

EVALUACION DEL PERSONAL DOCENTE

CURSO: REDES LAN DE MICROS PARTE II
FECHA: DEL 17 AL 26 DE MARZO DE 1994.

CONFERENCISTA	DOMINIO DEL TEMA	USO DE AYUDAS AUDIOVISUALES	COMUNICACION CON EL ASISTENTE	PUNTUALIDAD
ING. JUAN F. MAGAÑA CARRILLO (COORD)				
ING. SAUL MAGAÑA CISNEROS				
APOYO ACADEMICO				

EVALUACION DE LA ENSEÑANZA

1.- ORGANIZACION Y DESARROLLO DEL CURSO:

2.- GRADO DE PROFUNDIDAD LOGRADO EN EL CURSO:

3.- ACTUALIZACION DEL CURSO:

4.- APLICACION PRACTICA DEL CURSO:

EVALUACION DEL CURSO

CONCEPTO	CALIF.
CUMPLIMIENTO DE LOS OBJETIVOS DEL CURSO	
CONTINUIDAD EN LOS TEMAS	
CALIDAD DEL MATERIAL DIDACTICO UTILIZADO	
<input style="width: 50px; height: 20px;" type="text"/>	

ESCALA DE EVALUACION: 1 A 10

1.- ¿LE AGRADO SU ESTANCIA EN LA DIVISION DE EDUCACION CONTINUA?

SI	NO
----	----

SI INDICA QUE NO DIGA PORQUE.

2.- MEDIO A TRAVES DEL CUAL SE ENTERO DEL CURSO:

PERIODICO EXCELSIOR		FOLLETO ANUAL		GACETA UNAM		OTRO MEDIO	
PERIODICO EL UNIVERSAL		FOLLETO DEL CURSO		REVISTAS TECNICAS			

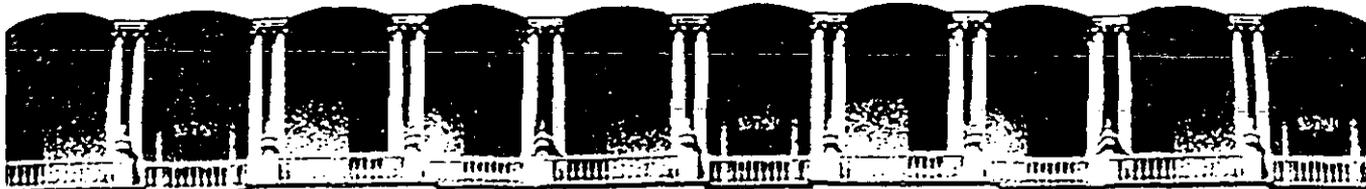
3.- ¿QUE CAMBIOS SUGERIRIA AL CURSO PARA MEJORARLO?

4.- ¿RECOMENDARIA EL CURSO A OTRA(S) PERSONA(S)?

SI		NO	
----	--	----	--

5.- ¿QUE CURSOS LE SERVIRIA QUE PROGRAMARA LA DIVISION DE EDUCACION CONTINUA.

6.- OTRAS SUGERENCIAS:



**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

**CURSO: REDES LAN DE MICROS PARTE II
MODULO II DEL DIPLOMADO DE REDES LOCALES**

**4.-) SOFTWARE Y APLICACIONES
VERTICALES**

EL ESTANDAR SQL

El significado de las siglas SQL es: Structured Query Languaje, o Lenguaje Estructurado para Consulta.

Un programa servidor de base de datos, es un motor que realiza matemáticas relacionales en grupos de datos. En un programa servidor de base de datos no es necesario que se le diga cómo encontrar los datos que se requieren, sino que solamente se pide la información, el único inconveniente es que se necesita usar el SQL del servidor. Muchos servidores soportan el ANSI SQL de nivel uno.

Cada programa servidor de SQL se equipa con un manejador de transacciones que asegura que las tablas y los índices sean sincrónicos, aún después de una falla en el sistema o en el programa.

El problema es que cuando un programa termina de manera abrupta, una transacción particular puede no haberse actualizado, o bien los datos dentro del buffer pueden perderse.

El manejador de transacciones detectará esta condición y automáticamente removerá todas las actualizaciones parciales, de esta manera las tablas e índices, sólo reflejarán transacciones terminadas normalmente.

Los servidores de SQL también protegen a los datos contra la pérdida de los mismos después de una falla en el medio de archivo. Tienen también utilerías para backup y restauración que crean y restauran copias de la base de datos. Al comprarlos vienen equipados con utilerías para recuperar datos a futuro, con procedimientos que recuperan todos los cambios que se completan entre el último backup y el punto en el que falle el medio de almacenamiento, comunmente un disco.

Todos los programas servidores SQL soportan una completa integridad por medio de la combinación de un único índice y el atributo de la columna no nula.

Otro tipo de integridad es la integridad referencial, para describirla correctamente haremos uso de un ejemplo:

Si se tienen dos tablas, digamos una de clientes y otra de facturas, uno se debe asegurar de que las facturas nuevas que sean creadas no sean agregadas a la base de datos a menos que el cliente al que se le está facturando exista en la tabla de clientes.

De otra forma, las tablas perderían integridad, ésta es la misma que se desea tener al borrar o actualizar datos sobre los clientes.

Algunos programas servidores de SQL no tienen integridad referencial, depende del usuario el cómo va a manejar el problema, lo que inevitablemente conducirá a tablas que no están sincronizadas del todo.



Servidores como SQL Server and Ingres soportan sistemas de seguridad referencial parecidos a los de los Data Base Management System. Estos servicios consisten en que las reglas de seguridad referencial deben ser colocadas dentro de la serie de reglas del DBMS de manera que son ejecutadas automáticamente para hacer más fácil la labor del programador, que al usar este servicio puede despreocuparse de la integridad referencial.

Todos los servidores de SQL excepto Progress, tienen programación de aplicaciones que soportan varios lenguajes de programación como C, pascal, y COBOL por ejemplo. Esto resulta muy útil ya que, si conocemos nuestra aplicación y conocemos además un lenguaje de programación, podemos realizar aplicaciones a nuestra medida.

Casi todos los servidores soportan índices por medio de árboles binarios de búsqueda, para la rápida dirección y secuenciamiento.

Los servidores incluyen página automática o seguros de grabación para maximizar la concurrencia cuando muchos usuarios están accedendo la base de datos.

También cuentan con detección de problemas que ocurren cuando dos o más transacciones están siendo detenidas por otras transacciones. Ya que ninguna de las transacciones puede continuar, el servidor de SQL debe abortar por lo menos a una transacción y mandar un mensaje al programa para poner de nuevo en espera a la transacción que se abortó.

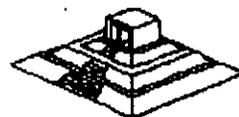
Existe una serie de características que bien vale la pena nombrar, ya que son de utilidad para escoger un servidor de SQL adecuado, éstas son:

- 1.- El precio relativo que tiene con respecto a otros servidores SQL .
- 2.- El sistema operativo para el que se creó (UNIX, DOS, VAX, etc.).
- 3.- El hecho de si soporta o no un 4GL.
- 4.- Qué lenguajes soporta para desarrollo de aplicaciones específicas, así como el nivel de bloqueo.
- 5.- La optimización que tenga en cuanto a la búsqueda de datos, las opciones que tenga en cuanto al almacenamiento de información y del almacenamiento de índices.
- 6.- La seguridad referencial o integridad referencial que pueda tener.
- 7.- El hecho de si tiene o no funciones definidas por el usuario, etc.

Existen múltiples servidores de SQL, a continuación se mencionarán algunos paquetes comerciales y sus características.

X D B

Es uno de los dos servidores SQL que pueden correr en MS-DOS, funcionará en cualquier NETbios LAN y requiere 640 Kb de memoria solamente. Se puede usar una versión especial para correr en memoria extendida.



Dependiendo de la aplicación particular que se desee implementar, XDB puede manejar hasta 15 usuarios. Este sistema tiene la ventaja de ser altamente compatible con el mainframe DB2 de IBM. La mayor parte de los DBMS del mercado tratan de copiar la sintaxis de DB2 SQL.

XDB en una sola máquina es lo mismo que correrlo en un servidor. Es muy fácil de instalar, además de tener una interface que nos es muy familiar.

Algunos de los otros sistemas se han derivado de Unix o de sistemas con VAX, que cuentan con una interface más apropiada para ese tipo de sistemas, el inconveniente de estos sistemas es que conllevan un exceso de bagaje ya que fueron creados para sistemas multiusuario mucho antes de la introducción de las PC's.

SQL BASE

Este es el otro sistema para MS-DOS. Fue el primer SQL server para PC. Inicialmente, podía correr en MS-DOS pero ahora además puede correr bajo OS/2. Está garantizado para correr en cualquier NETbios LAN y también como un DBMS bajo DOS.

La instalación y administración de los procedimientos de SQL base se diseñaron con el usuario de la PC en mente, los procesos de backup y recuperación son un buen ejemplo de lo anterior. Sólo se necesita un comando para hacer un backup en línea de la base de datos.

La compañía que produce este servidor SQL también tiene una aplicación para Windows llamada SQLWindows, que es una herramienta para desarrollo de aplicaciones sofisticadas en ambiente Windows.

SQL SERVER

Este sistema es de Microsoft, se conoce como Sybase, y puede correr en diferentes ambientes como Unix, OS/2 y VAX.

Tiene una capacidad limitada para actualizar a otras bases de datos lejanas, viene con funciones para coordinar las actualizaciones en múltiples bases de datos, pero es responsabilidad del programador hacer la correcta secuencia de llamadas a funciones.

Soporta la integridad referencial por medio de *gatillos* que son pequeños programas de SQL que son guardados en la tabla de comandos del DBMS.

Cada gatillo se relaciona con una tabla en particular y con una función particular para las actualizaciones, de esta forma se ejecutan de forma automática cada vez que se actualiza una base de datos.



ORACLE

Es la compañía líder en los DBMS para Unix. Tiene la gran ventaja de ser totalmente portátil entre diferentes plataformas siempre y cuando se tenga la misma versión de Oracle en todas las plataformas.

También tiene soporte para Gateways que no sean Oracle, como DB2, pero en la práctica estos Gateways tienen problemas de estabilidad y comportamiento, por lo que no se consideran muy confiables.

Oracle usa un sistema por usuario de arquitectura, cada usuario al conectarse demanda su propio proceso de servicio del servidor, la ventaja de lo anterior es que puede hacer uso de multiprocesadores, pero el problema es que consume mucha memoria y recarga mucho el trabajo en el CPU (en caso de existir sólo uno), lo que es importante considerar si se va a trabajar en una sola computadora basada en un procesador 80386, por ejemplo.

INGRES

Ingres compete con Oracle, corre en un buen número de plataformas para UNIX y VAX. Los Gateways para Ingres no han demostrado ser confiables, pero GCA parece resolver este problema. GCA es la primera arquitectura de Gateway basada en el estándar ANSI para acceso a datos remotos.

Ingres es el único DBMS que soporta arquitecturas con varios servidores, la ventaja es que los administradores pueden dirigir ciertas transacciones hacia servidores específicos, dando prioridad más alta a ciertas transacciones.

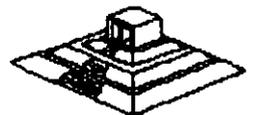
Ingres ha demostrado tener ciertas características que la hacen superior a sus competidores, por ejemplo: Ingres no sólo guarda cuentas sino también histogramas que describen mejor los datos, además es mejor para interpretar los comandos de SQL, soporta árboles de búsqueda binaria, que le da al administrador la flexibilidad para archivar físicamente los datos.

INFORMIX

Se ha encontrado que Informix es muy popular para aplicaciones pequeñas y medianas basadas en Unix. Es más fácil de administrar que otros sistemas basados en Unix, requiere además menor cantidad de hardware y tiene un comportamiento excelente.

Informix cuenta con excelente portabilidad, soporta más de 250 plataformas, tiene excelentes herramientas para desarrollo.

Podemos encontrar dos versiones de Informix, Informix-SE que es el software original de Informix para el DBMS y corre sobre su C-ISAM que es un manejador de archivos. La otra versión de Informix es Informix-OnLine, llamado también Informix Turbo, no puede correr en todas las plataformas en las que corre la otra versión y no se ha portado a VAX/VMS o DOS.



Informix usa una arquitectura de multiproceso, así cada usuario requiere su propia memoria pero puede compartirla con otros usuarios, lo que suena similar a la arquitectura de Oracle, la ventaja de esto es que se puede utilizar una computadora con capacidad de multiproceso por medio de varios procesadores, con las mismas desventajas que en su momento se describieron en Oracle.

NETWARE SQL

Es el único DBMS que corre como una adición a Novell, lo que significa que no necesita un servidor especial.

Cuenta con capacidades distribuidas limitadas, puede leer registros de un servidor remoto, uno a la vez, usando procesos de llamada remotos. El manejador de transacciones de este sistema no es tan sofisticado como los de otros sistemas.

PROGRESS

Progress ha probado ser el sistema preferido para pequeñas compañías, sus capacidades de DBMS son muy completas y tiene un 4GL para el desarrollo de aplicaciones. Es altamente portátil a través de docenas de plataformas de Unix y VAX, también se puede conseguir una versión para un solo usuario bajo MS-DOS.

Progress fue uno de los primeros DBMS verdaderamente relacionales en soportar SQL. No cuenta con un lenguaje procedural pero tiene interconstruido un soporte a SQL en su propio 4GL.

La parte más importante de Progress es su 4GL, ya que no soporta otros lenguajes, se deberán desarrollar todas las aplicaciones por este medio.

MANEJADORES DE BASE DE DATOS

Podría esperarse que todos los manejadores de base de datos fueran iguales pero lo anterior, desgraciadamente no es cierto.

Cada DBMS¹⁵ tiene características específicas y diferentes a las de los demás, lo que lo hace apropiado o no, para una cierta aplicación.

Además, pareciera que cada vendedor tiene la necesidad de agregar más y más características a la lista de cada DBMS, muchas de las cuales no son ni siquiera importantes o derivan en alguna verdadera utilidad. Es por esto, que cuando se desee comprar un DBMS es necesario verificar que contenga las características que se requieran para la aplicación en particular.

En un DBMS es necesario que se le diga cómo encontrar los datos que se requieren, no basta con que se le pida la información.

¹⁵ Data Base Management System



Algunos vendedores de DBMS han añadido algunas extensiones muy útiles a su SQL, como funciones sobre listas, matemáticas, estadística, etc; además de añadir tipos especiales de datos.

Una forma de manejar la integridad referencial es guardando las reglas en el catálogo del DBMS, ya que es el cuerpo de comandos y funciones para ese DBMS. Así, cada vez que una tabla se actualiza, las reglas de integridad referencial se ejecutan automáticamente. De esta manera los programadores no tienen que preocuparse por problemas con respecto a la integridad referencial.

Las reglas de integridad se centralizan de manera que sean consistentes en todas las aplicaciones y son más fáciles de mantener.

Una solución respecto de la integridad referencial es aquella en la que el vendedor del DBMS desarrolla todos los sistemas de seguridad referencial y los entrega a la tabla de comandos de alteraciones de SQL.

Así, el administrador de la base de datos no tiene que crear ninguna lógica para mantener asegurada la integridad referencial de la base de datos, ya que el "motor" del DBMS automáticamente se preocupa por mantener dicha integridad.

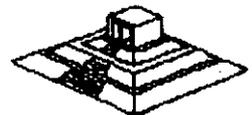
CORREO ELECTRONICO

La meta respecto del correo electrónico es uniformar las distintas plataformas de correo electrónico por medio de estándares, de manera que los usuarios puedan tener comunicaciones con cualquier sistema de correo electrónico.

El estandar que puede hacer esto último realidad es de CCITT con número X.400 que es una serie de protocolos para correo electrónico, y consta de ocho partes, todas ellas relacionadas con el manejo de mensajes:

- X.400** Referente al modelo del sistema y los elementos para dar servicio.
- X.401** Referente a los elementos básicos del servicio y opciones para el usuario.
- X.408** Referente a la información codificada y las reglas del tipo de conversión.
- X.409** Referente a la presentación, la sintaxis y la notación.
- X.410** Referente a las operaciones remotas y la confiabilidad de la transferencia de archivos.
- X.411** Referente a la capa de transferencia.
- X.420** Referente a la capa administradora de la mensajería interpersonal.
- X.430** Referente al protocolo de acceso para terminales habilitadas de telex.

Los sistemas de correo por computadora permiten dejar la computadora desatendida y dedicada a las comunicaciones, el correo electrónico se puede usar para recibir y mandar mensajes, reportes y archivos.



Una computadora se puede usar en una oficina como un sistema interno de memorándum para reducir la frecuencia de juntas cara-a-cara, para acordar asuntos, para anunciar noticias, para organizar las actividades entre personas con diferentes horarios, etc.

El incremento de la productividad generado por el uso de un sistema de este tipo, fácilmente justifica el costo del mismo y la dedicación de líneas telefónicas. Y de hecho los costos de comunicación fuera del área, también podrían reducirse drásticamente, adquiriendo un servicio con alguna compañía comercial dedicada al servicio de comunicación pública.

La mayor ventaja de los sistemas de correo electrónico desatendido es el control que le proporciona al operador local. Un sistema de correo electrónico, EMAIL, en una computadora puede proporcionar todas las capacidades de un sistema similar comercial, además de proporcionar control sobre la entrega y los tiempos de entrega de la información. Se puede decidir cuándo entregar ciertos mensajes y/o archivos, y el sistema automáticamente llamará a otros sistemas para entregar la información especificada en el tiempo especificado.

Los sistemas de correo electrónico nos dan ciertas facilidades como son: mantenimiento de direcciones, direcciones grupales, mandar a un buzón específico, mandar a un número telefónico, pedir respuesta a mensajes, buscar entre mensajes, imprimir mensajes y una gran variedad de utilerías más.

El mayor beneficio del correo electrónico, va más allá de un intercambio de información entre empleados, el envío de mensajes es la fundación de una nueva ola de software para grupos de trabajo que cambiará las estructuras hasta ahora conocidas, del trabajo grupal y que seguramente incrementará la productividad.

La gente tiende a pensar que el correo electrónico es solamente un intercambio de mensajes entre diferentes personas, pero eso es solamente la punta del iceberg que estamos descubriendo. El correo electrónico se puede usar también para la comunicación efectiva entre diversas personas y procesos, conocidos como usuarios virtuales.

Aplicaciones que se construirán sobre la estructura de mensajes incluye correo multimedia, direccionamiento de mensajes de fax, organización de horarios y compartición de documentos. Quizá la ruta donde se tienen mayores expectativas es la conocida como trabajo fluido que engloba la dirección de información, la automatización de diversas tareas, y el soporte de decisiones.

Expertos en correo electrónico para redes LAN, esperan que este sistema crezca durante los próximos años. Se estima que el número de usuarios de correo electrónico durante el último año creció un 60 % y se espera que siga creciendo, pero está limitado por la penetración en el mercado de las redes LAN.

Los tipos de aplicaciones que se basan en correo electrónico se pueden englobar en dos grupos:

Programas que pueden soportar el correo electrónico y programas centrados en correo electrónico, su transporte y envío.

La categoría central en las aplicaciones de mensajería es la organización de horarios de grupo, juntas y planeación de tiempos en las empresas, lo anterior también permite la adecuada administración de recursos de la empresa, como los salones disponibles para juntas o los auditorios, etc.



El correo electrónico se encuentra en un nivel de madurez en muchas empresas debido a su gran aceptación, además de las mejoras que se han introducido en el hardware y software para dichas aplicaciones, incluyendo la capacidad de comunicar dos sistemas de correo electrónico diferentes.

EL SUPERVISOR, DIAGNOSTICOS Y UTILERIAS

Las redes de área local deben ser administradas. Una red óptima es aquella que no inhibe el uso de recursos de la red, sin importar cuáles son estos recursos.

Quizá el problema más ignorado en la implantación de una red, es que toda red necesita ser administrada. Este es el trabajo del supervisor de la red.

El supervisor es la persona del departamento local, encargada de administrar adecuadamente la red. Con una red chica es posible que sólo se requiera el 10 ó 15 % del tiempo de esta persona, en una red de mayor tamaño es posible llegar a necesitar el 100 % del tiempo de esa persona. Un supervisor de una red óptima organizará las funciones del sistema, de manera que la gente ni siquiera sepa para qué está ahí.

Richard B. Freeman de IBM ha presentado un enfoque del manejo de una red, identificó seis disciplinas diferentes asociadas con el manejo de los componentes de una red:

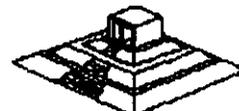
1. Determinación del problema
2. Análisis del desempeño
3. Manejo del problema
4. Manejo de cambios
5. Manejo de la configuración
6. Manejo de las operaciones

La Determinación del Problema se debe distinguir del mantenimiento y del servicio, ya que es el proceso de identificación de fallas de modo que se pueda llamar al distribuidor y organizaciones de servicio indicados.

La determinación del problema debe identificar qué elemento falló, no necesariamente por qué sucedió.

El reporte, registro y resolución de impedimentos de la posibilidad del usuario de comunicarse de manera efectiva con un dispositivo destino recibe el nombre de Manejo de Problemas.

Los cambios en los componentes de la red deben ser registrados, reportados y aprobados a través del proceso del manejo de cambios. El Manejo de la Configuración requiere la creación de una base de datos que contenga el inventario de las características físicas y lógicas pasadas, presentes y futuras de elementos de la red.



La base de datos de la configuración incluirá información sobre terminales y puertos, y la configuración exacta de cada dispositivo de acceso de la red.

Por último, el Manejo de las Operaciones tiene que ver con la manipulación distante o remota de diversos dispositivos de la red. Esto incluirá, pero no está limitado a, respaldo para el enlace de nuevos dispositivos, suministro de documentación acerca de cómo realizar ciertas funciones de la red y aspectos relacionados.

El aspecto principal que debe destacarse es que el manejo o administración de una red es un problema de manejo real, no tan solo un aspecto de garantizar que un cable sea tendido de un punto a otro y que se suelden conectores adecuados al mismo. A la lista de Freeman deben agregarse el respaldo de usuarios, capacitación y documentación, seguridad y planificación.

Judith Estrin y Keith Cheney de Bridge Communications han sugerido otro intento diferente para describir el manejo de una red:

1. Instalación y configuración
2. Monitoreo y control
3. Seguridad y control de acceso
4. Diagnóstico

Una red se instala para ofrecer servicios útiles a sus usuarios, una LAN departamental suele ser adquirida e instalada para realizar una o más funciones específicas, como:

Conectividad, acceso a dispositivos periféricos costosos, un sistema de base de datos común, acceso a software común, servicios de correo electrónico, calendario y agenda, vías de acceso, puentes de enlace y servidores de comunicaciones.

A fin de resolver adecuadamente los problemas de los usuarios, el supervisor de la red debe tener a su disposición cuando menos los siguientes manuales y documentos de apoyo:

Mensajes y códigos de todos los sistemas operativos de la red, así como también de todas las máquinas, mensajes y códigos de las aplicaciones importantes, guías para el operador relacionadas con todo el equipo a disposición del usuario, lo que incluye manuales de terminales, dispositivos de la red, métodos de acceso, guías de determinación de problemas de todo el equipo relacionado a la red, datos sobre la configuración de la red a fin de determinar si el usuario ha cambiado de alguna forma parámetros referentes a equipo de acceso a la red, esto implica que la interface del usuario tendrá también el equipo disponible para verificar la configuración actual o presente.

El objetivo fundamental de tener toda la documentación es mantener funcionando siempre la red. El mantenimiento de la red consiste en reparar interrupciones cuando éstas se presentan y lo que es más importante, evitar que ocurran interrupciones.



Para evitar interrupciones en el servicio, el mantenimiento contempla tareas como la actualización del software del sistema operativo de la red, prueba de cables y componentes activos del sistema de cableado, tarjetas de interface para la red y monitoreo de la carga del trabajo, rendimiento y tiempo de respuesta.

Cuando falle la red, será necesario que se recurra a todas las herramientas de diagnóstico que se puedan encontrar. Existen varios elementos evidentes que deben verificarse cuando ocurre una falla.

Primero lea las partes relevantes de todos los manuales y asegúrese de entender los mensajes de error. Después verifique el cable de empalme, después el cable troncal y por último el servidor. Si no tiene éxito tras el primer intento, pruebe con una búsqueda binaria, dividiendo a la red a la mitad y probando la operación de cada una de las mitades, después concéntrese en la mitad que no haya funcionado.

Aunque existe una escasez de hardware y software de diagnóstico, existen dispositivos que empiezan a salir al mercado que pueden ayudar al administrador de la red. Algunos de ellos son relativamente sencillos y están diseñados para probar continuidad o la existencia de cortos en el cable. Algunos de éstos son dispositivos automáticos, mientras que otros son tarjetas que se colocan en computadoras personales y cuando se combinan con el software adecuado, pueden ofrecer información concerniente a índices de colisión en una red Ethernet o bien, inspección de cuadros en una red Token Ring.

Un paso más allá de la simple prueba de continuidad es la creación de dispositivos algunas veces llamados reflectómetros de dominio de tiempo que no sólo indican en dónde hay una interrupción en el cable, sino que también señalan aproximadamente dónde ha ocurrido dicha interrupción.

Claro que este nivel de complejidad técnica tiene un precio alto, lo que dificulta justificar el costo de una red chica, sin embargo en una red de mayor tamaño, dicho costo no sería prohibitivo.

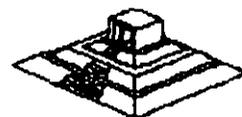
En el caso de redes de banda ancha se dispone de varios dispositivos, ya que la tecnología ha sido empleada por varios años, por ejemplo existen monitores que pueden probar en forma automática la calidad de las señales desde diversos puntos de la red.

Hay también analizadores de protocolo relacionados con monitores que pueden hacer un análisis detallado del comportamiento de un protocolo dentro de otros protocolos.

Aunque la red de área local debe ser diseñada con la posibilidad de expansión presente, el índice de expansión dependerá del capital disponible y de la disponibilidad de personal y productos.

La demanda del usuario de servicios de la red en una organización dinámica probablemente superará cualquier expansión planificada. La necesidad de expansión, modificación o reconfiguración dependerá del tráfico en la red, del rendimiento de la misma y de la disponibilidad del sistema en sitios organizacionales adecuados.

En un sentido estrecho, la planificación de la red consiste en la anticipación del cambio y la expansión a través del uso de modelos basados en datos referentes a desempeño. La función de planificación debe hacerse una parte intrínseca del manejo de una red, debido principalmente a que pocas personas desean llevarla a cabo.



El planificador debe servirse de todas las herramientas a su disposición y de datos concretos o reales como estadísticas de uso de terminales de sistemas de computación, nodos y transacciones totales, para representar la red a través de modelos y adquirir sentido de lo que está sucediendo.

Para que los programas de planificación sean tomados con seriedad es necesario tener una planificación orientada a metas, y también planificación de la implantación. Algunas veces puede ser necesaria la alteración de planes en el momento, pero la planificación por sí sola, con poco esfuerzo en la implantación de esos planes, es un ejercicio inútil, poco placentero y muy costoso en ineficacia.

Uno de los objetivos principales de las redes de computadoras, y en especial de las redes de área local, consiste en ofrecer acceso sencillo y conveniente a sistemas de computación dentro de una organización, y ese uso muy sencillo puede entrar en conflicto algunas veces con necesidades de seguridad.

En consecuencia el sistema de seguridad de la red debe tomar medidas para identificar a usuarios legítimos con fines autorizados al mismo tiempo de negar el acceso o uso no autorizados de datos importantes.

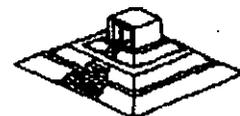
Se puede concebir un sistema de seguridad como una serie de círculos concéntricos que forman estratos de protección en torno a datos y recursos de computación. Los anillos exteriores representan la más baja seguridad y los interiores, la más alta seguridad.

Como uno de los objetivos primarios de una red es la conectividad, la óptima implantación de un sistema altamente conectivo tiende a frustrar algunos métodos de seguridad y control.

Los diversos estratos de seguridad están diseñados para impedir el acceso no autorizado y en esto está implícito un aspecto de seguridad importante: se debe averiguar en qué punto es más costoso conservar la seguridad que la existencia de una brecha en el sistema de seguridad. Desgraciadamente para esto existe una respuesta por cada empresa que haga uso de una red local.

