

## CAPITULO I

### ANTECEDENTES Y MARCO TEORICO

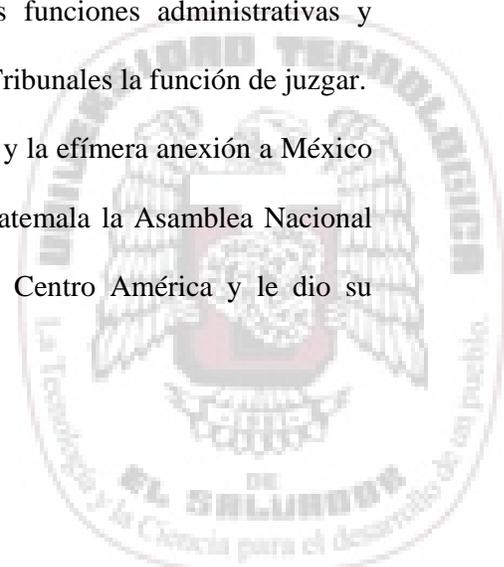
#### 1. Antecedentes de la Empresa

Las primeras autoridades judiciales establecidas en las Colonias eran los Capitanes Generales y Gobernadores de las Provincias, quienes conocían de asuntos Judiciales y Administrativos.

En 1543, Carlos I creó un Tribunal de Justicia llamado Audiencia de los Confines que tenía jurisdicción en casi toda América Central y el Sur de México, conocía de todas las causas criminales que habían sido sentenciadas por Alcaldes y Gobernadores de Provincia, también conocía de los negocios civiles con recurso al Consejo de Indias. La diversidad de materias que conocía la Audiencia de los Confines, volvió la administración de justicia lenta y complicada.

La Constitución de 1812 fue la primera que usó la denominación de Tribunal Supremo de Justicia para la autoridad judicial, nombre tomado de la Constitución francesa de 1792. En aquella se dividieron las funciones administrativas y judiciales, correspondiendo exclusivamente a los Tribunales la función de juzgar.

Después de los sucesos de Independencia en 1821 y la efímera anexión a México en 1822, el 24 de julio de 1823 se instaló en Guatemala la Asamblea Nacional Constituyente que creó la República Federal de Centro América y le dio su Constitución el 22 de noviembre de 1824.



La Federación estuvo formada por los Estados de Guatemala, El Salvador, Honduras, Nicaragua y Costa Rica. Por esos mismos días los Estados organizaron sus Congresos Constituyentes. El 18 de marzo de 1824, el Congreso Constituyente de El Salvador estableció la que fue la primera Corte Suprema de Justicia del Estado. Fue Presidente de dicho organismo el Licenciado Joaquín Durán y Aguilar, a quien acompañaron otros dos Magistrados. La Federación se extinguió prácticamente en 1840 y los cinco Estados se convirtieron en Repúblicas Independientes. Desde 1824 ha existido en el país una Corte Suprema de Justicia como máxima entidad del Órgano Judicial <sup>1</sup>.

En la actualidad la red Técnica- Jurídica que posee el Órgano Judicial de El Salvador, está compuesta por cuatro puntos de interconexión:

- Edificio Corte Suprema de Justicia (Ubicado en el Centro de Gobierno, San Salvador), se encuentran 350 computadoras.
- Unidad de Informática (Ubicado en la 43Ave. Norte y prolongación Calle Arce, N. 132), se encuentran 60 computadoras.
- Edificio Centro de Documentación Judicial (Ubicado en el Bo. San Miguelito, Final 19 calle poniente, N. 135), se encuentran 40 computadoras.
- Anexo Centro de Documentación Judicial ó Área de Legislación ( ubicado en la plaza San Antonio, tercer nivel, final Avenida Juan Pablo II), se encuentran 25 computadoras.

---

1 Sitio Web Oficial de la Corte Suprema de Justicia [www.csj.gov.sv](http://www.csj.gov.sv)



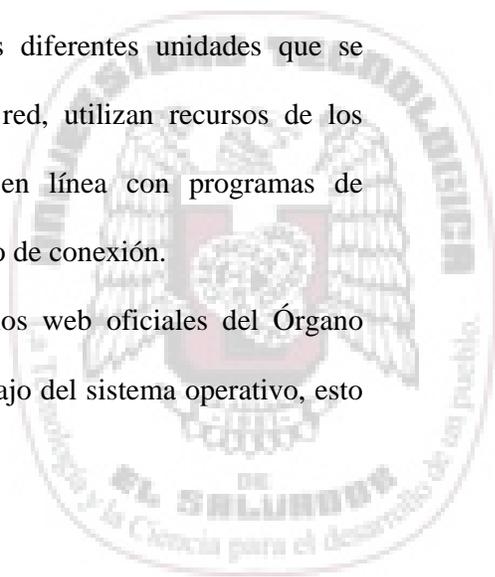
Actualmente estos puntos están interconectados por tecnología de fibra óptica, línea dedicada y sitios web oficiales del órgano judicial.

En cada punto de interconexión existen servidores de archivos, procesando altos volúmenes de información tanto jurídica como administrativos.

## **1.1 Situación Problemática**

La red informática se encuentra trabajando con anomalías en sus esquemas informáticos, tales como el alto tráfico de transmisión de datos dentro de la red, este tráfico ocasiona saturación en la comunicación de información en la estructura de la red, la transmisión de archivos de grandes volúmenes no laborales entre los puntos de interconexión de la red. La utilización de diferentes programas de navegación que se utilizan por Internet en horas picos demuestran que el rendimiento de la misma reduce su funcionalidad, y crea congestión en los diferentes paquetes de información, los programas que trabajan en línea (conectados a Internet) no son auditados en sus procedimientos por algún tipo de documento o normativa técnica. Cuando se encuentra trabajando la transmisión de información en las diferentes unidades que se encuentran interconectadas bajo el ambiente de red, utilizan recursos de los servidores de archivos que están trabajando en línea con programas de aplicación y procesos administrativos en cada punto de conexión.

La frecuencia de registros de ataques a los sitios web oficiales del Órgano Judicial quedan registrados en la bitácora de trabajo del sistema operativo, esto

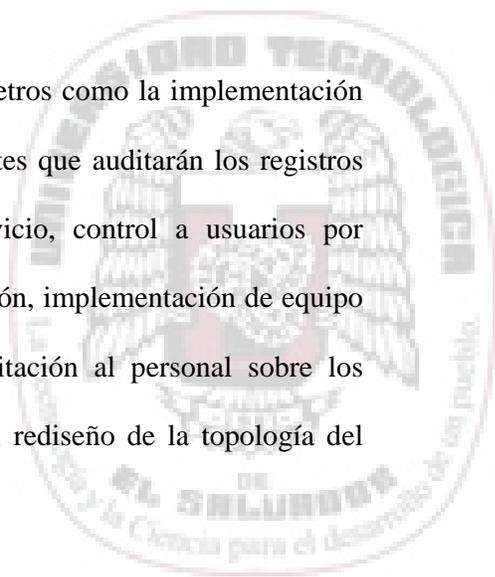


manifiesta la poca protección que existe en el esquema de la red informática. Otra situación importante dentro del esquema es el usuario que por desconocimiento del entorno de red, realiza procedimientos erróneos en los programas de aplicación que se encuentran trabajando en línea con las demás terminales de la red y a su vez afecta al rendimiento de la misma, tales como el envío de correos con archivos adjuntos de gran volumen.

El elevado índice de usuarios consultando las diferentes bases jurídicas publicadas en Internet se está realizando en servidores con capacidades mínimas de Hardware, lo cual el tiempo de respuesta no es óptimo para todos los procesos que se encuentran en cada uno de ellos.

El bajo rendimiento de la Red Informática posee parámetros claros que no benefician al desarrollo del funcionamiento de la Red Técnica, teniendo en cuenta congestión en la red por el volumen de información manejada, demasiada demanda al acceso de usuarios a los diferentes puntos de interconexión, utilizando programas no autorizados a la labor de la Institución, el equipo con características técnicas de Hardware mínimos, la confiabilidad con la seguridad tanto de información como de usuarios sin autorización registrándose a los diferentes Servidores de Archivos en uso.

Para ello se marcan controles a todos estos parámetros como la implementación de políticas de seguridad de Información y paquetes que auditarán los registros de bitácoras de trabajo de los equipos en servicio, control a usuarios por navegación en sus diferentes puntos de interconexión, implementación de equipo con características actuales de tecnología, capacitación al personal sobre los programas en uso y entorno del ambiente de red, rediseño de la topología del



anillo de comunicación del Órgano Judicial. Ya que con lo anterior la funcionalidad de la Red Técnica – Jurídica fuese más óptimo.

## **1.2 Justificación de la investigación**

Dada la problemática que presenta la red Informática del Órgano Judicial de El Salvador, se realizó una propuesta de seguridad de transmisión de datos y rendimiento de la red Técnica – Jurídica. Fue importante la investigación ya que con ello se pretende mejorar la seguridad, control y rendimiento. Lo antes mencionado brindará lo siguiente:

- Se transmitirán datos de una forma más rápida en una estructura moderna en su red de interconexión de datos.
- Habrá una red más segura contra ataques de virus y Hackers.
- Se promoverá al personal capacitaciones de informática y redes.
- La adquisición de tecnología por el Órgano Judicial de El Salvador, será trascendental en su área de Informática, ya que mejoraría su red LAN / WAN, así como su seguridad en sus datos.

## **1.3 Delimitación y alcance de la investigación**

### **1.3.1 Delimitación**

#### **1.3.1.1 Delimitación espacial**

La investigación de los cuatro puntos de interconexión se llevará a cabo en la ciudad de San Salvador.



### 1.3.1.2 Delimitación geográfica

Se realizará en los siguientes puntos de conexión:

En el Edificio de la Corte Suprema de Justicia, Centro de Gobierno, San Salvador.

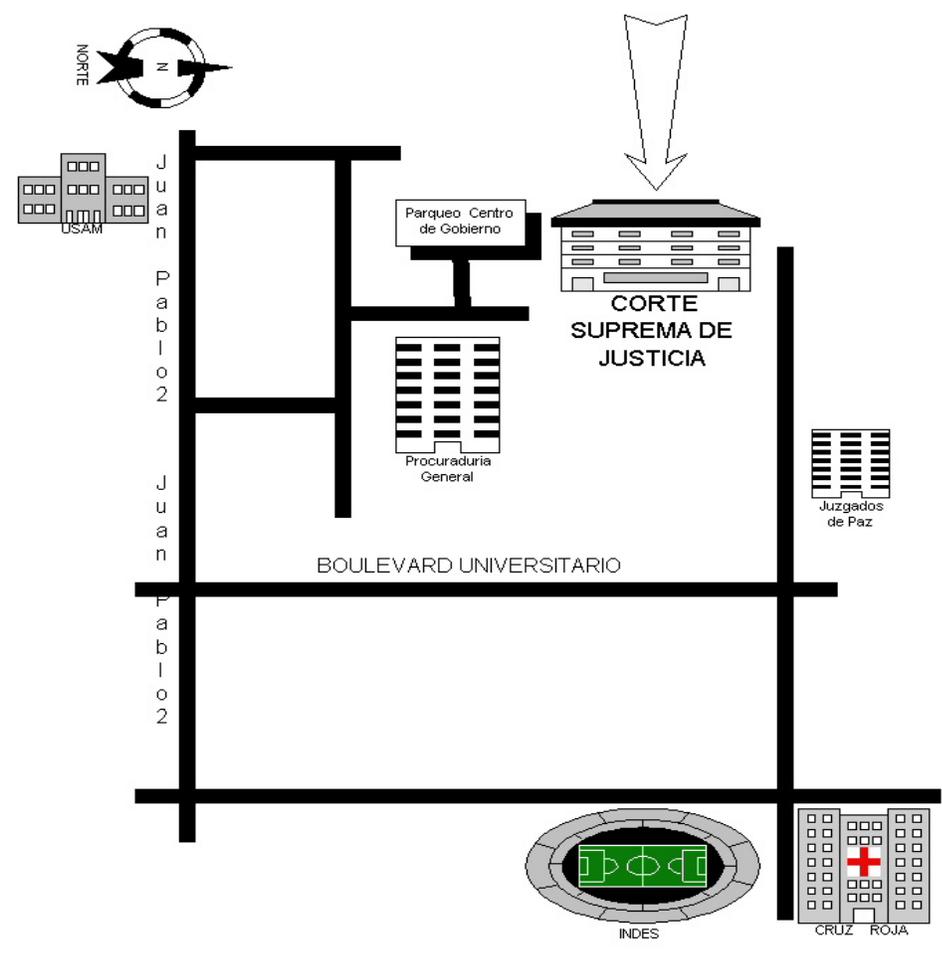
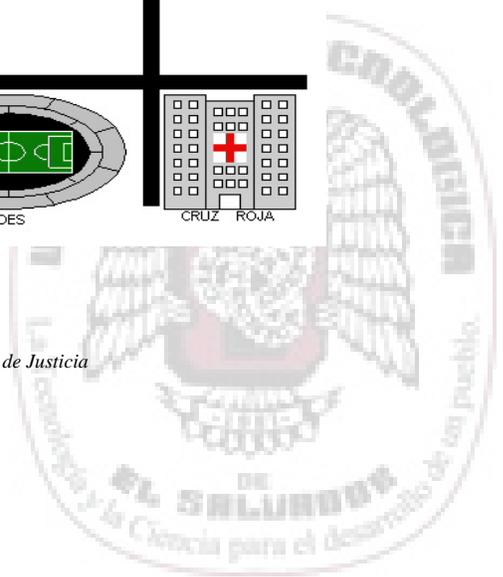


Figura No. 1 Edificio Corte Suprema de Justicia



En el Centro de Documentación Judicial, final 19 calle poniente, # 135, San Salvador.

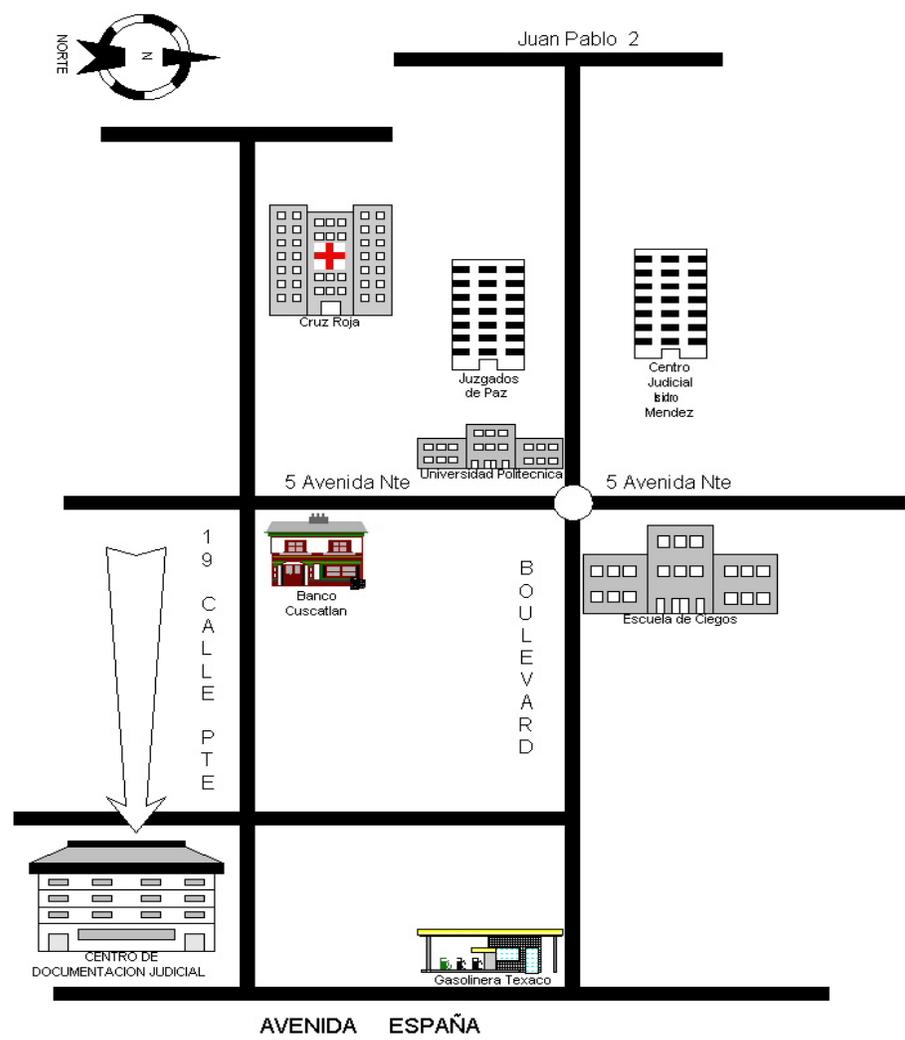


Figura No. 2 Centro de Documentación Judicial



En la Unidad de Informática, prolongación calle Arce y 43 avenida norte,  
# 132, San Salvador.

