

11126
539



**UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN**

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES-CUAUTITLAN

**Telefonía digital y RDSI:
"CONEXIÓN DE REDES LAN EN UN CENTRO DE
CONTROL DE TRAFICO AÉREO"**



DEPARTAMENTO DE
EXAMENES PROFESIONALES

TRABAJO DE SEMINARIO:
QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

LUIS GABRIEL MARTÍNEZ FLORES

ASESOR: ING. BLANCA DE LA PEÑA VALENCIA.

CUAUTITLAN IZCALLI, EDO. DE MEXICO 2003

1

**TESIS CON
FALLA DE ORIGEN**



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



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 esta 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.

**TESIS CON
FALLA DE
ORIGEN**

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES



ESTADOS UNIDOS MEXICANOS

U. D. A. E. S.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Telefonía Digital y RDSI

Conexión de Redes LAN en un Centro de Control de Trafico

Aéreo

que presenta al pasante: Martínez Flores Luis Gabriel

con número de cuenta: 9204222-5 para obtener el título de

Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E

"POR MI RAZA HABLARA EL ESPIRITU"

Cuautitlán Izcalli, Méx. a 3 de Febrero de 2003

MODULO

PROFESOR

I y II Ing. José Luis Rivera López

III Ing. Blanca de la Peña Valencia

IV Ing. Vicente Magaña González

FIRMA

Q. Ma. del Carmen García Mijares
11 de Febrero de 2003

**TESIS CON
FALLA DE ORIGEN**

2

*A quienes me han heredado el tesoro más valioso,
que puede dársele a un hijo: AMOR,
A quienes sin escatimar esfuerzo alguno,
han sacrificado gran parte de su vida,
para formarme y educarme.
A quienes la ilusión de su vida ha sido,
convertirme en persona de provecho.
A quienes nunca podré pagar todos sus
develos ni aun con las riquezas más
grandes del mundo por esto y lo que será....GRACIAS*

☞ A la mujer más maravillosa del mundo que para mi fortuna es mi MAMÁ:
OLGA FLORES GOMEZ

☞ Para quien ha sido mi maestro, guía y ejemplo a seguir mi PAPÁ:
LUIS MARTINEZ SEBASTIAN

☞ A esos tres hermosos tesoros que la vida me dio por hermanos porque pase lo que pase siempre han estado conmigo:
JOSE LUIS, DIANA y a mi KAREN PATRICIA

☞ A la vida por darme tan extraordinarios familiares y amigos que contribuyeron con alguna palabra de aliento o regaño para alcanzar esta meta.

☞ Mi más sincero agradecimiento a la maestra *BLANCA DE LA PEÑA VALENCIA* por su gran paciencia y por sembrar en mí las bases de una enseñanza profesional que a partir de hoy apenas empieza.

"GRACIAS"

.....

*"La Grandeza De Un Ideal No Es Solo Alcanzarlo, Sino Luchar Por El
Alcanzarlo Es Solo Una Recompensa."*

.....

*"Llegará Un Momento En Que Creas Que Todo Ha Terminado.
Ese Será Solo El Principio"*

| | |
|-------------------|----|
| INDICE..... | I |
| PROLOGO..... | IV |
| INTRODUCCION..... | VI |

CAPITULO 1.

REDES DE DATOS

| | |
|--|----|
| 1.1 Introducción..... | 1 |
| Definición de las redes de datos..... | 1 |
| Objetivo de las redes..... | 2 |
| Aplicación de las redes..... | 2 |
| Estructura de una red..... | 3 |
| Ventajas aportadas por el uso de una red..... | 4 |
| Tipos de redes..... | 4 |
| <i>Redes de área metropolitana.....</i> | 5 |
| <i>Redes de área extensa.....</i> | 8 |
| <i>Red global Internet.....</i> | 9 |
| <i>Redes de área local.....</i> | 10 |
| 1.2 Dispositivos para la interconexión de redes..... | 12 |
| Implementación de la arquitectura..... | 13 |
| <i>Repetidores.....</i> | 14 |
| <i>Puentes.....</i> | 15 |
| <i>Rutadores.....</i> | 18 |
| <i>Pasarelas.....</i> | 22 |
| <i>Concentradores.....</i> | 23 |
| <i>Módem.....</i> | 24 |
| 1.3 Topologías utilizadas en una red LAN..... | 26 |
| Topologías físicas..... | 26 |
| <i>Topología en anillo.....</i> | 26 |
| <i>Topología en bus.....</i> | 28 |
| <i>Topología en estrella.....</i> | 29 |
| <i>Topología en árbol.....</i> | 30 |
| Topología lógica..... | 30 |
| <i>Topología anillo - estrella.....</i> | 30 |
| 1.4 Tipos de servidores..... | 31 |
| Servidores de disco..... | 32 |
| Servidores de ficheros..... | 32 |
| Servidores de ficheros centralizados y distribuidos..... | 33 |
| Servidores de ficheros dedicados y no dedicados..... | 33 |
| Servidores de ficheros de una red punto a punto..... | 33 |
| Servidor impresión..... | 33 |
| Servidor de comunicaciones..... | 34 |

TESIS CON
FALLA DE ORIGEN

| | |
|---|----|
| 1.5 Modelo OSI..... | 34 |
| Transmisión del modelo OSI..... | 36 |
| Niveles OSI..... | 37 |
| <i>Nivel de aplicación.....</i> | 37 |
| <i>Nivel de presentación.....</i> | 38 |
| <i>Nivel de sesión.....</i> | 38 |
| <i>Nivel de transporte.....</i> | 39 |
| <i>Nivel de red.....</i> | 40 |
| <i>Nivel de enlace de datos.....</i> | 40 |
| <i>Nivel físico.....</i> | 41 |
| 1.6 TCP - IP..... | 41 |
| ¿Qué es y la arquitectura de TCP/IP?..... | 41 |
| Protocolos TCP/IP..... | 44 |
| Características de TCP/IP..... | 44 |
| ¿Cómo funciona TCP/IP?..... | 45 |
| ¿En qué se utiliza TCP/IP?..... | 45 |

CAPITULO 2.

RED SENEAM

| | |
|--|----|
| 2.1 Introducción..... | 46 |
| 2.2 Definición de las partes operativas de un centro de control de tráfico aéreo..... | 46 |
| Track..... | 46 |
| Termino correlación..... | 49 |
| FIR, Sectores Y Aerovías..... | 54 |
| Descripción del vuelo de una aeronave (comercial) desde su aeropuerto de salida hasta su aeropuerto destino..... | 55 |
| 2.3 La Red SENEAM..... | 56 |
| Servicios de la red SENEAM y configuración básica..... | 57 |
| El host PIRC..... | 58 |
| Unidad visual..... | 62 |
| El host RDP..... | 63 |
| El host FDP..... | 64 |
| Procesamiento de mensajes..... | 65 |
| Proceso de adquisición y creación de planes de vuelo..... | 66 |
| Proceso de control de sintaxis y semántica..... | 66 |
| Proceso de evolución del plan de vuelo..... | 66 |
| Proceso de manejo de tiras..... | 67 |
| 2.4 Red a nivel operativo..... | 68 |
| Etapas del plan de vuelo..... | 68 |
| <i>Et estos plan de vuelo y preactivación.....</i> | 69 |
| <i>Procedimiento de certificación de mensajes CPL.....</i> | 69 |
| <i>Formato del mensaje CPL.....</i> | 70 |
| 2.5 Consecuencias de falla y alternativas de la red SENEAM..... | 72 |
| Vía una red AFTN..... | 72 |
| Vía telefónica..... | 73 |

| | |
|-------------------------------|--------|
| | INDICE |
| CONCLUSIONES | 76 |
| ANEXO..... | 78 |
| GLOSARIO..... | 94 |
| ACRÓNIMOS..... | 106 |
| IDENTIFICADORES DE LUGAR..... | 108 |
| BIBLIOGRAFÍA..... | 110 |

PROLOGO

REDES DE AREA LOCAL

En las décadas de los 60 y 70 la informática se concebía como un servicio estructurado jerárquicamente, reflejando en gran medida la estructura interna de las organizaciones. En la década de los 80 surgieron las redes de área local, a la vez que nuevos métodos de organización proponiendo una estructuración de las organizaciones basada en grupos de trabajo especializados y coordinados entre sí, mediante mecanismos más dinámicos y flexibles. En la década de los 90 las redes de área local están dejando de ser entes aislados y ofrecen a las grandes organizaciones la posibilidad de crear redes virtuales extensas mediante nuevas tecnologías de conexión de redes.

Hasta ahora los requisitos para la conexión de redes LAN (Red de Área Local) han sido conducidas hacia aplicaciones que no requieren altas velocidades tales como sistemas de tratamiento de datos, correo electrónico, transferencia de ficheros y acceso a bases de datos. Sin embargo, nuevas aplicaciones están demandando la necesidad de interconexión de LANs a velocidades que permitan la integración de voz e imágenes. Ejemplos de estas aplicaciones pueden ser videoconferencia, acceso a bases de datos de imágenes y aplicaciones multimedia.

La creciente necesidad entre los usuarios de redes de área local de obtener servicios de datos a alta velocidad está conduciendo al desarrollo de nuevas tecnologías debido básicamente a:

- La necesidad de interconectar redes de área local aisladas sobre una única red troncal con mayor capacidad.
- El aumento de la potencia de los ordenadores y la disminución de su costo.

Los beneficios para el usuario son varios, entre ellos destacan:

- El aumento de sistemas de proceso distribuido con separación geográfica de Unidades Centrales de Proceso y otros recursos del sistema que pueden ser compartidos por muchos usuarios o dedicados a usuarios específicos que requieran capacidades adicionales.
- La evolución de procedimientos de respaldo (*backup*) y mantenimiento, permitiendo a los administradores de redes el desarrollo de rutinas de una manera efectiva en cuanto a coste.
- Aceptación generalizada de interfaces de usuario que emplean aplicaciones que integran texto y gráficos en color.
- La evolución de configuraciones más complejas que soporten las tecnologías por llegar.
- Se pueden compartir periféricos costosos, como son impresoras, plóters, módems, tarjetas RDSI o scanners.

- Se pueden compartir grandes cantidades de información mediante el empleo de gestores de bases de datos en red. Con ello se evita la redundancia de datos y se facilita el acceso y la actualización de los datos.
- La red se convierte en un mecanismo de comunicación entre los usuarios conectados a ella, ya que permite el envío de mensajes mediante el empleo del correo electrónico, ya sea entre usuarios de la red local o entre usuarios de otras redes o sistemas informáticos, programando reuniones o intercambiando ficheros de todo tipo.
- Se aumenta la eficiencia de los ordenadores, poniendo a disposición del usuario todo un sistema que hace que las consultas sean más rápidas y cómodas.
- Se trata de un sistema completamente seguro, pudiendo impedirse que determinados usuarios accedan a áreas de información concretas, o que puedan leer la información pero no modificarla. El acceso a la red está controlado mediante nombres de usuario y claves de acceso. El control de los usuarios que acceden a la red lo lleva a cabo el sistema operativo.
- Los sistemas operativos de red intentan dar la sensación de que los recursos remotos a los que accede el usuario son locales al ordenador desde el cual está trabajando el usuario. Por ejemplo, un usuario puede estar consultando la información de una base de datos. El usuario en ningún momento tiene conocimiento de si la información a la cual está accediendo se encuentra en su propio ordenador o en otro distinto dentro de su red local o en cualquier otra parte del mundo.

TESIS CON
FALLA DE ORIGEN

INTRODUCCION

Por norma general las empresas que recurren a la informática para satisfacer sus crecientes necesidades de información suelen empezar con unos pocos o un único ordenador y unos cuantos periféricos. Poco a poco se van ampliando tanto los recursos hardware como recursos software para gestión de la información. Esta ampliación suele llevar asociado un problema de redundancias, tanto de software, hardware, etc. Por ejemplo, cada nuevo equipo va a necesitar de su propia impresora para imprimir informes (redundancia hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa por lo que será necesario copiarlos en este (redundancia de datos), los ordenadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos.

Pues bien, todos estos problemas tienen una fácil solución: la Red de Área Local nos va a permitir compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, un escáner, etc., (se elimina la redundancia hardware) : poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Además una red de área local conlleva un importante ahorro, tanto de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica compartida por varios ordenadores conectados en red : como de tiempo, ya que se logra gestión de la información y del trabajo.

Las redes locales permiten interconectar ordenadores que estén dentro de un mismo edificio o en edificios colindantes, pero siempre teniendo en cuenta que el medio físico que los une no puede tener más de unos miles de metros.

Actualmente son muchas las organizaciones que tienen el objetivo de compartir recursos, de manera que todos los programas, datos y equipos estén disponibles para cualquier red que así lo solicite sin importar la localización física del recurso y del usuario. Además tienen la necesidad de proporcionar una alta fiabilidad en el intercambio de datos.

Las redes se han convertido en una parte muy utilizada dentro de la tecnología de la computación, es un tema complejo, por esa razón el presente trabajo pretende describir tanto operativa como técnicamente una aplicación concreta de las Redes de Área Local.

En el CAPITULO I se describen las características generales de la red LAN, arquitectura, dispositivos para la conexión, topologías utilizadas, el modelo OSI, así como protocolos de comunicación empleados en las redes LAN

El CAPITULO II expone, en la parte practica, una aplicación de una red LAN dentro del medio aeronáutico, cuya función principal es ayudar a controlar el tráfico aéreo con información de primera mano y en tiempo real. Tal función estratégica es realizada en nuestro país desde 1978 por el órgano descentralizado "Servicios a la Navegación en el Espacio Aéreo Mexicano", SENEAM, dependiente de la Secretaría de Comunicaciones y Transportes.

La red LAN SENEAM esta conformada por centros de control donde la función principal es el intercambio de información. Los centros de control antes mencionados no son otra cosa que equipos de computo conectados en redes locales para el manejo de información radar y planes de vuelo dando una presentación visual y adecuada a los usuarios de dichos sistemas, llamados también controladores de vuelo, siendo ellos los que conforman la parte operativa del mismo.

El servicio de tránsito aéreo se proporciona en los centros de control así como en las torres de control situados en cada uno de los aeropuertos de la red. Algunas de ellas están dotadas con sistemas de radar que le permiten al controlador de vuelo dar instrucciones al tránsito que sale y llega a cada uno de los aeropuertos.

La comunicación entre pilotos y controladores tiene un sistema eficiente de comunicación que forma un circuito entre la aeronave, la torre de control y el centro de control que esta aportando el servicio de navegación y los centros adyacentes, con una coordinación precisa que asegura realizar las operaciones aeronáuticas eficientemente.

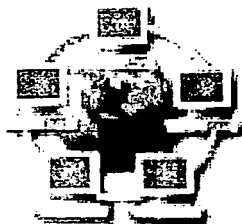
Los centros de control de tráfico aéreo utilizan una red tipo ETHERNET duplicada. La duplicación se realiza a nivel del cable y del adaptador. Un adaptador esta asociado con cada computadora; asegura el manejo de la red duplicada y al mismo tiempo permite hacer circular en la red la información generada. Una de estas dos LAN se utiliza como la LAN principal, la segunda supervisa la operación de la otra, de tal forma puede decirse que esta en estado de espera.

La red LAN con la que cuenta SENEAM se basa en principios simples y fiables. Todos los equipos conectados tienen la misma prioridad de acceso, es importante señalar que la red utiliza el protocolo TCP/IP para la comunicación con una velocidad de transmisión de datos bajo el modo banda base a 100Mbps y tres tipos de direccionamiento:

1. Direccionamiento general o broadcast.
2. Direccionamiento de grupo
3. Direccionamiento particular o a una dirección específica.

Finalmente, el presente trabajo dispone de un anexo con una breve descripción de los estándares del IEEE (Institute of Electrical and Electronic Engineers), para redes LAN.

CAPITULO I



REDES DE DATOS

PAGINACIÓN DISCONTINUA

1.1 INTRODUCCION

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadoras), así como a la puesta en órbita de los satélites de comunicación.

Las redes de ordenadores nacen como evolución de los sistemas de acceso y transmisión a la información y cumplen fundamentalmente el objetivo de facilitar el acceso a información remota, comunicación entre personas y entretenimiento interactivo.

Hay tres parámetros característicos en una red de ordenadores: su tamaño, su tecnología de transmisión y su topología.

El medio de transmisión consiste en un cable al que están conectadas todas las máquinas.

Su topología, es la forma en que conectan los ordenadores y puede ser en bus o en anillo.

DEFINICIÓN DE LAS REDES DE DATOS

Una de las mejores definiciones sobre la naturaleza de una red es la de identificarla como un sistema de comunicaciones entre computadoras. Como tal, consta de un soporte físico que abarca cableado y placas adicionales en las computadoras, y un conjunto de programas que forma el sistema operativo de red.

La diferencia sustancial entre un sistema basado en una mini computadora o gran computadora y una red es la distribución de la capacidad de procesamiento. En el primer caso, se tiene un poderoso procesador central, también denominado "host", y terminales "tontas" que funcionan como entrada y salida de datos pero son incapaces de procesar información o de funcionar por cuenta propia. En el segundo caso, los miembros de la red son computadoras que trabajan por cuenta propia salvo cuando necesitan un recurso accesible por red.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están desapareciendo con rapidez.

Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar, procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

TESIS CON
FALLA DE ORIGEN

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados si son capaces de intercambiar información. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

OBJETIVOS DE LAS REDES

La operación de las redes en general consiste en "compartir recursos" y uno de su objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tiene una mejor relación costo - rendimiento comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga simplemente añadiendo mas procesadores. Con máquinas grandes, cuando el sistema esta lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de ordenadores es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí. Con el ejemplo de una red es relativamente fácil, para dos o más personas que viven en lugares separados, escribir informes juntos.

APLICACIÓN DE LAS REDES

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad.

Para dar una idea sobre algunos de los usos importantes de redes de ordenadores, veremos ahora brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido.

Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver como pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a un ordenador remoto mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio mas bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuando se están transmitiendo los datos.

Una tercera forma como se muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (INTERNET). Por ejemplo, el tan conocido por todos correo electrónico (e-mail), que se envía desde una terminal a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar gráficos.

ESTRUCTURA DE UNA RED

En toda red existe una colección de máquinas para correr programas de usuario ó aplicaciones. Seguiremos la terminología de una de las primeras redes, denominada ARPANET, y llamaremos hostales a las máquinas antes mencionadas. También, en algunas ocasiones se utiliza el término Sistema terminal o sistema final. Los hostales están conectados mediante una subred de comunicación o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre hostales de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red se simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales).

Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión conocidas como circuitos, canales o troncales, se encargan de mover bits entre máquinas.

Los elementos de conmutación son ordenadores especializados que se utilizan para conectar dos o más líneas de transmisión, elementos que se verán con mas detalle mas adelante. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos

VENTAJAS APORTADAS POR EL USO DE UNA RED

1. Mantener bases de datos actualizadas instantáneamente y accesibles desde distintos puntos.
2. Facilitar la transferencia de archivos entre miembros de un grupo de trabajo.
3. Compartir periféricos caros (impresoras láser, plotters, discos ópticos, etc.)
4. Bajar el costo del software comprando licencias de uso múltiple en vez de muchas individuales.
5. Mantener versiones actualizadas y coherentes del software.
6. Facilitar la copia de respaldo de los datos.
7. Comunicarse con otras redes (bridge).
8. Conectarse con minis y mainframes (gateway).
9. Mantener usuarios remotos vía módem.
10. Si las estaciones que forman la red carecen de disquetera, además se puede:
 - Evitar el ingreso de virus
 - Evitar el hurto de información.
 - Facilita el acceso al sistema para usuarios inexpertos, ya que ingresa directamente a ejecutar sus aplicaciones.

TIPOS DE REDES

En un principio podemos clasificar las redes en dos tipos: redes de difusión y redes punto a punto. Con las primeras se puede dirigir un paquete o mensaje corto a todas las máquinas destinos quienes lo reciben y lo procesan. Sólo existe un canal de comunicación compartido por todas las máquinas de la red.

Con las segundas para ir del origen al destino un mismo paquete tiene que visitar una o varias máquinas intermedias, las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. A veces son posibles múltiples rutas de diferente longitud.

En general las redes geográficamente pequeñas suelen usar la difusión y las redes más grandes son de punto a punto.

Según la distancia entre computadoras se denominan a las redes de acuerdo a la siguiente clasificación: si los ordenadores se encuentran dentro de un mismo ámbito geográfico como una habitación, un edificio o un campus (como máximo del orden de 1 km) se llama **Red de Área Local**; si la distancia es del orden de la decena de kilómetro entonces se está ante una **Red de Área Metropolitana**; si la distancia es de varios cientos de kilómetros entonces se habla de una **Red de Área Extensa**; si se trata de una red que cubre todo el planeta entonces se habla de **Internet**. A continuación se hará una breve descripción de cada tipo de red.

Redes de Área Metropolitana

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbits/s hasta 155 Mbits/s.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Las redes de área metropolitana tienen muchas aplicaciones, las principales son:

- Interconexión de redes de área local
- Interconexión de centralitas telefónicas digitales
- Interconexión ordenador a ordenador
- Transmisión de vídeo e imágenes
- Transmisión
- Pasarelas para redes de área extensa

Una red de área metropolitana puede ser pública o privada. Un ejemplo de MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos. Los datos podrían ser transportados entre los diferentes edificios, bien en forma de paquetes o sobre canales de ancho de banda fijas. Aplicaciones de vídeo pueden enlazar los edificios para reuniones, simulaciones o colaboración de proyectos, tal como se muestra en la figura 1.1

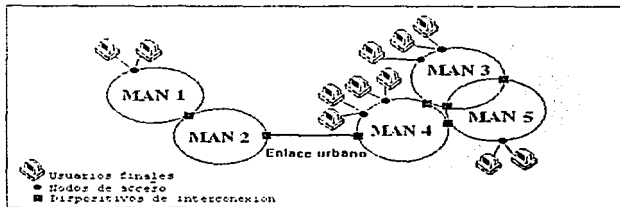


Figura 1.1 El uso de Redes MAN facilita el intercambio de datos en un área extensa.

Un ejemplo de MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

Las razones por las cuales se hace necesaria la instalación de una red de área metropolitana a nivel corporativo o el acceso a una red pública de las mismas características se resumen a continuación:

- Ancho de banda
- El elevado ancho de banda requerido por grandes ordenadores y aplicaciones compartidas en red es la principal razón para usar redes de área metropolitana en lugar de redes de área local.
- Nodos de red
- Las redes de área metropolitana permiten superar los 500 nodos de acceso a la red, por lo que se hace muy eficaz para entornos públicos y privados con un gran número de puestos de trabajo.
- Extensión de red
- Las redes de área metropolitana permiten alcanzar un diámetro entorno a los 50 kms, dependiendo el alcance entre nodos de red del tipo de cable utilizado, así como de la tecnología empleada. Este diámetro se considera suficiente para abarcar un área metropolitana.
- Distancia entre nodos
- Las redes de área metropolitana permiten distancias entre nodos de acceso de varios kilómetros, dependiendo del tipo de cable. Estas distancias se consideran suficientes para conectar diferentes edificios en un área metropolitana o campus privado.
- Tráfico en tiempo real
- Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real, donde es importante que ciertos mensajes atraviesen la red sin retraso incluso cuando la carga de red es elevada.
- Integración voz/datos/vídeo
- Adicionalmente a los tiempos mínimos de acceso, los servicios síncronos requieren una reserva de ancho de banda: para el tráfico de voz y vídeo. Por este motivo las redes de área metropolitana son redes óptimas para entornos de tráfico multimedia, si bien no todas las redes metropolitanas soportan tráficos isócronos (transmisión de información a intervalos constantes).

- Alta disponibilidad
- Disponibilidad referida al porcentaje de tiempo en el cual la red trabaja sin fallos. Las redes de área metropolitana tienen mecanismos automáticos de recuperación frente a fallos lo cual permite a la red recuperar la operación normal después de uno. Cualquier fallo en un nodo de acceso o cable es detectado rápidamente y aislado. Las redes MAN son apropiadas para entornos como control de tráfico aéreo, aprovisionamiento de almacenes, bancos y otras aplicaciones comerciales donde la indisponibilidad de la red tiene graves consecuencias.
- Alta fiabilidad
- Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red. En general la tasa de error para fibra óptica es menor que la del cable de cobre a igualdad de longitud. La tasa de error no detectada por los mecanismos de detección de errores es del orden de 10^{-20} . Esta característica permite a las redes de área metropolitana trabajar en entornos donde los errores pueden resultar desastrosos como es el caso del control de tráfico aéreo.
- Alta seguridad
- La fibra óptica ofrece un medio seguro porque no es posible leer o cambiar la señal óptica sin interrumpir físicamente el enlace. La rotura de un cable y la inserción de mecanismos ajenos a la red implica una caída del enlace de forma temporal.
- Inmunidad al ruido
- En lugares críticos donde la red sufre interferencias electromagnéticas considerables la fibra óptica ofrece un medio de comunicación libre de ruidos.

El ámbito de aplicación más importante de las redes de área metropolitana es la interconexión de redes de área local sobre un área urbana, pero otros usos han sido identificados, como la interconexión de redes de área local sobre un complejo privado de múltiples edificios y redes de alta velocidad que eliminan las barreras tecnológicas.

Redes de Área Extensa

Una Red de Área Extensa (WAN) es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes como se muestra en la figura 1.2. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí. Esta forma de comunicación aporta, como nota diferencial respecto a las Redes de Área Local (LAN) o las Redes de Área Metropolitana (MAN), que el ámbito geográfico que puede cubrir es considerablemente más amplio.

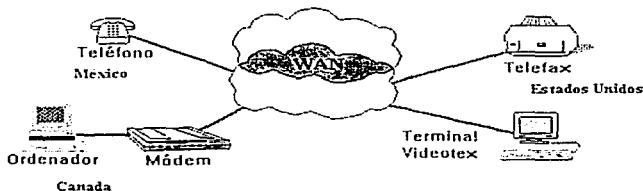


Figura 1.2 Una Red WAN ofrece la ventaja que pueden ser conectados diferentes dispositivos electrónicos en diferentes zonas geográficas con el fin de facilitar el intercambio de datos.

La tecnología WAN ha evolucionado espectacularmente en los últimos años, especialmente a medida que las administraciones públicas de telecomunicaciones han reemplazado sus viejas redes de cobre con redes más rápidas y fiables de fibra óptica, dado que las redes públicas de datos son el soporte principal para construir una WAN.

Cuando una organización se plantea el uso de una Red de Área Extensa, persigue una serie de objetivos:

- Servicios integrados a la medida de sus necesidades (integración de voz, datos e imagen, servicios de valor agregado).
- Integración virtual de todos los entornos y dependencias, sin importar donde se encuentren geográficamente situados.
- Optimización de los costes de los servicios de telecomunicación.
- Flexibilidad en cuanto a disponibilidad de herramientas y métodos de explotación que le permitan ajustar la configuración de la red, así como variar el perfil y administración de sus servicios.
- Mínimo coste de la inversión en equipos, servicios y gestión de la red.
- Alta disponibilidad y calidad de la red, soporte de los servicios.

