

44  
2 of

---

# REDES DE AREA LOCAL

## TOKEN RING

MARIA CRISTINA PEREZ SORIANO

ENRIQUE NAVARRETE GUZMAN

DIRECTOR: ACT. SERGIO CASTRO RESINES

1991



Universidad Nacional  
Autónoma de México



## **UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso**

### **DERECHOS RESERVADOS © PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

---

**A la Universidad Nacional Autónoma de México, por brindarnos la oportunidad de aprender y poner en práctica nuestros conocimientos.**

**Al Act. Sergio Castro Resines, por haber creído en nosotros dándonos parte de su experiencia, amistad y apoyo.**

**A la Ing. Salma Jalife Villalón, por sus consejos, ayuda y cariño.**

**A nuestros padres y hermanos por su gran apoyo moral y paciencia.**

**Y a todas las personas que de alguna forma nos ayudaron a llegar a este momento.**

**A todos MUCHAS GRACIAS**

**Cristina y Enrique**

---

# INDICE



# INDICE

---

## 1. REDES DE COMPUTADORAS

- 1.1 Introducción
- 1.2 Evolución de las redes de comunicación
- 1.3 Definición de Red de Computadora
- 1.4 Estándares para Redes

## 2. REDES DE AREA LOCAL.

- 2.1 Introducción
- 2.2 Definición de Red de Area Local (LAN)
- 2.3 Características de las LAN's
  - 2.3.1 Medios de transmisión
  - 2.3.2 Modos de transmisión
  - 2.3.3 Topología
  - 2.3.4 Protocolo de Control de Acceso al Medio
- 2.4 Proyectos de Estandarización para LAN's

## **3. TOKEN RING**

- 3.1 Introducción
- 3.2 Primeras redes de área local Token Ring
- 3.3 Tecnología Token Ring
  - 3.3.1 Estrella-Alambrada
  - 3.3.2 Medio de transmisión
  - 3.3.3 Modo de transmisión
  - 3.3.4 Codificación
  - 3.3.5 Sincronía
  - 3.3.6 Protocolo Token
  - 3.3.7 Monitoreo del anillo
  - 3.3.8 Unidades de Acoplamiento
- 3.4 Modelo de Colas de la Operación Básica de Token Ring

## **4. PROTOCOLO DE CONTROL DE ACCESO AL MEDIO**

- 4.1 Introducción
- 4.2 Principio de Operación del Protocolo de Control de Acceso al Medio

- 4.3 Estructura del Frame
  - 4.3.1 Descripción de los campos de ambos formatos
- 4.4 Trasmision y Recepcion de Frames
  - 4.4.1 Trasmisión
  - 4.4.2 Recepción
- 4.5 Control y Administración del Anillo
  - 4.5.1 Operaciones de Prioridad
  - 4.5.2 Administración del Anillo
  - 4.5.3 Monitor Activo del Anillo
  - 4.5.4 Señalización (Beaconing)
- 4.6 Diferencias en la FDDI
  - 4.6.1 Formato del Frame
  - 4.6.2 Protocolo MAC
- 4.7 Eficiencia (Performance)
  - 4.7.1 Velocidad contra distancia
  - 4.7.2 Factores que afectan al performance
  - 4.7.3 Límites del Performance
  - 4.7.4 Metodo para calcular los límites del Throughput y del retardo en función del numero de estaciones activas

## **5. REDES MULTI-ANILLOS**

### **5.1 Introducción**

### **5.2 Límites de los anillos sencillos**

### **5.3 Repetidores (Repeaters)**

#### **5.3.1 Repetidores de Cobre**

#### **5.3.2 Repetidores de Fibra Óptica**

### **5.4 Justificación de redes multi-anillos**

### **5.5 Diseño de Multi-anillos**

#### **5.5.1 Estructura Backbone**

#### **5.5.2 Topologías Multi-anillos**

### **5.6 Puentes (Bridges)**

#### **5.6.1 Técnica de Enrutamiento 'Source Routing'**

#### **5.6.2 Control de Liga de Datos**

### **5.7 Compuertas (Gateways)**



## **6. SISTEMA BASICO DE ENTRADA/SALIDA PARA RED (NETBIOS)**

6.1 Introduccion

6.2 NetBIOS

6.3 Relacion del NetBIOS con el Modelo OSI

6.4 Programacion del NetBIOS

6.4.1 Conceptos Basicos

6.4.2 Comandos del NetBIOS

6.4.3 Estructura NBC (Network Control Block)

6.4.4 Implementacion del NBC

## **7. PLANEACION Y OPERACION DE REDES DE AREA LOCAL.**

### **7.1 Introduccion**

### **7.2 Ciclo de Desarrollo de un Sistema de Informacion Basado en Redes de Computadoras**

### **7.3 Fase de Estudio**

#### **7.3.1 Investigacion y Analisis**

#### **7.3.2 Estudio de Factibilidad**

### **7.4 Fase de Seleccion y Diseño**

#### **7.4.1 Sistema de Seguridad**

#### **7.4.2 Consultas con los Usuario**

#### **7.4.3 Configuración**

#### **7.4.4 Evaluación de Software**

#### **7.4.5 Evaluación de Hardware**

### **7.5 Fase de Implantación**

#### **7.5.1 Plan de Implantación**

### **7.6 Fase de Operación**

## 8. CONCLUSIONES

## 9. APENDICES

A. Tabla de Distancias Maximias

B. Tabla de Distancias Maximias con Repetidores de  
Cobre

C. Lista de Comandos DEL NetBIOS

D. Lista de Requerimientos y Códigos de Regreso de  
los Comandos del NetBIOS

E. Descripción de Códigos de Regreso

F. Implementación del NCB en Ensamblador y C

## 10. GLOSARIO

## 11. BIBLIOGRAFIA

---

# 1. REDES DE COMPUTADORAS



## 1.1 INTRODUCCION

Las redes de computadoras surgen de la necesidad de intercambiar recursos (información, dispositivos, etc) entre diferentes sistemas de cómputo.

Esta necesidad comprende básicamente dos problemas. El intercambio de datos y su interpretación.

Para solucionarlos han surgido diferentes formas de comunicar sistemas de computadoras entre sí, su evolución ha traído como consecuencia el intercambio de información cada vez más confiable, de manera más rápida y en volúmenes cada vez mayores.

Esta tarea no ha sido fácil, debido a la variedad de sistemas de cómputo, ya que no solo difieren en arquitectura interna, si no también en propósito y aplicaciones.

Para atacar este problema algunos organismos internacionales desde hace varios años se han dedicado a estudiar diferentes maneras de estandarización.

Debido a lo anterior, en este capítulo se describe la evolución histórica que han tenido los sistemas de comunicación de datos, para definir a las redes de computadoras y el modelo creado para estandarizar el intercambio de información entre las mismas.

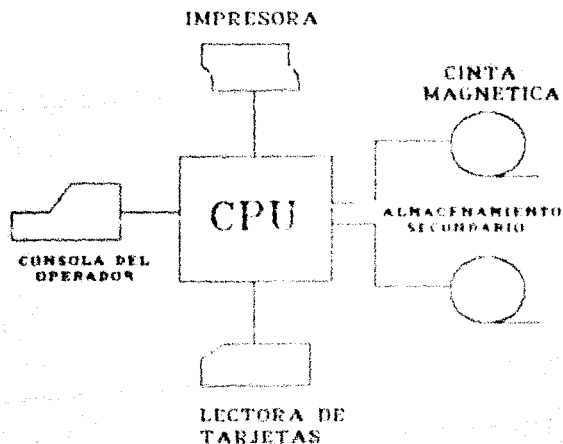
## 1.2 EVOLUCION DE LAS REDES DE COMUNICACION

La evolución histórica de los sistemas de comunicación de datos, se describe siguiendo el desarrollo que han tenido los sistemas de cómputo a través del tiempo.

En el inicio de las redes de comunicación de datos, una organización contaba con su sistema de cómputo centralizado formado de *hardware* caro y complicado y *software* primitivo.

Básicamente el sistema de cómputo consistía de una unidad central de proceso (CPU) con limitada cantidad de memoria de acceso aleatorio (RAM), algún elemento de almacenamiento secundario (cinta magnética o disco magnético), impresora, lectora de tarjetas y la consola del operador.

Los usuarios normalmente preparaban sus programas y datos fuera de línea, en una perforadora de tarjetas localizada en otro cuarto, y después el operador ejecutaba cada programa secuencialmente.



Conforme la tecnología de computadoras avanzó, se incrementó la rapidez de los dispositivos de almacenamiento secundario y los sistemas operativos permitieron la multiprogramación. Se hizo posible el "tiempo compartido", permitiendo a los usuarios trabajar con sus programas y datos almacenados de forma interactiva y simultánea, vía su propia terminal alejados de la computadora central.

Las terminales eran normalmente dispositivos electromecánicos que podían transmitir y recibir datos a grandes distancias.

Con el aprovechamiento este avance tecnológico, las organizaciones comenzaron a utilizar varias terminales bajo un sistema de multiproceso.

En un principio las terminales se colocaron cerca del computador central; pero después, gracias a sus características y adelantos tecnológicos, se distribuyeron a lo largo de diferentes oficinas y con la ayuda de las redes conmutadas de teléfonos y *modems*, se instalaron a través de grandes áreas geográficas.



#### NOTACION :

FEP PROCESADOR FRONTAL

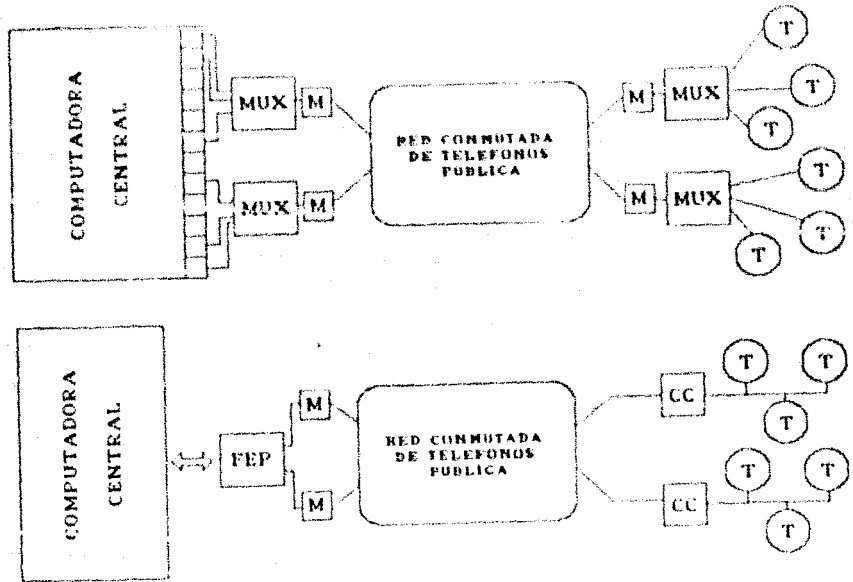
CC CONTROLADOR

MUX MULTIPLEXOR

T TERMINAL

M NODEN

El empleo de las redes conmutadas de telefonos propicio que se incrementara el costo de la linea telefonica. Para disminuir este incremento, se diseñaron dispositivos para aprovechar una sola linea para varias terminales (multiplexores y controladores).



El incremento en el uso de computadoras creció de tal manera que los sistemas llegaron a tener cientos de terminales, lo que trajo como consecuencia que la computadora central perdiera tiempo en realizar tareas de control y atención a cada una de las líneas de comunicación. Este problema se solucionó al introducir procesadores frontales (*Front End Processor - FEP*), los cuales se encargaron de controlar la sobrecarga que las tareas de comunicaciones representaban para el procesador central.

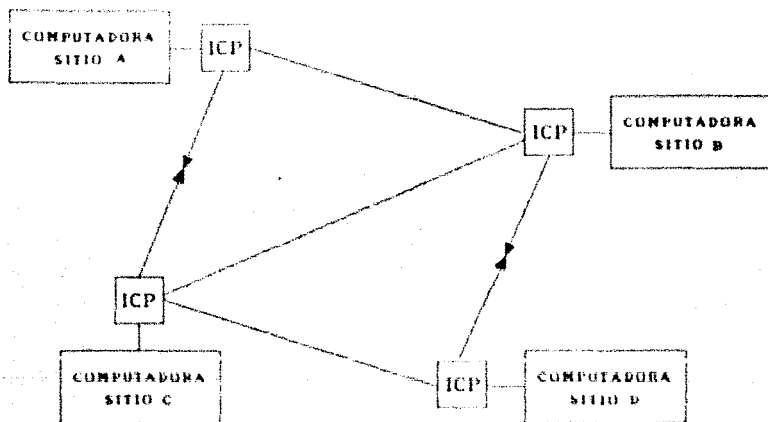
Lo anterior prevalecía en lugares que tenían su información en un lugar central que no siempre era necesario.



Algunas organizaciones tenían varios sistemas de cómputo independientes localizados en diferentes sitios, pero en ocasiones requerían intercambiar información o compartir recursos, por lo cual surgieron los primeros enlaces entre computadoras.

Este intercambio se basaba en la red pública conmutada de teléfonos (PSTN) y *modems* y tenía como limitante el volumen de información a transmitir.

Para solucionar este problema surgieron las redes telefónicas autónomas (PSDN) que además podían almacenar y direccionar la información.



Esta red telefónica, destinada especialmente al intercambio de información, tuvo la ventaja de transmitir grandes mensajes de datos. Pero como consecuencia el tiempo de respuesta se vio afectado ya que dependía del número de mensajes y del tamaño de los mismos, por lo que se optó por definir una unidad mínima de mensaje a lo que se le llamó paquete; así surgieron las redes de conmutación de paquetes.

Los continuos avances en circuitos integrados están provocando el cambio en la operación de la red telefónica de modo analógico a digital, por lo que han comenzado a surgir las redes digitales de servicios integrados (ISDN).

### 1.3 DEFINICION DE RED DE COMPUTADORAS

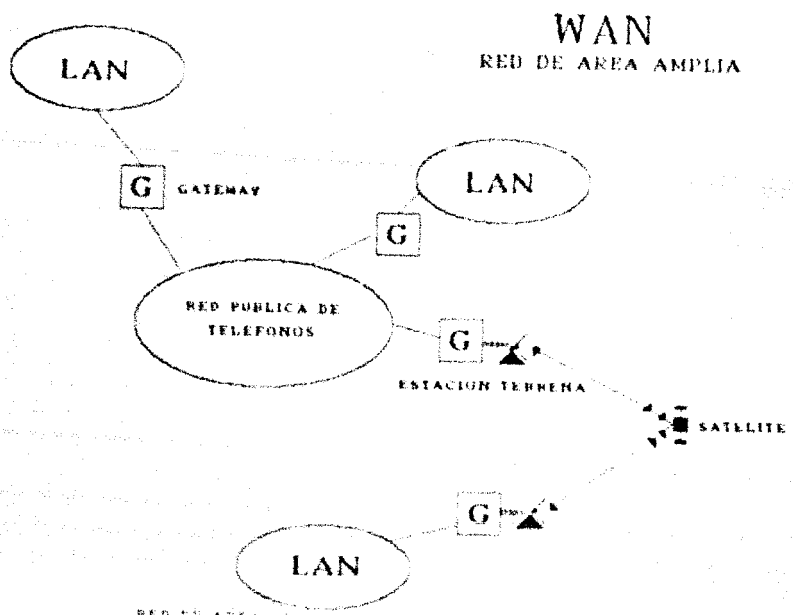
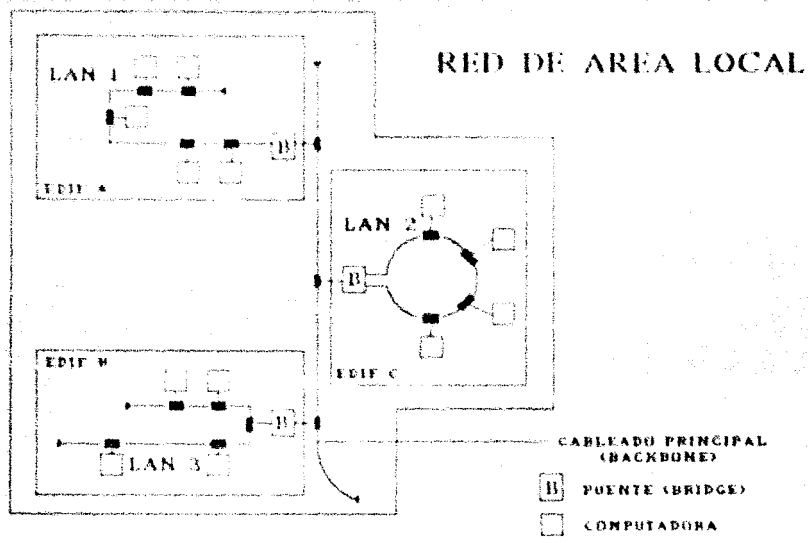
Una red de computadoras es la interconexión de las mismas a través de cualquier medio de comunicación.

La interconexión se puede establecer a través de diferentes medios de comunicación: red pública conmutada de teléfonos, red privada, redes digitales de servicios integrados, microondas, vía satélite o simplemente con una conexión punto a punto. La red más simple se forma por el enlace entre dos computadoras conectadas punto a punto.

De acuerdo a lo anterior se establecen básicamente dos tipos de redes de computadoras:

- Aquellas que al utilizar medios de comunicación públicos llegan a cubrir grandes áreas geográficas: Redes de Areas Amplias (WANs)
- Aquellas que se forman en áreas relativamente pequeñas y que emplean su propio canal de comunicación (LANs)

Existen muchos tipos diferentes de redes clasificadas de acuerdo a su topología, tipo de operación, etc., cada una de estas se utiliza dependiendo según las características y necesidades propias de cada organización.



## 1.4 ESTANDARES PARA REDES

Como las computadoras no solo son incompatibles en arquitectura sino también en propósito, sistemas operativos y programas de aplicación, comenzaron a surgir dispositivos para la comunicación de datos de diferentes tipos y para cada marca de computadoras, lo que las reafirmó como sistemas cerrados; desde hace varios años esto ha provocado la preocupación por lograr una estandarización entre los diferentes sistemas tanto de cómputo como de comunicación de datos y la interfase entre ambos, para lo cual han surgido organismos internacionales enfocados a plantear soluciones para este problema, como son la CCITT, ISO, ANSI, IEEE, ECMA, EIA, ITU, etc.

Dentro de estos organismos dedicados a buscar y establecer normas para la estandarización se encuentra el ISO "International Standard Organization", el cual propuso un modelo completo para la estructura de un sistema de comunicación entre computadoras.

Este modelo se le conoce como el modelo de referencia para la interconexión de sistemas abiertos "*Open Systems Interconnection*" (OSI).

El modelo OSI se apoya en una estructura jerarquizada que comprende diferentes niveles donde se ejecutan funciones bien definidas; cada nivel opera de acuerdo a un protocolo para el intercambio de mensajes entre niveles iguales de un enlace y además cada nivel cuenta con una interfase que lo conecta con sus respectivos niveles anterior y posterior.

Los niveles que OSI propone son 7: físico, enlace de datos, red, transporte, sesión, presentación y aplicación; y además los agrupa en 3 ambientes de trabajo: red, OSI y real.

Las funciones específicas que en cada nivel se realizan son:

El nivel **FISICO** establece todas las características eléctricas y funcionales del medio físico, así como las características eléctricas y funcionales y los procedimientos para accederlo.

El nivel de **ENLACE DE DATOS** establece las características de la transmisión de información través del enlace físico. Es decir, envía bloques de datos con la sincronización, control de error y control de flujo necesarios para que los datos se transmitan en forma segura.

El nivel de **RED** permite a los niveles superiores comportarse de manera independiente a la transmisión de los datos y se responsabiliza de establecer, mantener y terminar las conexiones. Esto es, se encarga de la correcta transmisión y recepción de los datos, genera algoritmos para el bloqueaje de los mismos y su transmisión en paquetes pequeños.

El nivel de **TRANSPORTE** proporciona una transferencia de datos transparente entre dos puntos terminales. Es decir, asegura la correcta conexión entre dichos puntos, con lo que establece la dirección antes de realizar algún tipo de comunicación, ya sea de transmisión o de recepción.

El nivel de **SESION** establece la estructura de control de la comunicación entre "aplicaciones". O sea que establece, mantiene y termina conexiones lógicas (sesiones) entre dos puntos.

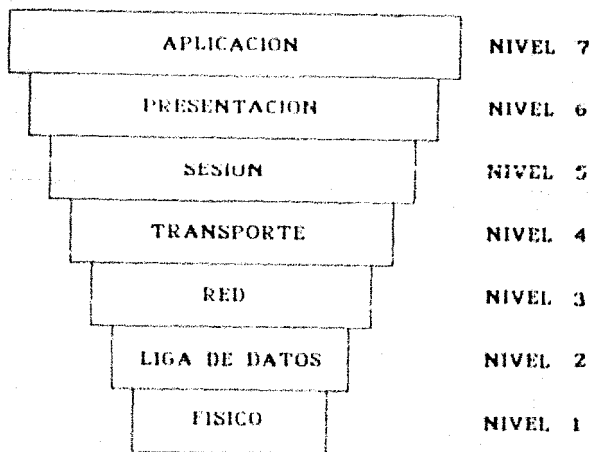
El nivel de **PRESENTACION** proporciona independencia a los procesos de la aplicación de las diferentes representaciones de los datos (sintaxis), es decir es donde se determina si los datos e instrucciones que se ejecutan en la computadora se trabajarán o no a nivel local.

El nivel de **APLICACION** permite que los usuarios accedan el ambiente **OSI**, con lo que les proporciona servicios de distribución de tareas. Es decir, es la interfase con el usuario y el programa de aplicación que utiliza, sin que se de cuenta de los detalles de comunicación involucrados.

Las diferentes operaciones (ó actividades) que en los ambientes del modelo OSI se llevan a cabo son:

1. Ambiente RED: engloba a protocolos y estandares relacionados a las bases de los diferentes tipos de redes de comunicacion de datos
2. Ambiente OSI: el cual abarca el nivel red, adicionandole los protocolos orientados a aplicaciones y los estandares que le permiten a los sistemas finales (computadoras) comunicarse con otro de manera abierta.
3. Ambiente de Sistemas Reales: el cual se base en el ambiente OSI para construir servicios y software apropiado para llevar a cabo una tarea en particular.

MODELO PARA LA INTERCONEXION  
DE SISTEMAS ABIERTOS  
(OSI)



---

## 2. REDES DE AREA LOCAL

## 2. REDES DE AREA LOCAL

---



### 2.1 INTRODUCCION

El continuo decremento en el costo del *hardware* acompañado del incremento en su capacidad ha repercutido en la manera en que la información se recolecta, procesa y utiliza en las empresas, esto, más el auge de las comunicaciones de datos y del mercado de las computadoras ha contribuido al desarrollo de diferentes maneras de enlace entre las mismas, lo que ha provocado el desarrollo de diferentes tipos de redes locales, para permitir que los usuarios individuales no trabajen de manera aislada y puedan contar con los beneficios de un sistema central que les permita intercambiar, compartir información o también compartir recursos sofisticados.

En el presente capítulo se da un panorama de lo que son las redes de computadoras de área local, sus características y clasificación.

Como en muchas áreas de las comunicaciones, la estandarización ha jugado un papel muy importante en la evolución de muchas tecnologías desarrolladas para LAN's. Por lo que en el presente capítulo, también se da una descripción de los principales proyectos de estandarización para redes de área local, el proyecto 802 de la IEEE (*Institute of Electrical and Electronics Engineers*) y el proyecto FDDI (*Fiber Distributed Data Interface*) de la ASC (*Accredited Standards Committee*).



## 2.2 DEFINICION

Una red local es un sistema de comunicación de datos que permite a diferentes dispositivos comunicarse entre si

Básicamente se distinguen 3 tipos de redes locales

- Redes locales de alta velocidad (HSLN)
- Intercambio privado digital ramificado (PBX)
- Redes de Area Local (LAN)

Con las siguientes características:

CARACTERISTICAS	LAN	HSLN	PBX
Medio de transmisión	Par Trenzado, CAT coaxial, Par Trenzado, Óptico, Fibra fibra óptica	Par Trenzado, CAT coaxial, Par Trenzado, Óptica, Fibra fibra óptica	Fibra óptica
Topología	Bus, Anillo, Bus, Estrella	Bus, Estrella	Estrella
Velocidad	1 a 20 Mbps	200 Mbps a 9 Mbps a 10Mbps	1 a 10Mbps
Distancia	25 Km	1 Km	1 Km
Técnica de conmutación	Paquetes	Paquetes	Circuitos
Número de dispositivos soportados	100 a 1000	10 a 50	100 a 1000
Costo aproximado	\$1,000 a \$10,000	\$50,000 a \$200,000	\$1,000 a \$10,000

Las redes locales de alta velocidad se diseñaron para la interconexión de computadoras *MAINFRAME* en lugares donde se requiere del proceso de grandes volúmenes de información, son de costo muy elevado y transmiten a grandes velocidades.

Los sistemas PBX permiten la transmisión de voz y datos sobre una misma red

Las redes de área local se distinguen de otros tipos de redes de datos por que:

- la comunicación se realiza en un área geográfica moderada.
- cuenta con un medio de transmisión propio y compartido entre las estaciones participantes proporcionando una capacidad de *broadcast*.
- cuenta con un protocolo distribuido (protocolo MAC), el cual controla el acceso al medio y proporciona mecanismos de recuperación cuando es necesario.
- cuenta con un conjunto de adaptadores cooperativos (*LAN's interfaces*) a través de los cuales las estaciones se conectan a la red, ejecutan el protocolo MAC y proporcionan la conexión lógica entre las estaciones conectadas.
- generalmente es propiedad de una misma empresa sin fines comerciales.
- su costo es relativamente bajo y su velocidad de transmisión es moderado (especificado en Mbps)

Las características básicas que diferencian a una red de área local de otra son:

- el medio de transmisión que utilizan para comunicarse,
- el modo de transmisión empleado
- la topología, es decir, la relación que guardan los diferentes nodos entre sí, y
- el protocolo que emplean para controlar el acceso a su medio de comunicación

## 2.3 CARACTERISTICAS DE LAS LAN'S

### 2.3.1 Medios de transmisión

Se refiere a la conexión física entre dispositivos fuentes y destinos; la cual se puede realizar a través de:

#### - Par de líneas

Este es el tipo más simple, donde cada línea se conecta punto a punto. Este tipo de conexión es adecuado cuando se conecta equipo muy cercano entre sí (aprox. 50 m) y donde se requiere de una velocidad de transmisión moderada (aprox. 10.2 Kbps), pero su estructura lo hace muy susceptible al ruido.

#### - Par trenzado

Es de los medios de comunicación más comunes pues se logran velocidades de unos cuantos Mbps y su costo es relativamente bajo. Su gran desventaja es que es muy susceptible a la interferencia y al ruido.

#### - Coaxial

El cable coaxial es de mayor costo que el par trenzado pero ofrece mejores ventajas, pues no es tan sensible al ruido y soporta a un mayor número de dispositivos conectados a él.

#### - Fibra óptica

Es el medio que mejores ventajas ofrece; tiene muy baja sensibilidad al ruido, ofrece una mayor velocidad de transmisión y mayor ancho de banda, entre otras cosas.

### 2.3.2 Modos de transmisión

#### - Modo de banda base (*BASEBAND*)

En este modo se emplea todo el ancho de banda para transmitir una sola señal a través del medio de transmisión

#### - Modo de banda ancha (*BROADBAND*)

En este modo el ancho de banda se divide en subcanales para permitir la transmisión de más de una señal a través del mismo medio de transmisión.

### 2.3.3 Topología

Es la clasificación de una red de acuerdo a su estructura física, esto es, como se relacionan los nodos entre sí.

Las más comunes y básicas son las de estrella, anillo y canal (*bus*). A partir de estas topologías se derivan otras más complejas.

#### - Estrella (*Star*)

En este tipo de configuración, se utiliza un nodo para conectar a todos los demás nodos de la red. El nodo central funciona como un elemento de conmutación central, establece una trayectoria que simula una conexión punto a punto entre dos estaciones, por lo que cuando tiene mucho tráfico se pueden generar cuellos de botella, lo cual se traduce en problemas al nodo central que pueden perjudicar a toda la red. Esta es una gran desventaja para este tipo de topología, además que si se desea tener otro nodo central de respaldo implica otra inversión que aumentada a la inicial da un costo muy elevado.

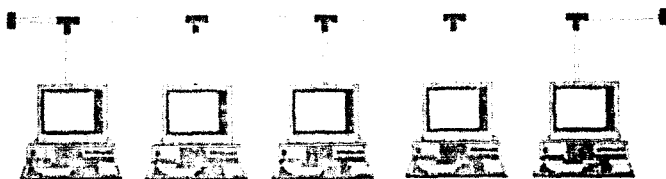
### - Anillo (*Ring*)

La topología anillo consiste de un ciclo cerrado donde cada nodo se conecta a un elemento repetidor. Los datos circulan alrededor del anillo sobre una serie de conexiones punto a punto. Si una estación necesita transmitir, espera su turno y entonces envía sus datos en forma de paquete. Este paquete contiene las direcciones destino y fuente, además de los datos. Cuando el paquete llega al nodo destino, éste lo copia y el paquete continúa circulando hasta llegar al nodo fuente como una forma de contestación. Se utiliza un protocolo de control para determinar la secuencia de nodos a transmitir. Como el anillo se construye a través de conexiones punto a punto, se puede usar cualquier tipo de medio de transmisión, de los cuales el más común es el par trenzado (a velocidades cercanas a los 4 Mbps). La fibra óptica se puede emplear para lograr mayores velocidades (16 Mbps).

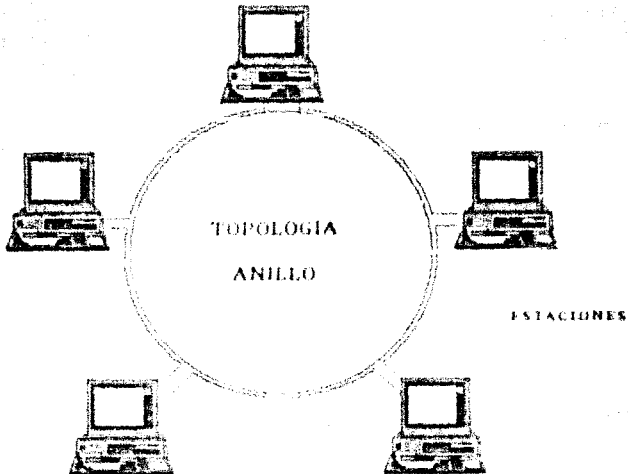
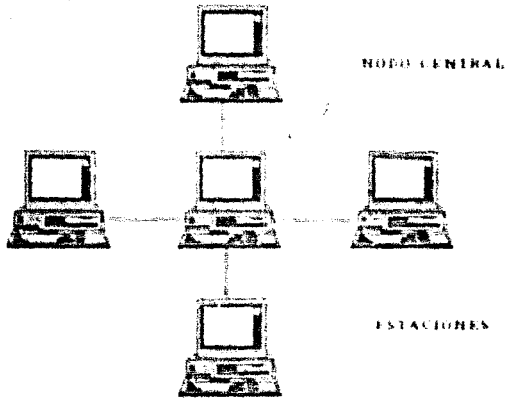
### - Canal (*Bus*)

La topología canal se caracteriza por emplear un medio de acceso múltiple. Todos los nodos comparten el mismo medio de comunicación, pero solo un par de dispositivos pueden comunicarse a la vez. Se debe utilizar un protocolo de acceso al medio para determinar cual es el siguiente nodo a transmitir. Como en la topología anillo, también en la topología canal se cuenta con un paquete que en sus campos contiene las direcciones fuente y destino. Cada estación monitorea el medio y copia el paquete que lleva la dirección de sí mismo. Lo más común en esta topología es emplear cable coaxial como medio de transmisión. Aunque no se descarta el empleo de fibra óptica.