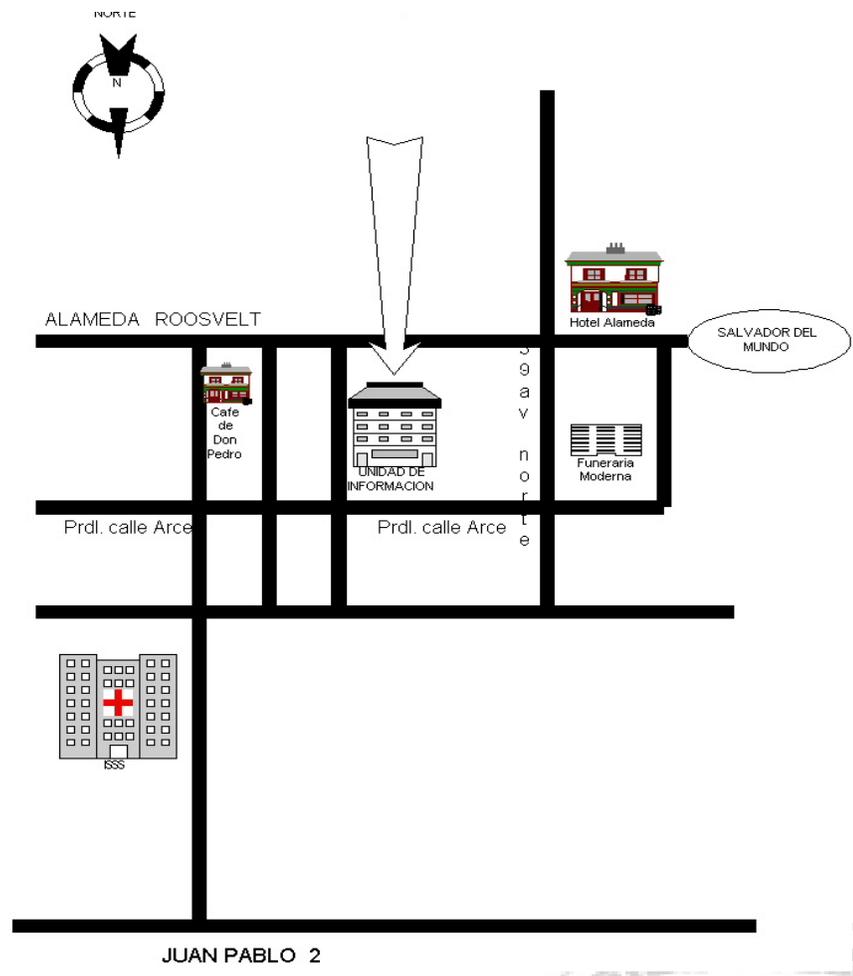


Figura No. 3 Unidad de Informática



Anexo Área de Legislación, prolongación Juan Pablo II, edificio San Antonio, tercer nivel, local # 1, San Salvador.

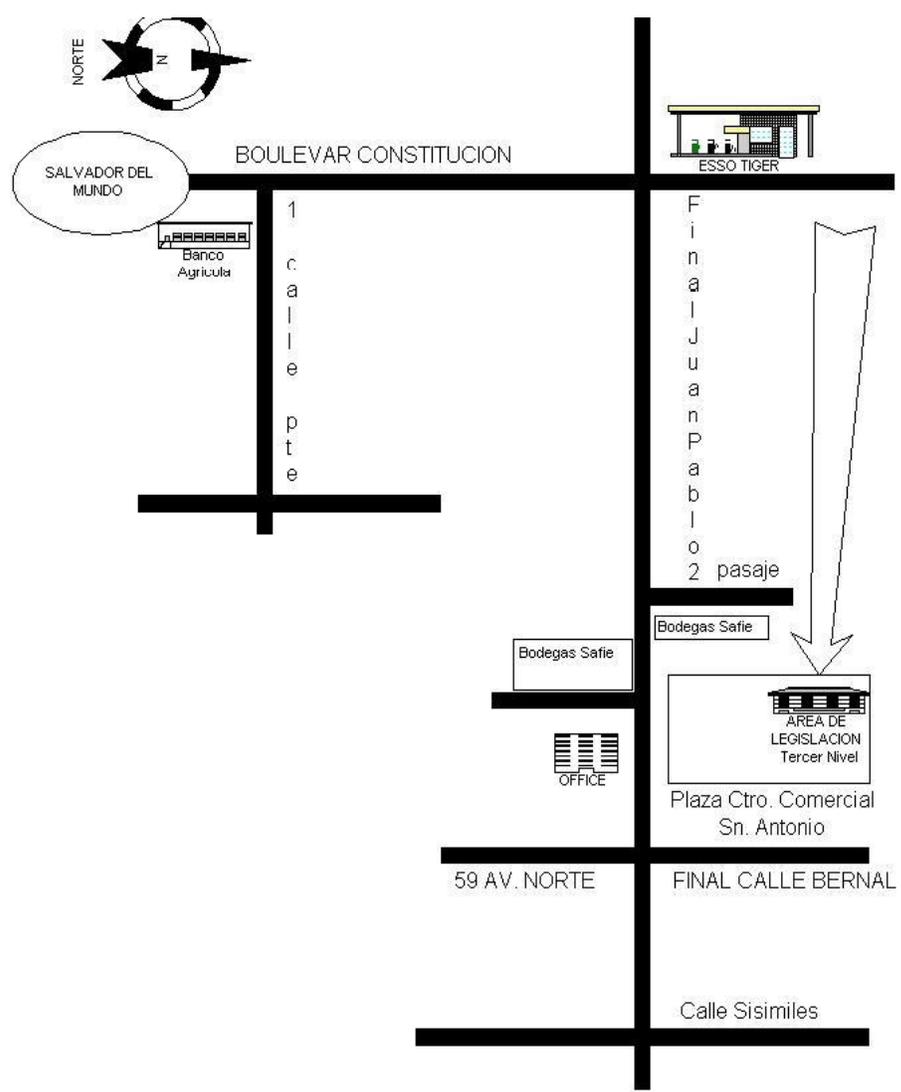
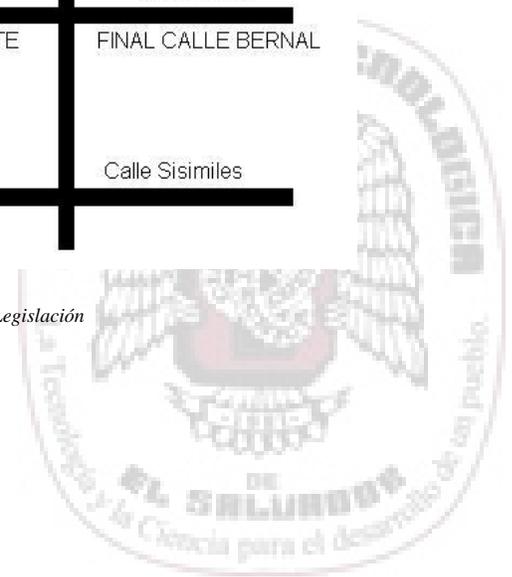


Figura No. 4 Área de Legislación



### 1.3.1.3 Delimitación específica

La investigación de la propuesta de seguridad de transmisión de datos y rendimiento de la red Informática del Órgano Judicial se realizó en cada punto de interconexión antes mencionado, analizando los procesos técnicos, manejo de paquetes, evaluación del entorno de trabajo y la red de transmisión de datos, los diferentes equipos de computación desde terminales a Servidores de Archivos, localización de la recepción de información y el despacho de los diferentes paquetes de aplicación por los usuarios que interactúan a diario con cada flujo técnico de Información.

### 1.3.1.4 Delimitación temporal

La investigación sobre la propuesta de Seguridad de Transmisión de Datos y rendimiento de la red informática del Órgano Judicial de El Salvador, se realizó desde febrero 2002 hasta Noviembre 2002.

### 1.3.2 Alcance

- Definir políticas de seguridad en cuanto a: El acceso a la red y sus recursos compartidos, confiabilidad en la transmisión de datos, normativas de acceso sobre el uso de Internet, controlar la obtención de



programas no autorizados, restricciones a páginas web xxx y chat.

- Proponer un diseño de red con tecnología actual, a través de aparatos de interconexión con tecnología de punta.
- Proponer alternativas de solución en cuanto a la distribución y segmentación de la red.

#### **1.4 Enunciado del problema**

¿ De qué manera se puede mejorar el rendimiento de la red Informática y las políticas de seguridad del Órgano Judicial?

#### **1.5 Objetivos de la Investigación**

##### **1.5.1 Objetivo General**

Diseñar una propuesta de Seguridad de Transmisión de Datos y Rendimiento de la red Informática del Órgano Judicial de El Salvador.

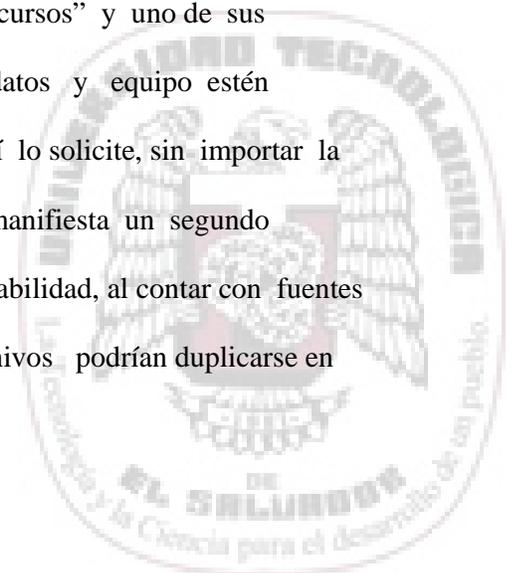


## 1.5.2 Objetivos Específicos

- Identificar la problemática relacionada con la transmisión de datos y rendimiento de la red informática.
- Identificar a través de los expertos de transmisión de datos, técnicas existentes con lo relacionado a la seguridad de transmisión de datos y rendimiento de redes informáticas.
- Proponer alternativas de solución de la seguridad de transmisión de datos y rendimiento de la red.

## 1.6 Marco Teórico

Las redes en general, consisten en “compartir recursos” y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Se manifiesta un segundo objetivo que consiste en proporcionar una alta habilidad, al contar con fuentes alternativas de suministro, es decir, que los archivos podrían duplicarse en



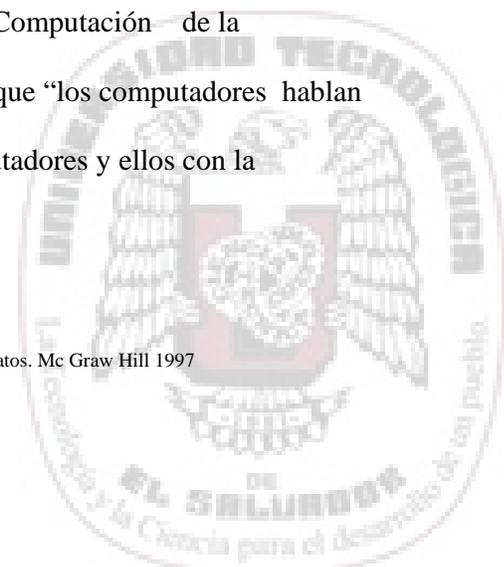
máquinas de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además la presencia de múltiples CPU's que significa que si uno de estos deja de funcionar el siguiente puede ser capaz de encargarse del trabajo, existente de los diferentes procedimientos y ambientes de trabajo en entorno de redes Informáticas, expresan sus ideas como el Ingeniero en comunicaciones y electrónica, **Armando Maldonado Talamantes**, dice que “A medida que avanzamos en este siglo, se ha dado una rápida convergencia en el área de comunicaciones y diferencias entre capturas, transporte, almacenamiento y procesamiento de Información. A medida que crece nuestra habilidad para recolectar, procesar y distribuir información crece todavía con mayor rapidez. La fusión de los ordenadores y las comunicaciones ha tenido una profunda influencia en la forma en que estos sistemas están organizados. El reemplazo de ordenadores de tipo separados por otro que se considera de gran número grande de ordenadores interconectados que efectúen el trabajo en tiempos óptimos, tales que se conocen como redes de ordenadores.”

“Los adelantos de la tecnología permiten que las comunicaciones tengan lugar a través de grandes distancias cada vez con mayor facilidad”, así manifiesta

**Néstor González Sainz**<sup>2</sup>, Ingeniero en Sistemas y Computación de la Universidad Nacional de Colombia. Además dice que “los computadores hablan a los computadores; la gente habla con los computadores y ellos con la

---

<sup>2</sup> González Sainz, Néstor. Comunicaciones Redes de Procesamiento de Datos. Mc Graw Hill 1997

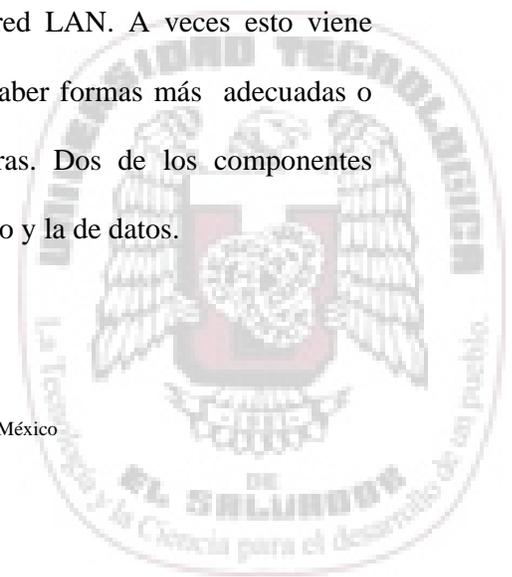


gente. Usando caracteres de control definidos, el protocolo de enlace proporciona una forma ordenada y precisa de asegurar que, entre otras cosas, una terminal remota o un computador se encuentre pronto y que el dispositivo remoto envíe datos cuando se les instruya y se notifique el emisor cuando reciba datos erróneos.” “Se prevé que la reducción en el retraso de la información puede ser el punto individual más importante en los estudios de comunicaciones” como expresa **Sergio Manzanares Basurto**<sup>3</sup>, Ingeniero en Comunicaciones Electrónicas, Escuela Superior de Ingeniería, México; “Debido a que la nueva tecnología de las comunicaciones se incorpora al complejo de la sociedad de Información a la velocidad con que el usuario es capaz en aprender el mantenimiento y utilización de las diferentes tecnologías”.

Esto conduce al concepto de Redes con varios ordenadores en el mismo área de trabajo o edificios, a este tipo de red de tipo LAN (Red de Área Local), en contraste con el extenso de una WAN (Red de Área Extendida), a la que también se conoce como red de gran alcance. Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores. Cuando se llega a cierto punto, deja de ser poco práctico seguir ampliando la red LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son: la red de teléfono y la de datos.

---

<sup>3</sup> Manzanares Basurto, Sergio(1998).Comunicación de Datos, Megabyte. México



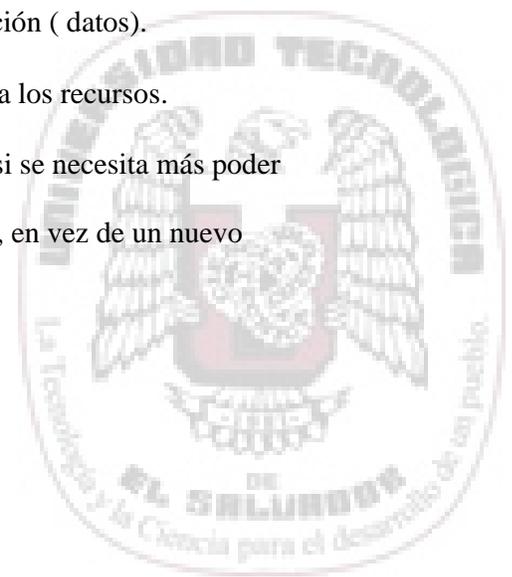
Son enlaces a grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN), casi todos los operadores de redes nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionen basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad como Frame Relay y ATM. Estos servicios de datos a alta velocidad suelen denominarse conexiones de Banda Ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que ha dado en llamarse autopistas de la información. Las grandes empresas disponen de redes corporativas de datos basadas en una serie LAN y Routers. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

A continuación se describen diferentes conceptos teóricos que ayudarán a la comprensión de estos y que permitirán darle solución a la problemática:

### **Estructura de Redes**

Una Red es una conexión interconectada de computadores autónomos que sirven para compartir recursos, especialmente la información (datos).

- Provee la confiabilidad de más de una fuente para los recursos.
- La estabilidad de los recursos computacionales: si se necesita más poder computacional, se puede comprar un cliente mas, en vez de un nuevo Mainframe.
- Comunicación.



Las redes pueden clasificarse mediante diversos aspectos:

### Según su tecnología de transmisión

**Broadcast.** Un solo canal de comunicación compartido por todas las máquinas.

Un paquete mandado por alguna máquina es recibido por todas las otras.

**Punto a Punto.** Muchas conexiones entre pares individuales de máquinas. Los paquetes de A hacia B pueden atravesar máquinas intermedias, entonces se necesita el ruteo para dirigirlos.

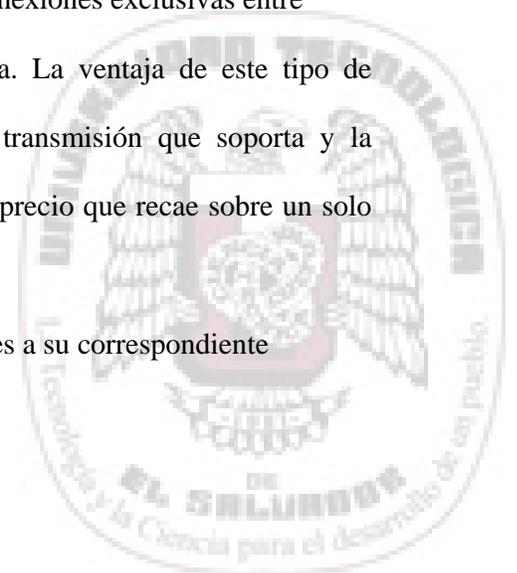
### Según su Utilización

**Redes Dedicadas.** Son aquellas utilizadas para conectar dos o más puntos de una red, en forma exclusiva, por motivos de seguridad, velocidad o ausencia de otro tipo de red.