Red Global Internet

Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica.

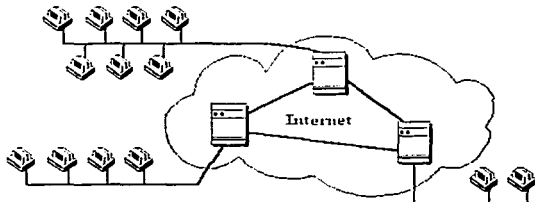


Figura 1.3 Internet hoy en día es una infraestructura informática ampliamente extendida.

Internet representa uno de los ejemplos más exitosos de los beneficios de la inversión sostenida y del compromiso de investigación y desarrollo en infraestructuras informáticas. A raíz de la primitiva investigación en conmutación de paquetes, el gobierno, la industria y el mundo académico han sido copartícipes de la evolución y desarrollo de esta nueva y excitante tecnología. Hoy en día, términos como *lgmf2001@correo.unam.mx* y *http: www.unam.mx* fluyen fácilmente en el lenguaje común de las personas.

Existe una evolución tecnológica que comienza con la primitiva investigación en conmutación de paquetes, ARPANET y tecnologías relacionadas en virtud de la cual la investigación actual continúa tratando de expandir los horizontes de la infraestructura en dimensiones tales como escala, rendimiento y funcionalidades de alto nivel. Hay aspectos de operación y gestión de una infraestructura operacional global y compleja. Existen aspectos sociales, que tuvieron como consecuencia el nacimiento de una amplia comunidad de inter nautas trabajando juntos para crear y hacer evolucionar la tecnología. Y finalmente, el aspecto de comercialización que desemboca en una transición enormemente efectiva desde los resultados de la investigación hacia una infraestructura informática enormemente desarrollada y disponible.

Su primer prototipo es a menudo denominado la Infraestructura de Información Nacional Global o Galáctica. Su historia es compleja y comprende muchos aspectos: tecnológico, organizacional y comunitario. Y su influencia alcanza no solamente al campo técnico de las comunicaciones computacionales sino también a toda la sociedad en la medida en que nos movemos hacia el incremento del uso de las herramientas *online* para llevar a cabo el comercio electrónico, la adquisición de información y la acción en comunidad.

Redes de Área Local

Una Red de Área Local se distingue de otros tipos de redes de datos en que las comunicaciones están normalmente restringidas a un área geográfica de tamaño limitado, como un edificio de oficinas, nave, o un campus, y en que puede depender de un canal físico de comunicaciones con una velocidad binaria media/alta y con una tasa de errores reducida.

Las redes de área local se basan en el hecho de que en distancias que se pueden considerar como locales, se producen el 80% de las comunicaciones tanto de voz como de datos. En un buen número de organizaciones un enorme tanto por ciento de las comunicaciones de voz son internas. Igualmente, la transmisión de datos o el intercambio de documentos son en su mayoría locales. Es posible, por tanto, desarrollar técnicas específicas para la transmisión y comunicación de datos en el entorno local.

El concepto de red de área local corresponde fundamentalmente a la necesidad de compartir recursos, tales como cableado interno, periféricos en una amplia variedad y, particularmente, compartición de datos y aplicaciones entre diferentes usuarios informáticos.

Las características básicas que definen una red de área local son las siguientes: Permite la interconexión de dispositivos heterogéneos, muchos de ellos capaces de trabajar independientemente.

- Aporta una velocidad de transferencia de información elevada (decenas de Mbits/s).
- Su empleo está restringido a zonas geográficas poco extensas, tales como departamentos de una empresa, edificios de oficinas, campus universitarios, etc., con a lo sumo unos pocos kilómetros de longitud total.
- Los medios de comunicación, así como los diferentes componentes del sistema, suelen ser privados. En relación con esto hay que tener en cuenta que la transmisión en este entorno reducido está libre de las regulaciones y monopolios característicos de la transmisión a larga distancia, lo cual ha facilitado el desarrollo de estos sistemas, pero, a la vez, actualmente está condicionando la expansión de este mercado.
- Se caracteriza por la facilidad de instalación y flexibilidad de reubicación de equipos y terminales, así como por el coste relativamente reducido de los componentes que utiliza.

La instalación de una red de área local en una organización supone una alta inversión en equipamiento, formación del personal y costes de explotación; además, la implantación de una red de área local supone un gran cambio en los procedimientos de trabajo y en los procesos de acceso a la información corporativa y departamental. Por todo lo anterior, queda claro que aunque una red de área local suponga un avance tecnológico y de organización en una empresa, es necesario analizar con detenimiento los costos y beneficios asociados para obtener argumentos de peso en la toma de decisiones. La figura 1.4 muestra una Red de Área Local.

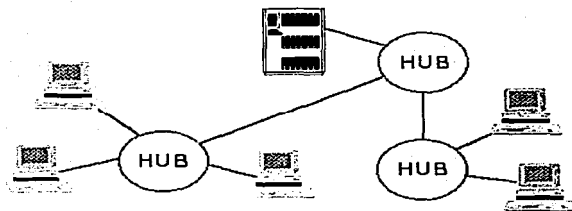


Figura 1.4 Una Red de Área Local se define como un tipo de red privada que permite la intercomunicación entre un conjunto de terminales o equipos informáticos, para la transmisión de información a gran velocidad en un entorno geográfico restringido

Las razones para proceder a la instalación de una red son las siguientes:

- Necesidad de compartición de recursos (equipamientos e información) Las redes locales facilitan el acceso de los usuarios a recursos compartidos permitiendo una utilización más eficiente y barata de:
 - ⊖ Módems y líneas de comunicaciones
 - ⊖ Discos y unidades de almacenamiento masivo
 - ⊖ Impresoras
 - ⊖ Aplicaciones e Información
- Proceso Distribuido
- Permite distribuir la carga de trabajo de las aplicaciones entre el servidor (sistemas encargados de proporcionar servicios de red a los demás puestos de trabajo) y los ordenadores personales o puestos de trabajo a él conectado.
- Sistemas de Mensajería
- En grandes corporaciones la posibilidad de acceder a un sistema de correo tanto interior como exterior asegura un flujo fácil y eficiente de información. Además, supone un ahorro de tiempo y recursos humanos importante.
- Bases de Datos
- Las redes locales son plataformas ideales para mantener y compartir bases de datos, hojas de cálculo multiusuario y otras aplicaciones de equipo lógico corporativo.
- Creación de grupos de trabajo

- Los grupos de usuarios pueden trabajar en un departamento o ser asignados a un grupo de trabajo especial.
- Gestión centralizada
- Debido a que los recursos de la red están organizados alrededor del servidor (sistemas encargados de proporcionar servicios de red a los demás puestos de trabajo) su gestión resulta sencilla. Las copias de seguridad y la optimización del sistema de archivos se pueden llevar a cabo desde un único lugar.
- Seguridad
- La información almacenada en servidores permanece más controlada que la información gestionada por cada usuario en su ordenador personal.
- Acceso a otros sistemas operativos
- El acceso a otros sistemas operativos permite la utilización de distintas aplicaciones de distintos entornos.
- Mejoras en la organización de la empresa
- Las redes pueden suponer un cambio en la estructura administrativa más importante de una organización al estimular modos de trabajo en grupo según los cuales los departamentos sólo existen a nivel lógico dentro de una gestión computerizada.

1.2 DISPOSITIVOS PARA LA INTERCONEXIÓN DE REDES

La década pasada se observó la primera generación de inter conectividad, la creación de las redes locales. El número de LAN's se incremento en número e importancia. Por la necesidad de conectar una con otra, con mainframes y servidores. Por lo mismo surge tal vez la segunda generación de conectividad, la habilidad de poder conectar redes con redes. A esta habilidad se le conoce con el término "internetworking" o interconexión de redes.

Por varias razones, la interconexión de redes no es tan sencilla. Típicamente conecta equipos de múltiples fabricantes, utiliza diferentes arquitecturas en la comunicación y se ejecuta sobre variados medios de transmisión. Tal complejidad requiere de centralizar y distribuir la administración de la red para permitir el aislamiento de errores y control de la configuración, seguridad, contabilidad y performance.

Aunque el crecimiento incrementa, la interconexión de redes se mueve hacia estándares coherentes y mejoramiento en su administración. El objetivo de la interconexión es asegurar la eficiencia global de las redes, la disponibilidad de recursos y la productividad de los usuarios sin importar donde se encuentren. A continuación se revisaran los conceptos básicos de las redes Ethernet y de los sistemas de interconexión .

Básicamente existen 4 tipos de productos para la interconexión de redes; repetidores, ruteadores, puentes y pasarelas. Cada uno de ellos representa un nivel diferente de conectividad y

funcionalidad correspondientes a los modelos de referencia IEEE802 y OSI. Estos modelos se aplican a cualquier conjunto de productos para conectividad desde módems hasta redes globales satelitales, la mayoría de los fabricantes se basan en ellos para diseñar sus productos.

IMPLEMENTACIÓN DE LA ARQUITECTURA.

Las redes están formadas por:

- Medios de transmisión sobre los cuales los mensajes son transportados. Por estos medios las señales viajan entre los dispositivos de la red. Los más usuales son: el cable coaxial y el par trenzado
- Líneas de transmisión de largo alcance como las líneas telefónicas o líneas de conmutación de datos (líneas T1 y T3)
- Cables de fibra óptica de alta velocidad, comúnmente utilizado para largas distancias.
- Interfaces para los dispositivos de la red. La interfaz por medio de la cual la computadora se conecta con la red generalmente es una combinación de hardware y software utilizado para controlar su acceso. La interfaz determina cuando la computadora puede acceder a la red, determina la iniciación y terminación de la interacción de esta con la red.
- Dispositivos para extender y administrar la red. Los medios para extender y controlar la red varían de la arquitectura de una red a otra. Los sistemas grandes típicamente usan dispositivos dedicados para la extensión y administración de la red. Los repetidores, puentes, ruteadores y pasarelas son ejemplos de dispositivos dedicados. En sistemas más pequeños, estas funciones están combinadas con otros dispositivos multiusos como serían los servidores de red o computadoras centrales.

Aunque en el término más sencillo la interconexión de redes es una red de redes, la interconexión es mucho más compleja. Esta complejidad surge debido a que deben soportar:

- Numerosas topología
- Diversos protocolos
- Diferentes medios de transmisión
- Un gran número de dispositivos

El mejor camino para considerar la implementación de una interconexión de redes es con relación a los sistemas que puede utilizar. Existen cuatro categorías de sistemas de interconexión: repetidores, puentes, ruteadores y pasarelas. La funcionalidad de estos sistemas corresponde a las características funcionales de las capas de la red, así como lo especifica el modelo OSI.

La relación con los dispositivos de interconexión y el modelo OSI se muestra en la figura 1.5

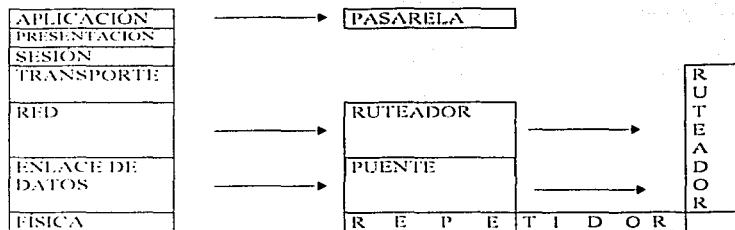


Figura 1.5 Relación de dispositivos de interconexión y el modelo OSI

Repetidores

Los repetidores funcionan en la capa más baja del modelo OSI, la capa física. Generalmente son utilizados para extender la cobertura geográfica de la red conectando localmente dos o más LAN's donde cada LAN en forma independiente se convierte en un segmento de la red, tal como se muestra en la figura 1.6

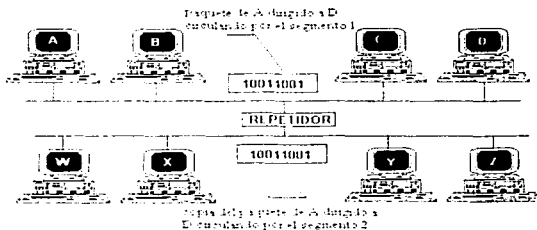


Figura 1.6 Los repetidores, como en la capa física directamente de un medio a otro y no llevan a cabo ningún procesamiento de alto nivel (carecen de inteligencia); por esto tienen mayor rendimiento en bps transmitidos que los puentes, ruteadores y pasarelas

Al propagarse a través de un medio de transmisión las señales transmitidas sufren gradualmente una disminución en su amplitud y una distorsión en su forma. Por esta razón se fija un límite a la longitud máxima del medio de transmisión que asegure que la atenuación y distorsión no impidan la interpretación correcta de las señales recibidas.

Sin repetidores, la longitud máxima del medio de transmisión depende tanto de la naturaleza del medio como la velocidad de transmisión. La forma IEEE 802.3 (derivada de Ethernet) establece, por ejemplo, que para una velocidad de transmisión de 10Mbps la longitud máxima es de 500 metros si se utiliza cable coaxial grueso y de 185 si se utiliza cable coaxial delgado; utilizando par trenzado es de 250 metros a una velocidad de 1 Mbps y si se desea conservar la velocidad de 10 Mbps es necesario disminuir la distancia a 100 metros.

Los repetidores son los elementos más sencillo para la interconexión de redes y como se menciono anteriormente operan al nivel más bajo del modelo OSI. Los repetidores físicamente extienden el alcance de una red regenerando señales (bits) de un medio de transmisión y retransmitiéndolas a otro. Esto puede lograrse con un repetidor que se conecta directamente a los dos medios, o utilizando dos repetidores remotos conectados por un enlace infrarrojo o de fibra óptica. Los medios conectados mediante un repetidor pueden ser de naturaleza distinta, por ejemplo coaxial grueso y coaxial delgado o coaxial y par trenzado. Es posible conectar también varios segmentos entre sí utilizando un solo repetidor multipuertos. Los repetidores interconectan segmentos para construir una sola red física. El número de repetidores que pueden conectarse en cascada para formar esta red está limitado por el protocolo de control de acceso al medio (MAC) utilizado, ya que existe un retardo de propagación máximo que debe respetarse.

Puentes.

Cuando se utilizan repetidores, las tramas enviadas por una estación de trabajo se propagan a todos los segmentos de la red sin importar la localización física de la estación receptora generando tráfico inútil en algunos segmentos de la red. Para solucionar este problema pueden utilizarse puentes que permitan aislar tráfico local de los diferentes segmentos de la red como se muestra en la figura 1.7

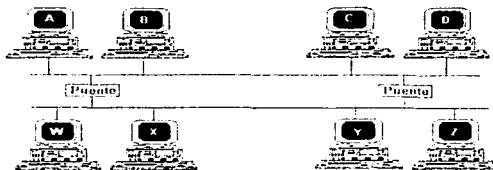


Figura 1.7 Además de proporcionar los mismos servicios de interconexión que los repetidores, los puentes son capaces de aislar algunos segmentos.

Los puentes funcionan en la capa de enlace de datos del modelo OSI. Debido a que solo envían los paquetes a dispositivos en otros segmentos que cumplan con la dirección correspondiente, los puentes pueden incrementar la eficiencia de toda la interconexión.

Debido a que operan en una capa inferior, los puentes son totalmente transparentes a protocolos de alto nivel incluyendo por ejemplo: TCP/IP, XNS, DECnet, etc. Estos serán transparentes al puente siempre y cuando el tamaño de su paquete no exceda el máximo del puente.

Los puentes permiten que los dispositivos, que corren bajo el mismo protocolo de alto nivel en cualquier red, puedan comunicarse unos con otros, pero los puentes no pueden convertir paquetes formateados en un protocolo de alto nivel a otro diferente.

Esto significa que los dispositivos de la red, conectados por un puente que utilizan diferentes protocolos de alto nivel no podrán comunicarse.

Los puentes son totalmente transparentes a los dispositivos de la red por lo cual la interconexión creada por estos forma una red lógica. Debido a que limitan la cantidad de tráfico que fluye entre los segmentos de la red, los puentes pueden mejorar considerablemente el desempeño y eficiencia de toda la interconexión. Esto se logra debido a la capacidad del puente de aprender, filtrar y reenviar operaciones.

¿Cómo funcionan los puentes?

El mecanismo por medio del cual el puente limita el tráfico entre los segmentos de la red es conocido como aprendizaje, filtrado y reenvío y se basa en el contenido de una tabla de ruteo que informa que dispositivo se encuentra en cual segmento de la red. Cuando un puente recibe una trama, lee la dirección origen y la compara con las tablas de ruteo, si la dirección origen no existe en la tabla el puente la adiciona. Por ello se dice que el puente "aprende" la dirección del dispositivo en la red. Esta particularidad nos ofrece la habilidad que los nuevos dispositivos sean añadidos a la red sin necesidad de reconfigurar al puente para acomodarlos.

Una vez terminado el proceso de aprendizaje, el puente determina la dirección destino y la compara con la tabla de ruteo. Si la dirección destino se encuentra en el mismo segmento de red que la dirección origen, el puente automáticamente descarta la trama para evitar un tráfico inútil en los otros segmentos, este proceso es conocido como filtrado. Si la dirección destino indica una estación en otro segmento, entonces el puente envía la trama solo a este segmento (mecanismo de reenvío). Pero si la dirección destino no se encuentra en la tabla, entonces envía la trama a todos los segmentos a los cuales este conectado (con excepción del segmento sobre el que se recibió la trama).

Los puentes regeneran cada trama que reenvían. Ni el número de nodos en el segmento ni la distancia que viaja una trama tiene efecto en la calidad de señal de la trama. Por lo tanto los puentes pueden utilizarse para extenderse sobre la distancia total del cableado. Sin embargo, grandes distancias pueden causar retardos, los cuales están relacionados con los requerimientos de distancia de los protocolos de alto nivel involucrados. Por ejemplo, el protocolo Ethernet limita el retardo máximo debido a los medios de transmisión a tan solo 950 nseg.

En la actualidad el mercado ofrece puentes simples e inteligentes. Todos los puentes son capaces de mecanismos de aprendizaje, sin embargo los puentes simples cubren las funcionalidades descritas anteriormente. Los puentes inteligentes ofrecen capacidades adicionales. Los administradores de redes pueden programar puentes inteligentes para filtrar tramas

selectivamente dependiendo de criterios de selección dados. Esto proporciona niveles de seguridad mayores debido al grado de aislamiento alcanzado en los segmentos. Otra función que los puentes inteligentes proporcionan es el reenvío explícito del origen, mediante el cual los administradores pueden asignar privilegios de acceso en la interconexión y definir direcciones en la tabla de ruteo accesibles o inaccesibles por grupos selectos de usuarios.

El proceso de funcionamiento de tres pasos de los puentes asume que solo un camino existe entre dos dispositivos cualesquiera en segmentos de la red conectados por puentes. Con una topología simple es relativamente sencillo garantizar un solo camino entre dos dispositivos. Pero conforme mas puentes son utilizados para conectar mas dispositivos y redes de interconexión la probabilidad de crear diversos caminos incrementa drásticamente.

Los múltiples caminos son conocidos como lazos o ciclos activos. Estos lazos activos entre dispositivos pueden causar un severo problema con los puentes en la interconexión, que nos lleva a una duplicación indefinida e innecesaria de tramas. Esta redundancia de tráfico puede degradar rápidamente el desempeño total de la red.

Ciclos activos de los puentes

El problema de caminos activos fue resuelto por medio de una algoritmo conocido como Spanning tree algorithm(STA) formulado por IEEE. Este construye un árbol de recubrimiento a partir de la topología de segmentos y puentes, evitando así la existencia de ciclos. Las topologías más usuales siempre y cuando no existan ciclos activos son:

- Cascada.- Se utiliza por lo general cuando el largo de la LAN debe extenderse mas allá de los requerimientos especificados. Figura 1.8

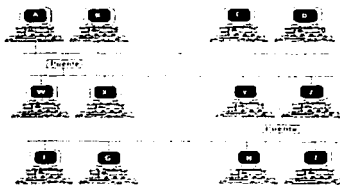


Figura 1.8 LAN con topología en cascada

- Estrella.- Más usual con WAN's ya que permite colocar localidades remotas con un mínimo de segmentos y sin ciclos. Figura 1.9



Figura 1.9 LAN con topología en estrella

TESIS CON
FALLA DE ORIGEN

Al igual que los repetidores, existen puentes locales y amplios. Los locales conectan redes que se encuentren geográficamente cerca una de otra por medio de la conexión directa. Los puentes de área amplia conectan redes que son geográficamente distantes una de la otra vía medios de largo alcance tales como líneas de transmisión T1. En la tabla I se muestran las ventajas y desventajas del uso de los puentes.

| VENTAJAS | DESVENTAJAS |
|--|---|
| Faciles de instalar | No pueden utilizar múltiples trayectorias |
| Conectan redes corriendo diferentes protocolos de alto nivel | Producen retardos |
| Conectan redes a diferentes velocidades y distancias | Incrementan el tráfico en la interconexión |
| Alto nivel de funcionalidad al administrador de la red | No proporcionan soporte para aislar fallas |
| Excelente desempeño a un precio relativamente bajo | Los administradores de red requieren conocer lo que se ejecuta en la red y en donde |

Tabla I Ventajas y desventajas con el uso de los puentes.

Ruteadores.

Los ruteadores conectan las redes a nivel de capa tres del modelo OSI. Su función es enviar los paquetes de acuerdo con el medio establecido por el protocolo de alto nivel, por lo cual poseen un nivel más alto de software inteligente que los puentes. Esta característica permite su uso en interconexiones complejas o grandes ya que pueden resolver varios caminos redundantes.

Existen diversos tipos de ruteadores. Como los puentes, los ruteadores pueden conectar redes de área local o amplia. Existen ruteadores estáticos y dinámicos.

Por medio de un esquema de direccionamiento jerárquico que distingue entre las direcciones de los dispositivos y de las redes, los ruteadores permiten la separación lógica de la interconexión lógica de la red a varias subredes. Estas subredes son dominios lógicos administrativamente independientes lo que permite el poder distribuir la administración de la red.

Los ruteadores al igual que los puentes, pueden extender el tamaño de una red, sin embargo proporcionan un nivel de conexión más inteligente y eficaz. Las redes a interconectar pueden utilizar diferentes protocolos en las capas físicas y de enlace de datos.

Estos dispositivos pueden discriminar la información: leen las direcciones de los paquetes de información y toman decisiones sobre la ruta que deben seguir a lo largo de una complicada red de área amplia, basándose en diversos factores como retraso, costo de transmisión, congestión o distancia; sin embargo, no examinan todos los paquetes, únicamente los dirigidos a ellos. Además, no lo hacen los puentes, sino que únicamente conocen a otros ruteadores de la red identificados por una dirección (subnetwork address). Para un ruteador no es importante el formato de un paquete ya que únicamente lee la dirección del mismo, decide la ruta y posiblemente envuelve el paquete en algún protocolo como N25 o frame relay. De esta manera podemos rutear paquetes en diversos protocolos como IPX, TCP/IP, DECnet, OSI, etc., de manera simultánea.

Existe un dispositivo más, conocido como brouter, el cual combina las características de un paquete y de un ruteador. Puede rutear determinados protocolos y los demás los maneja como puente, esto es muy útil cuando deseamos ingresar diversas redes con distintas topologías y protocolos.

Para poder entender el funcionamiento de un ruteador, nos basaremos en el caso A. En el se muestran 2 redes Ethernet y una token ring conectadas mediante un ruteador. Cada red es identificada por una dirección única (dirección de red) y cada dispositivo dentro de la misma es identificado con otra dirección (dirección de enlace de datos)

Red con ruteadores

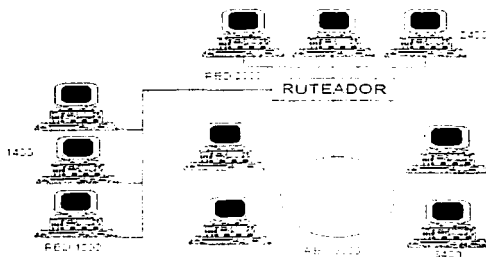


Figura 1.10 Los ruteadores no imponen ninguna restricción sobre la topología de interconexión de redes. Los ruteadores pueden manejar cualquier número de lazos activos. Esto permite que se lleve control eficiente debido a la distribución del tráfico en toda la red.

Supongamos que las direcciones de red son múltiplo de 1000 y que las direcciones de los dispositivos varían de 1 a 499. La dirección completa de cada dispositivo se formaría sumando ambas direcciones: 1400 identifica al dispositivo 400 de la red 1000; la 2400 identifica al dispositivo 400 en la red 2000. Para enviar un mensaje del dispositivo 1400 al 2400 realizamos lo siguiente: el origen compara su dirección de red (1000) con la del destino (2000), como son diferentes, el dispositivo sabe que el destino está en otra red y que no puede ser enviado directamente sino que debe ser ruteado.

Todos los dispositivos mantienen tablas de ruteo, las cuales contienen las direcciones de las redes adyacentes. En el caso del dispositivo 1400 la tabla de ruteo consta de un solo dato: la dirección del ruteador 1. El dispositivo lee esta dirección de su tabla y envía el mensaje con una envoltura especial al ruteador, el ruteador recibe el mensaje, elimina la envoltura, lee la dirección destino y la compara con los datos de su tabla, la cual contiene las direcciones de todas las redes adyacentes. En nuestro caso, el ruteador 1 tendría en sus tablas 3 direcciones:

- 1499 para su conexión con la red 1000
- 2499 para su conexión con la red 2000
- 3499 para su conexión con la red 3000

Con estos datos el ruteador compara sus direcciones de red (1000, 2000, 3000) con la del destino; la 2000 si coincide con sus datos y reconoce que debe enviar el mensaje a esa red formateándolo de acuerdo a los protocolos de Ethernet, como se muestra en la figura 1.10

Protocolos de ruteo

Hasta el momento podemos notar que los dos aspectos fundamentales para un ruteador son:

- Obtener información sobre los ruteadores adyacentes y las redes remotas
- Escoger la ruta más adecuada para llegar al destino

Ambos aspectos son solucionados mediante los protocolos de ruteo: protocolos que permiten conversar a los ruteadores para obtener su información y manejar un intercambio dinámico de estos datos.

Existen dos tipos de protocolos de ruteo, el primero de ello es el de vector de distancia, representado típicamente por el protocolo RIP (routing information protocol) el cual envía mensaje s periódicos propagando las tablas de ruteo a lo largo de la red. Proporciona un buen servicio en redes pequeñas y relativamente estables ya que en redes complejas, el envío periódico de tablas grandes representa un exceso de tráfico y utilización de ancho de banda.