TOPOLOGIA CANAL (BUS)



## TOPOLOGIA ESTRELLA



### 2.3.4 Protocolo de control de acceso al medio

Como las redes locales comparten el medio de transmisión (sin importar su topología) se requiere de un control para el acceso a su respectivo medio. De éstos los más comunes son el protocolo CSMA/CD y el protocolo *Token*

#### - CSMA/CD

La técnica que sigue el protocolo de acceso múltiple con sentido de portadora (CSMA) es la siguiente: cuando una estación desea transmitir sensa primero al medio para determinar si alguna otra estación se encuentra transmitiendo. Si el medio se encuentra libre la estación puede comenzar a transmitir, de lo contrario continúa sensando el medio. Una vez que la estación ha transmitido su mensaje, espera por un reconocimiento para identificar que su mensaje llegó correctamente o no.

Cuando una colisión se detecta durante una transmisión (CD), esta se detiene de inmediato y se transmite durante un breve periodo de tiempo una señal de bloqueo para asegurar que todas las estaciones se percataron de la colisión. Después de transmitir esta señal de bloqueo, la estación espera un periodo aleatorio de tiempo y reintentará transmitir empleando algún algoritmo de persistencia.

#### - *Token* para topología Anillo

Esta técnica se basa en el uso de un paquete llamado *token* que circula continuamente alrededor del anillo. Cuando ninguna de las estaciones transmite el paquete *token* se encuentra etiquetado como "libre".

Una estación que desea transmitir espera la llegada del *token* libre. Al recibirlo lo primero que hace es marcar al *token* como "ocupado" y enciende el bit correspondiente dentro del *frame*; entonces se inicia la transmisión del mismo en cuyo encabezado se incluye la dirección de la posible estación receptora. El *frame* lo repite cada estación conectada al anillo hasta que llega al mismo punto del cual

partió; sin embargo, solo lo copia la estación cuya dirección se encuentra marcada en el encabezado. Una vez copiado el *frame*, se encienden los bits de respuesta que indican que ya fue copiado. Al llegar al nodo inicial, este lo libera marcando al *token* como libre.

## 2.4 PROYECTOS DE ESTANDARIZACION PARA REDES DE AREA LOCAL

Con el desarrollo de múltiples redes de área local, surgió el problema de la incompatibilidad, por lo que la IEEE creó un comité enfocado al estudio de la estandarización de redes de área local conocido como proyecto IEEE 802, fundado en 1980 y seguido del FDDI.

El objetivo del estándar para redes de área local es para asegurar la compatibilidad entre equipos elaborados por diferentes compañías para que la comunicación de datos pueda llevarse a cabo entre los dispositivos con un mínimo de esfuerzo sobre las partes del equipo o sobre el sistema que contiene el equipo. Además, establece especificaciones que sugieren interfasas y protocolos comunes para las redes locales de comunicación de datos.

### 2.4.1 COMITE IEEE

El trabajo del comité IEEE 802 se basa en dos conclusiones:

- las tareas de comunicación que se llevan a cabo sobre una red local son lo suficientemente complejas que necesitan partirse en subtareas manejables.
- segundo, ninguna vía de aproximación técnica satisface todos los requerimientos.

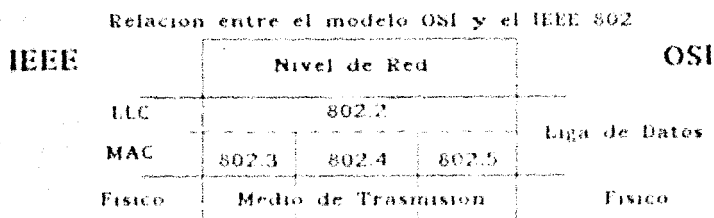


La primera conclusión sugiere tres niveles:

**FISICO** : Este nivel concierne a la naturaleza del medio de transmisión, a los detalles de conexión de dispositivos y a la señalización eléctrica.

**CONTROL DE ACCESO AL MEDIO** : Una red de área local se caracteriza por la colección de dispositivos que necesitan compartir un mismo medio de transmisión. Una manera de controlar el acceso es necesaria para que solo un dispositivo transmita a la vez.

**CONTROL DE ENLACE DE DATOS** : Este nivel engloba al establecimiento, mantenimiento y terminación de la liga lógica entre dispositivos.



802.2 = Protocolo de Control de Liga de Datos (LLC)

802.3 = CSMA / CD

802.4 = Token Bus

802.5 = Token Ring

Protocolos de Control de Acceso al Medio (MAC)

Lo anterior representa las siguientes diferencias con respecto al modelo OSI

En el modelo OSI el nivel fisico se representa por el equipo de comunicacion de datos, dentro del IEEE 802 se divide en tres capas (*TRUNK COUPLING UNIT, MEDIUM INTERFACE CONNECTOR, MEDIUM INTERFACE CABLE*)

El modelo OSI controla el enlace de datos completamente a través de una etapa (un solo protocolo), mientras que en el IEEE 802 esta necesidad se satisface mediante dos capas (*MEDIA ACCESS CONTROL, LOGICAL LINK CONTROL*)

El nivel de red (tercero dentro del modelo OSI) que originalmente se encuentra dividido en dos capas (1 de enrutamiento, y otra de circuito virtual), dentro del proyecto IEEE 802 el DATAGRAMA sustituye al circuito virtual

La segunda conclusión se apoyo en que, dada la existencia de gran variedad de redes de área local, ningún estándar simple satisficaría a las existentes. Por lo tanto el comité basó sus trabajos en los proyectos más serios en existencia en aquel entonces.

Debido a la segunda conclusión, el comité apoya:

- dos topologías (*ring* y *bus*),
- dos controles de acceso (*CSMA/CD* y *Token*) y
- dos modos de transmisión (*baseband* y *broadband*).

De ahí que el trabajo del comité IEEE 802 se encuentre organizado en varios subcomités.

IEEE 802.1 Estándar para interfaces de alto nivel

IEEE 802.2 Estándar para el control de flujo de datos

IEEE 802.3 CSMA/CD

IEEE 802.4 TOKEN BUS

IEEE 802.5 TOKEN RING

IEEE 802.6 REDIS DE AREA METROPOLITANA  
(MAN)

El subcomité para interfases de alto nivel, no desarrolla estandares, se dedica a trabajar en tópicos relacionados a interfases de alto nivel, interredes, direccionamiento y manejo de redes.

Los trabajos iniciales de los subcomites 802.2 802.3 802.4 se realizaron en 1983, y en 1984 se comenzó con 802.5 (*Token Ring*).

El trabajo en el comite 802.6 ha tenido poco progreso, en éste se han comenzado a desarrollar pequeñas alternativas para estudios posteriores.

#### 2.4.2 COMITE FDDI

La FDDI se comenzó a desarrollar en el comité **ASC** (*Accredited Standards Committee*), que se encarga de desarrollar estandares para las interfases de entrada y salida (*I/O interface standards*) con fibras ópticas como medio de transmisión entre computadoras.

La FDDI originalmente fue creada para aplicaciones finales de red (*back end network applications*), la conexión de procesadores y de dispositivos de almacenamiento de alta velocidad.

La FDDI se define en un conjunto de cuatro estandares.

- El documento **MAC** (*Media Access Control*), que es un estándar de la **ANS** y también del **DIS**.
- El protocolo de nivel físico (**PHY**) se encuentra en los últimos niveles de los documentos de la **ANS** y del **DIS**.
- El documento de la dependencia del nivel físico (**PMD**) se encuentra en revisión pública a la vez que se escribe en la propuesta del **DP** (*ISO Draft Proposal*).
- Actualmente el comité **ANSI X3T9.5** que se encuentra enfocado al documento **SMT** (*Station Management*).

---

El comité también se encuentra trabajando en un esquema híbrido llamado **FDDI-II**, para proporcionar al FDDI la capacidad de una conmutación de circuitos (*Circuit-Switching*).

---

### 3. TOKEN RING

## 3. TOKEN RING

---



### 3.1 INTRODUCCION

Los estándares que establecen las características de operación de una red de área local *Token* con topología de anillo (*Token Ring*), se encuentran dentro de los documentos de la IEEE 802.5 (par de cobre trenzado) y en los de la FDDI (fibra óptica).

En el presente capítulo se presenta una descripción de las primeras redes de área local basadas en tecnología *Token Ring*. También se presenta una descripción de la arquitectura y diseño de este tipo de redes locales, su comportamiento y posibilidades de aumentar su eficiencia; se muestra el modelo de colas que describe su operación básica y se da una introducción al protocolo de control de acceso al medio.

### 3.2 Primeras Redes de Area Local *Token Ring*

Una red con topología anillo consiste de una serie de estaciones conectadas por líneas de transmisión unidireccionales para formar una trayectoria cerrada. Las señales de información en el anillo pasan de una estación a otra regenerándose a través de cada estación. Los primeros sistemas de comunicación basados en esta técnica fueron:

Farmer y Newhall  
 Distributed Computing Systems (DCS)  
 Papeze  
 MIT (Massachusetts Institute of Technology)  
 Cambridge University  
 Zurich Research Laboratory (ZRL)

Para el Cambridge utilizaban un esquema para controlar el anillo de forma análoga en el cual varios paquetes de datos de longitud fija circulaban alrededor del anillo. Cada estación puede acceder al paquete que se encuentra justo para entrar en su área identificándolo por la dirección apropiada. Cada estación captura la información y la copia y se encuentra marcada con su dirección.

El segundo esquema de control aplicado en el sistema de anillo de Farmer y Newhall, es conocido como inserción de registro (buffer or register insertion), en el cual en un anillo el conflicto entre los datos lleva a un truncamiento por una estación y el flujo de datos que se circula en el anillo se reinicia por la estación maestra de un buffer con el suficiente espacio en el anillo.

El tercer esquema conocido como control de acceso por token (token access control), lo utilizan DCS, MIT, IBM, el cual se encuentra marcado como estándar dentro del IEEE 802.3 y también dentro del EDD.

En un anillo *Token Ring*, el acceso al canal de transmisión se controla pasando una señal especial, el permiso de acceso (token) a través del anillo. Cuando un sistema se inicia, una estación genera un token que viaja a través del anillo hasta que una estación lista para transmitir lo captura y entonces transmite sus datos. Al final de su transmisión, la estación marca el permiso de acceso y lo repone en la estación maestra y el proceso se repite.

En estos 3 esquemas de control todas las estaciones trabajan en pares (un emisor, un receptor) y automáticamente determinan cuando transmitir basándose en el estado del anillo. A comparación de otros esquemas de control en donde existe una estación maestra, responsable de controlar el acceso al medio o la trayectoria.

### 3.3 Tecnología *TOKEN RING*

*Token Ring* tiene características importantes que la hacen una solución muy atractiva como red de área local. Una muy importante y propia de *Token Ringes* es que la información fluye secuencialmente de una estación a otra alrededor del anillo. Esta transmisión unidireccional criticada como la mayor debilidad de *Token Ring*, porque aparentemente una simple falla puede hacer que se caiga todo el anillo, se puede solucionar con la introducción de una configuración Estrella Alambrada (*star wire*).

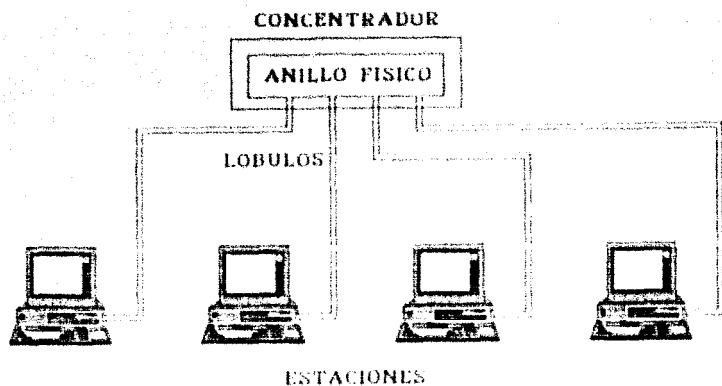
#### 3.3.1 Estrella-Alambrada

Cuando se utiliza este tipo de cableado se refiere a la conexión de cada estación hacia un concentrador. Internamente estos concentradores hacen las conexiones punto a punto. Los 'Lóbulos' (*wiring lobes*), que son la liga física existente entre cada estación y el concentrador, consisten de dos trayectorias de transmisión, una para enviar y la otra para recibir.

Los lóbulos se encuentran físicamente interconectados dentro de los concentradores hasta formar una liga serial.

El lóbulo solo se incluye en la trayectoria del anillo si la estación se encuentra activa, si no se lleva a cabo una función de puente para saltar a la siguiente estación activa. Si la función de puente posiciona a la estación en sí misma el lóbulo inactivo causará un incremento en la distancia que existe en las estaciones activas.





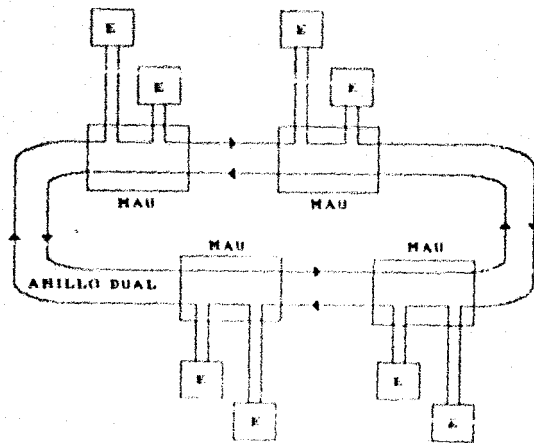
En un anillo que utiliza como medio de transmisión cobre, la función de puente comúnmente se realiza a través de un conjunto de relevadores que son activados por la estación conectada a través de un circuito fantasma (*phantom circuit*), donde una corriente de DC se aplica a través de los circuitos de entrada y salida, lo que implica que al apagar la estación, esta se removerá automáticamente del anillo.

Los concentradores (*wiring concentrators*) son completamente pasivos, contienen únicamente relevadores y ningún elemento activo como procesadores lógicos o fuentes de alimentación, y únicamente requieren del suministro necesario para activar los relevadores que insertan la estación al anillo, este suministro lo proporciona la misma estación de trabajo.

Cuando se utiliza fibra óptica para hacer la interconexión de las estaciones con el concentrador, las señales para insertar/remover se resuelven de manera diferente; en este caso se utilizan frames de control dentro del protocolo MAC (utilizan códigos que no están en uso).

En caso de emplear fibra óptica, los concentradores deben ser activos, es decir, contienen su propia fuente de alimentación, llevan a cabo procesos lógicos y tienen la capacidad de detectar y puentear fallas que ocurran en los segmentos del anillo y entre concentradores.

#### OPERACION NORMAL

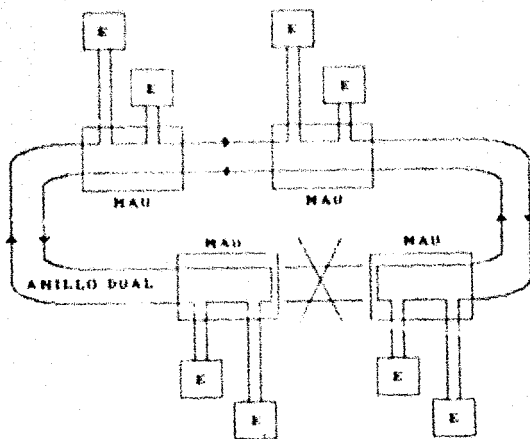


E - ESTACION DE TRABAJO

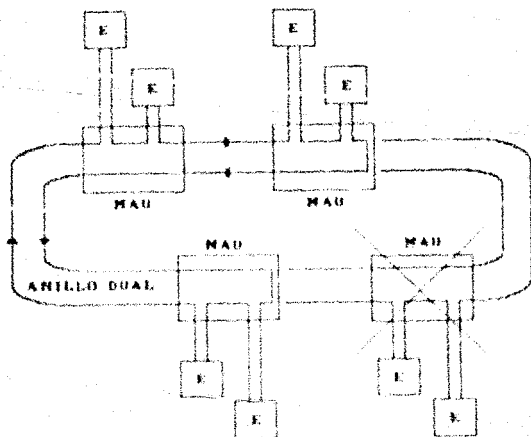
MAU = CONCENTRADOR

La dualidad de anillos (un segundo anillo como respaldo) es parte de la estructura de la FDDI y del proyecto IEEE 802.5. Este concepto utiliza dos anillos para interconectar los concentradores, un reloj maestro (*clockwise*) y un subcontador del reloj maestro (*counter-clockwise*). En caso de que ocurra una falla, el concentrador sobre algún lado de la liga rota se volteará de regreso (*wrap-back*), reconfigurándose internamente para eliminar la liga que falló. De la misma manera se ejecuta una reconfiguración cuando algún concentrador falla.

## FALLA DE UNA LIGA



## FALLA DE UN CONCENTRADOR



La configuración de Estrella Alambrada, tiene ventajas adicionales:

- Proporciona puntos centralizados en la instalación de la red para manejo de reconfiguraciones
- Las estaciones cuentan con gran movilidad dentro del lugar donde fueron instaladas
- El cableado se encuentra segmentado, en vez de ser un cable continuo, lo que le permite entremezclar diferentes medios de transmisión. Por ejemplo, par trenzado se puede utilizar para conectar las estaciones al concentrador y fibra óptica para conectar concentradores
- Por muy grande que sea el tiempo en que una estación permanezca en estado pasivo, no insertada en el anillo, el lóbulo se conecta a sí mismo de regreso, lo que le permite efectuar pruebas de chequeo ella misma antes de que se inserte en el anillo, permitiéndole detectar si la falla se localiza en sus propios componentes o en el cableado que la une a los concentradores, y le es posible quitarse ella misma del anillo.

### 3.3.2 Medio de transmisión

El medio de transmisión que prevalece en las LAN's *Token Ring*, es el par de cobre trenzado, sin embargo se ha incrementado el uso de fibra óptica. La degradación de los datos es balanceada debido a que ambos cables tienen la misma impedancia, y gracias también a que cada hilo se encuentra aislado antes de trenzarse lo que reduce de manera significativa la interferencia debida al *crosstalk*. El par trenzado proporciona una transmisión costable a 4 Mbps (IEEE 802.5), aunque según la distancia se puede utilizar para obtener velocidades de 16 Mbps.

La FDDI se ha convertido en el punto focal para la aplicación de tecnología óptica en el ambiente de redes de área local.

Cada liga punto a punto en las redes FDDI compromete a un cable dual de fibra óptica terminado con un conector duplex estándar. El diámetro de la cubierta de la fibra se encuentra especificado a 125  $\mu$ m y el núcleo de 85 o 62.5  $\mu$ m.

### 3.3.3 Modo de transmisión

La técnica de transmisión de datos que emplea la red *Token Ring* es banda base (*Baseband*) o sea que en la transmisión emplea un solo canal; así cuando una estación de trabajo toma su turno para transmitir cuenta con todo el ancho de banda para realizarlo.

### 3.3.4 Codificación

Los datos generados por una estación deben ser codificados para su transmisión en el anillo. Mientras que el IEEE 802.5 especifica el código *Manchester Diferencial* para codificar, la FDDI emplea la codificación 4B/5B que aunque es más compleja aprovecha de mejor manera el ancho de banda.

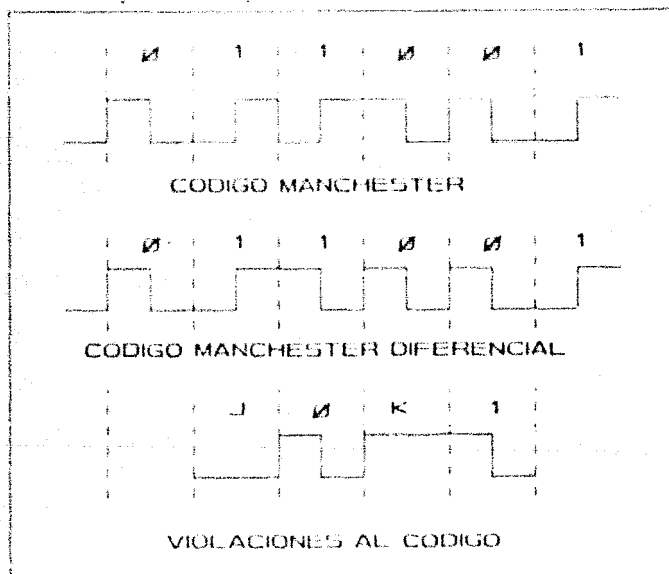
El código *Manchester Diferencial* se caracteriza por la transmisión de dos señales por bit. En el caso de un Uno o Cero binario un elemento de la señal de una polaridad se transmite a la mitad de tiempo de un bit seguido por la transmisión de un elemento de polaridad opuesta. Esto tiene dos ventajas:

- La señal resultante no tiene componente de DC y puede acoplarse inductivamente.
- La transición de medio bit conduce información inherente al tiempo (*inherent timing information*).

Los unos son diferentes de los ceros en el límite del bit principal. Un valor de uno no tiene señal de transición en el límite del bit, mientras

que un valor de cero si lo tiene. En la decodificación de la señal solo se detecta la presencia o ausencia de la señal de transición y no la polaridad actual, de este intercambio los dos cables del par trenzado no introducen errores en los datos.

Se pueden producir violaciones al código si no ocurren transiciones a la mitad del tiempo de duración del bit. Las violaciones al código se pueden provocar intencionalmente, por ejemplo, para marcar el comienzo y el fin de un *frame* de datos.



En el FDDI la información en el medio se transmite en 4 de 5 grupos codificados, a cada grupo codificado se le llama símbolo. De un conjunto de 32 símbolos, 16 son símbolos de datos, cada uno representa 4 bits de datos binarios ordenados, 3 se utilizan como delimitadores de comienzo y fin, 2 son indicadores de control y 3 para señalar el estado de la línea. Los 8 símbolos restantes no se utilizan. Los símbolos se transmiten en 'sin retorno a cero invertido' (NRZI).

La codificación por grupos 4B/5B es eficiente en un 80% , por ejemplo, en la FDDI a una velocidad de trasmisión de 100 Mbps envía una velocidad de señales de 125 MBd. El empleo del código *Manchester* diferencial en este caso requeriría de componentes ópticos y lógicos *front-end* a 200 MHz lo que se traduciría en un incremento muy considerable en costo y complejidad.

SÍMBOLOS DE DATOS	
GRUPO DE 5 SÍMBOLOS DE 5 DATOS DE 4 BITS DE 5 BITS	
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

SÍMBOLOS DE CONTROL	
Idle	11111
J	11000
K	10001
T	01101
R	00111
S	11001
QUIET	00100
HALT	00100

### 3.3.5 Sincronía

La sincronización es un problema clave técnico en el diseño de cualquier sistema de anillo. Entre varias técnicas dos son las que adoptaron los estándares de la IEEE 802.5 y del FDDI.

Los anillos construidos en base al IEEE 802.5 emplean una técnica de reloj centralizado. En una operación normal una estación en el anillo se designa como monitor activo. El monitor juega un papel muy importante en la supervisión del anillo, además proporciona un

reloj para el anillo maestro. Todas las demás estaciones del anillo se acoplan en fase y frecuencia al monitor.

La velocidad media del anillo la controla la estación que funciona como monitor activo; segmentos del anillo pueden instantáneamente operar a velocidades poco diferentes de la frecuencia del oscilador maestro. El efecto acumulativo de estas pequeñas variaciones en la velocidad son suficientes para causar variaciones de unos cuantos bits en la 'latencia del anillo'. A menos que la latencia del anillo permanezca constante los bits deberán suprimirse o aumentarse.

Para mantener la latencia del anillo constante el monitor cuenta con un *buffer* elástico. Si la señal recibida en la estación monitor activo es un poco más rápida que el oscilador maestro, el *buffer* se llenará hasta que sobren bits. Si la señal recibida es un poco más lenta el *buffer* será vaciado para agregar bits.

La mayor ventaja que tiene un reloj centralizado es que minimiza la latencia total del anillo y así permite el uso de un protocolo token como protocolo MAC en el IEEE 802.5 el cual, por razones de efectividad, requiere que la latencia del anillo sea muy pequeña.

El protocolo de control de acceso al medio de la FDDI, si se encuentra debidamente ajustado, es insensible a la latencia del anillo, de aquí que no es crucial diseñar un esquema de reloj para minimizar la latencia, por lo que la FDDI emplea un esquema de sincronización que cuenta con mayor latencia pero que es más fácil de implementar a altas velocidades de transmisión.

En la FDDI, la información se transmite entre dos estaciones asincrónicas; esto es, que cada estación tiene su fuente de reloj autónoma, para transmitir o repetir información en el anillo. Este tipo de operación requiere del uso de un *buffer* elástico en cada estación. La información se amarra (en reloj) dentro del *buffer* a la velocidad del reloj de la señal que se recupera, pero en el momento de salir se ajusta al reloj autónomo correspondiente. Un preámbulo que precede a cada frame habilita al *buffer* a ser reiniciado para la prioridad de su medio punto (*mid-point priority*) para la recepción del



*frame*. Esto incrementa o decrementa la longitud del preámbulo. Con un *buffer* elástico de 10 bits y un reloj transmisor de 0.005 por ciento de exactitud, los *frames* mayores a 4500 bytes pueden transmitirse sin exceder los límites de la elasticidad del *buffer*.

### 3.3.6 Protocolo *Token*

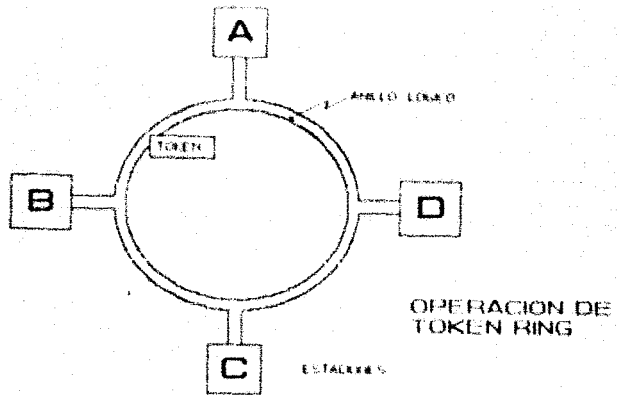
La información en un anillo *Token Ring* se transfiere secuencialmente de una estación activa a la siguiente. La estación que tiene acceso al medio transmite información sobre el anillo. Todas las demás estaciones repiten cada bit que reciben. La estación direccionada como destino copia la información mientras pasa. Finalmente, la estación que ha transmitido la información se quitará del anillo. Esta función de *stripping* difiere de un esquema a otro. En IEEE 802.5 la estación que transmite mantiene el anillo abierto hasta que su *frame* completo ha regresado. De cualquier modo en FDDI la dirección fuente del *frame* tiene que concordar con su propia dirección.

Una estación gana el derecho a transmitir cuando detecta un *token* que pasa por el medio. El *token* es una señal de control compuesta de una secuencia de señalización única que cualquier estación puede capturar. Capturar el *token* en IEEE 802.5 significa modificarlo para convertirlo en una secuencia de comienzo de *frame* (*start-of-frame*) y entonces agrega los campos apropiados de control y de dirección, de información del usuario, secuencias de chequeo y delimitadores de fin de *frame*.

En la FDDI, capturar el *token* significa la recepción completa de un *token* y removerlo del anillo, seguido por la transmisión separada del *frame* de datos. La captura del *token* es obviamente menos eficiente que la correspondiente operación IEEE 802.5, pero es más fácil de implementar a velocidades de transmisión altas.

Después de que se completa la transmisión de su información, la estación genera un nuevo *token* el cual proporcionará a otra estación la oportunidad de transmitir a través del anillo.

Los protocolos FDDI y IEEE 802.5, difieren en lo que respecta a la estrategia para la generacion del *token* (la trasmision de un *token* siguiendo al *frame* y prioridades).



### 3.3.7 Monitoreo del Anillo

La correcta operación de un anillo depende de la integridad del *token*. Por lo tanto, en cualquier red *Token Ring*, se proporcionan mecanismos para la detección de errores y mecanismos para su recuperación, para restablecer la operación de la red. Por ejemplo, los resultantes de la inserción y remoción del anillo que se traducen en errores de transmisión o errores pasajeros en el medio que ocasionan que el anillo se desvíe de su operación normal.

*Token Ring IEEE 802.5* utiliza una función de monitoreo del anillo que se ejecuta en una estación con la capacidad de dar respaldo (*back-up*) en todas las demás estaciones conectadas a la red. La función de monitoreo trabaja de la siguiente manera: las estaciones en el anillo seleccionan una estación que va a funcionar como monitor activo, esta es también la estación que funcionará como reloj maestro. El resto de las estaciones trabajarán como monitores *standby*.

El monitor activo cuidará la integridad del anillo y del *token*, al activar procedimientos de recuperación cuando sea necesario.

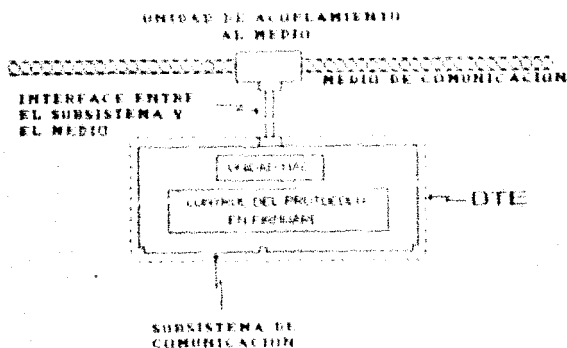
En la FDDI, las funciones de monitoreo se distribuyen a través de todas las estaciones del anillo; como no necesita de un reloj maestro centralizado, tampoco requiere de un monitor centralizado. Cada estación continuamente monitorea el anillo para condiciones inválidas, así como inactividad o actividad incorrecta, lo que requerirá reiniciar el anillo.

### 3.3.8 Unidades de Acoplamiento

La conexión entre el medio físico y la estación de trabajo se realiza a través de dispositivos llamados unidades de acoplamiento, adaptadores del anillo o interfaces de red.

Las funciones asociadas con la manipulación del *token* y la transmisión de datos se distribuyen en cada estación de la red.

La tecnología VLSI hace posible delegar una gran porción de sus funciones de comunicación al adaptador del anillo que existe en cada estación, y libera al dispositivo de realizar esta función. El adaptador maneja las funciones básicas de transmisión, incluso el reconocimiento de *frames*, generación de *token*, decodificación de la dirección, chequeo de errores, almacenamiento temporal de *frames* y la detección de fallas en la línea. También se encarga de las tareas de control de acceso al medio (Unidad MAC)



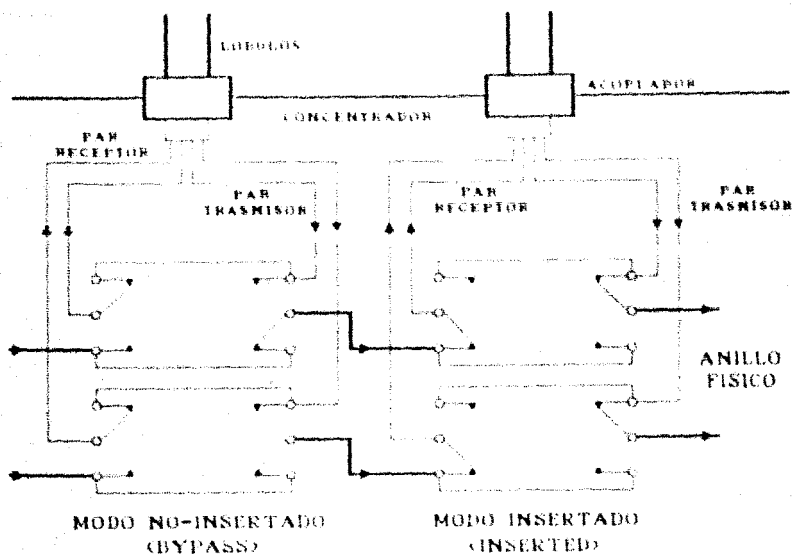
Las unidades de acoplamiento contienen a la unidad MAC y a los protocolos de control como módulos de *firmware*.