Pueden estructurarse en redes Punto a Punto o redes Multipunto:

**Red Punto a Punto.** Están constituidas por las conexiones exclusivas entre terminales y computadoras con una línea directa. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión que soporta y la seguridad que presenta. Con el inconveniente del precio que recae sobre un solo usuario.

**Redes multipunto.** Es la unión de varias terminales a su correspondiente



computadora compartiendo una línea única de transmisión. El costo es menor al de una red punto a punto, pero se cuenta con la desventaja de pérdida de seguridad y velocidad.

## **Redes Compartidas**

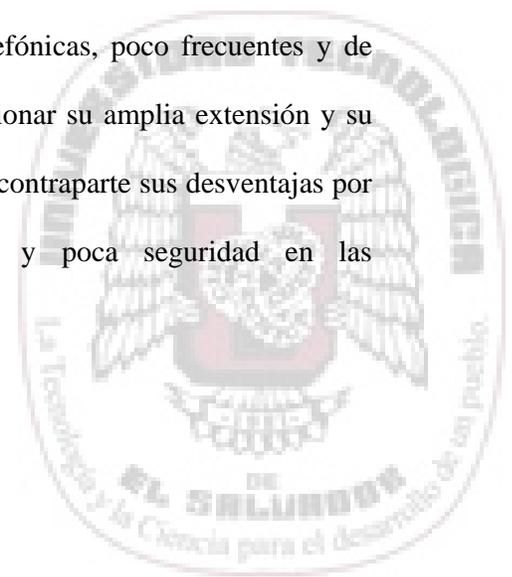
Estas unen un gran número de usuarios compartiendo todas las necesidades de transmisión. Las usuales son las de conmutación de paquetes y conmutación de circuitos.

**Redes de Conmutación de Paquetes.** Son redes en las que existen nodos desconcentración con procesadores que regulan el tráfico de paquetes siendo cada paquete parte de la información que cada usuario desea transmitir.

**Redes de Conmutación de Circuitos.** En estas, en los centros de conmutación se establece un circuito dedicado entre las estaciones que se comunican. Generalmente utilizan multiplexación por división de tiempo.

## **Redes Telefónica Conmutada**

Es la que se utiliza para las comunicaciones telefónicas, poco frecuentes y de poca duración. Entre sus ventajas se puede mencionar su amplia extensión y su precio, pues se paga por tiempo de utilización, en contraparte sus desventajas por baja velocidad de transmisión, baja calidad y poca seguridad en las transmisiones.



## Según su Extensión

Los dos tipos principales de redes son: LAN y WAN.

**LAN:** Una red de área local ( LAN , Local Area Network) es el bloque básico de cualquier red de equipos. Una LAN puede ser muy simple ( dos equipos conectados con un cable) o compleja (cientos de equipos y periféricos conectados dentro de una gran empresa). La características que distingue a un LAN es que esta confinada en un área geográfica limitada.

**WAN:** Por otra parte una red de área extensa (WAN, Wide Area Network), no tiene limitaciones geográficas. Pueden conectar equipos y otros dispositivos situados en extremos opuestos del planeta. Una WAN consta de varias LANS interconectadas (véase figura N° 5). Podemos ver Internet como la WAN suprema.

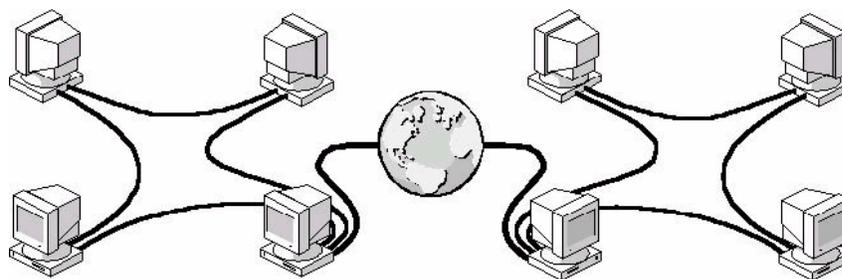


Figura N° 5 Esquema de una Red WAN



## Según su Topología

Así como hay diferentes maneras de instalar el cableado de las LAN también existen formas diferentes de redes conocidas como arquitecturas de redes o topologías. Tomando en cuenta que las formas de red LAN no limitan los medios de transmisión, tanto los cables de par trenzado como los coaxiales y los de fibra óptica, se pueden adaptar a estas diferentes topologías.

**Red en Bus.** Es una configuración en la que todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades de interfaz y derivadores.

Esta topología de red es como una súper carretera de datos que conecta a varias estaciones de trabajo de una LAN; las estaciones de trabajo examinan si un mensaje esta entrando de la súper carretera antes de enviar otros mensajes Todas las estaciones de trabajo comparten este bus por lo que todos los mensajes pasan por otras estaciones de trabajo camino a su destino. Cada estación examina la dirección del mensaje para ver si corresponde a su propia dirección copiando los mensajes dirigidos a ellas en la memoria RAM de su tarjeta interfaz de red y luego procesa la información. (véase figura N° 6).



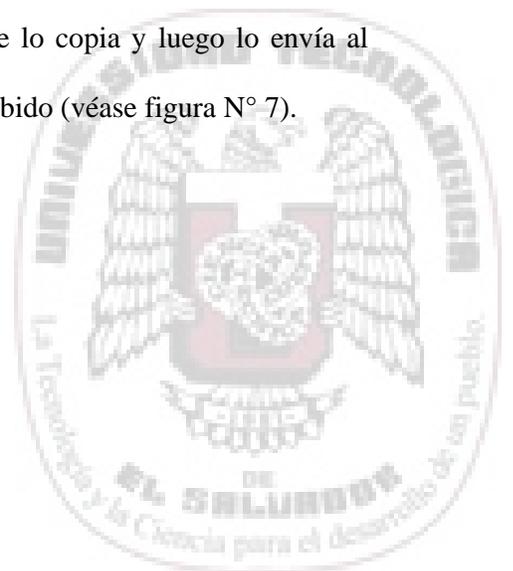


Figura N° 6 Esquema de una red con Topología en Bus

**Red en Árbol.** Esta es una variación de la red en Bus en la cual existen un cable principal y de este se deriva redes conectadas en forma de estrella.

**Red en Anillo.** Una topología de anillo consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. En unas redes de anillo pueden enviar mensajes bidireccional, no obstante solo son capaces de enviar mensajes en una sola dirección cada vez.

La topología de anillo permite verificar si se ha recibido un mensaje ya que cuando un nodo recibe un mensaje dirigido a este lo copia y luego lo envía al emisor con una bandera que indica que ha sido recibido (véase figura N° 7).



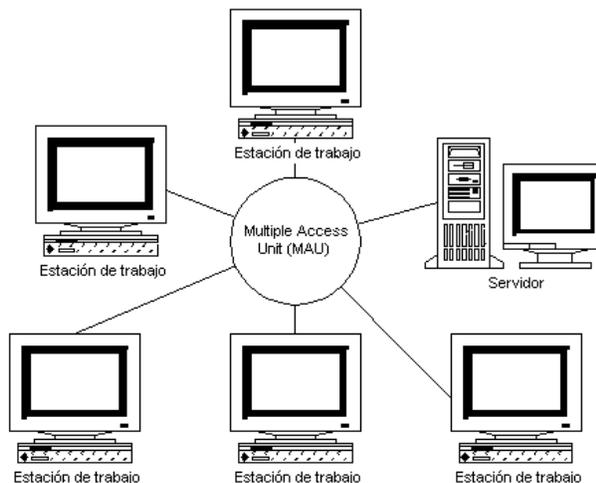


Figura N° 7 Esquema de una red con Topología en Anillo

**Red en Estrella.** Uno de los tipos más antiguos de topología de redes es la de estrella, la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico. De la misma manera en que las llamadas telefónica de un cliente (estación de trabajo) a otro cliente (estación de trabajo) se maneja mediante una estación central de comunicación, todos los mensajes de una topología Lan en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos (véase Fig. N° 8).

Esta arquitectura facilita la adición de nuevas estaciones de trabajo a la LAN para la cual se requiere de un cable que vaya del punto central de conexión (concentrador) a la tarjeta de interfaz de red de cada nueva microcomputadora.



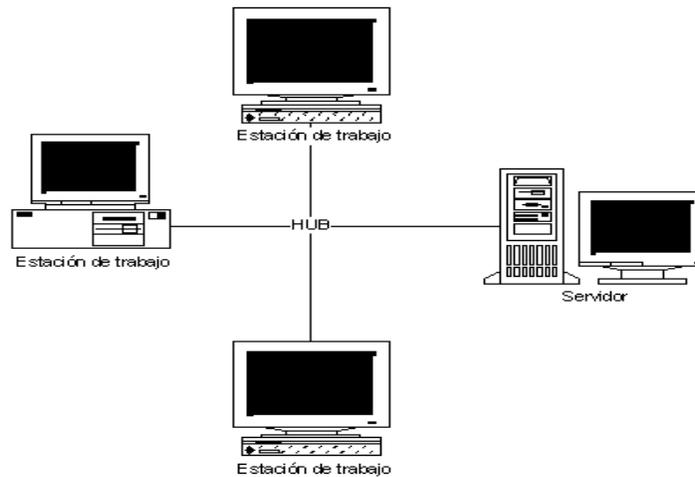


Figura N° 8 Esquema de una red con Topología en Estrella

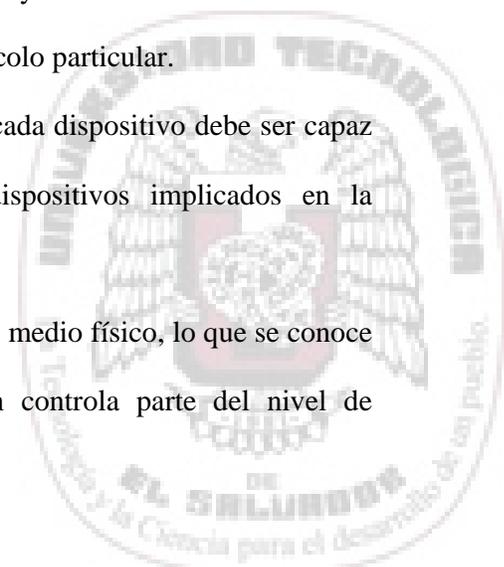
## Protocolos de Redes

Los protocolos de red proporcionan lo que se denominan servicios de enlace. Estos protocolos gestionan información sobre direccionamientos y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como Ethernet y Token Ring.

El protocolo en si es transparente para los usuarios y se introduce en el software de comunicaciones diseñado para utilizar un protocolo particular.

Independientemente del protocolo que se utilice, cada dispositivo debe ser capaz de interpretar los protocolos de los demás dispositivos implicados en la comunicación.

Los protocolos de bajo nivel controlan el acceso al medio físico, lo que se conoce como MAC ( Media Access Control), también controla parte del nivel de



transmisión de datos ya que se encarga de las señales de temporización de la transmisión. Sobre todos los protocolos de bajo nivel MAC se asientan los protocolos de control lógico del enlace LLC (Logical Link Control) definido en el estándar IEEE 802.2.

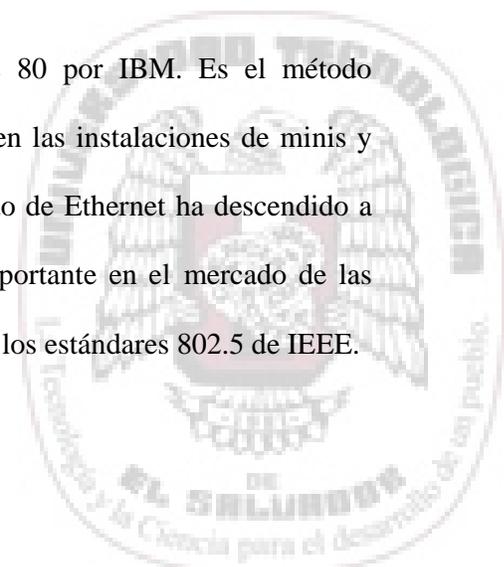
## **ETHERNET**

El protocolo Ethernet fue diseñado originalmente por Digital, Intel Xerox. Esta arquitectura de banda base utiliza una topología en bus, normalmente transmite 10 Mbps y utiliza CSMA/CD (Carrier sense Múltiple Access with Collision detection, Detección de Portadora de Acceso Múltiple y Detección de Colisiones), para regular el segmento de cable principal.

El medio Ethernet es pasivo lo que significa que no requiere una fuente de alimentación por lo que no fallará a no ser que el medio este cortado físicamente o no esté terminado correctamente.

## **TOKEN RING**

Token Ring fue desarrollada a mediados de los 80 por IBM. Es el método preferido de IBM y es el que se suele encontrar en las instalaciones de minis y Mainframes. Aunque la popularidad en el mercado de Ethernet ha descendido a favor de Token Ring sigue jugando un papel importante en el mercado de las redes . Las especificaciones de Token Ring siguen los estándares 802.5 de IEEE.



Token Ring se basa en un esquema de señales (Token Passing), es decir que pasa un señal (Token) a todas las computadoras de la red. La computadora que esta en posición de Token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el Token pasa a la siguiente computadora del anillo. Si la computadora que sigue según la secuencia del anillo, tiene que enviar información, esta acepta el Token y procesa a enviarla , de lo contrario el Token pasa a la siguiente computadora y el proceso continua.

### **Características básicas del Token Ring:**

- Topología de cableado del anillo en estrella
- Método de acceso de paso de testigo
- Cableado de par trenzada apantallado y sin apantallar
- Velocidades de transferencia entre 4 y 16 Mbps
- Transmisión banda
- Especificaciones 802.5

### **FDDI**

La Interfaz de datos distribuidos en Fibra (FDDI, Fiber Distributed Data Interfase.) Es una especificación de red sobre fibra óptica con topología de anillo doble, control de acceso al medio con paso de testigo y una velocidad de transmisión de 100 Mbps que admite 500 equipos en una distancia de hasta



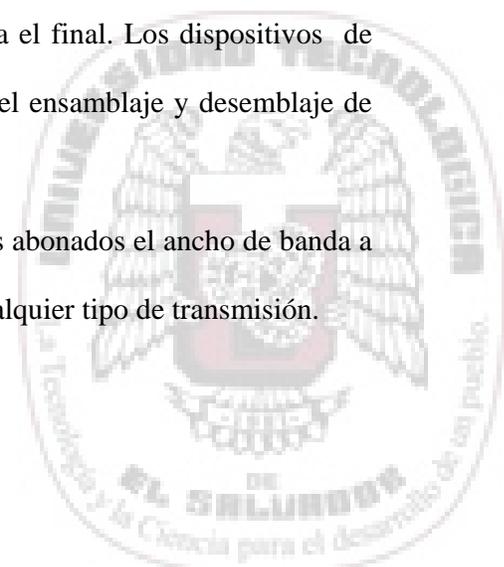
1,000 kilómetros; las LAN que requieren altas velocidades de datos y amplios anchos de banda pueden utilizar conexiones FDDI.

## **FRAME RELAY**

Se trata de una tecnología avanzada de conmutación de paquetes, digital y de longitud variable y que transmite paquetes a alta velocidad. Este protocolo (paso de tramas), puede ser tanto un servicio prestado por una compañía telefónica como una especificación de red privada, permite velocidades de 56kbps hasta 2 Mbps.

Es un sistema punto a punto que utiliza PVC (Circuito Virtual Permanente), para transmitir tramas de longitud variable en el nivel de enlace de datos. Los datos viajan desde una red sobre una línea digital alquilada hasta un conmutador de datos en una red Frame Relay. Pasan a través de la red Frame Relay y llegan a la red de destino. Estas redes se utilizan bastante puesto que realizan de forma más rápida las operaciones básicas de conmutación de paquetes con respecto a otros sistemas de conmutación. Esto se debe a que se utiliza PVC, lo que permite conocer el camino completo desde el origen hasta el final. Los dispositivos de Frame Relay no tienen la necesidad de realizar el ensamblaje y desensamblaje de los paquetes o proporcionar la mejor ruta.

Además, las redes Frame Relay proporcionan a los abonados el ancho de banda a medida que lo necesitan, permitiendo al cliente cualquier tipo de transmisión.



## **ATM**

El Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode) es una implementación avanzada de la conmutación de paquetes que proporciona tasas de transmisión de datos de alta velocidad para enviar paquetes de tamaño fijo a través de LAN y WAN de banda amplia o banda base.

ATM Permite: Voz, Datos, Fax, video en tiempo real, Audio en calidad CD, Imágenes y Transmisión de datos multimegabit.

Es un método de transmisión de celdas de banda amplia que transmite datos en celdas de 53 bytes en lugar de utilizar tramas de longitud variable. Estas celdas están constituidas por 48 bytes de información de ampliación y 5 bytes adicionales que incorpora información de la cabecera ATM.

## **RDSI**

La Red Digital de Servicios Integrados (RDSI o bien ISDN en inglés) es una especificación de conectividad digital entre LAN que permite voz, datos e imágenes. Las redes que quieren utilizar los servicios RDSI deben considerar si utilizar Basic Rate o Primary Rate en función de sus necesidades del rendimiento de los datos. RDSI es el reemplazamiento digital de PSTN y, como tal, se trata de un servicio de llamada.



## **IPX/SPX**

Internet Packet Exchange/Sequence Packet Exchange. Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos, y se utiliza para encaminar mensajes de un nodo a otro. Los programas de aplicación se manipulan sus propias comunicaciones cliente / servidor o de igual a igual de una red Novell puede acceder directamente al IPX o al protocolo SPX del netware.

El IPX no garantiza la entrega del mensaje como lo hace el SPX.