Las redes grandes y en crecimiento requieren protocolos de ruteo del segundo tipo: estado de enlace, representado por el OSPF (open shortest path first) o IS- IS (intermediate system to intermediate system). Estos protocolos no envían mensajes periódicos t, posiblemente, redundantes, sino que envían información de ruteo únicamente cuando hay algún cambio. En un protocolo de vector de distancia la mejor ruta es siempre la misma, la que tiene el menor número de puntos intermedios entre origen y destino. En los protocolos de estado de enlace la mejor ruta se determina dependiendo del retraso (velocidad de transmisión), rendimiento (capacidad), y confiabilidad de enlaces.

¿Cuándo nos conviene utilizar un puente y cuándo un ruteador? Los primeros son buena solución para ambientes departamentales o pequeños, ya que ofrecen un método barato para conexiones de dos puntos y son sencillos para extender los límites físicos de una red.

Los ruteadores son mas apropiados para ambientes empresariales y de área amplia, porque permiten conectarnos a diversos enlaces de datos, utilizan tecnologías de redundantes, buscan rutas alternas en caso de fallas, permiten tener administración de red y soportan múltiples protocolos.

Las principales diferencias entre puentes y ruteadores son las siguientes:

- Confiabilidad.- los puentes operan en la capa de enlace de datos y los protocolos a este nivel proporcionan cierto nivel de detección de errores, más no aseguran la entrega del mensaje a su destino.
- Disponibilidad.- La mayoría de los puentes no son tolerantes a fallas. La caída de un enlace puede afectar severamente el rendimiento del puente y provocar pérdida de

mensajes. Los ruteadores son más tolerantes a fallas, ya que fueron diseñados para operar en una red de red amplia que cuenta con múltiples enlaces y rutas alterna.

- Tiempo de tránsito.- Los puentes realizan poco proceso de información y por lo mismo representan retrasos mínimos. Sin embargo, el arribo de demasiados mensajes a un puente puede provocar congestión y perder ciertos mensajes.
- Los ruteadores realizan un proceso más sofisticado el cual puede representar un retraso, este retraso puede compensarse con la mayor disponibilidad.
- Detección de errores.- Los puentes realizan detección de errores en la capa de enlace de datos. Los ruteadores realizan detección de errores en la capa de enlace de datos y en la de red.
- Tamaño de mensajes.- Los puentes operan más eficientemente cuando las redes origen y destino manejan el mismo tamaño de mensajes. Los ruteadores permiten fragmentar y reensamblar mensajes para conectar redes diferentes pero debemos considerar lo siguiente:
- Costo.- Los puentes son más económicos que los ruteadores.
- Seguridad.- Los puentes ofrecen seguridad limitada. Los ruteadores ofrecen mayor protección contra accesos no autorizados a recursos e información.

Arquitectura típica de un ruteador.

Los ruteadores se basan en arquitectura de multiprocesadores simétricos, la cual permite una configuración escalable con alto rendimiento.

Esta arquitectura refleja beneficios directos en 4 principales áreas:

- I. Conectividad e interoperabilidad y rendimiento.
- II. Confiabilidad, disponibilidad y facilidad de mantenimiento.
- III. Estabilidad y compatibilidad entre productos.
- IV. Protección de la inversión.

Normas.

Los principales estándares de redes locales son los soportados por equipos incluyendo:

- Ethernet 802.3
- Token Ring 802.5 a 4 Mbps y 16 Mbps
- FDI

En cuanto a protocolos soportan los siguientes:

- Novell IPX
- TC/IP
- DECnet fase IV y V
- Xerox XNS
- Apple talk
- OSI
- Spanning tree learning bridge
- Source routing
- SNA

De esta manera las redes locales, utilizando cualquier protocolo, pueden interconectarse mediante:

- Líneas síncronas con velocidades de 1200 bps hasta 6 Mbps
- E0 y E1 provistas por la RDI
- X.25
- Frame relay
- SMDS y PPP

Pasarelas

Las pasarelas son el sistema de interconexión más compleja. Funciona en las tres capas superiores del modelo OSI: en la capa de sesión, presentación y aplicación. Las pasarelas pueden conectar redes que contengan diferentes arquitecturas. Para realizar estas funciones, las pasarelas convierten completamente una arquitectura de red (o stack de protocolo) a otro sin afectar los datos que se transmiten. Las pasarelas proporcionan diversos servicios sofisticados para la administración de las redes. Como los puentes y los ruteadores, las pasarelas pueden conectar redes de área local y amplia.

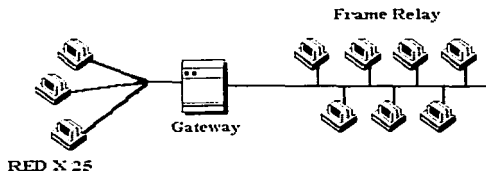


Figura 1.11 La pasarela realiza la traducción completa entre las familias de los protocolos proporcionando una conectividad completa entre redes de distinta naturaleza.

Las pasarelas proporcionan el servicio de conexión más inteligente pero también más lento. Así como la gente habla distintos idiomas, los equipos de cómputo también lo hace, sólo que a su

idioma se le llama protocolo. Como se ve en la figura 1.11 las pasarelas proporcionan servicios de traducción entre diferentes protocolos y permiten a los dispositivos de una red comunicarse no-solo conectarse con los dispositivos de otra completamente diferente.

Por ejemplo cuando se tenga que comunicar una red local y un gran ordenador(mainframe) o un mini ordenador que utiliza protocolos de nivel de transporte, sesión, presentación y aplicación distintas se necesitara de una pasarela.

De este modo podrá obtener datos del mini o del mainframe o enviarles datos para su almacenamiento.

El enlace entre ambos protocolos necesitará algún tipo de prueba que haga que la estación de trabajo imite el funcionamiento de una terminal y ceda el control al mini o mainframe. Esta emulación se puede conseguir por medio de software (con un programa) de hardware (con una tarjeta) o de ambos.

Concentradores.

Son dispositivos que permiten la comunicación entre un modem, conectado a un puerto de una computadora, varios módems conectados a DTE's en aplicaciones que usan protocolos de sondeo/selección. Con este tipo de concentrador podemos bajar los costos de las líneas de comunicación. El concentrador análogo es el encargado de crear un equilibrio eléctrico entre los distintos enlaces. Figura 1.12.

Los concentradores digitales también llamados Port- Sharing Devices permiten que varias estaciones de trabajo compartan un MODEM o un puerto de en aplicaciones que usan protocolos de sondeo / selección. Con este tipo de concentrador podemos ahorrar, puertos de un procesador de comunicaciones, host o módems requeridos para una conexión, dependiendo de cómo se conecten.

El número de concentradores que se necesitan depende de dos cosas:

- Cuantos puertos se van a convertir a un protocolo de alta velocidad
- La densidad de puerto de los concentradores que desea comprar

Si se tienen concentradores apilables, la unidad más pequeña que puede adquirir es un concentrador. Algunos concentradores apilables requieren terminadores separados. En el caso de contar con un modulo de chasis se debe de tomar en cuenta que este tipo de concentradores requiere cables especiales y conectores.

MAU (multistation access unit) - Concentrador que permite insertar en el anillo o eliminar hasta 8 estaciones. El MAU detecta señales procedentes de las estaciones de trabajo, en caso de detectarse un dispositivo defectuoso o un cable deteriorado elimina la estación en cuestión para evitar perdidas de datos.

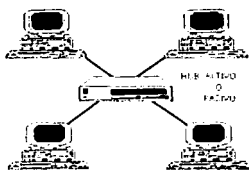


Figura 1.12 HUBS.- Concentradores de cableado en estrella integrados por microprocesadores, memoria y protocolos como SNMP, características que lo convierten en un nodo inteligente en la red capaz de controlar y diagnosticar incluso por un monitoreo remoto.

Módem

Es un dispositivo que convierte la señal digital en señal analógica y viceversa para posibilitar que el mensaje enviado por una estación de trabajo pueda llegar a otro(s) estaciones de trabajo a través de líneas analógicas. Este ejemplo se muestra en la figura 1.13

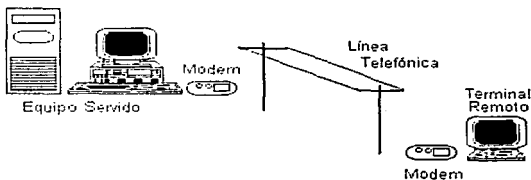


Figura 1.13 Un módem es un equipo para la transmisión de datos que convierte señales analógicas en digitales y viceversa, esta información es intercambiada entre dos ordenadores mediante una línea telefónica.

Los módems son seleccionados de acuerdo a:

- Línea Telefónica
- La velocidad de transmisión
- El tipo de línea que utiliza (dedicada, conmutada o ambas)
- La modulación que emplea (FSK, PSK, DPSK, QAM, TCM)
- Las posibilidades de compresión de datos para transmisión
- La modalidad de trabajo (punto a punto o multipunto)
- Si el módem es interno o externo.

MODEM interno- Es una placa de expansión que ocupa un conector de expansión. Se alimenta de la propia fuente de alimentación de la PC.

Los módems internos no requieren cableado, basta de disponer del cable telefónico que conecta el MODEM a la línea telefónica.

MODEM externo- Están protegidos por una coraza que puede ser de plástico o aluminio. El uso del MODEM externo requiere la existencia de un puerto serie en la PC, un cable del puerto al MODEM y una fuente de alimentación. Figura 1.14.

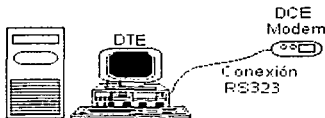


Figura 1.14 Conexión utilizada en un módem externo.

Modos de operación del módem.

El módem tiene dos tipos de funcionamiento que son:

- Estado de comandos.- El módem responde a los comandos que envía el ordenador. En este modo es posible configurar el módem o realizar las operaciones de marcado y conexión. Antes de que se pueda enviar un comando al módem este debe estar en el estado de comandos.
- Modo en línea.- En este modo cualquier información que reciba del ordenador será enviada al módem distante. En este modo el módem no procesa la información y simplemente la transmite a través de la línea de comunicación.

Por otra parte la velocidad módem está determinada por los protocolos de modulación, de los cuales existen dos estándares:

- V.32
- V.32 bis

Además de los protocolos de modulación, existen módems que soportan protocolos de control de errores, siendo los estándares:

- V.42
- MNP-4
- MNP-2
- MNP-3

1.3 TOPOLOGÍAS UTILIZADAS EN UNA RED LAN

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida

TOPOLOGÍA FÍSICA

Es lo que hasta ahora se ha venido definiendo: la forma en la que el cableado se realiza en una red. Existen cuatro topologías físicas puras:

1. Topología en anillo.
2. Topología en bus.
3. Topología en estrella.
4. Topología en árbol

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por más de una topología física. A continuación se hace una breve descripción de cada una de las topologías antes mencionadas.

Topología en Anillo

El anillo consiste en una serie de repetidores conectados entre sí mediante un único enlace de transmisión unidireccional formando un camino cerrado.

La información se transfiere secuencialmente, bit a bit, de un repetidor al siguiente a lo largo del anillo. Cada repetidor regenera y retransmite cada bit. Cuando una estación recibe información

destinada a ella, la incorpora a su memoria. En caso contrario se encargara de hacerla circular hasta la próxima estación, tal como se muestra en la figura 1.15. En algunos sistemas de anillo el paquete es eliminado por la fuente, y en otros, por el destino. Al igual que los canales, las anillas tienen una naturaleza de difusión. Cualquier paquete que se transmita puede ser visto por todos los nodos de la red, con lo que es posible transmitir datos a varios nodos con un solo paquete. Esto normalmente se hace reservando una dirección particular de la red que reconozca todos los nodos.

Los datos fluyen sólo en una dirección alrededor del anillo, y los dispositivos conectados al anillo pueden recibir datos de él. Para transmitir, es necesario que el dispositivo interrumpa los datos del anillo para poder introducir los suyos. Normalmente, los anillos son activos, esto es, incluyen circuitos regeneradores que deben operar continuamente. Esto significa que los anillos se pueden extender a cualquier tamaño si tiene suficientes circuitos regeneradores o repetidores.

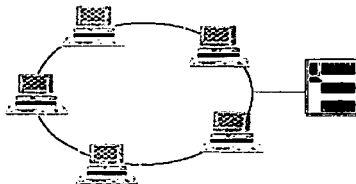


Figura 1.15 Topología en anillo.

Los repetidores constituyen un elemento activo de la red, pueden estar integrados en las propias estaciones. Sus principales funciones son:

1. Contribuir al correcto funcionamiento del anillo, realizando los servicios de inserción, recepción y eliminación de información.
2. Proporcionar el punto de acceso de las estaciones a la red.

Entre las ventajas de esta topología se pueden citar:

1. Tiempo de respuesta controlado
2. Gestión de averías.

Al circular la información por todas las estaciones se puede repartir equitativamente la capacidad de transmisión entre los usuarios también es posible identificar en que nodo de enlace se ha producido una avería.

Problemas potenciales en el anillo

La principal desventaja del anillo es que cada estación esta involucrada en la transferencia de datos, por lo que el fallo de un repetidor inutiliza por completo la red. Esto se puede resolver incorporando un anillo paralelo de respaldo. Esta técnica no es apropiada para anillos con pocos

nodos, ya que la probabilidad de error de las unidades de reconfiguración es mayor que la probabilidad de incrementar la fiabilidad de la red.

La topología en anillo requiere mecanismos de control sofisticados para detectar y anular las informaciones defectuosas e impedir la circulación indefinida de una información por fallo de la estación responsable de su emisión. Algunas redes dedican una estación monitora a estas tareas de control, mientras que otras reparten esta responsabilidad entre las estaciones.

El anillo como topología de red es particularmente propenso a sufrir los efectos de la corrupción de bits de los paquetes. Como la red es un lazo, un paquete con un campo de control erróneo podría circular indefinidamente. Esto no puede suceder en una red de línea común, ya que el paquete erróneo acabaría desapareciendo en uno de los extremos. Un ejemplo de este error es que el bit de lleno vacío de un anillo segmentado sea lleno cuando debería leer vacío. Esto impediría que ninguna estación usara ese segmento, y ninguna estación intentaría vaciarlo. Un caso similar es que la señal de permiso se cambie de libre a ocupado por un error en el anillo. Es posible que un nodo estándar de un anillo detecte esta situación, ya que parece que el protocolo de acceso está operando correctamente. Esta clase de error se debe detectar con un nodo central de control o con un algoritmo distribuido que se ejecute en los nodos conectados al anillo.

Topología en Bus

En esta topología todas las estaciones se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando una estación transmite, su señal se propaga a ambos lados del emisor hacia todas las estaciones conectadas al bus hasta llegar a los puntos de terminación donde la señal es absorbida; de aquí que el bus reciba también el nombre de canal de difusión.

En ella, todas las estaciones comparten el mismo canal de comunicaciones; toda la información circula por ese canal, y cada estación recoge la información que le corresponde, tal como se muestra en la figura 1.16



Figura 1.16 Topología en bus

Esta distribución es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones. En la mayoría de las redes en bus tienen la ventaja de estar constituidas por elementos pasivos, es decir, todos los

componentes activos se encuentran en las estaciones, por lo que una avería en una estación no afecta más que a ella misma; sin embargo, una avería en el bus afecta a la totalidad de la red, quedando incomunicadas las estaciones de una sección del bus con las de la otra sección.

Otras ventajas importantes son la modularidad es muy sencillo añadir o retirar estaciones a la red y la distribución geográfica de las estaciones con un costo reducido.

Entre sus inconvenientes destacan:

- Es fácil de intervenir por usuarios de fuera de la red sin perturbar el funcionamiento normal.
- La longitud no puede sobrepasar los 2 000 metros.
- El control de flujo, ya que aunque varias estaciones intenten transmitir a la vez, como hay un único bus, sólo una de ellas podrá hacerlo, por lo que será más complicado el control del flujo cuantas más estaciones tenga la red. Este control del flujo se puede realizar de dos maneras: por el método de acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD) o por el paso de testigo.

Topología en Estrella

Todas las estaciones que integran el sistema se comunican entre sí a través de un dispositivo central de conmutación o distribución con mayor o menor grado de inteligencia.

El nodo central aísla a una estación de otra, resultando una configuración fiable frente a averías en las estaciones. Sin embargo, una avería en el nodo central deja totalmente bloqueada a la red y sin posibilidad de reconfiguración. Permite incrementar o disminuir con sencillez el número de estaciones, aunque tales modificaciones pueden resultar costosas por la gran longitud del medio de comunicación a instalar y el aumento de conexiones en el nodo central. Figura 1.17

Por tanto, no es una configuración adecuada para redes con gran dispersión geográfica. Además, tampoco es posible cursar grandes flujos de tráfico por congestión del nodo central.

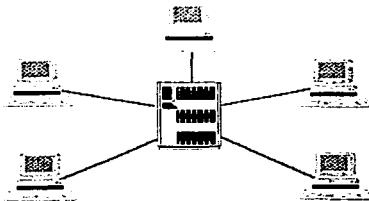


Figura 1.17 Topología en estrella.

Topología en Árbol

La topología en árbol es una generalización de la topología en bus en la que el cable se extiende en varios ramales mediante el empleo de dispositivos de derivación. Al igual que la topología en bus, las transmisiones se propagan por cada ramal de la red y llegan a todas las estaciones. Figura 1.18



Figura 1.18 Topología en árbol

Esta topología es especialmente interesante para las redes de banda ancha. Se puede utilizar, por ejemplo, para conectar estaciones de un edificio de varios pisos de la misma forma se distribuye la señal en una instalación de antena colectiva.

1.3.1 TOPOLOGÍA LÓGICA

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

1. Topología anillo-estrella: implementa un anillo a través de una estrella física.

Topología anillo-estrella

Para solventar los inconvenientes de la escasa flexibilidad ofrecida por la topología en anillo en temas de instalación, mantenimiento o reconfiguración, se han planteado topologías alternativas en las que la configuración física es distinta a la del anillo pero conservando la estructura lógica de éste. El ejemplo más claro lo ofrece la topología en anillo - estrella; configuración física de estrella - configuración lógica de anillo. Tal como se muestra en la figura 1.19

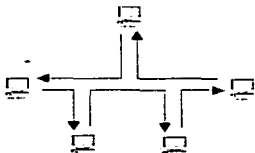


Figura 1.19 Topología anillo - estrella

En la topología anillo - estrella, las estaciones se conectan a través de una unidad de acceso de tal manera que físicamente forman una estrella, si bien lógicamente constituyen un anillo. En caso de que se averíe una estación o un segmento del cable, la unidad de acceso puede cortocircuitar automáticamente esa estación o segmento de cable, de tal manera que el resto del anillo lógico pueda permanecer activo, también se puede disponer de varias unidades de acceso en serie. Lo anterior se puede ver con claridad en la figura 1.20

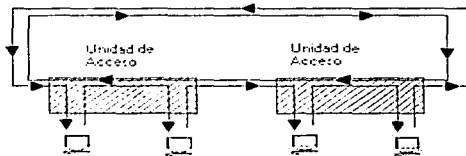


Figura 1.20 Aun cuando exista una falla en alguna terminal conectada a esta topología, la red sigue operando continuamente.

En operación normal de la red, la señal circula tal y como se representa en la figura. En caso de avería de una estación se cortocircuita ésta. Si la avería se sitúa en el cable entre unidades de acceso, el anillo se reconfigura. Así como se puede apreciar en la figura 1.21

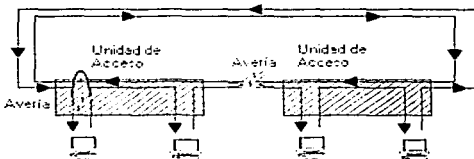


Figura 1.21 Esta topología tiene la característica que si existe una avería en el cable, se reconfigura.

1.4 TIPOS DE SERVIDORES

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

Servidores de Disco

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

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

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

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

Servidores de Ficheros

Un servidor de ficheros es mucho más eficiente y sofisticado que un gestor de disco. Contiene software especial que procesa comandos antes de que el sistema operativo los reciba. El servidor de ficheros contiene su propia FAT. Cuando una estación de trabajo pide un determinado fichero, el servidor de ficheros ya sabe donde está el fichero y lo envía directamente a la memoria de la

estación de trabajo. En este caso para la estación de trabajo el servidor de ficheros no es otra unidades discos más, como sucede con el servidor de disco. Es mucho más eficiente porque no necesita enviar una copia de la FAT a la estación que pide un fichero, y además no es necesario particionar la unidad de disco.

El servidor de ficheros se encarga de que en un momento dado, sólo hay un usuario utilizando un fichero determinado. Los usuarios pueden trabajar como si tuvieran un disco de gran capacidad conectado a su ordenador. Cualquiera puede tener acceso a los ficheros, a no ser que se establezcan claves de acceso.

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

Servidores de Ficheros Centralizados y Distribuidos.

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

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

Servidores de Ficheros Dedicados y No Dedicados.

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

Servidores de Ficheros de Una Red Punto a Punto.

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

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

Servidor de Impresión.

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

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

Para poder compartir impresoras, el servidor de impresión debe disponer del software adecuado y por lo general contiene lo que se conoce como un spooler de impresión, que es un buffer donde

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

Servidor de Comunicaciones.

Los servidores de comunicaciones están diseñados para liberar a la red de las tareas relativas a la transmisión de información. El servidor de comunicaciones funciona igual que una central telefónica haciendo las mismas funciones que un sistema PABX (central automática privada).

Por medio del servidor de comunicaciones una estación puede llamar a una red externa o cualquier otro sistema buscar cierta información y enviarla a la estación que la ha solicitado. El servidor de comunicaciones se puede utilizar también para conectar dispositivos incompatibles a una red.

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

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

1.5 MODELO OSI

El Modelo de Referencia OSI es el modelo que se ha estructurado más recientemente, por lo que a pesar de no existir muchas implementaciones OSI. Sí puede afirmarse que se trata del modelo que proporciona un nivel de formalización más abstracto.

Dentro del Modelo de Referencia OSI se establecen tres niveles de abstracción:

- La arquitectura OSI. Define los elementos básicos de los sistemas abiertos abstractos, es decir, de que manera debe verse un sistema desde el exterior.
- Las especificaciones de servicio OSI. Define los servicios proporcionados a los usuarios en cada nivel, es decir, los servicios proporcionados por un nivel al nivel exterior.
- Las especificaciones de protocolos OSI. Definen la información de control transmitida entre los distintos sistemas, así como los procedimientos para la interpretación de dicha información de control.

El Modelo de Referencia OSI es un modelo de redes estructuradas en capas o niveles. El objetivo es tratar de manera estructurada la totalidad de un sistema teleinformático. El conjunto de funciones del sistema se divide en niveles, facilitando su estudio y desarrollo, que sean fácilmente controlables de forma individual y que en conjunto resuelvan satisfactoriamente las necesidades de comunicación.

Cada nivel se desarrolla sobre el anterior, de tal forma que recibe una serie de servicios sin conocer los detalles de cómo se realizan dichos servicios.

Las diferentes funciones de la arquitectura OSI han sido estructuradas en siete niveles, siendo las funciones asignadas a cada uno de ellos complementarias. Figura 1.22

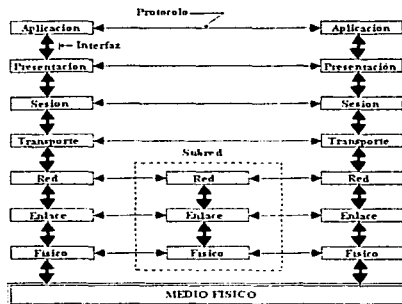


Figura 1.22 Es la arquitectura de una red que utiliza el modelo OSI.

Cada nivel se relaciona con el nivel inmediato superior e inferior a través del concepto de interfaz, que presenta el conjunto de elementos lógicos y físicos existentes entre dos niveles adyacentes.

Por otra parte, se define protocolo como el conjunto de reglas o convenciones que controlan el intercambio de información entre unidades funcionales del mismo nivel, tanto en la transmisión como en el control y recuperación de errores.

Los protocolos de niveles diferentes son independientes, solo tienen que conocer la definición de servicios de su interfaz, y no tienen nada que ver con los protocolos de los restantes niveles ni con los servicios de sus interfaces.

TRANSMISION DEL MODELO OSI

La comunicación entre dos nodos de una red significa que los correspondientes niveles de ambos nodos o niveles para estar hablando entre ellos. Para que dicha comunicación sea posible cada nodo deben tener idénticos protocolos de nivel esta comunicación se mantiene mediante el intercambio de mensajes con un formato común denominado unidades de datos de protocolo.

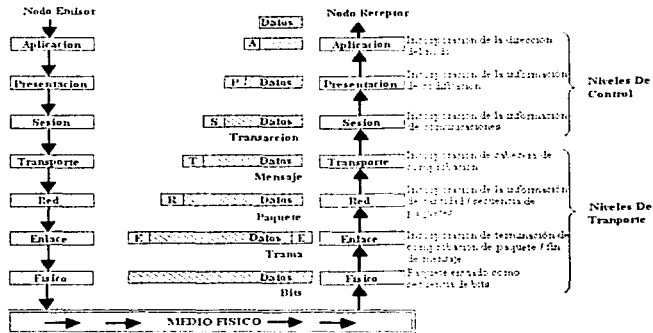


Figura 1.23 Una red con arquitectura OSI, tiene un nivel de transporte y un nivel de control.

La figura 1.23 muestra la transmisión de datos de una red con arquitectura OSI. Además se muestra la clasificación de los niveles en dos grupos. Los niveles de control son los relacionados con las necesidades de comunicación entre los usuarios finales, es decir, si dos usuarios no tuviesen necesidad de utilizar una red de comunicación, sólo utilizarían estos niveles. Los niveles de transporte son los encargados de transferir los mensajes a través de la red.

La transmisión de datos se da a través de una red que sigue el Modelo de Referencia OSI. Supongamos dos nodos, uno emisor y otro receptor. El nodo emisor pone a disposición de su nivel de aplicación los datos que desea transmitir. El nivel de aplicación incorpora a los datos pasados por el nodo la información propia del nivel mediante datos de cabecera y cola (datos situados al principio y a final del mensaje respectivamente): la totalidad de la información, cabecera más datos más cola es entregada al nivel de presentación, quien a su vez, añade una cabecera y cola propias del nivel, transfiriendo el resultado al nivel de sesión. Este proceso se repite en el resto de los niveles por los cuales va pasando el mensaje hasta llegar al nivel físico. En el nivel físico es donde realmente se realiza la transmisión de la información. En el nodo receptor el mensaje recibido sufre el proceso inverso al que se vio sometido en el emisor. A medida que el mensaje asciende por los niveles de la torre OSI del nodo receptor, se le quita la información de cabecera y cola correspondientes a cada nivel. De esta forma, los datos llegan al nodo receptor idénticos a como fueron enviados por el nodo emisor.

receptor el mensaje recibido sufre el proceso inverso al que se vio sometido en el emisor. A medida que el mensaje asciende por los niveles de la torre OSI del nodo receptor, se le quita la información de cabecera y cola correspondientes a cada nivel. De esta forma, los datos llegan al nodo receptor idénticos a como fueron enviados por el nodo emisor.