El CONCENTRADOR cuenta con un conjunto de relevadores y elementos electrónicos para manejar y recibir señales del medio físico. Los relevadores se encuentran retirados cuando una estación de trabajo está apagada, a pesar de estar conectada al medio físico; a este estado se le conoce como *by pass mode*.

La inserción de una estación de trabajo al anillo se controla a través de su propia unidad MAC, esta activa los relevadores de la unidad de acoplamiento y cuando esto ha sucedido ya pueden circular señales a través de la unidad MAC. A este estado de operación se le llama *insert mode*.

La conexión de los relevadores proporciona a la unidad MAC una forma de detectar fallas de circuito abierto o corto circuito en los

pares de cables para las señales de transmisión o recepción. También en el estado *by pass*, la unidad **MAC** puede realizar pruebas de diagnóstico.



La unidad **MAC** es la responsable de las funciones de codificación y decodificación de la información, detección de errores y la operación de los algoritmos de control de acceso al medio.

Además la unidad **MAC** cuenta con un reloj interno, con el cual se sincronizan las funciones de monitoreo de control, codificación y decodificación de la información. Cada estación de trabajo del anillo sincroniza su reloj interno con los otros relojes internos del anillo. Al sincronizarse los relojes internos se forma un reloj maestro. La ventaja de contar con un reloj maestro centralizado es que se minimiza el tiempo de espera en el anillo.

El tiempo de espera en el anillo se refiere a asegurar que el tiempo mínimo para la propagación de señales se considera de acuerdo al retardo de éstas. Este caso se presenta cuando el permiso de uso del medio circula constantemente alrededor del anillo y ninguna estación requiere usarlo. Se puede decir que las estaciones se encuentran en un estado de espera, lo que puede originar que el anillo pierda su sincronía. El anillo entrara a un estado latente de acuerdo al esquema de monitor activo para prevenir este problema.

Además, la unidad MAC cuenta con un circuito PLL ( *Phase-Locked Loop* ), junto con el reloj interno para llevar el control de la frecuencia y fase de las señales codificadas.

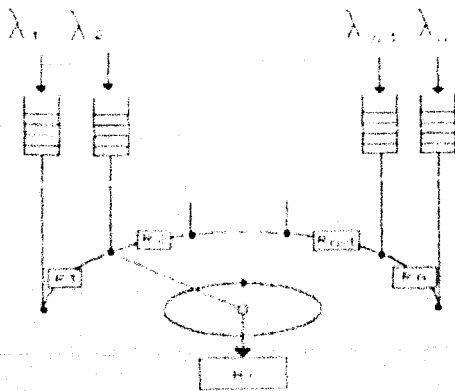
### 3.4 Modelo de Colas de la Operación Básica de Token-Ring

El principio del protocolo *token* se modela a través de un sistema de colas, en el que

- Las estaciones activas se representan por sus colas a transmitir
- Estas colas se atienden de una manera cíclica simbolizado por un switch rotatorio el cual representa el *token*.
- El tiempo que se necesita para pasar el *token* de una estación ( $i$ ) a otra estación ( $i+1$ ) se representa a través de una constante de retardo ( $\tau_i$ ), correspondiente al tiempo de retardo de la propagación de las señales entre las estaciones ( $i$ ) e ( $i+1$ ) (aproximadamente de 5  $\mu$ s por Km de cable) más la latencia causada en la estación ( $i$ )

El tráfico generado en la estación ( $i$ ) se caracteriza por

- un proceso de llegada de paquetes (*packet arrival process*) con tasa  $\lambda_i$
- y una distribución del tiempo de transmisión de los paquetes (*packet transmission-time distribution*)  $H_i$  con media  $h_i$  y un segundo momento  $h_i^2(2)$ , lo que representa el tiempo de servicio (*service time*).



La longitud del tiempo con que cuenta una estación para transmitir cuando tiene posesión del *token* se controla a través del tiempo de posesión del *token* (*token-holding timer*). Un tiempo amplio de posesión proporcionará un tipo de servicio exhaustivo, en el que cuando una estación posee el *token* transmite todos los frames que tenga encolados en ese momento. Con un tiempo corto se puede proporcionar un tipo de servicio no-exhaustivo, donde solo se puede transmitir un paquete por *token*.

Existe una gran variedad de modelos de servicio cíclicos. Los diferentes modelos difieren básicamente en número de *buffers*, la disciplina de servicio (exhaustivo o no), y en la manera de asumir las llegadas.



---

## 4. PROTOCOLO DE CONTROL DE ACCESO AL MEDIO

---

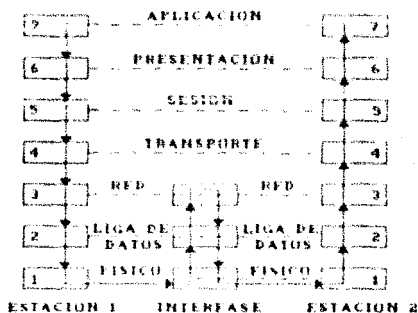
## 4. PROTOCOLO DE CONTROL DE ACCESO AL MEDIO



### 4.1 INTRODUCCION

Como se menciono anteriormente el sistema de comunicación que forman las redes de computadoras se encuentra organizado en 7 niveles jerarquicos, donde cada nivel realiza funciones especificas.

Cada nivel cuenta con un proceso que lo comunica con su correspondiente dentro de otra estación.



La información que va de una aplicación a la otra debe pasar por sus niveles hacia abajo y recorrer los siguientes hacia arriba. Únicamente el nivel físico mantiene una relación directa entre las estaciones.

El nivel de liga de datos es de vital importancia para que el intercambio de datos sea transparente para ambas aplicaciones.

Por lo tanto, en el presente capítulo se detalla el protocolo del nivel de liga de datos empleado en *Token Ring*. Y además se hace un análisis de su eficiencia tanto en IEEE como en FDDI.

## 4.2 PRINCIPIO DE OPERACION DEL PROTOCOLO DE CONTROL DE ACCESO AL MEDIO

El principio de operacion de la comunicacion entre las estaciones de trabajo de la red *Token Ring* se simplifica de la siguiente manera:

- Cada equipo terminal de datos (estacion o nodo) que desea transmitir informacion debe esperar a la llegada del *token* (permiso de transmision).
- Cuando recibe al *token*, se inicia la transmision de la informacion, convirtiendo al *token* en un *frame* (informacion a transmitir), donde incluye las direcciones origen y destino. Este *frame* es repetido por todas las estaciones activas en el anillo hasta que regresa a la estacion origen, donde de manera simplificada se presenta a una red *Token Ring* con varios de los componentes necesarios para conectar una estacion de trabajo al medio fisico.

La forma de controlar el acceso al medio de comunicacion es a traves del uso de un "permiso de acceso" al cual se le conoce como *token* de control.

Una estacion de trabajo solo puede transmitir un *frame* (Unidad de informacion que se transmite a traves de un enlace de datos) cuando tiene la posesion del *token*, despues de transmitir el *frame* la estacion de trabajo pasa el *token* a la siguiente estacion para que esta pueda acceder el medio.

La secuencia de operación será la siguiente:

- Primero se establece un anillo lógico, el cual enlaza a todas las estaciones de trabajo conectadas al medio físico y se crea un solo *token* de control.
- El *token* pasa de una estación de trabajo a otra alrededor del anillo lógico hasta que lo recibe una estación que este esperando enviar uno o varios *frames*.
- La estación de trabajo que espera, envía su *frame* y después de esto pasa el *token* de control a la siguiente estación del anillo lógico.

Para prevenir problemas, el monitoreo marca las bases para la iniciación y recuperación de la conexión del anillo lógico o *token* perdido, en caso de falla. El monitoreo es responsabilidad de todas las estaciones conectadas y activas al medio.

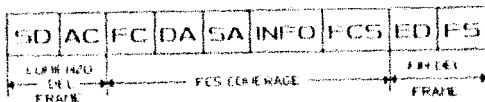
El medio físico no necesariamente tiene que estar conectado de acuerdo a la topología de anillo, el *token* también puede usarse para controlar el acceso al medio en una red con topología de canal (*bus*).

Cuando se trabaja con un anillo físico, la estructura lógica del anillo es igual a la física, además el paso del *token* sigue el mismo orden de las estaciones conectadas físicamente al anillo. Una característica del protocolo de control del *token* es la posibilidad de asociar prioridad al *token* para agilizar la transmisión.

### 4.3 Estructura del FRAME.

Existen dos tipos de estructuras básicas para los formatos de transmisión en *Token Ring*: Uno para el *token* de control y otro para el *frame*.

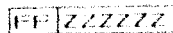
- El *token* de control es el que establece cual estación de trabajo es la que tiene derecho a transmitir y también es el que constantemente esta pasando de una estación a otra.
- El *frame* lo utilizan las estaciones de trabajo para enviar información de control de acceso al medio o datos al anillo.



CONTROL DE ACCESO (AC)



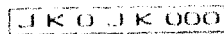
CONTROL DEL FRAME (FC)



FRAME STATUS (FS)



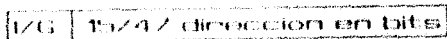
DELIMITADOR DE INICIO (SD)



DELIMITADOR DE FIN (ED)



DIRECCIONES FUENTE Y DESTINO (SA/DA)



### 4.3.1 Descripción de los campos de ambos formatos

El delimitador de inicio (SD) y el delimitador de fin (ED) son secuencias especiales de bits empleadas para asegurar la transparencia de datos. La codificación de bits se realiza por medio del método *Manchester* diferencial, a excepción de ciertos bits seleccionados en los delimitadores SD y ED.

Los bits J y K de estos delimitadores se alejan de las reglas propuestas por el método *Manchester* diferencial, estos símbolos (J,K) se emplean para representar niveles constantes para bits completos en un periodo. El símbolo J tiene la misma polaridad que su predecesor mientras que el símbolo K tiene la polaridad opuesta a su predecesor. De esta manera la recepción puede detectar el inicio y el fin de cada *token* o *frame* transmitido independientemente de su contenido o longitud.

En el delimitador de fin solo los primeros seis símbolos se emplean para indicar el fin de un *frame*. Los otros dos bits, I y E, tienen otras funciones.

- En un *token*, ambos bits I y E tienen un valor de 0.
- En un *frame* el bit I indica que se trata del primer *frame* (o inmediato) de una secuencia (cuando I = 1) o el último o único *frame* (cuando I = 0).
- El bit E se emplea para propósitos de detección de errores. La computadora origen le da un valor de 0, pero si alguna computadora detecta un error al momento de recibir o repetir el *frame*, el bit E toma el valor de 1, esto para indicar a la computadora origen que se ha detectado un error.

**EL campo de control de acceso (AC) contiene:**

- bits de prioridad
- bits de *token* y monitoreo
- bits de reservación.

Y como su nombre lo indica se utiliza para controlar el acceso al anillo.

Cuando se trata de un *token*, los bits de prioridad (PPP) indican cuales estaciones pueden utilizarlo para transmitir o recibir de acuerdo a la prioridad del *token*.

El bit del *token* (T) discrimina entre un *token* y un *frame* (0 indica *token* y 1 indica *frame*)

El bit de monitoreo (M), se altera para prevenir que un *frame* circule alrededor del anillo continuamente.

Los bits de reservación (RRR) indican la prioridad de la estación.

**El campo de control del *frame* (FC) define el tipo de *frame*:**

- de Control de Acceso al Medio **MAC**
- o de **Información**
- y tambien tiene ciertas funciones de control.

Si los bits de tipo de *frame* (F) indican que es

- un *frame* **MAC**, todas las estaciones de trabajo en el anillo lo interpretaran y actuaran de acuerdo a los bits de control (Z)
- si se trata de un *frame* de **INFORMACION**, los bits de control seran interpretados por las estaciones de trabajo como direcciones destino

La dirección origen (SA) y la dirección destino (DA) pueden variar entre 16 bits y 48 bits de longitud.

El campo DA identifica a una o varias estaciones de trabajo, a las que se dirige el *frame*. El primer bit de este campo indica si se trata de una dirección individual (0) o una dirección de grupo (1); la dirección individual identifica a una sola estación de trabajo en un anillo, mientras que la dirección de grupo se utiliza para enviar el *frame* a múltiples estaciones de trabajo. Además si todos los bits del campo DA son unos (1), se le conoce como una dirección global (address broadcast) e indica que el *frame* será transmitido a todas las estaciones de trabajo del anillo.

El campo de información (INFO) se utiliza para enviar los datos de información (o información adicional) de control cuando se envía un *frame* MAC. No existe una longitud máxima específica para este campo, en la práctica este se limita de acuerdo al máximo tiempo que una estación de trabajo toma para transmitir el *frame* (por ejemplo puede tener como tamaño máximo 132 bytes).

El campo de revisión de secuencia del *frame* (FCS) se genera de acuerdo al método CRC (Cyclic Redundancy Check) con un polinomio generador de 32 bits. Con el FCS se revisan el campo de control del *frame* (FC), los campos de dirección origen y dirección destino (DS y SA), el campo de información (INFO) y el mismo campo de revisión de secuencia del *frame* (FSC). Este campo tiene una longitud de 4 bytes.

Finalmente tenemos el campo de estado que como su nombre lo indica proporciona el estado del *frame* (FS). Este campo se divide en dos partes:

- el bit de reconocimiento de dirección (A)
- y el bit de copia del *frame* (C).

Ambos bits (A y C) toman el valor de 0, en la estación de trabajo que origina el *frame*. Si el *frame* lo reconoce una o más estaciones de trabajo en el anillo, la o las estaciones de trabajo dan al bit A el



valor de 1. Si el *frame* se copia, el bit C toma el valor de 1. De esta forma la estación de trabajo original puede determinar si la o las estaciones de trabajo direccionadas, no existen o están apagadas, si están activas pero no copiaron el *frame* o están activas y copiaron el *frame*.

A	C	ESTADO
0	0	no reconocido, no copiado
0	1	no reconocido, copiado
1	0	reconocido, no copiado
1	1	reconocido, copiado

#### 4.4 Trasmisión y Recepción de *frames*

##### 4.4.1 Trasmisión

Cuando se requieren los servicios de transmisión de datos (los cuales deben incluir la prioridad como parámetro), estos se encapsulan de acuerdo al formato estándar por la unidad de control de acceso al medio (MAC). Entonces la unidad MAC espera hasta recibir un *token* con una prioridad menor o igual a la del *frame* armado.

Por lo que, si un sistema emplea múltiples prioridades, debe existir un procedimiento que asegure que todas las estaciones de trabajo tengan la misma oportunidad de transmitir sus *frames*. Este trabajo se realiza de la siguiente manera:

Después de armar un *frame*, se espera a recibir un *token* apropiado (esto es, un *token* con menor o igual prioridad al del *frame* que está esperando), cada vez que un *token* o *frame* con mayor prioridad se transmite en el anillo, la unidad MAC lee el valor de los bits de reservación del campo AC (RRR). Si la prioridad es mayor a la que se espera, los bits de reservación no se alterarán. Si la prioridad es menor, la unidad MAC reemplazará a los bits de reservación por el valor actual de la prioridad del *frame* que espera. Entonces se asume que no existen *frames* con prioridades mayores esperando a ser transmitidos, por lo que el *token* se enviara hacia el usuario con esta

prioridad. La unidad **MAC** espera hasta detectar que la prioridad del *token* sea igual a la del *frame* que espera ser transmitido, cuando esto sucede el *token* se transforma en un *frame*.

Cuando la transmisión del *frame* comienza, la unidad **MAC** ya no tiene *token* que repetir y se detiene, permitiendo así que circulen por el anillo el o los *frames* necesarios. Además, los bits **A** y **C** del campo **FS**, determinan si el o los *frames* se han copiado o ignorado. Entonces se genera un nuevo *token*, para permitir que otra estación de trabajo gane el acceso al anillo.

Enviando más de un *frame* es posible determinar el tiempo total entre la transmisión de un *frame* y otro, a esto último se le conoce como tiempo de posesión del *token* (*Token Holding Time*).

#### 4.4.2 Recepción

Cuando se repiten las señales en el anillo, la unidad **MAC** junto con cada estación de trabajo activa, detectan el inicio de cada *frame* al reconocer la secuencia especial de inicio del *frame* (**SD**). Este determina si el *frame* debe repetirse o copiarse.

Si se identifica un *frame* **MAC** (a través de los bits **F**), el *frame* se copiará, los bits **C** se interpretarán y se modificarán si fuese necesario.

Si se identifica un *frame* de información y el campo de **DA** indica que se trata de la dirección individual o de grupo, el contenido del *frame* se copiará en un almacenamiento temporal antes de procesarse.

En cada caso, los bits **A** y **C** en el campo de estado del *frame* se ajustarán para ser repetidos.

## 4.5 Control y Administración del anillo

### 4.5.1 Operaciones de Prioridad

La prioridad asignada a un *token* por la unidad **MAC** después de ser totalmente transmitido, se determina mediante el siguiente mecanismo:

- (1) Los *frames* con mayor prioridad se transmiten siempre en el anillo.
- (2) Todas las estaciones de trabajo con *frames* en espera tienen la misma prioridad de acceso al anillo.

Las operaciones de prioridad se controlan de acuerdo al uso combinado de los bits **P** y **R** del campo **AC** de cada *frame*. Ambos junto con los elementos de control del anillo forman un mecanismo, el cual asegura que cada estación de trabajo después de incrementar su nivel de prioridad en el anillo, regrese a su nivel original después de la transmisión de un *frame* de prioridad más alta.

Para realizar este esquema, cada unidad **MAC** mantiene dos conjuntos de valores: el primero comprende tres variables **Pm**, **Pr** y **Rr**, y el segundo conjunto de valores consiste en dos pilas (*stacks*) conocidas como pilas **Sr** y **Sx**.

**Pm** especifica el valor más alto de prioridad contenido en cualquier *frame* que espera transmitirse. **Pr** y **Rr** se les conoce como registros de prioridad (*priority registers*) y contienen respectivamente, los valores de los bits de prioridad (**PPP**) y de reservación (**RRR**), obtenidos del campo **AC** del *token* o *frame* transmitido recientemente.

El proceso será el siguiente:

1. A todos los *frames* transmitidos por la estación de trabajo, se les asigna una prioridad en el campo **AC**, igual a la prioridad presente en los servicios de transmisión del anillo **Pr** y al campo de reservación se le asigna un valor de cero.
2. Después los *frames* que esperan transmitirse o tienen una prioridad mayor a la actual del anillo, se transmiten, esto ocurre hasta que la transmisión de otro *frame* no pueda realizarse, o sea, antes que el tiempo de posesión del *token* termine.
3. Cuando el tiempo de posesión termina, la unidad **MAC** genera un nuevo *token* de acuerdo al siguiente criterio:

(1) Si la estación de trabajo no tiene más *frames* esperando con prioridad igual o mayor que la prioridad de los servicios actuales de red, o no tiene un requerimiento de reservación mayor que la prioridad actual:

$$P = Pr \text{ y } R = \text{el valor mas grande de } Rr \text{ o } Pm$$

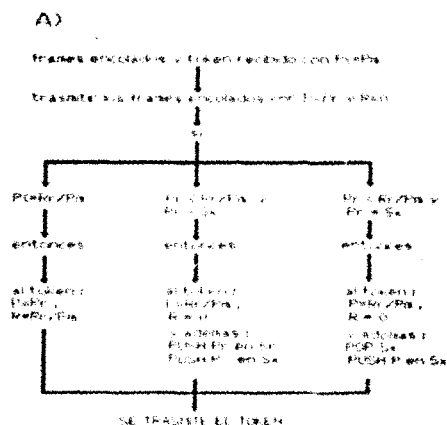
(2) Si la estación de trabajo tiene otro u otros *frames* esperando con prioridad mayor que la actual prioridad de **Pr**, o si el valor actual de **Rr** es mayor que la prioridad actual:

$$P = \text{al valor mas grande de } Rr \text{ y } Pm \text{ y } R = 0$$

Desde el ultimo caso en que la estación de trabajo incrementó efectivamente los niveles de servicio de prioridad en el anillo, ésta se convierte en lo que se conoce como estación de apilamiento (*stacking station*), la cual almacena el valor de los servicios de prioridad del anillo anterior (**Pr**) en la pila **Sr** y el nuevo valor de los servicios de prioridad del nuevo anillo (**P**) en la pila **Sx**.

Estos valores se almacenan bajo la responsabilidad de la estación de trabajo, esto lleva a que la estación de apilamiento lleve el control de la secuencia mas baja, cuando no existan más *frames* para transmitir en ningún punto del anillo con prioridad igual o mayor que el valor de P almacenado en la pila  $S_x$ . También la pila se utiliza como un registro unico esto, por que la estación de apilamiento necesita incrementar los servicios de prioridad del anillo mas de una vez antes de que los servicios de prioridad se regresen a un nivel de prioridad inferior.

Los diferentes valores asignados a los bits P y R del *token* y las acciones de mejoramiento de las dos pilas se resumen en la siguiente figura.



Al contar con la estación de apilamiento, la unidad MAC analiza cada *token* que se recibe, verifica que la prioridad sea igual entre la almacenada en la pila  $Sx$  y los bits  $R$  del campo AC, así se determina si los servicios de prioridad del anillo deben incrementarse, mantenerse o disminuirse. Entonces el nuevo *token* se trasmite con:

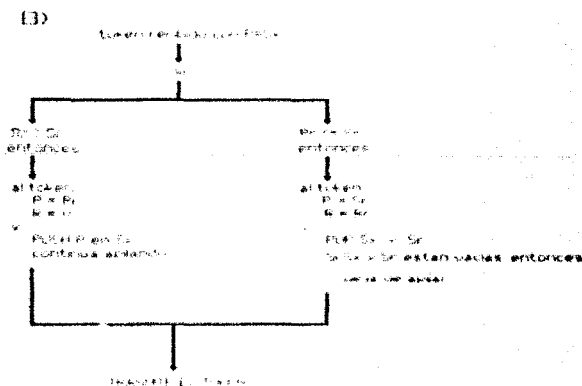
(A) Si el valor de los bits  $R$  es mayor al valor de  $Sr$ , entonces los nuevos servicios de prioridad del anillo  $P$  se introducen a la pila  $Sx$  y la estación de trabajo continua trabajando como estación de apilamiento.

$$P = Rr \text{ y } R = 0$$

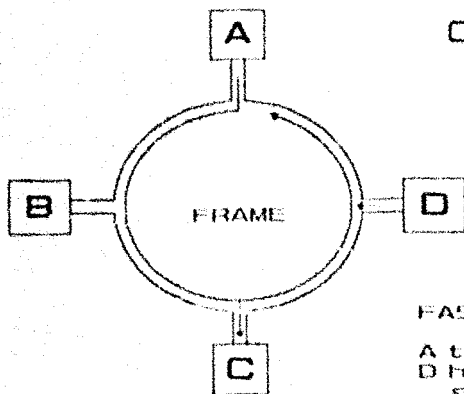
(B) Si el valor de los bits  $R$  es menor o igual al valor de  $Sr$ , ambos valores se encuentran en el tope de las pilas  $Sx$  y  $Sr$ , entonces se sacan de las pilas los valores, y la estación de trabajo deja de ser una estación de apilamiento.

$$P = Sr \text{ y } R = Rr \text{ (sin cambio)}$$

Estas dos últimas operaciones se resumen en la siguiente figura:



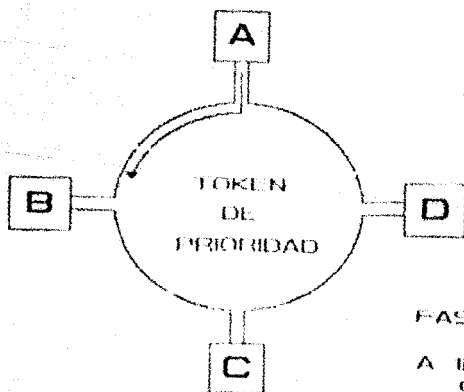
De manera esquemática el proceso se realizara de la siguiente manera :



## OPERACION DE PRIORIDADES

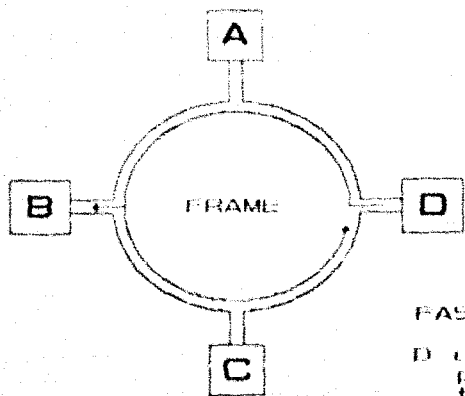
FASE 1:

A transmite a C  
D hace una reserva en  
el frame



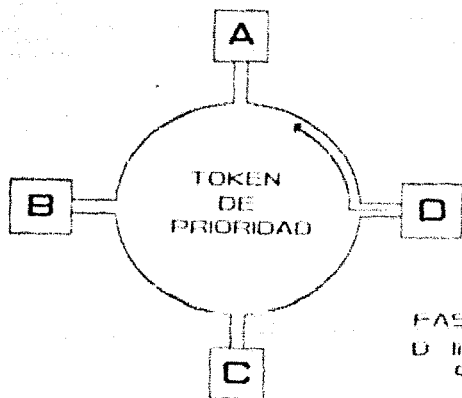
FASE 2:

A libera un token de  
prioridad y obtiene informa-  
cion en el nivel  
de prioridad



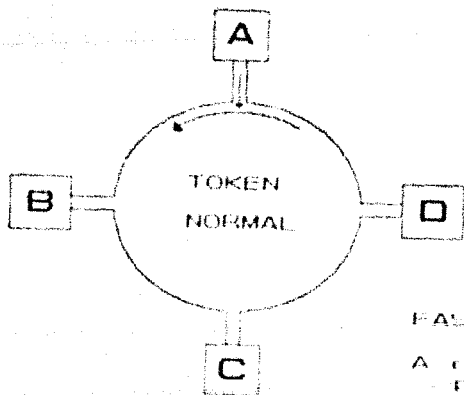
FASE 3:

D utiliza el token de prioridad para transmitir un frame a B



FASE 4:

D libera un token de prioridad



FASE 5:

A detecta el token de prioridad y lo cambia a su prioridad normal



#### 4.5.2 Administración del anillo

Antes de que se transmitan y reciban *frames* y *tokens*, el anillo debe iniciarse. También si una estación de trabajo desea trabajar con la red, debe pasar por un procedimiento de iniciación para asegurar que no interfiere con el correcto funcionamiento del anillo ya establecido. Además durante la operación normal, cada estación de trabajo activa en el anillo debe monitorear constantemente su correcta operación y de ser necesario tome una acción correctiva para tratar de restablecer la correcta operación. A estas funciones se les conoce como "administración del anillo", existen diferentes tipos de *frames* MAC asociados con estas funciones, por ejemplo:

TIPO DE DEBERCIÓN	FRAMA	FUNCION
DAT	DISPLICATE ADDRESS TEST	NO UTILIZA DURANTE EL PROCEDIMIENTO DE INICIALIZACION PARA QUE SE LE PERMITA A UNA ESTACION DETERMINAR QUE NINGUNA OTRA ESTACION DEL ANILLO ESTA EMPLEANDO SU MISMA DIRECCION.
MAP	CLAIMED MONITOR PRESENT	TAMBIEN SE UTILIZA DURANTE EL PROCESO DE INICIALIZACION PARA QUE LA ESTACION QUEVA DETERMINAR LA DIRECCION DE SU MONITOR EN EL RING DEL ANILLO.
AMP	ACTIVE MONITOR PRESENT	ESTE TIPO DE FRAMA SE TRANSMITE DUEMANT CLIENTE INTERACCION DE TOKEN EN EL MONITOR ACTIVO ACTUAL Y CADA ESTACION MONITOREA A SU PAGO.
CT	CLAIM TOKEN	ESTE SE UTILIZA EN EL PROCESO PARA DETERMINAR UN MONITOR MONITOR ACTIVO SI ES QUE EL ACTUAL FALLA.
PRO	PROBE	ESTE SE UTILIZA EL MONITOR MONITOR ACTIVO PARA INICIALIZAR A TODAS LAS ESTACIONES EN ESTADO INACTIVO.
BCN	BEACON	ESTE SE UTILIZA EN EL PROCESO DE REINICIALIZACION (OFF LINE) A S. 4.

Cuando una estación de trabajo desea ser parte del anillo, se establece una secuencia de inicio, primero se debe verificar que no existe otra estación empleando la misma dirección, y segundo, se debe informar quien es la estación de trabajo anterior en el flujo de datos dentro del anillo.

El procedimiento de inicio comienza con la transmisión de un *frame* MAC tipo **DAI** por la estación de trabajo con los bits **A** del campo **ES** iguales a 0. Al recibir cada estación activa del anillo el *frame* **DAT**, se analizará al campo **DA**, verificando su propia dirección, si la estación de trabajo determina que las direcciones son iguales, altera los bits **A** dándoles un valor de 1. Así, si el *frame* **DAT** regresa a la estación original con los bits **A** alterados, esta informa al nivel "administrador de red" y espera su respuesta. Este último determina si la estación de trabajo debe intentar de nuevo su conexión al anillo. Por otro lado si el *frame* **DAT** regresa sin que sus bits **A** hayan sido alterados, continúa la secuencia de inicio, con la transmisión un *frame* MAC tipo **SMP**.

Cuando una estación de trabajo recibe un *frame* **SMP** con valores iguales a 0 en los bits **A** y **C** y además este *frame* es transmitido por la estación de trabajo siguiente, de acuerdo al flujo de información, esta estación almacena en algunos registros del campo **SA** la dirección de la estación que le precede en el anillo. Esto es necesario para determinar y monitorear la estructura del anillo, con el objeto que cada estación conozca quien es la estación anterior en el anillo. Con esto último la fase de inicialización queda concluida.

#### 4.5.3 Monitor activo del anillo

Una vez concluida la secuencia de inicio, las estaciones de trabajo pueden comenzar a transmitir y recibir *frames* y *tokens*. Además las estaciones de trabajo entran a un "estado de alerta" (*standby monitor*) para monitorear constantemente la correcta operación del anillo. Esto se hace para verificar el paso de *tokens* y del *frame* MAC tipo **AMP**, los cuales son periódicamente transmitidos por el monitor activo.

Si los *tokens* o *frames AMP* no son detectados periódicamente, el monitor activo pasa del estado de alerta al estado de espera de *token claim* a *token state*.

