESS	Máscara de subred: () Cifra de 32 bits que especifica los bits de una dirección IP que corresponde a una red y a una subred. Normalmente será del tipo 255.255.255.0
SVC	Circuito Virtual Conmutado, (Switched Virtual Circuit).
SWITCH	(interruptor o conmutador). Dispositivo de interconexión de redes de ordenadores. Un switch interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo con la dirección de destino de los datagramas en la red. Los switches se utilizan cuando se desea conectar múltiples redes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las mismas.
TARJETA DE RED INALÁMBRICA	Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB
TCP	Protocolo de Control de Transmisión, (Transmisión Control Protocol)
TCP/IP	Protocolo que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes.
TDM	Multiplexión por División en el Tiempo, (Time Division multiplexing)

TDMA	Acceso Múltiple por División del Tiempo, (Time Division Multiple Access).
TELNET	Protocolo TELNET
TEXTO CODIFICADO	Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo.
ToS	Tipo de Servicio, (Type of Service)
TTY	Teletipo
UI	Información no Numerada, (Unnumbered Information). UDP.- User Datagram Protocol.
ULP	Protocolos de Capa Superior, (Upper Layer Protocols)
UTP	Par Trenzado no Blindado, (Unshielded Twisted Pair).
VC	Canal Virtual, (Virtual Channel).
VCC	Conexión de Canal Virtual, (Virtual Channel Connection)
VLAN	Virtual LAN
VPC	Conexión de Trayectoria Virtual, (Virtual Path Connection)
VPN	Red Privada Virtual. Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (*LAN*).

WEP	(Wired Equivalent Privacy). Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.
WAN	Red de cobertura amplia. Tipo de red compuesta por dos o más redes de área local (LANs) conectas entre si vía teléfono (generalmente digital).
WI FI ALLIANCE	Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado
WI FI	WiFi es el nombre comercial del estándar IEEE 802.11. Es una tecnología novedosa y práctica que se está difundiendo rápidamente por todo el planeta. No obstante, es una tecnología inmadura, que requiere de nuevos estándares, cada vez, o modificaciones de los ya existentes, en la medida en que van apareciendo inconvenientes.
WIMAX	Worldwide Interoperability for Microwave Access. Grupo no lucrativo formado en abril de 2003 iniciativa de Intel/Nokia/Fujitsu/entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica
WLAN	También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA	Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.
WPA	WPA - Protocolo de Seguridad en redes Inalámbricas. Protocolo de Seguridad para redes inalámbricas. Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i
WPA2	Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.

- Bibliografía -

- Introducción a la teleinformática.
  Eduardo Alcalde - Jesús García Tomás.
  Mc graw hill.

- Comunicaciones y redes de procesamiento de datos.
  Néstor González Saínz.
  Mc graw hill.

- Redes de computadoras.
  Andrew s. Tanenbaum.
  Prentice hall.
  Segunda edición.

- Enciclopledia lan times de redes (networking).
  Tom Sheldon.
  Mc graw hill.
  Primera edición.

- Aprendiendo tcp/ip en 14 días.
  Timothy Parker, ph.d.
  Traducción de Gabriel Sánchez García.
  Prentice hall p t r.
  1995.

- Fuentes –

- http://www.geocities.com/SiliconValley/8195/redes.html#uno
- http://lafacu.com/apuntes/informatica/redes/default.htm
- http://www.monografias.com/trabajos11/reco/reco.shtml
- http://www.geocities.com/SiliconValley/Campus/2208/CWred.html
- http://fmc.axarnet.es/redes/tema_02.htm
- http://www.geocities.com/nicaraocalli/Redes/Redes.htm
- http://www.geocities.com/SiliconValley/8195/redes.html#uno
- http://www.geocities.com/SiliconValley/8195/redes.html#uno
- http://lafacu.com/apuntes/informatica/redes/default.htm
- http://www.monografias.com/trabajos11/reco/reco.shtml
- http://www.geocities.com/SiliconValley/Campus/2208/CWred.html
- http://fmc.axarnet.es/redes/tema_02.htm
- http://www.geocities.com/nicaraocalli/Redes/Redes.htm
- http://www.geocities.com/SiliconValley/8195/redes.html#uno

- Objetivos –

Los objetivos generales del presenta trabajo son:

- Mostrar un panorama general en el diseño de redes informáticas

- Marcar las opciones existentes y sus posibles combinaciones para el eficiente y óptimo diseño de redes informáticas.

- Justificación –

A manera de justificación, se puede decir que un problema actual que aqueja a las organizaciones es el manejo de la información y el traslado de ésta en diferentes distancias a distintos usuarios.

En este sentido, se hace latente la necesidad de crear redes informáticas para que cumplan con este cometido de la manera más eficiente y segura posible.

El trabajo del diseñador de redes informáticas no es sencillo, pero se complica más si no posee la suficiente información para realizar un óptimo trabajo.

De ahí, se ve la función de este proyecto de tesis, en donde se muestran los caminos a seguir para un diseño óptimo de redes informáticas.

No obstante, no pretende ser una receta de cocina cuyos puntos deban ser seguidos con escrupuloso respeto; más bien pretende ampliar la visión de los diseñadores de redes para obtener el mayor provecho posible para un óptimo diseño de redes informáticas.