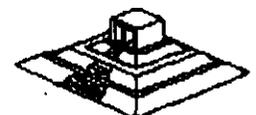
Así mismo, otros aspectos intervienen en el tema de la seguridad. El tamaño de una red puede impedir problemas de seguridad o acrecentarlos. En una LAN grande podrían necesitarse técnicas de codificación o de devolución de llamadas. Con una LAN chica quizá sea posible controlar los dispositivos conectados a un sistema, pero en una LAN grande dicho control puede ser más difícil de lograr.

Un método más adecuado sería aislar datos importantes y su acceso en redes concurrentes privadas que usen, quizá, un protocolo de comunicación alternativo junto con las técnicas de codificación y devolución de llamadas. En fin, la solución que se proponga depende de cada una de las características y problemas, así como los requerimientos específicos de cada una de las redes.



CURSO : REDES LAN DE MICROS PARTE II
MODULO II DEL DIPLOMADO DE REDES LOCALES

5.-) TECNOLOGIAS DE VANGUARDIA



CABLEADO ESTRUCTURADO

PUNTES, RUTEADORES, CONCENTRADORES

Puentes o *Bridges*

Más de una vez, se necesitan interconectar a las redes locales con otras redes. Esto es posible de realizar por medio de una gran variedad de productos, como son los puentes, ruteadores y concentradores.

El término *via de acceso* se ha utilizado para designar el hardware y software necesarios para hacer que se comuniquen entre sí dos redes tecnológicamente diferentes.

Un puente se usa a menudo para connotar el hardware y software que se necesitan para que se comuniquen dos redes que emplean la misma tecnología, o una similar.

Los puentes trabajan muy cercanos al hardware de la red. Básicamente los puentes toman los paquetes de una red y los ponen en la otra. De hecho son más que un repetidor, tiene suficiente información sobre los paquetes que maneja aunque no conoce la estructura propia de éstos.

Un puente no hace diferencia sobre el tipo de protocolo que se use para mandar los paquetes, solamente los envía. Como los puentes son una pieza de conexión que es transparente para niveles altos de software, para el sistema operativo, es como si tuviera una red de gran tamaño y no varias redes interconectadas por medio de puentes.

Los puentes se están mejorando, para que pueda realizar algunas funciones de un ruteador, con la ventaja de tener la velocidad de un puente.



Ruteadores o Routers

Los ruteadores son un dispositivo de nivel más alto que los puentes, un ruteador no sólo entiende qué es el paquete que está transmitiendo, sino además sabe suficiente de su estructura como para determinar el destino del mismo. Esta información le sirve al ruteador para tomar decisiones sobre cómo y hacia dónde redirigir los paquetes que recibe.

Un ruteador reduce en gran medida la cantidad de tráfico innecesario entre las redes locales conectadas, ya que sólo transmite los paquetes que son importantes para la red que recibe y la que manda.

Un ruteador puede además, escoger el mejor camino a seguir para un paquete, entre dos redes complejas.

Para que todo lo anterior sea posible, es necesario que el ruteador conozca y entienda un protocolo específico antes de que pueda rutear los paquetes que obedecen a ese protocolo. Los ruteadores son dependientes del protocolo, algunos pueden tener varios protocolos para funcionar y así cubrir un rango más amplio. Actualmente los ruteadores se están dotando cada vez de más protocolos, de manera que puedan competir con los puentes.

Concentradores

Un concentrador simplifica y centraliza el cableado de las redes locales, además de simplificar los cambios, movimientos y adiciones a la misma.

Al centralizar el cableado, se ahorra mucho tiempo en el seguimiento de cables, ya que el concentrador se encuentra en un closet y ahí mismo es de donde salen todos los cables a distribuir, lo que además hace más segura a la red.

Generalmente, se gastan miles de dólares al tratar de realizar un cambio en una red. Por medio de los concentradores, todos estos costos se abaten significativamente, si tomamos en cuenta que es posible necesitar o desear realizar numerosos movimientos al año.

Algunos nuevos productos de compañías como Bytex, Chipcom e IBM, permiten reconfigurar físicamente una red, por medio de software, ayudando a eliminar largas horas de trabajo enfrente del panel de parcheo.

Además de estas ventajas, los concentradores son relativamente económicos y escalables, son también sistemas estables.

Actualmente se está trabajando en la estandarización del software y el hardware de los concentradores. Los continuos avances en la tecnología de los semiconductores está haciendo posible que el tamaño de estos aparatos vaya reduciéndose considerablemente.



FIBRA OPTICA, BACKBONES, FDDI

Las nuevas tecnologías de interconexión de redes tienden al uso de la fibra óptica, como medio de comunicación, tiene una capacidad de transmisión de datos y de seguridad muy altas. Las fibras ópticas pueden soportar transmisiones de varios cientos de Mbps. Los cableados por medio de fibra óptica pueden soportar grandes distancias sin necesidad de repetidores, además de ser un medio inmune a la interferencia electromagnética.

Los costos de conexión con fibra óptica son típicamente altos, pero podemos esperar que estos precios bajen significativamente en los próximos años.

Ya existen en el mercado, proveedores que cuentan con las tarjetas necesarias para poder realizar conexiones con fibra óptica para las topologías Ethernet y Token Ring.

Muchas compañías están optando por la fibra óptica por diversas razones, entre ellas está la velocidad de transmisión de la que es capaz. Por ejemplo, FDDI¹⁷ soporta velocidades de transmisión de hasta 100 Mbits por segundo. En comparación con Ethernet que transmite a 10 Mbits por segundo o Token Ring que transmite a 4 ó 16 Mbits por segundo.

El comité 802.6 de la IEEE ha adoptado estándares para redes de área metropolitana, y el American National Standards Institute ha desarrollado los estándares FDDI y FDDI-II.

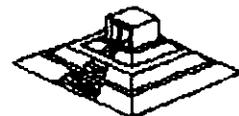
Además, la fibra óptica tiende a ser más segura que el cableado de cobre. Una red interconectada por medio de fibra óptica puede trabajar cerca de equipo eléctrico altamente sensible sin interferir uno con el otro. Un cable de fibra óptica entre dos edificios no atraerá rayos como el cable de cobre.

Al hablar de redes interconectadas por medio de fibra óptica, generalmente se está hablando de FDDI, diversos productos capaces de soportar FDDI han estado saliendo lentamente al mercado y se han dejado ver en diversas exposiciones de computadoras.

Como Token Ring, FDDI usa una topología con forma de anillo y un Token eléctrico para pasar el control de la red de una estación a otra, más no es compatible con Token Ring.

La mayor parte de las redes actuales con FDDI usan un doble anillo en donde cada nodo se une a los dos anillos independientes, transmitiendo los datos en sentidos opuestos. Esta configuración mejora la velocidad de transmisión así como la confiabilidad de la red, pero es muy caro.

¹⁷ Fiber Distributed Data Interface



Hasta ahora, FDDI se ha usado para interconectar PC's de alta velocidad o estaciones de trabajo con redes, o bien como *backbone* para interconectar estaciones más lentas, de igual manera que una carretera une los diferentes pueblos. Conectarse a FDDI es caro, dado el alto costo de los componentes ópticos, así como el costo del transreceptor y los integrados necesarios para FDDI.

Debido a sus características de ancho de banda, la fibra óptica se usa principalmente para backbones (que es un segmento que une varias redes locales).

Existe también FDDI-II que es una segunda versión de FDDI que nos permite transmitir voz y video además de datos. De manera distinta a FDDI que tiene un reloj corriendo de manera independiente, FDDI-II tendrá un marco de 125 microsegundos, permitiendo ser sincronizado con la red de comunicaciones.

REDES WAN, MAN

Además de las redes de área local LAN, existen las WAN¹⁸ y las MAN¹⁹. Al hablar de una red local (LAN) normalmente una persona se refiere a una red usada para la transferencia interna de datos e información de una cierta organización. Se debe entender interna como dentro de los límites de una oficina, un grupo de oficinas, un edificio o un grupo de edificios cercanos.

Reconociendo la necesidad de contar con estándares de mayor alcance que los aplicables a redes de área local, aunque sin llegar a redes de área vasta estándar, en 1981 se estableció el Metropolitan Area Network Group 802.6 de la IEEE.

A diferencia de las LAN que están diseñadas para la transmisión de datos, los estándares en surgimiento para redes de área metropolitana respaldan transmisiones de datos, voz e imágenes de video.

Como las MAN están diseñadas para redes que se extienden en distancias de más de cinco kilómetros y se conciben como redes de información integradas, los métodos de acceso de las LAN tienen graves deficiencias.

En consecuencia, el grupo de trabajo 802.6 cambió pronto a un protocolo de acceso múltiple con división de tiempo (TDMA).

Una forma de concebir una MAN es como una red de LAN's. Aunque los estándares en surgimiento aplicables a MAN no están limitados a enlazar redes de área local, ésta es realmente una aplicación importante.

¹⁸ Wide Area Network

¹⁹ Metropolitan Area Network



Se debe observar que el término "metropolitana" se usa en forma un tanto genérica para describir áreas de tamaño de hasta una ciudad, pero también puede referirse a instalaciones grandes multiedificios.

Aunque la IEEE ha adoptado un estandar para MAN o redes de área metropolitana, realmente sólo existen pocos ejemplos que se podrían denominar WAN y éstos ejemplos no se apegan al estandar de la IEEE. Estas redes están basadas principalmente en sistemas de CATV y a menudo reciben el nombre de Institutional Networks o redes institucionales o I-Nets.

Compañías, gobiernos locales, sistemas escolares, etc, han continuado la construcción de sus redes con base en líneas de teléfono rentadas, microondas privadas de corto alcance y a veces sistemas de transmisión por cable.

El comité 802.6 de la IEEE deberá designar los estándares para las redes de área amplia.

El comité describe varias metas para un estandar MAN: debe dar cabida a esquemas de transmisión de señales rápidos y robustos, debe garantizar seguridad y privacidad y hacer posible el establecimiento de redes privadas virtuales dentro de MAN, debe asegurar la alta confiabilidad, disponibilidad y facilidad de mantenimiento de la red, y debe promover la eficiencia de la MAN, sin que importe su tamaño.

La dificultad para describir estándares MAN es que éstos todavía continúan en su proceso de desarrollo, sin embargo, el desarrollo de un estandar óptimo es decisivo para el desarrollo de las MAN, ya que la operabilidad entre las redes de computadoras y de telecomunicaciones es un prerrequisito para realizar un lanzamiento exitoso de la nueva tecnología.

A diferencia de las LAN, las MAN se espera que transmitan información de voz y video, además de datos.

Se espera que el tráfico en una MAN comprenda:

Interconexión con LAN, gráficos e imágenes digitalizadas, transferencia de datos en grandes volúmenes, voz digitalizada, video digitalizado comprimido, y tráfico de estaciones convencionales.

Enlaces TCP/IP

TCP/IP es una familia de protocolos para interconectar computadoras de diversas naturalezas. Lo que se ha venido observando al paso de los años es que TCP/IP es un protocolo fuerte que no se ha visto desplazado por otros protocolos como se pensaba. Originalmente TCP/IP se creó por pedido del Pentágono y se usó en su principio para la red ARPA que interconectaba a varias universidades y centros de investigación relacionados con el Gobierno de los Estados Unidos.



Es interesante hacer notar que ARPA después derivó a ser Internet, la red más grande del mundo, **Internet**, que cuenta con millones de nodos.

La evolución de TCP/IP se remonta a los primeros años de la década de los 80 y según fue desarrollándose, se fue estandarizando.

La forma en que se desarrolla hoy en día es por medio de un comité llamado IAB, que está formado por personas altamente calificadas, así se publican trimestralmente las especificaciones de los protocolos o sus revisiones.

Existe una diferencia primordial en estos estándares y es que para que un protocolo reciba el nombre de estándar, debe haberse probado exitosamente en redes reales durante varios meses, lo que garantiza la funcionalidad del mismo.

Desde su planeación, TCP/IP se pensó para ser independiente del medio físico de enlace, es esto precisamente lo que ha hecho que sea un protocolo ampliamente usado en enlaces de redes locales entre sí, o bien, con redes amplias WAN.

Los ambientes que usan TCP/IP se basan en que cada elemento de la red tenga su **dirección IP**. El propósito de lo anterior es identificar de forma única a cada elemento del conjunto, para IP cada uno de los nodos de la red.

A los nodos que son computadoras se les denomina *hosts*, bajo la terminología de TCP/IP, y los Gateways son el equipo que tiene realmente funciones de ruteador, es importante notar que la connotación de estos términos bajo TCP/IP es diferente a la que normalmente nos hemos referido.

Las direcciones de IP tienen como objetivo:

- 1.- Identificar de manera única cada nodo de una red o un grupo de redes.
- 2.- Identificar también a miembros de la misma red.
- 3.- Direccionar información entre un nodo y otro, aún cuando ambos estén en distintas redes.
- 4.- Direccionar información a todos los miembros de una red o grupo de redes.

IP hace el trabajo de llevar y traer paquetes entre todas las redes que estén unidas y usando este protocolo, pero no nos garantiza que éstos lleguen a su destino. Para remediar esto, está TCP/IP tampoco nos regula el flujo de paquetes.



TCP tiene funciones importantes, las que se mencionan a continuación:

- 1.- Secuenciamiento y reconocimiento de paquetes.
- 2.- Control del flujo de la información.

TCP partirá en paquetes la información y la enviará. A cada paquete se le asigna un número. El reconocimiento significa que cuando un nodo recibe varios paquetes, debe informar al que los está enviando que efectivamente los está recibiendo, de esta manera se logra un cierto control sobre la información que se está transmitiendo.

El hecho de poder enviar los paquetes significa que antes de poder establecer comunicación entre dos nodos, es necesario un *handshake* que es el momento en que el receptor y el transmisor se ponen de acuerdo para poder establecer la comunicación.

Existe una serie de tareas que TCP/IP realiza y que son de suma utilidad, tales como la emulación de terminales, para poder entrar a una diversidad de equipos, así como la transferencia de archivos entre computadoras.

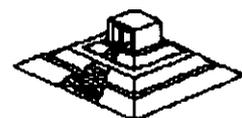
Dentro de las aplicaciones cliente-servidor, una de las que mayor auge ha tenido ha sido la de bases de datos, teniendo por un lado el equipo corriendo al manejador de bases de datos, y por otro, a muchas PC's conectándose a él a través de diversas herramientas e interactuando con la información.

Es importante recordar que las aplicaciones que corren en las PC's se denominan clientes y el equipo que tiene la base de datos se denomina servidor o *motor* de base de datos.

Como se desea poder realizar esa conexión entre clientes y servidores no importando si éstos están en la misma red o en redes distantes, la solución más sencilla es que ambos: clientes y servidores, se comuniquen usando TCP/IP, de hecho es la forma en que se ha comercializado. Oracle, Sybase, Gupta, Informix y varios más, usan TCP/IP como su forma de transporte de datos y comandos entre clientes y servidores.

Administración vía SMNP

La principal tarea dentro de la administración de las redes de área local es la emisión de mensajes de alerta para el administrador cuando surgen problemas. Estas alarmas le permitirán mantener la red activa y maximizar su funcionamiento para aprovecharla al máximo.



A pesar de que las redes hoy en día constan de múltiples tecnologías y equipos de diferentes proveedores, el reto es poder manejarlas como una unidad.

La ISO (Organización Internacional de Standards) ha categorizado las funciones de la administración de las redes como se vió anteriormente. Los dispositivos de interconexión entre las redes son inteligentes, simplificando la administración de la red a tal grado, que personas que no pertenecen al área técnica, pueden fácilmente identificar y corregir las fallas.

Muchos de los productos para las redes usan SMNP (Simple Network Management Protocol) . SMNP nació en 1988 con el propósito de administrar los dispositivos de la red TCP/IP más grande, que unía universidades, particulares, institutos de investigación, dependencias de gobierno y corporaciones privadas.

SMNP es el protocolo más popular para la administración de redes en la actualidad. Su éxito se puede medir por el aumento de más del 30% en los proveedores que participaron durante los cuatro años en la creación de productos basados en SMNP y el éxito de los productos en el mercado.

SMNP resulta ser muy simple y tiene pocos comandos (que son sólo tres) . Además, SMNP se puede intercambiar con casi cualquier protocolo de red local ya que a pesar de derivarse de TCP/IP, sus comandos requieren solamente de servicios de transporte básicos, lo que hace su protocolo independiente.

SMNP sirve como denominador común para los productos de administración de red y tiene tres componentes:

- 1.- Agente o agente apoderado
- 2.- Administrador
- 3.- Base de información para administración (MIB Management Information Base)

Estos tres componentes junto con los comandos de soporte comprenden el marco de trabajo de SMNP.

A continuación se explicarán estos componentes y la forma en que interactúan para desempeñar la administración de la red.

El administrador de la red debe ser capaz de presentar grandes proyectos con seguridad y modificarlos ágilmente según se requiera. El administrador de red debe además conocer un amplio espectro de tecnologías y tener noción del contenido de todos los manuales y boletines técnicos del equipo y las aplicaciones que incluye y que puede aceptar la red que supervisa.

Debe además, proveer un conocimiento profundo de las metas de la organización, poder realizar análisis de costos y diseño de sistemas. Además es deseable que pueda mantener la red libre de equipo obsoleto o defectuoso e incorporar de manera meditada, equipo de reciente lanzamiento.



El administrador de la red debe además, proponer el software que mejor resuleva las necesidades particulares de la organización, o bien programar a la medida si es requerido. Lo anterior incluye por supuesto la actualización del software y la compatibilidad e intercomunicación entre los paquetes. Debe conocer a fondo las direcciones, el volúmen y las características del flujo de información que se transmita sobre la red.

Es importante que la persona que sea el administrador tenga facilidad para relacionarse con el resto del personal y que sea paciente para poder ayudar a los usuarios con problemas, de alguna manera podemos ver al administrador de la red como un reentrenador.

El conocimiento de los sistemas operativos y de los principios básicos del cableado, así como tener conocimientos serios en sistemas de información o ciencias computacionales son requisitos indispensables para un administrador de una red. Debe además tener conocimientos de SMNP para poder llevar un registro cronológico de la información del sistema acerca de la actividad de la red. Cuando se instala una estación de trabajo, se refiere al administrador de estaciones de la red (NMS Network Management Station) por lo que estos dos términos en ocasiones se usan indistintamente.

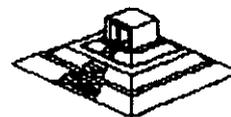
El administrado selecciona los dispositivos de red para recoger información y contiene una interfase numérica de tiempo real para el procesamiento de estos datos. El administrador sirve como una ventana para la red.

El agente es compatible con SMNP residente en el software de la red . Es un dispositivo inteligente capaz de monitorear las tareas de la estructura de comunicaciones colectando datos acerca de su ambiente, aún de procesos sofisticados.

Los dispositivos que no soportan SMNP un agente SMNP deben manejarse con un agente apoderado, este tiene la misma función que el agente pero al mismo tiempo sirve como convertidor de protocolo, ya que convierte los comandos del SMNP en instrucciones que pueden ser comprendidas por el dispositivo propietario y vice versa.

El agente responde a las peticiones del administrador para proveer información específica acerca de los periféricos. El administrador puede solicitar ciertos datos ambientales, como el IP (Protocolo Internet) del dispositivo o que se cambie el nombre asignado a un puerto específico. Así también, el administrador puede solicitar al agente que controle las comunicaciones, por ejemplo que active o desactive un puerto.

El administrador reacciona a las alarmas de los agentes, por ejemplo un mensaje intermitente cuando un HUB se ha accionado o un puerto ha sido dividido.



Asociado con cada enlace de comunicación, existen una serie de recursos que pueden ser controlados y monitoreados, estos recursos definen la personalidad de los periféricos. El conjunto de recursos constituye el MIB (Management Information Base).

MIB es la base de datos en el marco de SMNP, contiene un conjunto estándar de variables que es soportado por los agentes y administradores. El MIB también contiene los recursos específicos del proveedor. Estos son aumentados por el proveedor para mejorar el manejo de sus propios productos.

El MIB reside en cada agente o administrador de la red. Cada agente, para ser realmente compatible con SMNP debe contener un conjunto mínimo de los recursos estándar de MIB así como las variables específicas del proveedor. Así mismo cada administrador debe tener un depósito del MIB, una colección del MIB representando cada uno de los dispositivos en la red, el administrador usará la información de los dispositivos almacenada en el mismo para entender la información que recibe de los agentes.

La introducción de los nuevos productos basados en SMNP, trajo una proliferación de nuevos MIB's. Para controlar esta situación se han formado comités para desarrollar estándares para la creación de MIB en los diferentes tipos de productos. Este esfuerzo toma validez con la formación del repetidor IEEE 802.3 MIB, que identifica los recursos administrables en un repetidor Ethernet.

Cualquier tipo de comunicación requiere de un vocabulario común y de un uso gramático definido para ese vocabulario. Ambos MIB, tanto el que reside en el agente como en el administrador, proveen el vocabulario y el SMNP la gramática, juntos definen como se intercambiarán los mensajes.

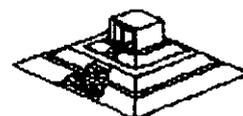
El SMNP es comunmente referido a un protocolo de estímulo-respuesta, para cada solicitud emite una respuesta. Hay tres verbos básicos en su conjunto de comandos:

Get, set y trap.

Al usar el comando *GetRequest* el administrador le solicita información al agente, este le manda la información necesaria con un comando *GetResponse*.

El administrador deberá usar el comando *SetRequest* para controlar el dispositivo cambiando el valor de una de las variables del MIB. Así, el agente responde con el comando *GetResponse*.

El *SetRequest* no es soportado por todos los proveedores, algunos lo soportan unicamente por un número limitado de variables. Es importante usar con cuidado el comando *Set* ya que puede afectar las operaciones de la red.



El agente también alerta al administrador, vía el comando *Trap* cuando encuentra algún problema y entonces el administrador liberará una alarma. Los mensajes de *Get*, *Set* y *Trap* se manejan entre el administrador y los agentes a través de un protocolo de transporte. Como el SMNP es un protocolo independiente, puede usar cualquier vehículo de paquete.

Por todo lo anterior, SMNP es una solución a la administración de redes, que contiene las características de flexibilidad, facilidad de uso e instalación, así como la provisión de estándares para la interacción con diferentes sistemas y ambientes.

Nuevas tecnologías de impresión

EL "DOWNSIZING"

La palabra *Downsizing* suele mal interpretarse. Si en idioma inglés es difícil de entender, mucho más en español, dado que cada quien la traduce como quiere. *Downsizing* evoca reducciones drásticas, recorte de personal, tirar los mainframes a la basura, y por supuesto, generación de ingresos para otros.

La industria sigue tratando de encontrar algún término que se ajuste más al verdadero objetivo de esta tendencia. Pero dejando a un lado la semántica, se tratarán de mostrar las funciones principales del *Downsizing*.

Su misión primordial es la de liberar a los mainframes de aquel procesamiento de datos que pueda realizarse en equipos más compactos y más económicos. De hecho no necesariamente significa una reducción en costos, especialmente en los primeros años del proceso, cuando el Gerente de Sistemas tiene que cablear sus instalaciones, adquirir e implantar redes locales, y sobre todo formar a su personal.

Conforme los usuarios han ido aprendiendo a utilizar las herramientas de cómputo, gracias al tremendo auge de las microcomputadoras, tanto ellos como los gurús de Sistemas van observando gradualmente cómo la excesiva concentración de datos en grandes equipos es ineficiente y que no necesariamente los sistemas se verán afectados si se ponen al alcance del usuario. En muchos casos es más eficiente acercar al usuario con su sistema, bajo esquemas compactos que sean sencillos de instalar y mantener.



MAINFRAMES O REDES LOCALES

Downsizing no significa perder poder, más bien significa ofrecer sistemas con mayor eficacia, cantidad y calidad. Es totalmente irreal pretender eliminar por siempre los grandes equipos, pero tampoco es lógico seguir manteniendo aplicaciones en un equipo central que sean utilizadas únicamente por uno o dos usuarios. Además con mercados cada vez más competidos, el típico "backlog" en el desarrollo de aplicaciones en grandes sistemas, es ya imposible de mantener.

Cuántas veces no hemos escuchado decir: "Hace dos años que pedí el sistema y no me lo han entregado". De hecho, en México más que hacer Downsizing, es más común observar el dilema de seguir desarrollando en host o iniciar el desarrollo en redes locales.

Las tecnologías de hardware y software para redes locales han alcanzado el desempeño y las características de una aplicación típica de mainframe. E incluso, la cada vez más dominante arquitectura cliente-servidor permite que los datos sigan permaneciendo en host mientras que el usuario tiene acceso a ellos a través de PC's amigables y económicas.

Downsizing no significa únicamente migrar aplicaciones de host a redes locales, también incluye el desarrollo de aplicaciones bajo las mismas. Lamentablemente, para muchos el desarrollo en LAN (red de área local) significa hacer una aplicación en Xbase, instalarla en un servidor y ofrecer pantallas más o menos agradables a los usuarios. Obviamente esto no compite ni de casualidad con los seguros y confiables sistemas de los mainframes.

POR DONDE EMPEZAR

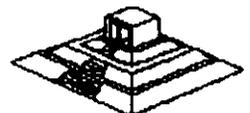
Si se va a decidir dejar de hacer aplicaciones en mainframes, o apostar al desarrollo de sistemas bajo redes locales, hay que analizar primero dos grandes áreas:

- * **La estrategia a seguir para la implantación del sistema.**
- * **El hardware y software necesario.**

Sin pretender dar alguna metodología, se sugieren algunos puntos dignos de tomar en consideración para cada área.

La estrategia a seguir para la implantación del sistema.

1.- Seleccionar una aplicación de poca visibilidad y bajo riesgo. Considerar que el proceso de Downsizing lleva varios años, y sobre todo, que no todas las aplicaciones son susceptibles de ser desconcentradas.



2.- Formar un grupo interdisciplinario liderado por un "gurú" que conozca ambos mundos, el de los mainframes y el de PC. Involucrar a las áreas de desarrollo (tanto en PC como en host), comunicaciones, PC y mantenimiento de sistemas. Además de involucrar al usuario hay que invitarlo a participar, pero eso sí, no hay que crearle expectativas que no se puedan cumplir.

3.- Minimizar el número de proveedores, pero mantener el espíritu integrador. Nadie nos dará la solución completa.

4.- Invertir en entrenamiento. Son muy variadas las áreas de experiencia que hay que cubrir. No hay que olvidar considerar la conectividad amplia, bases de datos relacionales, desarrollo de " front ends" (interfaces con el usuario), arquitectura cliente-servidor y telecomunicaciones.

5.- No hay que esperar a que sea demasiado tarde para iniciar el proceso de Downsizing. Este no es trivial y lleva tiempo. La experiencia ha mostrado que bajo presión se tienen pocas probabilidades de éxito.

6.- Hay que analizar todas las posibilidades pero sin exagerar. No hay que estar evaluando todo el tiempo, hay que aprovechar el momento para motivar al equipo de trabajo y llevarlo al logro de rápidos resultados.

7.- Medir el beneficio sin olvidar el antes y después. Eso ayudará a vender la idea más fácilmente. Hay que cuantificar los pesos y centavos del beneficio.

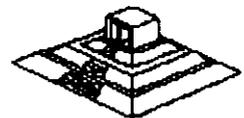
8.- Cuidarse de los charlatanes. En México existen pocas empresas serias integradoras de tecnología.

El hardware y software necesario

1.- Analizar en detalle la aplicación a implantar. Qué la caracteriza? Es transaccional o más bien es la típica aplicación intensa en procesamiento de datos? Esto será vital para la selección del hardware y software.

2.- Seleccionar el hardware. Probablemente sea más adecuado contar con un servidor con excelente manejo de memoria caché, más que con óptimos puertos de entrada-salida. Las características de su aplicación ayudarán a seleccionar el mejor grupo de pruebas de referencia a seguir para evaluar al servidor. Una marca de servidores puede ser más útil para sistemas de información que para aplicaciones transaccionales.

3.- No hay que subestimar la importancia del cableado. Esta es una de las inversiones más fuertes y el factor más común de fallas en una red. Es importante considerar su administración y mantenimiento, especialmente en México, en donde los edificios no están preparados para ser cableados.



4.- Qué nivel de conectividad se necesita? Tal vez se requiera soporte para servicios SNA o disponibilidad de protocolos de red amplia como TCP/IP. Esto seguramente nos llevará a seleccionar el equipo de interconexión necesario, incluyendo gateways, puentes, concentradores, etcétera.