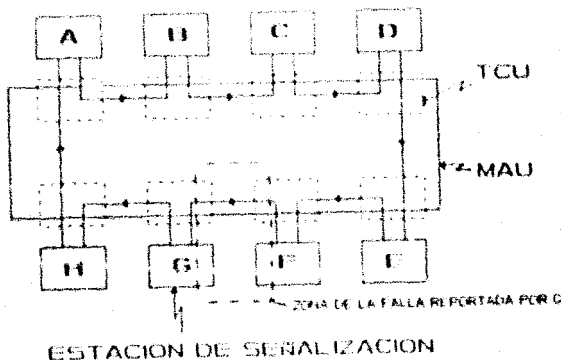
Cuando la estación de trabajo se encuentra en el estado de espera de *token*, continuamente transmite *frames MAC* del tipo CT y revisa el campo SA de cualquier *frame CT* que recibe. Cada *frame CT* transmitido contiene además las direcciones de la estación de trabajo que lo transmite y la de la estación predecesora. Esto para controlar que cada *frame CT* circula satisfactoriamente alrededor del anillo y así restablecer el monitoreo del anillo. Alternativamente si un *frame CT* que se recibe contiene un valor de SA mayor que su propia dirección, significa que otra estación de trabajo ha hecho una llamada anterior al procedimiento de monitoreo, esto causa que la estación de trabajo regrese a su estado de alerta y olvide la llamada que hizo por el *token*.

#### 4.5.4 Señalización (*BEACONING*)

Si ocurre un error serio en el anillo (por ejemplo un cable roto), a cada estación de trabajo se le informa que el protocolo *token* se suspende hasta que la falla sea localizada y reparada; a esto se le conoce como el procedimiento de señalización (*beaconing*). El campo de acción de este procedimiento es el siguiente:

- \* La estación que reporta la falla, a la cual se le conoce como "estación de señalización".
- \* La estación siguiente a la estación de señalización de acuerdo al flujo de información.
- \* El medio físico del anillo entre ambas estaciones.

Para ilustrar lo anterior se tiene el campo de acción que se asume al ocurrir una falla en el medio físico del anillo entre dos estaciones de trabajo.

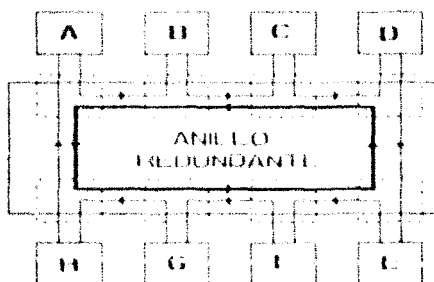


MAU = MÓDULO DE ACCESO AL USUARIO  
TCU = TRÁFICO DE CONTROL DE USUARIO

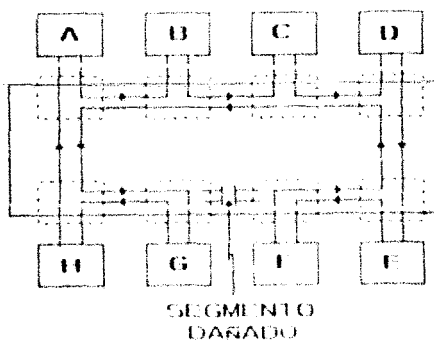
Donde la estación de señalización es la estación G y la estación F es la estación siguiente de acuerdo al flujo de la información. Cuando se detecta la falla, se empiezan a transmitir constantemente *frames MAC* del tipo BCN hasta que cada estación se entera de que existe una falla. Para esto se informa al nivel de administración de la red y la transmisión se detiene. Alternativamente, si un *frame BCN* se recibe con el campo SA igual a la dirección de la estación que lo recibe, la estación entra a un estado de espera de *token*, por el contrario, si el campo SA es diferente de la dirección de la estación, la estación entra a un estado de "monitor activo".

Cuando ocurre este tipo de error se requiere que sea reparado el segmento del anillo que presenta dicha falla para que la transmisión pueda continuar. Una opción que puede proporcionar *Token Ring* es la de utilizar un anillo secundario o anillo redundante cuya dirección de transmisión es opuesta a la del anillo principal.

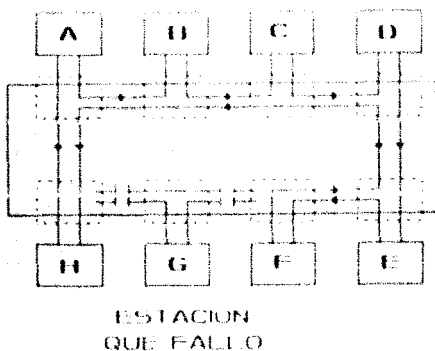
Para mostrar la acción correctiva se tiene:



La unidad de acoplamiento de algunas redes realiza las funciones de aislamiento del anillo en caso de falla. El aislamiento también se puede dar en un segmento del anillo. En resumen, al ser reportada y localizada una falla los relevadores de la unidad de acoplamiento se retraen para aislar la falla detectada. El aislamiento de la falla puede darse solamente en un segmento del medio físico de comunicación o en una estación de trabajo.



donde se puede observar como el anillo redundante no tiene una trayectoria directa hacia la unidad MAC y se emplea únicamente para las funciones de aislamiento



En conclusión, los procedimientos de control de acceso al medio que emplean las redes *Token Ring* son muy complicados comparados con otros. Pero la mayoría de estos procedimientos son ejecutados por controladores de circuitos integrados especialmente diseñados que contienen a la unidad MAC y realizan sus funciones de manera transparente al usuario. Además muchos de los procedimientos de administración del anillo solo son invocados cuando ocurren fallas en el anillo.

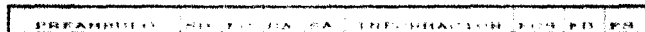
#### 4.6 Diferencias en la FDDI

La FDDI tiene características que la hacen diferir un poco del comportamiento del protocolo de los anillos IEEE 802.5.

##### 4.6.1 Formato del *Frame*

La estructura del *frames* de la FDDI es básicamente la misma del IEEE 802.5, con un delimitador de comienzo, un campo de control

del *frame*, direcciones fuente y destino, un campo de longitud variable para la información, secuencia de chequeo del *frame*, delimitador final, y un campo de estado del *frame*.



- SD - delimitador de inicio
- FC - control del *frame*
- DA - dirección destino
- SA - dirección origen
- FCS - secuencia de chequeo de *frame*
- ED - delimitador final
- FS - estado del *frame*

#### Formato del *frame* FDDI

diferencia con respecto al *frame* del IEEE 802.5 es la presencia de un preámbulo que precede a cada *frame* transmitido (y *token*). El preámbulo lo trasmite la estación fuente con un mínimo de 16 símbolos de relleno. Subsecuentemente las estaciones repetidoras pueden cambiar la longitud del patrón de relleno de acuerdo con los requerimientos de reloj.

La FDDI emplea un esquema de reloj distribuido el cual requiere de la inserción y remoción de símbolos ociosos entre *frames*, dependiendo de la velocidad relativa del reloj de los segmentos del anillo.

Las estaciones repetidoras pueden ver un preámbulo de longitud variable el cual puede ser más corto o más largo que el que originalmente se trasmite. Un *token* FDDI consiste de un preámbulo, delimitador de inicio, campo de control del *frame* y delimitador final. La distinción del *token* y de los diferentes tipo de *frames* se hace por que toman diferentes valores en el campo de control del *frame*.

#### 4.6.2 Protocolo MAC

La FDDI emplea un protocolo *token* el cual permite que la estación que esta transmitiendo pase el *token* inmediatamente después de terminar la transmisión del *frame*. Esto a diferencia del protocolo de la IEEE 802.5 el cual requiere que la estación que esta transmitiendo retarde la numeración de un nuevo *token* hasta que el encabezado del *frame* transmitido sea regresado.

El mecanismo de *prioridad* de la FDDI se designa para proporcionar diferentes clases de servicio que habiliten a la red para que simultaneamente soporte tráfico con diferentes requerimientos de transmisión. El tráfico restante en la FDDI pertenece a la clase asíncrona la cual se subdivide en ocho niveles de prioridad. La clase asíncrona también tiene un modo de *token* restringido el cual puede usarse para reservar temporalmente todo el ancho de banda no utilizado para transmisión sincrónica para un dialogo específico asíncrono.

La FDDI emplea un protocolo *timed token* en el cual, la longitud de tiempo que una estación tiene para transmitir *frames* de una clase dada (tiempo de posesión del *token*) depende del tiempo entre llegadas sucesivas del *token* en una estación que transmite (*token-rotation time*). El protocolo FDDI utiliza un numero de contadores (*timers*) y variables en cada estación para determinar estos tiempos. Asumiendo que todos los tiempos se inician en cero y que terminan cuando han contado hasta alcanzar su tiempo fuente.

Como parte del proceso de inicio del anillo, todas las estaciones negocian un tiempo fuente de rotación de *token* (*target token-rotation time TTRT*). El protocolo garantiza que el promedio del tiempo de rotación del *token* no exceda del TTRT y que el maximo tiempo de rotación del *token* no exceda de  $2 * TTRT$ . Así las estaciones que tienen requerimientos de retardos en transmisión estrictos deben solicitar un TTRT igual a la mitad del maximo retardo aceptado. Al final de la negociación, el TTRT mas corto solicitado llegara a ser el TTRT operativo y se usara para encender la variable *T\_Opr* idénticamente en cada estación.



Un contador de rotación de *token* (TRT) se usa en cada estación para medir el tiempo entre dos llegadas sucesivas del *token* en cada estación. Normalmente, el TRT se reinicia cada vez que el *token* se recibe para medir el tiempo que tardara la siguiente rotación. El TRT terminará si su cuenta hacia  $T_{Opr}$  llegó antes que el *token* regresara a la estación. Cuando el TRT termina, el contador *Late\_Ct* será iniciado en cero, se incrementara y el TRT se reiniciara a cero y continuara el conteo.

Cuando el *token* llegue tarde a una estación (*Late\_Ct*) el TRT no se reiniciará pero si se le permite que continúe el conteo y acumulará así los retardos de la rotación del *token* presente hacia el siguiente tiempo de rotación. El resultado de acumular retardos es que al seguir una rotación del *token* que exceda  $T_{Opr}$  para un tiempo  $A$ , la transmisión asincrónica se restringirá hasta que los retardos se hayan compensado por medio de rotaciones de *token* menores que  $T_{Opr}$  para un total de tiempo  $A$ . Esto asegura que el promedio del tiempo de rotación de *tokens* sea a lo mas  $T_{Opr}$ . Si *Late\_Ct* siempre excede 1 la recuperación de error se iniciara. *Late\_Ct* es reiniciada a cero cada vez que el *token* se recibe.

El tiempo de posesión del *token* (TOKEN-HOLDING TIME *THH*) se utiliza en cada estación para el control del tiempo que el *token* posee para transmitir *frames* asincrónicos. El *THH* se carga con el valor presente del TRT cuando el *token* se recibe a tiempo (*Late\_Ct* = 0) en una estación. Cuando el *THH* alcanza el tiempo umbral de posesión de *token* para un particular nivel de prioridad, el *token* no puede prolongarse para ser usado para transmitir *frames* en el nivel. Las transmisiones ya en progreso se completan cuando el *THH* termina.  $T_{Prnt}(1$  to 8) define el tiempo umbral de posesión de *token* para un nivel de prioridad (n asincrónico). La convención adoptada es que la prioridad incrementa de 1 a 8. Un gran valor de umbral permite mas tiempo para transcurrir del *THH* antes de que el *token* sea pasado. Así que el nivel de prioridad asociado tiene una gran ventana de transmisión y consecuentemente mayor prioridad que un nivel de prioridad con un pequeño tiempo umbral de posesión de *token*. El máximo valor de umbral para cualquier prioridad es  $T_{Opr}$ .

#### 4.7 EFICIENCIA (Performance)

La eficiencia (*Performance*) de una red, es un factor para determinar la productividad de un sistema, determinado por la combinación de diferentes parámetros: como son la disponibilidad, el throughput, y el tiempo de respuesta.

Las medidas básicas del *performance* en términos del protocolo de control de acceso al medio, son:

- **D**: El retardo que ocurre entre la generación de un paquete (frame), que será transmitido por un nodo, y la llegada de su confirmación de recepción exitosa enviada por el nodo destino.
- **S**: El throughput de una red local, o sea el total de información útil transmitida entre nodos en un periodo de tiempo.
- **U**: La utilización del medio de transmisión, o sea la fracción de la capacidad total (**C**) que se está utilizando.

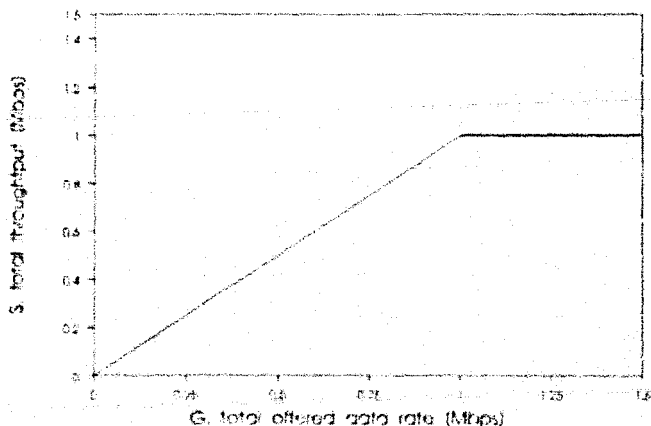
La manera en que estas medidas se relacionan determinan el *performance* de la red, en combinación con el número de dispositivos conectados en la red.

El parámetro **S** por lo regular se normaliza y expresa como una fracción de la capacidad (**C**). por ejemplo, si sobre un periodo de un segundo la suma de los datos transferidos entre dos nodos es de 1 Mb sobre un canal de 10 Mbps, entonces **S** es igual a 0.1, esto es 1/10. El análisis generalmente se realiza en términos del total de bits transferidos, incluyendo los bits de control y direcciones, este análisis aísla los efectos del *performance* directos sobre una sola trayectoria de la red de área local, para determinar el throughput efectivo se debe incluir la trayectoria de respaldo.

Los resultados para  $S$  y  $B$  generalmente se grafican como una función de la carga ofrecida (Offered Load, Offered Data Rate o  $G$ ), la cual es conocida como la carga actual o tráfico demandado por la red de área local. Cabe hacer notar que  $S$  y  $G$  son diferentes.  $S$  es la normalización del total de paquetes de datos exitosamente transmitidos;  $G$  es el total del número de paquetes generados en la red, lo cual incluye paquetes de control (como tokens y frames destruidos que necesitan ser retransmitidos).  $G$  también se expresa como una fracción de la capacidad. Se espera que  $D$  se incremente con  $G$ . A mayor tráfico compitiendo por el tiempo de transmisión se incrementa el retardo para las transmisiones individuales.  $S$  también debería incrementarse con  $G$ , pero existe un punto de saturación a partir del cual la red no puede manejar más carga.

La siguiente figura muestra la situación ideal: La utilización del canal se incrementa para acomodar la carga sobre una carga ofrecida igual a la capacidad completa del sistema; entonces la utilización llega hasta un 100%. Por supuesto, cualquier sobretlujó o ineficiencia causará que el *performance* se vea afectado.

UTILIZACION IDEAL



La gráfica de S & G, muestra la conducta del sistema basado en su carga actual desde un punto de vista global. Pero es más práctico conocer el comportamiento del throughput y el retardo en función del dispositivo que genera los datos que serán puestos en el sistema a los cuales se les conoce como carga de entrada (Input Load o I).

Para ejemplificar la relación que existe entre los parámetros I, S, G, D y U, se simplifica la siguiente tabla, donde se asume que la red tiene una capacidad de transmisión de  $C = 1000$  frames por segundo. Por simplicidad I, S y G se expresan en frames por segundo. Se asume que el 1% de los frames transmitidos se pierden y deben ser retransmitidos, así que, si consideramos una entrada de  $I = 100$  frames por segundo, en promedio un frame por segundo será repetido y además  $S = 100$  y  $G = 101$ . Asumiendo también que la carga de entrada llega en lotes, una vez por segundo, de aquí que en promedio para  $I = 100$ ,  $D = 0.0005$  segundos. La utilización se define como  $S/C$ .

#### RELACION ENTRE LAS MEDIDAS DEL PERFORMANCE

I	S	G	D	U
100.0	100.0	101.0	0.0005	0.101
200.0	200.0	201.0	0.0010	0.202
900.0	900.0	901.0	0.0010	0.901
1000.0	999.0	999.0	0.0010	0.999

Como se puede notar para  $I = 990$  se está utilizando la capacidad completa del sistema ( $G = 1000$ ). Si I se incrementará después de este punto, el sistema no podrá mantenerse. Solamente 1000 frames por segundo serán transmitidos, así que S se mantendrá en 990 y U en 0.99, pero G y D crecerán sin límite, acumulando más y más frames a ser transmitidos. No existe un valor de estado fijo (Steady-State Value).

#### 4.7.1 Velocidad contra distancia

Recordando dos de las principales características de una red de área local, se tiene a la velocidad de transmisión empleada ( $R$ ) y la distancia de la trayectoria de comunicación ( $d$ ). El producto de estos dos términos ( $Rd$ ), el cual puede utilizarse para caracterizar a las redes de área local y es uno de los parámetros más importante para determinar el *performance* de una red.

Para visualizar el concepto de  $Rd$  se debe dividir entre la velocidad de propagación del medio de transmisión, la cual para la mayoría de medios de interés (cable coaxial y par trenzado) es casi una constante cercana a las dos terceras partes de la velocidad de la luz ( $V = 2 \times 10^8$  m/s). Un análisis dimensional de la fórmula  $Rd/V$ , muestra que esto es igual a la longitud del medio de transmisión en bits, esto es, el número de bits que pueden viajar entre dos nodos en cualquier tiempo.

Una manera útil de visualizar esto último, es considerar la longitud del medio comparado con el frame típico transmitido.

La longitud del medio expresado en bits comparado con la longitud del frame típico se denota por  $a$ :

$a$  = longitud de la trayectoria (en bits) / longitud del frame  
o lo que es igual:

$$a = Rd/VL$$

Donde  $L$  es la longitud del frame. Pero  $d/V$  es el tiempo de propagación sobre el medio en el peor de los casos y  $L/B$  es el tiempo que se emplea en transmitir un frame completo sobre el medio. Así que:

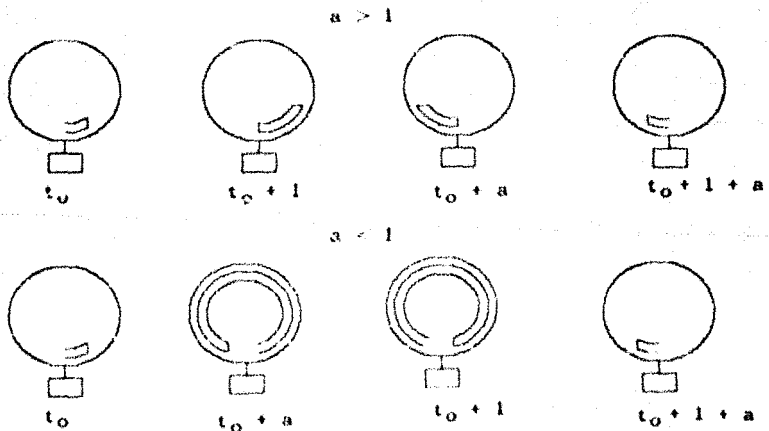
$$a = \text{tiempo de propagación} / \text{tiempo de transmisión}$$

Los valores típicos de  $a$  van desde 0.01 hasta 0.1 para una red de área local.

El parámetro  $a$  determina el límite superior de la utilización de una red local. El cual varía inversamente con respecto a  $a$ .

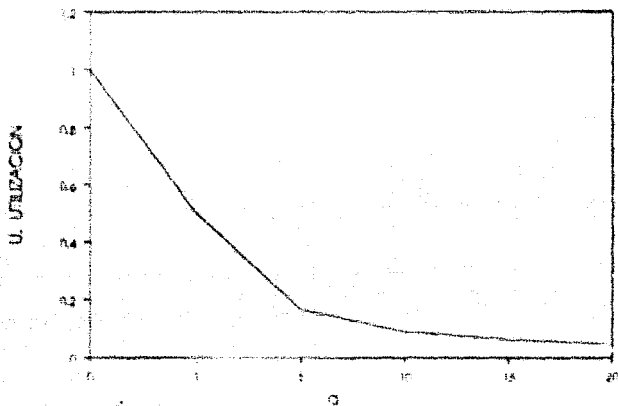
Para visualizar lo anterior asumiremos que una estación transmite y espera a recibir su propia transmisión. Para lo cual se seguirá la siguiente secuencia:

- 1) La estación empieza a transmitir en  $t_0$
- 2) La recepción comienza en  $t_0 + a$
- 3) La transmisión termina en  $t_0 + 1$
- 4) La recepción termina en  $t_0 + 1 + a$



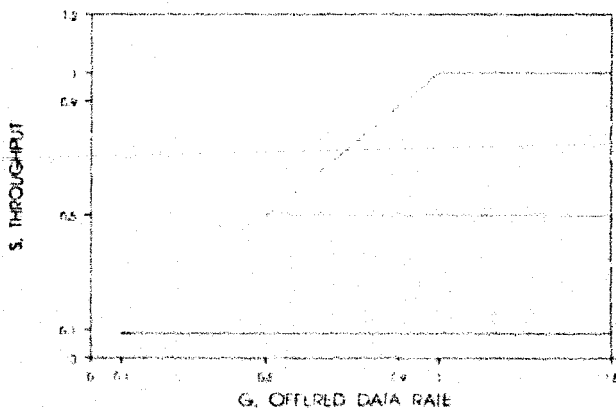
La ecuación  $U = 1 / (1 + \alpha)$  se grafica en la siguiente figura.

UTILIZACION COMO FUNCION DE  $\alpha$



Las consecuencias de  $\alpha$  en el Throughput se muestran en la siguiente gráfica :

EFFECTO DE  $\alpha$  EN EL THROUGHPUT



Cuando la carga ofrecida se incrementa el throughput permanece igual a la carga ofrecida hasta alcanzar la capacidad máxima de la red.

Por lo tanto se puede decir que el límite superior de la utilización o *performance* de una red de área local es

$1 / (1 + a)$ , sin importar el protocolo de control de acceso al medio que se este utilizando

#### 4.7.2 Factores que afectan el *performance*

Los principales factores que afectan el *performance* de una red de área local son:

- \* Capacidad
- \* retardo de propagación
- \* número de bits por frame
- \* protocolo de redes locales
- \* carga ofrecida
- \* número de estaciones activas

Los tres primeros determinan el valor de *a* y se discutieron anteriormente.

El protocolo de redes locales se divide en tres niveles físico, MAC y LLC.

- Al nivel físico no se le considera como un factor relevante
- El nivel LLC le agrega algunos bits de control y administrativos a cada frame
- El nivel MAC tiene un efecto significativo sobre el *performance* de la red



La carga ofrecida y el número de estaciones generalmente se tratan como variables independientes. el análisis se enfoca en determinar el *performance* en función de estas dos variables

Otro factor que no se a tomado en cuenta es el error en la trasmisión, un error en un frame que se trasmite necesita ser retrasmitado, pero como la tasa de errores en redes locales es muy baja no se le considera como un factor relevante

Se han desarrollado muchos analisis sobre el *performance* de varios protocolos para redes de area local, esta sección solo presenta los resultados disponibles en la literatura sobre los protocolos más comunes

#### 4.7.3 Límites del *Performance*

En cualquier LAN existen tres regiones de operacion:

- \* Una región de bajo retardo en la red donde la capacidad es más que la adecuada, para manejar la carga ofrecida.
- \* Una región de gran retardo, donde la red se vuelve un cuello de botella. En esta región, relativamente, se emplea mas tiempo para controlar el acceso a la red y menos en la trasmision de datos, comparado con la región de bajo retardo
- \* Una región de retardo ilimitado, donde la carga ofrecida excede la capacidad total del sistema

Esta ultima region es muy facil de identificar, por ejemplo, para una capacidad de 1 Mbps, con 1,000 estaciones, 200 bytes y un tamaño de frame promedio de 1,000 bits, además si en promedio cada estación genera a una velocidad excedente a un frame por segundo, entonces el total de carga ofrecida excede 1 Mbps. El retardo en cada estación crecerá sin limite.

La tercera región se puede evitar claramente, el problema se encuentra en evitar la segunda región.

La segunda región implica un ineficiente uso de la red. Una red debe operar basada en la carga proyectada y en sus características propias.

El límite de la tercera región es fácilmente identificable, es el límite entre la primera y segunda región el que requiere una técnica especial para poder ser determinado. Si la red opera bajo este límite no causará un cuello de botella, si opera sobre de este límite es una buena razón para considerar un rediseño.

La carga de una red varía con respecto al tiempo y solamente puede ser estimada, como dicha carga no es precisa no es necesario conocer el límite exacto, pero si una buena aproximación, con la cual la red puede ser dimensionada para que la carga ofrecida caiga por debajo del segundo límite.

En el ejemplo anterior, la carga estimada es de 1 Mbps, si la capacidad de la red es tal que el límite es aproximadamente 4 Mbps, entonces el diseñador puede estar seguro de que la red no caerá en un cuello de botella.

#### 4.7.4 Método para calcular los límites de *Throughput* y retardo en función del número de estaciones activas.

Es necesario conocer 4 parámetros:

- **Tidle**: Tiempo promedio en que una estación está desocupada entre intentos de transmisión (no tiene mensajes esperando ser transmitidos).
- **Tmsg**: Tiempo requerido para transmitir un mensaje una vez que se tiene la oportunidad para hacerlo.
- **Tdelay**: Retardo medio del tiempo que emplea una estación desde que tiene frame para transmitir hasta que

ha concluido la transmisión; incluye el tiempo en que estuvo encolado y el tiempo de transmisión.

- **THRU** : Media del total del throughput de mensajes por unidad de tiempo.

Asumiendo que se tienen **N** estaciones activas cada una con los mismos requerimientos de generación de carga. Para encontrar el límite superior sobre el total de throughput hay que considerar el caso ideal en el cual no hay retardos en la cola: cada estación transmite cuando esta lista. De aquí que cada estación alterna entre estar desocupada y transmitiendo con un throughput de  $1 / (Tidle + Tmsg)$ . El máximo throughput posible es justamente la suma de los throughputs individuales de las **N** estaciones.

$$THRU = \frac{N}{(Tidle + Tmsg)}$$

Este límite superior se incrementa cuando **N** se incrementa, pero solo es razonable sobre el punto inicial de la capacidad, el cual puede expresarse como :

$$THRU = \frac{1}{(Tmsg)} \quad (A)$$

El punto de equilibrio entre estos dos límites ocurre en :

$$\frac{N}{(Tidle + Tmsg)} = \frac{1}{(Tmsg)}$$

$$N = \frac{(Tidle + Tmsg)}{(Tmsg)} \quad (D)$$

Este punto de equilibrio define dos regiones de operación. Con el número de estaciones abajo del punto de equilibrio, el sistema no generará suficiente carga para utilizar completamente la capacidad del sistema. Sin embargo, por encima del punto de equilibrio, la red se saturará: será completamente utilizada y no será capaz de satisfacer la demanda de las estaciones conectadas.

Para visualizar el razonamiento de este punto de equilibrio, consideremos que la capacidad de la red es de  $1 / Tmsg$ . Por ejem. si se toma  $1 \mu$  para transmitir un mensaje, la velocidad de transmisión será de  $10^6$  mensajes por segundo. El total del tráfico que están generando las  $N$  estaciones es:

$$\frac{N}{Tidle + Tmsg}$$

Si el tráfico excede la capacidad de la red, los mensajes se comenzarán a acumular y el retardo se incrementará. El tráfico también se puede incrementar a través del número de estaciones (aumentando  $N$ ) o incrementando la velocidad a la cual las estaciones pueden transmitir mensajes (decrementando  $Tidle$ ).

Estas mismas consideraciones permiten también fijar el límite inferior en el retardo:

$$Tdelay = Tmsg \quad (C)$$

considerando que para cualquier carga se tiene la siguiente relación

$$\text{THRU} = \frac{N}{T_{idle} + T_{delay}} \quad (B)$$

Puesto que  $1 / (T_{idle} + T_{delay})$  es el throughput en cada estación, combinando (A) y (B) se tiene que

$$T_{delay} = N T_{msg} / T_{idle}$$

El cálculo del punto de equilibrio se obtiene combinando (C) y la ecuación anterior donde se puede observar que el resultado es el mismo que (D).

Estos límites son las asíntotas de las verdaderas curvas de Retardo y Throughput, el punto de equilibrio delimita estas dos regiones: Por debajo del punto de equilibrio, la capacidad está subutilizada y el retardo es bajo, sobre este punto de equilibrio la capacidad se satura y el retardo crece.

Los otros límites son fáciles de encontrar. El retardo será maximizado si todas las  $N$  tienen un mensaje para transmitir simultáneamente:

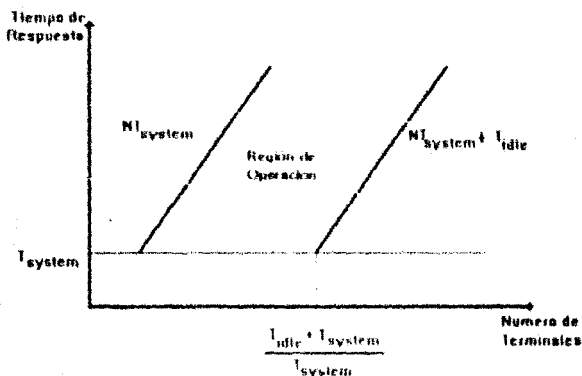
$$T_{delay} = N T_{msg}$$

Combinando con la ecuación (B) se tiene que

$$\text{THRU} = \frac{N}{T_{idle} + N T_{msg}} \quad (B)$$

Estos límites dan una idea de la conducta del sistema. Permite hacer un simple cálculo para determinar si un sistema propuesto se encuentra dentro de los límites razonables. Si la respuesta es no, se habrá ahorrado mucho análisis. De lo contrario se tendrá que realizar un análisis más profundo.

### Región de Operación



Como conclusión se puede establecer que las señales, como en cualquier rama de las comunicaciones, sufren degradaciones que dependen en este caso de muchos aspectos como son:

- distancia entre estaciones
- distancia entre concentrador y estación
- distancia entre concentradores
- tipo de medio físico empleado y característica de impedancia e inmunidad al ruido
- tráfico en cada estación
- etc

Y que influyen de manera significativa en la calidad del servicio que ofrece cualquier tipo de red.

Por lo que cuando se desea planear una red de cualquier tipo, estos son algunos de los aspectos que se deben de tomar en cuenta para su diseño.

Para establecer las tolerancias y límites los fabricantes de equipo de comunicación, de equipo de cómputo, de equipo eléctrico, etc. determinan las especificaciones para cada uno de sus productos.

Para planear y diseñar una red basta con recurrir a las especificaciones y sugerencias propuestas por cada fabricante.

En el caso de *Token Ring* se cuenta con diferentes tablas que ayudan a determinar las distancias máximas entre cualquier dispositivo para mantener la calidad del servicio óptimo, como son las que ayudan a determinar las distancias máximas de transmisión, distancias máximas en segmentos del anillo con repetidores, etc., las cuales también van de acuerdo al tipo de cable empleado para la conexión (ver anexos A y B).

---

## 5. REDES MULTI-ANILLOS



## 5. REDES MULTI-ANILLOS

---



### 5.1 INTRODUCCION

Como cualquier sistema de comunicacion de datos, una red sencilla tiene limitaciones, algunas de las cuales pueden atacarse empleando arquitecturas multi-anillo.

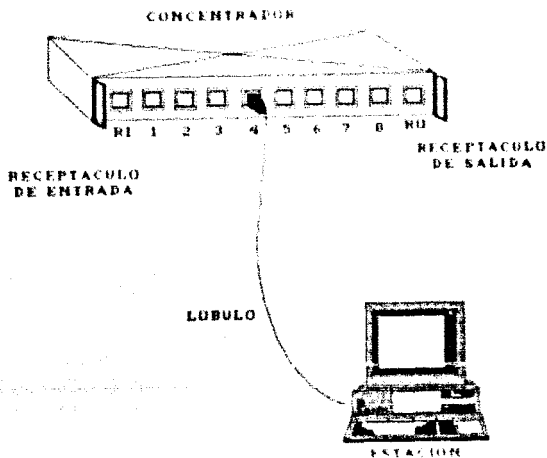
En el presente capitulo se describen algunos componentes de una red multi-anillo, algunos aspectos que hay que tomar en cuenta para su diseño fisico.