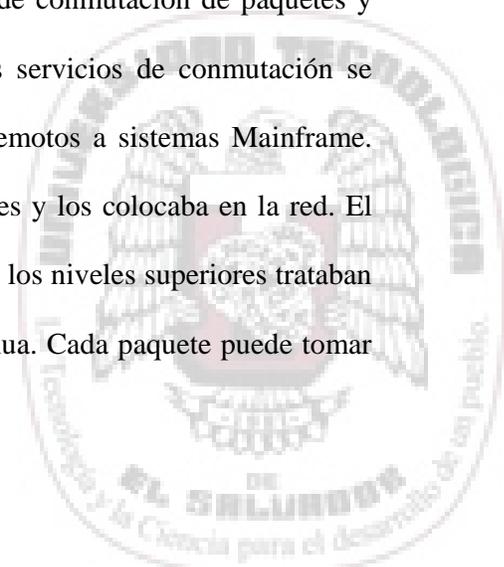
SPX garantiza que un mensaje completo llegue intacto y emplea protocolo netware IPX como mecanismo de distribución.

En otras palabras IPX/SPX es un protocolo que se encarga de direccionar mensajes de un nodo de la red a otro y a la vez asegura, de que este llegue a su destino a salvo.

## **X.25**

Es un conjunto de protocolos WAN para redes de conmutación de paquetes y esta formado por servicios de conmutación. Los servicios de conmutación se crearon originalmente para conectar terminales remotos a sistemas Mainframe.

La red dividía cada terminación en varios paquetes y los colocaba en la red. El camino entre los nodos era un circuito virtual, que los niveles superiores trataban como si se tratasen de una conexión lógica continua. Cada paquete puede tomar



distintos caminos entre el origen y el destino. Una vez que lleguen los paquetes, se reorganizan como los datos del mensaje original.

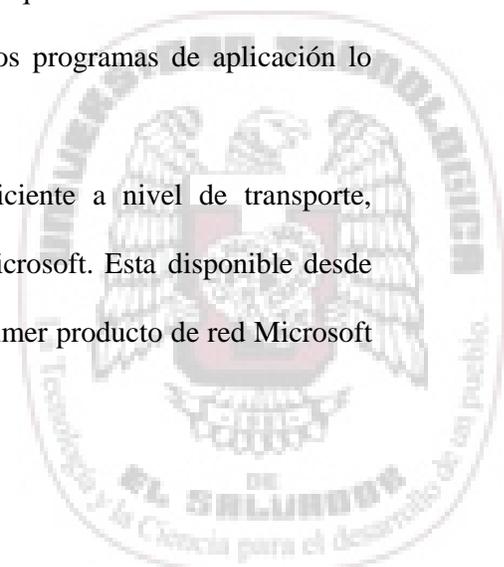
Un paquete típico esta formado por 128 bytes de datos; sin embargo el origen y el destino, una vez establecida la conexión virtual, puede negociar tamaños de paquetes diferentes. El protocolo X.25 puede soportar en el nivel físico un máximo teórico de 4.095 circuitos virtuales concurrentes entre un nodo y una red x.25. la velocidad típica de transmisión es 64 Kbps.

## **NETBEUI**

Es el acrónimo de interfaz de usuario ampliada Netbios. Originalmente Netbios y Netbeui estaban casi unidos y se les consideraba como un protocolo sin embargo varios fabricantes separaron Netbios el protocolo a nivel de sesión de forma que pudieran utilizarse con otros protocolos de transporte encaminables.

Netbios (Sistema Básico E/S de la red), es una interfaz para Lan a nivel de sesión de IBM que actúa como una interfaz de aplicación para la red. Netbios proporciona a un programa las herramientas para que establezca en la red una sesión con otro programa y debido a que muchos programas de aplicación lo soportan, es muy popular.

Netbeui es un protocolo pequeño, rápido y eficiente a nivel de transporte, proporcionado con todos los productos de red Microsoft. Esta disponible desde mediados de los ochenta y se suministro con el primer producto de red Microsoft MS-NET.



## TCP/IP

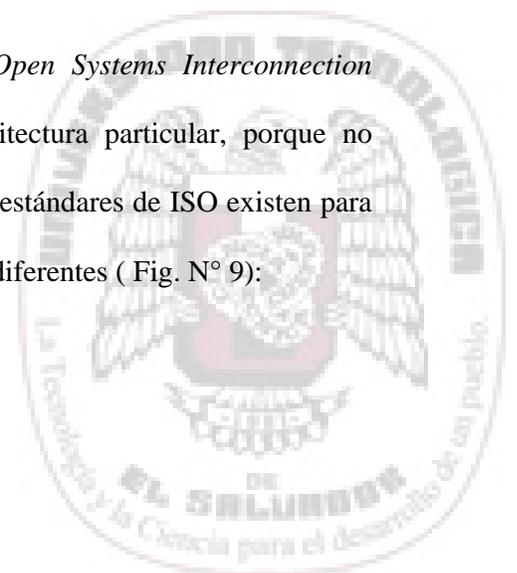
El protocolo de control de transmisión / protocolo Internet (TCP/IP), es un conjunto de protocolo aceptados por la industria que permite la comunicación en un entorno heterogéneo (formado por elemento diferentes). Además TCP/IP proporciona un protocolo de red incaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que esta formadas por redes más pequeñas.

El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos. Y el protocolo IP, funciona en el nivel de red del modelo de referencia OSI, que nos permite encaminar nuestros datos hacia otras máquinas.

## Modelos de referencia de redes

### OSI

OSI es el Sistema de Interconexión Abierto (*Open Systems Interconnection Reference Model*). En realidad no es una arquitectura particular, porque no especifica los detalles de los niveles, sino que los estándares de ISO existen para cada nivel. El modelo OSI consta de siete niveles diferentes ( Fig. N° 9):

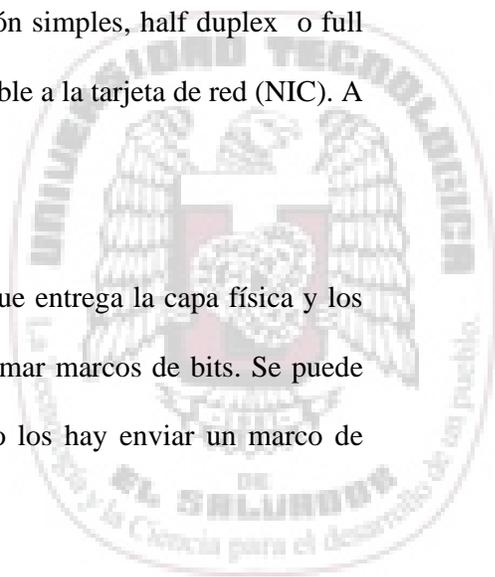


Nivel	Nombre del Nivel
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de Datos
1	Físico

Figura N° 9 El Modelo de Referencia OSI

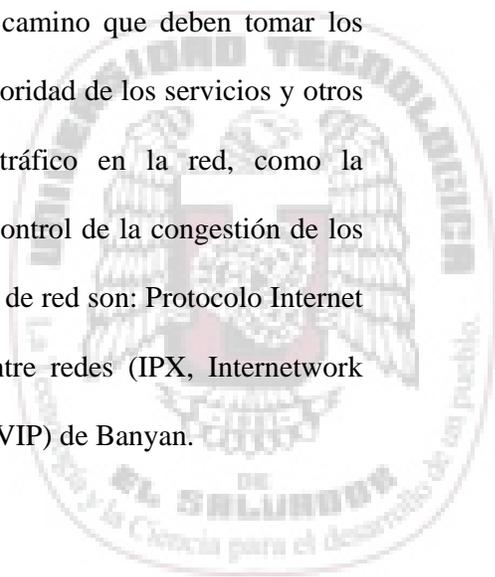
**Nivel físico.** El nivel 1, el más bajo del modelo OSI. Este nivel tiene que ver con el envío de bits en un medio físico de transmisión y se asegura de que si de un lado del medio se envía un 1 del otro lado se reciba ese 1. También tiene que ver con la impedancia, resistencia y otras medidas eléctricas o electrónicas del medio y de qué forma tiene (tamaño, número de patas) en conector del medio y cuáles son los tiempos aprobados para enviar o recibir una señal. También se toma en cuenta si el medio permite la comunicación simples, half duplex o full duplex. Este nivel define la forma de conectar el cable a la tarjeta de red (NIC). A menudo, este nivel es llamado “nivel hardware”.

**Nivel de enlace.** En esta capa se toman los bits que entrega la capa física y los agrupa en algunos cientos o miles de bits para formar marcos de bits. Se puede hacer en este nivel un chequeo de errores y si no los hay enviar un marco de



acuse de recibo (acknowledge). Para detectar los límites de un marco se predefinen secuencias de bits de control. Si un marco se pierde o daña en el medio físico esta capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo Frame se duplique en el destino, dado el caso es obligación de esta capa detectar tal anomalía y corregirla. Por eso se dice que este nivel es el responsable de proporcionar una transferencia libre de errores de las tramas ( Una Trama de datos es una estructura lógica y organizada en la que se pueden colocar los datos) desde un equipo hacia otro a través del nivel físico. Esto permite que el nivel de red prevea una transmisión virtualmente libre de errores sobre la conexión de la red. Normalmente, cuando el nivel de enlace de datos del receptor detecta cualquier problema que pudiera haber ocurrido con la trama durante la transmisión. Las tramas que se han dañado durante la transmisión o las que no han recibido confirmación se volverán a enviar.

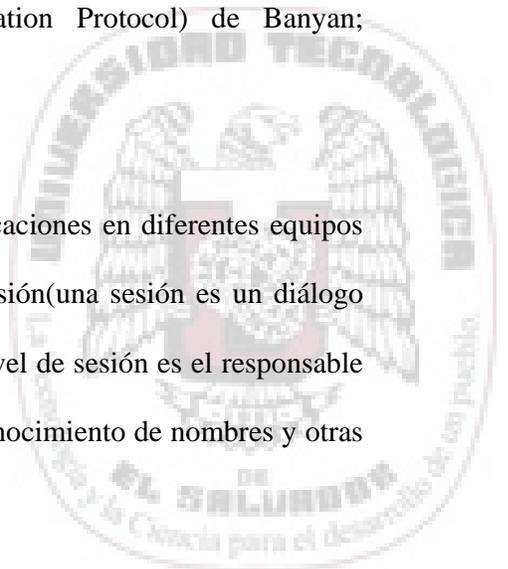
**Nivel de red.** Es el responsable del direccionamiento de los mensajes y la traducción de las direcciones y nombres lógicos en direcciones físicas. Este nivel también determina el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez. Determina el camino que deben tomar los datos basándose en las condiciones de la red, la prioridad de los servicios y otros factores. También gestiona los problemas de tráfico en la red, como la conmutación y encaminamiento de paquetes y el control de la congestión de los datos. Los protocolos genéricos que ocupa el nivel de red son: Protocolo Internet (IP); protocolo x.25; Intercambio de paquetes entre redes (IPX, Internetwork Packet Exchange) y el Protocolo Internet VINES (VIP) de Banyan.



**Nivel de transporte.** Este nivel proporciona un nivel de conexión adicional por debajo del nivel de sesión. El nivel de transporte garantiza que los paquetes se envíen sin errores, en secuencia, y sin pérdidas o duplicados. En el equipo emisor, este nivel vuelve a empaquetar los mensajes, dividiendo los mensajes grandes en varios paquetes y agrupando los paquetes pequeños en uno. Este proceso asegura que los paquetes se transmitan eficientemente a través de la red. En el equipo receptor, el nivel de transporte abre el paquete, reagrupa los mensajes originales y, normalmente, envía una confirmación de que se recibió el mensaje. Si llega un paquete duplicado, este nivel reconocerá el duplicado y lo descartará.

El nivel de transporte proporciona control de flujo y manejo de errores, y participa en la resolución de problemas relacionados con la transmisión y recepción de paquetes. Protocolo de control de transmisión (TCP, Transmisión Control Protocol); Intercambio secuencial de paquetes (SPX, Sequenced Packet Exchange) de Novell; Protocolo de datagramas de usuario (UDP, User Datagram Protocol) de Internet; Protocolo de comunicación entre procesos VINES (VICP, VINES Interprocess Communication Protocol) de Banyan; NetBios/NetBEUI de Microsoft.

**Nivel de sesión.** Este nivel permite que dos aplicaciones en diferentes equipos abran, utilicen y cierren una conexión llamada sesión (una sesión es un diálogo altamente estructurado entre dos estaciones). El nivel de sesión es el responsable de la gestión de este diálogo. Éste realizará el reconocimiento de nombres y otras



funciones, como la seguridad, que se necesita para permitir que dos aplicaciones se comuniquen a través de la red.

El nivel de sesión sincroniza las tareas de usuario colocando puntos de control en el flujo de datos. Los puntos de control dividen los datos en grupos más pequeños para la detección de errores. De esta forma, si la red falla, sólo tienen que retransmitirse los datos posteriores al último punto de control. Este nivel también implementa control de diálogo entre los procesos de comunicación, como la regulación de qué parte transmite, cuándo y durante cuánto tiempo.

**Nivel de presentación.** Este nivel define el formato utilizado para el intercambio de datos entre equipos conectados en red. Se puede ver como el traductor de la red. Cuando los equipos de diferentes sistemas (como IBM, Apple y Sun) necesitan comunicarse se debe realizar una cierta traducción y reordenación de bytes. Dentro del equipo emisor, el nivel de presentación traduce los datos del formato enviado por el nivel de aplicación en un formato intermedio, generalmente reconocido. En el equipo receptor, este nivel traduce el formato intermedio en un formato que pueda ser útil para el nivel de aplicación de ese equipo. El nivel de presentación es el responsable de la conversión de protocolos, la traducción de los datos, la encriptación de los comandos básicos. El nivel de presentación también gestiona la comprensión de datos para reducir el número de bits que se necesitan transmitir.

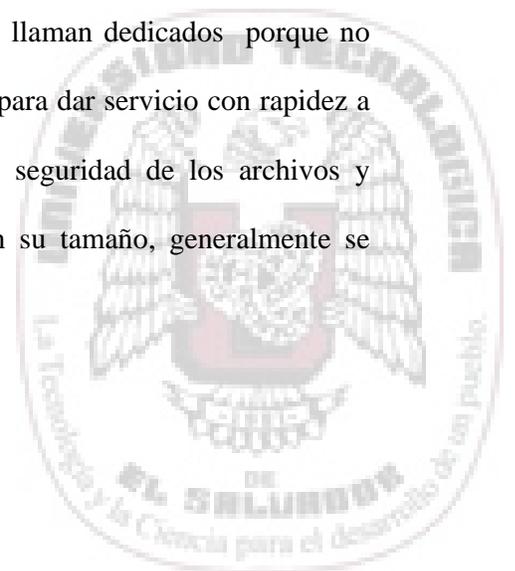
**Nivel de aplicación.** Este nivel es el más alto del modelo OSI. Se relaciona con los servicios que soportan directamente las aplicaciones de usuario, como



software para transferencia de archivos, acceso a base de datos y correo electrónico. El nivel de aplicación sirve como una ventana a través de la cual los procesos de las aplicaciones pueden acceder a los servicios de la red. En el envío de un mensaje a través de la red entra al modelo OSI por este punto y sale por el nivel de aplicación del modelo OSI del equipo receptor. Los protocolos del nivel de aplicación pueden ser programas en sí mismos como el Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol) o pueden ser utilizados por otros programas, como el Protocolo de Transferencia de Correo Simple (SMTP, Simple Mail Transfer Protocol), utilizado por la mayoría de los programas de correo electrónico, para redirigir datos a la red. Los niveles inferiores soportan las tareas que se realizan en el nivel de aplicación. Estas tareas incluyen el acceso general a la red, el control de flujo y la recuperación de errores.

## **Servidores**

Un Servidor es un equipo que proporciona recursos compartidos a los usuarios de la red. Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación. Los servidores se llaman dedicados porque no son a su vez clientes, y porque están optimizados para dar servicio con rapidez a peticiones de clientes de la red, y garantizar la seguridad de los archivos y directorios. A medida que las redes incrementan su tamaño, generalmente se necesita más de un servidor.

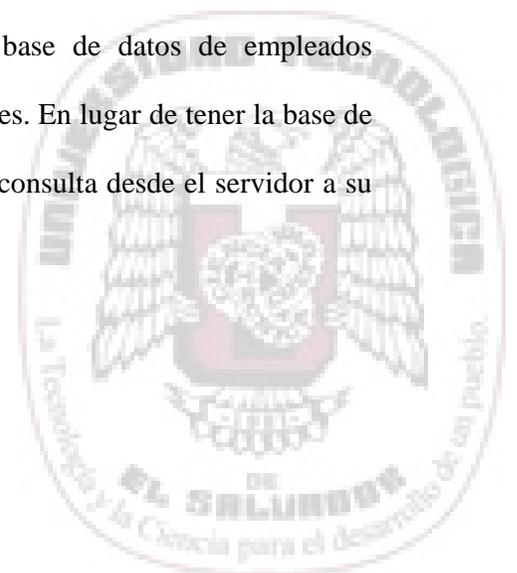


## **Servidor de Archivos e Impresión**

Los Servidores de Archivos e Impresión gestionan el acceso de los usuarios y el uso de recursos de archivos e impresión. Por ejemplo, al ejecutar una aplicación de tratamiento de textos, la aplicación de tratamiento de textos se ejecuta en su equipo. El documento de tratamientos de textos almacenado en el Servidor de archivos e impresión se carga en la memoria de su equipo, de forma que pueda editarlo o modificarlo de forma local. Es decir, este tipo de servidores se utiliza para el almacenamiento de archivos y datos. Los datos o el archivo son descargados al equipo que hace la petición.