5.- Qué motor de base de datos utilizar? SQL o no-SQL? Cuántos "front ends" lo soportan? Son propietarios o abiertos? No hay que creer que todos los motores de bases de datos son iguales, existen diferencias sustanciales en cuanto a programación, ayudas, herramientas de administración, conectividad con otras bases de datos (principalmente mainframes), etcétera. Hay que tomarse el tiempo para entender este punto y pedir referencias.

6.- Qué ambiente operativo se utilizará? DOS, OS/2, Unix/Xenix, Macintosh o Windows, entre los más populares.

7.- Finalmente, pero no menos importante, hay que determinar qué sistema operativo de red se utilizará. Se recomienda que la información anterior conjunta ayude a decidir este elemento, y no al revés, como comunmente sucede.

8.- Incluir productos que trabajen integrados y sobre todo que hayan sido probados en conjunto. Si es posible, apoyarse en la experiencia de otras empresas.

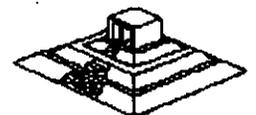
Una implantación inadecuada de las primeras fases del Downsizing puede crear más problemas de los que nos podamos imaginar. Pensar en que justificar fuertes inversiones, y sobre todo, romper esquemas ya establecidos de operación no es nada alentador. Hay que aprender a llevar al grupo a esta tecnología con un buen plan de capacitación.

Normalmente la gente que proviene del esquema centralizado del mainframe ve a las PC's como juguetes y no aceptarán fácilmente que su querido monstruo deje de ser el alma de la empresa.

Por otro lado, hay que considerar también la manera de enfrentar el éxito. No hace mucho, en una empresa financiera se realizó exitosamente la puesta en marcha de una aplicación en una red local en tiempo récord (menos de cuatro meses), con costos bajos y con el beneficio adicional de automatizar al grupo usuario con correo y agendas electrónicas. Fue tal el éxito que la demanda por este tipo de sistemas se incrementó drásticamente.

Como en todo, el Downsizing también tiene sus obstáculos. Los siguientes son los principales factores que comunmente propician el retraso de esta fuerte tendencia. Hay que analizarlos y sacar conclusiones:

1.- **Convencimiento:** Si no se está completamente convencido, no se iniciará el cambio. Si la cabeza de la empresa no cree, será difícil que motive y lleve a un feliz término el cambio de estructuras.



2.- Temor al rompimiento de las normas y flujos de información: El mismo desconocimiento y, en cierta medida, la falta de madurez de algunos elementos, dejan un grado de incertidumbre en la seguridad de la información. Se quiera o no, el usuario tendrá elementos para poder alterar los flujos de información sin que el Gerente de Sistemas se entere. Algunos Gerentes de esta área quisieran estar más seguros de cómo controlar esta situación.

3.- Situaciones técnicas asociadas con el hardware: Es común encontrar que el hecho de conectar al mainframe con redes y micros implica cambiar o instalar nuevos elementos de hardware. Obviamente la inversión se magnifica.

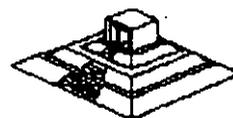
4.- Situaciones técnicas asociadas con las redes: Similar al punto anterior, el 11.4% de los entrevistados no está preparado para la instalación de redes, y es difícil de creer, pero en ciertos casos el Gerente de Sistemas ni siquiera piensa que deban depender de él.

5.- Reentrenamiento de usuarios: El factor entrenamiento podría ser fundamental en el cambio. Muchos usuarios utilizaban sus PC's únicamente como emuladores de terminal. Habría que enseñarles a usar DOS o Windows, a cargar archivos, a usar el ratón, etcétera. Cuando se trata de cientos de personas, éste es un factor a evaluar, no hay duda.

6.- Costos e implantación: En este punto la gran mayoría coincide en que la inversión es el mayor obstáculo. Hay que pensar en que el edificio no está preparado para ser cableado, que se tienen que conectar "n" localidades remotas con esquemas de comunicación más sofisticados, y que no es muy claro el ahorro en costos en el corto plazo. Las opiniones aquí son variadas: una estadística muestra que el 60% de los Gerentes de Sistemas de "Las 500 empresas del Fortune" opina que su organización se vería beneficiada en los siguientes dos años, mientras que tan sólo el 1% piensa que se beneficiaría en los siguientes diez. El restante 33% habla de un periodo de tres a cinco años.

7.- Convencimiento a la Dirección: La venta a la Dirección es también un obstáculo importante. El factor seguridad, pero sobre todo la inversión pueden agrandar este obstáculo. Hay que hacer cuentas.

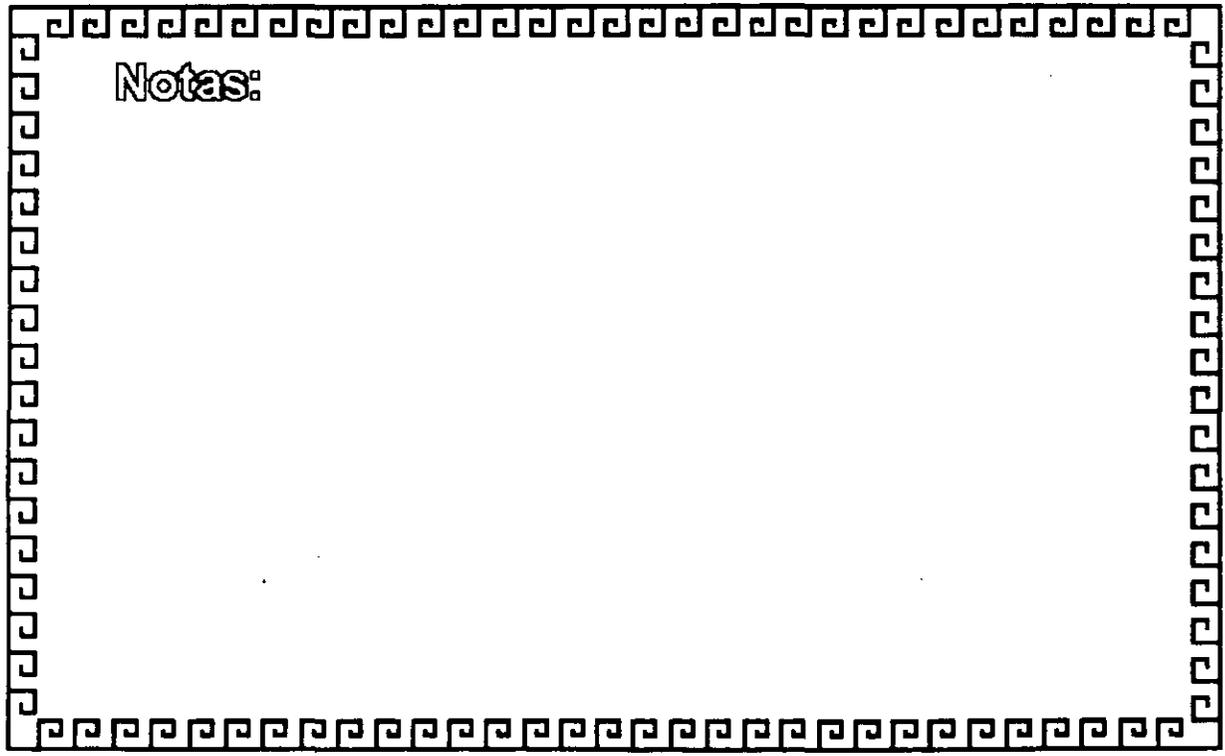
Como se puede ver, no sólo basta con romper el paradigma de basar todo en el mainframe, si no que es necesario volverse experto de la noche a la mañana en la tecnología de redes locales, servidores de bases de datos y ambientes operativos, además de convertirse en un buen analista financiero. No hay que desanimarse, de todos modos se tendrá que hacer algún día.





INTRODUCCION

**TCP/IP Y LA INTEGRACION
DE AMBIENTES
HETEROGENEOS**



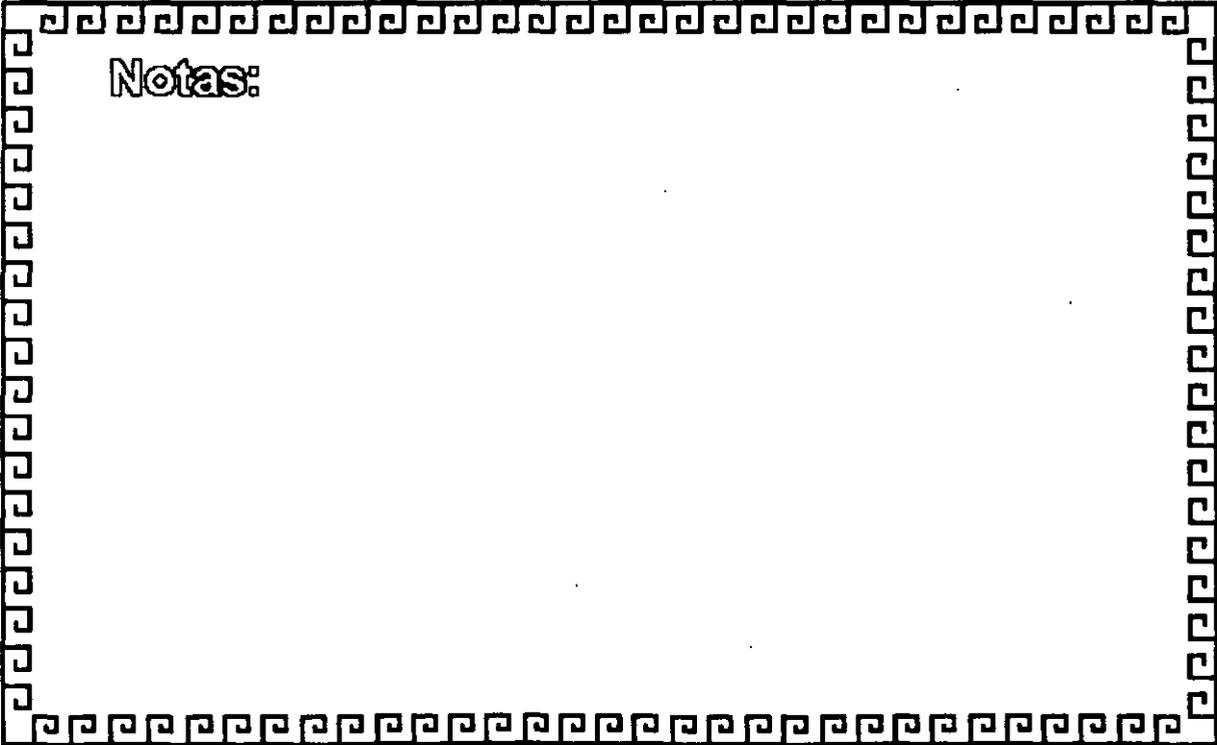
Notas:



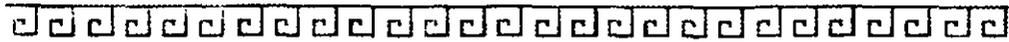
HISTORIA Y GENERALIDADES

¿POR QUE TCP/IP?

- Aceptado ampliamente por los centros de investigación y desarrollo en todo el mundo
 - Desde 1984 fue requerido por el gobierno y la defensa de los E. U. A.
 - Los sistemas basados en Berkley-Unix, lo proveen
 - SUN (Sun Microsystems) le da a TCP/IP un posicionamiento comercial
 - Los ambientes más técnicos adoptan TCP/IP
 - Son los únicos protocolos realmente abiertos y estándares disponibles actualmente
 - Predecesores de los protocolos ISO
- 



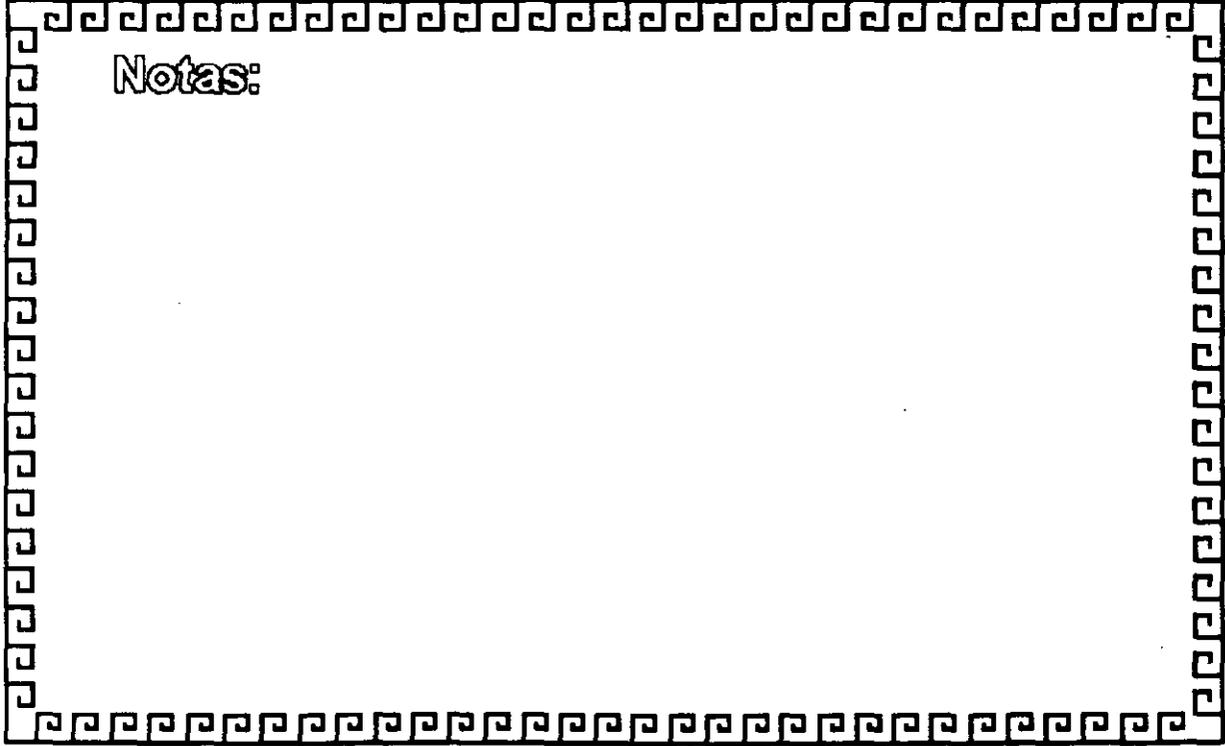
Notas:



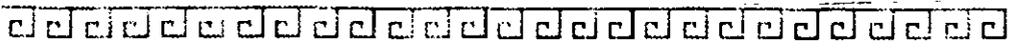
ARQUITECTURA

Protocolos a nivel de Red

IP	Internet Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
EGP	External Gateway Protocol
OSPF	Open Shortest Path First

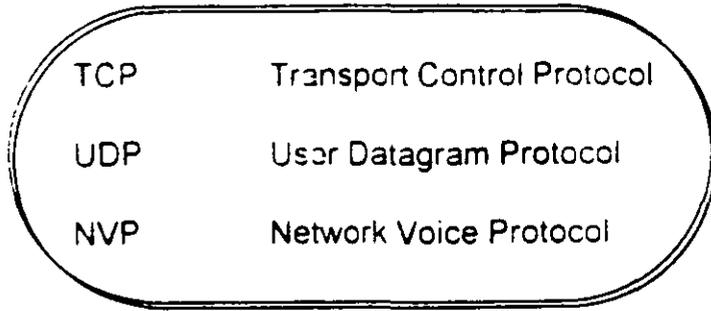


Notas:

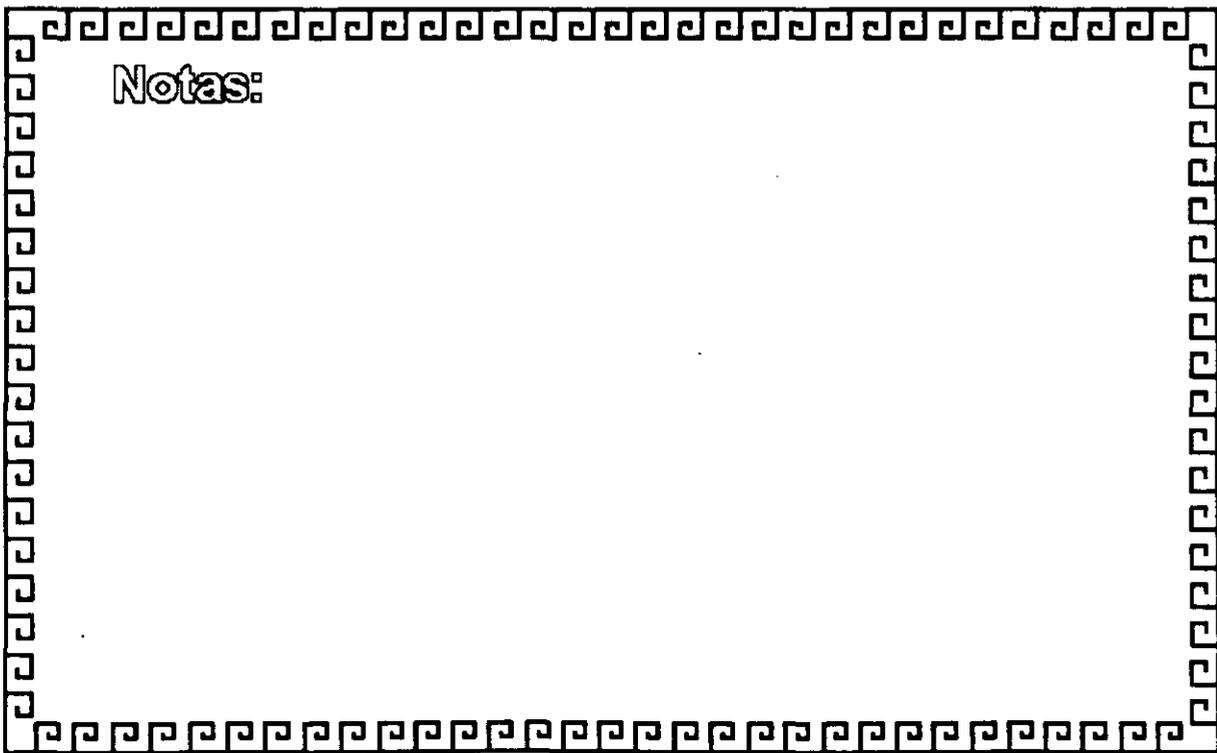


ARQUITECTURA

Protocolos a nivel de Transporte



TCP	Transport Control Protocol
UDP	User Datagram Protocol
NVP	Network Voice Protocol



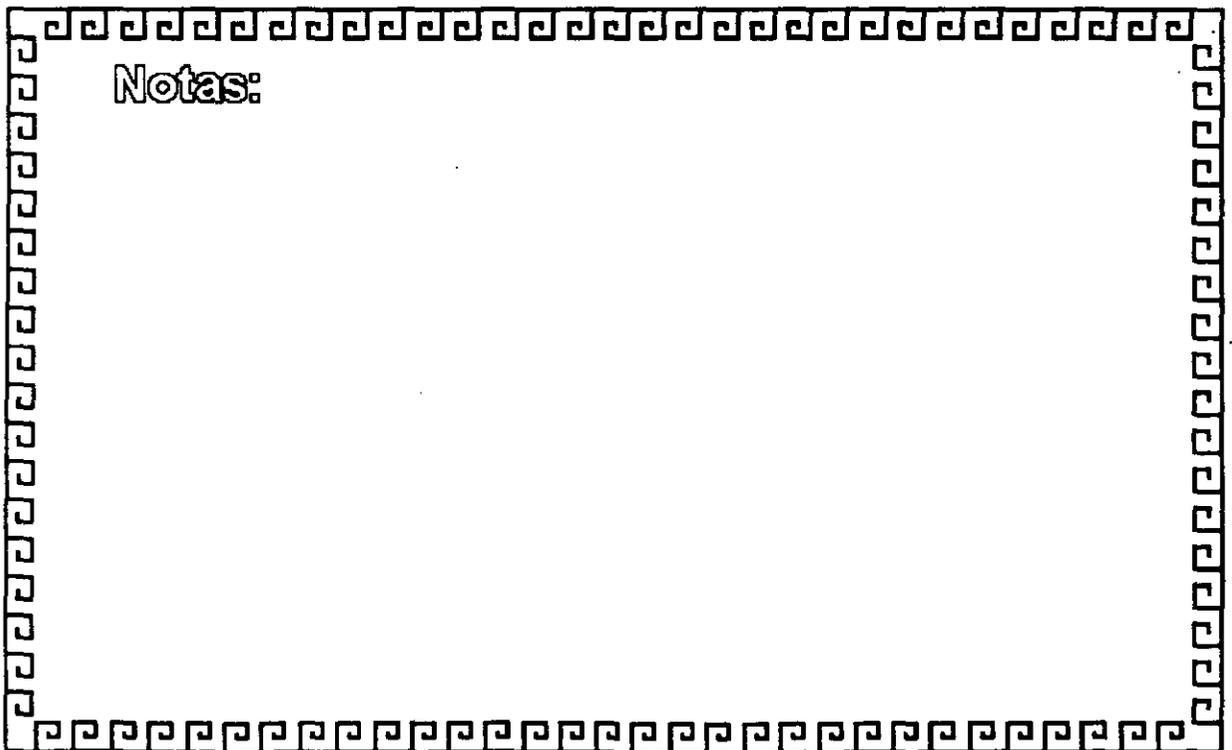
Notas:



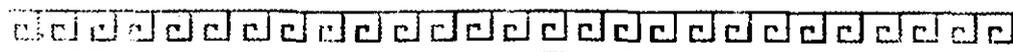
ARQUITECTURA

Protocolos a nivel de Aplicación

SMTP	Simple Mail Transfer Protocol
FTP	File Transfer Protocol
TELNET	Comunicación de Terminal
DNS	Domain Name Service
NSP	Name Service Protocol



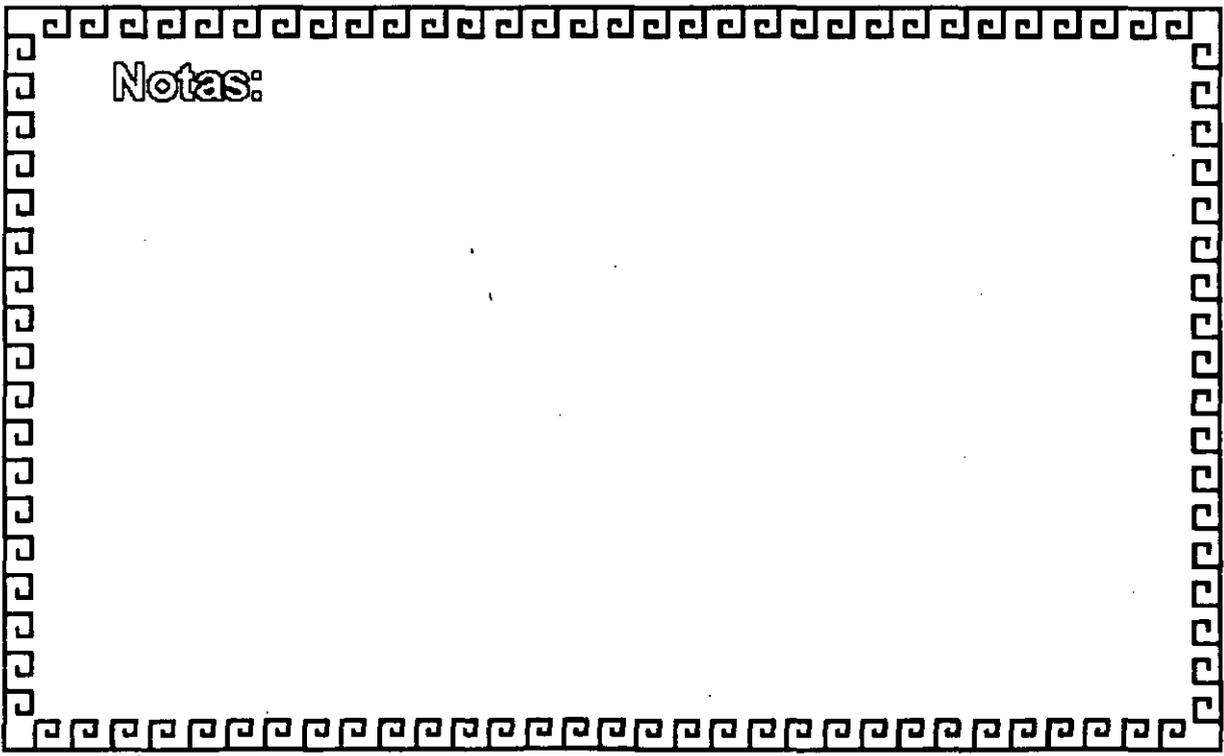
Notas:



Nivel 3. Protocolos de Red

El nivel 3 provee un fuerte poder de transmisión y otros servicios

- Entrega de paquetes punto a punto
 - Amplio direccionamiento
 - Identificación a varios niveles
 - Fragmentación
 - Datagramas de mayor envergadura
 - Uso de redes con ancho de banda limitado
 - Permite operación Inter-Red
- 



Notas:



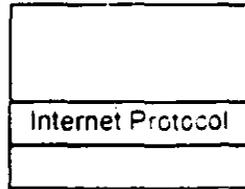
IP: Internet Protocol

Brinda dos servicios básicos

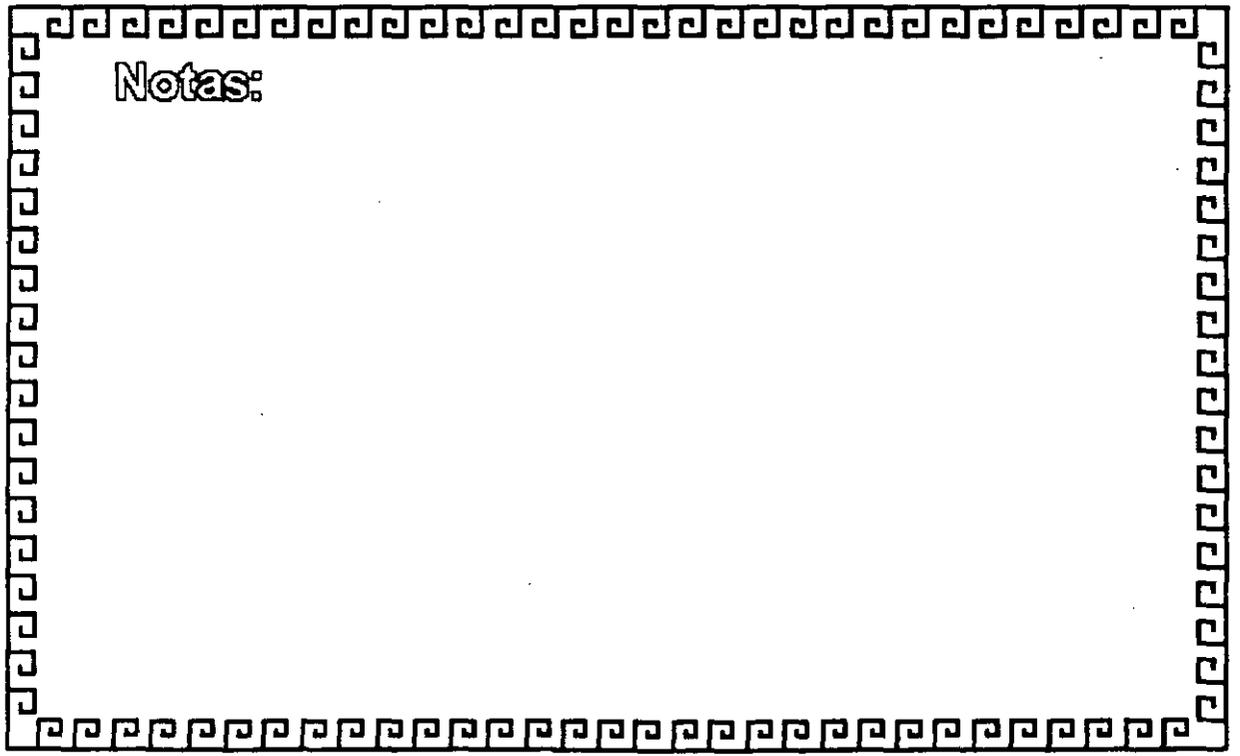
- *Enrutamiento
- *Fragmentación/Re-ensamblaje

Utiliza direcciones IP para decidir el ruteo

Aísla los protocolos superiores de las características específicas de la red



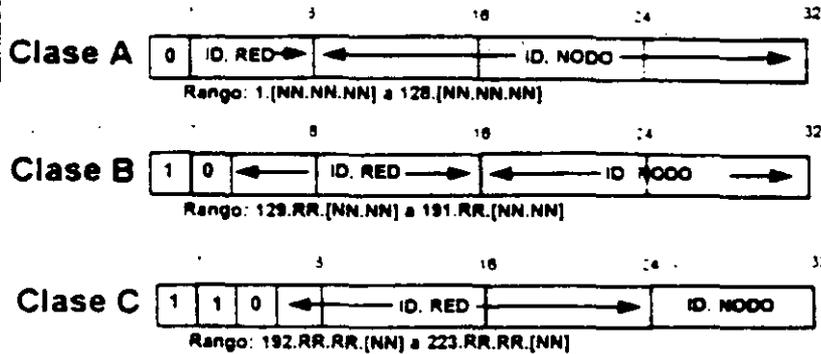
Notas:



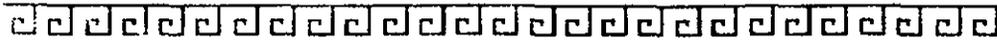
IP: Internet Protocol

Formato de las direcciones IP

Existen 4 clases de direcciones IP: A, B, C y D



Notas:



IP: Internet Protocol

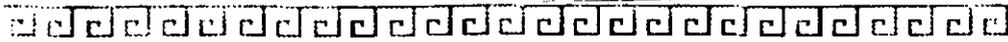
Ejemplo.