Un aspecto interesante es ampliar la red de area local conectandola hacia redes de diferentes tipos para crear estructuras mas complejas pero de gran importancia y que algunas veces ya no entran en el concepto de redes de area local sino en el de redes de areas amplias (WAN). En el presente capitulo se presenta una introducción a este tipo de estructuras.

## 5.2 LIMITES DE LOS ANILLOS SENCILLOS

Los concentradores son básicamente elementos pasivos que proporcionan un anillo principal y uno de respaldo para transmitir señales dentro de la red.

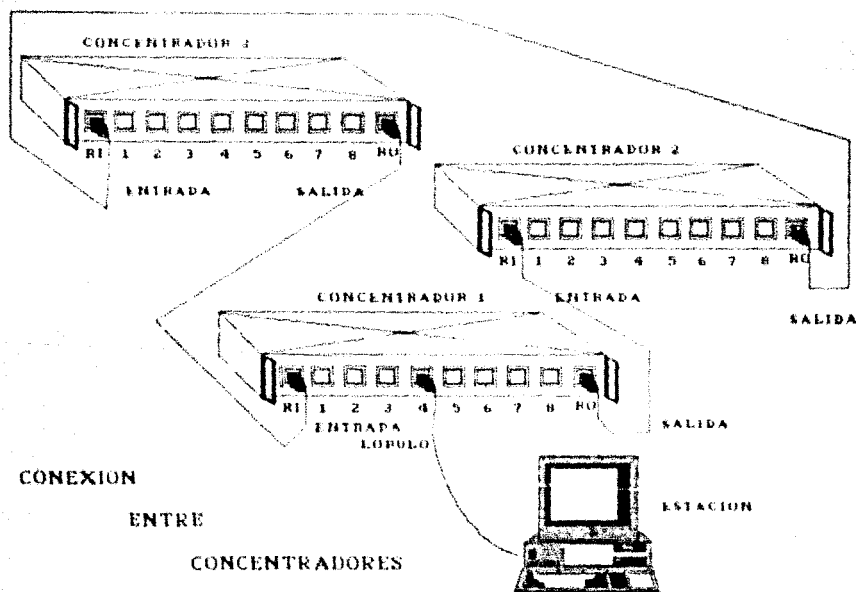
Un concentrador típico cuenta con 10 entradas, ocho de los cuales se utilizan para conectar estaciones y los dos restantes, los receptáculos "Ring In" y "Ring out", se emplean para continuar el anillo principal y el anillo de respaldo para conectar una serie de más concentradores y así formar anillos de más de 8 estaciones.



Un mínimo anillo local lo formarían un Concentrador y desde 2 hasta 8 estaciones de trabajo. Para formar anillos con más estaciones, se forman redes locales y después se interconectan a través de los concentradores. Este tipo de red puede llegar a un máximo de 256 estaciones interconectadas, formando el anillo total de la red, esto es un total de 27 concentradores.

Una gran desventaja de este tipo de estructura es que solo se genera un *token* por todo el anillo lo que aumentara el tiempo de espera entre la primera estacion y la ultima deseosa de transmitir.

En el caso en que la red de area local requiera cubrir un area geografica mas grande, se debe tomar en cuenta que la máxima distancia especificada entre una estacion y el concentrador es de 130 mts. La distancia máxima entre un concentrador y otro puede ser hasta 250 mts. La conexión en serie de concentradores se realiza a partir de los receptáculos RI y RO de los concentradores.



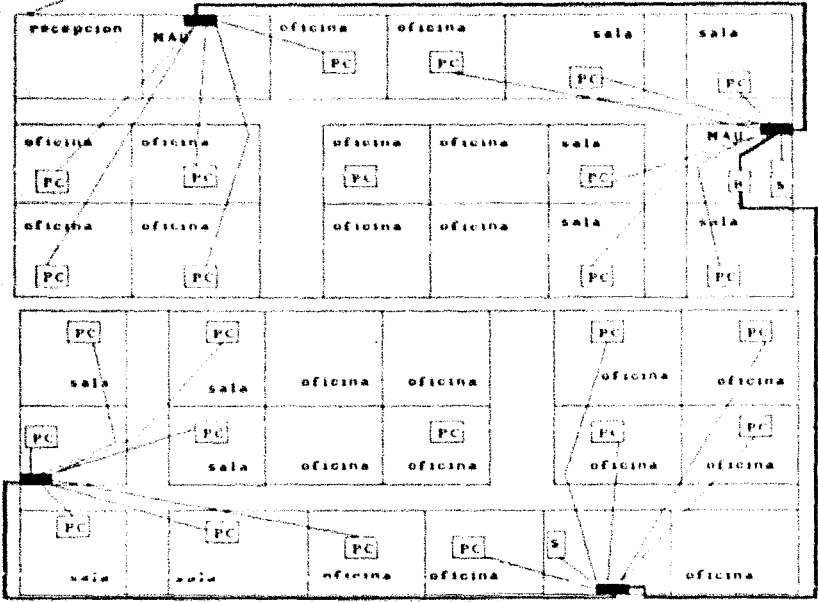
Cuando se desea extender la distancia entre un concentrador y otro, se pueden emplear dispositivos conocidos como Repetidores (*repeaters*), estos dispositivos se encargan de regenerar y amplificar las señales que se transmiten, al utilizar un repetidor la distancia entre un concentrador y otro puede incrementarse hasta 400 mts.

### 5.3 REPETIDORES (REPEATERS)

Antes de emplear repetidores en una red de cualquier tipo, se debe hacer un análisis para determinar si el empleo del repetidor es necesario. Primero, se verifica que la distancia de transmisión permita el buen funcionamiento del anillo, para lo cual se calcula la máxima distancia de transmisión (MDE) y se compara con las especificaciones; si la distancia calculada se encuentra dentro de los límites permisibles el diseño de la red es válido. De otra forma habrá que ajustar nuevamente las distancias y efectuar de nuevo los cálculos. Si no se logra caer dentro del rango permitido entonces será necesario utilizar repetidores, en cuyo caso se compararán las distancias con nuevas especificaciones.

La máxima distancia de transmisión es la longitud ajustada del anillo (ARI) más la longitud del lobulito más grande. El ARI es la longitud de la trayectoria principal del anillo (consta de los concentradores y de las longitudes de los cables entre ellos) menos la longitud más corta entre closets de alambrado.

La distancia de transmisión se compara con las especificaciones considerando el número de 'closets de alambrado' y el número de concentradores.



PC - COMPUTADORA PERSONAL  
 R - (BRIDGE) PUENTE  
 S - SERVIDOR  
 NAU - CONCENTRADOR

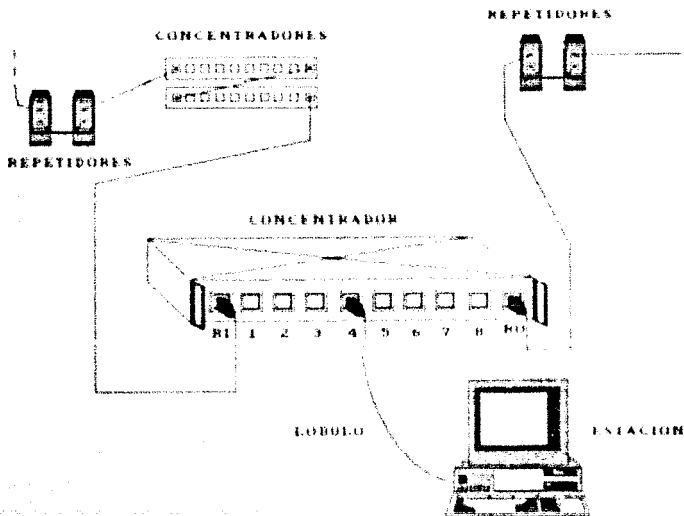
### 5.3.1 Repetidores de Cobre.

Permiten construir anillos sobre áreas geográficas mayores

Para determinar la colocación de los repetidores de cobre en la trayectoria del anillo principal se debe conocer el número de concentradores en cada clóset de alambrado, número de clósets de alambrado y su localización, además de la longitud de cada cable entre clósets, y obviamente el tipo de cable.

Los repetidores permiten considerar el segmento entre dos pares de ejos como un anillo con el propósito de determinar la distancia de manejo permisible (la longitud de cable y dispositivo sobre la cual una señal puede transmitirse confiablemente)

Los repetidores de cobre se colocan en parejas sobre la trayectoria principal del anillo y nunca se usan sobre los lóbulos.



**Para planear la ubicación de los repetidores de cobre en un anillo, además hay que considerar:**

- 1.- Colocar el primer par de repetidores de cobre a la entrada (antes del primer concentrador) del closet de alambrado con el mayor número de concentradores (MAU's)
- 2.- Colocar el siguiente par de repetidores tan lejos como sea posible del par previo sin exceder las especificaciones de distancias máximas con repetidores. Para prevenir posibles expansiones, este par de repetidores se debe colocar lo más cerca al par previo. Por lo regular, para propósitos tanto de planeación como de expansión, la localización más conveniente para un par de repetidores es la entrada o salida de un closet de alambrado.
- 3.- Calcular la distancia de manejo permisible de un segmento de acuerdo al siguiente procedimiento:
  - A. Tratar cada segmento entre repetidores separadamente, calculando una distancia de manejo para cada segmento del anillo.
  - B. Para cualquier segmento que contiene supresores de pico, decrementar la distancia de manejo permisible por cada supresor en aproximadamente 30 m.
  - C. Determinar la longitud del lobulo conectado al anillo.
  - D. Determinar la longitud del cable entre cada par de repetidores y el concentrador más cercano a ellos en el segmento del anillo.

Al intentar el diseño con repetidores se puede caer en diferentes problemas

**Caso 1:** La longitud del lóbulo más grande es mayor que la longitud de cualquiera de los cables entre el par de repetidores y el concentrador más cercano a ellos

La distancia de manejo en este caso es la suma de la longitud del lóbulo más grande, más la longitud de todos los cables entre el primero y el último concentrador en el segmento del anillo.

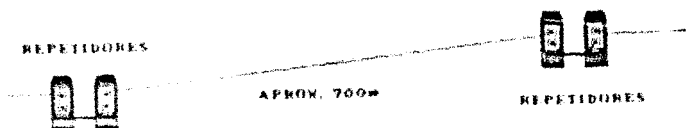
**Caso 2:** La longitud del lóbulo más grande es menor que la longitud de uno o de ambos cables entre repetidores y sus concentradores más cercanos

La distancia de manejo en este caso se calculará como la suma de la longitud más grande de los dos cables entre repetidores y sus concentradores más cercanos y el total de todos los cables entre el primero y el último concentrador en el segmento.

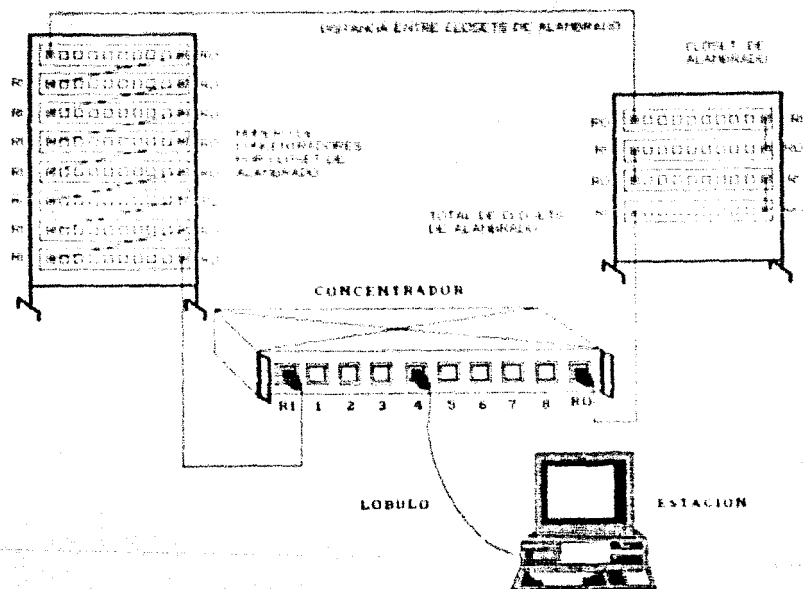
**Caso 3:** No hay concentradores en el segmento del anillo.

La distancia de manejo será constante (aprox. 770 m) entre pares de repetidores. Reducir la distancia de manejo permisible por cada supresor (aprox. 30 m)

Dependiendo del tipo de cable usado entre los closets de alambrado los valores y los cálculos varían.







Si la distancia de manejo permisible no cae dentro de los límites máximos, como alternativas se tiene:

- 1.- Tratar de hacer algún ajuste dentro del segmento del anillo
- 2.- Seguir colocando pares de repetidores hasta que el último segmento del anillo este dentro de una longitud de anillo permisible

### 5.3.2 Repetidores de Fibra Óptica

El cableado de fibra óptica es recomendable cuando se desea transportar señales sobre segmentos del anillo principal que son muy largos, segmentos entre edificios o sobre segmentos expuestos a alta interferencia.

Para fibra óptica entre closets de alambrado se necesitarán repetidores de fibra óptica en la trayectoria del anillo principal.

Un repetidor de fibra óptica es capaz de convertir una señal de un impulso eléctrico a una señal luminosa y transmitirla sobre aproximadamente 2 kilómetros de cable de fibra óptica.

Los repetidores no contemplan una protección o aislamiento de los mensajes que circulan a través de toda la red y solamente amplían las dimensiones máximas que puede alcanzar una red *Token Ring* sencilla (utilizando el número máximo de concentradores y alargando al máximo las distancias entre estos con repetidores).

## 5.4 JUSTIFICACION DE REDES MULTI-ANILLOS

La interconexión de un conjunto de redes puede parecer como una gran red, sin embargo, cada una de estas redes puede conservar su propia identidad para lo cual se requiere de mecanismos especiales, a la red completa resultante se le conoce con el nombre de Inter-Red (*INTERNET*), a cada una de las redes que la conforman se le llama Subred (*SUBNET*)

Para lograr la conexión de subredes se cuentan con 2 dispositivos básicos: el puente (*BRIDGE*), y la compuerta (*GATEWAY*). Estos dispositivos proporcionan una trayectoria de comunicación y la lógica necesaria para que los datos puedan intercambiarse entre las subredes. La diferencia básica entre estos dispositivos es el protocolo o manera en que interconectan a las subredes

La conexión de dos o más subredes sencillas con topología anillo a través de estos dispositivos forman una red multi-anillo

La forma más simple de interconectar dos subredes es empleando puentes, este dispositivo fue diseñado para emplearlo entre dos subredes de área local que utilizan el mismo protocolo de comunicación en el nivel físico y en el nivel *MAC*

Se requiere de una red con múltiples anillos cuando

- Los requerimientos de transferencia de datos exceden la capacidad de un anillo sencillo
- cuando las estaciones conectadas se encuentran muy dispersas y no es posible cubrir las distancias ni siquiera empleando repetidores.
- Para que alguna parte de la red permanezca aislada y su actividad no degrade al resto de la misma

- Por confiabilidad, para evitar el riesgo de que conectados los dispositivos sobre una misma trayectoria de comunicación si ocurriera una falla todos los dispositivos quedarían incommunicados.
- Por *performance*, pues su empleo decremente el número de estaciones activas en comparación con un repetidor, en lugar de extender la misma red, formara dos subredes independientes; o simplemente porque es necesario aislar una subred de otra para mantener la calidad del servicio.
- Por seguridad, el establecimiento de múltiples subredes puede mejorar la seguridad de que se contará con rutas alternas de comunicación. Además de que se pueden formar subredes con diferentes tipos de tráfico, con usuarios de diferentes niveles de seguridad y de privilegios, además de que permite controlarlos y monitorearlos, esto es para que se mantengan y controlen de manera independiente.

Un beneficio más de la interconexión de redes, es que se realizan como sistemas totales capaces de ejecutar múltiples redes independientes con la flexibilidad para mapear una estructura organizada de un edificio a una correspondiente red de área local.

## 5.5 DISEÑO DE REDES MULTI-ANILLOS

Un puente es un dispositivo de alta velocidad capaz de rutear *frames* entre 2 anillos de acuerdo a la información de dirección de estos. Además, puede ejecutar cambios de velocidad entre un anillo y otro. Cada anillo contará con un mecanismo de *token* individual y de esta manera podrá aislarse para seguir funcionando si el otro anillo falla.

Un puente es una combinación de *hardware* y *software* usado para conectar dos subredes que usan el mismo protocolo de comunicación y el cual es capaz de transferir *frames* de un anillo a otro.

Con el empleo de puentes se pueden unir anillos en subredes que puedan servir a más de 256 nodos. Cada anillo mantiene su propia identidad, su propio mecanismo de *Token* e inclusive puede permanecer en una configuración 'standalone' en el caso de que el puente o el anillo vecino fallen.

Las características básicas de un puente son:

- Esta formado por una estación conectada a los dos anillos que comunica, de ahí la razón de utilizar dos unidades de acoplamiento. La interfase de un puente a un anillo es la misma que para cualquier estación.

- a la estación se le adiciona el equipo necesario para realizar sus funciones de ruteo, cambios de velocidad y almacenamiento.

- cuenta con el almacenamiento necesario para contener *frames* hasta que puedan ser transferidos al siguiente anillo.

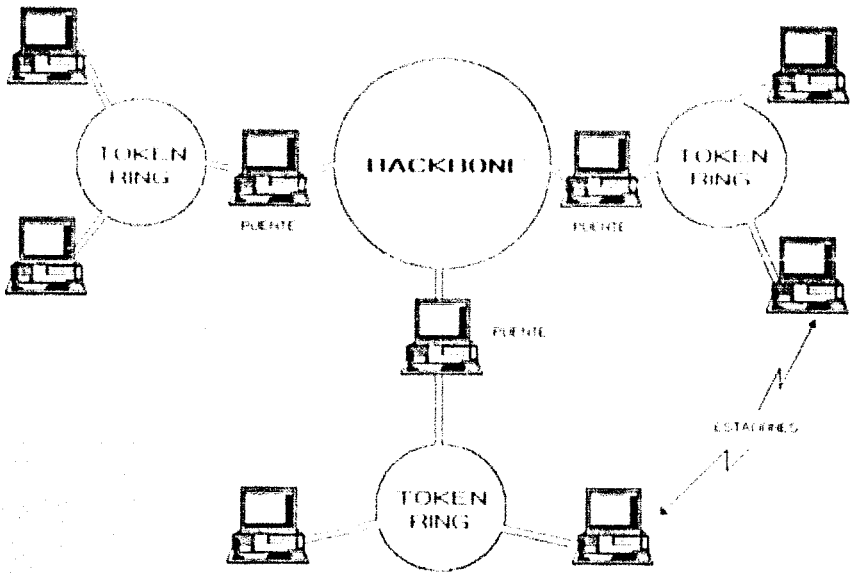
- no altera la información de los *frames* que recibe.

- además realiza las mismas funciones de un repetidor, es decir, regenera y amplifica las señales.

La estación designada como Puente estará dedicada específicamente a realizar sus funciones de puente y no podrá utilizarse para otra clase de aplicaciones a menos que se supriman dichas funciones.

Básicamente los puentes pueden ser de dos tipos: locales y remotos. La diferencia básica entre estos es el medio de transmisión que utilizan para ligar dos subredes.

RED MULTIANILLO  
FORMANDO UNA ESTRUCTURA MASHONE



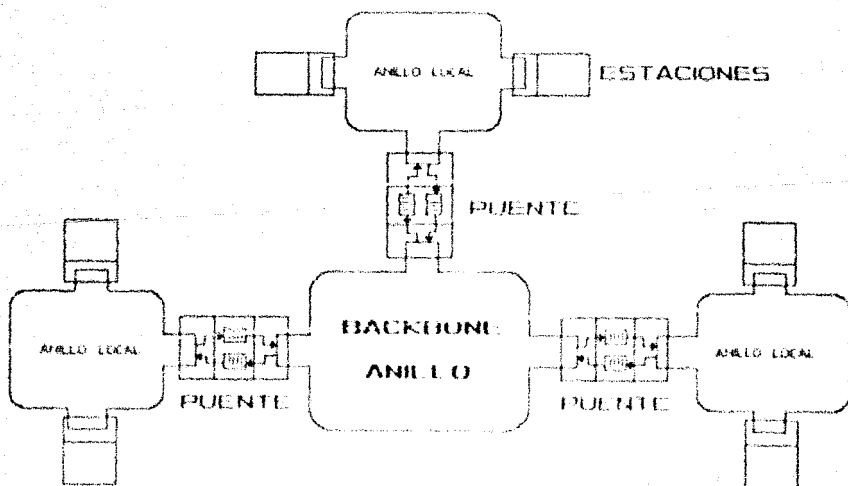
### 5.5.1 Estructura *BACKBONE*

Un anillo *backbone* conecta a otros anillos entre sí con puentes para formar una red que provee comunicación de cualquier punto a través de varios anillos, es decir es una red de subredes.

Esta estructura es capaz de:

- Proporcionar la trayectoria promedio más corta entre dos nodos de la red.
- Proporcionar el acceso más directo a dispositivos compartidos, tales como servidores de impresión y de archivo e inclusive servicios de *algún host*.

Se debe tomar en cuenta que el diseño de un *backbone* esta sujeto a las mismas consideraciones de planeación que el anillo sencillo.



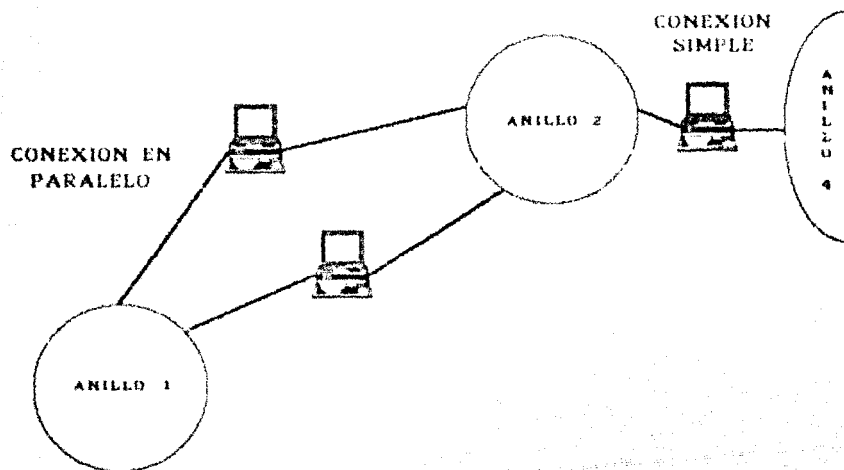
## 5.5.2 Topologías Multi-anillos

### A - Conexión Simple

Para unir simplemente dos anillos cuyo tráfico entre ambos es muy alto y no se desea que el mismo repercuta en el resto del multi-anillo

### B - Conexión en Paralelo

Este tipo de conexión se emplea para dar mayor confiabilidad al intercambio entre dos subredes, o cuando es muy necesaria la transferencia de información entre dos subredes y es indispensable que siempre exista comunicación, en cuyo caso uno sirve como respaldo si el otro falla, se pueden emplear hasta 16 puentes paralelos entre dos anillos.



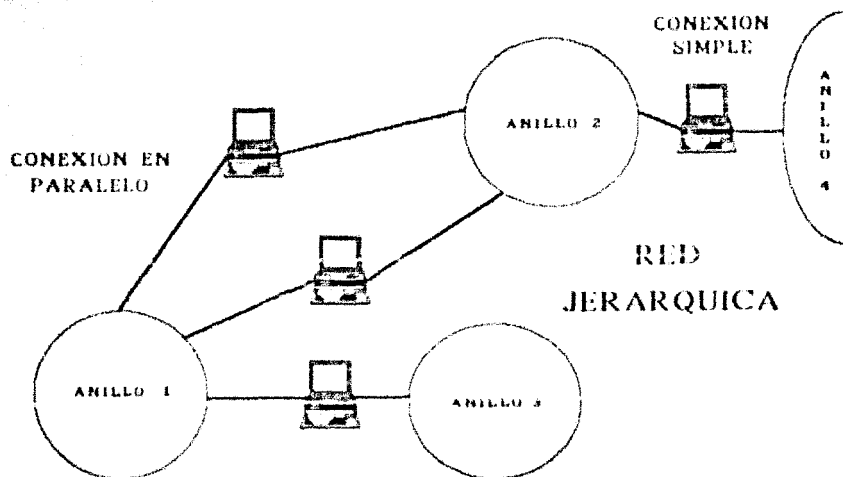


### C - Red Jerárquica

Proporciona una sola trayectoria vía anillos intermedios entre un anillo fuente y un anillo destino.

Un *frame* cuya fuente está en el anillo 3 debe pasar por el puente C, por el anillo 1 y ya sea por el puente A o B para llegar a su destino en el anillo 2.

Ninguna otra trayectoria es posible. Para este ruteo el anillo 1 siempre será el único anillo intermedio posible.

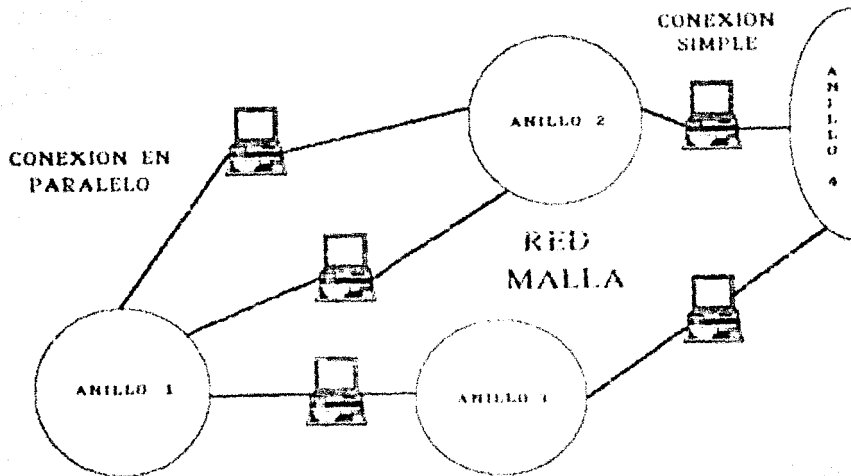


### - Red de Malla

Proporciona múltiples trayectorias vía anillos intermedios entre anillos fuente y anillos destino.

Un *frame* cuya fuente está en el anillo 3 y cuyo destino está en el anillo 2 tiene dos trayectorias posibles. El *frame* puede pasar desde el anillo 3 a través del puente C, del anillo 1 y ya sea por el puente A o B hasta el anillo 2.

El *frame* también puede pasar desde el anillo 3 a través del puente E, del anillo 4 y del puente D a su destino en el anillo 2.



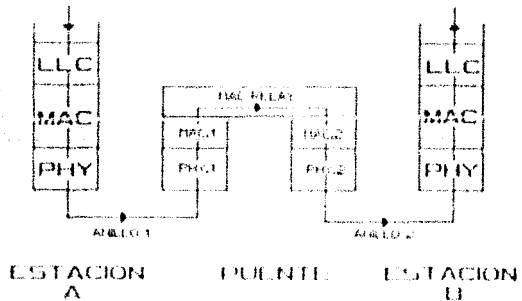
## 5.6 PUENTES (BRIDGES)

El puente (*bridge*), se encarga de mantener aislada a cada una de las subredes, realizando funciones de enrutamiento de mensaje; además regenera y amplifica las señales.

Un puente opera de la misma manera que cualquier estación de trabajo dentro de una red *Token Ring*, excepto que éste debe distinguir y copiar los *frames* destinados para cada una de las subredes a interconectar. El puente debe tener la capacidad para almacenar temporalmente los mensajes que desean ir de una subred a otra. El puente no toma ninguna acción de prevención de errores o correctiva si alguno de los *frames* se pierde. La tarea de detección y recobro de los *frames* corresponde a las estaciones de trabajo.

La siguiente figura muestra el modelo en el cual se basa la operación de un puente:

MODELO DE LA ARQUITECTURA DE UN PUNTE



Las funciones del control de ruteo en los puentes las realiza el nivel de enlace de datos (LLC). La operación de puentes se encuentra bajo consideración para incluirse en el estándar IEEE 802.5.

La técnica específica de enrutamiento sugerida para un enlace entre subredes *Token Ring* es el llamado " *Source Routing* ", el

estándar IEEE 802.5 también considera otras técnicas de ruteo como el método "Transparent" o el "Spanning Tree".

### 5.6.1 Técnica de enrutamiento *SOURCE ROUTING*

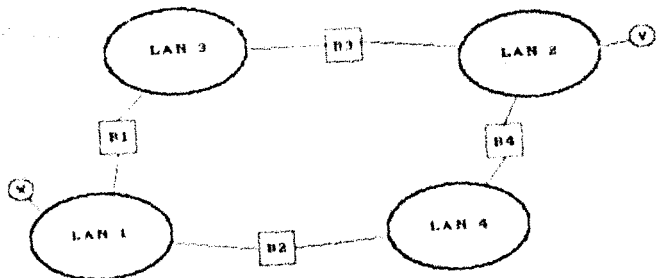
El *Source Routing* es un mecanismo utilizado por la estación trasmisora para determinar la ruta que el *frame* seguirá incluyendo dicha información en el *frame*; los puentes leen la información de la ruta para determinar si dejan pasar o no el *frame*.

#### - Operación básica

Con la configuración de la siguiente figura se describe el algoritmo de la Operación básica del método *Source Routing*. La *frame* A de la estación X puede llegar a la estación Y a través de las siguientes dos rutas:

\* LAN 1, puente B1, LAN 3, puente B3, LAN 2

\* LAN 1, puente B2, LAN 4, puente B4, LAN 2



La estación X puede escoger cualquiera de las dos rutas y proporcionar la información de la secuencia de las subredes y puentes que debe recorrer en el campo de 'información de ruta' del *frame* que se va a transmitir. Cuando un puente recibe un *frame* este lo retransmitirá si dicho puente está designado en la ruta; cualquier otro *frame* será descartado. En este caso, en la primera ruta arriba especificada, los puentes b1 y b3 dejarán pasar el *frame*; en la segunda ruta los puentes b2 y b4 dejarán pasar el *frame*.

Con este esquema los puentes no necesitan mantener tablas de rutas. El puente hace la decisión de dejar o no pasar un *frame* de acuerdo a la información básica contenida en el *frame*. Todo lo que se requiere es que el puente reconozca su propio identificador y los identificadores de las subredes a las cuales está conectado. La responsabilidad de determinar la ruta cae sobre la estación transmisora.

Para que este esquema funcione, debe existir un mecanismo para que cada estación pueda determinar la ruta de cualquier destino, para lo cual primero hay que conocer algunos modos de ruteo.

#### - Modos de ruteo

El esquema de *Source Routing* diseñado por el comité IEEE 802.5 incluye cuatro modos de ruteo. Cada *frame* que se transmite incluye un indicador del tipo de ruteo designado. Los cuatro modos son los siguientes:

- \* Nulo (*NULL*). Ninguna ruta asignada. En este caso, el *frame* solamente puede circular en la misma subred en la que se encuentra la estación origen.