Se entiende que realmente no existe una comunicación directa entre los niveles a excepción del nivel físico. Cuando se realiza una comunicación entre usuarios de diferentes sistemas se establece una relación lógica entre los niveles 7 de ambos utilizando el protocolo de nivel 7. Este protocolo requiere los servicios del nivel 6, obligando, por lo tanto, a los dos niveles 6 a comunicarse a través de su propio protocolo de nivel 6 y así sucesivamente hasta llegar al nivel 1 donde se realiza la comunicación.

NIVELES OSI

Como se mostró en las figuras anteriores, el modelo OSI consiste en siete niveles de especificaciones que describen como deben manejarse los datos durante las diferentes etapas de la transmisión.

Cada capa proporciona un servicio para la capa inmediata superior.

Durante una sesión de comunicación, los procesos que se ejecutan en cada capa de cada computadora se comunican unos con otros. La capa inferior define los componentes físicos reales como conectores y cables, la transmisión eléctrica de los bits de datos entre los sistemas. La capa inmediata superior define los métodos de empaquetado y direccionamiento de datos. Por encima se encuentran los métodos para mantener activas las sesiones de comunicación. Finalmente las capas más altas describen como las aplicaciones utilizan los sistemas subyacentes de comunicación para interactuar con las aplicaciones de otros sistemas.

Cada capa define el procedimiento y las reglas que los subsistemas de comunicación que deben seguir para poder comunicarse con sus procesos correspondientes de los otros sistemas.

El modelo OSI asigna siete capas diferentes para los complejos procedimientos necesarios para las comunicaciones de datos a lo largo de una red. El modelo OSI está diseñado para facilitar la consecución de un acuerdo inicial en las capas más bajas y, por último, en las siete capas completas. La jerarquía de capas se realiza desde lo general, en la capa más alta, hasta lo particular en la capa de menor nivel.

A continuación se describen las funciones básicas y los elementos de cada nivel del modelo OSI.

Nivel de Aplicación

El nivel superior de la arquitectura OSI y tiene como misión controlar y coordinar las funciones a realizar por los programas de usuarios de manera que les permita el acceso al entorno OSI. Los procesos de aplicación se comunican entre sí por medio de las entidades de aplicación a las que están asociadas, controladas por protocolos de aplicación utilizando servicios de presentación (de su nivel inferior inmediato nivel 6)

Se puede distinguir tres tipos de procesos de aplicación:

- Proceso del propio sistema.- Son los que ejecutan funciones para controlar y supervisar operaciones de los sistemas conectados a la red de comunicación.
- Proceso de gestión de aplicación.- Son los encargados de controlar y supervisar las operaciones de los procesos de aplicación
- Proceso de aplicación de usuarios.- Son los que procesan la información real para los usuarios finales.

A continuación se mencionan unas de las principales aplicaciones del nivel de aplicación dentro del modelo OSI.

- Transferencia de archivos (FTP).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail).
- Acceso a bases de datos
- Terminales virtuales
- Remote jobs Servicios de directorio.
- Sistemas Operativos de Red (NOS)
- Aplicaciones Cliente/servidor

Nivel de Presentación

El nivel de presentación es el encargado de la transferencia de los datos contenida en los protocolos de aplicación. En este nivel intervienen los aspectos sintácticos de la información o, lo que es igual, la forma o código en que se presentan los datos.

A través de este nivel, los procesos de aplicación adquieren independencia de la representación de los datos e incluyen en su entorno las posibles transformaciones de códigos.

Los protocolos de la capa de presentación forman parte del sistema operativo y de la aplicación que el usuario ejecuta en una estación de trabajo. En esta capa se da formato a la información para visualizarla o imprimirla. Se interpretan códigos que están en los datos.

Funciones importantes del nivel de presentación

- Establece una sintaxis y semántica de la información transmitida.
- Se define la estructura de los datos a transmitir.
- Define el código a usar para representar una cadena de caracteres (ASCII).
- Compresión de datos.
- Encriptación de datos.
- Interpretación de formatos de números (complemento uno o complemento dos).
- Es el nivel clave para el sistema de seguridad del modelo OSI.

Nivel de Sesión

El propósito de este nivel es proporcionar los medios necesarios para controlar el diálogo entre entidades de presentación. Este diálogo se realiza a través del establecimiento y uso de una conexión, denominada sesión.

Los servicios proporcionados por el nivel de sesión son los siguientes:

- Establecimiento de la conexión de sesión. Se realiza la conexión de dos entidades de presentación a petición del usuario.
- Intercambio de datos. Es el servicio que permite la transferencia de datos. Puede ser en un sentido, en otro o en ambos.
- Liberación de la conexión de la sesión. Una vez finalizado el intercambio de datos se procede a la desconexión.
- Sincronización y mantenimiento de la sesión. Se realiza la sincronización y control de la comunicación de manera que se produzca un intercambio ordenado de datos.
- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Maneja la sincronización en la administración de mensajes, es decir, si aborta un mensaje no lo retransmite completo si no la parte que hace falta, por otra parte hace la recuperación de archivos durante la transmisión.
- Reporte de excepciones

Nivel de Transporte

El objetivo del nivel de transporte es proporcionar un mecanismo fiable para el intercambio de datos entre procesos en diferentes sistemas. Este mecanismo independiza al nivel de sesión superiores de los elementos de comunicación que constituyen la red; es decir, oculta a los niveles superiores los detalles específicos de la red a través de la cual se transmite la información.

El nivel de transporte pasa los datos del nivel de sesión al nivel de red, fragmentándolos en unidades más pequeñas si es necesario y asegurando que todos llegan correctamente a su destino. Para ello emplea funciones de direccionamiento, multiplexación, establecimiento de la conexión, desconexión, transferencia y control de flujo de los datos.

El nivel de transporte puede, además, ofrecer servicios detección y corrección de errores, para asegurar la integridad de los datos, así como niveles de calidad de servicio. Por ejemplo, una entidad de sesión podría especificar tasas de errores aceptables, retardo máximo y prioridad. La complejidad del protocolo de transporte dependerá del tipo de servicio ofrecido por el nivel de red. Cuanto más fiable sea el servicio proporcionado por el nivel de red, más sencillo o menos funciones incluirán el protocolo del nivel de transporte.

Algunas características del nivel de transporte del modelo OSI

- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Es el primer nivel de comunicación entre usuarios o sistemas, conocido con primer nivel extremo a extremo.
- Es el nivel que aísla todas las funciones del sistema final de la tecnología de intercambio de datos a través de la subred.
- Aísla el nivel de sesión de los cambios inevitables de la tecnología del Hardware.
- Provee flujo de datos TRANSPARENTE entre entidades de sesión.
- Maneja la contabilidad a través de la red.
- Ejecuta recuperación de errores.
- Control de congestión.
- No le importa como llegan los datos al otro lado, sino como manejarlos cuando llegan.

Nivel de Red

La comunicación generalmente tiene lugar en el ámbito de una red, sea ésta pública o privada. Este nivel es el responsable de asegurar que la información se transmita correctamente a través de la red. Proporciona a las entidades del nivel de transporte de una transferencia de datos transparente. En este sentido libera al nivel de transporte de la necesidad de conectar los mecanismos de transmisión de datos o tecnologías utilizadas para conectar sistemas.

El nivel de red tiene como funciones la conexión, desconexión de las redes, sincronización, control del flujo de las transferencias y la detección de errores en la transmisión; recuperándolos en caso necesario. En el caso de que hubiera más de una red implicada en la transmisión también tiene como función el encaminamiento entre redes.

Características importantes del nivel de red.

- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Su servicio básico es proveer transferencia de datos transparente entre entidades de transporte.
- Control de operaciones de la subred de comunicaciones.
- Maneja rutas estáticas o dinámicas.
- Control de errores.
- La secuencia de paquetes de red a través de la subred.

Nivel de Enlace de Datos

Este nivel es el responsable de mantener la integridad de los datos de una transmisión sobre un canal de comunicaciones. Es decir, proporciona un canal fiable para la transmisión de datos sobre un medio físico, por lo general, no exento de ruido, por ello entre sus funciones se encuentran las detecciones y corrección de errores de transmisión que pudieran ocurrir en el medio físico.

Los protocolos del nivel de enlace definen el establecimiento y liberación de un enlace de datos, controlan la correcta transferencia de información y recuperación de anomalías, así como la gestión del propio nivel.

- Estructura el flujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).
- Provee control de flujo.
- Controla el acceso al medio físico.

- Ensambla y reensambla mensajes provenientes del nivel de red y los envía en tramas o frames a través del medio físico.
- Detecta y corrige errores provenientes del medio físico.
- Posee mecanismos de control de congestión.
- Sincronización de frames.
- Protocolos orientados a bit u orientados a carácter.
- Algunas arquitecturas de redes dividen este nivel en dos subniveles: LLC (Logical Link Control) y MAC (Medium Access Control).

Nivel Físico

El nivel físico es el responsable de la definición de las características mecánicas, eléctricas y funcionales de la transmisión y recepción de la información utilizando un medio de comunicación específico. Entre sus funciones básicas se encuentran la identificación de los circuitos de datos, la secuencia de los mismos y la gestión del nivel.

- Especifica cables, conectores y componentes de interfaz con el medio de transmisión.
- Transmisión de bits por el canal de comunicaciones.
- Especifica el medio físico de transmisión (Coaxial, F.O., Par trenzado, etc.).
- Niveles de voltaje y pulsos eléctricos o corriente para representar 1's ó 0's.
- Aspectos mecánicos y eléctricos de la interfase de red.

1.6 TCP – IP

Protocolo.

Establecen una descripción formal de los formatos que deberán presentar los mensajes para poder ser intercambiados por equipos de cómputo; además definen las reglas que ellos deben seguir para lograrlo.

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel (e.g. la transmisión de flujos de bits a un medio físico) hasta aquellas de más alto nivel (e.g. el compartir o transferir información desde una computadora a otra en la red).

Tomando al modelo OSI como referencia podemos afirmar que para cada capa o nivel que él define existen uno o más protocolos interactuando. Los protocolos son entre pares, es decir, un protocolo de algún nivel dialoga con el protocolo del mismo nivel en la computadora remota.

¿QUÉ ES Y LA ARQUITECTURA DE TCP/IP?

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software* incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI, figura 1.24. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).
- **Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- **Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- **Físico :** Análogo al nivel físico del OSI.
- **Red :** Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

| |
|---------------------|
| NIVEL DE APLICACION |
| NIVEL DE TRANSPORTE |
| NIVEL DE INTERNET |
| NIVEL DE RED |
| NIVEL FISICO |

Figura 1.24 Niveles que ocupan los protocolos TCP/IP en una red con arquitectura OSI.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (*datagram*), y son conjuntos de datos que se envían como mensajes independientes.

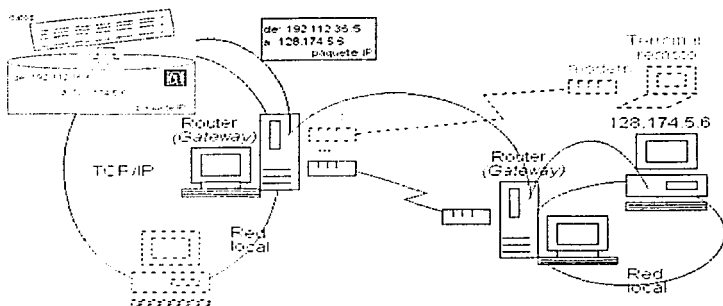


Figura 1.25 Protocolo TCP/IP en una red LAN.

La figura 1.25 muestra que dentro de una red local, el encaminamiento de la información es simple. En Ethernet por ejemplo todos los ordenadores 'escuchan' la red para detectar los paquetes que se le dirigen a ellos. En la Internet este procedimiento es inviable.

Los routers (antes llamados gateways) son los elementos encargados del encaminamiento de los mensajes IP. Los routers conocen las máquinas conectadas a la red y toman la decisión de como encaminar los paquetes de datos a través de unos enlaces u otros.

Cada router sólo necesita saber por conexiones están disponibles y cual es el mejor "próximo salto" para conseguir que un paquete este mas cerca de su destino (El paquete va "saltando" de router a router hasta llegar a su destino).

Las máquinas de la Internet, fuera del entorno de la red local, utilizan un router para encaminar los paquetes. La dirección IP de esta máquina es la única información que deben conocer, del resto se encargan los routers.

PROTOSCOLOS TCP/IP

| | |
|----------------------------|------------------------------|
| FTP, SMTP, TELNET | SNMP, X-WINDOWS, RPC, NFS |
| TCP | UDP |
| IP, ICMP, 802.2, X.25 | |
| ETHERNET, IEEE 802.2, X.25 | |

Tabla 2 Diferentes protocolos.

- **FTP** . Se utiliza para transferencia de archivos.
- **SMTP**. Es una aplicación para el correo electrónico.
- **TELNET**. Permite la conexión a una aplicación remota desde un proceso o terminal.
- **RPC**: Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- **SNMP**. Se trata de una aplicación para el control de la red.
- **NFS**. Permite la utilización de archivos distribuidos por los programas de la red.
- **X-Windows**. Es un protocolo para el manejo de ventanas e interfaces de usuario.

CARACTERÍSTICAS DE TCP/IP

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

- La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen *IP mueve los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.*
- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, se ordenará y combinará cuando llegue a su destino. Compare esto con la manera en que se transmite una conversación telefónica. Una vez que establece una conexión, se reservan algunos circuitos para usted, que no puede emplear en otra llamada, aún si deja esperando a su interlocutor por veinte minutos.
- Los datos no trenen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino. Éste, claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos computadoras aunque no estén conectadas directamente entre sí. Lo que realmente sorprende es que sólo se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a

otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.

- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.
- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

¿CÓMO FUNCIONA TCP/IP?

IP está basado en la idea de los datagramas interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el hostal fuente hasta el hostal destinatario, quizás recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera: la capa de transporte toma los mensajes y los divide en datagramas, de hasta 64K octetos cada uno. Cada datagrama se transmite a través de la red interred, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un datagrama IP consta de una parte de cabecera y una parte de texto.

¿EN QUE SE UTILIZA TCP/IP?

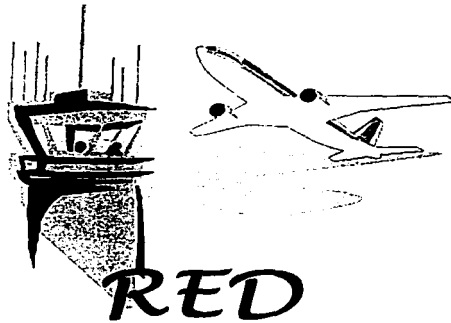
Muchas grandes redes han sido implementadas con estos protocolos, incluyendo Internet. De igual forma, una gran variedad de universidades, agencias gubernamentales, empresas de ordenadores y Aeropuertos que se analizará posteriormente. Estas diferentes redes están conectadas mediante los protocolos TCP/IP. Cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada Internet. Las máquinas en Internet son denominadas "hosts" o nodos.

TCP/IP proporciona la base para muchos servicios útiles, incluyendo correo electrónico, transferencia de ficheros y login remoto.

El correo electrónico está diseñado para transmitir ficheros de texto pequeños. Las utilidades de transferencia sirven para transferir ficheros muy grandes que contengan programas o datos. También pueden proporcionar chequeos de seguridad controlando las transferencias.

El login remoto permite a los usuarios de un ordenador acceder a una máquina remota y llevar a cabo una sesión interactiva.

CAPITULO II



SENEAM

45A

TESIS CON
FALLA DE ORIGEN

2.1 INTRODUCCIÓN

SENEAM.

SERVICIOS A LA NAVEGACION EN EL ESPACIO AEREO MEXICANO.

Es un órgano descentralizado dependiente de la SCT. Esta empresa fue iniciada por el gobierno federal en el año de 1978, mismo en que fue requisada por él, para constituirse en organismo descentralizado.

La función principal es proporcionar los servicios de navegación aérea en el espacio aéreo mexicano tales como meteorología, servicio de despacho e información de vuelos y control de tráfico aéreo, con un alto grado de confiabilidad y seguridad, para lo cual instrumenta una infraestructura técnica-operativa de lo más moderna con base en radares, centros de control, equipos de aeronavegación, estaciones terrenas enlazadas en red, etc., todo con la finalidad de proporcionar los servicios a las compañías de aeronavegación, comercial y privada.

Esto quiere decir que una aeronave que esté en nuestro espacio aéreo tendrá que utilizar los servicios que ofrece la empresa, para garantizar la seguridad de sus tripulantes o pasajeros.

Otra función que se lleva a cabo dentro de esta importante empresa es formular programas a corto, mediano y largo plazo para el desarrollo de servicios, construcción de instalaciones e inversiones diversas.

2.2 DEFINICIONES DE LAS PARTES OPERATIVAS EN UN CENTRO DE CONTROL DE TRAFICO AEREO

Para facilitar el entendimiento de la aplicación, se necesita definir algunos términos técnicos-operativos, se empezará por:

Track.

Se le nombra track a la identificación de una aeronave que estará en un código denominado SSR que es proporcionado por el radar de vigilancia secundario, asociado con un símbolo provisto por el sistema de procesamiento o también llamado centro de control, esta identificación es finalmente visualizada en la pantalla del controlador -el controlador de vuelo es el usuario del sistema, siendo ellos los que conforman la parte operativa en los centros de control-, tal como se muestra en la figura 2.1.

Para explicar mejor este concepto se mencionan algunas características básicas del radar.

El principio del funcionamiento de un Radar es la transmisión de una determinada señal de Radiofrecuencia que incide en un objeto llamado "blanco", -para nuestro caso será una aeronave-el cual refleja la señal en varias direcciones, una porción de esta señal "eco" es captada por un receptor, que es la misma antena de transmisión que una vez capturada esta señal la amplifica y la procesa para obtener información del "blanco". Al medir el lapso de

tiempo entre la señal transmitida y la recibida así como por la posición de la antena y elevación, se puede determinar la posición exacta de la aeronave. El nivel de señal recibida proporciona la intensidad de reflectividad y por tanto, le indica al controlador las posiciones de altitud, rumbo, dirección y velocidad a la que esta volando esa aeronave en el espacio aéreo controlado.

El radar abarca los 360 grados de azimut y su antena gira a una velocidad entre 6 y 15 vueltas por minuto. Dicha antena envía al aire dos preguntas:

¿QUIEN ERES?

¿QUE ALTURA TIENES ?

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | ECO PRIMARIO |
| <input type="checkbox"/> | ECO SECUNDARIO |
| <input checked="" type="checkbox"/> | ECO SECUNDARIO ASOCIADO CON ECO PRIMARIO |
| <input type="checkbox"/> | ECO DE IDENTIFICACION |
| <input checked="" type="checkbox"/> | ECO REFLEJADO |
| <input type="checkbox"/> | ECO PRIMARIO A PERDERSE EN MODO CONECTADO |
| <input type="checkbox"/> | ECO PRIMARIO A PERDERSE EN MODO BY PASS |

Figura 2.1.- Símbolos empleados en la presentación en pantalla

En la figura 2.2 se puede observar que la transmisión es codificada y enviada para el control de aeronaves, para este fin se utilizan canales de comunicación VHF en la banda de la aviación civil.

Actualmente los aviones también tienen una antena que transmite y recibe. Este al estar volando recibe dicha codificación del radar, y por medio de un equipo llamado transponder, contesta a dichas preguntas del radar, informando por tanto quién es (dato de 4 dígitos, código SSR) y que altura tiene (información también de 4 dígitos en pies).

La información transmitida por el avión y recibida por la antena de radar es procesada y enviada a los centros de control. En éstos la información recibida es procesada aun más para finalmente ser enviada a través de la red local a las posiciones de control para su visualización. Como se observa en la figura 2.3 a esta información se le asigna un símbolo para asociarla con la aeronave. En otras palabras, el "cuadrado" (símbolo) que ve el controlador es en realidad la aeronave y junto a ese símbolo existen 5 informaciones más, mostrados en la misma figura, como son:

1. Código SSR (Secondary Surveillance Radar). Identificación de la aeronave.
2. Velocidad de la aeronave, calculada por el radar o en su defecto por el sistema de procesamiento, en millas náuticas.
3. Altitud de la aeronave en pies y además por comodidad en la visualización, se le quitan dos ceros al momento de su presentación en la pantalla del controlador.

Finalmente a esta información visual en la pantalla (símbolo con información asociada), se le conoce técnicamente como TRACK.

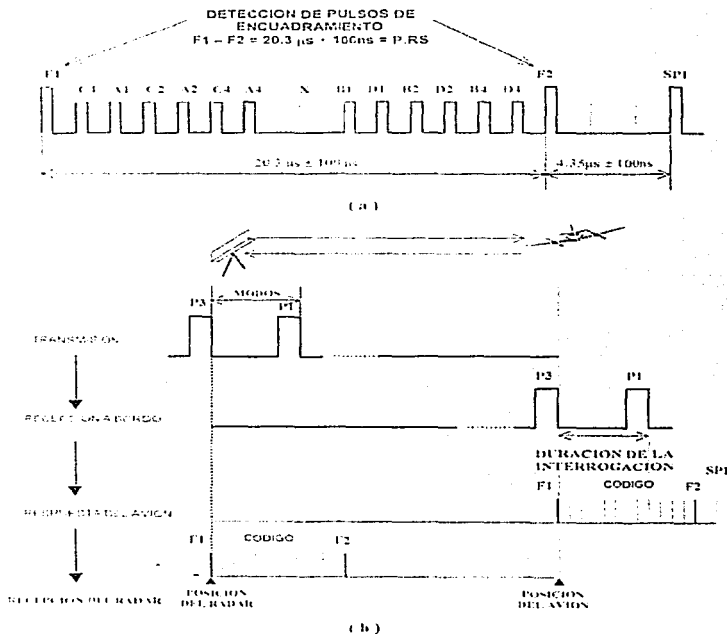


Figura 2.2.- (a) Respuesta del transpondedor a bordo; (b) Principio del radar secundario.

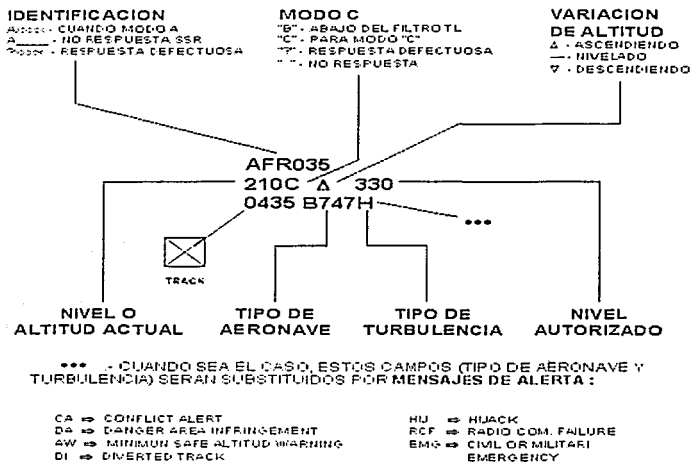


Figura 2.3.- Formatos de Etiquetas : Etiqueta Completa (contiene todos los caracteres)
 ; Etiqueta Limitada (igual a la completa pero sin identificación de la aeronave).

Término correlación.

Generalmente para autorizar el despegue de un avión se necesita lo que se conoce como plan de vuelo, que es una información generada por la compañía a la cual pertenece el avión y donde se especifica el plan a volar de la aeronave. Por ejemplo:

- Aeropuerto de salida y destino
- Escalas
- Hora de salida y hora de llegada
- Características de la aeronave
- Por donde volará, es decir, por que carreteras aéreas (llamadas aerovías).

TESIS CON
 FALLA DE ORIGEN

Esta información es enviada a los centros de control de área ACC's o a los centros de control de aproximación APP's, por diferentes medios, de parte de las compañías aéreas o particulares vía electrónica o telefónica. Esta información una vez en los centros de control es insertada al sistema de procesamiento para formar parte de su base de datos la cual va a ser accedida básicamente por el host FDP (Flight Data Processor), para poder hacer la "correlación" en su momento. Figuras 2.4 y 2.5.

Cuando un avión está despegando del aeropuerto de salida generalmente en ese momento es detectado por el radar, figura 2.5. Esto quiere decir que el radar interroga a la aeronave y el avión contesta quién es y qué altura tiene, y es hasta ese momento donde se habla de una detección radar. Esta información como ya se mencionó es enviada a la parte de procesamiento de los centros de control, para que el controlador pueda visualizar en su pantalla dicho símbolo correspondiente a la aeronave (track).

También en ese momento la parte de procesamiento asocia la información radar con la base de datos planes de vuelo y visualmente cambia la presentación de su código SSR, por el Call-Sign, Figura 2.6, que viene a ser una sustitución del código de 4 dígitos por una abreviación que representa a la compañía aérea y el número de vuelo. Por ejemplo; un código "5454" es cambiado por "MXA311", que representa un vuelo de la compañía Mexicana de Aviación (MXA) con número 311.

A este cambio de información en la presentación y su correspondiente asociación con un plan de vuelo se le conoce como **correlación**.

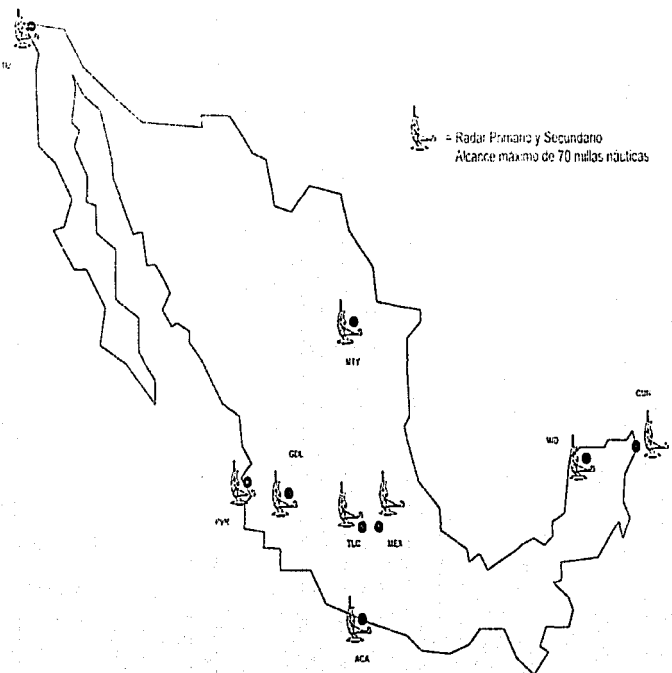


Figura 2.5.- Centros de control de aproximación.