Nodo que envia

- Toma datos de TCP
- Pone los datos en un paquete (datagrama)
- Decide si es necesaria la fragmentación
- Determina ruta de acceso
- Envia el datagrama
 - + Local: consigue la dirección física y envia
 - + Remoto: envia a un ruteador

Notas:



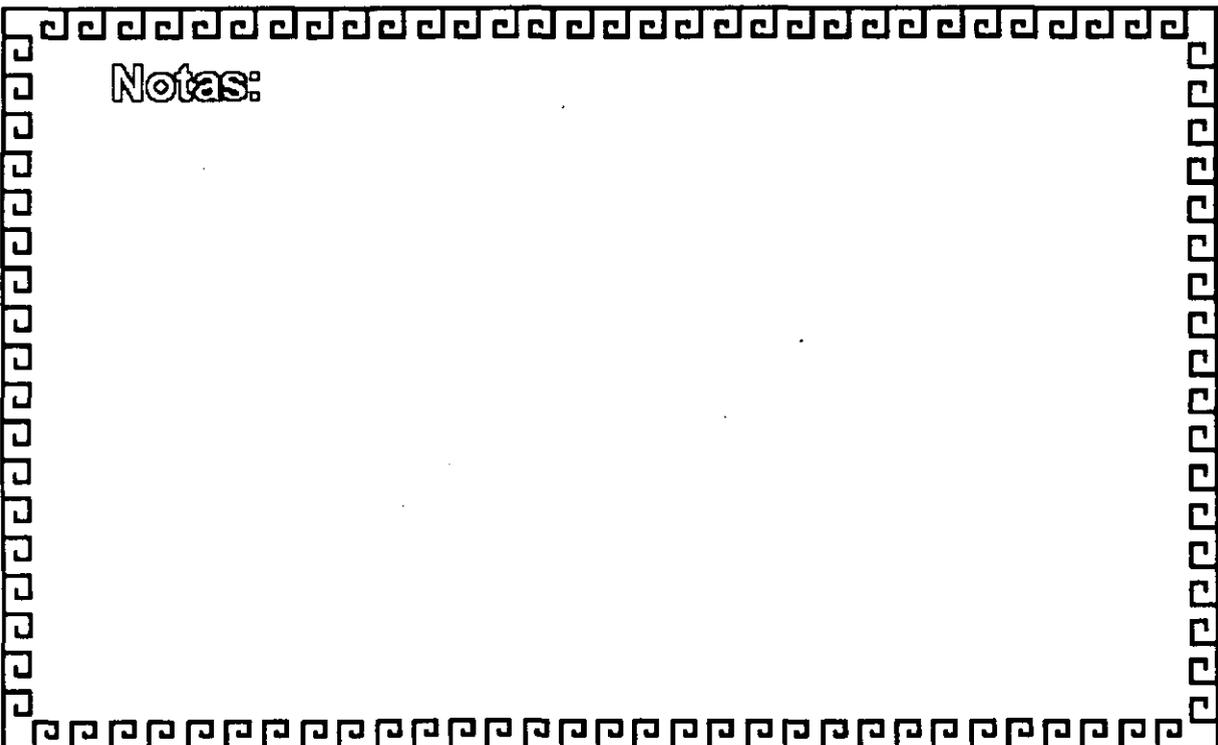


IP: Internet Protocol

Ejemplo

Nodo que recibe

- Toma el paquete del nivel de enlace
 - Determina si el paquete ha sido fragmentado
 - Si esta fragmentado lo re-ensabla
 - Pasa el datagrama a TCP
- 



Notas:



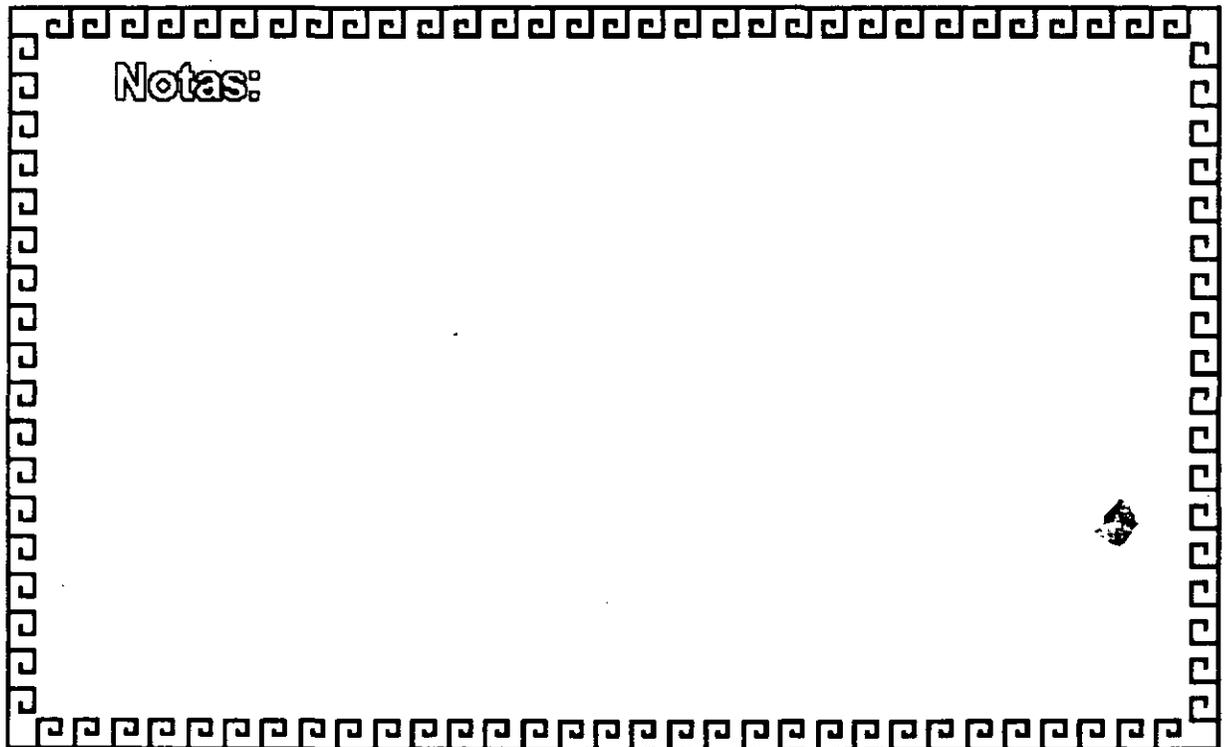
ARP

Address Resolution Protocol

- * Encuentra la dirección Ethernet (MAC) para una determinada dirección IP
 - * Verifica en cache local
 - * Emite un broadcast si la dirección no está en el cache



Notas:

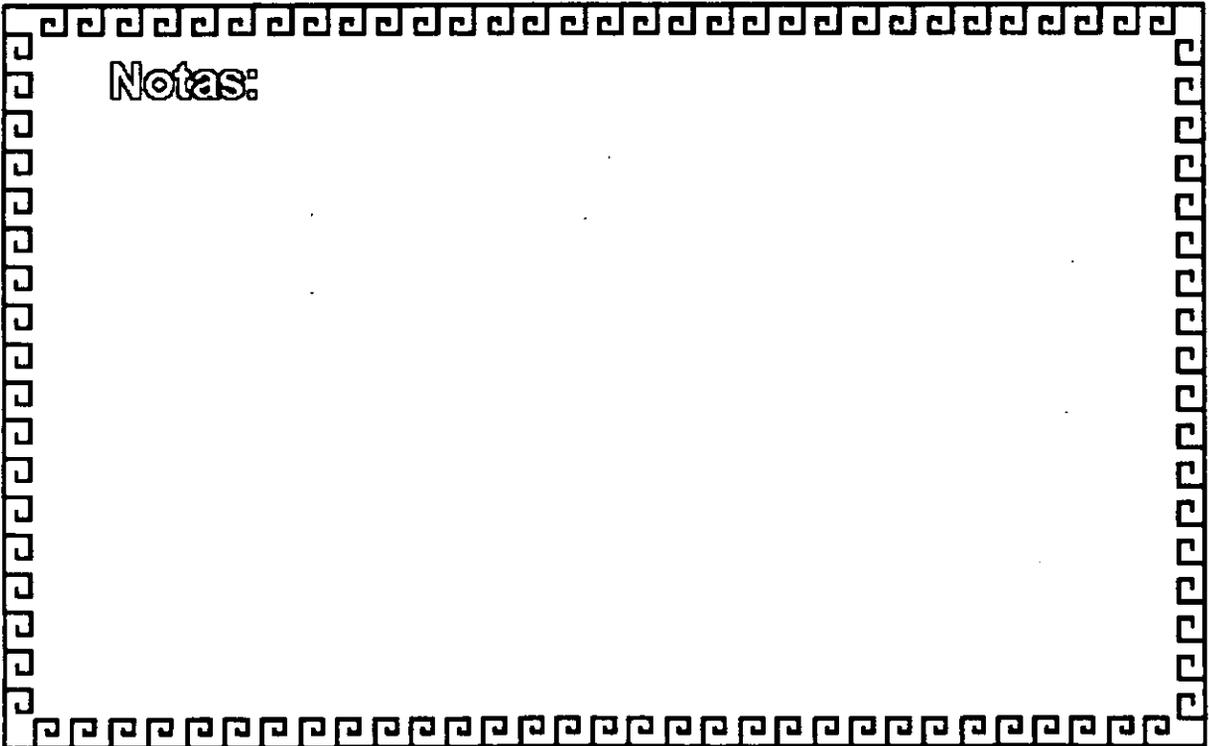




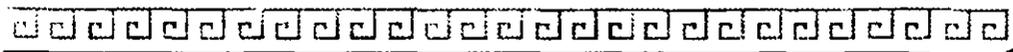
RARP

Reverse Address Resolution Protocol

- * Encuentra la dirección IP para una determinada dirección Ethernet (MAC):
 - * La operación se realiza a través de un broadcast
 - * Se requiere de un proceso de servidor RARP por cada red
- 



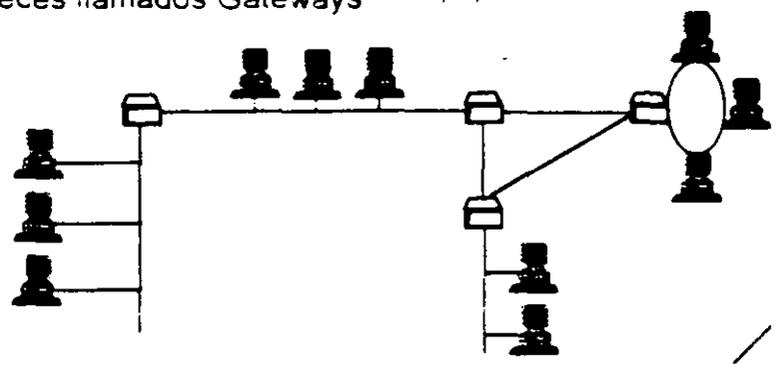
Notas:



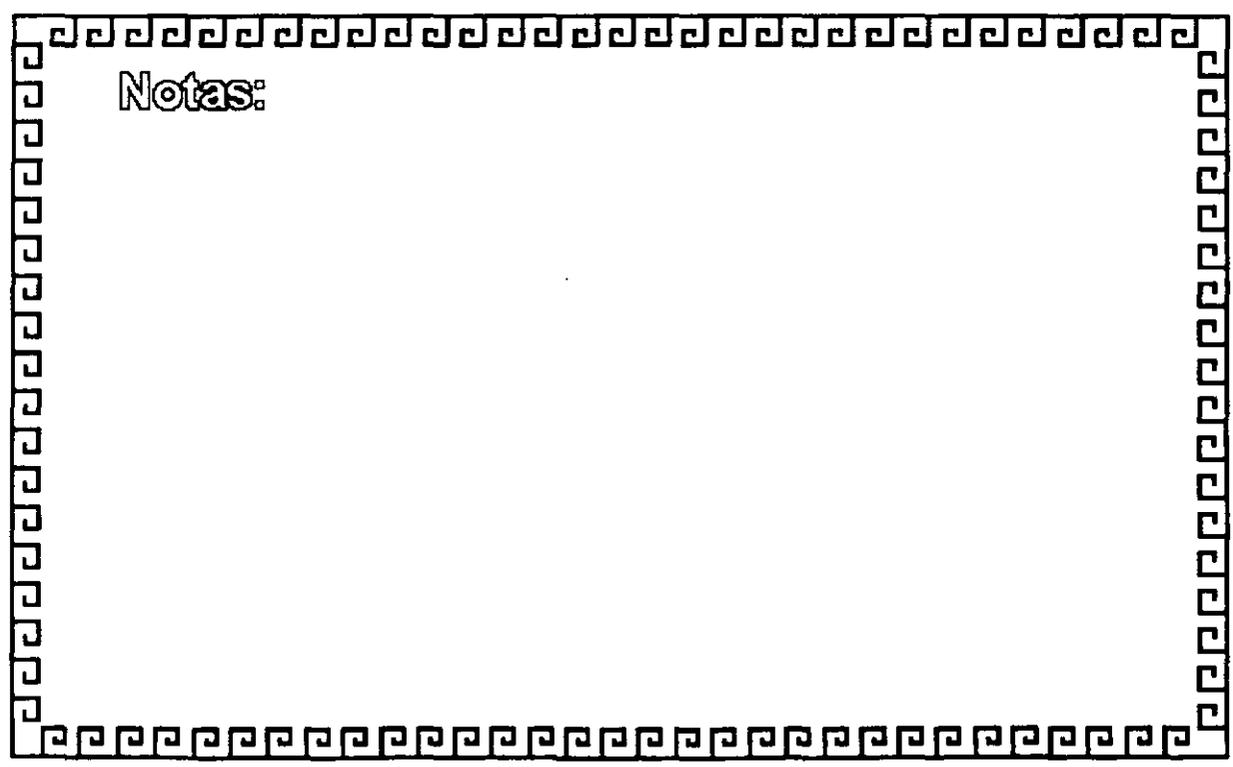
IP: Internet Protocol

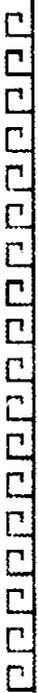
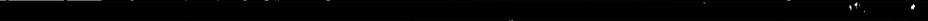
Direccionamiento Inter-Red

* Una Inter-red (internet), esta formada por una colección de redes individuales, unidas por ruteadores, a veces llamados Gateways



Notas:



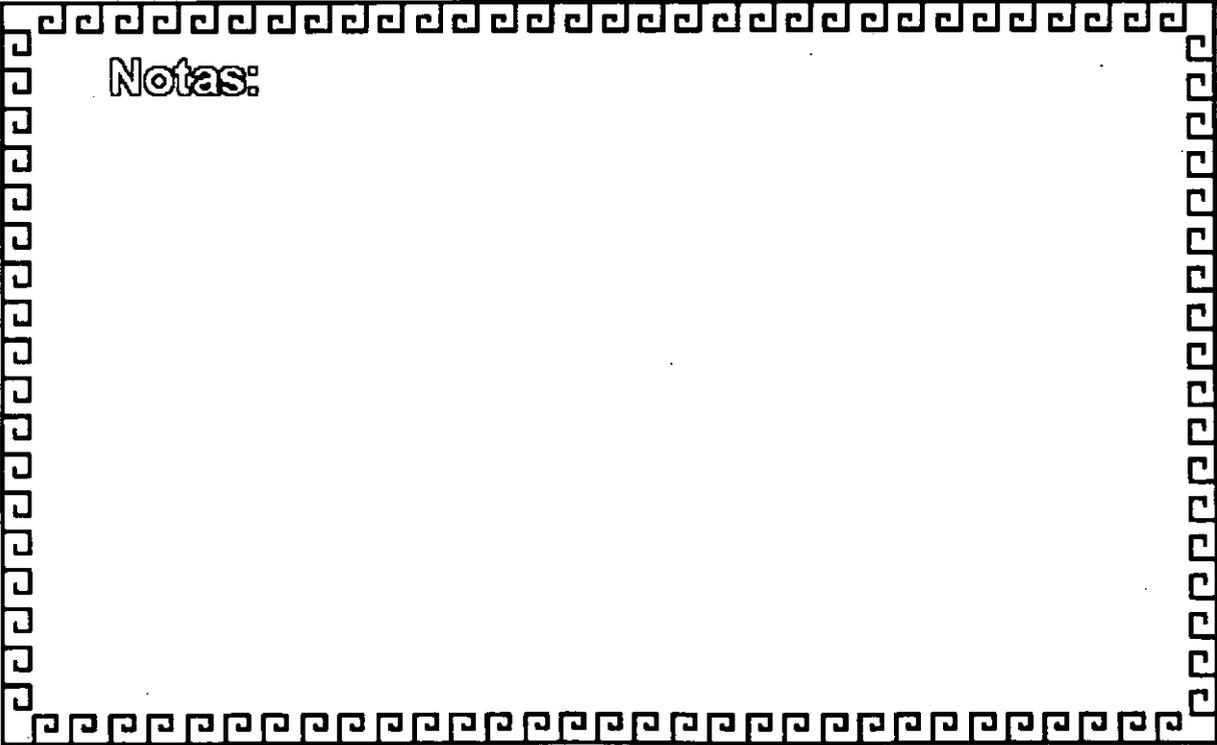


Ruteo de IP

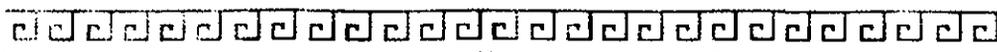
Protocolos de ruteo

*Intercambiar entre dispositivos (generalmente routers) información acerca de las redes que conectan.

- * Protocolos Intradominio
- * Protocolos Interdominio



Notas:



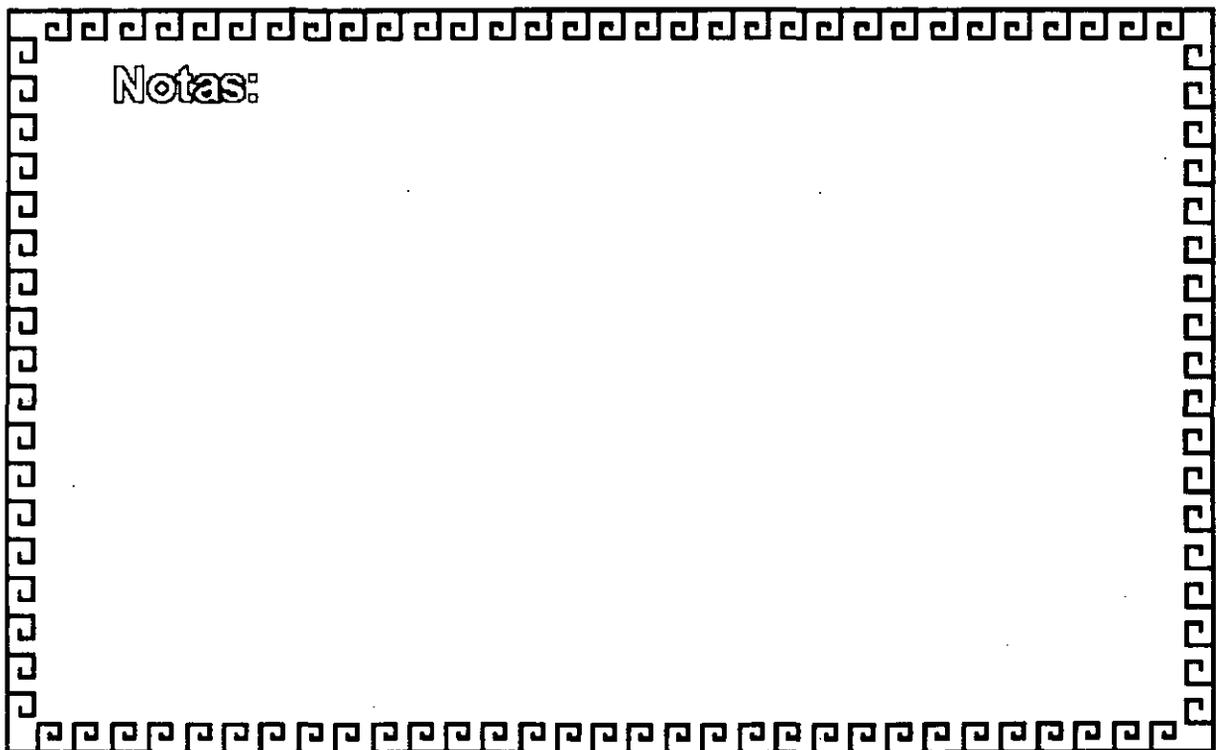
Protocolo OSPF

Open Shortest Path First

- Protocolo no propietario
- Divide las redes en
 - Area
 - Sistema Autónomo
 - Sistema Global
- Sistema de seguridad para la propagación de las rutas disponibles
- Uso de diferentes tipos de métricas

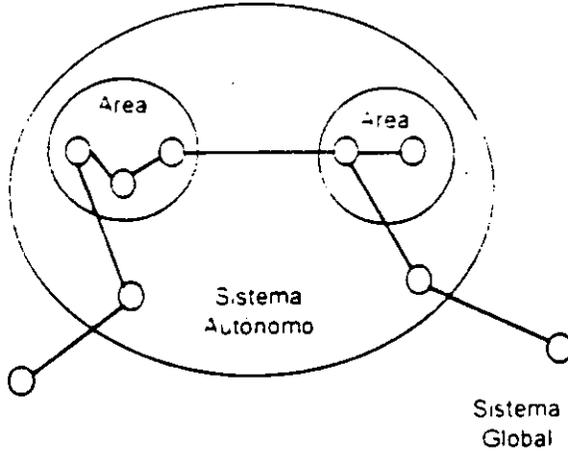


Notas:



Protocolo OSPF

Divisiones o particiones



Notas:



Nivel 4. Protocolos de Transporte

El nivel de transporte provee a una máquina con conexiones punto a punto independientes de la subred y servicios de transacción

Provee enlaces confiables y eficientes entre procesos

Forma en conjunto con los niveles inferiores una robusta plataforma de comunicaciones

Realiza los enlaces virtuales

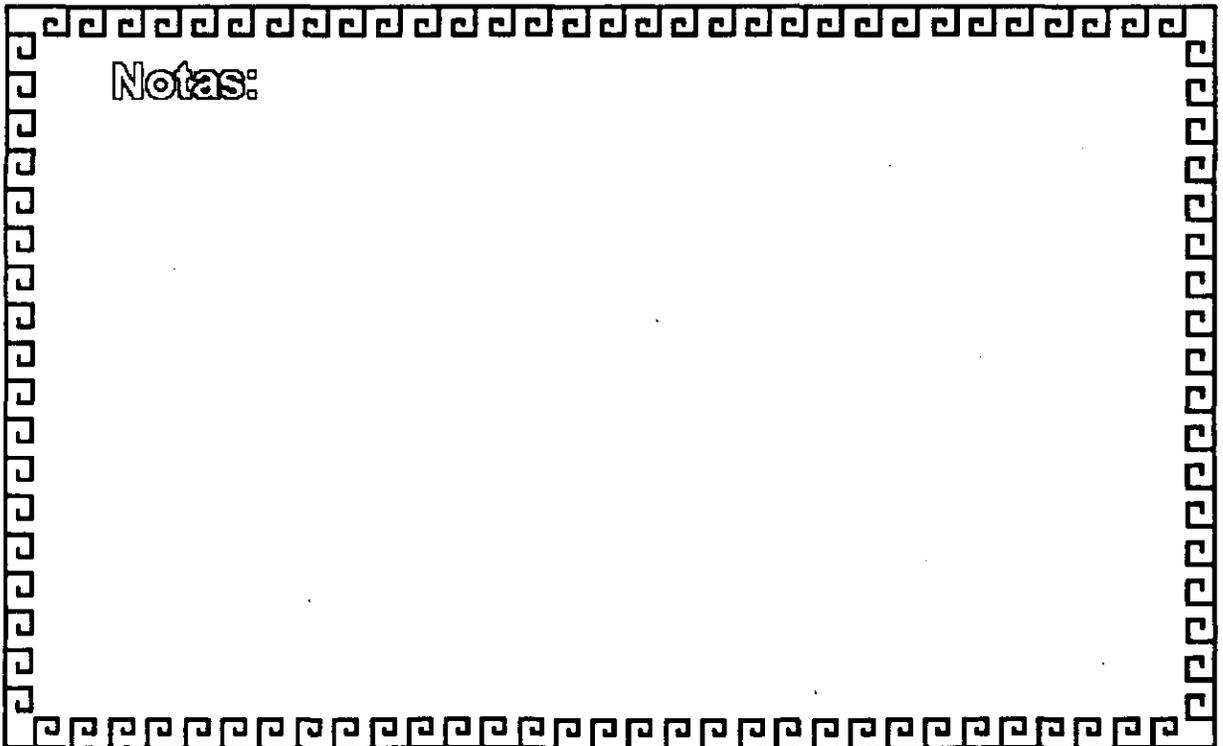
Tiene dos protocolos principales

TCP

UDP



Notas:





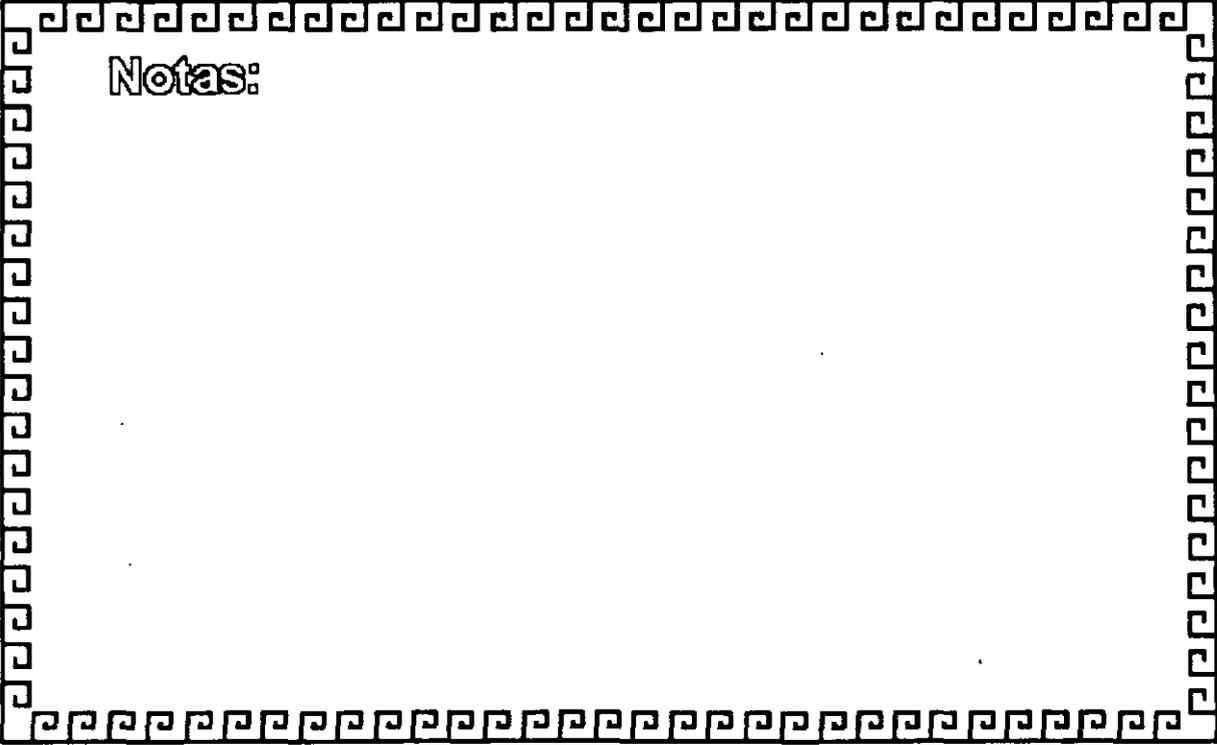
Protocolo TCP

Transmisión Control Protocol

- Asignación de números de puerto para transmisión de datos
- Reconocimiento de Datos recibidos
- Regulación del flujo de datos
- División de los mensajes en datagramas
- Verificación de los datagramas