- **No simultáneo (*NONE BROADCAST*)**: El *frame* incluye una ruta la cual consiste de una secuencia de identificadores de subredes e identificadores de puentes que definen una ruta única entre la estación origen y la estación destino. Solo los puentes designados en esta ruta permiten el paso del *frame* y solo una copia del *frame* llega a la estación destino.
- **Todas las rutas simultáneas (*ALL-ROUTES BROADCAST*)**: El *frame* pasa por todas las subredes de la Inter-Red a través de todas las rutas posibles. Cada puente permite el paso del *frame* por lo que la estación destino recibe una copia del *frame* por cada ruta posible.
- **Una ruta simultánea (*SINGLE-ROUTE BROADCAST*)**: Sin hacer caso a la dirección destino del *frame*, al *frame* lo transmiten únicamente los puentes que se encuentran en un Spanning tree (con el nodo destino como raíz) de la inter red. La estación destino recibe solo una copia del *frame*.

Los últimos dos modos de ruteo los emplea una estación fuente que desea conocer la ruta para la estación destino. Por ejem., la estación origen puede utilizar todas las rutas simultáneamente para enviar un *frame*, la estación destino envía su respuesta usando una ruta (*NONE-BROADCAST*), o sea la ruta determinada por la estación origen. La estación origen guarda esta ruta para mensajes futuros. Alternativamente la estación origen puede usar una ruta simultánea (*SINGLE-ROUTE BROADCAST*) para enviar un *frame* a la estación destino. La estación destino puede enviar su respuesta via todas las rutas simultáneas (*ALL-ROUTES BROADCAST*). El *frame* de respuesta puede revelar más rutas posibles hacia el destino. También la estación origen puede guardar estas rutas para mensajes posteriores. Finalmente el modo de ruta simultánea (*SINGLE-ROUTE BROADCAST*) puede usarse con un grupo de direcciones.

Cada *frame* debe incluir un indicador de cual de los cuatro tipos de ruteo esta empleando:

- \* Nulo (**NULL**) El *frame* es ignorado por el puente.
- \* No simultaneo (**NONE BROADCAST**) El *frame* contiene la secuencia a seguir, un puente lo deja pasar solo si contiene su identificador dentro de la secuencia.
- \* Todas las rutas simultaneas (**ALL-ROUTES BROADCAST**) La estación origen marca al *frame* con este tipo de ruteo pero no se incluye informacion de ruta. Cada puente que permita el paso de este *frame* le aumenta el numero de este y de la subred. Para prevenir *frames* repetidos o sin destino, el puente primero examina la informacion de ruta, si el campo contiene el identificador de la subred en la cual se encuentra el puente, este se abstiene de repetirlo en dicha subred de otra forma le permite el paso a la red que todavia no se ha visitado.
- \* Una ruta simultanea (**SINGLE ROUTE BROADCAST**) Es necesario contar con un *spanning tree* de la Inter-Red. Este se puede desarrollar de forma manual o automatica. En cualquier caso uno de los puentes es el designado para que por el transiten los *frames* de este tipo.

Es importante hacer notar la relacion que existe entre los modos de ruteo y de direccionamiento.

MODO DIRECCIONAMIENTO	DE NULO	NO RUTA	TODAS LAS RUTAS	UNA RUTA
INDIVIDUAL	Recibido por la estación si se encuentra en la misma subred	Recibido por la estación si se encuentra en algunas de las subredes de la ruta	Recibido por la estación en la que se encuentra	Recibido por la estación si se encuentra en la que se encuentra
GRUPO	Recibido por todos los miembros del grupo que se encuentran en la misma subred	Recibido por todos los miembros del grupo de estaciones de todas las subredes visitadas por la ruta	Recibido por todos los miembros del grupo en todas las subredes	Recibido por todos los miembros del grupo en todas las subredes
BROADCAST	Recibido por todas las estaciones de la misma subred	Recibido por todas las estaciones de las subredes visitadas por la ruta	Recibido por todas las estaciones en todas las subredes	Recibido por todas las estaciones en todas las subredes

### - Descubrimiento de Ruta y Selección

Con el método de *Source Routing*, los puentes no desarrollan las funciones de almacenar y utilizar la información de las rutas. Esto lo desarrollan las estaciones que desean transmitir *frames*. Es obvio que se necesita de un mecanismo mediante el cual las estaciones origen puedan conocer la ruta hacia cada destino para los cuales serán enviados *frames*.



Básicamente se definen 3 estrategias:

- \* Manualmente cargar la información en cada estación. Este es mas simple de los mecanismo y tiene varias desventajas, por ejem., con un cambio en la configuración, la información de rutas de todas las estaciones se debe actualizar y tampoco proporciona un ajuste automático si llegase a fallar algun puente de la subred.
- \* Una estación de la subred puede interrogar a otras estaciones de la misma subred acerca de las rutas para estaciones distantes. Este mecanismo tiene la ventaja de que reduce el número de transmisiones de reconocimiento que se tengan que hacer (en comparación con el siguiente punto), pero sin embargo, por lo menos una estación de cada subred debe tener la información de todas las rutas, por lo que no se le considera una solución completa.
- \* Cuando una estación necesita aprender la ruta hacia otra estación, ejecuta un procedimiento dinámico para el descubrimiento de rutas.

La opción 3 es la mas flexible y la unica especificada por el comité IEEE 802.5. La estación origen puede transmitir por todas las rutas posible hacia la estación destino (*ALL-ROUTES*), así todas se descubren todas la posibles rutas. La estación destino puede contestar a cada *frame* que le llejo mediante el modo simultaneo (*NONE*), para permitirle a la estación origen seleccionar la ruta para las subsiguientes transmisiones. Este metodo incrementa el tráfico en ambos sentidos y requiere de que la estación destino conteste el mismo *frame* varias veces (una vez por cada ruta). Una alternativa es que la estación origen transmita un *frame* de una sola ruta (*SINGLE ROUTE*), solo un *frame* llegara a la estación destino, la estación destino contestara con un *frame* de todas las rutas (*ALL-ROUTES*), para que la estación origen conozca todas las rutas posibles, así la estación origen podra escoger la mejor ruta.

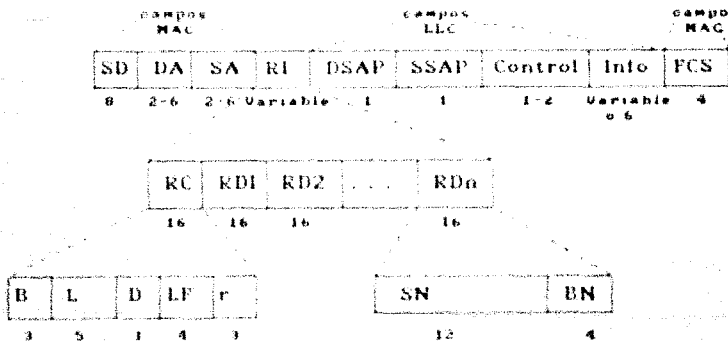
Una vez que se cuenta con un conjunto de rutas, la estación origen necesita seleccionar una. El criterio más obvio sería el de seleccionar la ruta más corta, o seleccionar la ruta de menor costo (donde el costo de una red es inversamente proporcional a su velocidad de transmisión). En cualquier caso, si dos o más rutas son equivalentes, se cuenta con las siguientes alternativas para su discriminación:

1. Escoger la ruta cuyo mensaje de respuesta llegó primero. Asumiendo que es la menos congestionada por haber llegado primero.
2. Escoger aleatoriamente, lo que nivelaría la carga en los puentes.

Otro punto a considerar, es que tan frecuente se deben actualizar las rutas ya que estas cambian ya sea por fallas, congestionamiento, etc. una posibilidad es descubrir nuevamente las rutas con cada nueva conexión, otra alternativa es asociar un contador a cada ruta seleccionada y redescubrir las rutas cuando su tiempo expira.

#### - Formato del *Frame*

Con el método *Source Routing* se le debe agregar un nuevo campo al formato del *frame* del protocolo MAC.



El nuevo campo que se le agrega es el de información de ruta (**RI, Routing Information field**) el cual consiste de un campo de control de ruta seguido por un campo global de longitud variable (0 a 8 subcampos) que conforman los campos de designación de ruta (**RDI, Route Designator i**). El campo de control de ruta, está formado por los siguientes subcampos:

- Simultaneo (**Broadcast**) indica el modo de ruteo (3 bits)
- Longitud (**Length**) indica la longitud del campo de control de información de ruta en octetos (5 bits).
- Dirección (**Direction**), le indica a un puente si el **frame** está viajando de la estación origen a la destino o viceversa. Permite que la lista de los campos de designación de ruta aparezcan en el mismo orden para los **frames** que viajan en ambas direcciones a través de la ruta (1 bit)
- Largo del **frame** (**Largest frame**) especifica el tamaño máximo del campo de información **MAC** que puede ser transmitido por esta ruta. Este campo está codificado para indicar ciertos tamaños comunes, por ejemplo 0011 indica 1500 octetos, 0111 indica 4472 octetos. Cuando un puente recibe un **frame**, actualiza este campo si el valor actual excede la capacidad del puente o si su subred adyacente lo permite. De esta manera, el proceso de descubrimiento de ruta también encuentra el máximo tamaño de **frame** que puede manejar una ruta en particular (4 bits)

El resto del campo de información de ruta consiste de un secuencia de designadores de ruta, cada designador corresponde a un salto. El designador de ruta consta de un número de 12 bits para el número de la subred y de 4 bits para el número del puente

### 5.6.2 Control de flujo de datos

El estándar LLC para redes de área local IEEE 802.2 define dos tipos de operación.

- tipo uno: UCS - *Unacknowledged Connectionless Service* (servicio de desconocimiento de mínima conexión). Un servicio de datagramas por el cual las entidades LLC en dos dispositivos intercambian *frames* sin el beneficio que el nivel de flujo de datos ofrece como son la recuperación de errores o el control de flujo de datos.

- tipo dos: COS - *Connection Oriented Service* (servicio de conexión orientada), el cual proporciona recuperación al extravío, duplicación o desorden en los *frames* y permite a las estaciones regular el flujo de datos entre ellas para que no existan confusiones. Para proporcionar este servicio, el tipo dos de conexión depende de las conexiones establecidas, y de diferentes tipos de *frames* para el inicio de la conexión, para transferencia de datos, para reconocimiento de estaciones y control de flujo.

Un tercer tipo de operación aprobado por el IEEE 802 en 1986 es llamado como ACS - *Acknowledged Connectionless Service*, el cual proporciona algo de confiabilidad pero no control de flujo y requiere menos información de estado y menor rigurosidad en la forma de iniciar la conexión.

El que comúnmente se emplea es el tipo 2, en el que las unidades de datos proporcionadas por un usuario de los servicios del nivel dos se transmiten en *frames* de información (I). El subnivel del LLC hace uso de los *frames* llamados Supervisores (S +) para las funciones de control como son el establecimiento y terminación de conexiones, reconocimientos positivos y negativos e información de control.

El control de flujo se realiza por un mecanismo ventana (**W, WINDOW**), esto es, al emisor se le permite transmitir  $W$  frames de información (tamaño de la ventana) sin tener que esperar por un reconocimiento. El receptor utiliza *frames* de 'listo para recibir' (*Receive Ready RR-*) para reconocer los *frames* de información correctamente y para indicar al emisor que más *frames* de información se pueden transmitir. En el protocolo original tipo dos del IEEE 802 el tamaño de la ventana  $W$  se encuentra especificado a un valor constante definido en el momento en que se inicia la liga (*link-initialization time*). Para mejorar la eficiencia de este mecanismo el estándar cuenta con una opción para que el tamaño de la ventana se ajuste dinámicamente en caso de existir una congestión en la red.

El control proporcionado por la operación tipo 2, se basa en dos mecanismos primordiales, la Recuperación *Reject* y el Mecanismo *Time-Out*:

**Recuperación *Reject***: Si se recibe un *frame* de información con una secuencia de chequeo de *frame* incorrecta (FCS) este será descartado. Cuando se ha recibido un *frame* de información que tiene una secuencia correcta pero su número de secuencia enviado no es igual, el receptor regresará un *frame Reject* (REJ-), el cual descartará todos los *frames* de información hasta que el *frame* esperado se reciba correctamente. Cuando el emisor recibe un *frame Reject*, éste retransmite los *frames* de información comenzando con el número de secuencia recibido en el *frame Reject*.

**Mecanismo *Time-Out***: Cuando se transmite un *frame* de información, un contador se inicia (si no lo estaba). Cuando el emisor recibe un *frame RR*, este reiniciará el contador si existen *frames* de información sin reconocer. Cuando un contador termina la estación ejecuta una función de *Check Pointing*, transmitiendo un *frame RR* con el bit dedicado a esta función encendido a uno (P-bit). Después de recibir este *frame* el receptor debe regresar un *frame RR* con el P-bit encendido en uno. Cuando este *frame RR* lo ha recibido, este procede con la transmisión de nuevos *frames* de información o con la retransmisión de los anteriores, dependiendo del número de secuencia contenida en el *frame RR* recibido.

Este dispositivo se utiliza para rutear mensajes entre nodos intermedios

## 5.7 COMPUERTAS (GATEWAYS)

Una compuerta (*gateway*) proporciona una interfase entre una Red de Area Local (LAN) y una Red de Area Amplia (WAN) para establecer comunicaciones a larga distancia entre nodos dentro de la misma red de área local y nodos de otra red de área local o que son accedidos directamente sobre una WAN, donde se están empleando protocolos de comunicacion diferentes.

Las WANs incluyen redes de paquetes conmutados privadas y comerciales, enlaces satelitales, líneas privadas u otro tipo de enlaces terrestres. Generalmente operan a tasas de transmisión más bajas que las de las redes de área local.

Con una compuerta se pueden llevar a cabo las traducciones de direcciones necesarias, como proveer las conversiones de protocolo y de velocidad que se requieren para hacer la conexión de una LAN con una WAN. Funciones similares son las que se requieren para hacer la conexión entre un *host* y una red de área local *Token Ring*. También puede usarse como un nodo intermedio entre una LAN *Token Ring* y un nodo de una LAN *CSMA/CD* o de un PBX.

Sobre una compuerta *Token Ring* existen básicamente dos tipos de conexiones:

1. Hacia una red de conmutacion de paquetes (X.25)
2. Hacia un *host*.

El establecimiento de una compuerta hacia una red de conmutación de paquetes, requiere de interfaces tanto de *hardware* como de *software* que permitan a cualquier estación en una LAN establecer enlaces de estación de trabajo a *mainframe* y de estación a estación a través de redes de conmutación de paquetes que trabajan bajo el protocolo X.25, con lo que incluso las estaciones pueden comunicarse hacia *hosts* remotos emulando terminales, o para hacer transferencias de archivos.

#### - Conexión entre Compuerta y Host

El *host* debe contener la declaración de la compuerta que se va a utilizar. Se debe de contar de antemano con *modem* y con las líneas telefónicas para realizar el enlace.

Las compuertas trabajan a bajas velocidades pero esto es solo en el enlace entre el *host* y la LAN. El tráfico local en la LAN se mantiene a su velocidad normal.

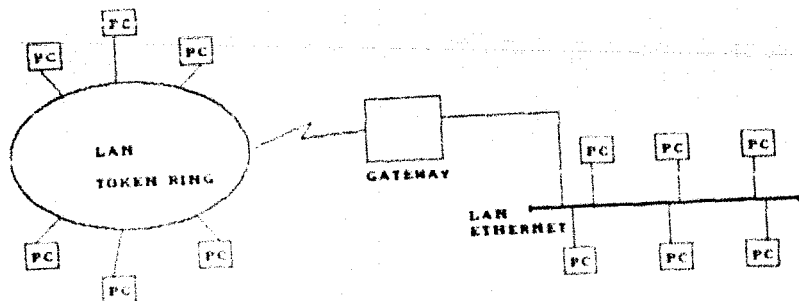
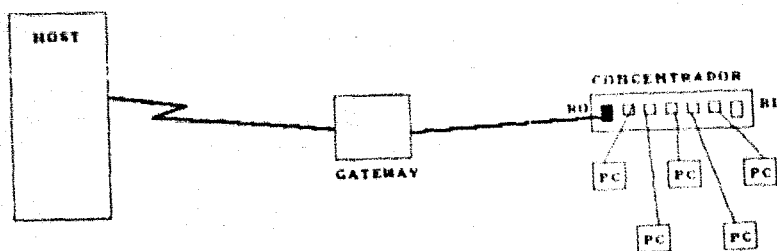
La configuración de una compuerta con estaciones de trabajo funcionará como un servidor (*Server*) de comunicaciones para las estaciones que están conectadas hacia él. Les proporciona acceso a algún *host* (soportando sesiones simultáneas). Las estaciones asociadas a la compuerta pueden llevar a cabo funciones de transferencias de archivos, impresiones remotas, y emular terminales para mantener sesiones.

El nodo compuerta deberá contar con dos unidades de acoplamiento, una que la mantenga como una estación más de la red de área local y otra que le sirva para realizar las funciones de una compuerta que le permitan comunicación con el *host*.

No solo a través de compuertas (*gateways*) se puede comunicar una LAN con un *host*. También se puede lograr con una conexión directa, específicamente al controlador de comunicaciones de dicho *host*.

La ventaja que tiene esta conexión directa hacia un *host* en comparación a una compuerta es que cada conexión opera a velocidades medias (la misma que la LAN)

Otra aplicación práctica de las compuertas es para lograr la comunicación de una LAN con canales *Ethernet*.





Esta comunicacion se puede llevar a cabo de dos maneras.

1. A través de adaptadores de canales.
2. O A través de computadoras que sirvan como puentes para realizar el enlace (con *hardware* y *software* adecuados)

---

## 6. SISTEMA BASICO DE ENTRADA/SALIDA PARA RED (NETBIOS)

## 6. SISTEMA BASICO DE ENTRADA-SALIDA PARA RED (NETBIOS)

---



### 6.1 INTRODUCCION

Una vez que se tiene planeada, diseñada o incluso instalada físicamente una red, surge la inquietud de conocer como las estaciones pueden disponer de los dispositivos, archivos, impresoras, etc. a los cuales se tiene acceso. Debido a lo cual en el presente capitulo se presenta a la interfase para programas de aplicacion que permite a las aplicaciones hechas para las estaciones (especificamente computadoras personales) acceder las facilidades que las redes de área local ofrecen.

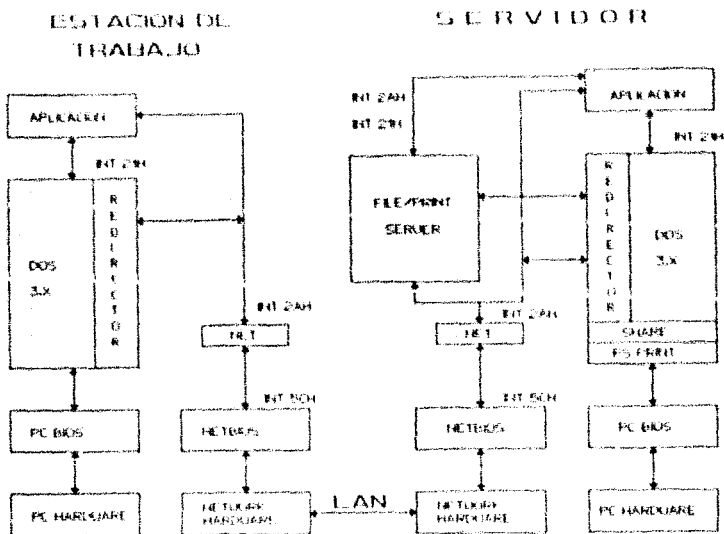
### 6.2 NETBIOS

NetBIOS (*NETwork Basic Input/Output System*) es una interfase para programas de aplicacion actualmente aprobada como estándar dentro del OSI con la que es posible acceder los recursos de una red de área local.

Las llamadas a *NetBIOS* permiten transmitir cualquier orden de informacion hacia una aplicacion en otra maquina y ademas, los comandos que trabajan con *Token Ring* trabajan sin cambios en *Ethernet*, *ARCnet*, *StarLAN*, etc. por lo que también son independientes del *hardware*.

Esta combinacion de independencia, tanto en el *hardware* como en el *software*, hace que las aplicaciones para red sean muy versátiles.

La interfase *NetBIOS* se puede esquematizar de la siguiente manera:



### 6.3 RELACION DEL *NETBIOS* CON EL MODELO OSI

*NetBIOS* proporciona los servicios de dos niveles del modelo OSI: el nivel de RED y el nivel de sesión (*Session Layer*), ninguno de los otros tienen una relación directa.

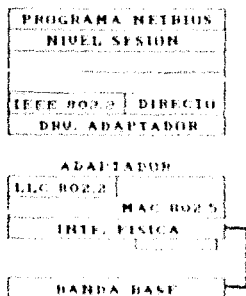
El nivel de RED es el nivel más bajo soportado por *NetBIOS*, lo que se hace es simplemente enviar paquetes de datos entre estaciones de trabajo dentro de la red. Los comandos de soporte de mensajes operan en este nivel. Las aplicaciones pueden recibir y enviar un mensaje (*datagram*) usando estos comandos. Sin embargo, el nivel red no reconoce la recepción de un mensaje o asegura que el programa lo esté recibiendo y contestando a la vez. Este modo de comunicación requiere de la unidad de acoplamiento y del *NetBIOS* mismo.

El nivel de sesión, es el nivel que realiza más tareas dentro del modelo OSI, y el mayor soportado por *NetBIOS*. En este se coordinan las interacciones entre las aplicaciones y el soporte de la transmisión de datos entre otras cosas. Cuando *NetBIOS* establece una sesión entre dos aplicaciones, cada uno de ellos le dice al otro si hay o no mensajes que recibir.

Además se cuentan dos niveles por encima del nivel de sesión, que combinados con programas manejadores de red, el sistema operativo soporta aplicaciones de red (niveles de presentación y de aplicación).

Estos programas manejadores de red usan al *NetBIOS* como parte de su mecanismo para compartir recursos tales como discos e impresoras a través de la red. Existen otros que utilizan su propia arquitectura para compartir recursos y que son capaces de emular al *NetBIOS*. En algunos casos, el aprovechamiento de la emulación del *NetBIOS* hace que la red se ejecute de manera más rápida, sin embargo, puede causar problemas de incompatibilidad. Se deben analizar a las aplicaciones que utilizan ambos tipos de *NetBIOS* para asegurar el buen funcionamiento de los sistemas.

Formalizando la relación que existe entre el *NetBIOS* y el modelo OSI se basa en el siguiente esquema:



## Niveles del modelo OSI con respecto al *NetBIOS*

### NIVEL 3. Nivel de red

Este es el nivel encargado de direccionar y conmutar los datos a través de una red de área local y otras conectadas entre sí. Este es el nivel más bajo donde el *NetBIOS* aparece, el *NetBIOS* se encarga de reconocer las direcciones de la red para dar un trato apropiado a los paquetes de información. Este nivel es la parte más deficiente del *NetBIOS*, ya que su diseño no contempla la interconexión de redes basadas en otra tecnología.

### NIVEL 4. Nivel de transporte

Este nivel se encarga de reanudar las transferencias de información entre las estaciones de la red y de llevar el control de secuencia de paquetes. *NetBIOS* en este nivel utiliza un protocolo propiedad de *Sytek Inc.* para reanudar las transferencias de información.

### NIVEL 5. Nivel de sesión

Este nivel se encarga de dar soporte a los nombres lógicos de las estaciones de la red y de establecer sesiones o ligas lógicas entre los nombres de la red. El *NetBIOS* en este nivel además de realizar todas las tareas anteriores, proporciona la interfase entre la computadora personal y una computadora *HOST*. La forma interna de operación del *NetBIOS* en este nivel es propiedad privada, mientras que la interfase es de dominio público.

### NIVEL 6. Nivel de presentación

Este nivel se encarga del cuidado de la sintaxis de la información que pasa al siguiente nivel. Este nivel no forma parte del *NetBIOS*, se maneja de manera virtual en cada estación. El sistema operativo es parte del nivel de presentación ya que establece la comunicación con las aplicaciones.

## 6.4 PROGRAMACION DEL *NETBIOS*

Una de las ventajas de *NetBIOS* es que oculta la complejidad de las redes de área local y da un nivel alto de interfase para las funciones de la red. Para programar al *NetBIOS* se necesita comprender algunos conceptos, su formato y las interrupciones al procesador que lo invocan.

### 6.4.1 Conceptos Básicos

#### NOMBRE

Una parte fundamental de la programación del *NetBIOS* es el concepto de nombre. Cada adaptador de red de área local puede tener alrededor de 17 nombres y cada uno es de 16 bytes. Uno de estos nombres es el permanente del nodo.

El nombre permanente del nodo es físicamente la tarjeta adaptadora con su propio nombre único. El fabricante de la tarjeta asegura que este nombre sea único, pues viene grabado en una *EPROM* contenida en el adaptador. Este número puede ser una serie de 6 bytes. Otros fabricantes de adaptadores, para asegurar que el nombre sea único, lo forman de 10 bytes de ceros binarios seguido de un número formado en una serie de 6 bytes.

#### TABLA DE NOMBRES

Cada adaptador también usa una tabla de nombres locales en la cual se almacenan 16 nombres seleccionados de software que se reconocen en la red. Cada uno puede tener un nombre único que el adaptador reserva para su uso exclusivo dentro de la red o un nombre de grupo que lo pueden utilizar otros adaptadores.

Cuando un nombre se agrega a la tabla, intencionalmente el adaptador envía un mensaje con ese nombre a todas las demás estaciones para asegurar que el nombre sea único. Cuando un nombre se agrega a la tabla de nombres *NerBIOS* regresa el número de ranura en el cual reside, este número del nombre lo utilizan varios comandos del *NerBIOS* para hacer un acceso rápido a la tabla.

## DATAGRAMAS

La manera más simple con la cual se puede comunicar a través del *NerBIOS* es con un datagrama (*datagram*) que está formado por un bloque de datos de 0 a 512 bytes de longitud, que pueden ser enviados a un nombre único, nombre de grupo o hacia todos los nombres de la red.

Los datagramas no son reconocidos por los adaptadores en el fin de la recepción y se pierden si el adaptador hacia el cual van no se encuentra listo para recibirlos.

## SESION

Mientras que un datagrama va en un solo sentido, una sesión se establece en dos. Un nodo en una red puede estar involucrado en más de una sesión. La sesión da la confirmación de que el receptor se encuentra 'escuchando' y cada datagrama que se envíe será recibido. A través de la sesión podemos enviar datagramas más grandes, de 0 a 65,535 caracteres.



## OPCIONES WAIT Y NO-WAIT

Se pueden ejecutar varios comandos *NetBIOS* con otras partes de un programa si se les invoca con la opción de NO ESPERA (*no wait*).

De los 19 comandos *NetBIOS* se pueden ejecutar 16 con la opción de No Espera. Para invocar un comando *NetBIOS* se debe ejecutar una interrupción de software y además apuntar hacia el NCB (*Network Control Block*).

### 6.4.2 COMANDOS DEL NETBIOS

NetBIOS tiene 19 comandos agrupados en 4 conjuntos de funciones básicas.

- propósito general ( *general-purpose* )
- soporte de nombres ( *name support* )
- soporte de mensajes ( *datagram support* )
- Soporte de sesión ( *session support* )

Casi todos estos comandos se pueden ejecutar bajo dos opciones: **WAIT** y **NO WAIT**. Se logra encendiendo o apagando el bit más significativo de su código.

- \* *Comandos de propósito general:* El comando 'reset' reinicia el adaptador de la red de una máquina, borra la tabla de nombres locales, aborta todas las sesiones e instala los buffers para manejar el máximo número especificado de sesiones y comandos más relevantes. Debe utilizarse con precaución pues puede romper las sesiones dañando los programas que se encontraban ejecutándose en la máquina y hace los dispositivos, directorios, impresoras que se estén compartiendo hacia otras computadoras inaccesibles. Tiene la ventaja de que

si se desea utilizar en el servidor, este comando deja libres todos los recursos para su utilización propia.

El comando 'cancel' cancela a uno que no haya sido completado todavía. Es muy útil cuando se están utilizando comandos sin espera (opción *NO WAIT*).

El comando 'adapter status' da la información de cómo se encuentra un adaptador de la red, no necesariamente en la que uno se encuentra. Entre sus características se encuentran: 6 bytes para el número de identificación, tráfico, errores estadísticos, el contenido de la tabla de nombres locales, etc.

El comando 'unlike' lo usa el sistema que ha sido arrancado (*booted*) desde otro disco. Durante un arranque remoto el adaptador de la red intercepta la lectura del disco destino (*floppy*) y obtiene los datos del disco de arranque del server. Con la llamada al comando 'unlike' termina la emulación del disco arrancado.

\* Comandos de soporte de nombres - Los comandos 'add name' y 'add name group' agregan un nombre a la tabla de nombres locales, 'add name' se puede utilizar si el nombre que se desea agregar no se ha usado. 'add group name' se puede utilizar si otra estación no ha empleado el mismo.

El comando 'delete name' quita un nombre de la misma tabla. Se necesitan terminar la operaciones o sesiones pendientes antes de remover un nombre.

\* Comandos de soporte de mensajes - Los comandos de 'send datagram' y 'receive datagram' como sus nombres lo dicen envían o reciben mensajes hacia o de un nombre específico. Los comandos de 'send broadcast datagram' y 'receive broadcast datagram' reciben y envían mensajes de y hacia todas las computadoras.

**\* Comandos de soporte de sesión** - El comando 'call' es una petición inmediata para iniciar una sesión y el comando complementario 'listen' le indica al adaptador que acepte la petición. Durante una sesión se pueden utilizar comandos de recepción y envío para intercambiar mensajes. El comando 'cham send' envía un mensaje que se ha concatenado de dos fuentes, cuando el mensaje viene con un encabezado seguido de su cuerpo. El comando 'receive' recibe un mensaje de algún nombre el cual tiene una sesión activa. El comando 'hang up' finaliza una sesión. Para más detalles referencíase a los anexos C, D y E.

### 6.4.3 Estructura NCB (Network Control Block)

El NCB es una estructura de datos que contiene información acerca del comando a ejecutar.

Una vez definida la estructura para el comando que se desea llevar a cabo hay que invocar *NcbIOS* a través de la interrupción 5CH, recordando que los registros ES y BX deben apuntar hacia la dirección donde se encuentra el NCB.

Estructura o formato que debe seguir el NCB

NOMBRE CAMPO	DEB. (LONG.)	TIPO	DESCRIPCIÓN
NCB_COMMAND	001	DB	COMANDO
NCB_RETRY	001	DB	CANTIDAD DE REINTENTOS
NCB_LEN	001	DB	NUMERO DE BYTES LOCAL
NCB_LEN	001	DB	NUMERO ARIENADO AL NUMERO
NCB_BUFFER	004	DB	APUNTADE A LA DIRECCION DE BUFFER DEL MENSAJE (OPORTUNAMENTE)
NCB_LENGTH	002	DB	LONGITUD DE BUFFER DEL MENSAJE (ENTERO)
NCB_CALLNAME	016	DB	NOMBRE DEL ADAPTADOR LOCAL O REMOTO. PARA EL COMANDO CHATB SERMO LOS PRIMEROS 2 BYTES INDICAR LA LONGITUD DEL SEGUNDO BUFFER Y LOS SIGUIENTES 4 BYTES APUNTAN A LA DIRECCION DEL SEGUNDO BUFFER
NCB_NAME	016	DB	NOMBRE DEL ADAPTADOR LOCAL
NCB_RTO	004	DB	VALOR DE TIEMPO FUERA EN LA REGION DE RECEPCION
NCB_UTO	004	DB	VALOR DE TIEMPO FUERA EN LA REGION DE ENVIO
NCB_RETRY	004	DB	APUNTADE A LA RUTINA (SERIO) (OPORTUNAMENTE)
NCB_LANA_NUM	001	DB	001 PARA EL ADAPTADOR PRIMARIO 002 PARA EL ADAPTADOR ALTERNO
NCB_CMD_COMPLETE	001	DB	ESTADO DE COMANDO COMPLETO
NCB_RETRY	004	DB	RESERVA

## Descripción de campos

### NCB\_COMMAND

Es un campo de 1 byte. Los comandos tienen dos modos de operación: *WAIT* y *NO WAIT*. La opción *NO WAIT* se selecciona encendiendo el último bit de mayor orden. Los siguientes 7 bits determinan el comando que se desea ejecutar. La opción *NO WAIT* se utiliza para una máxima independencia entre el adaptador y la estación.