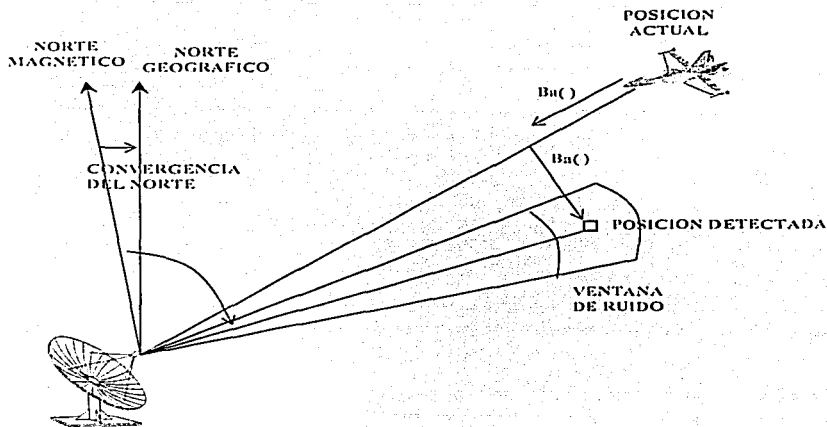


Figura 2.6.- Orientación del radar SSR y detección en coordenadas polares

FIR, Sectores Y Aerovías.

Para el control de tráfico aéreo en todo el mundo cada país divide a su territorio por áreas de control y en cada área es asignado un centro de control o procesamiento de información, esto se puede ver en la figura 2.7.

FIR

A la división virtual en áreas se le conoce como FIR (Flight Información Región), o en otras palabras es la frontera entre un centro de control y otro ó una área y otra en dicho territorio.

Sectores.

Cada área de control se subdivide en áreas más pequeñas para tener un control sobre estos sectores. Esta división se hace solo en cada centro de control. Generalmente se le asigna una posición de control por sector.

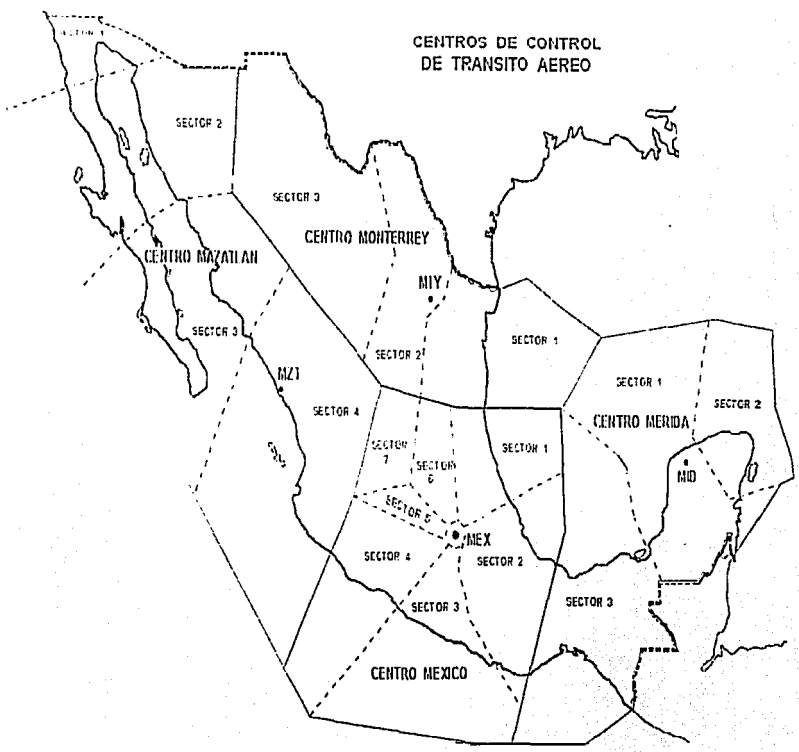


Figura 2.7.-Centros de Control de Tránsito Aéreo

Aerovías.

Las aerovías vienen a ser "carreteras aéreas" por donde los aviones tienen que volar, o sea, un avión no puede volar por donde quiera, debe volar por una aerovía, éstas son en ambos sentidos; por ejemplo, cuando un avión viaja en un sentido y otro viaja en sentido contrario por la misma aerovía, uno tendrá que volar a una altitud y el otro a una altitud diferente, para que haya seguridad en el momento de su cruce por el mismo punto. La maniobra anterior es responsabilidad del controlador.

Descripción del vuelo de una aeronave (comercial) desde su aeropuerto de salida hasta su aeropuerto destino:

Retomando el ejemplo anterior un avión, identificado por el sistema como MXA311, que volará de México a Cancún debe tener un plan de vuelo con anterioridad, generado por la compañía en este caso Mexicana de Aviación y debe de enviarlo a SENEAM, para que lo tenga en su base de datos.

Este avión que puede ser un DC10 (tipo de aeronave) una vez que se encuentra en el aeropuerto, el piloto se comunica con la torre de control para corroborar su plan de vuelo, el controlador le autoriza su despegue y le menciona el código SSR que el piloto debe colocar en su equipo transponder, dicho código lo asigna el sistema de procesamiento, garantizando que el avión tengan esta identificación y que por ninguna razón sea repetida. El controlador de la torre de control al corroborar el plan de vuelo, observa el código SSR asignado por el sistema de procesamiento y se lo informa al piloto.

En el momento del despegue de la aeronave, el piloto activa su equipo transponder, para que empiece a contestar las interrogaciones del radar y se inicie la detección del avión una vez ya teniendo las respuestas del avión, ¿Quién eres? y ¿Qué altura tiene? Esta información es enviada como se mencionó al sistema de procesamiento, donde será procesada para ser presentada visualmente al controlador, tanto de torre como en el centro de control con su correspondiente símbolo y sus campos de información. Esta información le servirá al controlador para iniciar su trabajo de control operativo de la aeronave, garantizando la seguridad e integridad de la misma.

Una vez en el aire el avión inicia el trayecto descrito por su plan de vuelo, tomando una aerovía para llegar a su destino. Esta aeronave será transferida de un área de control, a otra llamada sector "terminal", después de aproximadamente 70 millas. El control de la aeronave será nuevamente transferida a un sector de ruta en el nuevo centro de control, cuando la región de control de vuelo correspondiente sea cruzada. **Esta transferencia se hace automáticamente vía la red SENEAM transfiriendo su plan de vuelo de un centro de control a otro.** Y a su vez el control operativo de la aeronave.

Esta transferencia se observa operativamente, cuando en la pantalla del controlador el Call-Sign cambia de color, para indicar que la aeronave y el control de la misma se ha transferido con éxito. Todo ello automáticamente.

En este ejemplo el avión pasara de la torre de control México (MEX) a el centro de control ubicado en Mérida (MID), aquí se sigue un procedimiento similar, es decir, un sector de ruta en el área cubierta por MID, transferirá la aeronave hacia otro sector en el centro de control en Cancún, hasta llegar a la torre de control del mismo lugar, donde aterrizará dicha aeronave; cumpliéndose con ello la seguridad e integridad del avión en su trayecto en el espacio aéreo mexicano siendo lo anterior la principal función de SENEAM.

En cada transferencia de un centro de control a otro, también se transferirá el plan de vuelo de la aeronave.

Como se puede notar el avión siempre debe de tener una supervisión desde tierra por un centro de control, vía el controlador de vuelo, a través de toda una infraestructura de radares, comunicaciones vía satélite, radio enlaces y equipos de procesamiento en redes LAN.

Cabe mencionar que muchas funciones de control, como es el envío de mensajes vía la red SENEAM a través del satélite, son automáticas para que el controlador tenga una mayor atención y cuidado en el control de las aeronaves bajo su responsabilidad.

2.3 LA RED SENEAM.

La red SENEAM consiste en una red privada de conmutación de paquetes que conecta dos redes de área local a través de una red pública de conmutación de paquetes. De manera simple, una trama procedente de una LAN se encapsula en una trama, y se transmite por la red hasta la LAN destino. Los centros de control vienen a ser los nodos de dicha red.

La ISO (International Standards for Organization), define la conmutación de paquetes como un procedimiento de transferencia de datos mediante paquetes provistos de direcciones, en el que la vía de comunicación se ocupa solamente durante el tiempo de transmisión de un paquete, quedando a continuación la vía disponible para la transmisión de otros paquetes.

Una red de transporte de paquetes esta constituida básicamente por un conjunto de líneas de transmisión que enlazan un conjunto de nodos o centros de conmutación de paquetes. El nodo de interconexión esta constituido por una computadora, la cual recibe informaciones a través de los caminos que a ella llegan, las almacena, determina el nuevo camino que debe seguir para llegar a su destino y las retransmite.

En el funcionamiento de un nodo de interconexión se materializan dos conceptos ya clásicos en el campo de los sistemas distribuidos:

Almacenamiento y retransmisión.- Hace referencia al sistema de establecer un camino lógico de forma indirecta haciendo pasar la información desde el origen al destino a través puertos de conexión con una velocidad de acceso de 64 Kbps.

Control de ruta. Hace referencia a la selección mediante un nodo del camino por el que debe retransmitirse una información para hacerla llegar a su destino. En ocasiones, a los nodos de un sistema de este tipo se les denomina "conmutadores de paquetes" debido a las funciones que realizan.

Los nodos de la red consisten en equipos conmutadores de paquetes, llamados ECOMS o PASS, que manejan automáticamente el encaminamiento o ruteo básico de los datos hacia otros centros y que ofrecen la posibilidad de añadir líneas. el host RDP controla la transmisión de información (planes de vuelo) entre los diferentes centros conectados. La figura 2.8 ilustra los enlaces establecidos

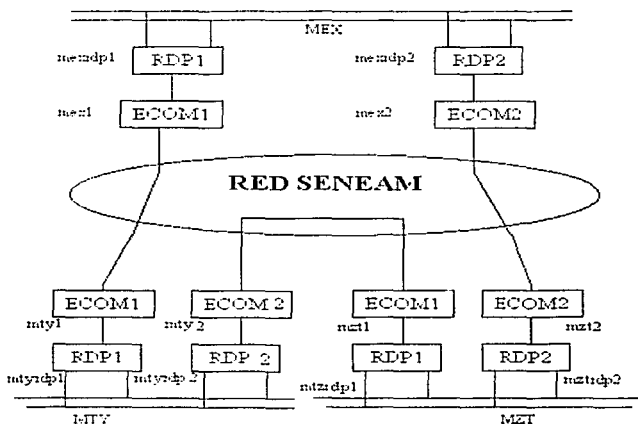


Figura 2.8.- Red SENEAM

Servicios de la red SENEAM y configuración básica

La red SENEAM tiene como función principal intercambiar mensajes de planes de vuelo (Datos en la red), entre centros de control en la república mexicana.

Los centros de control ATCC (Air Traffic Control Centre) son los nodos básicos de la red, de ahí la importancia de los mismos.

En los centros de control ATCC, sus sistemas de procesamiento están diferenciados por área de control, ya sea centros de control de área (ACC) o en los centros de control de aproximación (APP), como se nota en las figuras 2.9 y 2.10.

Un centro de control de área esta basado en una red de área local **Fast-ethernet**, en donde los servicios de la red efectúan funciones muy específicas, necesarias para la operación del mismo.

La red LAN esta compuesta por computadoras, conectadas a un HUB conformando una red en estrella, pero en realidad su topología será BUS.

Esta red esta duplicada por cuestiones de seguridad y confiabilidad.

Los Servidores de esta red se conocerán por su función en el sistema:

PIRC.- Procesador de Interfaz Radar y Comunicaciones

RDP.- Procesador de Datos Radar

FDP.- Procesador de Datos de Plan de Vuelo

VISU.- Unidad Visual

En todos los centros de control se utiliza una red **Fast-Ethernet**, definida como un estándar mundial según la IEEE en su 802.3u que se basa en principios simples y confiables. Todos los equipos conectados tienen la misma prioridad de acceso y utilizan el método de acceso CSMA/CD (Carry Sense Multiple Access/ Collision Detect), que es una competencia por el acceso a la red.

Este tipo de red utiliza un cable tipo "par trenzado" que soporta las velocidades de envío de información en la red 100 Mbs y usando una transmisión en banda base.

Es importante señalar que en la red local se utiliza el protocolo TCP/IP (transport Control protocol / Internet Protocol) para la comunicación

En los centros de control de Ruta la red esta duplicada, a nivel de cableado y en las tarjetas de red: una de estas dos redes actúa como red principal, mientras que la segunda supervisa la operación de la otra, de tal suerte que puede decirse que esta en Stand-by. En los centros llamados de Aproximación esta red LAN es única

Ahora se mencionará las funciones principales de los hosts en esta red local.

El Host PIRC

El Procesador de Interfaz Radar y Comunicaciones (PIRC), es el encargado de la recepción de los datos radar que proviene de distintos puntos en la república mexicana.

La función de datos radar, consiste básicamente en la recepción de todos los datos que llegan de los radares y los centros de control externos conectados al sistema, con el fin de obtener las condiciones actual del tráfico aéreo y de esta forma proporcionar al host VISU la información relevante (tracks, correlación y alertas) para su presentación.

Los datos radar son procesados por el PIRC cumpliendo las siguientes funciones:

- Correlación de la información radar con los parámetros locales.
- Cambio del formato de datos a un formato estándar reconocible en la red por otros hosts.
- Los datos que son procesados por el PIRC, los TRACKS LOCALES, que finalmente son enviados a la red local para poder ser recibidos principalmente por los Hosts (RDP y VISU).

El procesador FRONTAL NIU 2000 forma parte de este nodo, este procesador cumple con la función principal de recibir y decodificar toda la información proveniente de los radares conectados a la RED SENEAM.

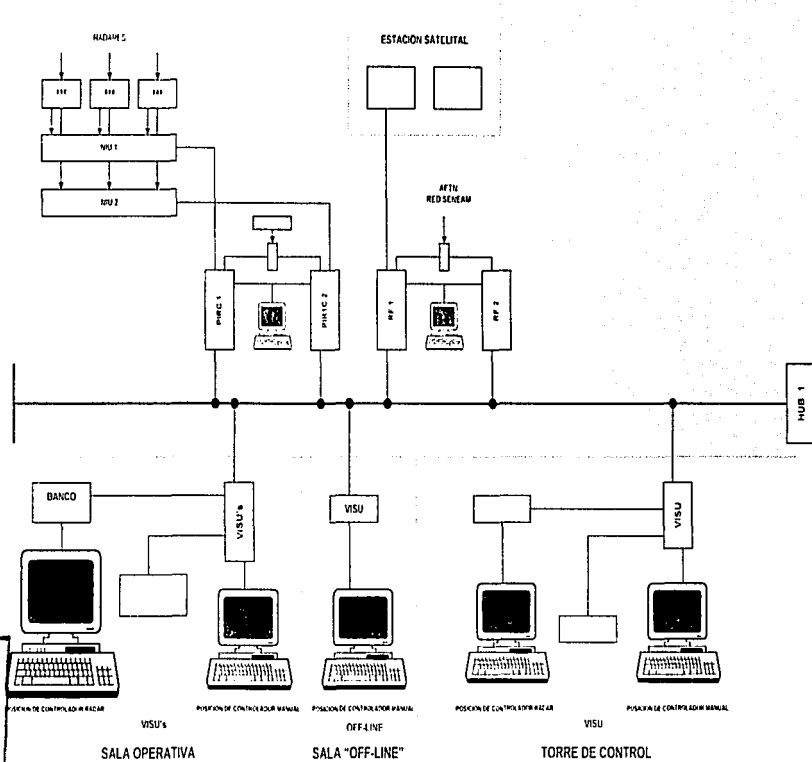
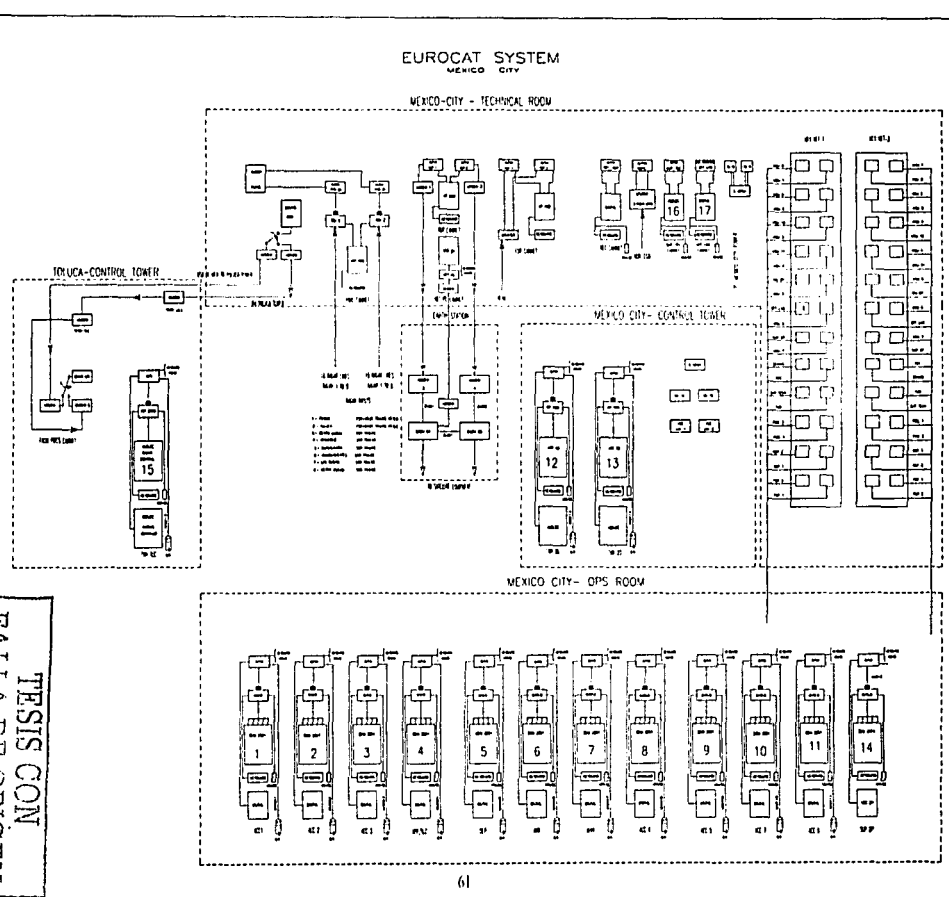


Figura 2.9.- Centro de control de Aproximación

TESIS CON
 FALLA DE ORIGEN

Figura 2.10.- Centro de control de Ruta



TESIS CON
 FALLA DE ORIGEN

Unidad visual

Los símbolos de las figuras 2.1 y 2.3 serán visualizadas en este host. La figura 2.11 muestra la posición del controlador formada básicamente por dos estaciones de trabajo:

- Posición de control radar
- Posición de control manual

La posición manual es la más importante ya que esta estación de trabajo es el servidor de la posición radar y el nodo de enlace con todo el sistema. Gracias a una interfaz gráfica se posibilita el diálogo entre los sistemas y el controlador, por medio del software X-windows, sobre una plataforma UNIX que es el sistema operativo del sistema.

Posición de control radar.- En esta pantalla se visualizan los mapas meteorológico y tracks

Posición de control manual.- Esta dedicada a la presentación de los planes de vuelo, e información general, así como también una visión alterna del radar.

Aunque las posiciones de control manual y radar utilizan las capacidades de los monitores (color, barrido y de muy alta resolución), conservan al mismo tiempo la filosofía que permite el diálogo. En las posiciones actuales se necesita reducir los tiempos de adaptación de los controladores, además de ofrecer la flexibilidad o ventaja de multi-ventanas.

La posición de control radar recibe las pistas monoradar y los planes de vuelo involucrados en el sector controlado por el usuario. El espacio aéreo es representado en forma de un mosaico.

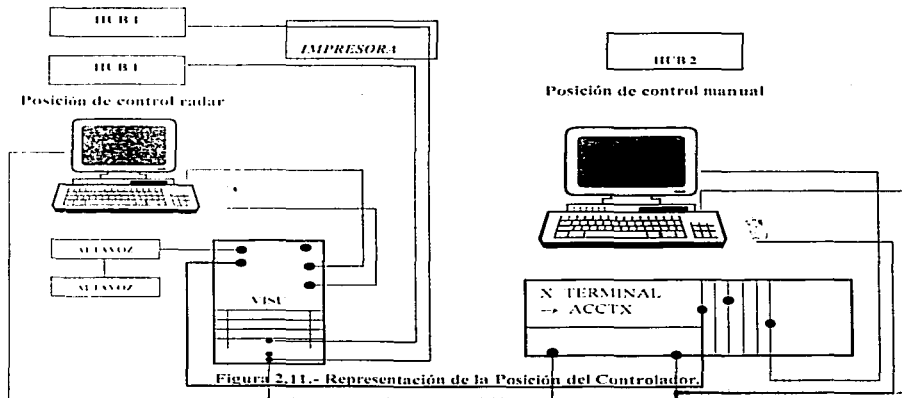


Figura 2.11.- Representación de la Posición del Controlador.

El Host RDP

La principal función del Procesador de Datos Radar (RDP), es asegurar el procesamiento de combinación de todos los posibles tracks locales que identifican a una sola aeronave, para formar con los diferentes radares una sola detección y un solo seguimiento, para así obtener lo que es llamado pista sistema y posteriormente enviarlo para su presentación en las posiciones de control y los centros de control adyacentes. Éste nodo es ilustrado en la figura 2.12

Esta información es enviada a la red específicamente a la unidad visual para que sean presentadas en tiempo real a los controladores de vuelo.

Principales funciones efectuadas por el host RDP:

- ❖ **Controlar todas las conexiones exteriores de la RED SENEAM.** función que es llevada a cabo, estando conectado el nodo RDP a un conmutador de paquetes, el cual maneja automáticamente el enrutamiento de los datos hacia los otros centros de control a través de enlaces dedicados capaces de soportar la velocidad de la red, misma que es de 64 Kbps.
- ❖ **Transmisión de planes de vuelo** entre los diferentes centros conectados, con los estándares de OACI (Organización Internacional de Aviación Civil), para garantizar todas las transferencias de datos en los planes de vuelo y según un formato estandarizado.
- ❖ **Asegurar el procesamiento de las informaciones meteorológicas.**
- ❖ **La Correlación,** se refiere a la asociación entre un track, un código de llamada y su plan de vuelo, de tal manera que el sistema pueda monitorear la trayectoria del vuelo de acuerdo a la ruta planteada y estar en posibilidades de actualizar automáticamente los tiempos estimados en el plan de vuelo y con ello asegurar un adecuado seguimiento de la aeronave.
- ❖ **Alarma de Conflicto.** El sistema esta en posibilidad de predecir posibles conflictos entre aeronaves, de acuerdo a las trayectorias esperadas y alertar con ello al controlador.
- ❖ **Alarma Mínima de Altitud.** Tiene como propósito Con el propósito de dar una forma de monitoreo sobre los posible obstáculos y dar a los controladores una alarma inmediata.
- ❖ **Alerta de Infracción de Área de Peligro.** Por medio de esta función se pretende llamar la atención del controlador sobre aquellos tráfico que pretendan ingresar en áreas predefinidas al sistema como zonas restringidas, las cuales podrían ser las áreas militares.

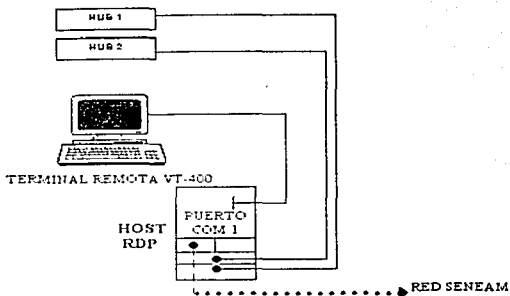


FIG. 2.12.- Representación de la RDP

El Host FDP

El Procesador de datos de vuelo (FDP), esta dentro de los servidores principales y utiliza toda la información recibida por la red. El FDP recibe del host RDP todos los mensajes del plan de vuelo procedentes del exterior para actualizar su base de datos y efectuar el seguimiento de los planes de vuelo durante su ciclo de vida. Figura 2.13.

La FDP también toma en cuenta las instrucciones de los controladores y las valida. En consecuencia éste informa a las posiciones de control VISU de los cambios que ocurrieron durante la vida del plan de vuelo. Los planes de vuelo del centro de control se transmiten vía la red SENEAM a través del host RDP a los centros adyacentes conectados a él.

Para los centros de control de Ruta las funciones RDP y FDP son realizadas por computadoras separadas. El software es idéntico para todos los centros de control de ruta y aproximación. El conjunto de computadora y NIU está duplicada para permitir una conmutación en caso de falla. Para los centros de control de aproximación las funciones RDP y FDP están alojadas en la misma computadora.

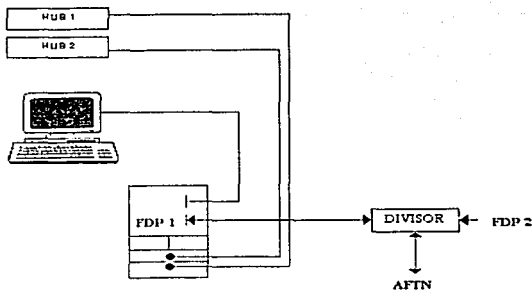


FIG. 2.13 Representación de la FDP

Ahondando en los procesos que realiza la FDP y debido a que es un nodo importante en el proceso de envío de mensajes vía la red SENEAM, se mencionan a continuación los procesamientos más importantes:

Procesamiento de mensajes

Este proceso básicamente maneja los mensajes con formato AFTN y la red SENEAM. Los mensajes vía la red AFTN, es una vía alterna para envío de planes de vuelo, serán transmitidos y recibidos por el puerto serial del host.

Este proceso se encarga de verificar la sintaxis de los mensajes recibidos, así como también construye la sintaxis de los mensajes a transmitir, la salida de este proceso tendrá las siguientes posibilidades:

- ❖ Enviar los mensajes erróneos meteorológicos y otros hacia la cola de datos para el procesamiento manual.
- ❖ Hacia el proceso de evolución de planes de vuelo.- Aquí llegarán por ejemplo activaciones, confirmaciones, actualizaciones de planes de vuelo.
- ❖ Proceso de control de RPL's, este proceso se encarga de leer sistemáticamente el archivo de base de datos cada minuto para extraer los planes de vuelo que se requieren pasar al proceso de adquisición y creación.

Proceso de adquisición y creación de planes de vuelo

Este proceso es de gran importancia ya que aquí se originan los planes de vuelo desde el punto de vista de la sintaxis para ser validado y controlado por los demás procesos. éste recibirá información de cuatro vías posibles para la creación de planes de vuelo:

1. Desde el procesamiento de mensajes (mensajes de red AFTN).
2. Desde la lista de mensajes a solicitud del controlador.
3. Bajo correcciones manuales del proceso del manejador de RPL's.
4. De las acciones del controlador de tráfico aéreo, desde la VISU.

Aquí también serán controlados los datos meteorológicos enviados desde la posición del supervisor operativo.

Los planes de vuelo serán enviados al proceso de control y semántica. Una vez verificado es regresado y almacenado en una base de datos creada en un directorio de control.