Administración

- Establecimiento
- Mantenimiento
- Terminación



Notas:



Protocolo UDP

User Datagram Protocol

UDP brinda servicio de datagramas a los programas del usuario
No garantiza una transferencia confiable de los datos
Envia/Recibe datos. sin capacidad de retransmisión
Supone que la aplicación de mas alto nivel realiza la validación

Utilizado por:

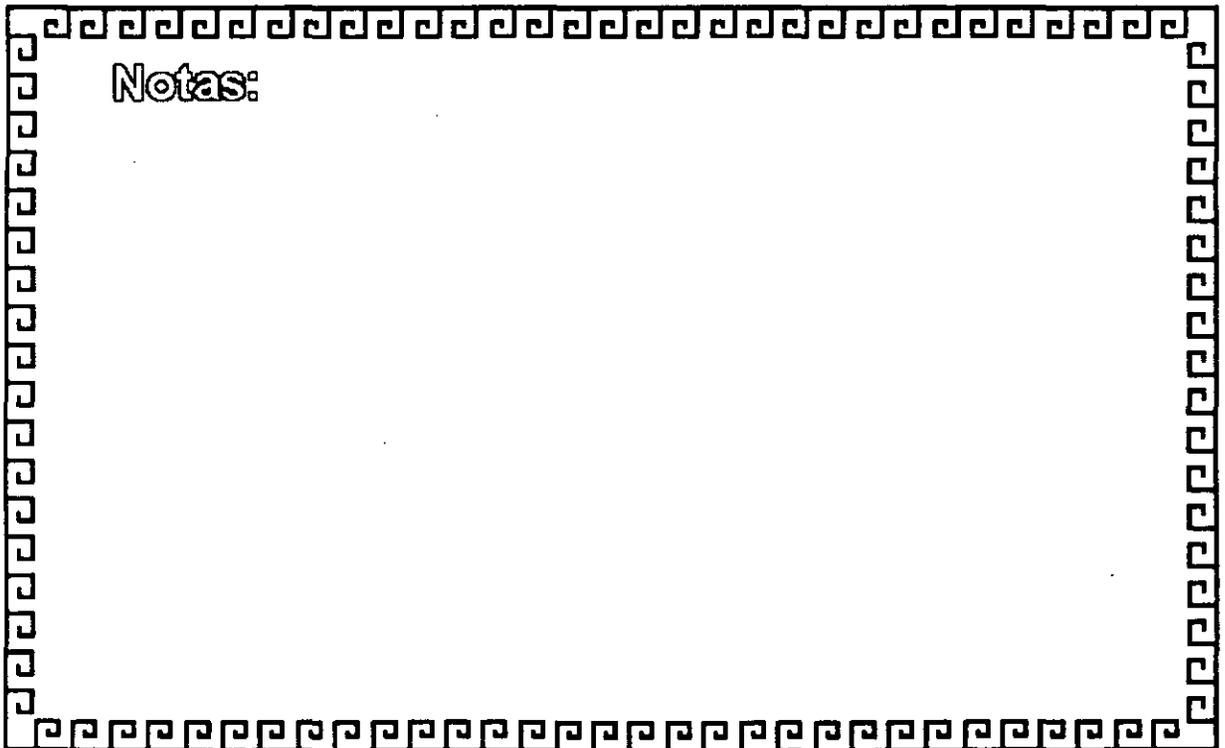
NFS (Network File System)

SNMP

TFTP



Notas:





Protocolo NVP

Network Voice Protocol

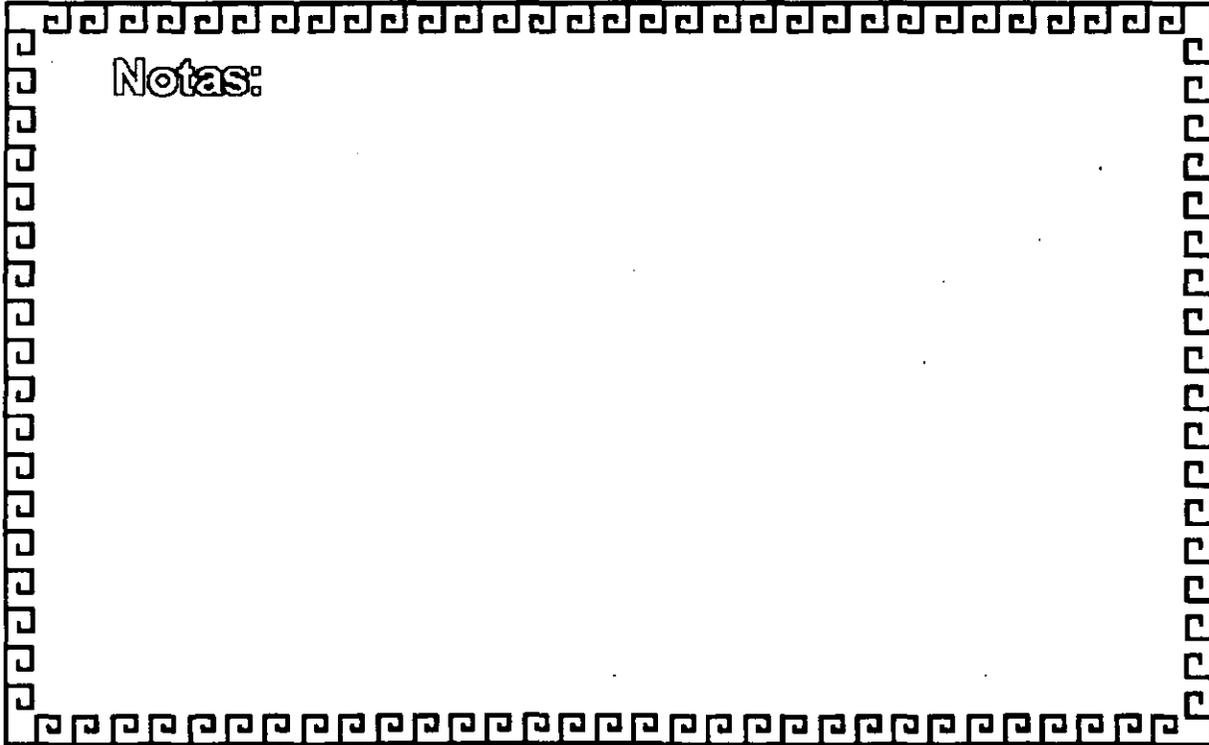
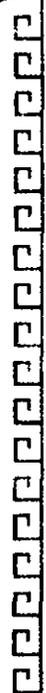
Servicio para transporte de voz digitalizada

Protocolo de transacción de tiempo real

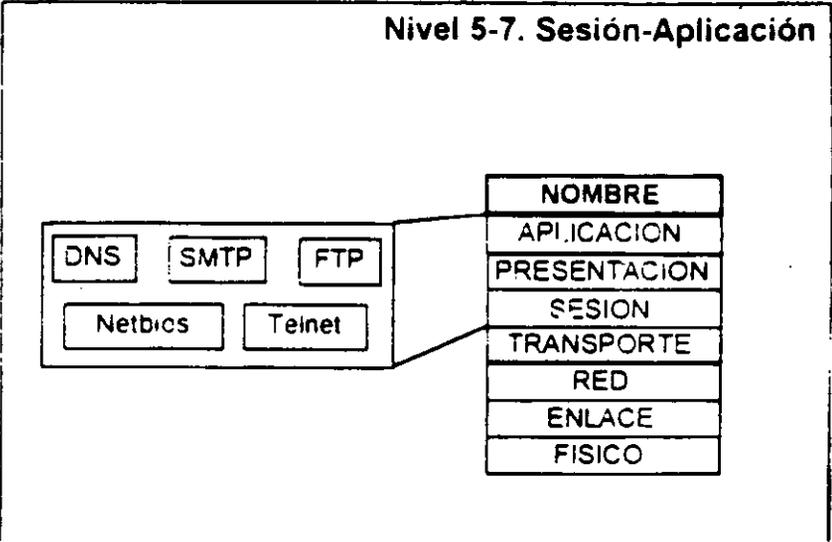
Utiliza IP para transmitir Información

Emplea algoritmos de compresión

Es connection less



Notas:



Notas:

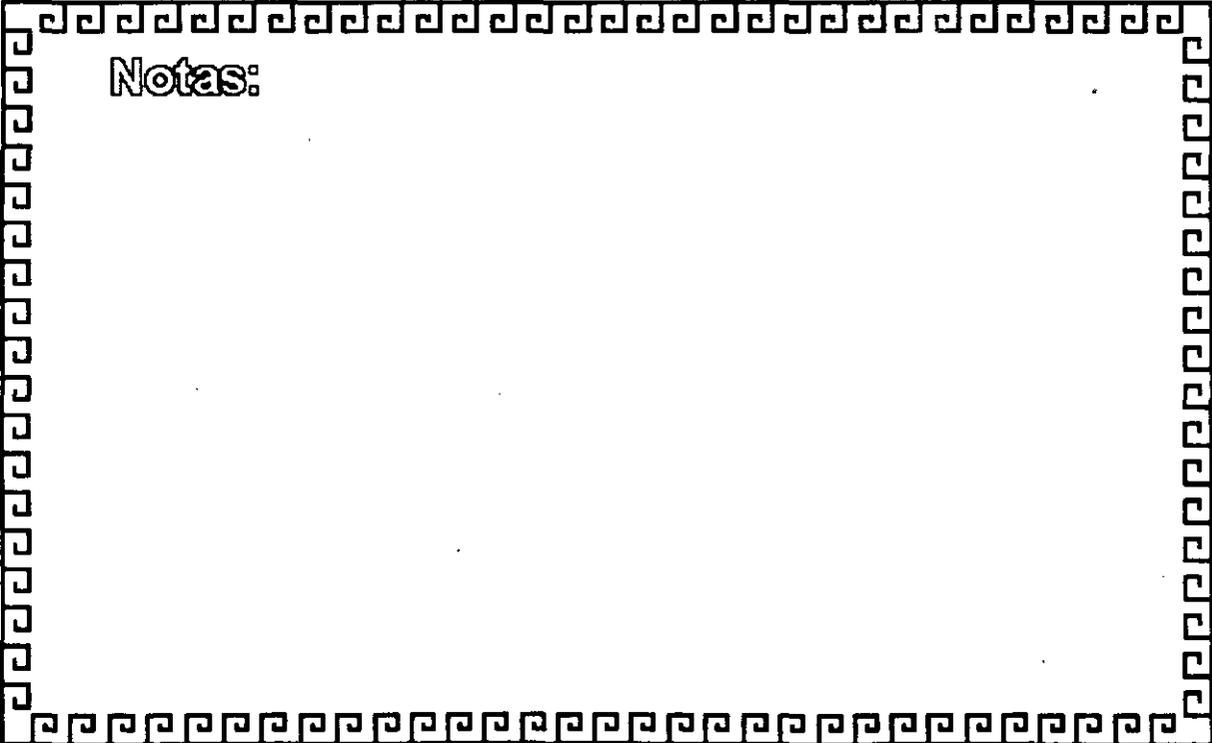


Protocolo Telnet

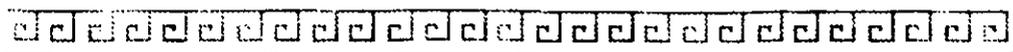
Protocolo de Acceso Remoto e Interactivo de terminal

Brinda una conexión virtual a nodos remotos

Permite a los usuarios acceder nodos remotos, como su fueran terminales "Físicamente Conectadas" a el Host



Notas:



Protocolo Telnet

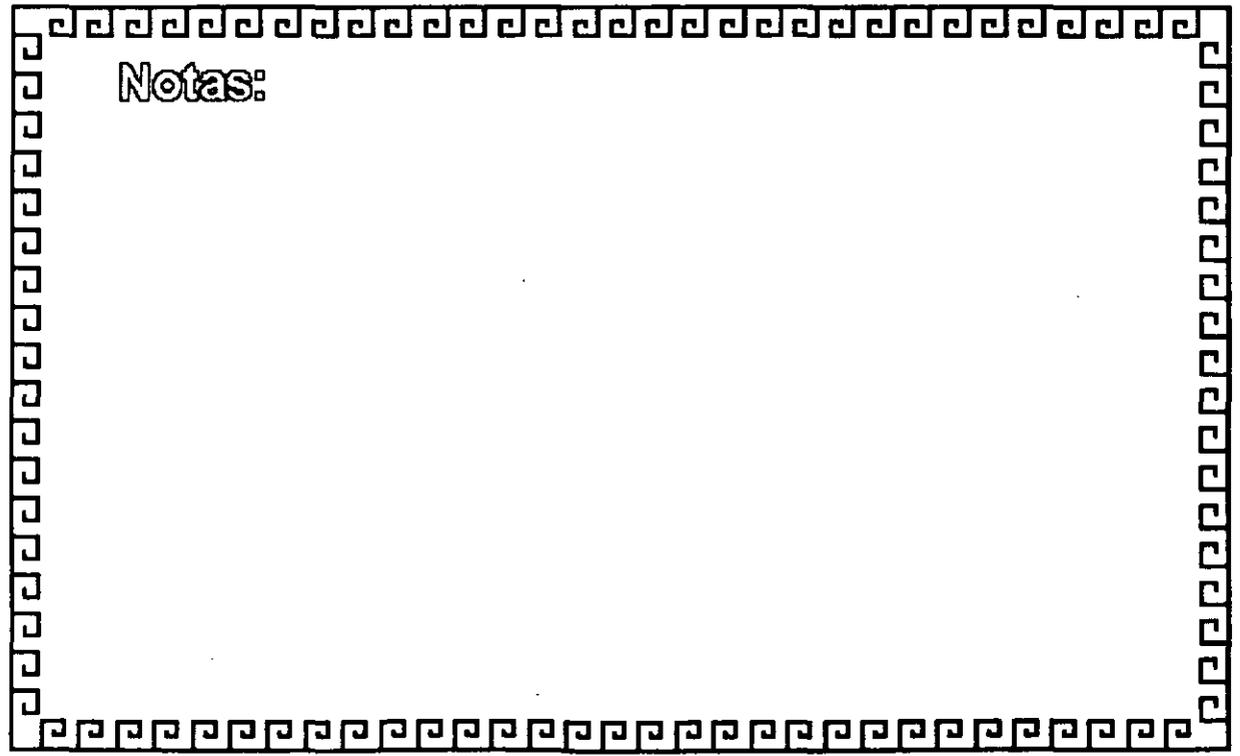
Ejemplo

```
Telnet>open apollo1
Trying...open
Connected to apollo1
Escape Character is '^]'

Username:
Password:
```



Notas:

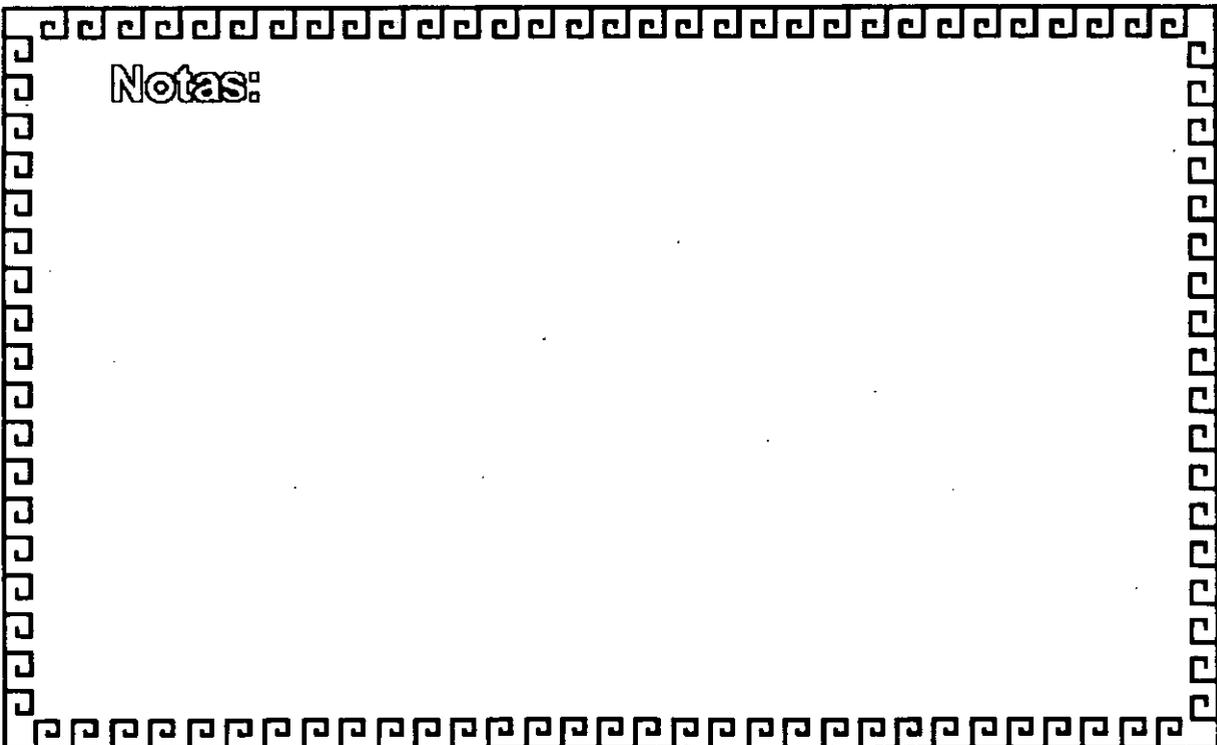




Protocolo Telnet

Comandos

open	Conectarse a un host
close	Cerrar sesion actual
escape	Definir caracter de escape
exit	Fin de telnet
local echo apagado)	Cambio de eco (Encendido,
status	Información de cada sesión
?	Ayuda



Notas:



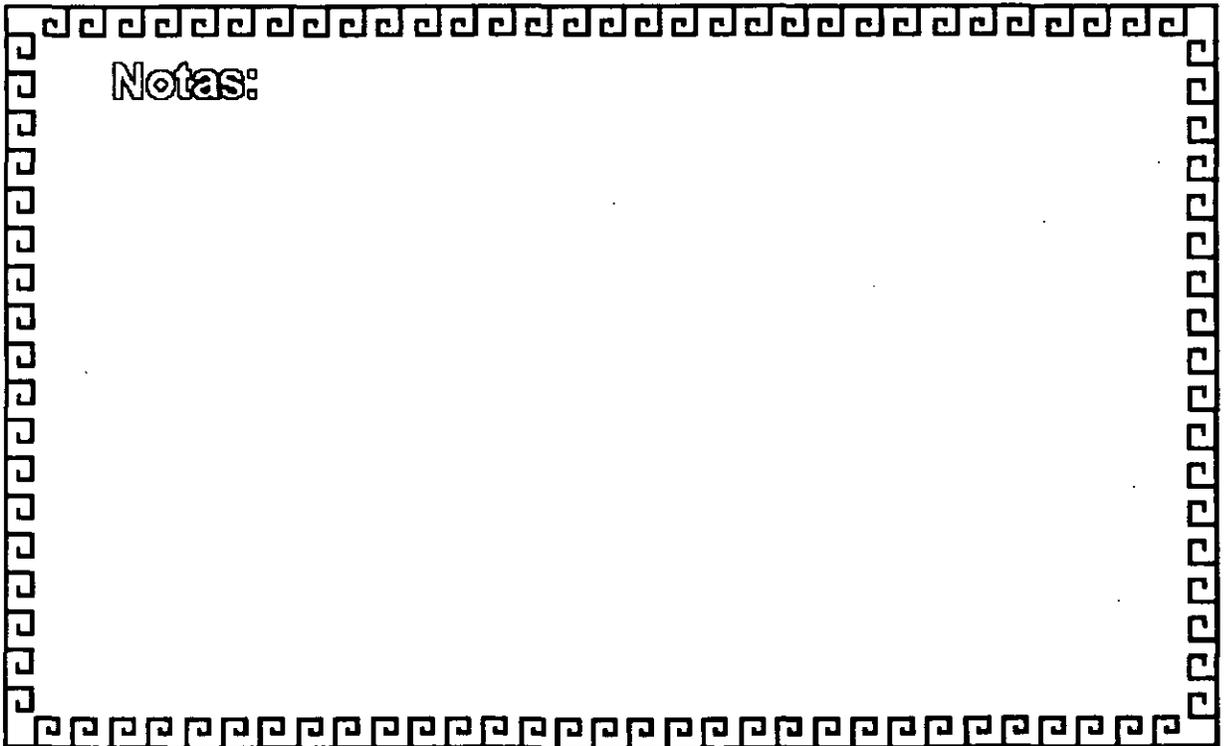
Protocolo FTP

File Transfer Protocol

- FTP permite el envío y recepción de uno o mas archivos en forma interactiva
- Soporta formatos de archivo en ASCII, Binario y EBCDIC
- Modo de transmisión: "Stream", Bloque o comprimido
- Permite las manipulaciones sencillas dentro de los sistemas de archivos Locales y Remotos



Notas:

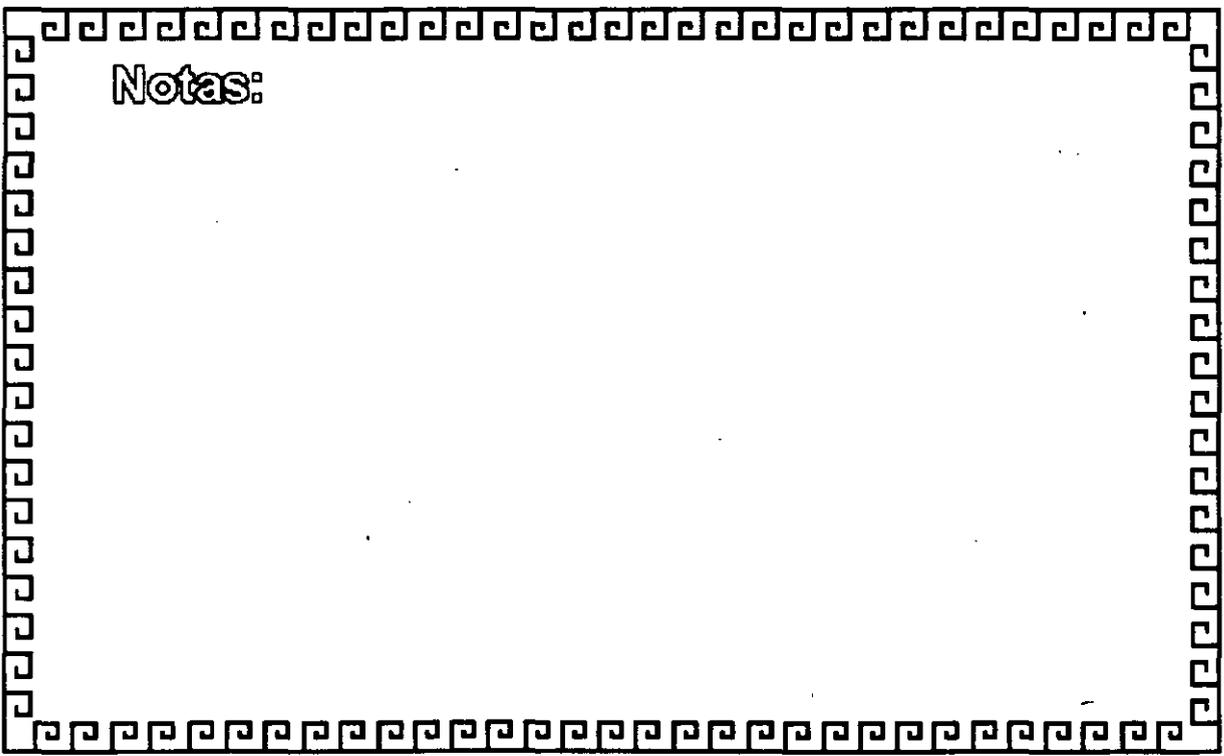




Protocolo FTP

Ejemplo

```
$ftp
* open vax1
Name:
<Enter PASS Comand)
Password
<User logged inn. default directory)
.
*get remotefile local.file
*put local.file mewfilename
bye
$
```



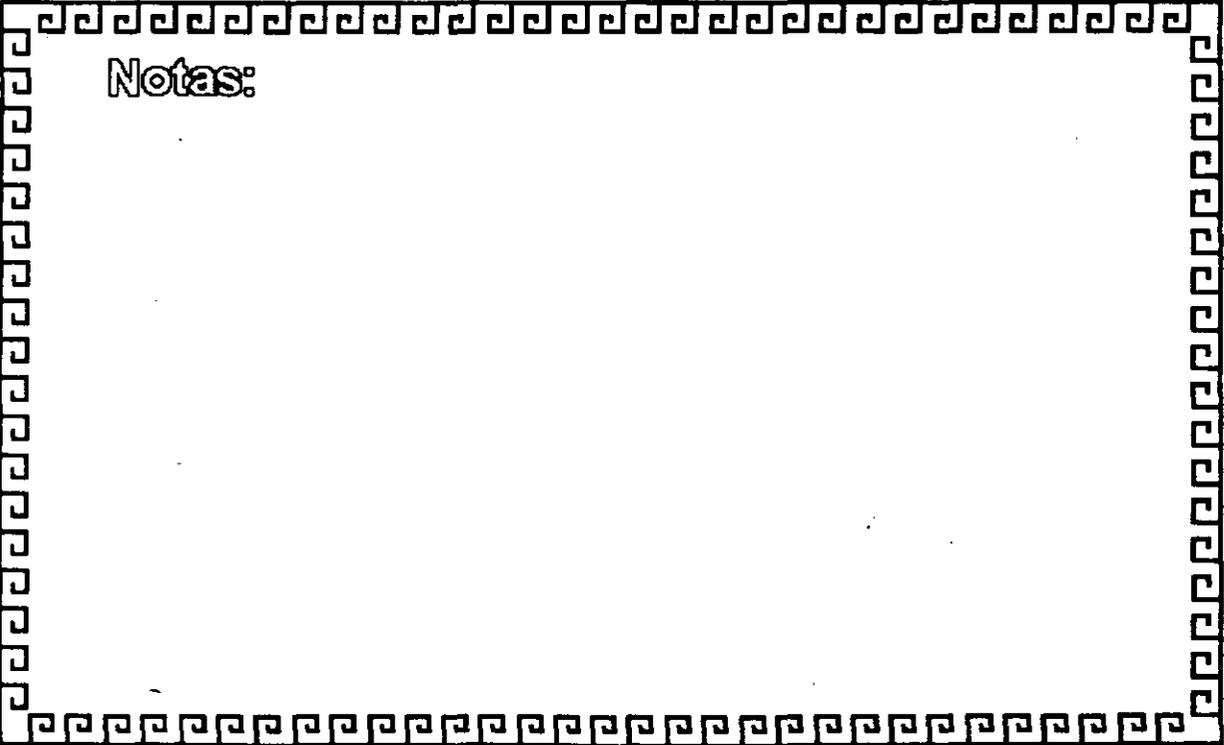
Notas:



Protocolo NFS

Network File System

- Originado y popularizado por SUN Microsystems
 - Diseñado para ser portado fácilmente a diferentes sistemas operativos
 - Brinda acceso transparente a sistemas remoto de archivos
 - Los usuarios no necesitan saber la localidad física de los discos
- 