La interfase para programar al *NetBIOS* es diferente dependiendo de la selección de *WAIT/NO WAIT* que se elija.

En este campo se regresa un FFh para indicar que el comando se encoló pero no se ha completado. Cuando el comando se completa los resultados se regresan en el campo de *NCB\_RETCODE* y en el campo de *NCB\_CMD\_CPLET*.

Cuando el adaptador interrumpe el programa de aplicación del usuario, el código de regreso final se puede obtener del registro AL, del campo *NCB\_RETCODE*, o del campo *NCB\_CMD\_CPLET*. Si se chequea el campo *NCB\_CMD\_CPLET*, un cambio en el valor FFh (estatus pendiente) indica el comando completo. Este valor representa el código de regreso final. El posible código de regreso final depende del tipo de comando.

Si el código de regreso intermedio es diferente de 00h, el adaptador no puede ejecutar el comando solicitado y el adaptador terminará el proceso.

### NCB\_RETCODE

Es un campo de 1 byte de longitud que indica el código de regreso de un comando. Si es 00h la operación resultó exitosa. Cualquier otro número indica que el comando no se pudo completar.

Cuando un comando se ha completado, el adaptador interrumpe al programa principal en la dirección POST. Se puede escoger entre chequear el registro AL o el campo NCB\_CMD\_CPLT en lugar del campo RETCODE.

#### NCB\_LSN

Es un campo de 1 byte que indica el número de sesión. Este es el número de sesión que se tiene con otro nombre en la red. En los comandos de soporte a datagramas este campo no se utiliza.

#### NCB\_NUM

Es un campo de 1 byte. Indica el número que se regresa después de ejecutar un comando para agregar un nombre o un nombre de grupo.

#### NCB\_BUFFER@

Este es un campo de 4 bytes que es un apuntador al buffer de datos que se desea usar con un comando. Este campo se define en un formato de *DOUBLE-WORD (offset:segmento)* y debe contener una dirección de memoria.

#### NCB\_LENGTH

Es un campo de 2 bytes que indican el tamaño en bytes del dato que se desea transferir.

#### NCB\_CALLNAME

Es un campo de 16 bytes en los cuales se indican el nombre con quien se desea comunicar. Se deben utilizar los 16 bytes. El nombre puede estar en el propio adaptador o en otro.

### NCB\_NAME

Es un campo de 16 bytes los cuales indican el nombre con que uno es conocido dentro de la red. Siempre se deben usar los 16 bytes. La tabla de nombres del adaptador puede almacenar hasta 16 nombres. Uno será siempre el nombre permanente. El nombre permanente consta de 10 bytes de ceros binarios, seguido de 6 bytes de identificación que se regresan a partir del comando STATUS.

### NCB\_RTO

Es un campo de 1 byte utilizado para especificar el periodo de TIME-OUT de recepción. El TIME-OUT de recepción es el máximo valor permitido antes que el comando RECEIVE regrese un error, se especifica en incrementos de 500 ms.

### NCB\_SIO

Es un campo de 1 byte utilizado para significar un TIME-OUT de envío. Este TIME-OUT de envío es el valor máximo antes de que el comando SEND regrese un error. También se especifica en incrementos de 500 ms.

### NCB\_POST<sub>at</sub>

Es un campo de 4 bytes que indica la dirección de la rutina que se va a ejecutar cuando el adaptador termine de procesar un comando. Este campo solo se usa con opciones NO-WAIT y campo se define en formato de DOUBLE-WORD (*offset segmento*), debe contener una dirección de memoria válida.

**NCB\_LANA\_NUM**

Es un campo de un byte el cual indica cual adaptador se va a usar. El valor 00h marcara el primer adaptador, y el 01h hacia el adaptador alterno (*alternate*).

**NCB\_CMD\_CPLT**

Es un campo de 1 byte que indica el estado del comando (COMMANDSTATUS). Si el valor que se encuentra en este campo es un FFh indica que el comando esta pendiente. Un valor 00 indica que el comando se completo. Cualquier otro valor indica que el comando se ejecuto con un error.

**NCB\_RESERVE**

Es un campo de 14 bytes reservado para que *NetBIOS* almacene variables temporales.



#### 6.4.4 Implementación del NBC

- Estructura del NCB en Pascal

Un ejemplo claro de como implementar esta estructura es su declaración en el lenguaje de programación *Pascal*, que tendrá la siguiente forma:

---

```

Type
  NetName = array [1..16] of char;
  NameOrBufInfo = record
    case boolean of
      FALSE: (name : NetName);
      TRUE : (nextbuflen : word;
              nextBufPtr : pointer)
    end
  end
  NCB = record
    command,
    retcode,
    lsn_num   : byte;
    bufptr   : pointer;
    len      : word;
    callname : NameOrBufInfo;
    name     : NetName;
    rto,
    sto      : byte;
    post     : pointer;
    lana_num : 0..1;
    cmd_cplt : byte;
    reserved : array [1..14] of byte;
  end;

```

---

**NOTA:**

**NetName** es el formato de un nombre usado en las operaciones de red.

**NameOrBufInfo** es un *record* variable que soporta el uso del campo **callname** de un NCB para cada uno e los nombres de red o para el encadenamiento de buffers.

Los tiempos (*timeout*) de **no** y **sto** se dan en medios segundos.

La llamada a *NetBIOS* se implementa a través de la siguiente función:

---

Function **NetBIOS** (var n : NCB) : byte;

```

inline($5B      { pop bx }
/$07           { pop es }
/$CD/$5C      { int $5C }
);

```

---

Esta función llama a *NetBIOS* con el NCB que se le da y regresa el mismo valor que aparece en el campo **RETICODE** del NCB después de la llamada. Los comandos seleccionados con la opción de *NO-WAIT* y la rutina *NO INTERRUPT COMPLETION* regresarán sus resultados finales en el campo **CMD\_CPLT**.

El apéndice E muestra las implementaciones del NCB en lenguaje ensamblador y C.

---

## 7. PLANEACION Y OPERACION DE REDES DE AREA LOCAL



## **7. PLANEACION Y OPERACION DE REDES DE AREA LOCAL**

---

### **7.1 INTRODUCCION**

Para poner en operacion una red de área local se debe pasar por un proceso de planeacion. En esta planeacion se llevan a cabo una serie de pasos esquematicos y procedimientos para su implantacion.

Los pasos esquematicos y procedimientos aseguraran una buena y eficiente instalacion, estos se dividen en cuatro categorias o fases, a las que se les conoce conjuntamente como el ciclo de vida o ciclo de desarrollo de un sistema de informacion basado en computadoras.

### **7.2 CICLO DE DESARROLLO DE UN SISTEMA DE IN- FORMACION BASADO EN REDES DE COMPUTA- DORAS**

La etapa de planeacion de un sistema de informacion basado en computadoras comprende cuatro fases:

**ESTUDIO**

**SELECCION Y  
DISEÑO**

**IMPLANTACION**

**OPERACION**

**Cada una de estas fases se forma de diferentes subfases las cuales deben ser cubiertas para poder pasar a la siguiente**

CUADRO DE DESARROLLO DE UN SISTEMA DE INFORMACION  
BASADO EN REDES DE COMPUTADORAS

FASE 1	OBJETIVO	PUNTO	CONSERVACION	
ESTUDIO	INVESTIGACION Y ANALISIS	RECOLECCION DE INFORMACION		
		DEFINICION DE PROBLEMAS		
		REQUERIMIENTOS DE INFORMACION O DEL USUARIO		
		IDENTIFICACION DE HARDWARE, SOFTWARE Y RECURSOS HUMANOS		
		REPORTE ESCRITO		
ESTUDIO DE FACTIBILIDAD	ANALISIS DE LOGICABILIDAD	REPORTE DE LA FASE DE ESTUDIO	RECOMENDACION DE EFICIENCIA, COSTOS, SEGURIDAD, CONTROL, SERVICIOS Y AREA DE ANEXOS	
FASE 2	OBJETIVO	PUNTO	CONSERVACION	
SELECCION Y DISEÑO	SISTEMA DE SEGURIDAD	DE FISICA Y LOGICA	INSTRUMENTAL (P. DE CONTINGENCIAS)	
		CONSULTA CON EL USUARIO	DESARROLLO DE PROCEDIMIENTOS	
		DESARROLLO DE FICHA DE INFORMACION		
		CONFIGURACION	FISICA Y LOGICA	INSTANCIAS, MEDIO, SERVIDORES, USUARIOS
		EVALUACION DE SOFTWARE		
		EVALUACION DE HARDWARE		
		DEFINICION Y DISEÑO		
REPORTE ESCRITO	RESULTADOS DE LAS EVALUACIONES	DISEÑO PROPUESTO		

PAGE 3	SUBFASE	PUNTOS	OBSERVACIONES
IMPLEMENTACION	PLAN DE IMPLEMENTACION	DISEÑO DE PROGRAMAS	REVISION DEL PLAN
		INSTALACION DE EQUIPO	
		MANEJO DE LAS PRINCIPALES	
		PROBAR EL SISTEMA	
		PROBAR PRUFA	
		E DE MANEJO	
		CAPACITACION DEL PERSONAL	USUARIOS, ADMINISTRADORES DE LA RED
		R DE AVANCES	
PAGE 4	SUBFASE	PUNTOS	OBSERVACIONES
OPERACION	ETAPA DE CAMBIO		RAPIDA, PARALELO O EN FASES
	rutinas de OPERACION	MANTENIMIENTO	HARDWARE, SOFTWARE Y FORMACION
	EVALUACION DEL DESEMPEÑO DEL SISTEMA	ANALISIS DE COSTO	
		RECUPERACION DE INFORMACION	
		INTEGRIDAD DE DATOS	
		CONTACTO CON EL SISTEMA	
		VOLUMEN DE INFORMACION PROCESADA	
		SEGURIDAD Y MANEJO	
	CAMBIO DE SISTEMA		

## 7.3 FASE DE ESTUDIO

La fase de estudio se inicia, de acuerdo a las necesidades y/o justificación para implantar un red de área local en una empresa, organización o corporación. La fase de estudio consta de dos subfases:

- a. Investigación y análisis
- b. Estudio de Factibilidad

### 7.3.1 INVESTIGACION Y ANALISIS.

La parte de la investigación y análisis de la fase de estudio consiste de la recopilación de información concentrada en un reporte escrito. Los hechos e información pueden obtenerse por los siguientes medios:

- a. Recopilación de información de entorno.
  - b. Definición de problemas
  - c. Requerimientos del usuario o información
  - d. Identificación de recursos, fuerzas y debilidades
  - e. Reporte escrito
- 
- a. Recopilación de información de entorno.

Esta es la primera función del proceso de investigación y análisis. La información debe ser proporcionada por la empresa antes de que cualquier análisis pueda completarse. Esta información debe contener la historia de la empresa, su estatus actual y sus perspectivas de crecimiento, políticas de operación, estilos de dirección, ambiente de dirección, ambiente de oficina, componentes únicos de la empresa, un panorama de los presentes sistemas de oficinas y procedimientos, y las actitudes o puntos de vista de las personas que serán afectadas por la red de área local.

Entender las políticas de la empresa le da al análisis un buen panorama, de como debe de crearse o implantarse la red de área local.

#### b. Definición de problemas

Por lo regular existen problemas concretos en los procesos de información de una empresa de la magnitud suficiente para prevenir el análisis de un sistema. Muchas veces, estos problemas no se muestran abiertamente, el identificarlos es una actividad sana dentro del análisis del sistema. Usar la información del entorno de la empresa, hace más fácil esta tarea de identificación de problemas.

#### c. Requerimientos del usuario o información

Cualquier sistema de información que no proporciona a tiempo y de manera adecuada la información tiene una vida corta

Debe tenerse mucho cuidado para asegurar que la información requerida por una empresa y sus empleados se identifique. Este requerimiento implica mucho análisis.

Se debe conocer el volumen y el tipo de información a ser procesado por un sistema de información basado en computadoras:

- área que necesita la información
- tipo de programas de aplicación
- tipo de reportes y formato
- tareas a ser ejecutadas conjuntamente en la red y cuales de manera local
- crecimiento de la organización (a corto, mediano y largo plazo)
- este crecimiento debe ser proyectado y documentado.



Los requerimientos a largo plazo de la gente y de la empresa deben ordenarse para asegurar que la red de área local es una solución viable. De no ser así la más sofisticada red de área local es inservible.

#### d. Identificación de Recursos

Durante la fase de investigación y análisis, los recursos de la empresa deben ser documentados.

Los recursos organizacionales que impactan en la implantación de un sistema de cómputo cae en dos categorías:

- Fuerzas y debilidades en los sistemas de *hardware* y *software*.
- Fuerzas y debilidades en Recursos Humanos

Lo primero a examinar son los recursos de *hardware* y *software* que la empresa actualmente tiene, esto es:

- personal que tiene su propia computadora
- se cuenta con minicomputadoras o computadoras *mainframe* y que tipo de acceso se realiza, es decir, acceso via terminal tonta o se tiene *software* emulador de terminales.
- Las aplicaciones de *software* que la empresa posee

Lo anterior hace posible identificar las verdaderas necesidades además de estimar costos.

Las personas involucradas en la implantación de la red de área local, también deben de ser identificadas. Su nivel y sus actitudes hacia las computadoras y aplicaciones que deben conocer. Esto es necesario para identificar el nivel de capacitación, y quien dará soporte a la red de área local.

Los recursos de una empresa, pueden tomar diferentes formas, incluso los recursos financieros tienen que ser considerados en una primera instancia

#### e. Reporte Escrito

Después de que esta fase de investigación y análisis inicial, se ha completado, toda la información debe ser recopilada, organizada y plasmada en un documento, esta documentación será usada en la siguiente fase de estudio, el estudio de factibilidad.

### 7.3.2 Estudio de Factibilidad

Toda la información recopilada en la etapa de análisis e investigación, debe aplicarse para determinar la factibilidad de la instalación de la red de área local además de elaborar un análisis de costo beneficio, y debe ser plasmado en un reporte escrito.

#### a. Costo y beneficio

Esto debe demostrar, el precio, los beneficios ganados al instalar la red de área local y su justificación en precio. Se debe enriquecer presentando tablas en las cuales se muestre los costos, el tiempo de recuperación de estos, incluyendo tablas de amortización.

#### b. Reporte de la fase de estudio

Este reporte debe contener todos los detalles que no se cubrieron durante la investigación y los resultados del estudio de factibilidad. Toda la información acumulada es estudiada y aplicada para determinar las posibilidades ofrecidas por la red de área local. Si alguna información específica acerca de la red de área local no se tiene, debe obtener información adicional que la sustituya. Finalmente este reporte debe ser una recomendación

Seguramente no todas las necesidades y problemas de una empresa pueden ser detectados, pero el análisis dará el conocimiento de como

opera la red de área local y si esta puede ser beneficiosa. Mas de un análisis debe involucrarse en esta primera etapa. Un primer análisis puede determinar o identificar problemas, procedimientos, limitaciones y recursos. Un segundo análisis puede ser muy controversial en tipo de tecnología de la red de área local y sus aplicaciones, esta información puede obtenerse de la primera alternativa de análisis.

Se debe estar seguro de lo que una red puede ofrecer antes de hacer cualquier tipo de recomendación, esto es muy importante para asegurar el éxito de cualquier estudio de factibilidad o de cualquiera de las fases subsecuentes de implantación.

Siempre debe tenerse cuidado de quien realiza el estudio de factibilidad, si este lo realiza un vendedor, la información y la recomendación podrían inclinarse hacia una producto en específico.

Siempre es aconsejable, conocer quien proporciona que parte de la información, esto con el objeto de realizar el estudio más imparcial posible.

El reporte de la fase de estudio, generalmente se presenta en una junta con aquellos que están relacionados con el proyecto de la red, después de discutir el reporte y sus descubrimientos, se pueden tomar tres alternativas:

- 1) El proyecto se pospone o se cancela. Si este es el caso, toda la investigación y análisis se detiene.
- 2) Se decide que hace falta más información para tomar la decisión. Esto implica que se requiere más información y análisis.
- 3) Se toma la decisión de realizar el proyecto, esto es el ciclo de vida de la red entra en la siguiente fase.

En muchos casos las razones específicas de una empresa para investigar la factibilidad de la instalación de una red de área local no son determinadas. No es común que una red se instale sin razones específicas, pero existe quien también para estar a la moda, decide instalar un red local, esté justificada o no

El fin que persigue la instalación de una red de área local debe basarse en las siguientes premisas:

- Incrementar la eficiencia
- Incrementar el control
- Incrementar la productividad
- Incrementar los servicios
- Ahorrar costos
  
- Incrementar Eficiencia

Al crear una operación más eficiente, debe ser la principal razón para iniciar el estudio del sistema. El análisis debe contemplar cada aspecto de la empresa que sea susceptible de ser eficientado, estos puntos requieren un análisis y una investigación substancial. Todos los sistemas actuales, todos los procedimientos usados y los planes de crecimiento deben ser examinados. Un punto particular que crea ineficiencia y requerimientos específicos de una red de área local es el crecimiento de las empresas.

Posiblemente la empresa ya cuenta con computadoras personales y periféricos que pueden ser incluidos en la red local. Tal vez en empresas muy grandes una solución viable, sea la conexión de un computador *mainframe*.

- Incrementar el control

Actualmente las empresas que los departamentos que las integran, tomen sus propias decisiones sobre el control y procesos de su información. Es preferible esto a tener toda la información concentrada en un solo computador central. Esto implica además

tener personal especializado, el cual puede ser substituido por computadoras personales ya que son menos riesgosas al ser manejadas por personal sin experiencia.

- Incrementar la productividad

El objetivo principal de un jefe es incrementar la productividad de su gente. Una herramienta para lograr esto es la computadora. Claro que una computadora centralizada no puede tal vez ofrecer el tiempo de respuesta y la flexibilidad de procesos que una computadora personal proporciona. Es por esto que cada vez mas se esta optando por proporcionar computadoras conectadas en red a los departamentos de muchas organizaciones.

- Incrementar los servicios

El ideal de cualquier empresa es la de incrementar el tipo de servicios y la calidad de estos. El proceso computarizado de estos puede ser la clave.

La recuperación de la información es fundamental para la buena operación y calidad de cualquier servicio, es por esto que una red puede ser la solución a esta necesidad.

- Ahorro de Costos

Una red de área local debe garantizar que los costos se recuperaran. Por lo regular una red de área local es mas barata que instalar un minicomputador o un pequeño *mainframe*.

Las computadoras personales han abaratado el proceso de la información considerablemente. Las mismas operaciones de cómputo ahora pueden ser realizadas sin necesidad de contar con un *mainframe*. Además una red de computadoras puede ser reubicada en cualquier momento.

## 7.4 FASE DE SELECCION Y DISEÑO

Iniciar con la fase de diseño, implica tomar en cuenta las consideraciones arrojadas por el estudio de factibilidad y los beneficios que se tendrán al implantar la red de área local. Mucha de la información obtenida en la fase de análisis debe ser considerada también en esta fase de diseño.

La selección y diseño deben basarse en los siguientes puntos:

- Sistema de Seguridad
- Consultas con el usuario
- Configuración
- Evaluación del *Software* disponible
- Evaluación del *Hardware* disponible

### 7.4.1 SISTEMA DE SEGURIDAD

El recurso más valioso con que cuenta una empresa después del recurso humano es la información por lo que cualquier medida de seguridad correctiva o preventiva que se aplique debe contemplar a ambos. Para establecer medidas preventivas o correctivas existe un tema muy amplio que se denomina Seguridad Informática

La seguridad informática es la protección de todos los recursos, entendiéndose por estos a personas, instalaciones y datos, contra daños naturales, accidentales o provocados.

La seguridad informática abarca políticas, acciones y equipos relacionados entre sí para brindar el máximo grado de protección posible. La falta en cualquiera de estos puntos debilitaría a la seguridad.

**La seguridad informática en sistemas es necesaria para :**

- **Garantizar que la institución tenga continuidad en su operación, es decir que se pueda seguir trabajando en el caso de que ocurra un desastre y**
- **Que la información procesada en los equipos de cómputo se mantenga confiable (que no se altere) y confidencial (únicamente consultada por personal autorizado)**

**La seguridad va más allá de la protección del centro de cómputo o del lugar designado para colocar al Servidor de una red de área local, puesto que la información es accesible desde terminales remotas o desde los demás nodos de la red**

**Para establecer las medidas de seguridad adecuadas se tienen que identificar los riesgos a los que pueden estar expuestos tanto el personal como los datos, programas, edificio y equipos. Estos riesgos se pueden agrupar de la siguiente manera:**

**Externos :** Los que presenta el medio ambiente que rodea a la instalación de cómputo, ejem., temblores, tornados, sabotaje, vandalismo, etc.

**INTERNOS :** Los que se generan dentro del centro de cómputo, ejem., incendio, alteración de los datos o de información, robo de información, etc.

**Para cada clase de riesgo por lo menos existe una medida de seguridad que adecuadamente implantada minimize su impacto. En seguridad informática estas medidas se clasifican en FÍSICAS y LÓGICAS.**

### Seguridad Física

Contempla las medidas que permitan garantizar la integridad de equipos y recursos de cómputo. Para lograr una adecuada implantación es necesario establecer un PROGRAMA DE SEGURIDAD FISICA.

### Seguridad Lógica

Engloba las medidas que permiten proteger directamente los datos e información contra su pérdida, modificación o divulgación ya sea accidental o intencional. También es necesario establecer un PROGRAMA DE SEGURIDAD LOGICA.

Es importante considerar que para que las medidas de seguridad tanto físicas como lógicas cumplan su objetivo, es necesario establecer procedimientos administrativos adecuados (seguridad procedural), dentro de esta tercera clasificación de seguridad se incluye el Plan de Contingencias.

### PLAN DE CONTINGENCIAS

Su objetivo es contar con procedimientos para el manejo de emergencias en caso de catástrofes o amenazas mayores, para proteger al personal, minimizar el daño a las instalaciones y equipo, así como reducir la magnitud de la interrupción en el servicio.

Los procedimientos de emergencia se aplican a condiciones previas o poco después de una catástrofe y se ejecutan en situaciones no usuales. Son de naturaleza temporal.

Ya que el servicio de cómputo debe mantener una alto grado de privacidad, seguridad, disponibilidad e integridad se define un desastre o contingencia en computación como aquel momento en que alguna de estas características se ve disminuida en la operación de la institución.



**El Programa de Seguridad Física debe abarcar los siguientes aspectos :**

- Ubicación del equipo de cómputo
- Consideraciones en la adecuación del local o en su construcción en caso de que no exista un lugar predeterminado para el equipo cómputo, que reduzcan los riesgos detectados y que faciliten afrontar problemas en caso de que se presenten.
- Control de acceso a zonas restringidas, como es el caso de guardias de seguridad, circuito cerrado, gafetes de personal autorizado, etc.
- Soporte ambiental como son sistemas de aire acondicionado y humedad relativa, determinar rangos ambientales, estos dependen del equipo.
- Protección contra Fuego, Agua, y fallas en el suministro de energía eléctrica para la protección de información, equipo y del personal. Se establecen estándares para una oportuna detección del fuego las medidas a seguir si este se propaga. También medidas preventivas para evitar inundaciones o goteras, acciones para evitar la pérdida o daño de la información a causa de una interrupción en el suministro de energía eléctrica.
- Programa de atención interna y de mantenimiento  
Establecer prácticas de mantenimiento preventivo y correctivo (instalaciones eléctricas, plantas de emergencia y no break, equipo de cómputo, equipos especiales y auxiliares de cómputo, equipo de aire acondicionado, boyedas externas, y tubos de iluminación, pasillos y puertas de emergencia, equipo portátil de pasillo, al almacén de papelería, mobiliario y equipo, etc.

a) **Mantenimiento al *hardware*.** - Una vez que el *hardware* ha sido instalado se deben de tomar en cuenta ciertos procedimientos para asegurar su correcta operación. El *hardware* debe de probarse periódicamente para asegurar su buena operación. Un *software* de diagnóstico puede ser suficiente. Por supuesto si el *hardware* falla debe de repararse o reemplazarse rápidamente. Deben tenerse siempre a la mano los datos suficientes para llevar a cabo el mantenimiento del *hardware*, esto es: número de serie, diagramas del *hardware*, etc.

#### El programa de seguridad lógica debe incluir

- **Esquemas para password.** - Este es un aspecto muy importante. Este procedimiento necesita que los passwords definidos sean almacenados en un lugar seguro en caso de emergencia. Además se deben de crear procedimientos para hacer cambios regulares en los passwords de los usuarios.
- **Archivos de datos.** - Los respaldos de los datos son una parte crucial en el mantenimiento de una red. Se deben crear procedimientos que establezcan y definan la periodicidad de los respaldos, como se deben de realizar, el tipo de dispositivo a emplear y la rotación que deben de tener las cintas.
- **Capacitación al usuario.** - Procedimientos de capacitación a usuarios nuevos se deben establecer. Así como debe crearse un departamento específico el cual sepa sobre la administración de los recursos de la red, sea el encargado de la capacitación a los usuarios.
- **Políticas para la programación de aplicaciones en red.** - Se deben crear procedimientos los cuales proporcionen archivos batch que den soporte a nuevos usuarios.

Además se deben crear los procedimientos para los accesos a las bases de datos que estén en red. Esto es particularmente especial dado que se deben guardar la confiabilidad de los datos.

- **Conexión con otros sistemas.** - Se debe considerar que el departamento especializado en redes cubra las necesidades de conexión de redes entre sí o una red hacia computadores *mainframe*.
- **Estadísticas de uso de red.** - Toda la información acerca de la red de área local debe ser almacenada esto es por si una persona hizo la instalación de la red y se retire no surgan problemas, además deben de conservarse registros de entrada y salida a la red de cada uno de los usuarios.
- **Nuevos usuarios.** - Se deben de tener procedimientos para los nuevos usuarios, para que aplicación tienen permiso de acceso, si pueden utilizar el correo electrónico.
- **Borrado de viejos usuarios.** - Cuando un usuario se retira debe de ser borrado del sistema, esto es borrar su password, archivos, etc.
- **Instalación de *software*.** - Cuando un nuevo *software* es instalado en la red, tiene que ser instalado en el *hardware* necesario para que los usuarios que lo requirieron lo utilicen, además se les debe de avisar que ya fue instalado dicho *software*.

- **Planes de crecimiento de la red** - En el diseño de la red se deben tomar en cuenta las áreas que crecerán dentro de la empresa, esto para configurar adecuadamente la red.
- **Impresiones de red** - Las impresoras deben ser colocadas estratégicamente en el lugar donde haya mayor requerimiento de impresión
- **Monitoreo de la red** - Se debe tener un procedimiento que monitoree el desempeño de la red esto con el fin de prevenir un problema antes de que empiece
- **Mantenimiento al software** - Se deben establecer políticas de mantenimiento del sistema que se realicen sobre la red de área local. Una vez que una aplicación de software ha sido instalada casi siempre requiere poco mantenimiento de hecho solo se actualiza dicha aplicación. Es necesario llevar un registro de todas las aplicaciones con sus números de series y versiones. Parte de este mantenimiento a las aplicaciones los usuarios la pueden llevar a cabo. Esto significa que configuren el sistema escriban archivos parche o modifiquen programas de acceso de acuerdo a sus necesidades. Se deben mantener copias de todos los programas de aplicación instalados en un lugar seguro, así como de los archivos de configuración esto es parte fundamental del mantenimiento al software.

#### 7.4.2 Consulta con los usuarios

Este punto en la fase de diseño requiere que se categorice y se le dé prioridad a los requerimientos del usuario. Sin consultas al usuario una red de área local puede ser técnicamente excelente pero fallar en el momento de ser utilizada o puede no ser utilizada por no cubrir las necesidades del usuario, esto quiere decir que no importa cuanto tecnología o dinero se utilice en una red si no se toma en cuenta al usuario

### - Desarrollo de Nuevos Procedimientos

Conjuntamente con el usuario se deben determinar nuevos procedimientos puesto que cuando un nuevo sistema se va a introducir en una empresa, los métodos de trabajo empleados por ésta deben ser modificados o eliminados muchas veces aparecen nuevos procedimientos que deben ser desarrollados contemplando la operación de la red. Es importante tener la capacidad de preparar y diseñar nuevos métodos para la operación de la empresa.

### - Desarrollo de cartas del flujo de la información

La información se recoge de muchos lugares tanto de la fase de estudio como del medio ambiente de la empresa. Cuando la red de área local se diseñe no solamente cambiarán procedimientos sino que también el flujo de información debe cambiar.

## 7.4.3 Configuración

### - Selección de la mejor topología

En gran parte depende de la marca y equipo que se tiene.

En lo que a token ring se refiere, por ser un sistema abierto, tiene gran capacidad de interconexión.

### - Selección del medio de transmisión adecuado.

El cable coaxial (Para *Ethernet* y *Arnet*) tiene una increíble base instalada y es ampliamente utilizado, pero hay quienes se inclinan por el par de cable trenzado por versátil y menos caro. Para redes *Ethernet* y *Arnet* el cable de par trenzado es una excelente opción, para *Token Ring* es la única.

En muchos casos, la opción es cable blindado o no blindado. El cableado blindado se puede emplear en distancias mayores y hace posible alcanzar grandes distancias de transmisión, aunque es más

costo. El cableado con fibra óptica es otra opción aunque es muy frágil y requiere de un alto nivel de seguridad.

La fibra óptica se emplea para cubrir las trayectorias más grandes o muy verticales, y el par trenzado para cablear los closets de distribución y áreas cortas. En redes *Ethernet*, el cable coaxial delgado puede ser empleado para rutas verticales o muy largas.

#### 7.4.4 Evaluación de *software*

Es responsabilidad del diseñador de la red evaluar los diferentes paquetes de *software* disponibles y seleccionar aquellos que más se ajusten a los requerimientos de los usuarios. El *software* de aplicación para los usuarios debe ser determinado en la fase de estudio. En este punto el *software* adecuado debe ser identificado para cubrir esas necesidades.

Existen muchas consideraciones que deben tenerse en cuenta cuando se evalúa *software* como:

- que cubra las necesidades de los usuarios
- se considere fácil de usar.
- compatibilidad con el sistema operativo
- que cubra con los requerimientos de seguridad propuestos por la empresa. Sin embargo el diseño de la red puede compensar la seguridad no ofrecida por el paquete de *software*
- requerimientos de *hardware*
- potencial del *software* de red
- Si al *software* se le han encontrado posibles adaptaciones disponibilidad del proveedor o del vendedor para realizar las adecuaciones.

- costo del *software*.
- costo de las actualizaciones
- documentación proporcionada suficiente, adecuada e informativa.
- compatibilidad del *software* con la red
- capacitación

#### 7.4.5 Evaluación de *hardware*

Para realizar una buena evaluación de *hardware*, se deben considerar los siguientes puntos :

- Verificar el *software* que incluye la red
- Soporte al *software* que ha sido recomendado.
- Capacidad del proveedor para proporcionar soporte en sus propias instalaciones
- Garantía por un periodo de tiempo
- Contrato de servicio de mantenimiento
- Debe cumplir con la industria de estándares
- Documentación adecuada
- Capacitación si es que es necesario
- Costo del *hardware*.
- Flexibilidad para cubrir necesidades futuras.