Proceso de control de sintaxis y semántica

El sistema verifica primero la sintaxis de la entrada de datos, que corresponda al formato OACT. Desde el punto de vista de la semántica, se pueden considerar los siguientes puntos importantes a verificar:

- ❖ Las literales de los aeropuertos deben de ser conocidos por el sistema
- ❖ Las características de la aeronave:
- ❖ Niveles de vuelo
- ❖ Velocidad convertida a nudos.
- ❖ Que tenga código SSR y sea compatible con la aeronave
- ❖ Que los puntos de la ruta establecida sean conocidos.

Proceso de evolución del plan de vuelo.

Existe un conjunto de archivos para el control de los tiempos necesarios y la evolución de los planes de vuelo, es decir, dependiendo del tiempo el plan de vuelo deberá pasar por diferentes estados (Pending, Active, etc.), de igual manera para lograr la interacción entre sectores se deberá de generar tiras de plan de vuelo pasando la orden al proceso de manejo de tiras. Ahora la interacción entre los centros de control, se logra a través de la conexión con el procesador de mensajes.

Este proceso se apoya también en el manejador de códigos SSR para la asignación de los códigos. Un punto importante es la comunicación que debe tener con el RDP, donde éste realiza la correlación de los tráficos aéreos de acuerdo a los TRACKS sistema mismos datos generados por la RDP, una vez realizada la correlación, la RDP informa a la FDP que deberá cambiar de estado al plan de vuelo o modifique los tiempos estimados para la generación de las tiras y estas estén de acuerdo a la posición real del track.

2.4 LA RED A NIVEL OPERATIVO.

Se inicia mencionando las etapas que atraviesa un plan de vuelo, figura 2.15 se le llamará "vida del plan de vuelo".

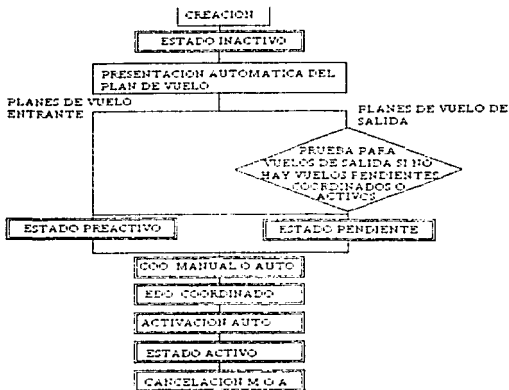


Figura.2.15.- Diagrama de flujo que muestra la vida de un plan de vuelo

Etapas del plan de vuelo:

- Estado inactivo.- El plan de vuelo ha sido creado manualmente por el controlador o automáticamente por el sistema y fue guardado, pero en esta etapa no es usado para el control de tráfico aéreo. El plan de vuelo es insertado en una lista de planes no activos en la posición de control para el primer sector o aeropuerto de salida.
- Estado preactivo.- En esta segunda etapa el subsiguiente sector ya puede tener el plan de vuelo, este proceso depende del tiempo del estado anterior.
- Estado Pending.- Este estado existe solo para los vuelos de salida, el sistema intenta correlacionar el plan de vuelo con una detección radar. Una tira de Alerta será impresa en todos los sectores involucrados.

- **Estado Coordinado.**- La entrada del plan de vuelo en el subsiguiente sector confirma el sobrevuelo a un punto de transferencia ya sea manualmente o automáticamente con los siguientes mensajes CPL vía la red SENEAM

- **Estado Activo.**- El plan de vuelo es usado actualmente para el control de tráfico aéreo y es asociado con un track. El plan de vuelo es insertado en la lista de planes de vuelo activos.

Eventos del plan de vuelo y preactivación

Funcionalmente este será el primer evento en la vida del plan de vuelo, su proceso será calculado basándose en un tiempo estimado en su base de datos. Dependiendo del tipo de vuelo, ya sea, de salida de un aeropuerto o de entrada a un FIR. Por lo que el procesamiento de esta información dependerá de la categoría del vuelo.

Determinación del FIR adyacente. Para eventos automáticos de mensajes CPL(s), la FDP tendrá que determinar a cual FIR asignarlos, para hacer lo anterior, tendrá en cuenta el último punto geográfico que sobrevuela la aeronave y este punto tendrá que estar en la base de datos.

Ningún cálculo será hecho para vuelos dentro del mismo FIR.

Proceso de Coordinación Este proceso confirma planes de vuelo preactivos y pendings, así como su entrada a un FIR; es decir, el tiempo y punto de entrada son confirmados. Serán rechazados otros planes de vuelo con la misma identificación SSR. Este proceso se inicia sólo después de la llegada de un mensaje CPL. Existiendo como alternativa a la coordinación manual o telefónica.

Procedimiento de verificación de mensajes CPL.

Los mensajes CPL son recibidos de un centro adyacente, como se muestra en la figura 2.17, vía la red de datos SENEAM o en su defecto la red AFTN, solo para vuelos entrantes al FIR.

En este proceso se chequea los siguientes parámetros:

- Chequeo de sintaxis del mensaje y debe corresponder a la sintaxis de OACI
- Chequeo de semántica del mensaje y no se permite el envío de planes de vuelo con la misma identificación de la aeronave.
- Se actualizan los datos de coordinación
- Tiempo de llegada, salida etc.
- Código de identificación de la aeronave
- El valor del tipo de aeronave y otros datos particulares de la misma.

En esta etapa se envían los datos del plan de vuelo a la computadora RDP, para su automática correlación y se estiman los tiempos de reporte.

Si existe un error en el envío de información el plan de vuelo es asignado a una lista o tabla de mensajes llamada OLDI, que puede ser accedida por el controlador, para ver el mensaje "erróneo" y poder corregir lo necesario para insertarlo nuevamente al sistema o red local.

Un mensaje LAM (Logical Acknowledgement message) es enviado al centro origen del plan de vuelo, indicando que se ha recibido correctamente. Como un reconocimiento de la información. Si el mensaje es recibido con errores como de sintaxis, semántica, etc. Se envía un mensaje de NO ACT LAM (No Activation LAM), de regreso al centro origen. Además que el controlador en el centro destino puede acceder este mensaje en la tabla o ventana de vuelos OLDI, para verificar o corregir dicho mensaje. Así como en la pantalla del controlador radar, se pone de color rosa, para remarcar que el mensaje llegó con errores. Esta alerta se puede desactivar manualmente.

En una tabla o base de datos estarán definidos los centros a los cuales los mensajes serán enviados. Si por alguna razón no se envía este mensaje ninguna coordinación o correlación será ejecutada para ese centro de control ACC(s).

Para el envío de mensajes CPL(s), al centro adyacente la transmisión debe ser habilitada en la base de datos, además el vuelo no debe ser visual y el plan de vuelo debe estar activo. Además el número de reintento de envío del CPL también es definido en la base de datos.

Los siguientes mensajes aparecerán en la pantalla del controlador dependiendo del estado del envío del mensaje (CPL).

- Ningún FIR ha sido computado
- El mensaje CPL, no ha sido recibido todavía.
- El mensaje CPL, fue recibido (LAM O.K.) exitosamente.
- El mensaje CPL, no fue recibido (NO ACT LAM) , con éxito.

Formato del mensaje CPL

El formato OACI de un mensaje CPL se integra con los siguientes datos:

- Tipo de mensaje
- Identificación de la dependencia ATC(Air Traffic Control) emisora
- Identificación de la dependencia ATC receptora
- Numero de serie del mensaje
- Identificación de la aeronave (Call-Sign)
- Modo del equipo transponder
- Código del transponder (SSR)
- Reglas de vuelo
- Tipo de vuelo
- Tipo de aeronave
- Tipo de turbulencia
- Equipo de comunicación y navegación
- Aeropuerto de salida
- Altitud o nivel que esta volando
- Velocidad verdadera

- Nivel o altitud solicitado
- Aerovía que volara desde el punto de entrada
- Aeropuerto destino
- Tiempo de ruta
- Aeropuerto(s) alterno(s)

En la figura 2.16 se muestra un ejemplo de la ventana de una posición de control manual con su respectivo plan de vuelo.

| M | | PLANNING WINDOW | | | | | | | | | | Q |
|------------------------------|-----------|-----------------|------|--------|-----------|-------|-----|-------|--|--|--|---|
| CREATE | | MODIFY | | | TERMINATE | | | ESTIM | | | | |
| SEARCH | | PREV | | | NEXT | | | RESET | | | | |
| VALID | | | | | | | | | | | | |
| ORIG | CALL SIGN | SSR | FR | FT | NR | TYPE | WTC | | | | | |
| RPL | AMX56941 | 2537 | I | S | | B747 | H | | | | | |
| EQUIP | ADEP | ETD | ADES | EET | EQUIP | | | | | | | |
| S | C | KSAN | 0840 | MMM | | MMTO | | | | | | |
| TAS | RFL | | | | | | | | | | | |
| 350 | 370 | | | | | | | | | | | |
| ROUTE | | | | | | ROUTE | | | | | | |
| TIJ LIMO CHX DGO ZCL OET MEX | | | | | | | | | | | | |
| RE-MARK | | | | | | | | | | | | |
| CFL | BPM | ETB | PFL | BPX | ETX | FIR | | | | | | |
| | | | | | | | | | | | | |
| SECTORS | | ACT/PAC | | STATUS | | | | | | | | |
| | | | | | | | | | | | | |

Figura.2.16.- Ventana de plan de vuelo en la Posición de Controlador

2.5 CONSECUENCIAS DE FALLA Y ALTERNATIVAS DE LA RED SENEAM

En el caso de que se presente una falla en la red SENEAM el envío de mensajes CPL(s) de un centro de control a otro, tendría severos problemas ya que es de vital importancia tener conocimiento actualizado con intervalos de tiempo corto, en que momento una aeronave entra o sale de un centro de control y también saber a donde se dirige en tiempo real por que SENEAM tiene como principal función el salvaguardar la integridad física de tanto tripulantes como de pasajeros en el momento que aborden cualquier aeronave dentro del territorio nacional o en el extranjero.

Pero operativamente existen dos alternativas manuales hasta el momento, para continuar con un alto grado de confiabilidad y garantizar la seguridad en cada vuelo. Las dos alternativas son:

- 1.- Vía una red AFTN
- 2.- Vía Telefónica.

1. Vía una red AFTN (Aeronautical Fixed Telecommunications Network).

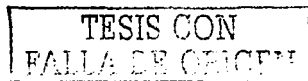
La AFTN es una red de telecomunicaciones dedicada al intercambio de mensajes entre las empresas aéreas, las estaciones nacionales e internacionales y en general el medio aeronáutico, tal como se muestra en la figura 2.17.

Los Transmisores y receptores son las herramientas con las que los controladores de vuelo que pueden comunicarse con los pilotos de las aeronaves, tanto para transmitir como para recibir mensajes del control de aeronaves, para este fin se utilizan canales de comunicación VHF en la banda de la aviación civil que se encuentran en cada torre de control y como en las estaciones remotas que enlazan a los centros de control y con las torres de control a través de canales de la Red Nacional de Microondas, Fibra Óptica y los Satélites de Comunicación, estos enlaces son en realidad punto a punto o llamados enlaces dedicados, que al unir los nodos forman la red AFTN. Esta red viene a ser una vía alterna de envío de planes de vuelo, entre centros de control.

Esta red esta conectada al host FDP por medio de una conexión serial (RS-232), por donde se transmite y recibe información de planes de vuelo.

Operativamente el controlador tiene en su posición de control una aplicación para poder enviar mensajes a la red AFTN, con el destino que el escoja, por ejemplo, otro centro de control. Una vez recibida la información en el otro centro de control, el controlador en el centro destino podrá accezarla para conocer el mensaje, también a través de la misma aplicación en su posición de control.

Este proceso es manual y es usado operativamente por el controlador cuando algún nodo de la red SENEAM, esta fuera de servicio.



Como se mencionó, esta vía no deja de ser una vía alterna, debido a que la vía principal es la red SENEAM y es automática.

2. Vía telefónica

Esta otra vía alterna, es mediante la cual el controlador puede enviar y recibir información de planes de vuelo vía telefónica, figura 2.18

En la posición de control existen unos teléfonos instalados, que son conectados a un equipo de comunicación llamado Frequentis cuya función principal es y puede tener comunicación vía microondas o Telmex (LADA) o satélite, el controlador tiene acceso a otro centro de control o aeropuerto.

Dependiendo del aeropuerto destino de la conversación el controlador puede usar el sistema Frequentis o Telmex, para comunicarse.

Una vez establecida la comunicación se puede enviar la información requerida planes de vuelo, básicamente, al otro centro de control o al otro controlador. De tal suerte que en el aeropuerto destino, el controlador cree un plan de vuelo manualmente con la información recibida vía voz, del aeropuerto origen.

Una vez creada la información del plan de vuelo esta será insertada en el sistema de procesamiento, para su seguimiento automático en la vida del plan de vuelo.

Como se podrá notar, esta vía, también será poco usada por el controlador, ya que sigue siendo manual, y la vía principal es automática.

Remarcando algunas diferencias entre las alternativas, en la red AFTN, el controlador no tiene que insertar el plan de vuelo al sistema ya que éste es insertado primero y después el controlador nota la recepción del mismo.

Otra ventaja de la vía AFTN sobre el envío de información oralmente, es que en la primera, si el plan es transferido correctamente, el sistema de procesamiento lo correlacionara automáticamente de no llegar correctamente, se le informa al controlador que tiene un mensaje erróneo o que acaba de llegar un mensaje incorrecto en alguno de sus parámetros. Ya enterado el controlador podrá reeditar el mensaje para corregirlo y que el sistema una vez corregido, sea capaz de correlacionarlo automáticamente.

Resumiendo, existen dos alternativas para la transferencia de información de planes de vuelo, aunque ambas son manuales, no dejan de ser vías alternas en caso de falla de la red SENEAM.

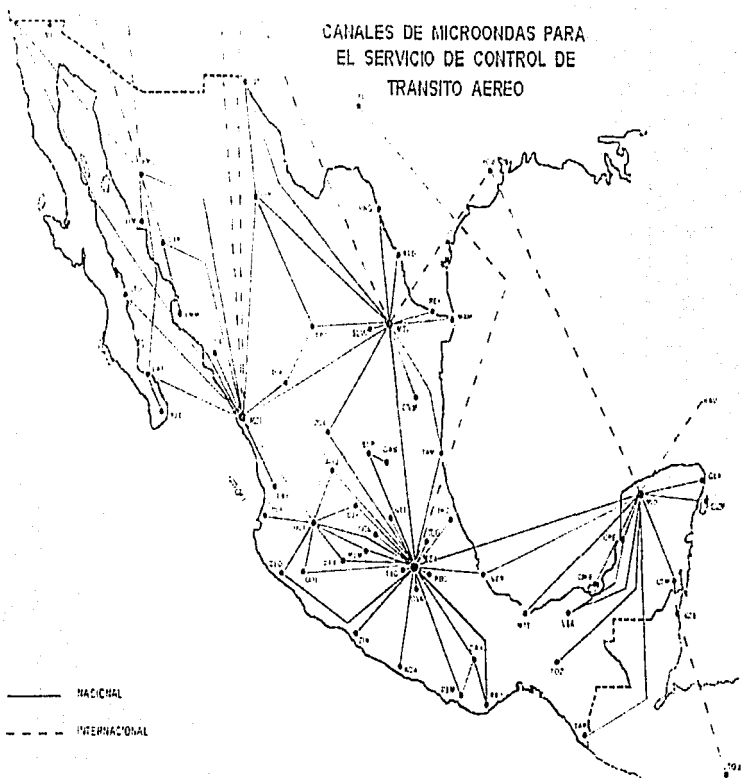


Figura 2.18.- Canales de Microondas

CONCLUSIONES

75A.

TESIS CON
FALLA DE ORIGEN

Con lo expuesto a lo largo del primer capítulo de este trabajo se concluye que el futuro de las redes va encaminado a un objetivo muy importante el cual es lograr que todos los dispositivos no importando donde se encuentren puedan estar comunicados unos con otros, tal vez con la ayuda de un cable o con nuevas tecnologías inalámbricas.

Se puede pensar que todo este avance en la tecnología de redes nos hace más fácil el trabajo a los seres humanos, ya que a través de un teléfono celular o una computadora portátil podamos acceder a la información que tenemos en nuestra oficina simplemente estando comunicados sin tener que recorrer grandes distancias.

La tecnología que rodea a las redes de datos ha ido evolucionando día a día, una parte muy importante que ha hecho posible muchos logros es la Internet.

La velocidad con la cual se realizan nuevos adelantos en las redes de datos es impresionante que las tecnologías que en estos momentos se consideran como novedosas al cabo de seis meses o un año quedaran relegadas por otras que ofrecerán mejores desempeños y a un bajo costo.

Por otro lado en el capítulo dos se hizo una breve descripción de la Red de datos utilizada en un centro de control de tráfico aéreo. El personal adscrito a esta dependencia se encarga de regular el tráfico aéreo de una forma rápida segura y ordenada, salvaguardando las vidas humanas que van en los aviones.

Se trato de explicar de manera técnica las funciones desarrolladas por el sistema en las diferentes estaciones de trabajo, este sistema esta enlazado en una red LAN. Cada nodo de nuestro sistema - PIRC, RDP y FDP - cumple con una o varias funciones como se menciona. La red es por lo tanto utilizada para comunicarse y obtener datos o enviar resultados de las acciones emprendidas en cada nodo.

Es importante remarcar que cada nodo en el sistema es en realidad un nodo dual, es decir, que se encuentra acoplados dos nodos idénticos, duplicados como se menciono por razones de seguridad. Un nodo corre en modo operacional, mientras que el otro opera en "stand-by". El nodo que se encuentra en "stand-by" es capaz de cambiar a modo operacional en caso de falla del otro. Esta transición se conoce como "switch-over", la cual puede ser en forma manual o automática. La forma automática se da en caso de falla de la computadora operacional, mientras que la manual es el resultado de un comando del supervisor técnico.

De manera general se da una explicación lo mas clara y concisa posible, ya que dicha información es demasiado técnica y especializada, de como es generado, actualizado y enviado un plan de vuelo, que como se menciono fluye a través de la red LAN.

También se hablo de la red SENEAM, que interconecta cada uno de los centros de control y aproximación con el propósito de intercambiar pistas sistema, mensajes de servicios de control de tránsito aéreo, para crear o actualizar los planes de vuelo en tiempo real.

Cada centro de control o nodo de la red, debe de contar con los recursos técnicos, administrativos y humanos necesarios para cumplir con su función y operación, para ello brindar con seguridad los servicios a las aeronaves en su viaje.

En caso de una falla en la red, existen dos alternativas como son la red AFTN y la comunicación oral por microondas. Estas alternativas son importantes pero como se menciono no totalmente automáticas, con lo cual tiene esa desventaja respecto a la red SENEAM.

Finalmente SENEAM como compañía que esta ala vanguardia en telecomunicaciones, tendrá que emigrar de su actual sistema de comunicación buscando nuevas tecnologías que con un alto grado de eficacia garantice la seguridad en los servicios a la navegación en el espacio aéreo mexicano.

Nosotros como profesionistas debemos tener una misión parecida de estar siempre a la vanguardia en nuevas tecnologías, tratar de estar siempre en una constante actualización, ya que esta profesión de elegimos cambia día a día y en nuestras manos esta el contribuir a esos cambios y al desarrollo de nuestro país.

ANEXO

770.

TESIS CON
FALLA DE ORIGEN

ESTÁNDARES DEL IEEE PARA REDES LAN

Los estándares del IEEE (Institute of Electrical and Electronic Engineers), se crearon para asegurar la compatibilidad entre los productos de diferentes fabricantes.

De los más conocidos tenemos los comités 802, que definen las normas de redes de área local. La mayoría de estas normas se establecieron en los años ochenta, muchas de ellas son también normas de ISO (Organización Internacional de Estandarización). Por ejemplo la 802.3 del IEEE es la 8802.3 de ISO.

Estandares IEEE 802.3 - Ethernet. Este estándar data de 1985 y se basa en el protocolo Ethernet creado por Xerox en los años setenta. Contiene la especificación de un protocolo basado en acceso por contienda utilizando el mecanismo CSMA/CD El CSMA/CD (Carrier Sense Multiple Access with Collision Detection) o sea "Acceso Múltiple con detección de portadora y detección de colisiones" es un método en el cual cuando un nodo tiene que transmitir en primer lugar observa el medio para ver si existe algún nodo transmitiendo.

IEEE 802.3 admite la utilización de distintos tipos de cableado: coaxial, UTP, fibra óptica.

- Ethernet 10Base2 conocido como thin ethernet se instala en topología física de bus, utilizando cable coaxial con terminaciones de 50 ohmios.

Una de las implantaciones más comunes de Ethernet es mediante el uso de UTP y concentrador. Cuando se utiliza esta estructura para la Ethernet se suele referir a la misma como Ethernet 10BaseT.

El IEEE 802.3u es el comité para Fast Ethernet 100Base-T a velocidad de 100 Mbps.

- Gigabit Ethernet. Es una extensión del estándar IEEE 802.3 pero con velocidad de 1 Gbps (1000 Mbps)

El modelo IEEE tiene dos niveles o capas: Nivel Físico: Relacionado con el medio de transmisión, la conexión, señales eléctricas, etc.

Nivel de Enlace: dividido en

- Control de enlace lógico (LLC, Logical Link Control). Su objetivo es manejar distintos tipos de servicios de comunicación que se pueden ofrecer a través del medio.
- Control de acceso al medio (MAC, Media Access Control). Ofrece la dirección física del equipo conectado a la red y los mecanismos utilizados para el uso del medio.

A continuación se hace una breve descripción de las normas más importantes de los estándares del IEEE.

ENLACE LÓGICO DE DATOS LLC

El estándar 802.2 describe los servicios, características y protocolos del subnivel LLC (Logical Link Control), en el contexto de la torre de las redes de área local.

El subnivel LLC constituye el nivel superior del nivel de enlace y es común para los diferentes métodos de acceso al medio.

El nivel de enlace para redes locales se asemeja en gran medida a la mayoría de los niveles de enlace existentes. Al igual que éstos, su principal función está relacionada con la transmisión de tramas de datos entre dos estaciones sin la utilización de nodos intermedios. Tres son los aspectos es los que difiere de los niveles de enlace tradicionales:

- Debe soportar la función multidestino. La diferencia con multipunto es que no existe el concepto de estación primaria
- Algunos detalles del acceso al enlace son cubiertos por el nivel de control de acceso al medio.
- Debe proporcionar algunas de las funciones del nivel de red.

La figura A-1 puede ayudar a clarificar los requerimientos del nivel de enlace. Se consideren dos estaciones o sistemas comunicados a través de la red de área local (bus o anillo). Los niveles superiores (los equivalentes a transporte y superiores) proporcionan los servicios extremo a extremo entre las estaciones. Por debajo del subnivel LLC, el subnivel de control de acceso al medio (MAC) suministra la lógica necesaria en la obtención del acceso a la red para la transmisión y recepción de tramas.

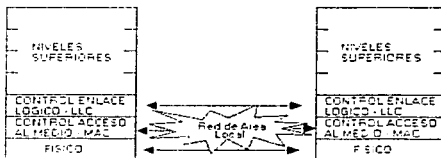


Figura A-1

Como mínimo, el subnivel LLC debe realizar las funciones normalmente asociadas al nivel de enlace:

- Control de errores extremo a extremo. El nivel de enlace debería garantizar una transmisión libre de errores a través de la red.
- Control de flujo extremo a extremo
- Control de secuencia. Las tramas son entregadas por la red en el mismo orden en que fueron enviadas

Debido a la inexistencia de nodos intermedios, la red local no requiere un nivel de red independiente; en su lugar, las funciones esenciales del nivel 3 se incorporan al nivel 2:

- Servicio no orientado a conexión. Este tipo de servicios es necesario para el soporte eficiente de un tráfico altamente interactivo.
- Servicio orientado a conexión.
- Multiplexación. Generalmente la estación se conecta a la red mediante un único enlace físico. Por ello debería ser posible proporcionar transferencia de información con múltiples puntos finales en el enlace.

Debido a que no existe la necesidad de encaminamiento, las funciones anteriormente citadas son proporcionadas de una manera sencilla. El servicio no orientado a conexión únicamente requiere la utilización de campos de dirección de emisor destino. La estación emisora debe indicar la dirección de destino; de esta forma el envío de la trama se realiza correctamente. Igualmente, debe indicarse la dirección del emisor de manera que el receptor sepa de donde vino la trama.

La norma 802.2 describe las especificaciones de la interfaz de servicio del subnivel LLC con:

- Nivel de Red : Define una descripción de los diversos servicios que el subnivel LLC ofrece a dicho nivel.
- Subnivel MAC: Define una descripción de los servicios que el subnivel LLC requiere del subnivel MAC
- Función de gestión del subnivel LLC. Proporciona una descripción de los servicios de administración proporcionados al subnivel LLC por la función de gestión del subnivel LLC

Los servicios del subnivel LLC son definidos independientemente del modo de acceso al medio y de la naturaleza del propio medio.

Todas las especificaciones de las interfaces de servicio señaladas anteriormente son proporcionadas mediante primitivas que representan de manera abstracta el intercambio lógico de la información y control entre el subnivel LLC y la función de servicio específica, según se trate (el nivel de red, subnivel MAC o función de gestión del subnivel LLC).

Por otra parte el estándar proporciona una descripción de los protocolos igual a igual que se definen para la transferencia de información y control entre cualquier par de puntos de Acceso al Servicio al Nivel de Enlace de Datos. Los procedimientos LLC son independientes del tipo de control de acceso al medio utilizado.

TESIS CON
FALLA DE ORIGEN

CONTROL DE ACCESO AL MEDIO, MAC, CSMA/CD

El estándar IEEE 802.3 parte de la red Ethernet pero no son idénticos, aunque son capaces de coexistir en el mismo medio. Su principal diferencia reside en la cabecera del paquete de red.

El estándar original IEEE 802.2 especificaba la operación CSMA/CD en la banda base sobre cable coaxial. Posteriormente IEEE ha desarrollado variaciones para CSMA/CD banda base sobre cable coaxial fino y par trenzado, así como banda ancha y operación a Mbps.

La técnica de control de acceso al medio utilizada en IEEE es la de acceso múltiple con detección de portadora y colisión, CSMA/CD.

Esto es que si en este modo de operación, la estación que desea transmitir, en primer lugar, escucha el medio para determinar su situación; si no existe ninguna transmisión en proceso (detección de portadora) puede transmitir sus datos. Puede darse el caso de que varias estaciones encuentren libre el medio e inicien sus transmisiones a la vez o casi simultáneamente, dando lugar a una colisión. Los datos de las transmisiones involucradas se interferirían y no serían recibidos correctamente.