## **Servidor de aplicaciones**

Los servidores de aplicaciones constituyen el lado servidor de las aplicaciones cliente / servidor, así como los datos, disponibles para los clientes. Por ejemplo, los servidores almacenan grandes cantidades de datos organizados para que resulte fácil su recuperación. La base de datos permanece en el servidor y sólo se envían los resultados de la petición al equipo que realiza la misma. Una aplicación cliente que se ejecuta de forma local accede a los datos del servidor de aplicaciones. Por ejemplo, podría consultar la base de datos de empleados buscando los empleados que han nacido en “x” mes. En lugar de tener la base de datos completa, sólo se pasará el resultado de la consulta desde el servidor a su equipo local.



## **Servidor de Correo**

Los servidores de correo funcionan como servidores de aplicaciones, en el sentido de que son aplicaciones servidor y cliente por separado, con datos descargados de forma selectiva del servidor al cliente.

## **Servidor de Fax**

Los servidores de Fax gestionan el tráfico de fax hacia el exterior y el interior de la red, compartiendo una o más tarjetas módem fax.

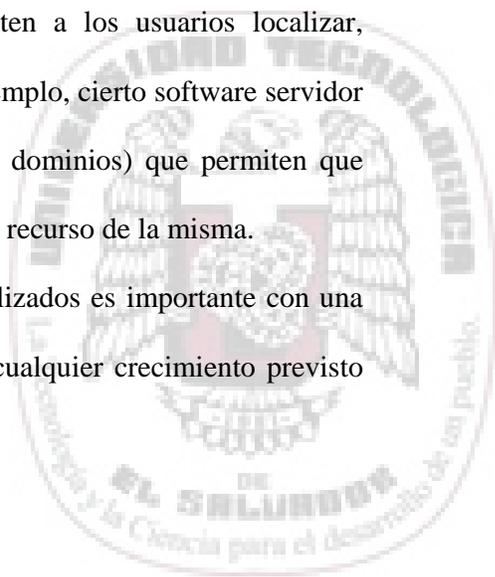
## **Servidor de Comunicaciones**

Los servidores de comunicaciones gestionan el flujo de datos y mensajes de correo electrónico entre las propias redes de los servidores y otras redes, equipos Mainframes, o usuarios remotos que se conectan a los servidores utilizando módems y líneas telefónicas.

## **Servidor de servicios de directorio**

Los servidores de servicios de directorio permiten a los usuarios localizar, almacenar y proteger información en la red. Por ejemplo, cierto software servidor combina los equipos en grupos locales (llamados dominios) que permiten que cualquier usuario de la red tenga acceso a cualquier recurso de la misma.

La planificación para el uso de servidores especializados es importante con una red grande. El planificador debe tener en cuenta cualquier crecimiento previsto



de la red, para que el uso de ésta no se vea perjudicado si es necesario cambiar el papel de un servidor específico.

## **Según su Transmisión de Datos**

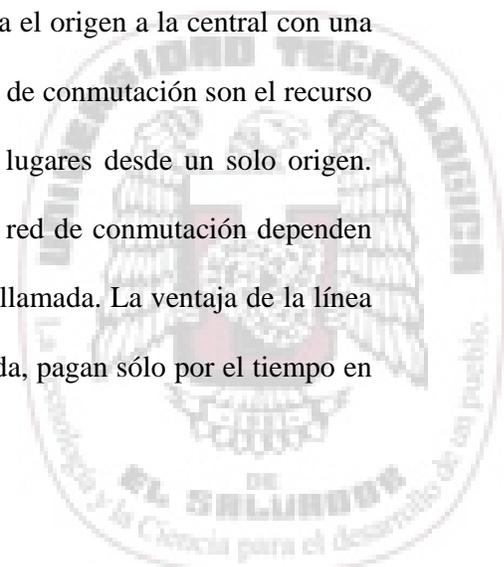
### **Tipos de Líneas de Transmisión**

Lo que determina la dirección de la transmisión de datos, es el tipo de línea que se utiliza, los cuales pueden ser:

#### **Conmutadas**

La red telefónica pública es conocida como una red de conmutación. El nombre proviene de la manera en la que las llamadas siguen la ruta desde el origen hasta el destino, usando líneas telefónicas regulares. Cuando se marca un número telefónico ya sea para conversar o transmisión de datos, se está usando una línea de transmisión, se establece la ruta de ese lugar hasta la oficina de conmutación telefónica más cercana y de ahí al destino.

La oficina central o centro de conmutación conecta el origen a la central con una ruta que unirá al centro con el destino. Los centros de conmutación son el recurso que permiten la interconexión con muchos otros lugares desde un solo origen. Los cargos por transmisión de datos mediante la red de conmutación dependen de la distancia, la hora del día y la duración de la llamada. La ventaja de la línea conmutada es que los usuarios que hacen la llamada, pagan sólo por el tiempo en el que realmente usan la red.



## **Dedicadas**

Las Líneas Dedicadas o Privadas se utilizan cuando la transmisión es frecuente o se desean velocidades mayores de las posibles con las líneas conmutadas. Se dispone de líneas de comunicación durante todo el día, por una cuota mensual fija, además las líneas se dedican exclusivamente al uso del que se suscribe, no forman parte de la red pública de conmutación, se prepara y cablea una ruta fija alrededor de la oficina central de comunicación.

El acondicionamiento de líneas es posible solamente con líneas privadas en renta, que se dediquen a un conjunto particular de instalaciones. La velocidad máxima en las líneas normales de voz es de 9,600 bits/seg. El rango de velocidad de estas líneas va desde los 56 Kbps hasta por encima de los 45 Mbps.

## **Según tipos de Transmisión de Datos**

### **Transmisión Analógica**

Las señales que maneja son de tipo analógico, es decir, que pueden tener cualquier valor de forma continua y dentro de unos límites. La transmisión analógica, utiliza medios diseñados para la transmisión de voz, por lo que se utilizan módems.



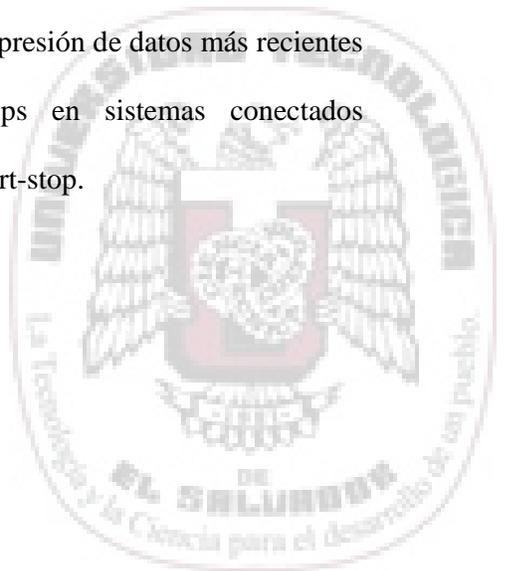
## **Transmisión Digital**

La transmisión digital es aquella que maneja señales discretas por medios diseñados específicamente para este tipo de transmisión, basados en tecnologías de alta y muy alta escala integración LSI y VLSI. Con esta modalidad se consigue una alta calidad y velocidad de transmisión debido a los pulsos altos y bajos (0 y 1) con los que trabaja, enviándose más de dos estados para aumentar la velocidad de transmisión, a lo que se denomina transmisión por niveles múltiples.

## **Transmisión Asíncrona**

En la transmisión asíncrona, los datos se transmiten un carácter a la vez usando bit de inicio-final. La transmisión de los bits de datos comienza y termina con secuencias especiales de inicio-final. Para que el receptor sea capaz de reconocer los datos que van llegando, cada carácter incluye un bit de inicio y uno o dos bits finales, después de los bits de datos.

Este tipo de transmisión se utiliza en las terminales de teclado que no tienen almacenamiento interno. Estos dispositivos transmiten datos en intervalos aleatorios. Las transmisiones asíncronas en líneas telefónicas pueden alcanzar hasta 28,800 bps. No obstante, los métodos de compresión de datos más recientes permiten pasar de 28,800 bps a 115,200 bps en sistemas conectados directamente. También es conocido como modo start-stop.



## **Transmisión Síncrona**

Este tipo de transmisión permite el envío simultáneo de varios caracteres en bloque, los cuales constituyen las unidades de envío, de tal suerte que se logra enviar una mayor cantidad de información en un menor tiempo. Normalmente se insertan caracteres de control al inicio y final de cada bloque, con el fin de confirmar que la información no sufrió trastornos durante la transmisión. La transmisión Síncrona permite mayores velocidades que la asincrónica.

## **Según el modo de Transmisión**

Una línea de comunicación tiene dos sentidos de transmisión que pueden existir simultáneamente o no, por lo que existen los siguientes modos de transmisión:

**Líneas Simplex.** Es el formato más básico de transmisión de datos o de información. Los datos se envían en una única dirección, desde el emisor al receptor. Ejemplos: la radio y la televisión. También se le conoce como Unidireccional.

**Líneas Semiduplex.** Es conocida como transmisión alterna o halfduplex, los datos se envían en ambas direcciones, pero en un momento dado sólo se envían en una dirección. Ejemplos de tecnología que utilizan la comunicación alterna son: las ondas cortas de radio y los walkie-talkies. La World Wide Web es una



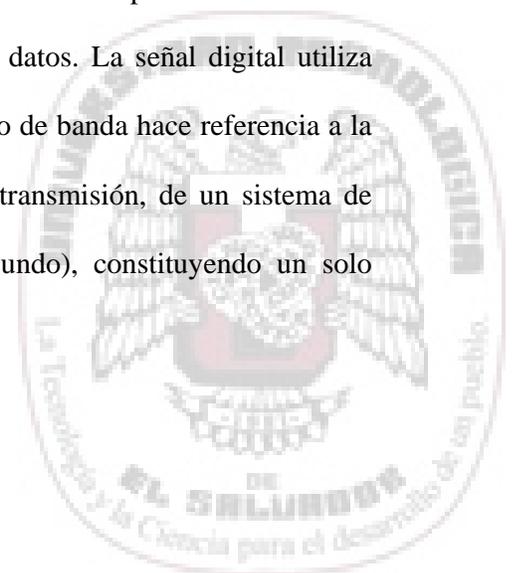
forma de transmisión de datos alterna. Se envía una petición a una página Web y se espera mientras la está devolviendo. La mayoría de las comunicaciones por módem utilizan transmisión de datos alterna.

**Líneas Duplex.** Estas transmiten datos en ambas direcciones y simultáneamente. Este tipo de línea es la más eficiente porque permite a una instalación transmitir y recibir información al mismo tiempo. La mayoría de las líneas privadas son de cuatro cables. Las líneas de cuatro cables son siempre Duplex (Full Duplex). Sin embargo, las líneas de dos cables, pueden ser Semiduplex o Duplex.

## Según Técnicas de Transmisión

### Banda Base

Los sistemas en banda base utilizan señalización digital en un único canal. Las señales fluyen en forma de pulsos discretos de electricidad o luz. Con la transmisión en banda base, se utiliza la capacidad completa del canal de comunicación para transmitir una única señal de datos. La señal digital utiliza todo el ancho de banda del cable (el término ancho de banda hace referencia a la capacidad de transferir datos, o la velocidad de transmisión, de un sistema de comunicaciones digital, medido en bits por segundo), constituyendo un solo canal.



La señal viaja a lo largo del cable de red, y por tanto, gradualmente va disminuyendo su intensidad, y puede llegar a distorsionarse. Si la longitud del cable es demasiado larga, la señal recibida puede no ser reconocida o puede ser tergiversada.

Como medida de protección, los sistemas en banda base a veces utilizan repetidores para recibir las señales y retransmitirlas a su intensidad y definición original. Esto incrementa la longitud útil de un cable.

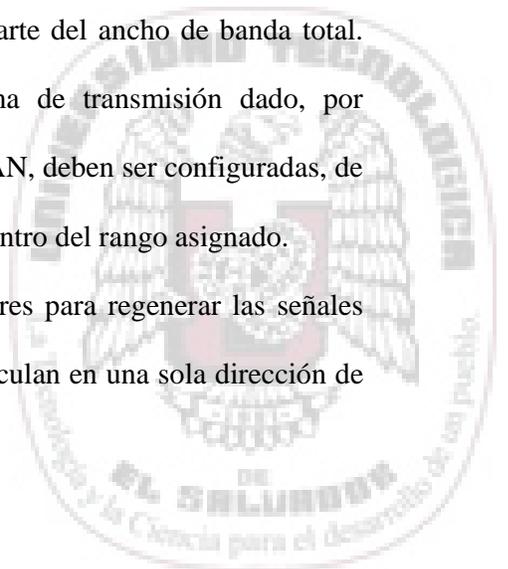
## **Banda Ancha**

Los sistemas de banda ancha, utilizan señalización analógica y un rango de frecuencias. Con la transmisión analógica, las señales son continuas y no discretas. Las señales circulan a través del medio físico en forma de ondas ópticas o electromagnéticas. Con la transmisión en banda ancha, el flujo de la señal es unidireccional.

Si el ancho de banda disponible es suficiente, varios sistemas de transmisión analógica, como la televisión por cable y transmisiones de redes, se pueden mantener simultáneamente en el mismo cable.

A cada sistema de transmisión se le asigna una parte del ancho de banda total. Todos los dispositivos asociados con un sistema de transmisión dado, por ejemplo, todos los equipos que utilicen un cable LAN, deben ser configuradas, de forma que sólo utilicen las frecuencias que están dentro del rango asignado.

Los sistemas de banda ancha utilizan amplificadores para regenerar las señales analógicas y su intensidad original. Las señales circulan en una sola dirección de



forma que debe existir dos caminos para el flujo de datos para que una señal alcance todos los dispositivos. Hay dos formas de realizar esto:

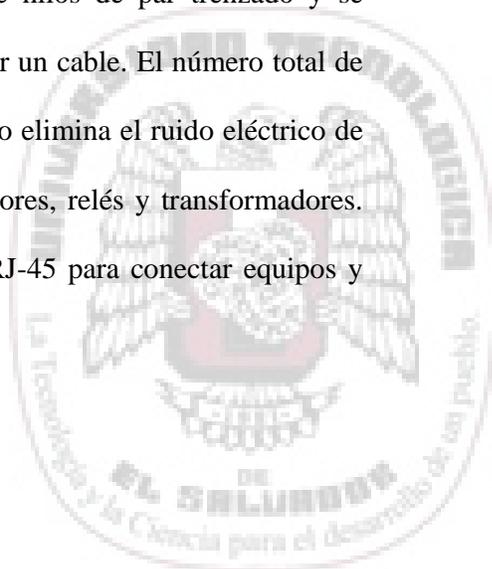
- A través de una configuración de banda ancha con división del medio, el ancho de banda se divide en dos canales, cada uno usando una frecuencia o rango de frecuencias diferentes. Un canal transmite señales y el otro las recibe.
- Configuración en banda ancha con doble cable, a cada dispositivo se unen dos cables. Un cable se utiliza para enviar y el otro para recibir.

## Medios Físicos de Transmisión de Datos

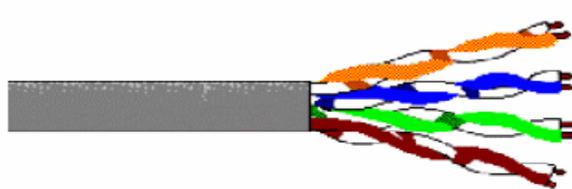
Los Medios de transmisión de datos se clasifican en dos tipos: aéreos y terrestres.

### Medios Físicos Terrestres

**Cable de Par Trenzado.** El cable de par trenzado es el tipo más económico y más común de medio de red el cuál consta de dos hilos de cobre aislados y entrelazados. A menudo se agrupan una serie de hilos de par trenzado y se encierran en un revestimiento protector para formar un cable. El número total de pares que hay en un cable puede variar. El trenzado elimina el ruido eléctrico de los pares adyacentes y de otras fuentes como motores, relés y transformadores. Este tipo de cable utiliza conectores telefónicos RJ-45 para conectar equipos y hubs. Existen dos tipos de cables de par trenzado:



**Par Trenzado sin Apantallar (UTP, Unshielded Twisted Pair).** El UTP , con la especificación 10 Base T, es el tipo más conocido de cable de par trenzado y se está convirtiendo de forma rápida en el cableado LAN más utilizado. El segmento máximo de longitud de cable es de 100 metros, unos 328 pies (véase Fig. N° 10).



*Figura N° 10 Esquema de Cable UTP*

El cable UTP tradicional, consta de dos hilos de cobre aislados. Existen cinco categorías de UTP:

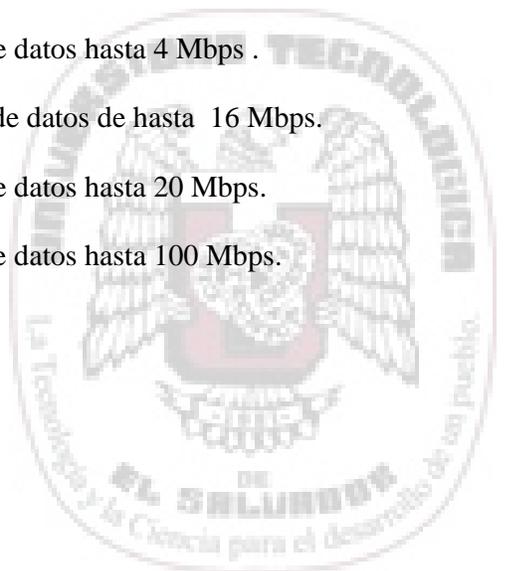
**Categoría 1.** Hace referencia al cable telefónico UTP tradicional que resulta adecuado para transmitir voz, pero no datos.