Para crear la red local mas apropiada para una ambiente se requiere de toda la información recopilada en la fase de estudio y el reporte de factibilidad. Además la información de la evaluación de *hardware* y *software* debe estar disponible en el proceso de diseño.

Los problemas identificados durante la fase de estudio deben ser tomados en cuenta para diseñar un sistema que direcciona y corrija cada uno de los problemas listados. Además el sistema debe cubrir los requerimientos establecidos en las evaluaciones de *hardware* y *software*. También es importante poder hacer cambios al diseño y poder considerar productos alternos.

### Reporte de la fase de diseño

Una vez que el sistema ha sido diseñado, el diseño debe ser presentado en un reporte. Este reporte debe ser revisado por el comité que este involucrado en este proyecto. Si el diseño es aceptado, entonces la siguiente fase, la implantación comenzará. Si el diseño no es aceptado, entonces otro diseño debe ser creado que direcciona las objeciones del comité.

## 7.5 FASE DE IMPLANTACION

La fase de implantación o fase de desarrollo como comúnmente se le llama es donde la red de área local es entregada, instalada, probada, y puesta en operación.

Este es el punto donde los usuarios empiezan a ver el sistema. Donde la recolección de información y análisis muestran los resultados de forma tangible. El trabajo diario comenzará a cambiar durante la implantación del sistema, así que el instalador, esto es, la persona responsable de la implantación actual debe estar al tanto de los usuarios y de sus inquietudes. El responsable del proyecto debe de tomar tiempo para hablar con los usuarios, para explicarles el cambio que se hará y ayudarlos a adquirir una actitud positiva entorno a la red.

Cabe mencionar que los componentes designados durante el diseño de la red de área local pueden ser modificados aquí. Consideraciones que fueron omitidas durante la fase estudio y diseño pueden ser corregidas en este punto. Debe notarse que cualquier cambio al *software* o *hardware* seleccionados, deben ser comunicados al comité de seguimiento del proyecto.

Para entrar a la fase de implantación, lo primero que hay que hacer es desarrollar un Plan de Implantación que plasme paso a paso todos los procedimientos necesarios para habilitar el sistema.



### 7.5.1 Plan de Implantación

Una vez que el sistema a sido seleccionado y las especificaciones detalladas, el siguiente paso es desarrollar un plan, el cual describirá como se instalara el sistema. El plan de implantación debe plasmar en papel cuidadosamente todos los procedimientos y pasos necesarios para habilitar al sistema.

En el se deben tomar en cuenta las siguientes actividades :

- a. Diseño de programas de computadora
- b. Reunión de avances
- c. Instalación del equipo
- d. Desarrollo de los programas de computadora
- e. Pruebas del sistema
- f. Pruebas del *software*
- g. Desarrollo de Manuales
- h. Capacitación del Personal
- i. Reunión final de avances

Es común que la fase de implantación tome más tiempo que las fases de estudio o diseño. Una gran cantidad de trabajo debe realizarse antes que se pueda completar.

El tiempo de instalación de una red de área local puede variar. Como puede durar un par de semanas o varios meses, esto depende de la magnitud del proyecto.

Dependiendo del tamaño del proyecto, el plan de implantación puede ser complejo o muy simple. Este plan incluso debe permitir cierta flexibilidad.

Aquellos que participan en el plan de implantación deben ser totalmente competentes y experimentados en este tipo de

situaciones. Si un vendedor es el encargado de este plan, es recomendable la participación de un asesor que valide este plan.

#### a. Diseño de los programas de computación

Los programas de computación que se consideran en esta fase son los que se crearán o adecuaran, e incluso los paquetes comerciales que se acordaron durante la fase de diseño.

Adecuar *software* ya desarrollado puede ser necesario. Esto generalmente no es realizado por el departamento especializado en redes, si no que es encargado al departamento de desarrollo de *software*.

#### b. Reunión de avances

A esta altura del proyecto ya se debieron haber concertado varias reuniones de avances al finalizar las etapas de estudio y diseño. Se aconseja tener una reunión intermedia en la fase implantación, esto para determinar que el plan de implantación se aprueba por las personas relacionadas con el proyecto de la red de área local.

Dos cosas deben resultar de esta reunión. La primera, si el plan de implantación no es aceptado, se debe modificar o totalmente se debe rediseñar. Segunda, si el plan es aprobado la instalación continúa adelante.

#### c. Instalación del equipo

El vendedor del equipo puede ser contratado también para realizar la instalación de la red, o se puede contratar a otra empresa para que realice esta etapa. No importa quien instale el equipo, lo que si importa es que la instalación debe ser supervisada. Generalmente esta supervisión la lleva a cabo la persona que realizó el plan de implantación.

Una vez que el equipo ha sido instalado, se deben realizar diagnósticos. Esto para evitar problemas que generalmente se presentan después de la instalación de un equipo.

#### d. Desarrollo de los programas de computadora

El desarrollo de los programas que requieran ser desarrollados o modificados se puede llevar a cabo mientras se realiza la instalación del equipo, de hecho se pueden empezar una vez que el comité ha aprobado el proyecto.

Una persona debe monitoriar el desarrollo de estos programas. Este puede ser un líder de proyectos el cual reporte a un gerente de desarrollo. Estas personas deben estar familiarizados con las fases de estudio y diseño. Además claro que deben manejar las técnicas y metodologías de programación.

#### e. Pruebas del Sistema

Una vez que los componentes se han probado después de su instalación, el sistema en conjunto debe ser probado. Se debe estar seguro que todas las piezas funcionan independientemente y como un todo. Estas pruebas se deben ejecutar varias veces simulando diferentes variantes.

##### 1. Pruebas del Software.

Ya probados todos los componentes de *hardware*, los programas de aplicación pueden ser instalados en la red de área local. Estos programas deben ser probados para asegurar la integridad de los datos. Es preferible tomarse más tiempo, para asegurarse que los programas hayan sido bien diseñados o instalados, que perder el tiempo después para tratar de componerlos ya estando en producción.

### g. Desarrollo de Manuales

Se deben desarrollar manuales para documentar cada fase del sistema. El administrador de manuales debe tener una copia de las especificaciones del cableado, el mapa del cableado, la estructura del computador servidor, incluyendo la estructura de su disco duro, en resumen, cualquier cosa que impacte en el diseño de la red, debe ser documentada en los manuales del sistema.

Toda la documentación es muy valiosa, no importa el tiempo que se tome para la realizarla, si en un futuro nos ahorrará dinero y tiempo.

### h. Capacitación de personal

La capacitación debe ser considerada durante el plan de implantación, pueden existir dos diferentes tipos de capacitación:

- para el administrador de la red
- para el usuario de la red

Una sola persona o varias pueden tomar el compromiso de la red de area local. Un red no puede trabajar por si sola diariamente, es necesario realizar diferentes tareas y monitorearla. Los seleccionados para esto deben ser entrenados en el *software* y *hardware* de la red.

Los usuarios de la red solo deben conocer lo básico de ciertos comando de su operación, esto para que no estén constantemente preguntado que hacer al administrador de la red.

### i. Reunión final de avances

Después que los planes de capacitación se han llevado a cabo, se debe realizar una reunión final. Estas reuniones toman dos posibles caminos. Si todo va de acuerdo al plan y la implantación marcha satisfactoriamente, la fase de operación se aproxima. Por el otro lado, si la implantación no es satisfactoria, las áreas involucradas deben detenerse a redefinir y discutir.

Esta reunión determina si el proyecto pasa a la siguiente fase.

## 7.6 FASE DE OPERACION

La última fase del ciclo de vida de un sistema de información basado en redes de computadoras es la etapa de operación, la cual se puede dividir en cuatro categorías:

- a. Periodo de cambio.
- b. Rutinas de operación
- c. Evaluación del desempeño del sistema
- d. Cambios al sistema

La fase de operación se considera como la más larga en el ciclo de vida de una red de área local.

- a. Periodo de cambio

Normalmente se requiere un periodo de transición para cambiar de un sistema viejo a uno nuevo. Este periodo de cambio es el punto más crítico en un sistema de información.

El periodo de cambio por lo regular es un proceso en una sola dirección, el cual debe resultar en la aceptación del sistema. Claro está que pueden existir problemas e incidentes en esta frontera. Esto implica que se debe tener mucho cuidado en conservar las actitudes positivas en todos los involucrados en el cambio.

Existen diferentes métodos para realizar este periodo de cambio. Los tres mas comunes son los siguientes:

- Una conversión rápida
  - Una conversión en paralelo
  - Una conversión por fases
- Conversión rápida

En esta conversión simplemente el sistema viejo termina y el sistema nuevo empieza. Este método generalmente tiene el impacto mas severo sobre los usuarios, los fines de semana y los días festivos son perfectos para este tipo de conversión.

Esta conversión es la mas simple y menos costosa, pero si la mas riesgosa. El mayor riesgo es que el nuevo sistema no opere como se esperaba, y cree mucho mas problemas. Esta tecnica no es aconsejable para organizaciones que tienen una gran necesidad de información.

Si este método se selecciona, debe existir un plan de contingencia. Este plan es una alternativa que debe contemplar las fallas del sistema y como solucionarlas.

- Conversión en paralelo

La conversión en paralelo permite que el viejo sistema sea cambiado al nuevo con un desfaseamiento.

El nuevo sistema es puesto en operación al mismo tiempo que el viejo sistema esta trabajando, así ambos sistemas están operando al mismo tiempo.

Durante este periodo ambos sistemas son comparados para aislar los problemas que el nuevo sistema puede ocasionar. Con la conversión en paralelo, si un error es detectado en el nuevo sistema, la empresa

no sufre, esto porque el viejo sistema aun esta trabajando. Una ventaja adicional es que el nuevo sistema puede ser afinado.

El método de conversión en paralelo esta libre de riesgos, pero debe ser soportado con una mayor cantidad de recursos ya que deben de tenerse dos sistemas operando simultáneamente.

#### - Conversión por fases

Como su nombre lo indica esta conversión se realiza por módulos o fases. El viejo sistema es convertido al nuevo sistema de acuerdo a una serie de fases preplaneadas. Cuando una fase se termina y se valida se comienza con la siguiente fase. Este proceso se continua hasta que todas las fases se han concluido, transformando así al viejo sistema en el nuevo.

La ventaja de este método es que si una fase presenta problemas o errores, puede ser corregida y ajustada.

Este metodo de conversión es mas barato que el método de conversión paralelo.

#### b. Rutinas de operación

Cuando la fase de conversión se ha terminado, la red de área local es considerada como operacional. Desafortunadamente no se toman en cuenta pequeñas consideraciones o recursos para la operación y mantenimiento del sistema. Todo sistema de información debe tener rutinas de mantenimiento y operación en las siguientes áreas esta para asegurar su óptima operación.

- Mantenimiento al *Hardware*
- Mantenimiento al *Software*
- Mantenimiento a la Programación

### - Mantenimiento al *Hardware*

El *hardware* debe tener un mantenimiento preventivo, no se debe esperar a que suceda una falla para darle un mantenimiento.

Esto implica que debe existir un plan de mantenimiento preventivo al *Hardware* de la red de área local. Además de contemplar todos los requerimientos de este *Hardware* para su operación.

### - Mantenimiento al *Software*

El *Software* y los datos siempre deben de ser almacenados en un dispositivo secundario, si los programas o datos se pierden una empresa puede verse en verdaderas dificultades.

Los procedimientos de respaldo son parte fundamental de la operación de una red.

El mantenimiento al *Software* no parece ser tan importante como el mantenimiento al *Hardware*, pero de hecho es la parte más importante. Una computadora personal puede ser remplazada, pero no así los datos que se han acumulado a lo largo de seis meses de trabajo, por ejemplo.

### - Mantenimiento a la programación

Para aquellos sistemas que fueron modificados, adecuados o creados para la red de área local el mantenimiento a los programas puede ser necesario. Se requieren procedimientos parecidos a los del mantenimiento de *Software*. Estos cambios requieren ser monitoreados constantemente.



### c. Evaluación del desempeño del sistema

Después que el nuevo sistema de información ha trabajado por un periodo razonable de tiempo, el sistema debe ser evaluado. Los resultados de esta evaluación se presentan en un reporte de evaluación, el cual permite a la empresa ver que la red de área local esta proporcionando los resultados esperados.

En este punto los fuertes y debilidades del sistema llamarán la atención de los ejecutivos de la empresa. Es aquí también donde correcciones al sistema se pueden dar.

Los siguientes puntos se pueden considerar para realizar dicha evaluación del sistema:

- Análisis de costos
- Facilidad en la recuperación de información
- Integridad de datos
- Personal en contacto con el sistema
- Cantidad de datos procesados
- Seguridad
- Mantenimiento

### d. Cambios al sistema

Todas las empresas son dinámicas; siempre buscan el cambio, esto debe de considerarse en la implantación de cualquier sistema de información.

Durante la evolución de la empresa, puede ser necesario realizar cambios dentro de la red.

Esto concluye con el ciclo de vida de un sistema de información basado en redes de computadoras.

---

## 8. CONCLUSIONES

Después de realizar el presente trabajo nos damos cuenta que en la actualidad no siempre es necesario contar con sistemas centralizados, ya que las redes de área local permiten a los usuarios trabajar de manera independiente y a la vez aprovechar recursos comunes para el intercambio de información o para el empleo de dispositivos especializados, por lo que esto también permite abaratar costos.

La versatilidad de *token ring* permite tener acceso a diferentes sistemas de cómputo centralizado que procesen la información de manera instantánea y entonces aprovechando las bondades de los sistemas de comunicación distribuirla a cualquier punto.

Para lograr lo anterior es indispensable contar con la rapidez, facilidad y confiabilidad en las actividades que se desean desarrollar, por lo que *Token Ring* gracias a sus características es capaz de proporcionar toda la seguridad requerida pese a lo complejo de sus procedimientos internos de control.

Este documento describe el esquema básico de entorno en cuanto a *Token Ring* se refiere.

El presente trabajo es una base para los diseñadores de redes que deseen trabajar con redes de área local, además de dar los puntos para que las investigaciones en este campo continúen.

*Token Ring* es una red de área local técnicamente muy planeada por lo que su diseño involucra especialistas de diferentes áreas como son ingenieros eléctricos, electrónicos, mecánicos, en computación, industriales, matemáticos, etc. y la bibliografía es bastante amplia. Para su desgracia comercialmente se lanzó al mercado muy tarde, cuando otras topologías ya tenían mucha fuerza comercial y además la firma comercial que la apoyó se considera como una de las más caras del mercado aunque técnicamente es muy buena.

**El último capítulo de la presente tesis, es una guía para lograr la operación óptima de una red de área local y abarca los puntos que cualquier buen diseño debe cubrir y que la mayoría de las veces se pasan por alto por lo que lo consideramos uno de los más importantes puntos a considerar del trabajo.**

---

## 9. APENDICES

# 9. APENDICES



## APENDICE A

### TABLA DE DISTANCIAS MAXIMAS CON MULTIPLES CLOSETS DE ALAMBRADO

NC NUMERO DE CLOSETS DE ALAMBRADO

	2	3	4	5	6	7	8	9	10	11	12
02	1182										
03	1163	1148									
04	1145	1120	1104								
05	1106	1081	1074	1061							
06	1078	1062	1047	1032	1017						
07	1049	1034	1019	1004	0989	0974					
08	1021	1005	990	975	0960	0945	0930				
09	0992	0977	0962	0947	0932	0916	0901	0886			
10	0964	0948	0933	0918	0903	0888	0873	0858	0843		
11	0935	0920	0905	0890	0874	0859	0844	0829	0814	0799	
12	0906	0891	0876	0861	0846	0831	0816	0801	0786	0770	0755
13	0878	0863	0848	0833	0817	0802	0787	0772	0757	0742	0727
14	0849	0834	0819	0804	0789	0774	0759	0744	0729	0713	0698
15	0821	0805	0791	0775	0760	0745	0730	0715	0700	0685	0670
16	0792	0777	0762	0747	0732	0717	0702	0687	0671	0656	0641
17	0764	0749	0733	0718	0703	0688	0673	0658	0643	0628	0613
18	0735	0720	0705	0690	0675	0660	0645	0629	0614	0599	0584
19	0707	0691	0676	0661	0646	0631	0616	0601	0586	0571	0556
20	0678	0663	0648	0633	0618	0603	0587	0572	0557	0542	0527

NOTA : LAS UNIDADES SE ENCUENTRAN EN PIES  
NC : NUMERO DE CONCENTRADORES

**APENDICE B**

**TABLA DE MANEJO DE DISTANCIAS  
CON REPETIDORES DE COBRE**

**NC** NUMERO DE CLOSETS DE ALAMBRADO

0	1	2	3	4	5	6	7	8	9	10	11	12
1	1235											
2	1207	1192										
3	1179	1164	1148									
4	1150	1135	1120	1104								
5	1121	1106	1091	1076	1061							
6	1093	1078	1062	1047	1032	1017						
7	1064	1049	1034	1019	1004	989	974					
8	1036	1021	1005	990	975	960	945	930				
9	1007	992	977	962	947	932	916	901	886			
10	979	964	948	933	918	903	888	873	858	843		
11	950	935	920	905	890	874	859	844	829	814	799	
12	921	906	891	876	861	846	831	816	801	786	770	755
13	893	878	863	848	833	817	802	787	772	757	742	727
14	864	849	834	819	804	789	774	759	744	729	713	698
15	836	821	806	791	775	760	745	730	715	700	685	670
16	807	792	777	762	747	732	717	702	687	672	657	642
17	779	764	749	733	718	703	688	673	658	643	628	613
18	750	735	720	705	690	675	660	645	630	615	600	585
19	721	707	691	676	661	646	631	616	601	586	571	556
20	693	678	663	648	633	618	603	587	572	557	542	527

**NOTA:** LAS UNIDADES SE ENCUENTRAN EN PILES  
**NC:** NUMERO DE CONCENTRADORES

## APENDICE C

### LISTA DE COMANDOS DEL NETBIOS

CODIGO (HEX)	COMANDO	ESTADO (OPCION)
10	wait	wait
11	listen	wait
12	send	wait
14	send	wait
15	receive	wait
16	receive ADV	wait
17	chain send	wait
21	send datagram	wait
21	receive datagram	wait
22	send multiplexed datagram	wait
23	receive multiplexed datagram	wait
30	add name	wait
31	delete name	wait
32	reset	wait
33	adapter status	wait
34	session status	wait
35	cancel	wait
36	add group name	wait
70	union	wait
90	call	no wait
91	listen	no wait
92	hang up	no wait
94	send	no wait
95	receive	no wait
96	receive ADV	no wait
97	chain send	no wait
A0	send datagram	no wait
A1	receive datagram	no wait
A2	send multiplexed datagram	no wait
A3	receive multiplexed datagram	no wait
B0	add name	no wait
B1	delete name	no wait
B3	adapter status	no wait



## APENDICE D

### LISTA DE REQUERIMIENTOS Y CODIGOS DE REGRESO DE LOS COMANDOS DE NETBIOS

COMANDO	ADRESA O C H A KWAITWAI	REQUIERE	REGRESA
START	22	1, 2, 4, 12	2, 12
CANCEL	23	1, 2, 12	2, 12
ADAPTER STATUS	B3 23	1, 8, 6, 7, 12 111, 12	2, 6, 13
ONLINE	29	12	2, 13
ADD_NAME	B0 29	1, 8, 111, 12	2, 4, 12
ADD_GPO_NAME	B6 29	1, 8, 111, 12	2, 4, 12
DELETE_NAME	B1 21	1, 8, 111, 12	2, 12
CALL	90 10	1, 7, 8, 9, 10, 11 112	2, 3, 13
LISTEN	91 11	1, 7, 8, 9, 10, 11 112	2, 3, (7), 13
HANG UP	92 12	1, 2, 111, 12	2, 13
SEND	94 14	1, 2, 9, 8, 2, 13 111, 12	2, 13
CHAIN SEND	97 17	1, 2, 6, 7, 111, 12	2, 2, 13
RECEIVE	9D 15	1, 2, 5, 111, 12	4, 8, 13
RECEIVE ANY	9E 16	1, 2, 4, 5, 6, 2, 3, (4), 6, 13 111, 12	2, 3, 13
SESSION STATUS	B4 14	1, 8, 6, 7, 12, 13 111, 12	2, 6, 13
SEND DATAGRAM	A0 20	1, 4, 6, 6, 7, 2, 13 111	2, 13
SEND BROADCAST DATAGRAM	A2 22	1, 4, 6, 6, 2, 13 111, 12	2, 13
RECEIVE DATAGRAM	A1 21	1, 4, 6, 6, 2, 6, 7, 13 111, 12	2, 6, 7, 13
RECEIVE BROADCAST DATAGRAM	A3 23	1, 5, 6, 111, 2, 6, 7, 13 12	2, 6, 7, 13

#### NOTACION

- 1 NÚM. COMANDO
- 2 NÚM. BUCLEO
- 3 NÚM. LÍM.
- 4 NÚM. NÚM.
- 5 NÚM. BUFFER
- 6 NÚM. LONGITUD
- 7 NÚM. CALLNAME
- 8 NÚM. NOMBRE
- 9 NÚM. BTO
- 10 NÚM. STG
- 11 NÚM. POST@
- 12 NÚM. IANA NÚM.
- 13 NÚM. CMD. CPT
- 14 NÚM. RTRV

## APENDICE E

### DESCRIPCION DE CODIGOS DE REGRESO

VALOR	TIENE	INDICIA	DEL	TIPO	DE	REGRESO
00						COMMAND COMPLETED
01						INVALID BUFFER LENGTH
02						INVALID COMMAND
03						COMMAND TIME-OUT
04						MESSAGE INCOMPLETE
05						INVALID LOCAL SESSION NUMBER
06						NO RESOURCE AVAILABLE
0A						SESSION ALREADY
0B						COMMAND SCHEDULED
0C						DUPLICATE NAME IN LOCAL NAME TABLE
0E						NAME TABLE FULL
0F						COMMAND COMPLETED
11						LOCAL SESSION TABLE FULL
12						SESSION WITH REQUESTED
13						INVALID NAME NUMBER
14						NO ANSWER
17						INVALID HOST
18						NAME IN USE ON REMOTE NODE
17						NAME DELETED
1D						SESSION ENDED AND DROPPED
19						NAME IN FLIGHT DELETED
21						INTERFACE Busy
22						THE NAME COMMANDS OVERHANDLING
23						INVALID NUMBER IN PORT AND LOCAL FIELD
24						COMMAND COMPLETED WHILE CHANNEL IS OCCUPYING
26						COMMAND NOT VALID IN LABEL
40						ADAPTER MALFUNCTION IN
50						ADAPTER HAS FUNCTION
FF						COMMAND PENDING STATUS

## APENDICE F

### Implementacion del NCB en Ensamblador y C

MASM:

```

;      Ncb Structure

Ncb    struc
      Ncb_Command    db 00h
      Ncb_RetCode    db 00h
      Ncb_Lsn        db 00h
      Ncb_Num         db 00h
      Ncb_BufferOff  dw 0000h
      Ncb_BufferSeg   dw 0000h
      Ncb_Length     dw 0000h
      Ncb_CallName   db 16 dup(0)
      Ncb_Name       db 16 dup(0)
      Ncb_Rto        db 00h
      Ncb_Sto        db 00h
      Ncb_PostOff    dw 0000h
      Ncb_PostSeg    dw 0000h
      Ncb_Lana_Num   db 00h
      Ncb_Cmd_Cplt   db 00h
      Ncb_Reserve    db 14 dup(0)
Ncb    ends

```

**C:**

```
# define USGC unsigned char
# define USGI unsigned
# define USGL unsigned long
```

```
struct Neb
```

```
{
    USGC  NebCommand;
    USGC  NebRetCode;
    USGC  NebLsn;
    USGC  NebNum;
    char  * NebBufferOffset;
    USGI  NebBufferSegment;
    USGI  NebLength;
    char  NebCallName[16];
    char  NebName[16];
    USGC  NebRto;
    USGC  Sto;
    char  * NebPostRtnOffset;
    USGI  NebPostRtnSegment;
    USGC  NebLanaNum;
    USGC  NebCmdCplt;
    char  NebReservedArea[14];
} ZeroNeb;
```

---

## 10. GLOSARIO



## 10. GLOSARIO

---

### **ANSI:**

American National Standards Institute. Es una organización que funciona como coordinadora de estándares en los Estados Unidos de América.

### **ASCII:**

American Standards Committee for Information Interchange. Es la organización americana, encargada en imponer los estándares del intercambio de información.

### **BACK END NETWORK APPLICATION:**

Aplicación de red que apoya a ésta dentro del computador anfitrión.

### **BACKBONE:**

Trayectoria principal de la interconexión de redes, generalmente enlaza a los puentes de una red para lograr una estructura de alta velocidad.

### **BASEBAND:**

Método de transmisión de señales, el cual emplea una sola frecuencia como base de la comunicación.

### **BIT:**

Minima unidad de información, la cual se puede representar por un 1 ó 0, T ó F, etc.

**BRIDGES:**

Puente, es una unidad de hardware y software dentro de una red, que puede realizar la interconexión de redes con el mismo entres sí y asegurar su independencia.

**BROADBAND:**

Método de transmisión de señales el cual emplea todo el ancho de banda para realizar la comunicación.

**BROADCAST:**

La transmisión de un mismo mensaje a todas las estaciones de una red, simultáneamente.

**BUFFER**

Es un área de almacenamiento temporal, que guarda los datos a ser transmitidos por un momento.

**CCITT**

*Consultative Committee International Telegraph and Telephone* La cual es un organismo internacional para regular todos los estándares de comunicación de datos.

**CIRCUIT SWITCHING**

Conexión física entre dos nodos de una red de comunicación, la cual se emplea en una red conmutada.

**CLOCKWISE:**

Movimiento de acuerdo a las manecillas del reloj.

**COUNTER:**

Es un dispositivo, que puede ser un registro o una localidad de memoria, el cual se usa para representar el número de ocurrencias de un evento.

**CPU:**

Central Processing Unit. (unidad central de proceso)

**CSMA/CD:**

Control Sense Medium Access / Carrier Detected

**DATAGRAMA:**

Es el paquete de mínima información que fluye a través de una red.

**DC**

Direct Current, (corriente directa)

**DES:**

Data Encryption standars



**DPLL:**

Digital Phase-Locked Loop, es un circuito de control de fase digital.

**ECMA:**

European Computer Manufacturers Association

**EIA:**

Electronic Industries Association

**FDDI:**

Fiber Distributed Data Interface

**FEP:**

Front End Processor, Procesador frontal, el cual se dedica a realizar toda la labor de comunicaciones para el computador anfitrión.

**FIRMWARE:**

Es un programa que se encuentra dentro de una memoria de solo lectura (ROM), es una combinación de software y hardware.

**FRAME:**

Es un paquete de información, el cual viaja a través de una red.

**GATEWAYS:**

Es un dispositivo, el cual permite la interconexión de redes con diferente protocolo de comunicación.

**HARDWARE**

Es conocido como el conjunto de elementos eléctricos, mecánicos y electrónicos de los sistemas de cómputo.

**IEEE.**

Institute of Electrical and Electronics Engineers Computer Society, la cual es una organización interesada en los sistemas de cómputo y sus usuarios.

**IP:**

Internet Protocolo

**ISDN:**

Integrated Services Digital Network, Servicios de red digital integrados

**ITU:**

International Telecommunications Union

**LAN:**

Local Area Network, Red de Area Local

**LLC:**

Logical Link Control, es el nivel de liga de datos

**MAC:**

Medium Access Control, es el control de acceso al medio

**MODEM:**

MOdulator/DEModulator, es un dispositivo, el cual transforma las señales digitales en señales analógicas y viceversa.

**MSAU:**

MultiStation Access Unit, Es un dispositivo de hardware diseñado para las redes token ring, donde todas las estaciones se concentran, también se le conoce como MAU.

**NCB:**

**Network Control Block**, es un espacio de almacenamiento dedicado por el sistema operativo para el manejo de las interrupciones de red.

**NETBIOS**

**Network Basic Input Output System**, es una extensión del sistema operativo para realizar todo el manejo de la red.

**PHANTOM CIRCUIT:**

Es el circuito virtual que forman los relevadores internos del concentrador.

**PSDN:**

**Public Switch Data Network**, Red pública de conmutación de datos.

**PSTN:**

**Public Switch Telephone Network**, Red pública de Teléfonos.

**RAM:**

**Random Access Memory**, memoria de acceso aleatorio.

**REGISTER:**

Es un dispositivo de alta velocidad, el cual se usa como una unidad de almacenamiento temporal, en la unidad de proceso temporal.

**REPEATER:**

Es un dispositivo de hardware, empleado para regenerar las señales eléctricas en una red, cuando la distancia de la conexión directa se excede de un cierto límite.

**SNA:**

System Network Application, es el estándar de redes de IBM.

**SOFTWARE:**

Es el conjunto de programas e instrucciones que le indican a un sistema de cómputo que hacer.

**SPANNING TREE**

Es una técnica de ruteo, la cual desarrolla automáticamente una tabla de rutas, que se actualiza dinámicamente en respuesta a cualquier cambio de topología.

**STAR-WIRE:**

Es una topología de redes donde las estaciones de trabajo se unen en un solo punto conocido como concentrador.

**TOKEN:**

Es un conjunto de bits, empleado para indicar que una estación de trabajo puede hacer uso de la red.

**TOKEN ACCESS CONTROL:**

Protocolo de comunicación, el cual usa el concepto de token para permitir el acceso al medio de transmisión

**WAN:**

Wire Area Network, Red de comunicación de cobertura amplia.

**WIRING CONCENTRATOR:**

Es la estructura donde se apilan, los concentradores de la red de área local, también se les conoce como racks

**WIRING LOBES:**

Es el cableado que va desde la estación de trabajo hasta el concentrador

**WRAP-BACK:**

Es la ruta alterna que toma el flujo de información cuando el concentrador falla.

---

## 11. BIBLIOGRAFIA



## **11 . BIBLIOGRAFIA**

---

### **1) DATA COMMUNICATIONS, COMPUTER NETWORKS AND OSI**

Fred Halsall

### **2) TUTORIAL: COMPUTER COMMUNICATIONS, ARCHITECTURES, PROTOCOLS AND STANDARDS**

Williams Stallings

Computer Society, 1989

### **3) INTEGRATED PERSONAL COMPUTING HANDBOOK DIGITAL, 1990**

### **4) NETBIOS APPLICATION DEVELOPMENT GUIDE**

IBM, 1989

### **5) C PROGRAMMER'S GUIDE TO NETBIOS**

David Schwaderer

Howard W. SAMS, 1990

### **6) INSIDE NETBIOS**

J. Scott Haugdahl

Architecture Technology Corporations, 1988

### **7) OPERATING THE IBM PC NETWORKS**

Paul Berry

SYBEX, 1990



---

**8) NETWORKING PERSONAL COMPUTERS 3rd Edition**

Durr Gibbs

QUE, 1991

**9) LAN PRIMER ( AN INTRODUCTION TO LOCAL AREA NETWORKS)**

Greg Nunnemaker

M & T, Books, 1990

**10) LOCAL AREA NETWORKS**

Alan Rinzler and David Ganzler

ComputerLand, 1991

**11) LOCAL NETWORKS / 3ed**

William Stallings

Mac Millan, 1990

**12) Articulos de las revistas**

BYTE.

PC WORD.

DATA COMUNICATIONS

COMPUTER WORD

LAN

UNIX WORD.