Puesto que solo puede transmitir una estación en un momento o espacio de tiempo dado, es necesario un mecanismo de control que determina el procedimiento a seguir por una estación cuando encuentra el medio ocupado u ocurre una colisión. Este mecanismo comprende los siguientes pasos:

- Paso 1. Si el medio esta libre, transmite; si no realiza el paso 2.
- Paso 2. Si el medio esta ocupado continúa escuchando hasta que se encuentre libre y transmite inmediatamente.
- Paso 3. Si se detecta una colisión durante la transmisión, transmite una señal de colisión para asegurar que todas las estaciones han reconocido la colisión, y cesa la transmisión.
- Paso 4. Después de transmitir la señal de colisión espera durante un espacio de tiempo aleatorio e intenta transmitir de nuevo (vuelve al paso 1).

En el procedimiento anterior se ponen de manifiesto varios aspectos relacionados con el tiempo, con todos en función de un único parámetro denominado tiempo de ranura o slot time. Este parámetro se define como un valor superior a la suma del retardo de propagación ida y vuelta en el nivel físico (dos veces el tiempo que tarda la señal en recorrer el medio de un extremo a otro) más el tiempo de *jamb* del subnivel MAC. En función de este parámetro se definen los siguientes aspectos del protocolo:

- Límite superior del tiempo que se tarda en detectar una colisión y, por lo tanto, de la cantidad de ancho de banda desperdiciada en una colisión.
- Límite superior del tiempo de adquisición del medio, es decir, si transcurre ese intervalo de tiempo sin producirse una colisión, entonces ya no se producirá y puede considerarse que se ha adquirido el canal.
- Longitud máxima del fragmento de trama generado en una colisión.
- Unidad de tiempo utilizada en el procedimiento de retransmisión.
- Longitud mínima de la trama para que pueda detectarse la colisión antes de finalizar la transmisión.

La figura A-2 muestra el tiempo de slot en un bus banda base en el caso más desfavorable: que las dos estaciones involucradas en la colisión se encuentren lo más apartadas posible la una de la otra. Por mencionar algún ejemplo se puede decir que, T representa el tiempo de propagación y τ un tiempo infinitamente pequeño. En el instante t_0 el nodo A comienza la transmisión y detecta la colisión tras un intervalo de tiempo $2T$ equivalente al doble del tiempo de propagación.

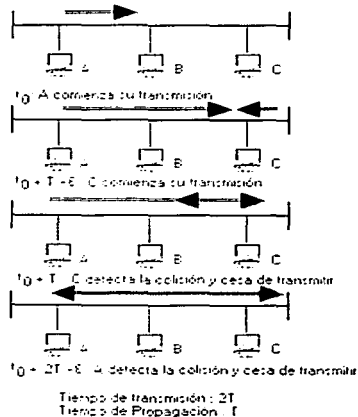


Figura A-2

En el caso de un bus de banda ancha el tiempo de espera es incluso mayor al de banda base.

El tiempo de *slot* en el peor de los casos, es decir, cuando la topología es dual-bus en banda ancha. El tiempo necesario para detectar una colisión equivale al tiempo que tarda la señal en hacer un recorrido cuatro veces la distancia máxima entre estaciones que se define en 2.5 Km. Puesto que la señal recorre el medio a una velocidad de 5 microsegundos por kilómetro (considerando la velocidad de la señal de 200 000 km/sg), el tiempo del recorrido es $4 \times 2.5 \text{ km} \times 5 \text{ micro} = 50 \text{ micros}$. En una red de 10 Mbps equivale a 500 bits. El estándar especifica, de hecho, 512 bits, es decir 64 octetos, equivalente a 51.2 microseg.

El tiempo de slot también se utiliza como referencia en el algoritmo de retrasmisión. Para evitar que dos estaciones involucradas en una colisión vuelvan a retransmitir un tiempo determinado por una distribución aleatoria. Es importante señalar que al disminuir las retransmisiones tras una colisión, puesto que generan tráfico adicional y pueden llegar a colapsar la red si las retransmisiones a su vez dan lugar a colisiones y así sucesivamente se incrementa para compensar la carga extra de la red.

ESTRUCTURA DE LA TRAMA MAC.

El estándar 802.3 CSMA/CD define sobre la estructura del nivel MAC, el marco estructural para sistemas de comunicaciones de datos utilizando procedimientos del subnivel MAC. También define las posiciones relativas de los diversos componentes de la trama MAC. Especifica el método para representar direcciones de estaciones y define particiones del espacio de direcciones en direcciones individuales o de grupo, y en direcciones administrativas globalmente o por usuario. La figura A-3 muestra los campos de un paquete MAC:

- **PREÁMBULO:** Es un campo de 7 octetos que se utiliza para permitir a los circuitos PLS alcanzar estados regulares.
- **DELIMITADOR DE PARTIDA:** Es una secuencia "10101011" que sigue al preámbulo y señala la partida de un paquete válido.
- **DIRECCIONES:** Cada paquete MAC contiene dos campos de direcciones: la dirección de destino que especifica las direcciones a las cuales el paquete va dirigido y la dirección de origen que permite identificar la estación desde la cual el paquete fue enviado. La primera puede ser una dirección individual o de grupo. La segunda no es interpretada por el subnivel CSMA/CD MAC
- **LONGITUD:** Este campo de dos octetos tiene un valor que indica el número de octetos de datos LLC en el campo de datos.
- **CAMPO DE DATOS Y RELLENO:** El campo de datos contiene una secuencia de n octetos. Se proporciona transparencia total en el sentido de que cualquier secuencia arbitraria de valores puede aparecer en el campo de datos. Dicho campo de datos debe tener un tamaño mínimo. Si no lo alcanza, el subnivel MAC añadirá automáticamente unos octetos (PAD) hasta obtener dicho tamaño mínimo necesario.

- **SECUENCIA DE VERIFICACIÓN:** Un código de redundancia cíclica es utilizado por los algoritmos de transmisión y recepción para generar este campo compuesto por 4 octetos de valores.

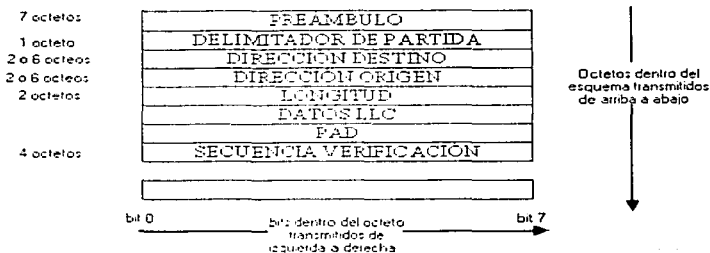


Figura A-3

Los campos son de tamaño fijo con la excepción de los campos de datos LLC y PAD.

Los octetos de un paquete son transmitidos de arriba a bajo y los bits de cada octeto de izquierda a derecha.

Se puede definir un paquete MAC inválido como aquel que cumple, al menos, una de las siguientes condiciones:

- Es identificado como tal por el nivel físico
- Su longitud no es un número entero de octetos
- No contiene dos direcciones de campo, un campo de longitud, un campo de FCS y un mínimo de información MAC, en el orden que corresponde
- Los bits de la trama que se recibe no generan un valor CRC idéntico al que recibido

Los contenidos de los paquetes MAC inválido no serán transmitidos al LLC, y se comunica su existencia a las funciones de gestión de red.

ESPECIFICACIONES DEL NIVEL FÍSICO

En la norma IEEE 802.3 se han definido varios tipos de medios físicos de transmisión y distintas topologías para dar soluciones a las necesidades de diferentes clases de aplicaciones. La notación utilizada para las distintas opciones es la siguiente:

<velocidad de la red en Mbps><tipo de transmisión><máxima longitud del segmento en centenares de metros>

Las opciones definidas dentro de la norma son:

- ⊗ 10 BASE 5
- ⊗ 10 BASE 2
- ⊗ 1 BASE 5
- ⊗ 10 BASE T
- ⊗ 10 BROAD 36
- ⊗ 100 BASE T

10 BASE y 100 BASE T no siguen totalmente la notación especificada. T representa el tipo de medio utilizado, refiriéndose al par trenzado. BASE indica tipo de transmisión banda base mientras que BROAD especifica banda ancha.

| Parámetro | 10 BASE 5 | 10 BASE 2 | 1 BASE 5 | 10 BASE T | 10 BROAD 36 |
|---|------------------------------|------------------------------|-----------------------------------|--------------------------------|------------------------------|
| Medio de Transmisión | Cable coaxial 50 Ω | Cable coaxial 50 Ω | Par trenzado no apantallado | Par trenzado no apantallado | Cable coaxial 75 Ω |
| Técnica de señalización | Banda base (Manchester) | Banda base (Manchester) | Banda base (Manchester) | Banda base (Manchester) | Banda ancha (DPSK) |
| Velocidad (Mbps) | 10 | 10 | 1 | 10 | 10 |
| Longitud may. Del segmento (metros) | 500 | 185 | 500 | 100 | 1800 |
| Longitud total de la red (metros) | 2500 | 925 | 2500 | 500 | 3600 |
| Nodos por segmento | 100 | 30 | - | - | - |

Tabla A-1. Especificaciones del nivel físico.

10 BASE T Y 100 BASE T no sigue totalmente la notación especificada. T representa el tipo de medio utilizado, refiriéndose al par trenzado. BASE indica tipo de transmisión banda base mientras que BROAD especifica banda ancha.

El estándar 802.3 prevé que, muchos casos, las estaciones estén situadas a una corta distancia del medio físico de la red local. En esta configuración, se precisa de una pequeña parte del hardware en una unidad de conexión al medio adyacente a la red, mientras que la mayor parte del hardware y todo el software se ubicarán en la estación. Las funciones del MAU serán: transmisión de la señal en el medio, recepción de la señal procedente del

medio, recepción de la señal procedente del medio, reconocimiento de la presencia de señal en el medio y reconocimiento de una colisión.

FAST ETHERNET

Una de las opciones más simples para obtener alta velocidad en Redes De Área Local consiste en adaptar el estándar IEEE 802.3 para CSMA/Cd a la velocidad de 100 Mbps. La idea básica es conservar el método de acceso, MAC, con objeto de mantener la máxima compatibilidad con la extensa base instalada de redes Ethernet e IEEE 802.3/ISO 8802-3. Puede destacarse las siguientes características:

- Coste reducido, en línea con la norma Ethernet / IEEE 802.3
- Mantener el MAC, para simplificar el inter operación con las redes existentes y poder utilizar el mismo software
- Utilización de cable UTP (Par Trenzado sin Apantallar), por ser el más extendido y económico.
- Fácil coexistencia y migración con los estándares existentes. La situación ideal sería disponer de tarjetas que operen a 10/100 Mbps.

Las limitaciones fundamentales se derivan del propio método de acceso CSMA/CD: distancia, tiempo de respuesta no controlado en condiciones de alta carga, poca adecuación a aplicaciones con tiempo de respuesta crítica.

PASO DE TESTIGO EN BUS

La norma IEEE 802.4 define el protocolo de control de acceso al medio (MAC) para paso de testigo en bus (*Token Bus*). Incluye también varias opciones sobre medios físicos de transmisión y velocidades de red.

El objetivo que dio lugar al estándar fue el de anular la simplicidad de las redes en bus y la garantía de un tiempo máximo de retardo de las redes de paso de testigo, en este sistema se puede garantizar el tiempo máximo de envío en condiciones normales de trabajo; características que es muy importante para algunas aplicaciones, como las de control de procesos.

En el paso de testigo en bus las estaciones forman un anillo lógico, es decir, cada estación tiene asignada una posición lógica, independiente de la física, dentro de una secuencia ordenada y circular, en la que a la última estación le sigue la primera. Cada una de las estaciones conoce la dirección de su estación antecesora y la de su estación sucesora.

El derecho de acceso al medio viene regulado por una trama de control denominada testigo o token. La estación que posee el testigo obtiene el control del medio durante un período de tiempo determinado. Durante este tiempo puede transmitir cuantas tramas desee, consultar estaciones y recibir respuestas. Finalizada la transmisión o el tiempo asignado cede el testigo a la siguiente estación en el orden lógico, que ahora tendrá el permiso para

transmitir. El método de operación consiste en fases alternas de transmisión y transferencia del testigo. En la red pueden existir estaciones que no hagan uso del testigo aun conectadas para responder a consultas o peticiones de confirmación.

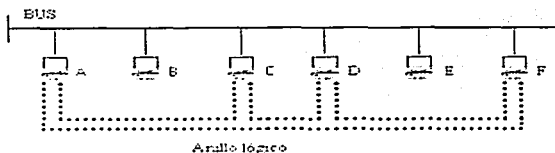


Figura A-4

La figura A-4 ilustra una red de paso de testigo en bus. De todas las estaciones, en cualquier momento, un cierto número pueden encontrarse activas y recibir tramas: todas o parte de estas estaciones activas son las que forman el anillo lógico. En la figura las estaciones A, C, D, F componen el anillo y las estaciones B y E están activas pero no se encuentran incluidas en el anillo.

Como se dijo anteriormente, cada estación conoce la dirección de su estación antecesora (EA), aquella que le transfiere el testigo, y de su sucesora (ES), aquella a la que transfiere el testigo. Las direcciones de las estaciones EA y ES se determinan dinámicamente con el objetivo de mantener un único anillo lógico. Este anillo se crea y mantiene de manera que las estaciones se ordenan lógicamente por orden descendente de sus direcciones MAC, a excepción de la última estación que tiene la dirección MAC más baja que es seguida por la estación que tiene la dirección más alta.

La esencia del método de acceso por testigo se puede sintetizar en las siguientes consideraciones:

- Un testigo o token controla el acceso ordenado al medio físico, la estación que posee el testigo tiene momentáneamente el control sobre el medio.
- El testigo circula por todas las estaciones que residen en el medio. Se requiere, por tanto, la existencia de un anillo lógico.
- El mantenimiento del anillo se asegura a través de las funciones proporcionadas por las propias estaciones: iniciación del anillo, recuperación del testigo, adición y eliminación de una estación y manejo general de anillo lógico.

Generalmente, el medio compartido puede utilizarse de dos formas: difusión y secuencial. La norma IEEE 802.4 trata únicamente de la técnica de difusión, en la que cada estación puede recibir todas las señales transmitidas; el medio se configura usualmente mediante un bus físico.

Desde una perspectiva lógica, sin embargo, el subnivel de control de acceso al medio provee acceso secuencial al bus compartido pasando el control del medio de estación de un modo circular. El subnivel MAC determina cuándo la estación tiene el acceso al medio compartido por reconocimiento y aceptación del testigo emitido desde la estación predecesora y determina cuándo se debe pasar el testigo a la siguiente estación.

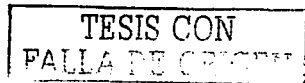
Las funciones generales del subnivel MAC son:

- ⊙ Temporización para identificación de pérdida del testigo
- ⊙ Inicialización de la transmisión
- ⊙ Tiempo de posesión del testigo (para múltiples clases de servicio)
- ⊙ Limitación de datos en el bus
- ⊙ Reconocimiento de dirección de nodos
- ⊙ Encapsulado de tramas (incluyendo preparación de testigo)
- ⊙ Generación de FCS y verificación
- ⊙ Reconocimiento de testigo válido
- ⊙ Adición de nuevos miembros al anillo
- ⊙ Recuperación de errores en un nodo.

ESTRUCTURA DE LA TRAMA MAC.

En la figura A-5 muestra el formato de la trama del protocolo IEEE 802.4. Los campos que contiene son los siguientes:

- **PREAMBULO:** un patrón de uno o más octetos utilizando por el receptor para establecer la sincronización de bit.
- **DELIMITADOR DE TRAMA:** indica el comienzo de la trama. Contiene patrones de señalización distintos a los datos. Su codificación es XX0XX000, donde X representa un símbolo carente de información. La forma de este símbolo depende de la codificación de señal utilizada en el medio.
- **TRAMA DE CONTROL:** los dos primeros bits indican si se trata de una trama de control o de una trama de datos LLC. Las tramas de control se emplean para gestionar el protocolo de testigo en bus.
- **DIRECCIÓN DESTINO:** igual que 802.3
- **DIRECCIÓN ORIGEN:** igual que 802.3
- **DATOS:** contiene la unidad de datos LLC o información para control del modo de operación.
- **SECUENCIA DE VERIFICACIÓN DE TRAMA:** igual que 802.3
- **DELIMITADOR DE TRAMA:** indica el final de la trama.



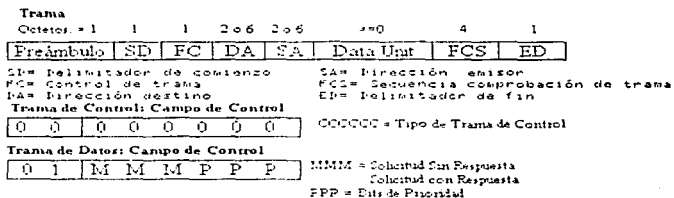


Figura A-5

Las funciones básicas de gestión y mantenimiento del acceso al medio deben ser realizadas por al menos una estación. Estas funciones básicas son las siguientes:

- Adición al anillo: las estaciones no participantes en el anillo deben tener periódicamente la oportunidad de incorporarse al mismo
- Eliminación del anillo: una estación debe ser capaz por sí misma de retirarse del anillo.
- Iniciación del anillo: cuando se arranca la red o esta se recupera de un fallo de funcionamiento, debe suministrarse un mecanismo descentralizado que decida el orden de iniciación del anillo.
- Recuperación del testigo: son necesarios funciones de recuperación ante la pérdida del testigo.

ESPECIFICACIONES DEL NIVEL FISICO

La norma IEEE 802.4 define cuatro posibles alternativas de medio físico. Sus características principales se muestran en la tabla A-2. Dos de estas alternativas son conocidas como carrierband o sistemas de banda ancha de un único canal. Las principales características de estas redes son su transmisión bidireccional y la utilización de una topología en bus. Como método de modulación de la señal se emplea el método FSK (frequency-shift keying), a bajas frecuencias; lo que supone una ventaja, pues la atenuación es menor a frecuencias más bajas. Igualmente ofrece como ventajas la mayor simplicidad de sus componentes y un menor costo.

| Parámetro | Carrierband | Carrierband | | Banda Ancha | | | Fibra Óptica | | |
|--------------------------|-------------------------|----------------------|-----|-------------------------|--------|--------|--------------------------|----|----|
| | Fase Continua | Fase Coherente | | | | | | | |
| Velocidad (Mbps) | 1 | 5 | 10 | 1 | 5 | 10 | 5 | 10 | 20 |
| Ancho de banda | N.A | N.A | N.A | 1.5 Mhz | 12 Mhz | 12 Mhz | 270 nm | | |
| Modulación de frecuencia | Manchester FSK continuo | FSK Fase Continua | | Multinivel AM / FSK | | | On - off | | |
| Topología | Bus omnidireccional | Bus omnidireccional | | Bus direccional (árbol) | | | Estrella pasiva o activa | | |
| Medio | Cable coaxial (75 Ω) | Cable coaxial (75 Ω) | | Cable coaxial (75 Ω) | | | Fibra óptica | | |

Tabla A-2. de medios alternativos del nivel físico IEEE 802.4

PASO DE TESTIGO EN ANILLO

Una red de paso de testigo en anillo consiste en un conjunto de estaciones conectadas por un medio de transmisión. La información se transmite secuencialmente. BIT desde una estación activa a la siguiente. Cada estación activa regenera y repite cada BIT. Una estación en concreto introduce la información en el medio, donde la información circula pasando por las estaciones. La estación destino de la información copia los datos al mismo tiempo que los pasa a la red. Finalmente, la estación emisora retira la información del anillo. Una estación obtiene el derecho a transmitir su información cuando detecta un testigo o token en el medio. El testigo es una señal de control compuesta por una secuencia especial de bits que circulan por el anillo cuando todas las estaciones están inactivas. Cualquier estación, tras la detección del testigo, puede capturar este modificándolo y convirtiéndolo en el comienzo de una trama y añadiendo campos de control y estado, direccionamiento, información, secuencia de comprobación de una trama y secuencia de finalización de trama.

Tras la finalización de la transferencia de información y después de las operaciones de comprobación de errores, la estación emisora inicia un nuevo testigo, proporcionando así la oportunidad de obtener el acceso a la red a las demás estaciones del anillo. Un temporizador de posesión de testigo controla el período máximo que una estación ocupa el medio antes de pasar el testigo. Tal como se ve en la figura A-6

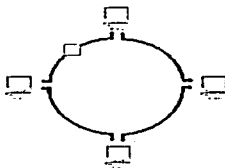


Figura A-6 Paso de Testigo en Anillo

Es posible definir múltiples niveles de prioridad con asignación independiente y dinámica en función de la clase de servicio requerida por un mensaje. La asignación de prioridades se realizará mediante acuerdo mutuo entre los usuarios de la red.

Es posible definir múltiples niveles de prioridad con asignación independiente y dinámica en función de la clase de servicio requerida por un mensaje. La asignación de prioridades se realizará mediante acuerdo mutuo entre los usuarios de la red.

Asimismo, se proporciona mecanismo de recuperación y detección de errores con la finalidad de asegurar el estado normal de funcionamiento en el caso de que los errores de transmisión o perturbaciones en el medio provoquen el incorrecto funcionamiento del método de acceso. La detección y recuperación de estos errores la realiza una determinada estación a través de una función de monitorización de la red. En el caso de que esta tuviera algún problema, las demás estaciones son capaces de sustituirla en el ejercicio de esta función de monitorización.

El correcto funcionamiento de una red en anillo se basa en tres funciones básicas: inserción de datos, recepción de datos y retirada de datos. Estas funciones son realizadas por unos dispositivos denominados repetidores. En el anillo, al tratarse de un bucle cerrado, las tramas circularán indefinidamente a no ser que sean retiradas. Las tramas pueden ser retiradas por el repetidor destino o por el emisor una vez hayan completado una vuelta en el anillo. Este último caso es más aconsejable, en primer lugar porque es posible un reconocimiento automático y en segundo lugar porque permite la transmisión *multicasting*: Un paquete es enviado simultáneamente a varias estaciones.

El protocolo de paso de testigo en anillo (*Token ring*) se basa en una pequeña trama que circula a lo largo del anillo. El testigo puede encontrarse libre u ocupado. Un bit de la trama indica su estado. Cuando todas las estaciones de la red están inactivas, es decir, sin datos para transmitir, el testigo se encuentra libre y simplemente circula por el anillo pasando de una estación a la siguiente. La estación que desea transmitir debe esperar a recibir el testigo libre, modifica el estado del testigo alterando el bit de estado, pasando de libre, modifica el estado del testigo alterando el bit de estado, pasando de libre a ocupado, e inserta, a continuación del testigo, la información a enviar junto con su propia dirección y la de la estación destino.

En este momento no existe testigo libre en el anillo y, por lo tanto, las demás estaciones que deseen transmitir deben esperar. El trama de datos prosigue su circulación por el anillo hasta llegar a la estación receptora, que copia su contenido y lo vuelve a poner en circulación. Cuando la trama vuelve a llegar a la estación emisora, ésta elimina la trama de datos de la red. La generación de un nuevo testigo libre es responsabilidad de la estación emisora. Pueden adoptarse dos estrategias:

- a) (1) Se genera un testigo libre cuando la estación ha finalizado la transmisión de su trama y (2) el testigo ocupado vuelve a la estación.
- b) Se genera un testigo libre inmediatamente después de que la estación finalice la transmisión de su trama. Esta estrategia se denomina testigo anticipado.

El procedimiento a) es el más simple. Sólo permite la existencia de una trama en el anillo en un momento del tiempo. En caso de que la longitud en bits del anillo sea menor que la longitud de la trama de datos, cuando el testigo ocupado retorna a la estación emisora ésta no ha finalizado todavía la transmisión de la trama; es decir, la condición (1) implica la (2)

A medida que se incrementa la velocidad es más probable que la longitud de la trama sea inferior a la longitud del anillo en bits. Por ello es más conveniente utilizar la estrategia b) para obtener mayor rendimiento. En este caso los mecanismos de recuperación de errores son más complejos, puesto que pueden existir varias tramas en el anillo.

ESTRUCTURA DE LA TRAMA MAC

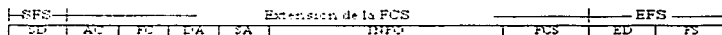
La figura A.7 muestra los formatos de testigo y trama definidos por el protocolo IEEE 802.5.

El formato completo de la trama consta de los siguientes campos:

- Delimitador de Comienzo – Starting Delimiter (SD): indica el comienzo del testigo o de la trama. Consiste en un patrón de señalización distinguible siempre de los datos. Se codifica de la siguiente manera: JK0JK000, donde J y K son símbolos que representan la ausencia de datos. Su implementación depende de la codificación de señales.

- Control de Acceso - Access Control (AC): contiene los bits de prioridad y reserva utilizados en el mecanismo de prioridad, y el bit de monitorización empleado en el mecanismo de mantenimiento (véase figura 10.3). Contiene también el bit de testigo que indica si trata de un testigo o de una trama. En el caso de ser un *token* o testigo sólo se acompaña de un campo más, el delimitador de final.
- Control de trama - Frame Control (FC): indica si la trama contiene datos LLC o es una trama de control MAC. En este último caso, los bits de control indican el tipo de trama MAC.
- Dirección de Destino - Destination Address (DA): especifica la estación o estaciones a la que va dirigida la trama. Puede ser una única dirección MAC (una estación), una dirección de grupo (un grupo de estaciones) o una dirección global (todas las estaciones del anillo). La elección entre una dirección de 16 bits o una de 48 bits es una decisión de implementación, debiendo ser igual para todas las estaciones de la red local.
- Dirección Origen - Source Address (SA): Especifica la dirección de la estación que envió la trama. Su tamaño debe ser igual al de la dirección destino.
- Información - Information (I): Contiene los datos en el caso de una trama de datos o un "vector" MAC si es una trama MAC.

A) Formato de trama



SFS = Secuencia de comienzo de trama

INFO = Información (0 o más octetos)

SD = Delimitador de comienzo (1 octeto)

FCS = Secuencia de comienzo de trama (4 octetos)

AC = Control de acceso (1 octeto)

EFS = Secuencia de fin de trama

FC = Control de trama (1 octeto)

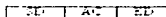
ED = Delimitador de fin (1 octeto)

DA = Dirección destino (2 ó 6 octetos)

FS = Estado de trama (1 octeto)

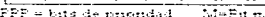
SA = Dirección origen (2 ó 6 octetos)

B) Formato de token



EL = Código de acceso (AC)

E) Código de trama



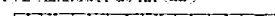
PPP = Bits de prioridad

M = Bit monitor

T = Bit de token

RRR = Bits de reserva

F) Delimitador de fin (ED)



J = no datos J

L = bit de trama intermedio

K = no datos K

E = bit de error detectado

L = uno binario

C) Delimitador de comienzo (SD)

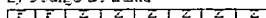


J = no datos J

U = Cero binario

K = no datos K

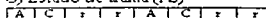
E) Código de trama



PP = Bits de tipo de trama

ZZZZZZ = Bits de control

G) Estado de trama (FS)



A = Bits de reconocimiento

C = Bits de copiados

r = Bits reservados

Figura A-7

GLOSARIO

93 A

TESIS CON
FALLA DE ORIGEN

-- oOo --

A

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

Ancho de banda. Margen de frecuencias capaz de transmitirse por una red de telecomunicaciones.