**Categoría 2.** Permite velocidades de transmisión de datos hasta 4 Mbps .

**Categoría 3.** Alcanza velocidades de transmisión de datos de hasta 16 Mbps.

**Categoría 4.** Permite velocidades de transmisión de datos hasta 20 Mbps.

**Categoría 5.** Permite velocidades de transmisión de datos hasta 100 Mbps.



**Par Trenzado Apantallado (STP, Shielded Twisted Pair).** Este tipo de cable utiliza una envoltura con cobre trenzado, más protectora y de mayor calidad que la usada en el cable UTP. El cable STP utiliza una lámina rodeando cada uno de los pares de hilos. Esto ofrece un excelente apantallamiento en los STP para proteger los datos transmitidos de intermodulaciones exteriores, lo que permite soportar mayores tasas de transmisión que los UTP a distancias mayores.

**Cable Coaxial.** Las razones por las cuales se utiliza este cable es relativamente barato, y ligero, flexible y sencillo de manejar. Un cable coaxial consta de un núcleo de hilo de cobre rodeado por un aislante, un apantallamiento de metal trenzado y una cubierta externa (véase Fig. N° 11).

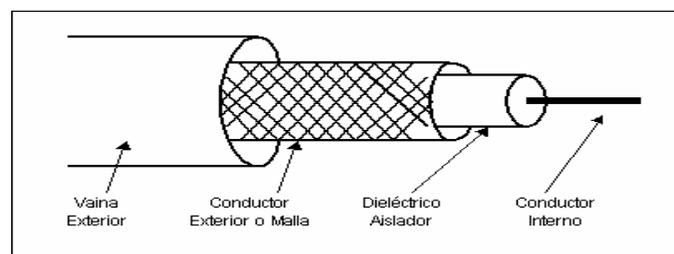
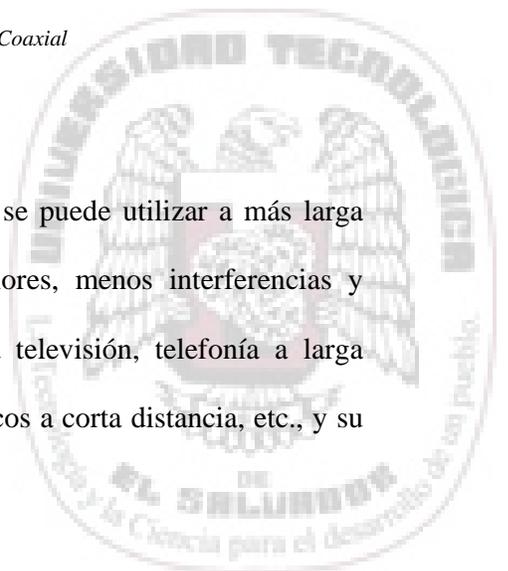


Figura N° 11 Esquema de Cable Coaxial

Este cable es más caro que el par trenzado, pero se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones. Se utiliza para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc., y su



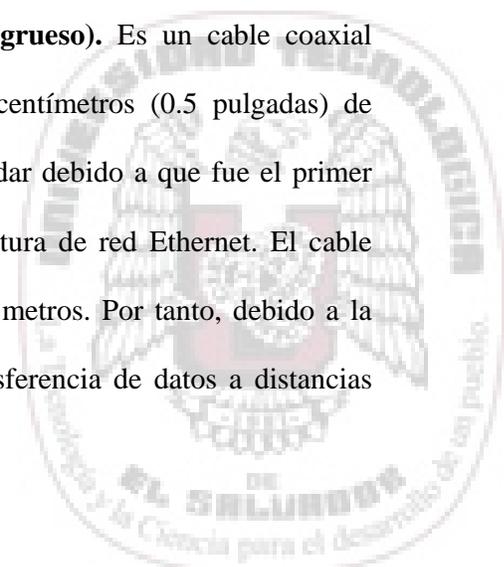
instalación suele ser compleja y requerir obra civil al tener que enterrar los cables.

Sus inconvenientes principales son: atenuación, ruido térmico y ruido de intermodulación, por lo que está siendo sustituido siempre que es posible por la fibra óptica. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada pocos kilómetros.

Hay dos tipos de cable coaxial:

**Cable Coaxial Fino o Thinnet (Ethernet fino).** Es un cable coaxial flexible de unos 0.64 centímetros de grueso (0.25 pulgadas). Este tipo de cable se puede utilizar para la mayoría de los tipos de instalaciones de redes, por su flexibilidad y fácil manejo. El cable coaxial thinnet puede transportar una señal hasta una distancia aproximada de 185 metros (607 pies) antes que la señal comience a sufrir atenuación. Este cable está incluido en un grupo que se denomina RG-58 y tiene una impedancia (es la resistencia, medida en ohmios, a la corriente alterna que circula en un hilo.) de 50 ohm.

**Cable Coaxial Grueso o Thicknet (Ethernet grueso).** Es un cable coaxial relativamente rígido de aproximadamente 1.27 centímetros (0.5 pulgadas) de diámetro. A veces se le denomina Ethernet estándar debido a que fue el primer tipo de cable utilizado con la conocida arquitectura de red Ethernet. El cable Thicknet o Grueso puede llevar una señal a 500 metros. Por tanto, debido a la capacidad de Thicknet para poder soportar transferencia de datos a distancias



mayores, a veces se utiliza como enlace central o backbone para conectar varias redes más pequeñas basadas en thinnet.

**Cable de Fibra Óptica.** Se trata de un medio, muy flexible y muy fino, que conduce energía de naturaleza lumínica (fotones) con muy bajas pérdidas.

Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo (véase Fig. N° 12). Todo este conjunto se recubre para proteger el contenido de aplastamientos, abrasiones, humedad, etc.

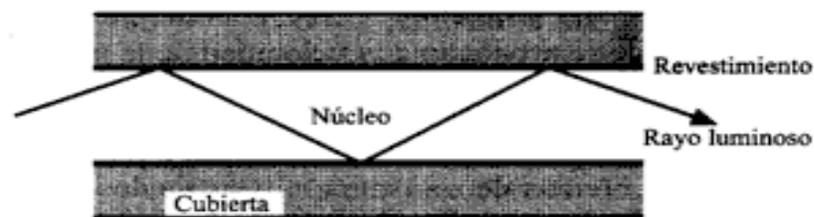
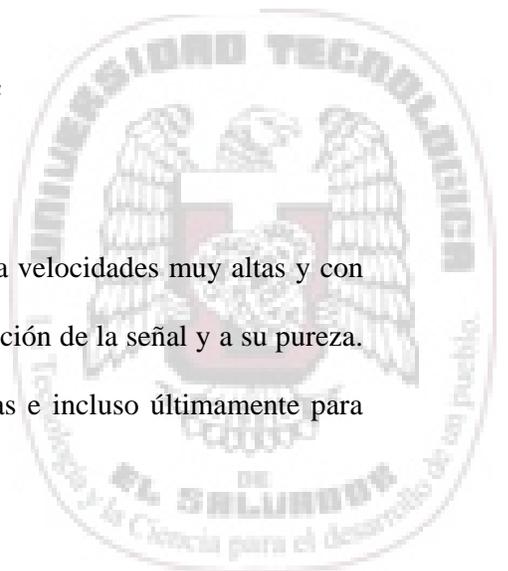


Figura N° 12 Esquema de Fibra óptica

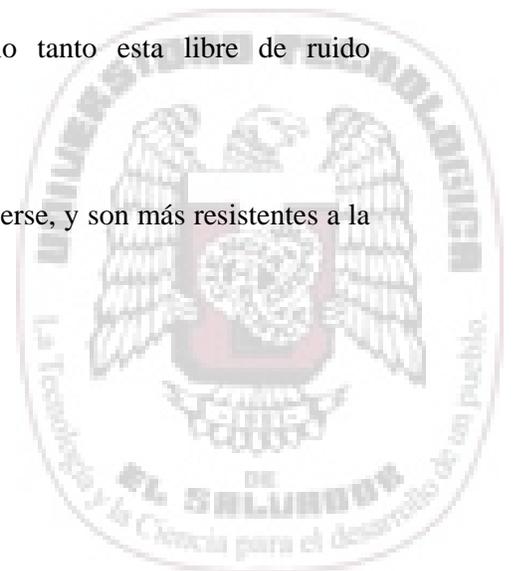
Es un medio muy apropiado para transmitir datos a velocidades muy altas y con grandes capacidades debido a la carencia de atenuación de la señal y a su pureza. También es muy apropiado para largas distancias e incluso últimamente para



LAN. Sus beneficios frente a cables coaxiales y pares trenzados son: Permite mayor ancho de banda, menor tamaño y peso, menor atenuación, total aislamiento electromagnético, mayor separación entre repetidores. Las transmisiones no están sujetas a intermodulaciones eléctricas y son extremadamente rápidas, comúnmente transmiten a unos 100 Mbps, con velocidades demostradas de hasta 1 gigabit por segundo(Gbps). Pueden transportar una señal (el pulso de luz) varios kilómetros.

#### Ventajas de la Fibra Óptica:

- La principal es su ancho de banda, la cual, puede transportar grandes cantidades de información a grandes velocidades.
- Son inmunes al ruido generado eléctricamente y por ello su frecuencia de error es muy baja.
- El tamaño pequeño y bajo peso de los cables de fibra dan a los usuarios, mejores oportunidades para asegurar este medio físico.
- Este tipo de cable no es conductor, por lo tanto esta libre de ruido electromagnético.
- Las fibras no son tan frágiles como podría suponerse, y son más resistentes a la corrosión que el cobre.



Consideraciones sobre el cable de Fibra Óptica:

El cable de Fibra Óptica se utiliza si:

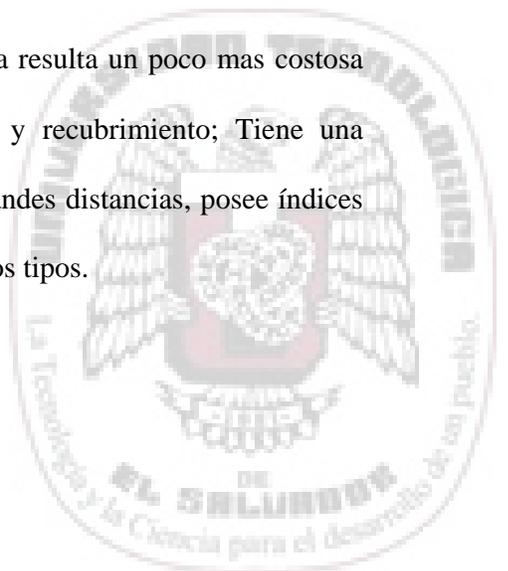
- Necesita transmitir datos a velocidades muy altas y a grandes distancias en un medio muy seguro.

El cable de Fibra Óptica no se utiliza si:

- Tiene un presupuesto limitado.
- No tiene el suficiente conocimiento para instalar y conectar los dispositivos de forma apropiada.

Existen tres tipos de fibras ópticas, los cuales han sido clasificados de acuerdo al modo de preparación que dentro de ellas describen los rayos de luz emitidos:

- Monomodo. En este tipo de fibra óptica, los rayos de luz transmitidos viajan linealmente y la conexión con otros dispositivos es muy difícil. Este tipo de fibra es el modelo más sencillo de fabricar.
- Multimodo de Índice Gradual. Este tipo de fibra resulta un poco más costosa debido al índice de fabricación de su núcleo y recubrimiento; Tiene una capacidad realmente amplia aunque no cubre grandes distancias, posee índices de transmisión muy altos y mayores a los otros dos tipos.



- Multimodo de Salto de Índice o Índice Escalonado. Este tipo de fibra es menos costoso que las demás. No tiene una capacidad tan grande, pero la calidad final es alta. Su Índice de refracción del núcleo es uniforme.

## Medios Físicos de Espacio Aéreo

**Microondas.** Los sistemas de microondas son una buena opción para la interconexión de edificios en sistemas pequeños y con cortas distancias, como un campus o un parque industrial. Es excelente para la comunicación entre dos puntos a la vista como:

- Enlaces de satélite a tierra.
- Entre dos edificios.
- A través de grandes áreas uniformes y abiertas, como extensiones de agua o desiertos.

Un sistema de Microondas consta de:

- Dos transceptores de radio: uno para generar (estación de transmisión) y otro para recibir (estación de recepción) la transmisión.
- Dos antenas orientables apuntadas frente a frente para realizar la comunicación de la transmisión de señales por los transceptores. Estas antenas, a menudo, se



instalan en torres para ofrecer un mayor rango y para evitar todo aquello que pudiera bloquear sus señales.

**Infrarrojos.** Todas las redes sin hilos infrarrojas operan utilizando un rayo de luz infrarroja para llevar los datos entre los dispositivos. Estos sistemas necesitan generar señales muy fuertes, porque las señales de transmisión débiles son susceptibles de interferencias desde fuentes de luz, como ventanas. Muchas de las impresoras altas de gama que se venden actualmente están preconfiguradas para aceptar señales infrarrojas.

Hay cuatro tipos de redes infrarrojas:

**Redes de línea de visión.** Como su nombre indica, esta versión de redes de infrarrojos transmite sólo si el transmisor y el receptor tienen una línea de visión despejada entre ellos.

**Redes Infrarrojas de dispersión.** En esta tecnología, las transmisiones emitidas rebotan en paredes y suelo y, finalmente, alcanzan el receptor. Estas son efectivas en un área limitada de unos 30.5 metros (100 pies).

**Redes reflectoras.** Los transeptores ópticos situados cerca de los equipos transmiten a una posición común que redirige las transmisiones al equipo apropiada.

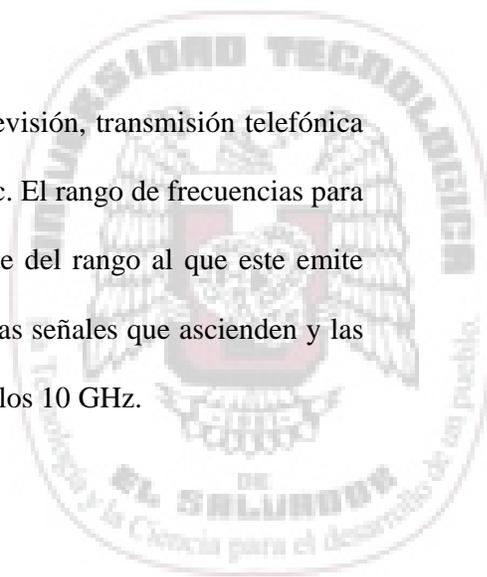


**Telepunto óptico de banda ancha.** Esta LAN sin hilos infrarroja ofrece servicios de banda ancha y es capaz de ofrecer requerimientos multimedia de alta calidad que pueden alcanzar los ofrecidos por una red cableada.

Aunque su velocidad y conveniencia están despertando interés, los infrarrojos tienen dificultad para transmitir a distancias mayores de 30.5 metros. También están supeditados a interferencias de la fuerte luz ambiental que se encuentra en los entornos comerciales.

**Vía Satélite.** El satélite, situado a cientos o miles de kilómetros de la Tierra recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores en tierra, el satélite debe ser geoestacionario. El mayor inconveniente es el elevado coste de situar un satélite en el espacio y su mantenimiento. Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores (hasta 0,5 segundos entre el tiempo de propagación y el de procesado), ha de tenerse cuidado con el control de errores y de flujo de la señal.

Se suele utilizar este sistema para: Difusión de televisión, transmisión telefónica a larga distancia, constitución de redes privadas, etc. El rango de frecuencias para la recepción del satélite (uplink) debe ser diferente del rango al que este emite (downlink), para que no haya interferencias entre las señales que ascienden y las que descienden, y se utiliza unas bandas en torno a los 10 GHz.



## **Dispositivos de Transmisión de Datos**

### **La Tarjeta de Red (NIC)**

Las Tarjetas de Red (NIC, Network Interface Cards) son tarjetas de expansión que proporcionan la interfaz entre el equipo y el cable de la red. La función de la NIC es preparar, enviar, recibir y (en una topología de anillo) retransmitir los datos por la red. Contiene el hardware y la programación firmware (rutinas software almacenadas en la memoria de sólo lectura, ROM) que implementa las funciones de Control de acceso al medio y Control de enlace lógico en el nivel de enlace de datos del modelo OSI. Las tarjetas más modernas utilizan la tecnología Plug and Play (PnP).

### **Concentradores (HUB)**

Es un dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. También se dice que es un componente de conexión que proporciona una conexión común entre equipos en una red configurada en estrella.

Un concentrador permite a cada nodo comunicarse con todos los otros nodos conectados. Se pueden conectar dos o más concentradores, lo que permite extender la red fácil y económicamente (véase Fig. N° 13).