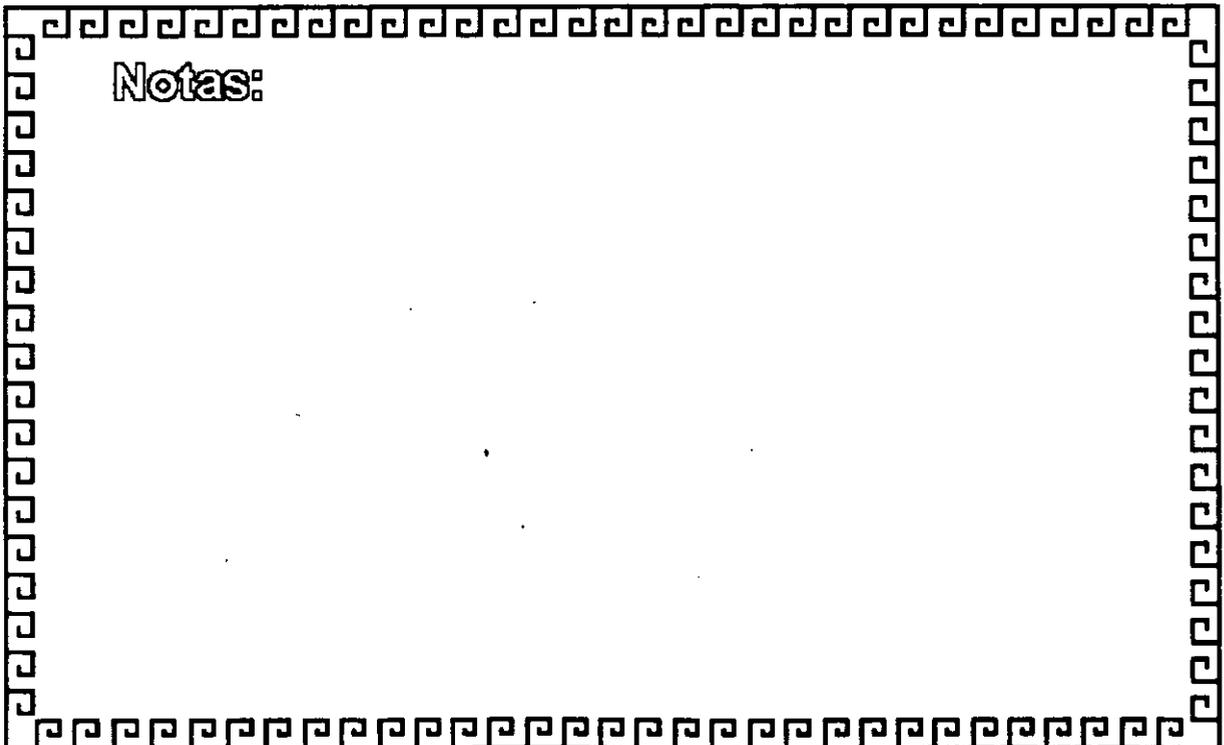
Notas:



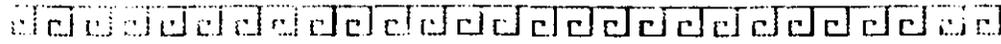
Protocolo SMTP

Simple Mail Transfer Protocol

- Un de los protocolos mas implementados
 - Define como transmitir mensajes entre 2 usuarios
 - Se basa en Spooling para el envio de Mensajes
 - Se conoce como envio de mensajes punto a punto
 - Describe la estructura del mensaje y especifica el protocolo para el intercambio de correo
- 



Notas:



Servicios de Nombramiento

Hosts

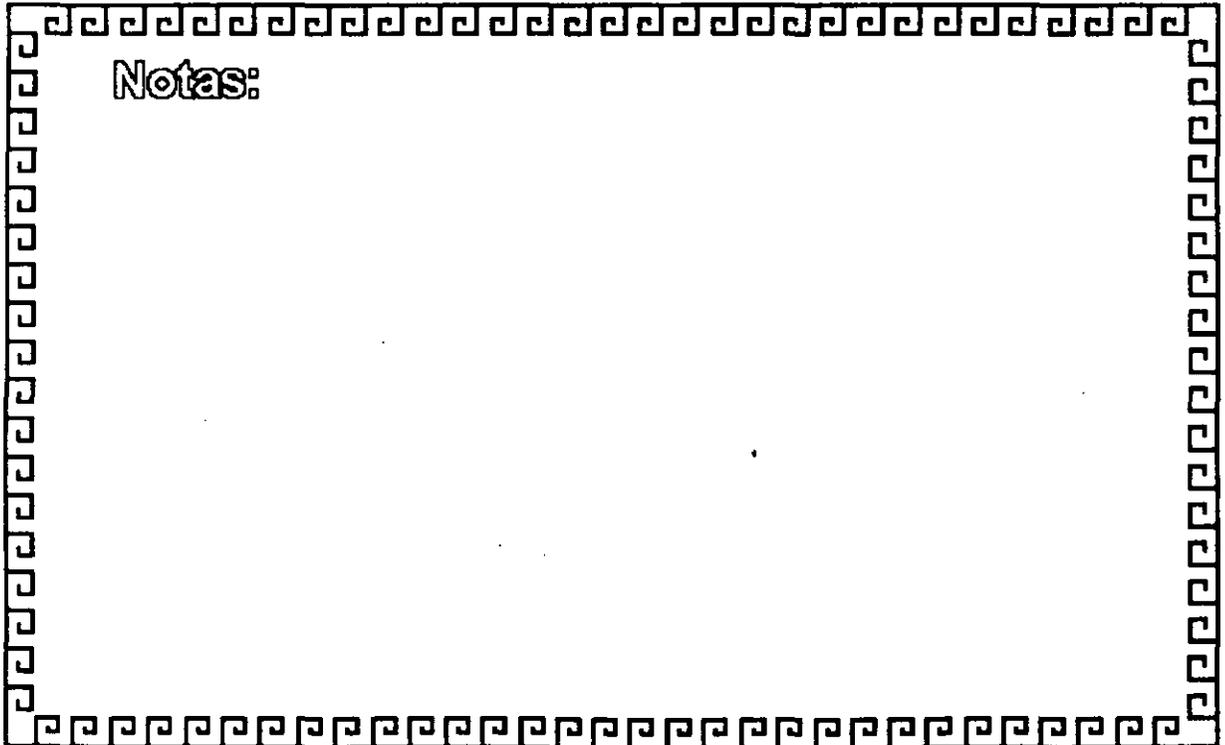
Contiene relación de nombres y direcciones IP sobre cada nodo de la red

Name Service

Un servicio central de nombramiento. El archivo de nombres en el servidor es similar al archivo de "HOSTS"

Domain Name Service

Sistema descentralizado de nombramiento
Utiliza varios archivos para resolver las direcciones de IP
Especificación RFC 1032-1034



Notas:



DNS

Domain name Service

Protocolo de nombramiento

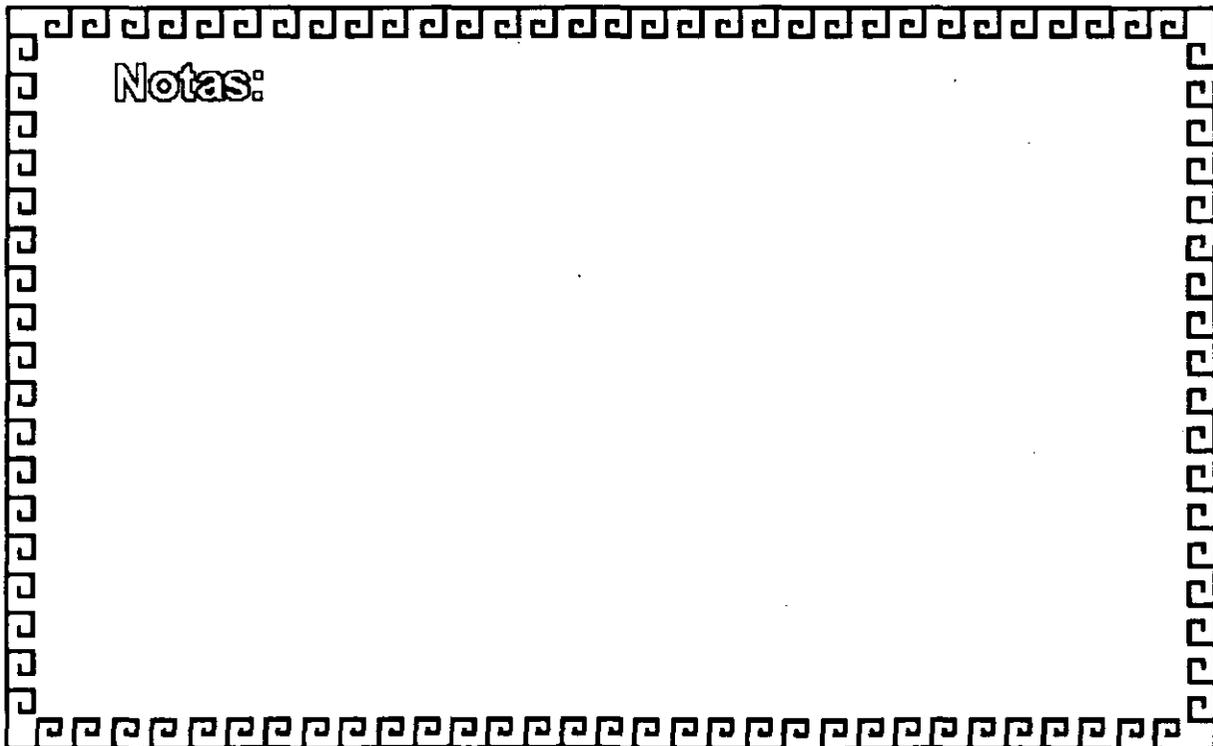
Brinda traducción de nombre-dirección IP

Dominio: Grupo de Hosts

"Domain Name Server"



Notas:





Domain Name Service

Información del servidor

Dirección Internet

Tipo de computadora

Lista de servicios brindado por computadoras

Servidor

Servidores Maestros

Primario

Secundario



Notas:





TCP/IP Sobre X.25

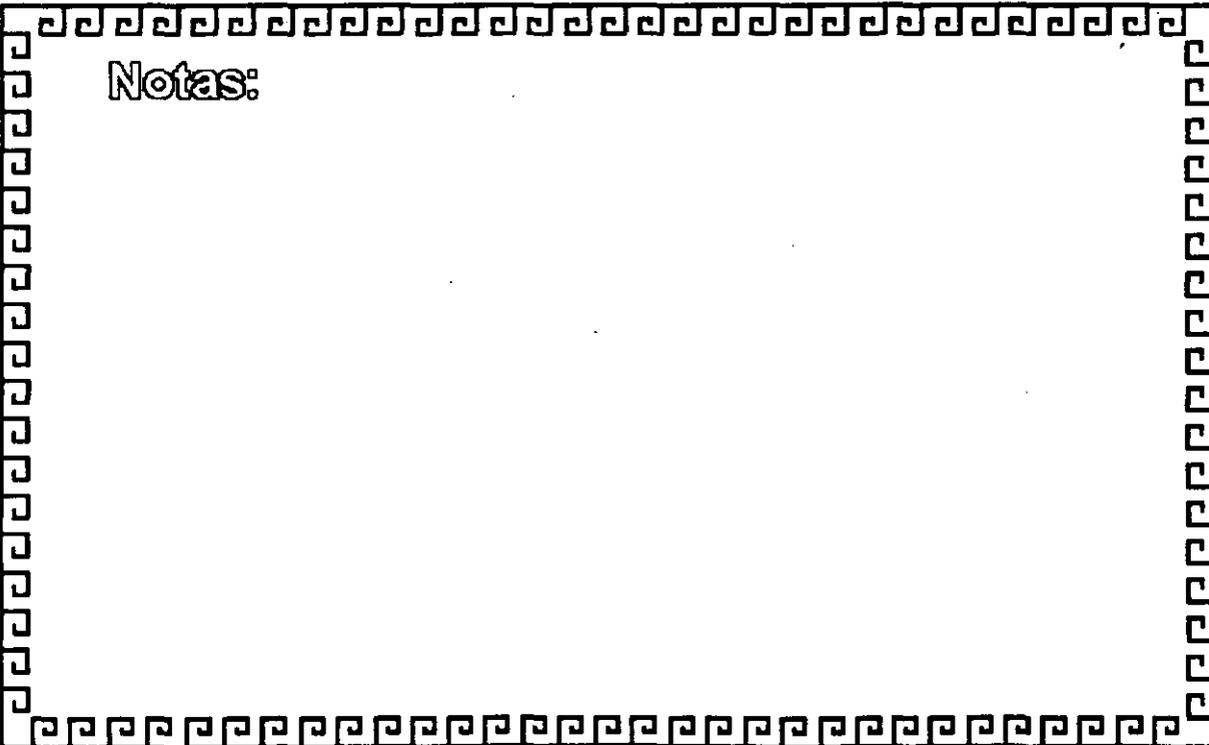
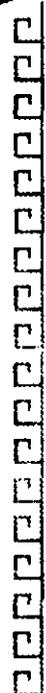
Implementacion de TCP/IP para redes de area amplia

2 opciones interno o externo

Generalmente con conexiones dinamicas

En caso de no usar la linea esta se desconecta temporalmente

La fragmentación la realiza X.25



Notas:

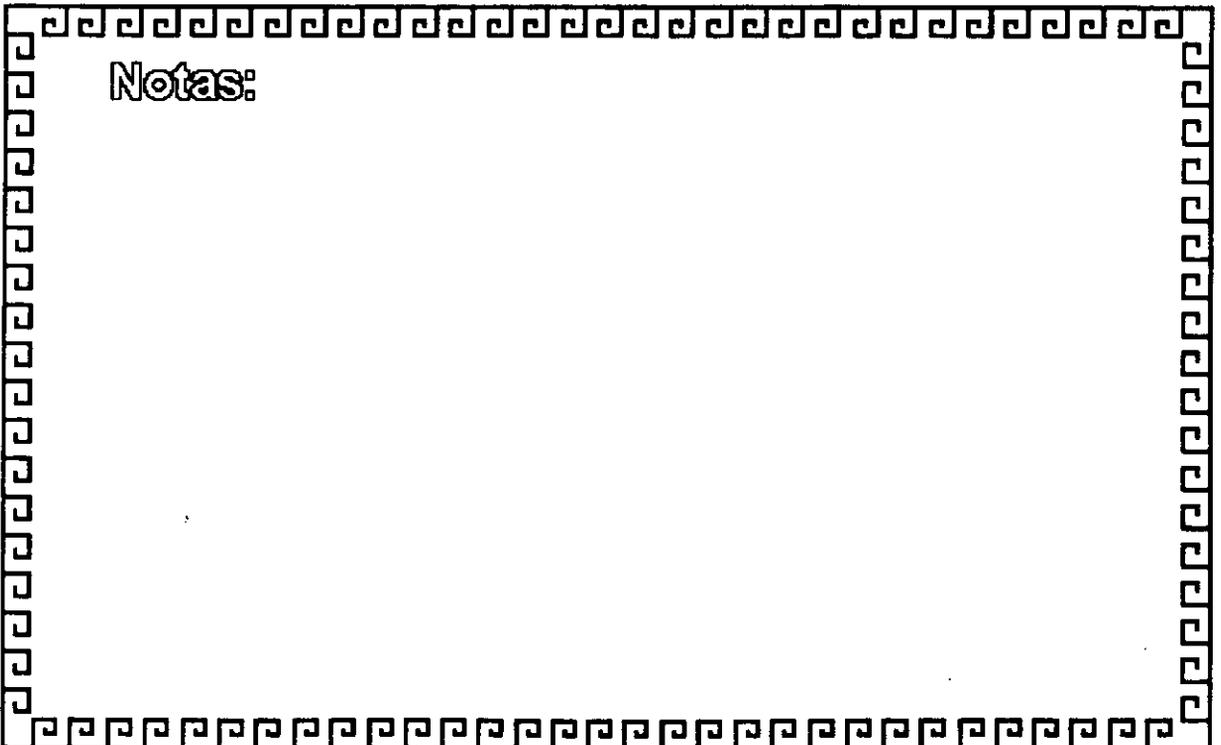


TCP/IP Sobre X.25

Se requiere tablas de conversion para determinar equivalencias entre X.25 y TCP/IP

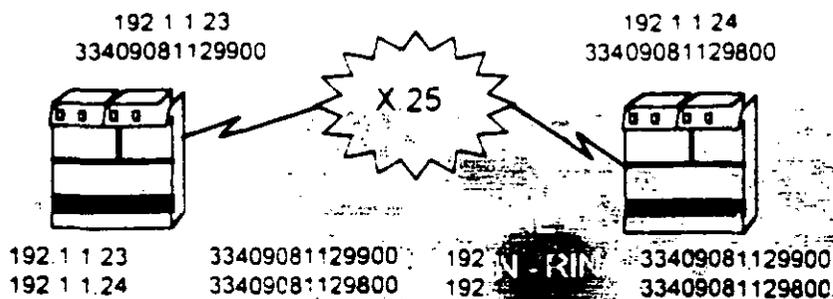
Ejemplo

192.1.20.3	33409081129900
192.1.21.5	38219087113800



Notas:

TCP/IP Sobre X.25



Notas:



SNMP



Simple
Network
Management
Protocol

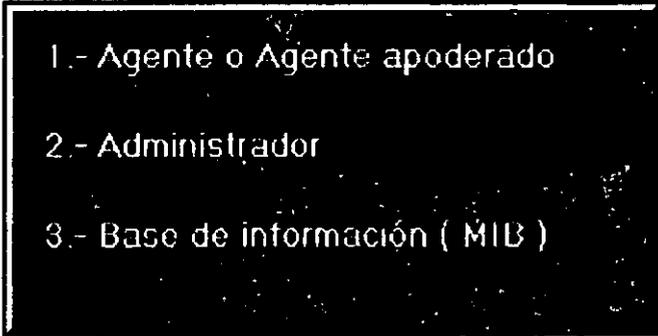


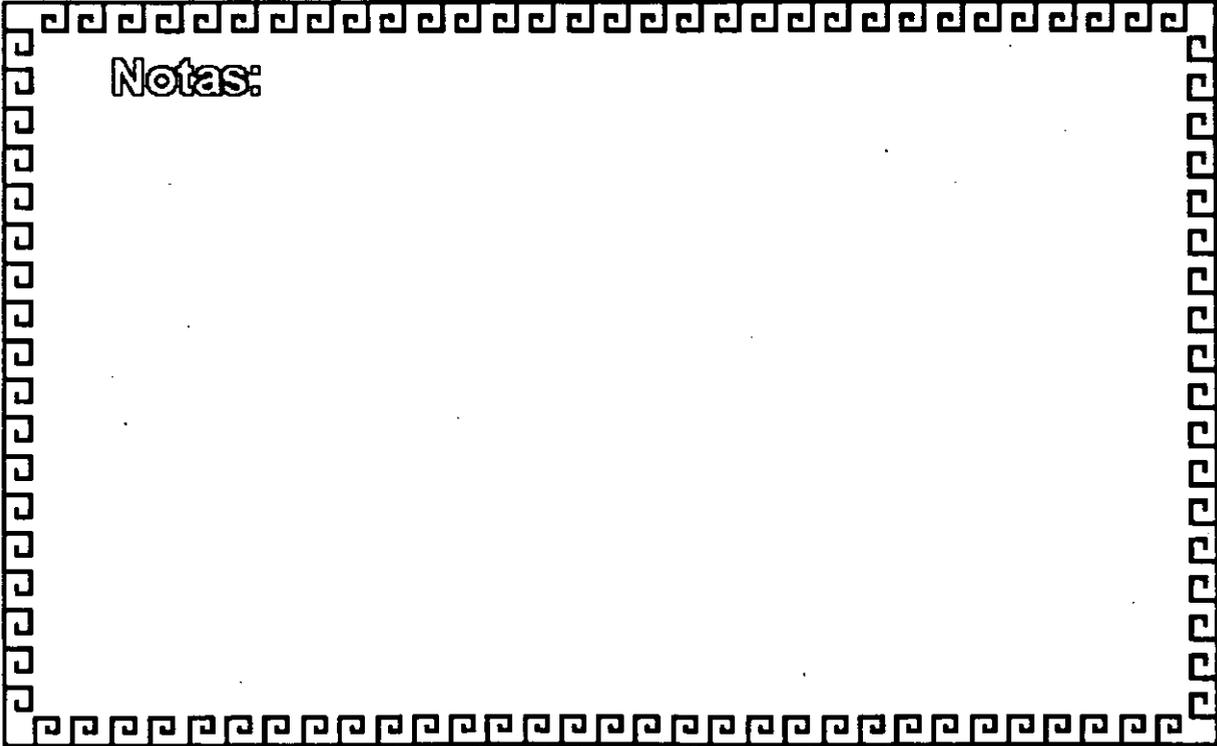
Notas:



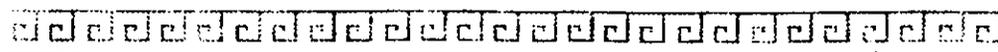
SNMP

COMPONENTES

- 
- 1.- Agente o Agente apoderado
 - 2.- Administrador
 - 3.- Base de información (MIB)



Notas:

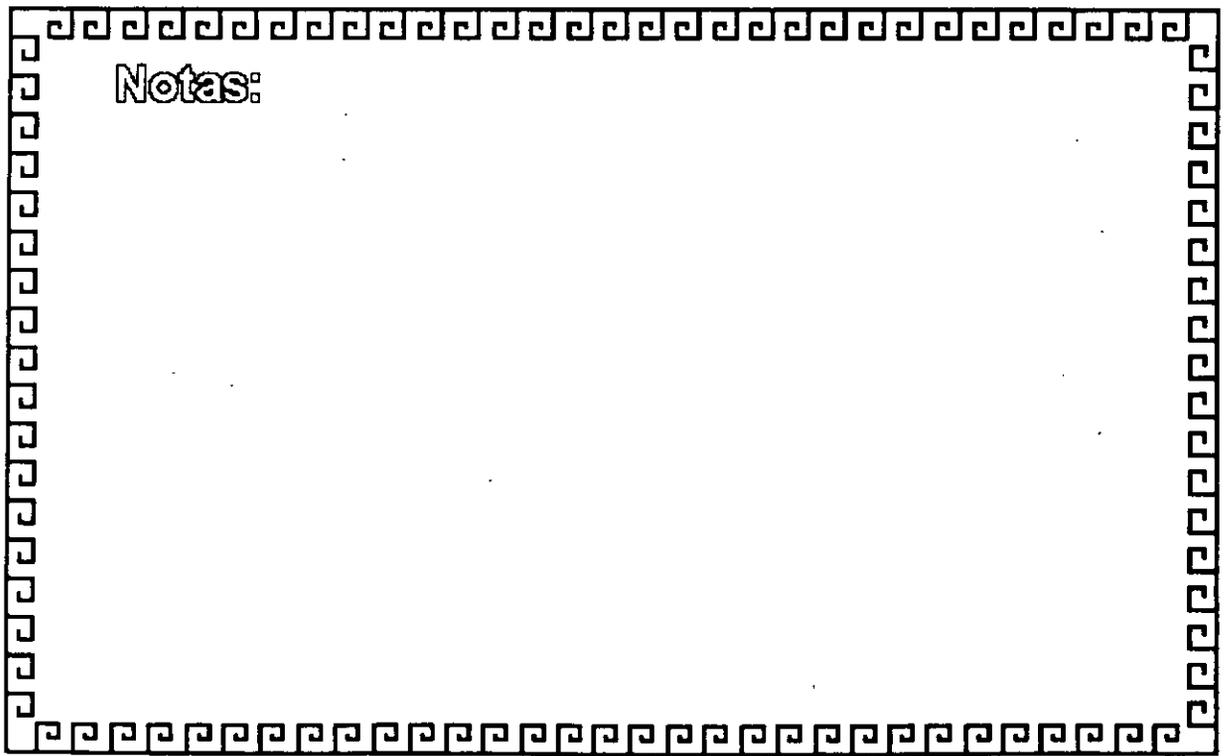


SNMP

Agente o Agente apoderado

- * Dispositivo compatible con SNMP
- * Monitor de comunicaciones
- * Informa sobre periféricos

El agente apoderado es además un conversor de protocolo.

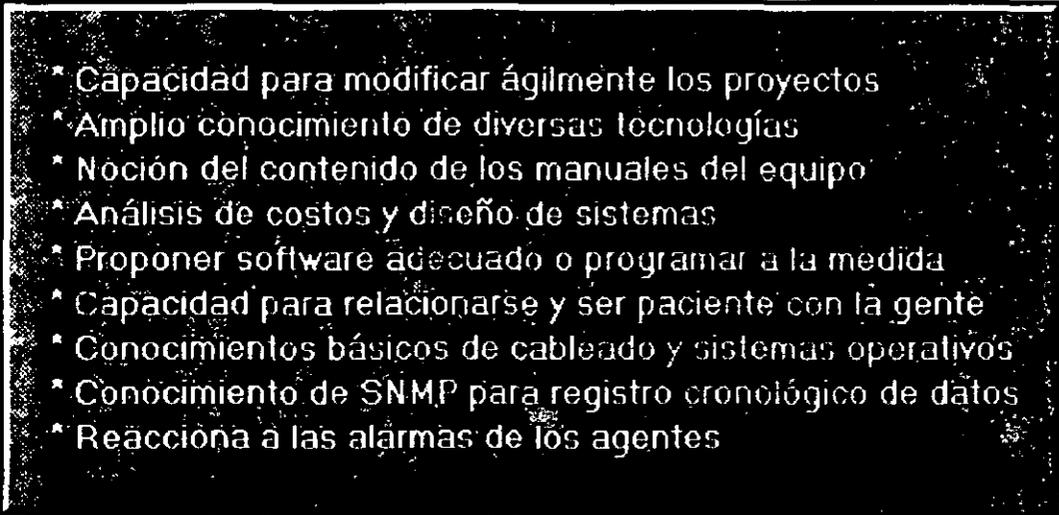


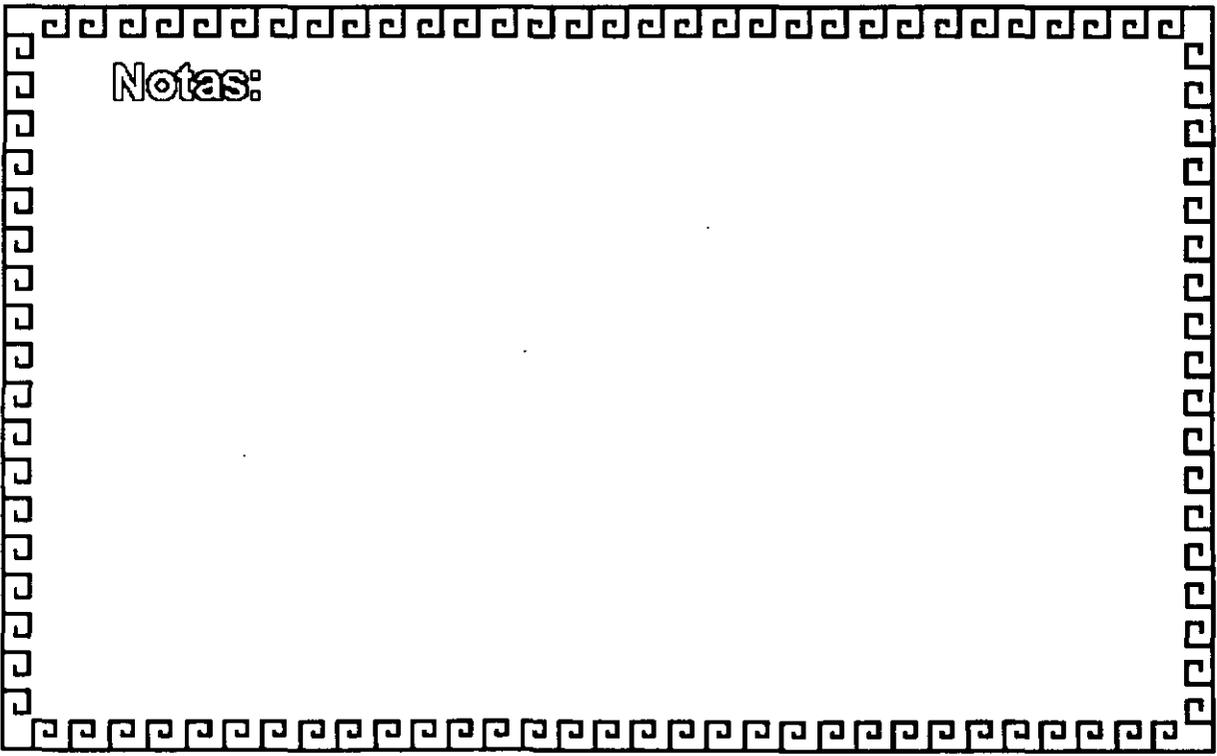
Notas:



SNMP

CARACTERISTICAS DESEABLES DE UN ADMINISTRADOR DE RED

- 
- * Capacidad para modificar ágilmente los proyectos
 - * Amplio conocimiento de diversas tecnologías
 - * Noción del contenido de los manuales del equipo
 - * Análisis de costos y diseño de sistemas
 - * Proponer software adecuado o programar a la medida
 - * Capacidad para relacionarse y ser paciente con la gente
 - * Conocimientos básicos de cableado y sistemas operativos
 - * Conocimiento de SNMP para registro cronológico de datos
 - * Reacciona a las alarmas de los agentes
- 



Notas:

SNMP

BASE DE INFORMACION (MIB)

- Base de datos dentro del marco de SNMP
- Con cada enlace de comunicación existen recursos controlables
- Reside en cada agente o administrador
- Estándar 802.3 MIB de IEEE

Notas:

SNMP

COMANDOS

- * Es un protocolo de Estímulo-Respuesta
Tiene tres verbos principales:

Set, get y trap

GetRequest - Pide información al agente

GetResponse - Contesta al administrador

- *SetRequest - Para controlar los dispositivos

Trap - Alerta en caso de problemas

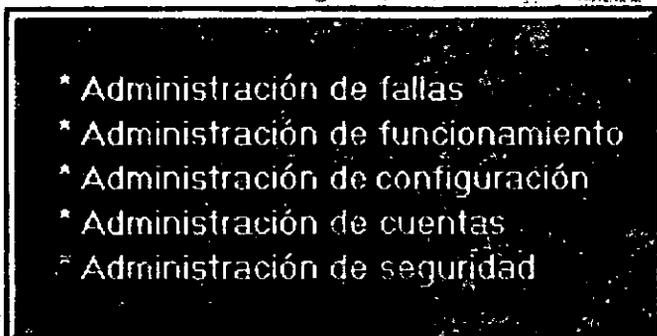
Set puede afectar el funcionamiento de la
red

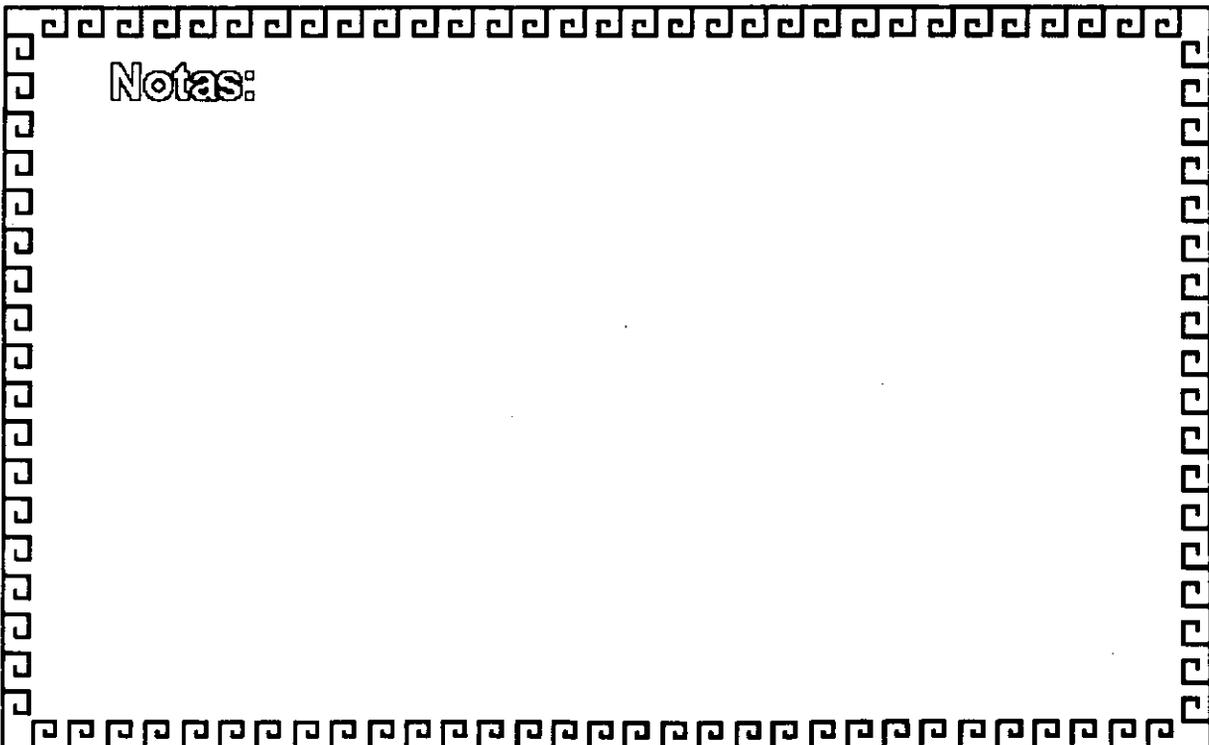
Notas:



SNMP

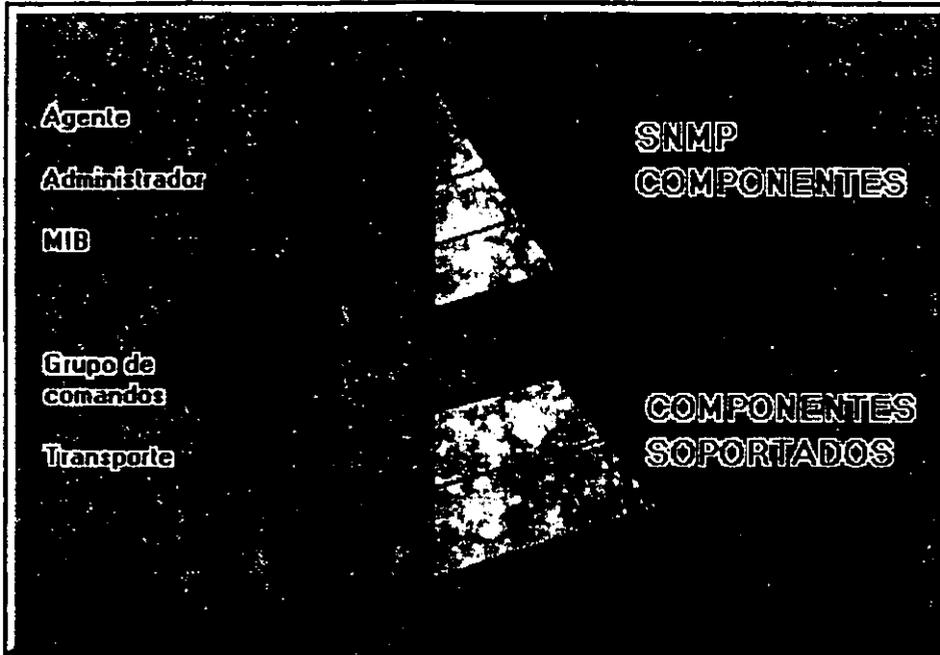
EL ADMINISTRADOR

- 
- * Administración de fallas
 - * Administración de funcionamiento
 - * Administración de configuración
 - * Administración de cuentas
 - * Administración de seguridad



Notas:

COMPONENTES



Notas:



FDDI

TOKEN-PASSING OFRECE UNA TRANSMISION DE DATOS MAS EFICIENTE, YA QUE CONFORME AUMENTA EL TRAFICO SE REQUIERE UN MAYOR ANCHO DE BANDA. TRT 85 %

CSMA/CD RESULTA MAS EFICIENTE CUANDO SE UTILIZA UN MENOR ANCHO DE BANDA



Notas:

FDDI

FDDI emplea una codificación 4B/5B, tasas de transmisión a 100 Mb/S - 125 MHz, 80% de eficiencia en el ancho de banda.

ETHERNET Y TOKEN - RING emplea una codificación Manchester.

Tasa de transmisión - ETHERNET :	10 Mb/S - 20 MHz
- TOKEN RING :	16 Mb/S - 32 MHz

50% DE EFICIENCIA EN EL ANCHO DE BANDA

Notas:

FDDI

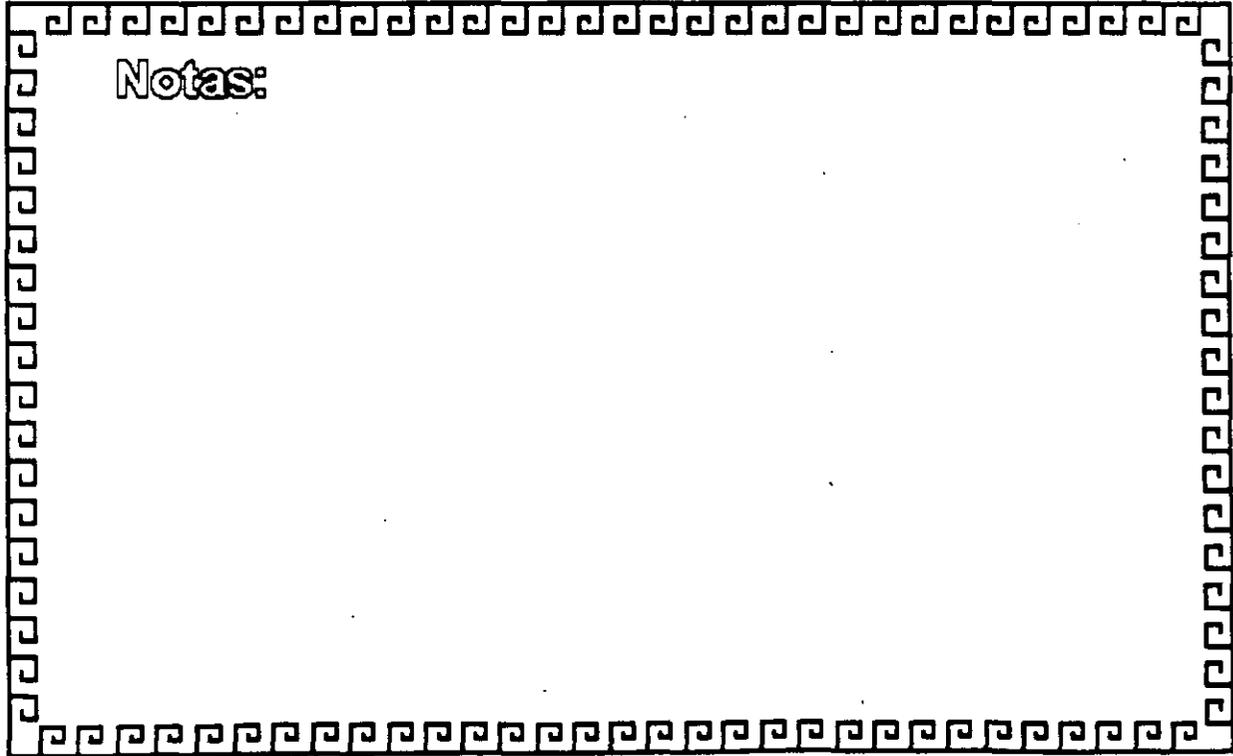
FDDI: VS. TOKEN - RING 16MB/S.	
Reloj distribuido recuperación de errores	{ Monitor Activo
Doble anillo	{ Anillo Sencillo
Rotación del "TOKEN "	{ Sistema de reservación por prioridad
Uso de Fibra Optica	{ Uso de Par Trensado/Fibra Optica

Notas:



FDDI

LA RED LOCAL OPTICA
DE ALTA VELOCIDAD



Notas:



FDDI

FIBER DISTRIBUTED DATA INTERFACE
RED ANILLO TOKEN-PASSING 100 Mb/s CON
REDUNDANCIA (ANSI-X3T9)
ANILLO PRINCIPAL = CONEXION PUNTO A PUNTO
ENTRE NODOS PARA
TRANSMISION DE DATOS
ANILLO SECUNDARIO = TRANSMISION DE DATOS/
RESPALDO DEL ANILLO
PRINCIPAL EN CASO DE FALLA
FDDI PROVEE COMUNICACIONES POR CONMUTACION
DE PAQUETES Y TRANSMISION DE DATOS EN
TIEMPO REAL



Notas:



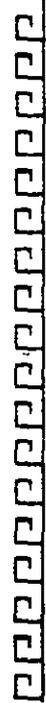
FDDI

CONSIDERACIONES

MANEJO
SMT (INTERFACE SNMP)
ESTADISTICA DE LAS ESTACIONES
RESET - SOPORTE PARA DESHABILITAR

300 KM - 180 MILES

EL CONTROL ES CRITICO PARA LAS REDES DE
GRAN TAMAÑO Y CAPACIDAD



Notas:



FDDI

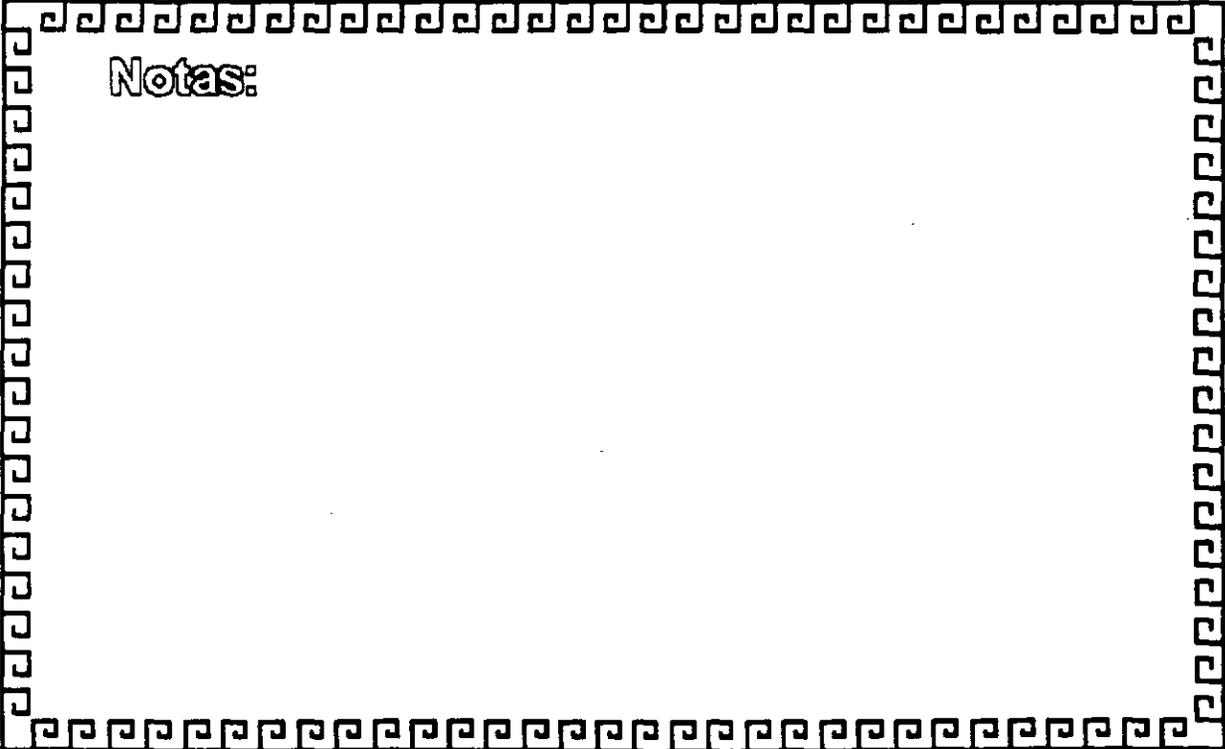
FDDI ofrece hasta 1000 conexiones físicas (500 Estaciones) y una distancia total de 200 Km. de extremo a extremo.

La distancia máxima entre nodos activos es la de 2 Km.

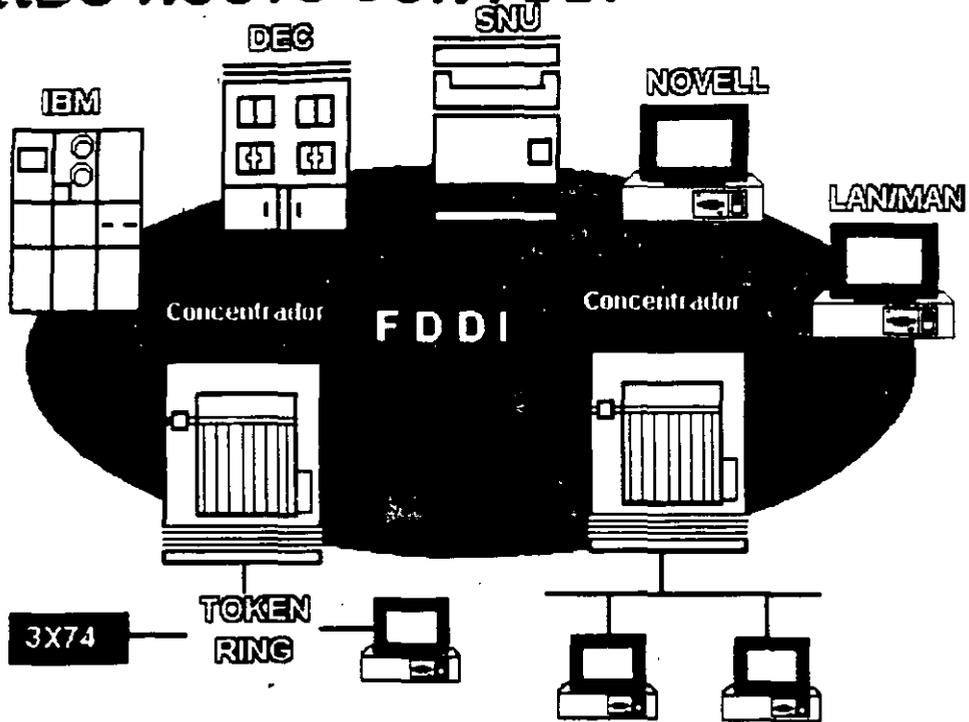
Fibras Ópticas empleadas:

- A) Fibra tipo unimodo, con gran ancho de banda (GHz) y largas distancia (20 - 30 Km.)
- B) Fibra tipo multimodo. Fibras con núcleo 50 - 62.5 Micras y Medianas distancias (10 - 20 Km.) a 1300 nanometros

Notas:



USANDO HOSTS CON FDDI



Notas:

Figura FDDI 5



FDDI

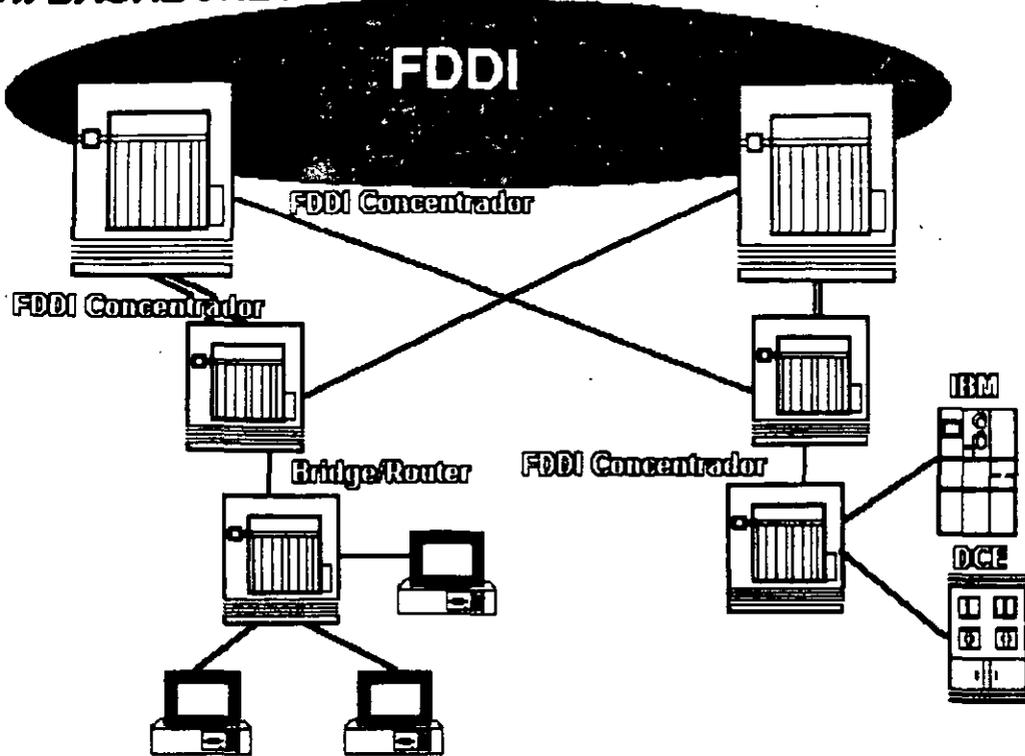
ESTACIONES	
TIPO CLASE A	SE CONECTA DIRECTAMENTE AL ANILLO DOBLE
TIPO CLASE B	SE CONECTAN AL CONCENTRADOR DE PUERTOS MULTIPLES EN RED ESTRELLA O ESTACIONES CON POSIBILIDAD DE CONEXION SENCILLA. LOS CONCENTRADORES PUEDEN SER CONECTADOS EN CASCADA



Notas:

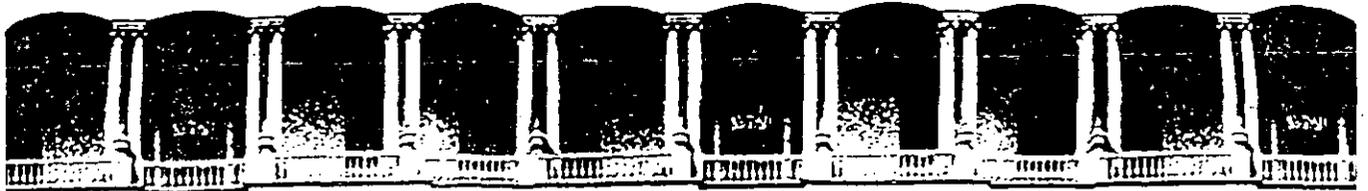
Figura FDDI 6

FDDI: BACKBONES TOPOLOGIAS



Notas:

Figura FDDI 7



**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

**REDES (LAN) DE MICROS PARTE II
(DIPLOMADO)**

MATERIAL COMPLEMENTARIO

MARZO, 1994



MODELOS

Nivel 1

NIVEL FISICO
Define cómo será transmitida la información binaria:

- Niveles de Voltaje
- Modulación
- Velocidad de Transmisión



Notas:

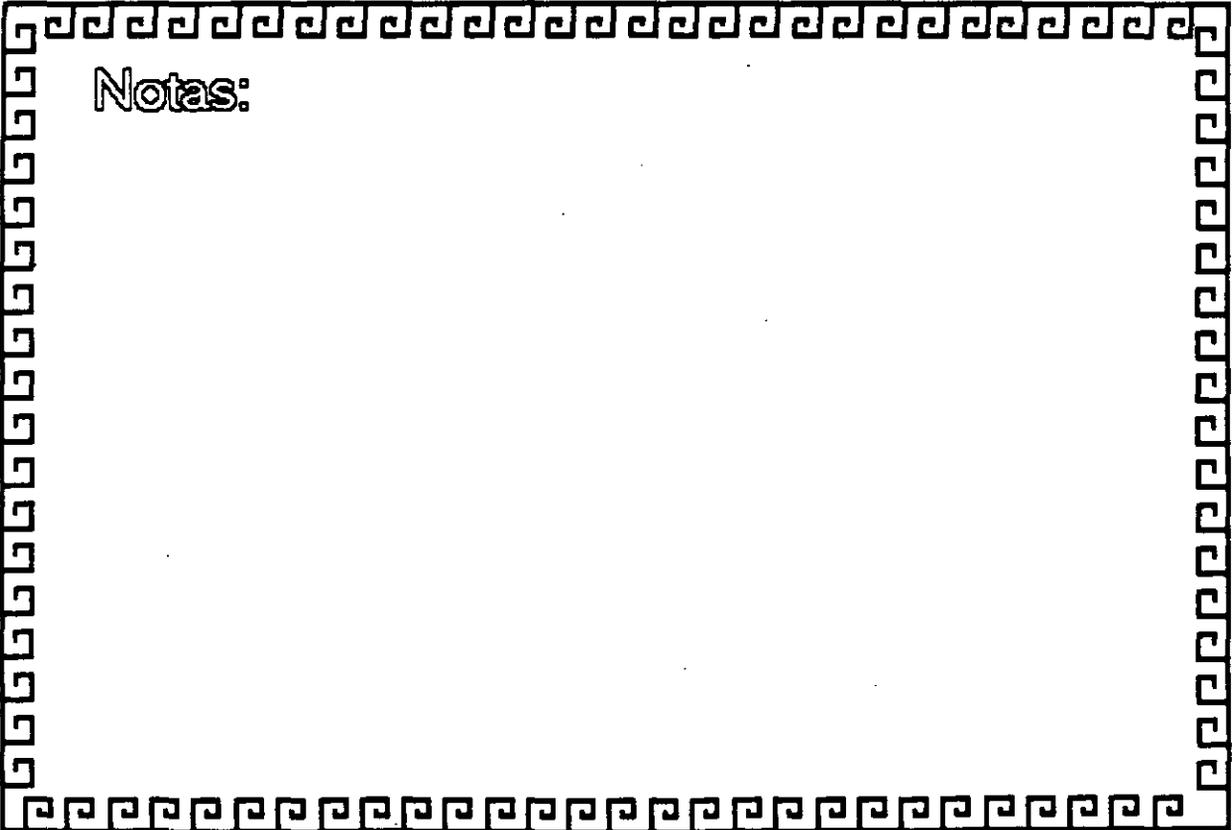
Figura 2-2



MODULOS

Nivel 3

NIVEL DE RED
Agrupa en paquetes y define qué camino toma cada paquete (enrutamiento).



Notas:

Modelo OSI

Nivel 5

NIVEL DE SESION

Define el procedimiento para iniciar la comunicación entre dos procesos a nivel de presentación.

Usualmente este nivel es la interface del usuario (y del software), de la RED.