ANSI. *American National Standards Institute.* Instituto Nacional Americano para la Estandarización. Organismo oficial dedicado a fomentar la adopción de normativas en materia de informática, comunicaciones, etc.

AnyLan. Ethernet a 100 Mbps.

API. *Application Programmer Interface.* Interfaz de Programación de Aplicación. Lenguaje y formato de mensaje utilizados por un programa para activar e interactuar con las funciones de otro programa o de un equipo físico.

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

Árbol de decisión. Modelización de una decisión con una estructura jerárquica cuyos nodos son preguntas y los arcos valores posibles para estas preguntas.

ASCH. *American Standard Code for Information Interchange.* Código estándar americano para intercambio de la información. Esquema normalizado de codificación de caracteres introducido en 1963 y muy utilizado en muchas máquinas. Sistema de codificación de caracteres alfanuméricos en 7 bits para la operación interna del computador y su comunicación con los periféricos. Este sistema, promovido por el ANSI (*American National Standards Institute*), es ampliamente utilizado por ordenadores personales, estaciones de trabajo y miniordenadores.

Asíncrono. Transmisión no sincronizada en la que el sincronismo entre el emisor y el receptor se establece de nuevo en el terminal para cada carácter transmitido.

Asociación FTAM. Enlace lógico entre dos sistemas FTAM. Se realiza sobre un medio físico denominado conexión FTAM. Se pueden establecer múltiples asociaciones FTAM (incluso simultáneas) sobre una misma conexión FTAM.

Atenuación. Disminución del valor recibido de una señal con respecto a su valor original de emisión.

ATM. *Asynchronous Transfer Mode.* Modo de Transferencia Asíncrona. Técnica de conmutación por paquetes de alta velocidad adecuada para redes de área metropolitana (MAN). transmisión de banda ancha y redes digitales de servicios integrados (RDSI).

-- oOo --

B

Backbone. Red principal de una red de comunicaciones.

Banda ancha. Técnica de comunicaciones en la que las señales digitales se transmiten moduladas, pudiendo enviarse por un solo canal múltiples señales simultáneas. La UIT-T define también como banda ancha a las comunicaciones digitales a más de 2 Mbps..

Banda base. Técnica de comunicaciones en la que las señales digitales codificadas se transmiten en su forma original, es decir, sin modulación.

Base de datos. *Data base.* Conjunto de datos no redundantes, almacenados en un soporte informático, organizados de forma independiente de su utilización y accesibles simultáneamente por distintos usuarios y aplicaciones. La diferencia de una BD respecto a otro sistema de almacenamiento de datos es que estos se almacenan en la BD de forma que cumplen tres requisitos básicos: no-redundancia, independencia y concurrencia.

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

Router. Combinación de *bridge* y *router* (puente y encaminador).

Buffer. Segmento reservado de memoria que se usa para almacenar datos mientras se procesan. Conjunto de registros conectados en paralelo que actúan como memoria intermedia para almacenar datos temporalmente para compensar y adaptar diferencias de velocidad entre emisor y receptor.

Bus. Conjunto de líneas que transportan información binaria entre la UCP, la memoria principal y la unidad de entrada salida. Facilitan la transmisión de datos entre dispositivos situados en dos puntos terminales, pudiendo, únicamente, transmitir uno de ellos en un momento dado.

Bus de direcciones. Bus que transmite las direcciones de las celdas de memoria RAM para identificarlas y poder así grabar un Byte en ellas o recuperar el Byte que contienen.

Bus local. Tecnología que emplea ranuras de expansión en la placa base del ordenador que se conectan directamente al bus de la unidad central de proceso.

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

-- 000 --

C

Canal. Denominación general para una vía de transmisión lógica o física.

Cascada (avance en). Método de paso de una fase a la siguiente en las metodologías de desarrollo de sistemas, según el cual no se cambia de fase hasta que no esté completamente terminada la fase anterior.

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

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

Código. Cada una de las secuencias de caracteres que transforman los elementos de un repertorio en otro.

Código binario. Código en el que los elementos se representan solamente por los valores "1" y "0". Es el código empleado principalmente dentro de los circuitos de los equipos físicos.

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

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

-- oOo --

D

Decodificación. Conversión de un valor digital en una señal analógica. || Proceso de reconversión de un mensaje codificado al mensaje que dio lugar a la codificación.

DECnet. Red de comunicaciones de Digital, que soporta RAL de estilo Ethernet y WAN de banda base y de banda ancha en líneas públicas y privadas.

-- oOo --

E

Espiral (avance en). Método de paso de una fase a la siguiente en las metodologías de desarrollo de sistemas, según el cual se cambia de fase aunque no esté terminada la anterior, volviendo a la misma después de probar los resultados. Este proceso se repite varias veces.

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

ETD. Equipo Terminal de Datos. Lado de una interfaz que representa al usuario de los servicios de comunicación de datos en una norma como RS232C o X.25. Los ETD son generalmente, ordenadores o terminales de ordenador.

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

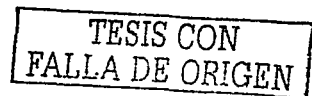
-- oOo --

F

FDDI. *Fiber Distributed Data Interface.* Especificación de una red de área local con topología en anillo, método de acceso por paso de testigo cuya estructura se implementa sobre un cable de fibra óptica. Esta norma fue desarrollada por el ANSI.

FDDI-II. *Fiber Distribute Data Interface II.* Especificación de una red de área metropolitana con posibilidad de ofrecer servicios isócronos de voz e imagen.

Fichero. Archivo que contiene un conjunto de registros de datos que se refieren a un mismo asunto.



Fichero Inverso. En bases de datos textuales, es un fichero especial de índices que permite la recuperación a velocidad elevada de términos que están situados dentro de campos de texto. Son ficheros en los que cada palabra presente en un campo de descripción forma un campo de un registro, existiendo un registro por cada palabra. El resto de los campos de este registro indican la posición en la base de datos del documento que posee esa palabra en su campo de descripción. Los tamaños de estos ficheros pueden llegar a ser del orden de 300 veces mayor que los de los ficheros de datos.

Fichero virtual. Modelo lógico que sirve para tratar todos los posibles tipos de ficheros de todos los posibles sistemas reales de igual forma. Está formado por un árbol de nodos, en donde puede haber en cada nodo (opcionalmente) datos que se corresponden con una parte del fichero real.

Frame. Encuadre, bloque, secuencia, trama.

Frame Relay. Sistema de transporte para la transmisión de datos (paquetes) a alta velocidad (hasta 45 Mbits/s) mediante celdas de longitud variable.

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

FTP. File Transfer Protocol. Protocolo para la Transferencia de Ficheros.

-- oOo --

G

Gateway. Puerta de acceso, pasarela. Unidad de interfuncionamiento. Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red RAL, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

-- oOo --

H

HDLC. High level Data Link Control. Protocolo de comunicaciones orientado al bit, normalizado por ISO.

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

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

-- oOo --

I

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

Interfaz. *Interface.* Punto (o puntos), donde se efectúa la comunicación entre dos sistemas, y método según el cual se realiza.

Interfaz API. Conjunto de definiciones de rutinas que permiten llamadas directas. Utilizadas por los programadores de un sistema para llamar a las funciones de otro, del cual tienen especificada su API.

Interfaz de usuario. Forma en que un sistema informático permite la comunicación bidireccional con el usuario.

Interfaz integrada. Tipo de interfaz que existe cuando un sistema y otro están unidos a través de programación, y el usuario final no tiene conciencia de qué sistema realiza la tarea deseada. Normalmente, se utiliza la API de un sistema para construir una interfaz integrada con otro.

Interfaz interactiva. *Interactive interface.* Tipo de interfaz en la cual los dos sistemas cooperan para efectuar la comunicación. Por ejemplo, la comunicación hombre máquina.

Interoperabilidad. Es la capacidad de interconectar sistemas de distintos fabricantes y hacerlos trabajar conjuntamente para satisfacer las necesidades del negocio. Algunos ejemplos son: intercambio de mensajes entre sistemas, compartición de recursos, como por ejemplo datos entre aplicaciones que se ejecutan en distintas plataformas *hardware* y *software*, etc.

IP. *Internet Protocol.* Protocolo Internet, Protocolo sin conexión (*connectionless*) encargado de controlar la información por la red. Permite la integración de otras subredes. Véase TCP/IP.

ISO. *International Organization for Standardization.* Organización Internacional de Normalización. Es el máximo organismo de normalización a nivel internacional con sede en Ginebra. Su *Technical Committee 97* (TC97) es responsable del modelo de referencia de siete capas definidos para sistemas de comunicaciones directas (Véase OSI). Edita propuestas de normas internacionales "*Draft International Standard (DIS)*". Juntamente con el IEC son los dos organismos competentes para emitir normas internacionales.

-- uOo --

J

Jerarquía. Red ordenada de conceptos u objetos en la cual unos están subordinados a otros.

-- oOo --

K

Kbps. Kilobits por segundo. Medida de velocidad de transmisión.

KiloByte. KB. Unidad de medida de memoria. Equivalencia: 1 KByte = 10^3 Bytes = 1.024 Bytes.

-- oOo --

L

LAN. Local Area Network. Red de área local. Véase RAL.

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

-- oOo --

M

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

Mainframe. Ordenador central con gran capacidad de proceso y de almacenamiento. Sistema de proceso orientado a transacciones de base de datos, capaz de dar servicio a cientos o miles de usuarios simultáneamente.

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

Mapa de memoria. Espacio de memoria direccionable por el ordenador.

MAU. Multistation Access Unit. Unidad de acceso multiestación. Concentrador de dispositivos en estrella para redes TokenRing.

Medio de transmisión. Medio físico que soporta la comunicación de datos.

TESIS CON
FALLA DE ORIGEN

Memoria. Zonas de un ordenador o periférico donde se almacenan temporalmente los datos y los programas con los cuales se trabaja en un determinado instante.

Microprocesador. Es la unidad central contenida en un circuito integrado que, juntamente con la memoria y dispositivos periféricos, componen un microordenador.

Miniordenador. Ordenador de gran potencia que se sitúa entre la categoría de las estaciones de trabajo y de los *mainframes*. En general, suelen estar basados en chips y sistemas operativos no abiertos, aunque UNIX está penetrando con fuerza en este mercado.

Módem/Fax. Módem que también permite enviar y recibir datos desde una máquina fax.

Módem. Modulador/demodulador. Equipo para la transmisión de datos que convierte señales analógicas en digitales y viceversa. Elemento físico que permite transmitir información entre dos ordenadores mediante una línea telefónica.

Modulación. Modificación de alguno de los parámetros de una onda portadora por una señal moduladora que se quiere transmitir.

Multiplexación. Procedimiento mediante el cual se reúnen o entrelazan varias señales en otra señal de orden superior con la que sea posible su transmisión.

Multiplexación por división de frecuencia. Procedimiento por el cual las frecuencias de las señales se trasponen a otro margen de frecuencias superior en el que sea posible su transmisión simultánea.

Multiplexación por división en el tiempo. Sistema de Multiplexación en el que una vía común es compartida por asignación de intervalos periódicos de tiempo.

Multiusuario. Capacidad del sistema operativo para trabajar con dos o más usuarios simultáneamente.

-- oOo --

N

Nivel. En un árbol de nodos de un fichero virtual es la distancia (medida en nodos) desde un nodo dado al nodo raíz, que es el de nivel cero.

-- oOo --

Ñ

TESIS CON
FALLA DE ORIGEN

-- oOo --

O

Octeto. Ver Byte.

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

-- oOo --

P

Pasarela. Véase *Gateway*.

Portadora. Frecuencia portadora. Señal con una determinada frecuencia utilizada en transmisión como soporte para transmitir información.

Procesador. Dispositivo compuesto por uno o varios microprocesadores, que procesa los datos conforme a un programa almacenado en memoria.

Protocolo. Conjunto formal de convenciones que gobiernan el formato y control de datos. Conjunto de procedimientos o reglas para establecer y controlar transmisiones desde un dispositivo o proceso fuente a un dispositivo o proceso objeto.

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

Protocolo Internet. Véase IP.

Protocolos de pruebas. Conjunto de valores de prueba, condiciones y normas para efectuar las pruebas de un programa.

Prototipo. Modelo operacional de prueba indicado para la evaluación de las especificaciones de un sistema de información, o para un mejor entendimiento de cómo los requerimientos son plasmados en la aplicación desarrollada.

-- oOo --

Q

-- oOo --

R

RDSI (ISDN). Red Digital de Servicios Integrados (*Integrated Services Digital Network*). Red que evoluciona a partir de la red telefónica; permite la conectividad digital de usuario a usuario, proporcionando servicios telefónicos y no-telefónicos.

Red semántica. Formalismo de representación del conocimiento en la que éste viene representado por nodos y las relaciones por arcos entre los nodos.

Repetidor. Equipos que amplifican, regeneran y sincronizan la señal en un segmento de una RAL para pasar a otro segmento de la misma RAL.

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

Ruido. En términos documentales, la obtención de información no requerida junto con la deseada al hacer una pregunta documental a un SGBDD.

-- oOo --

S

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

SENEAM. SERVICIOS A LA NAVEGACION EN EL ESPACIO AEREO MEXICANO. Es un órgano descentralizado dependiente de la SCT. Proporciona los servicios de navegación aérea tales como meteorología, servicio de despacho e información de vuelos y Control de Tráfico Aéreo; así como formular programas a corto, mediano y largo plazo para el desarrollo de servicios, construcción de instalaciones e inversiones diversas.

-- nOo --

T

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

Testigo. Trama especial que circula por la red y se transfiere desde una estación a la siguiente.

Tiempo de respuesta. Por regla general, tiempo transcurrido entre la acción realizada por el usuario de un sistema informático y la recepción de alguna clase de respuesta o realimentación del sistema. || Ante una avería, tiempo que transcurre desde la comunicación de la incidencia hasta el mantenedor se pone en disposición de resolverla.

Tiempo de acceso. Suma de los tiempos que tarda en posicionarse el brazo de la cabeza de lectura-escritura de un disco en la pista deseada (**tiempo de búsqueda**) más el tiempo que tarda la información de la pista en pasar delante de la cabeza de lectura-escritura (**tiempo de latencia**).

Tiempo de búsqueda. Tiempo que tarda en posicionarse el brazo de la cabeza de lectura-escritura de un disco en la pista deseada.

Token Bus. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en anillo. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.4 del IEEE y en la norma 8802.4 de la ISO.

Token Ring. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en bus. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.5 del IEEE y en la norma 8802.5 del ISO.

Trama. Bloque de datos formado por bits y limitado por indicadores.

TESIS CON
FALLA DE ORIGEN

-- 000 --

U

UNIX Internacional. Grupo liderado por AT&T y Sun Microsystems, que patrocinan el sistema operativo UNIX System V Release 4 (SVR4) como la versión estándar universal de UNIX.

UNIX. Sistema operativo multiproceso, multiprograma y multiusuario. *Software* diseñado por AT&T para ingeniería de telecomunicación. Ha sido el primer sistema operativo concebido con independencia de los fabricantes. Posee una gran facilidad para adaptarse a ordenadores con diferentes arquitecturas, siendo ampliamente autónomo respecto del *hardware*. Está escrito en lenguaje de alto nivel C.

-- 000 --

V

-- 000 --

X

X.25. Interfaz para la transmisión de datos en redes de conmutación de paquetes (PSDN, *Packed Switched Data Network*). Está definido por las 3 primeras capas del modelo OSI. Permite circuitos virtuales así como recuperación de datos y recuperación de errores. Son recomendaciones de la UIT-T para intercomunicaciones de paquetes. Véase Iberpac.

-- 000 --

Y

-- 000 --

Z

TESIS CON
FALLA DE ORIGEN

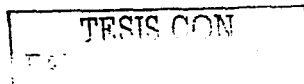
ACRÓNIMOS

105A

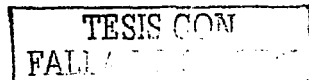
TESIS CON
FALLA DE CALIDAD

Lista de Acrónimos

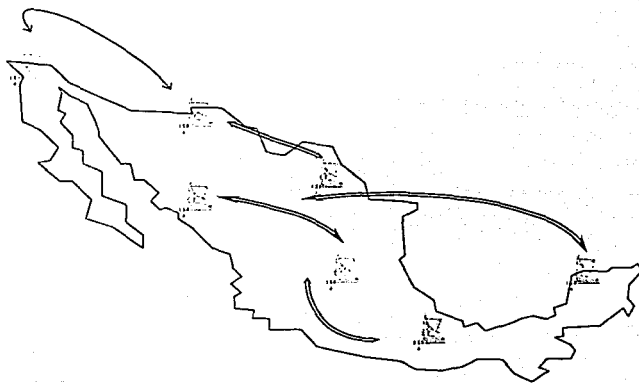
ABI.- Advanced Boundary Information message (OLDI)
 ACC.- Area Control Center
 ACT.- Activation (O.LDI message)
 ADEP.- Aerodrome of DEParture
 ADES.- Aerodrome of DESTination
 AEROVÍAS.- Vías aéreas o carreteras aéreas, por donde transitan los aviones.
 AFL.- Actual flight Level
 AFTN.- Aeronautical Fixed Telecommunication Network
 APP.- Approach
 ASC.- AFTN Switching Center
 ATC.- Air Traffic Control
 ATCC.- Air Traffic Control Center
 ATM.- Asynchronous Transfer Mode
 ATS.- Air Traffic Control
 BPN.- Boundary Point: eNtry point
 BPN.- Boundary Point: eNit point
 BUS.- Tipo de topología (arreglo) en redes Lan.
 DCE.- Data Communications Equipment
 CCIFF.- Comité consultativo internacional de telegrafía y telefonía
 CHL.- Channel Check message (AFTN)
 CPU.- Central Process Unit
 CPL.- Current flight plan
 CSMA/CD.- Carrier Sense Multiple Access with Collision Detection
 DEC.-Digital Equipment Corporation
 EST.- ESTimate a flight plan (function)
 ETA.- Estimate Time of Arrival
 ETB.- Estimate time of Boundary
 ETD.- Estimate Time of Departure
 ETN.- Estimate Time Next Point
 ETO.- Estimate Time of Overflight
 ETX.- Estimate Time of eNit point
 FDP.- Flight Data Processor
 FIR.- Flight Information Region
 FL.- Flight Level in hundred of feet
 FPL.- Flight Plan
 HOST.- Computador principal, o computadora en red
 HUB.- Concentrador de red LAN.
 IEEE.- Institute of Electrical and Electric Engineers
 IP.- Internet Protocol
 ISO.- International Standards for Organization
 LAM.- Logical Acknowledgement Message
 LAN.- Local Area Network
 Mbs.- Mega bits por segundo
 MONORADAR.- Un solo radar.
 MULTIRADAR.- Varios radares



NO-ACT-LAM.- No Active LAM.
NOTAM.- Notice To AirMen
OACI.- (ICAO).- International Civil Aviation Organization
OFFLINE.- Directorio principal que contiene la base de datos del host fdp.
OLDI.- On-Line Data Interchange.
OSI.- Open System Interconnection
PIRC.- Processor of interface for Radars and Communications
RAM.- Read Access Memory
RDP.- Radar Data Processor
RDSL.- Red Digital de Servicios Integrados
ROM.- Read Only Memory
ROUTER.- Enrutador
ROUTING.- Encaminamiento
RPL.- Repetitive Flight Plan
SCPC.- Simple Carrier per Channel
SECTORES.- Area virtual de trabajo en un centro de control.
STAND-BY.- En espera
TCP/IP.- Transmission Control Protocol / Internet Protocol.
TRACK.- Simbolo para designar una aeronave (etiqueta).
TMA.- Terminal Manoeuvring Area
TWR.- ToWeR
VISU.- Visual Unit.



IDENTIFICADORES DE LUGAR



TESIS CON
FALLA DE ORIGEN

| <u>IATA</u> | <u>OACI</u> | <u>LUGAR O ESTACION</u> |
|-------------|-------------|-------------------------|
| ACA | MMAA | ACAPULCO, GRO |
| | MMIAN | MONTERREY |
| | MMAS | AGUASCALIENTES |
| | MMCC | CD. ACUÑA INTL |
| CDM | MMDM | CD. MANTE TAMPS. |
| CEN | MIMCN | CD. OBREGON, SON. |
| CJS | MMCS | CD. JUAREZ, CHIH. |
| CME | MMCE | CD. DEL CARMEN, CAMP. |
| CNA | MMCA | CANANEA, SONORA |
| CPE | MMCP | CAMPECHE |
| | MMCY | CELAYA |
| CTM | MMCM | CHETUMAL, QR. |
| | MMICH | CHILPANCINGO |
| CUL | MMCL | CULIACAN, SIN. |
| CUN | MIMUN | CANCUN, QR. |
| CUU | MMCU | CHIHUAHUA |
| CVA | MMCB | CUERNAVACA, MOR. |
| | MMIA | COLIMA |
| CVM | MMCV | CD. VICTORIA, TAMPS |
| CZM | MMCZ | COZUMEL, QR. |
| | MMLO | GUANAJUATO |
| DGO | MMDO | DURANGO |
| GLD | MMGL | GUADALAJARA, JAL. |
| GYM | MMGM | GUAYMAS, SON. |
| HMO | MIMHO | HERMOSILLO, SON. |
| HUN | MMBT | HUATULCO, OAX. |
| IYO | MMHO | SALTILLO, COAH |
| | MIMM | ISLA MUJERES |
| IZT | MMIT | IXTEPEC, OAX |
| | MMJA | JALAPA |
| | MMLC | LAZARO CARDENAS |
| LAP | MMLP | LA PAZ B.C.S. |
| LEO | MMLO | LEON, GTO. |
| | MMLT | LORETO INTL |
| LMM | MMLM | LOS MOCHIS, SIN. |
| NAM | MMMA | MATAMOROS, TAMPS. |
| MEX | MMMX | MEXICO, D.F. |
| | MMEX | MEXICO (ACC/AOC/FIC) |
| MID | MMMD | MERIDA, YUC. |
| NOV | MMMV | MONCLOVA, COAH. |
| | MIMM | MORELIA |
| MIT | MIMT | MINATITLAN, VER. |

**TESIS CON
FALLA DE ORIGEN**

IDENTIFICADORES DE LUGAR

| | | |
|-----|------|-------------------------|
| MTY | MMMY | MONTERREY, N.L. |
| MXL | MMML | MEXICALI, B.C.N. |
| MZI | MMMZ | MAZATLAN, SIN (MMZT) |
| NAU | MMNU | NAUTLA, VER. |
| NCG | MMCG | N. CASAS GRANDE, CHIH. |
| NLD | MMNL | NUEVO LAREDO, TAMPS |
| NOG | MMNG | NOGALES, SON. |
| OAX | MMOX | OAXACA, OAX. |
| | MMPC | PACIUCA |
| PAZ | MMPA | POZA RICA, VER. |
| PBC | MMPB | PUEBLA |
| PNG | MMPG | PIEDRAS NEGRAS, COAH. |
| PPE | MMPE | PUERTO PEÑASCO, SON. |
| PVR | MMPR | PUERTO VALLARTA, JAL. |
| PXM | MMPS | PUERTO ESCONDIDO, OAX. |
| QET | MMQT | QUERETARO |
| REX | MMRX | REYNOSA, TAMPS. |
| | MMIO | SALTILLO |
| SLP | MMSP | SAN LUIS POTOSI, S.L.P. |
| | MMSF | SAN FELIPE |
| | MMSD | SAN JOSE DEL CABO INTL |
| | MMSM | SANTA LUCIA |
| TAM | MMTM | TAMPICO, TAMPS. |
| TAP | MMTP | TAPACHULA, CHIS. |
| TEQ | MMTQ | TEQUESQUITENGO, MOR. |
| | MMEP | TEPIC |
| | MMHC | TEHUACAN, PUE. |
| TGZ | MMTG | TUNTLA GUTIERREZ, CHIS. |
| TJ | MMTJ | TIJUANA, B.C.N. |
| TLC | MMTO | TOLUCA, EDO. MEX. |
| TMN | MMTN | TANUIN, S.L.P. |
| TRC | MMTC | TORREON, COAH. |
| TCG | MMTL | TULANCINGO, HGO. |
| TUX | MMTX | TUXPAN, VER. |
| | MMPN | URUAPAN |
| VER | MMVR | VERACRUZ, VER. |
| VSA | MMVA | VILLAHERMOSA, TAB. |
| | MMZC | ZACATECAS |
| | MMZM | ZAMORA |
| | MMZO | MANZANILLO |
| | MMZP | ZAPOPAN (MIL) |
| ZIH | MMZH | ZIHUATANEJO, GRO |

TESIS CON
 FALLA DE ORIGEN

BIBLIOGRAFÍA

TESIS CON
FALLA DE ORIGEN

- Black Ugless, GUJA PRACTICA DE COMUNICACIONES Y REDES LOCALES, Editorial Ci.
- Halsall, Fred, COMUNICACIÓN DE DATOS DE REDES DE COMPUTADORAS Y SISTEMAS ABIERTS, Pearson educación
- Jeinkins, Neil, REDES DE AREA LOCAL, México- Nueva Cork, Prentice-Hall
- Stalling, William, COMUNICACIONES Y REDES DE COMPUTADORAS, Prentice Hall
- Stoltz, Kevin, TDO ACERCA DE LAS REDES DE COMPUTADORAS, México Prentice-Hall
- Thomas, Madron, REDES DE AREA LOCAL, Editorial Mega Byte Noriega Editores S.A.
- Matt Gayden APRENDIENDO REDES AREA DE COMUNICACIONES, Prentice may
- Merilee Ford H. Kim Lew TECNOLOGIA DE INTERCONECTIVIDAD DE REDES CISCO SYSTEMS 2000, Tem Strevenson
- MANUAL DE NIVELACION REDES DE DATOS TELECOMUNICACIONES, Teleor S.A de C.V
- MANUAL TECNICO- OPERATIVO DE LA RED SENEAM, Secretaria de Telecomunicaciones
- INSTITUTO TECNOLÓGICO DE COMUNICACIONES DE MEXICO, ALCATEL.
- Mlieha Schwartz, REDES DE TELECOMUNICACIONES PROTOCOLOS MODELO Y ANALISIS, Departamento de Ingeniería Eléctrica y Centro de Investigación
- ThomsonCSF AIRSYS, RADAR CONTROLER POSITION, Francia, Thomson
- MANUAL DE CAPACITACION DEL CENTRO DE CONTROL MEXICO, SENEAM

TESIS CON
FALLA DE ORIGEN