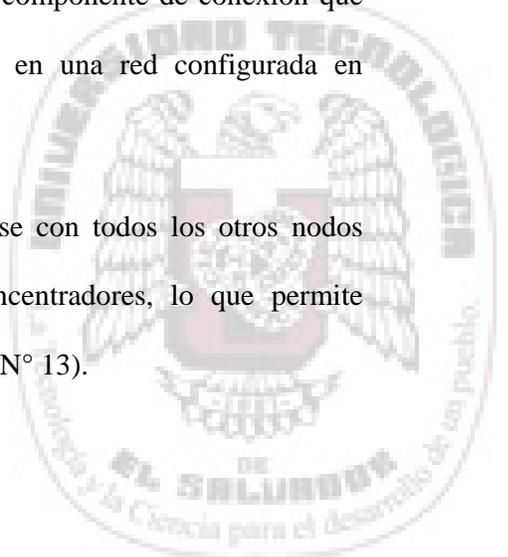


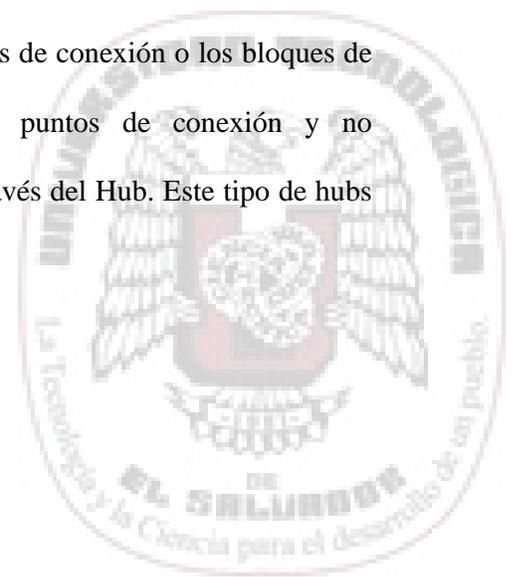


Figura N° 13 Esquema de un HUB

Los concentradores o Hubs pueden ser activos (repiten las señales que les llegan) o pasivos ( sólo reparten las señales que les llegan, no las repiten).

**Hubs Activos.** La mayoría de los Hubs son activos; es decir, regeneran y retransmiten las señales del mismo modo que un repetidor. Como generalmente tienen de ocho a doce puertos para conexión de equipos de la red, a menudo se les llama repetidores multipuerto. Además requieren corriente eléctrica para su funcionamiento.

**Hubs Pasivos.** Ejemplos de estos están los paneles de conexión o los bloques de conexión (punch-down blocks). Actúan como puntos de conexión y no amplifican o regeneran la señal; la señal pasa a través del Hub. Este tipo de hubs no necesita corriente eléctrica para funcionar.



## Repetidores

Son equipos que funcionan en el nivel físico del modelo de referencia OSI para regenerar las señales de la red y reenviarla a otros segmentos. El repetidor toma una señal débil de un segmento, la regenera y la pasa al siguiente segmento. Para pasar los datos de un segmento a otro a través del repetidor, deben ser idénticos en cada segmento los paquetes y los protocolos LLC (Control Lógico de enlace).

Los repetidores no traducen o filtran señales. Constituyen la forma más barata de extender una red. Cuando se hace necesario extender la red más allá de su distancia o limitaciones relativas a los nodos, la posibilidad de utilizar un repetidor para enlazar segmentos es la mejor configuración, siempre y cuando los segmentos no generen mucho tráfico ni limiten los costes.

Los Repetidores se utilizan para conectar dos segmentos de medios similares o distintos y para regenerar la señal, de forma que se incremente la distancia transmitida. Y no deberían utilizarse si el tráfico de red es alto, si los segmentos están utilizando diferentes métodos de acceso o es necesario realizar el filtrado.

## Bridge

Estos equipos se utilizan asimismo para interconectar dos segmentos, de forma que se permita extender la longitud o número de nodos en la red, para reducir el



tráfico segmentando la red o para conectar redes distintas. Estos tienen todas las características de los repetidores.

Se pueden utilizar para:

- Extender la longitud de un segmento.
- Proporcionar un incremento en el número de equipos de la red.
- Reducir los cuellos de botella de tráfico resultantes de un número de equipos de la red.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo que la red sea más eficiente.
- Enlazar medios físicos diferentes como par trenzado y Ethernet coaxial.

Los Bridges o puentes trabajan a nivel de enlace de datos del modelo de referencia OSI, con direcciones físicas, por lo que filtra tráfico de un segmento a otro. Todos los protocolos se pasan a través de los Bridges, de forma que aparecen en los equipos personales para determinar los protocolos que pueden reconocer. Los Bridges trabajan en el nivel MAC (Control de acceso al medio).

## **Routers**

Se utilizan para conectar dos redes, para limitar el tráfico innecesario y para separar las redes desde un punto de vista administrativo. Estos equipos trabajan a nivel de red del modelo de referencia OSI, es decir que pueden filtrar

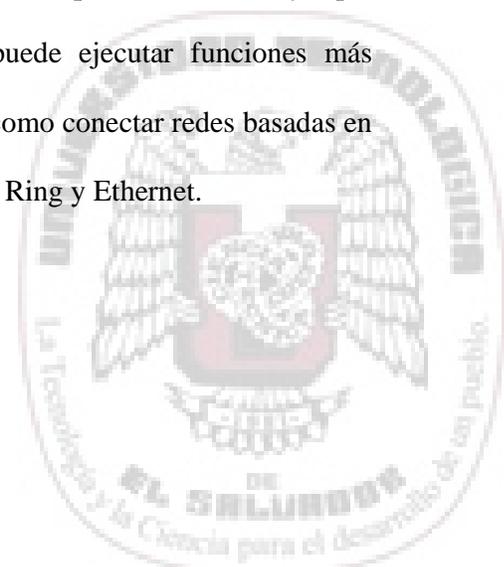


protocolos y direcciones a la vez. Los equipos de la red saben que existe un Router y le envían los paquetes directamente a él cuando se trate de equipos en otro segmento.

Además los Routers o Ruteadores pueden interconectar redes distintas entre sí; eligen el mejor camino para enviar la información, balancean tráfico entre líneas, etc.

El Router trabaja con tablas de encaminamiento o enrutado con la información que generan los protocolos, deciden si hay que enviar un paquete o no, deciden cual es la mejor ruta para enviar un paquete o no, deciden cual es la mejor ruta para enviar la información de un equipo a otro, pueden contener filtros a distintos niveles, etc.

Poseen una entrada con múltiples conexiones a segmentos remotos, garantizan la fiabilidad de los datos y permiten un mayor control del tráfico de la red. Su método de funcionamiento es el encapsulado de paquetes. Los Routers requieren por lo general que cada red tenga el mismo Sistema Operativo de Red, ya que con un Sistema Operativo común, el Router puede ejecutar funciones más avanzadas que las que podría permitir un Bridge, como conectar redes basadas en topologías completamente diferentes, como Token Ring y Ethernet.



## Gateway

También llamados traductores de protocolos, son equipos que se encargan, como su nombre indica, a servir de intermediario entre los distintos protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí.

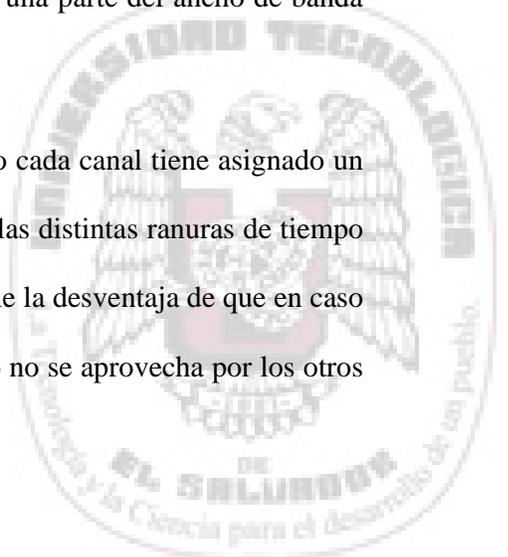
Así que los Gateways son los que realizan la conversión de datos y de protocolo. Además están limitados de diversas formas; son de tarea específica, caros y pueden resultar lentos.

## Multiplexores

Es un dispositivo utilizado para dividir una transmisión en dos o más canales. Puede ser un programa guardado en un equipo. También sirve para conectar un número de líneas de comunicación a un equipo.

**Multiplexor por División de Frecuencia.** Divide el ancho de banda de una línea entre varios canales, donde cada canal ocupa una parte del ancho de banda de frecuencia total.

**Multiplexor por División de Tiempo.** En este tipo cada canal tiene asignado un período o ranura de tiempo en el canal principal y las distintas ranuras de tiempo están repartidas por igual en todos los canales. Tiene la desventaja de que en caso de que un canal no sea usado, esa ranura de tiempo no se aprovecha por los otros canales, enviándose en vez de datos bits de relleno.



**Multiplexor por División de Tiempo Estadísticos.** No le ofrece ranuras de tiempo a los canales inactivos y además podemos asignar prioridades a los canales.

## Switch

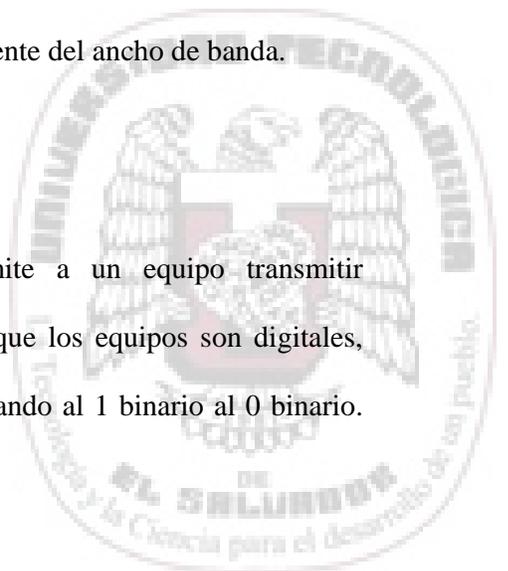
Un Switch es un dispositivo de Red situado en el nivel 2 ó Enlace de Datos del modelo de referencia OSI. El Switch se denomina puente multipuerto. Son capaces de tomar decisiones basándose en las direcciones MAC, así hacen que la LAN sea mucho más eficiente. Los Switch hacen esto “conmutando” datos solo desde el puerto al cual está conectado el host correspondiente.

El propósito del Switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el Switch como un elemento que puede combinar la conectividad de un Hub con la regulación de tráfico de un puente en cada puerto. El Switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total.

Básicamente un Switch es un administrador inteligente del ancho de banda.

## Módem

Es un dispositivo de comunicación que permite a un equipo transmitir información por una línea telefónica. Debido a que los equipos son digitales, funciona con señales eléctricas discretas representando al 1 binario al 0 binario.



Un teléfono es analógico y lleva una señal que puede tener varias variaciones. Los Módems son necesarios para convertir señales digitales a analógicas y, luego, deshacer el cambio. Al transmitir, los módems imponen (modulan) una señal digital de un equipo en una frecuencia portadora continua en la línea telefónica. Al recibir, los módems extraen (demodulan) la información de la portadora y la transfieren de forma digital al equipo.

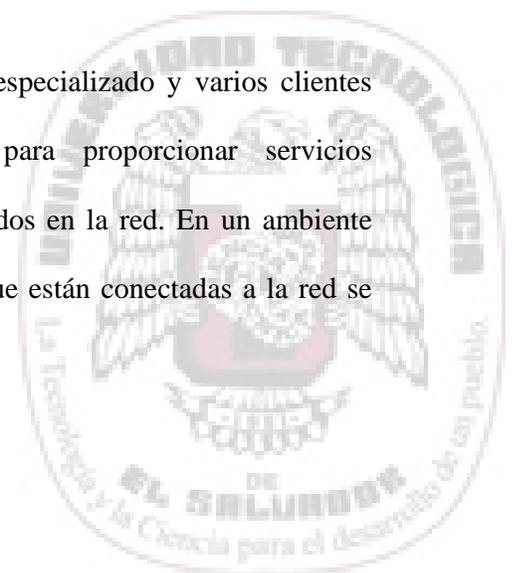
### **Cliente / Servidor**

Se refiere a un modelo en el que el procesamiento de datos es compartido entre el equipo cliente y el equipo servidor, más potente. El enfoque Cliente / Servidor puede beneficiar a cualquier organización en la que muchas personas necesiten acceder continuamente a grandes cantidades de datos.

La Red Cliente / Servidor es la forma más eficaz de ofrecer:

- Acceso y gestión de bases de datos para aplicaciones tales como hojas de cálculo, contabilidad, comunicaciones y gestión de documentos.
- Gestión de la red.
- Almacenamiento centralizado de archivos.

La red se compone de uno o varios servidores especializado y varios clientes diferentes. Los servidores están diseñados para proporcionar servicios centralizados y los clientes son los diferentes nodos en la red. En un ambiente cliente / servidor, las computadoras personales que están conectadas a la red se llaman “clientes, nodos o estaciones de trabajo”.



## **Sistemas Operativos de Red**

### **Windows NT**

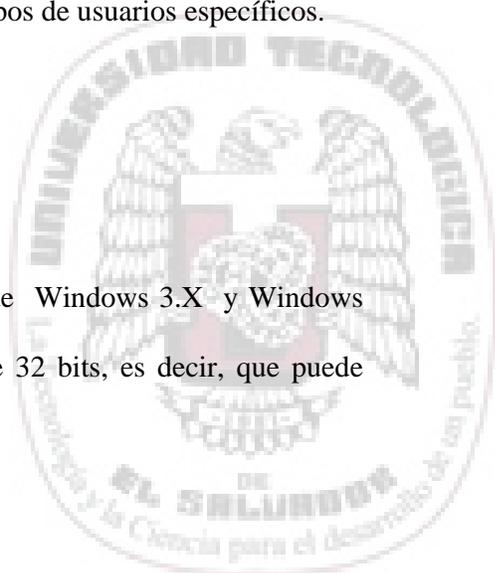
Windows NT es un sistema operativo de 32 bits para computadoras personales y fue creado para ser un sistema operativo de alto rendimiento diseñado principalmente para estaciones de trabajo y servidores de red potentes. Microsoft separó Windows NT en dos productos distintos: Windows NT Workstation y Windows NT Server.

Windows NT Server incorpora las mismas características que tiene Windows NT Workstation, pero también tiene otras capacidades. Windows NT Server funciona como un sistema operativo para servidores de archivo y de impresión, y en otros sistemas que proporcionan servicios para otras computadoras LAN o Internet.

Este sistema operativo incorpora mucha mayor seguridad que los otros sistemas operativos de Microsoft, ya que requiere que un usuario tenga cuenta ya sea en la computadora que está usando o en un servidor en la red. Los recursos en la computadora local, al igual que los recursos en servidores remotos, pueden configurarse para limitar el acceso a usuarios y grupos de usuarios específicos.

### **Windows 95**

El Sistema Operativo Windows 95 es el sucesor de Windows 3.X y Windows para trabajo en grupo y ofrece procesamiento de 32 bits, es decir, que puede



intercambiar información con impresoras, redes y archivos en fragmentos de 32 bits, en lugar de fragmentos de 16 bits como en Windows 3.X y DOS.

También ofrece multitarea preferente de 32 bits, es decir, que si un programa falla, todavía se tiene acceso a todos los demás programas cargados en memoria.

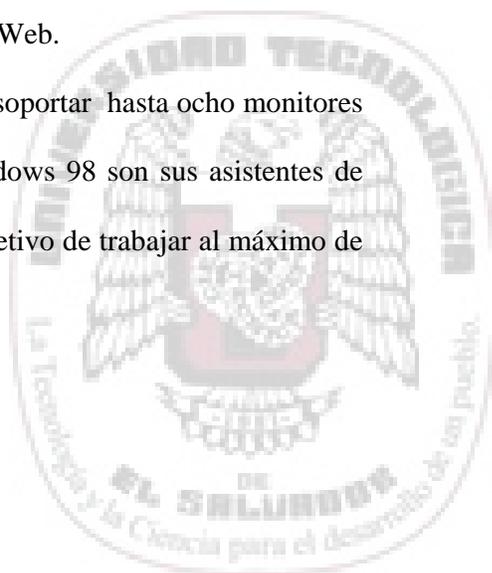
Pero lo mejor de este sistema operativo es su interfaz gráfica, que es una mejora notable sobre Windows 3.X. Otras Ventajas de Windows 95 son : Plug and Play para incorporar hardware nuevo y la compatibilidad con software de redes como IntranetWare y Windows NT Server.

## **Windows 98**

Es la versión mejorada de Windows 95, aunque incorpora e incluye todas sus características, pero agrega varias características nuevas.

Windows 98 incluye la herramienta Active Desktop, el cual proporciona una sola interfaz de usuario para buscar en Internet al igual que en los recursos de la computadora local. También cuenta con soporte para canales de televisión, páginas Web y controles Activos. Este sistema operativo ejecuta la versión 4.0 de Internet Explorer que permite navegar en los sitios Web.

Una característica interesante es la capacidad para soportar hasta ocho monitores a la vez. Pero la ventaja más importante, de Windows 98 son sus asistentes de optimización y de liberación de espacio, con el objetivo de trabajar al máximo de su capacidad.



## Windows 2000

Windows 2000 representa un esfuerzo por unificar lo que hasta ahora eran dos sistemas operativos distintos, Windows 9X y Windows NT. Es la nueva versión de Windows NT 4.0 Workstation y NT Server.

Este sistema operativo ofrece lo mejor de ambos: La solidez y la seguridad de NT, junto a la facilidad de manejo, soporte de hardware y multimedia de Windows 98.

Entre lo mejor de Windows 98 que ofrece la versión 2000, se encuentra la Interface renovada, la presencia de la versión 5.0 de Internet Explorer y del reproductor de medios, y el soporte para las nuevas tecnologías como USB, FAT32, Administración Avanzada de Energía, etc. Active Directory (AD) es el servicio de directorio incluido en Windows 2000.

La familia Windows 2000 está integrada por cuatro versiones:

**Windows 2000 Professional.** Sucesor de NT Workstation, está destinado a ser un cliente de red seguro y una estación de trabajo corporativa. Soporta hasta 2 procesadores.

**Windows 2000 Server.** Sucesor de NT Server, soporta hasta 4 procesadores y está destinado a ser el servidor de impresión, archivos, aplicaciones e, incluso, Web de una empresa pequeña a mediana.



**Windows 2000 Advanced Server.** Sucesor de NT Server Enterprise Edition, soporta hasta 8 procesadores y será el servidor departamental de aplicaciones en empresas medianas a grandes, con más de un dominio y tareas de misión crítica. Entre otras prestaciones, se incluye soporte para RAID y fault tolerance.

**Windows 2000 Data Center Server.** Soporta hasta 32 procesadores y sólo se entregará sobre pedido. Está destinado a grandes empresas que requieran data warehousing, análisis econométricos, simulaciones científicas e ingenieriles a gran escala, etc.

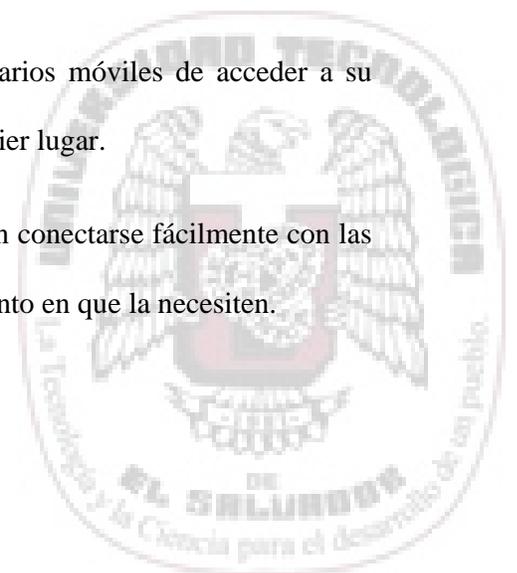
## **Windows XP**

Es el nuevo Windows para la computación del hogar y de negocios. Una meta importante del diseño de Windows XP es ofrecer experiencias completas tanto para los usuarios en el hogar como los de negocios en las siguientes áreas:

**Comunicaciones enriquecidas.** Uso compartido de voz, video y aplicaciones en tiempo real que permite a las personas comunicarse de manera más efectiva .

**Movilidad mejorada.** La habilidad para los usuarios móviles de acceder a su información en cualquier momento y desde cualquier lugar.

**Ayuda y soporte mejorados.** Los usuarios pueden conectarse fácilmente con las personas y recursos para recibir ayuda en el momento en que la necesiten.



**Fotos y videos digitales sencillos.** Windows XP facilita crear, organizar y compartir memorias digitales.

**Música y entretenimiento emocionantes.** Windows XP ofrece la mejor experiencia para el descubrimiento, descarga, personalización y reproducción de contenidos de audio y video de alta calidad.

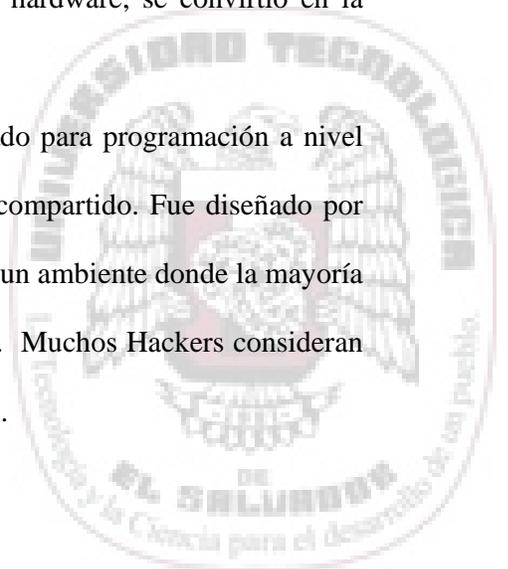
**Habilitar "Hogares conectados".** Windows XP ofrecerá a las personas una manera sencilla de compartir información, dispositivos y conexiones de Internet dentro del hogar.

## UNIX

UNIX es más antiguo que todos los demás sistemas operativos para PC (Computadoras Personales), y de muchos modos sirvió como modelo para ellos.

Es un Sistema Operativo Multiusuario y Multitarea de AT&T que corre en muchos tipos diferentes de computadoras: en supercomputadoras Cray, en PC y todo lo que está en medio, incluyendo Mainframes y minicomputadoras. Debido a su capacidad para trabajar con tantas clases de hardware, se convirtió en la columna vertebral de Internet.

UNIX está escrito en Lenguaje C, que está diseñado para programación a nivel de sistemas. Es un sistema interactivo de tiempo compartido. Fue diseñado por programadores, para programadores, y cuyo uso es un ambiente donde la mayoría de los usuarios son ingenieros y usuarios técnicos. Muchos Hackers consideran que UNIX es el auténtico y único sistema operativo.



## Linux

Linux es una versión de UNIX de libre distribución, inicialmente desarrollada por Linus Torvalds en la Universidad de Helsinki, en Finlandia. Fue desarrollado con la ayuda de muchos programadores y expertos de UNIX a lo largo y ancho del mundo, gracias a la presencia de Internet. Cualquier habitante del planeta puede acceder a Linux y desarrollar nuevos módulos o cambiarlo a su antojo.

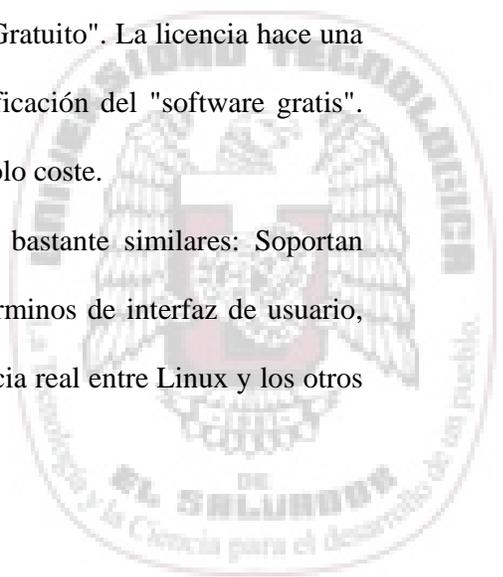
Linux es un sistema operativo completo con multitarea y multiusuario (como cualquier otra versión de UNIX). Esto significa que pueden trabajar varios usuarios simultáneamente en él, y que cada uno de ellos puede tener varios programas en ejecución.

Linux dispone de los dos principales protocolos de red para sistemas UNIX: TCP/IP y UUCP (UNIX-to-UNIX Copy; es un viejo mecanismo usado para transferir ficheros, correo electrónico y noticias entre maquinas UNIX).

Los programas de comunicaciones para Linux son muy parecidos a los que se pueden encontrar para MS-DOS y otros sistemas operativos.

Linux esta regido por lo que se conoce como la Licencia Publica General de GNU, o GPL ( General Public License). La GPL fue desarrollada para el proyecto GNU por la "Fundación por el Software Gratuito". La licencia hace una serie de previsiones sobre la distribución y modificación del "software gratis". "Gratis" en este sentido se refiere a libertad, y no solo coste.

Técnicamente, OS/2, Windows NT y Linux son bastante similares: Soportan aproximadamente las mismas características en términos de interfaz de usuario, redes, seguridad, y demás. Sin embargo, la diferencia real entre Linux y los otros



es el hecho de que Linux es una versión de UNIX, y por ello se beneficia de las contribuciones de la comunidad UNIX en pleno.

Linux tiene varias distribuciones, y cada una de ellas posee sus propias características y software lo cual la hace única. Entre los proveedores tenemos a: Phat Linux, Red Hat, Mandrake, Suse, Debian, Kheops, Slackware, etc.

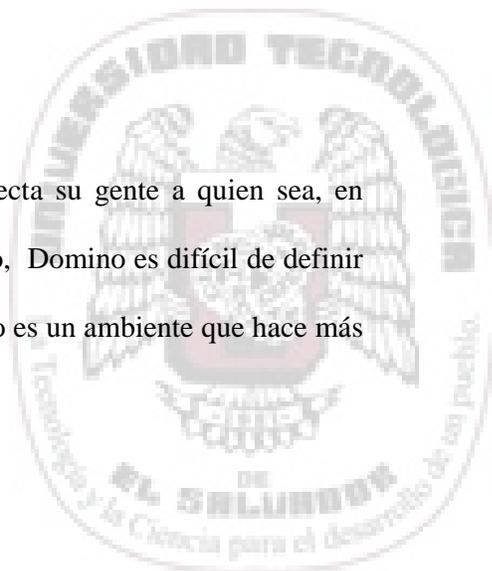
### **Lotus Notes**

Fue el primero en traer colaboración basada en computadoras y correo electrónico a las PCS. Se dice que mucho de la versión original de Notes permanece intacto hoy. Notes es un “agente procesador de información.” Notes entrega la información que ha recopilado de una variedad de recursos.

La mayor parte de su éxito se debe a que los usuarios pueden ver el valor del cliente de Notes en un browser y en la integración de e-mail, aplicaciones, discusiones, movilidad y otras características que hace de Notes una combinación muy poderosa.

### **Lotus Domino Server**

Domino es software, una infraestructura que conecta su gente a quien sea, en donde sea, a cualquier hora. Al igual que su trabajo, Domino es difícil de definir porque se adapta a tareas de muchos tipos. Domino es un ambiente que hace más



fácil para usted crear trabajo no estructurado (de una manera productiva), usando una riqueza de información y de conocimiento que es cambiante.

Domino es el nombre verdadero del producto servidor, y Notes es el del cliente. A menudo, los usuarios piensan en Domino como si se tratase de un solo producto. En cambio, dentro de Domino se ofrecen muchos productos: Domino Mail Server provee soporte de base de datos de correo electrónico y discusión. Domino Application Server agrega un servidor Web y el soporte de la aplicación GroupWare que los usuarios normalmente consideran como Domino. Domino Enterprise Server añade soporte de aplicación para clustering, equilibrio de carga y recuperación de fallos para los clientes Notes y Web además de soporte para Microsoft Cluster Server.

## Seguridad

La Planificación de la seguridad es un elemento importante en el diseño de una red. Es mucho más sencillo implementar una red segura a partir de un plan, que recuperar los datos perdidos. Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son :

- Acceso no autorizado
- Soborno electrónico
- Robo
- Daño intencionado o no intencionado



## **Técnicas para vencer la seguridad**

### **Secuestros (Hijacking)**

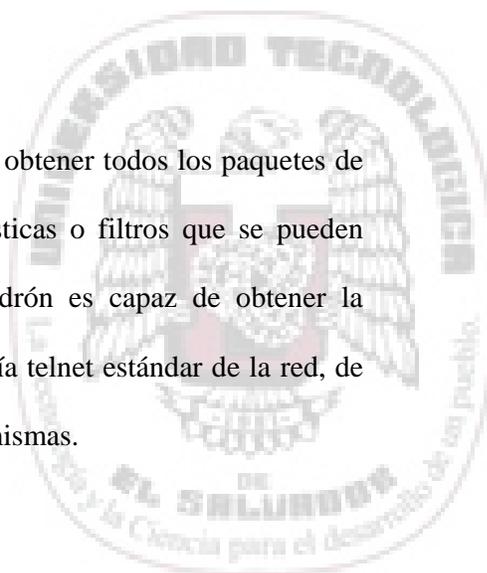
Una vez que un intruso ha conseguido acceso como súper usuario (root) a un sistema, éste puede utilizar una herramienta que modifique el núcleo del sistema operativo de forma que sea capaz de secuestrar las conexiones por acceso remoto o terminal que cualquier usuario haga desde el sistema local. Así de esta forma, el intruso espera a que un usuario se haya autenticado al sistema remoto y una vez hecho esto, el intruso secuestra la conexión del usuario, de forma que el sistema remoto queda comprometido y a disposición del intruso.

En este ataque, cuando el intruso secuestra una conexión, el usuario puede detectar actividad anormal. Una vez que el ataque se ha completado es difícil detectar, aunque algunas veces se pueden encontrar rastros de la actividad del intruso, como ciertos módulos existentes en el núcleo diseñados a tal fin.

No hay otra manera de combatir este ataque que evitar que un intruso gane acceso a un sistema como súper usuario.

### **Robo (Sniffing)**

El Robo o Sniffing, es una técnica que consiste en obtener todos los paquetes de una red local acordes con una serie de características o filtros que se pueden configurar por el usuario. De esta forma, un ladrón es capaz de obtener la mayoría de los paquetes de todas las conexiones vía telnet estándar de la red, de forma que puede hacerse con la contraseña de las mismas.



Para detectar la presencia de un ladrón en un sistema sólo se tiene que chequear que la tarjeta de red no está en modo promiscuo.

Existen varias formas de prevenir este ataque: una de ellas es utilizar programas que mantengan conexiones codificadas. Otra solución es la utilización de concentradores inteligentes que evitan el robo en la red local. También la utilización de contraseñas de un solo uso. La utilización de tarjetas que no soporten el modo promiscuo es otra posibilidad.

### **Caballos de Troya**

Son archivos ejecutables que realizan las funciones esperadas pero en la realidad ejecutan comandos adicionales que sirven para corromper la seguridad del sistema. Un intruso puede reemplazar un archivo por el suyo y dotarle de propiedades análogas al reemplazarlo. Lo que se hace es confiar en algoritmos de redundancia cíclica, algoritmos basados en la codificación o funciones hash. Con estos algoritmos se calcula la suma de chequeo (checksum) de los archivos existentes para luego compararlos con el de los originales. La mejor manera de evitarlos es no ejecutar nunca un archivo de lote (script) que no sea conocido.

### **Vándalos e intrusos**

#### **Hackers**

Los Hackers o Vándalos son expertos en computación que hurgan en los sistemas, pero cuyo código de ética no los lleva a hacer daño, salvo para borrar



sus huellas, ni sacar dinero directamente; la palabra Hacker es una palabra que se refiere a alguien persistente, que trata de adivinar las cosas hasta averiguar como funcionan.

## **Crackers**

Los Crackers o intrusos son aquellos que tratan de entrar a los sistemas a toda costa, para ganar prestigio y demostrar que se puede, o con fines económicos, dañando generalmente la información almacenada.

Un Cracker puede instalar en una estación del sistema un pequeño programa que captura la secuencia de las teclas digitadas. Es el denominado Caballo de Troya, y actúa capturando y guardando en un archivo todo lo que se escriba después de ciertas palabras claves. Luego revisa desde un lugar remoto el contenido del archivo que obtuvo. Esta técnica es simple y generalmente nadie nota nada.

Debido a la persistente labor de los Hackers y Crackers, además de adivinar las cosas, el trabajo es robar información teniendo acceso a sistemas ajenos. Las razones de querer llevar a cabo este acceso pueden ser:

- Sólo para mirar
- Por Diversión
- Para robar recursos del sistema, secretos industriales y otra información propietaria.



## Medidas de Seguridad

### Cortafuegos (Firewalls)

Un Cortafuegos o Firewalls es un sistema de seguridad, normalmente una combinación de hardware y software, que está destinado a proteger la red de una organización frente a amenazas externas que proceden de otra red, incluyendo Internet.

Los cortafuegos evitan que los equipos de red de una organización se comuniquen directamente con equipos externos a la red, y viceversa. En su lugar, todas las comunicaciones de entrada y salida se encaminan a través de un servidor proxy que se encuentra fuera de la red de la organización. Además, los cortafuegos auditan la actividad de la red, registrando el volumen de tráfico y proporcionando información sobre los intentos no autorizados de acceder al sistema.

Un servidor Proxy es un cortafuegos que gestiona el tráfico de Internet que se dirige y genera una LAN. El servidor proxy decide si es seguro permitir que un determinado mensaje pase a la red de la organización. Proporciona control de acceso a la red, filtrado y descarte de peticiones que el propietario no considera apropiadas, incluyendo peticiones de accesos no autorizados sobre datos de propiedad.



## **Auditoría**

La revisión de los registros de eventos en el registro de seguridad de un servidor se denomina Auditoría. Este proceso realiza un seguimiento de las actividades de la red por parte de las cuentas de usuario. La auditoría debería constituir un elemento de rutina de la seguridad de la red. Los registros de auditoría muestran los accesos por parte de los usuarios(o intentos de acceso) a recursos específicos. La auditoría ayuda a los administradores a identificar la actividad no autorizada.

Además permite realizar un seguimiento de las siguientes funciones:

- Intentos de entrada
- Conexiones y desconexiones de los recursos designados
- Terminación de la conexión
- Desactivación de cuentas
- Apertura y cierre de archivos
- Modificaciones realizadas en los archivos
- Creación o borrado de directorios
- Modificación de directorios
- Eventos y modificaciones del servidor
- Modificaciones de las contraseñas
- Modificaciones de los parámetros de entrada



Los registros de auditoría pueden indicar cómo se está utilizando la red. El administrador puede utilizar los registros de auditoría para generar informes que muestren las actividades de sus correspondientes fechas y horarios.

### **Equipos sin disco**

Los equipos sin disco, como su nombre implica, no tiene unidades de disco o discos duros. Pueden realizar todo lo que hacen los equipos con unidades de disco, excepto almacenar datos en una unidad de disco local o en un disco duro. Los equipos sin disco constituyen una opción ideal para el mantenimiento de la seguridad puesto que los usuarios no pueden descargar datos y obtenerlos.

Estos equipos no requieren discos de arranque. Se comunican y se conectan al servidor por medio de un chip de arranque ROM especial instalado en la tarjeta de red del equipo. Aunque estos equipos proporcionen seguridad, no tienen mucha aceptación. Toda la actividad del equipo debe realizarse a través de la red cuando no se dispone de un disco local donde almacenar los datos y aplicaciones. Tenemos, por tanto, que el tráfico de la red incrementará y la red deberá controlar el incremento de demanda.