Notas:

Nivel 6

NIVEL DE PRESENTACION

Realiza transformaciones en la información:

- **Conversión de Código**
- **Compresión**
- **Encriptación**
- **Conversión de Formatos de Archivo**

Notas:



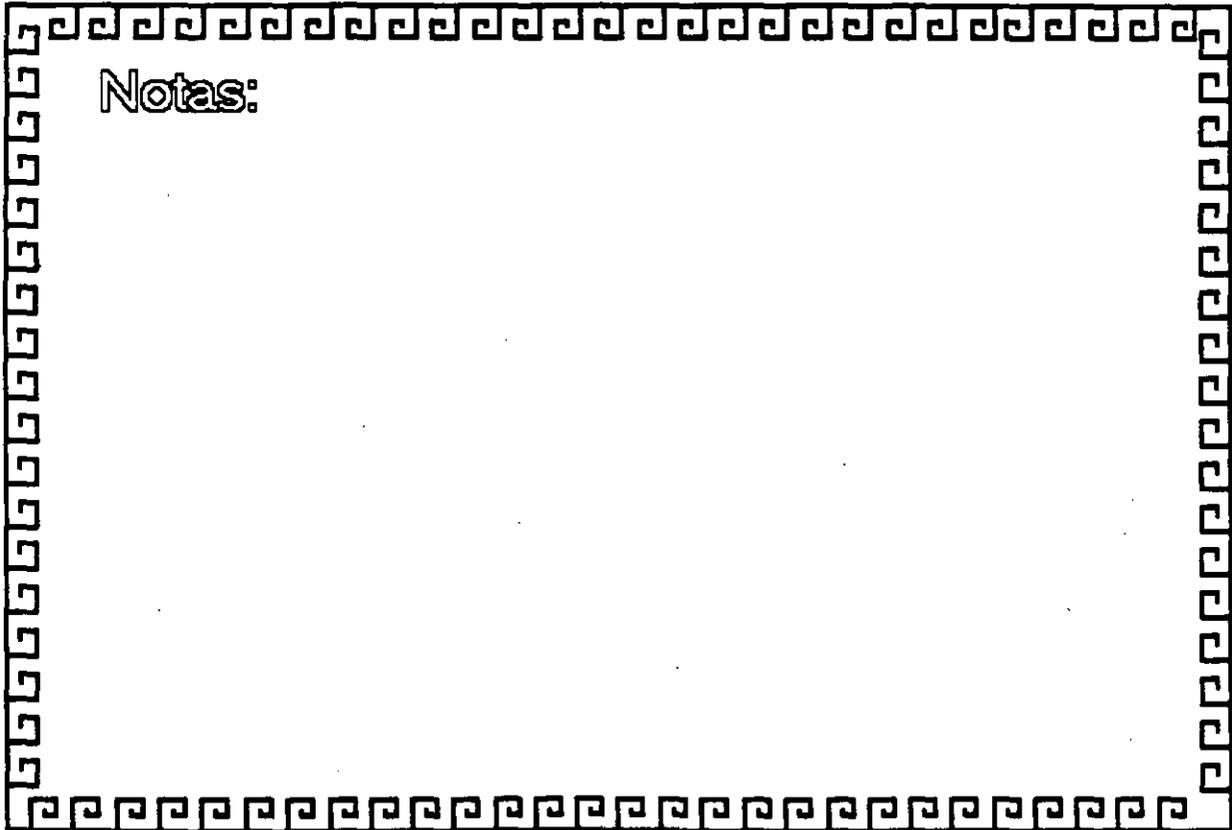
MODELO OSI

Nivel 7

NIVEL DE APLICACION

Provee servicios a los usuarios de la RED

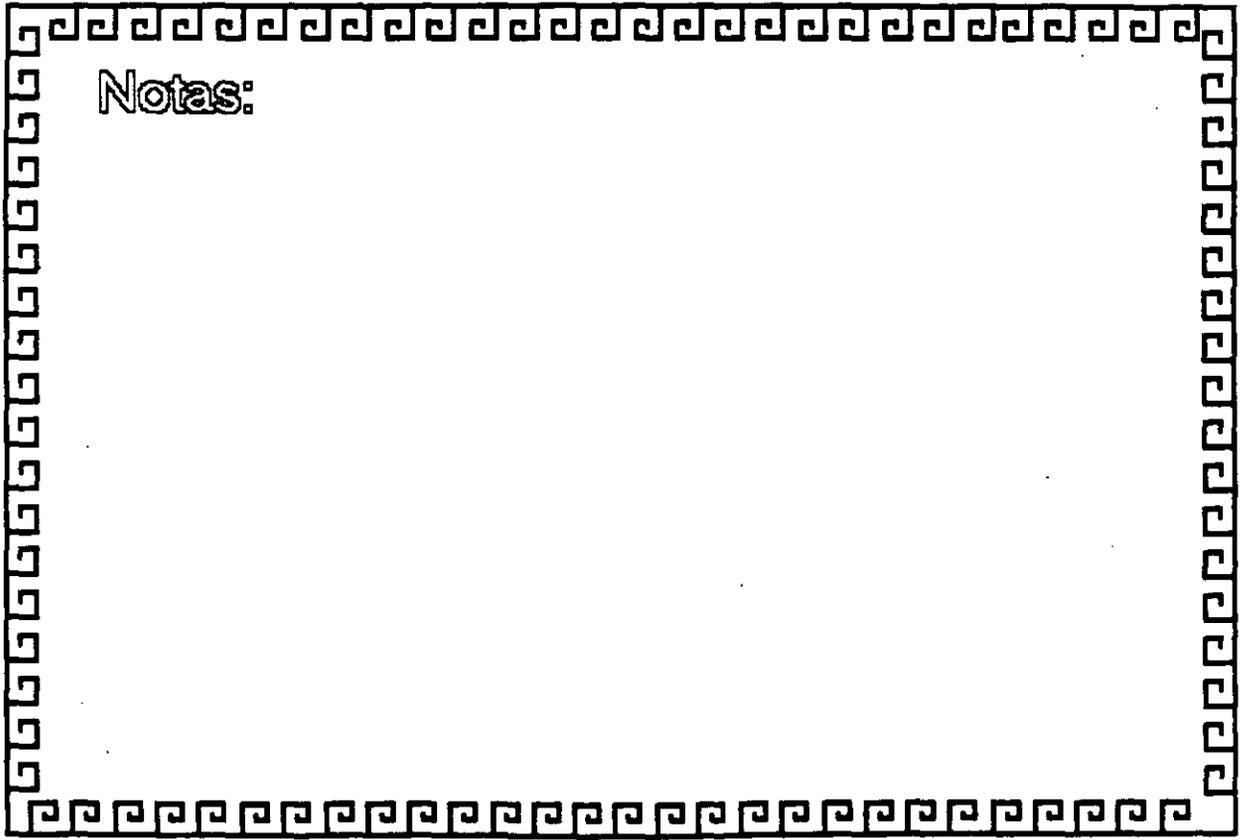
- Correo Electrónico
- Transferencia de Archivos
- Emulación de Terminales



Notas:



INSTALACION DE SISTEMAS
OPERATIVOS PARA RED



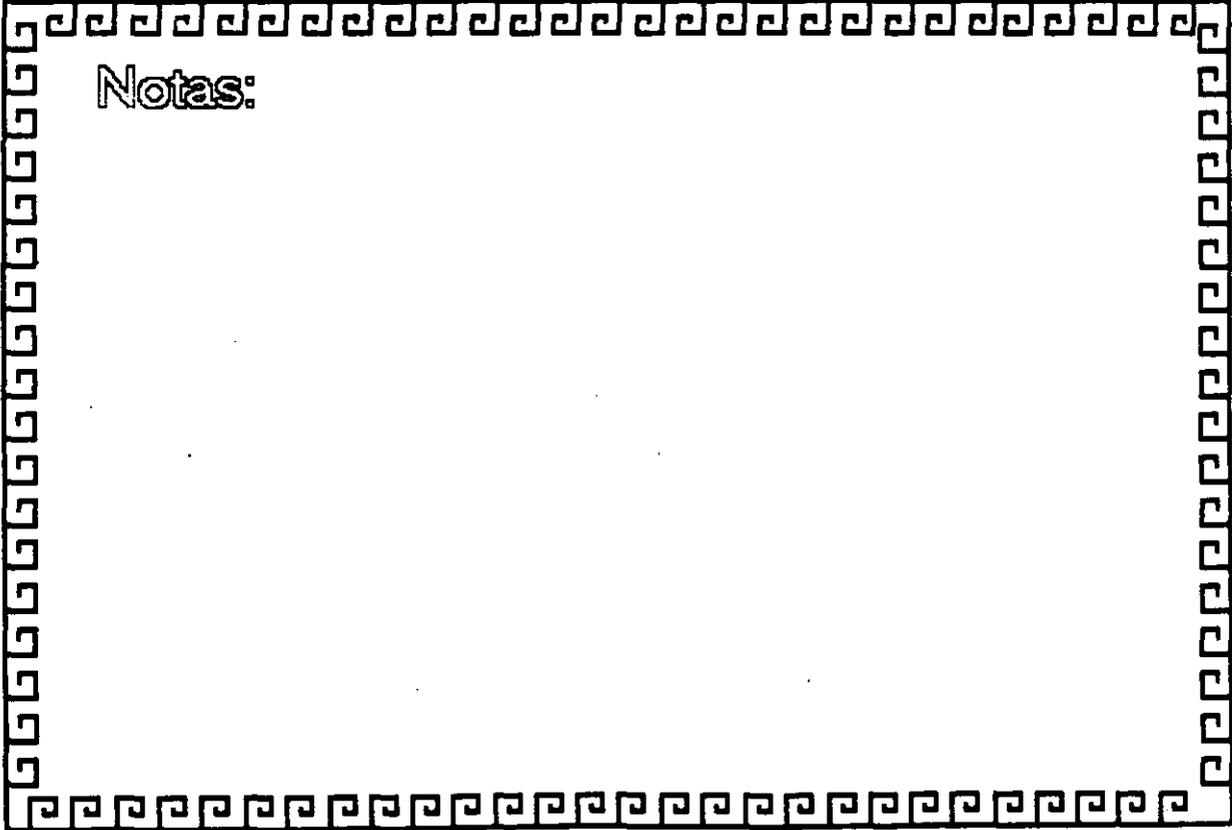
Notas:



DISEÑO CONCEPTUAL



- Definir plataforma base
 - Elección de tipo de Sistema Operativo
 - Elección del Sistema Operativo y versión
 - Determinar número y tipo de Servidores
 - Determinar configuración de Servidores
 - Determinar calendarios de instalación
 - Instalación
 - Determinar tipo de pruebas de aceptación
 - Electuar pruebas de aceptación
 - Puesta a punto de la RED
- 

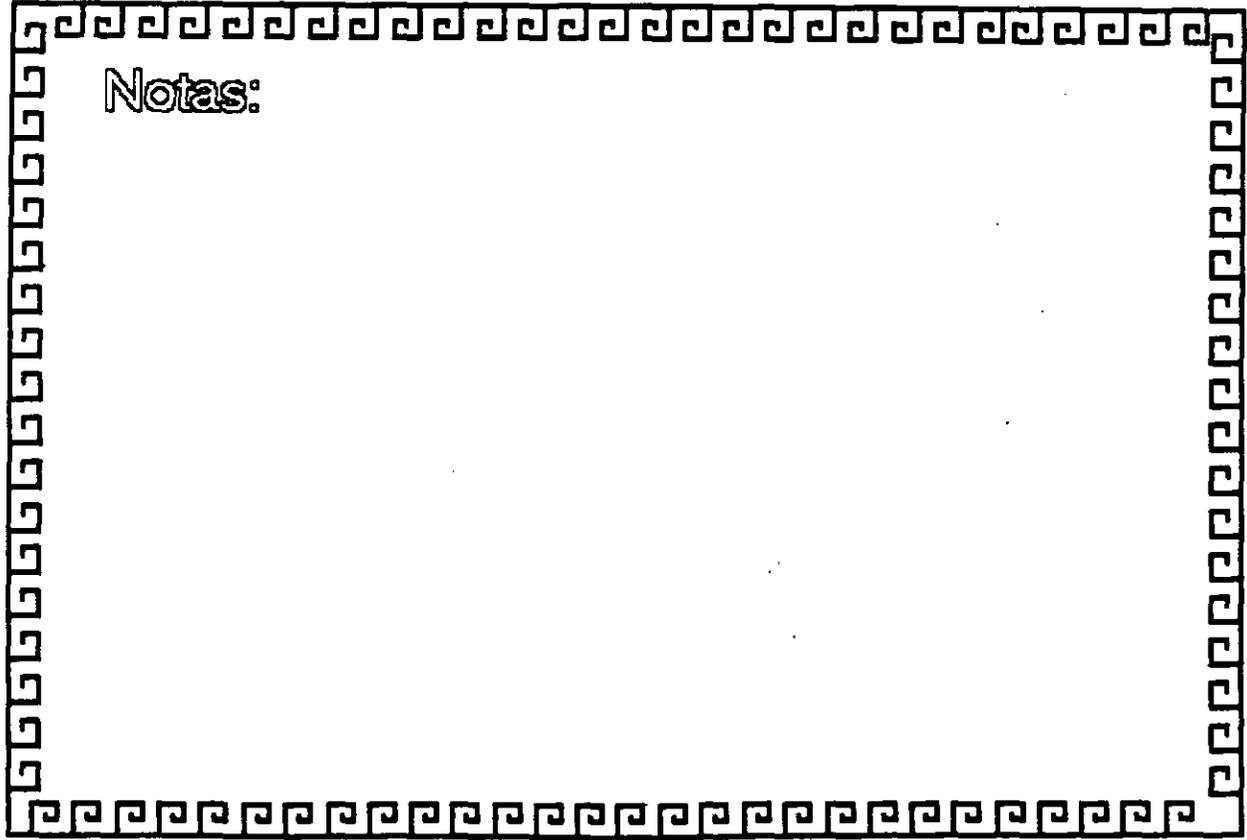


Notas:



PRINCIPALES PLATAFORMAS DEL MERCADO

- MS - DOS
- Windows
- DR - DOS
- MAC - 7
- UNIX
- Windows NT

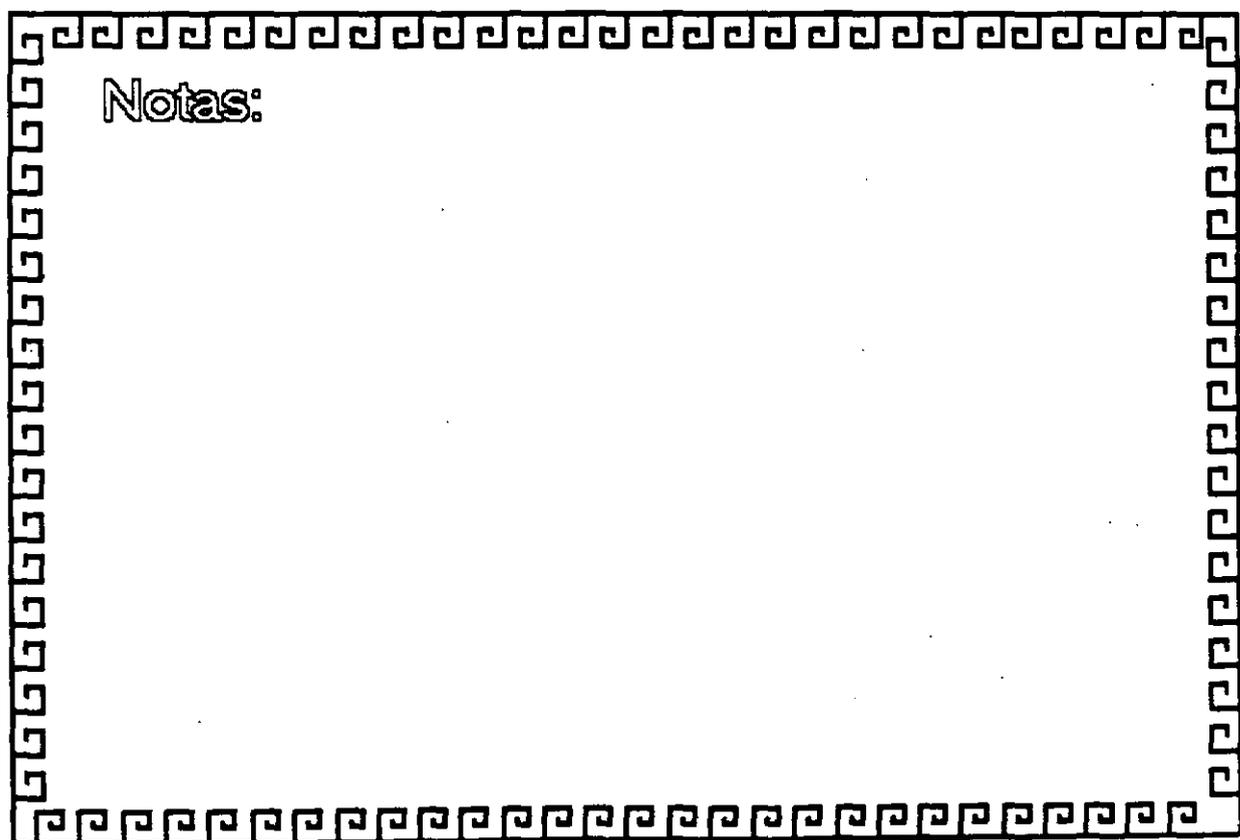


Notas:



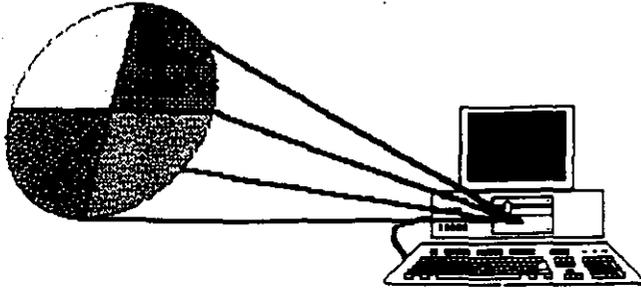
TIPOS DE SISTEMAS OPERATIVOS

- 1.- Servidores de Discos
- 2.- Servidores de Archivos
- 3.- Arquitectura Cliente - Servidor
- 4.- Arquitectura Peer to Peer (cliente - cliente)
- 5.- Servidor de Base de Datos



Notas:

SERVIDOR DE DISCOS



Se comparte sólo el disco duro del servidor.

Se asigna una partición virtual a cada nodo.



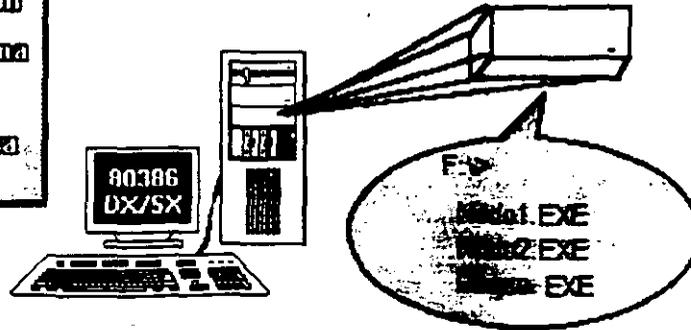
Notas:

SERVIDOR DE ARCHIVOS

El usuario efectúa una petición

El servidor manda el programa y el archivo a la estación

La estación de trabajo procesa la petición



F:\> Nodo1.EXE



F:\> Nodo2.EXE



F:\> Dbase.EXE



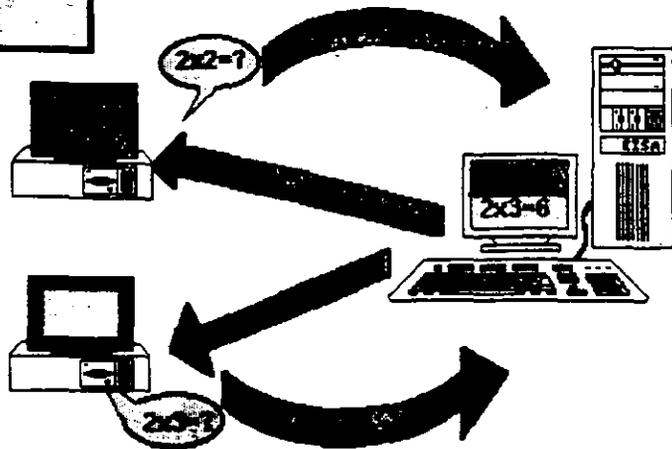
F:\> Dbase.EXE

Notas:

ARQUITECTURA CLIENTE - SERVIDOR

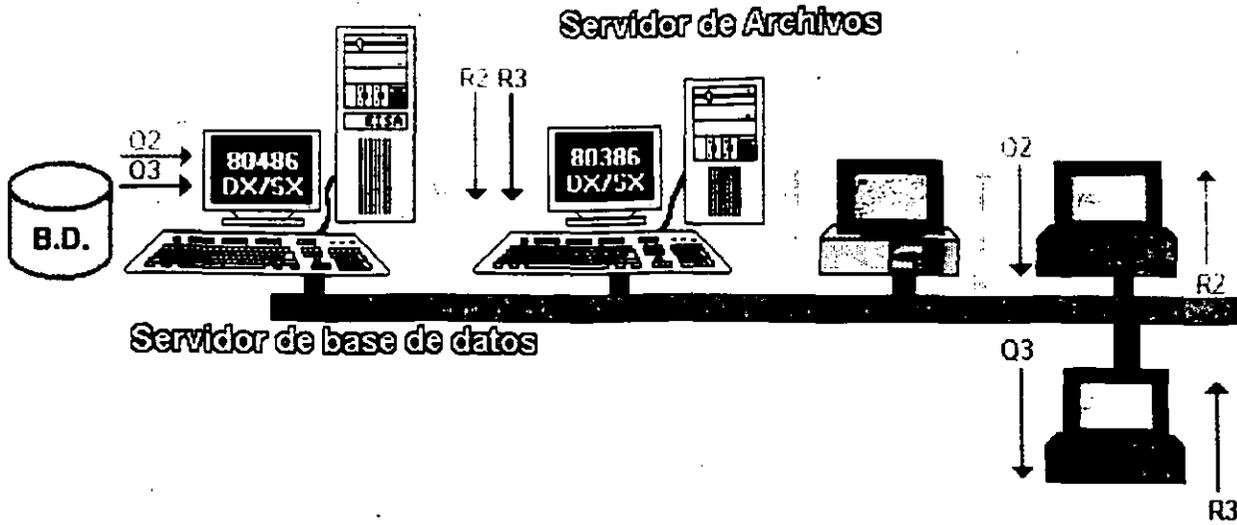
El usuario efectúa una petición

El servidor procesa la petición solamente envía resultados.



Notas:

SERVIDOR DE BASE DE DATOS



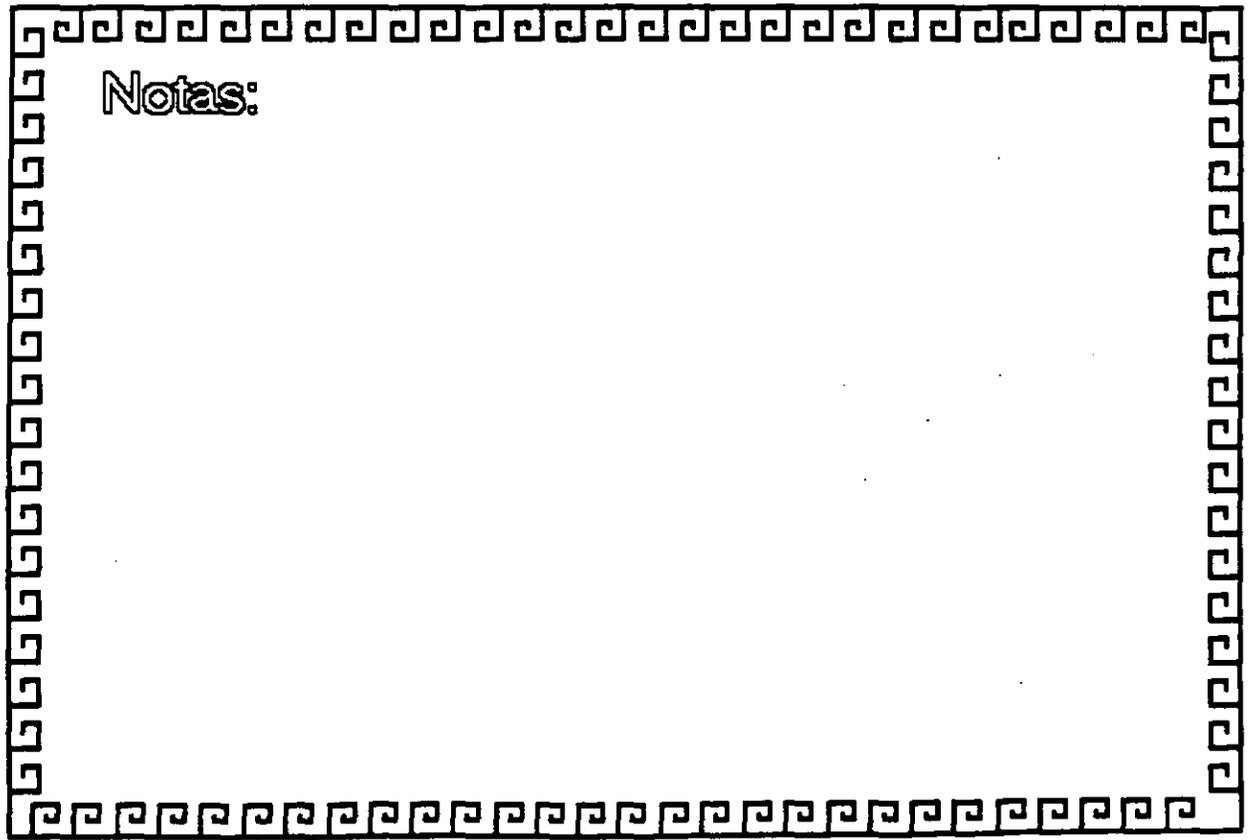
Notas:



Principales Sistemas Operativos para RED

Microsoft

- Lan - Manager OS/2 Server v. 2.2
- Lan - Manager Servicios para Macintosh
- Windows for Workgroups v. 3.1 (1.5.20.100 us.)



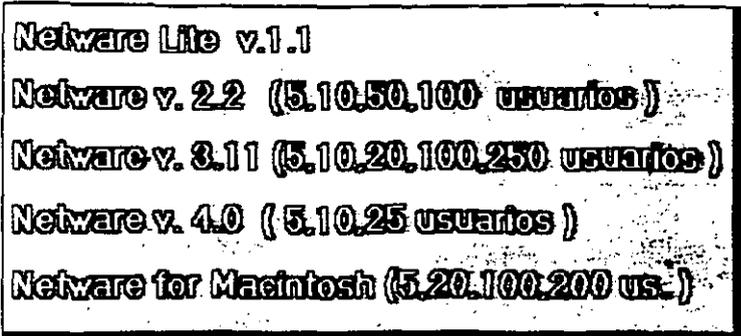
Notas:

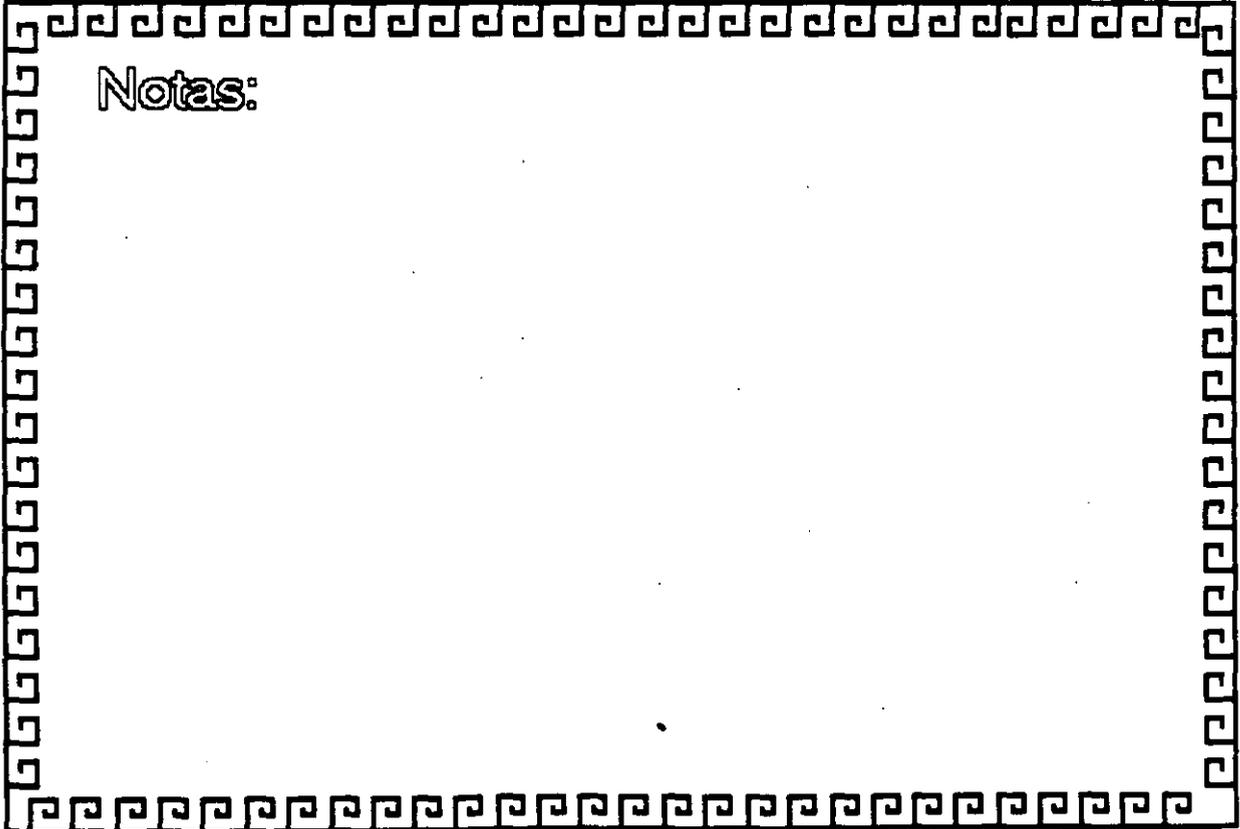
Figura 3-9



Principales Sistemas Operativos para RED

Novell

- 
- Netware Lite v.1.1
 - Netware v. 2.2 (5.10.50.100 usuarios)
 - Netware v. 3.11 (5.10.20.100.250 usuarios)
 - Netware v. 4.0 (5.10.25 usuarios)
 - Netware for Macintosh (5.20.100.200 us.)



Notas:



Principales Sistemas Operativos de RED

Arisoft

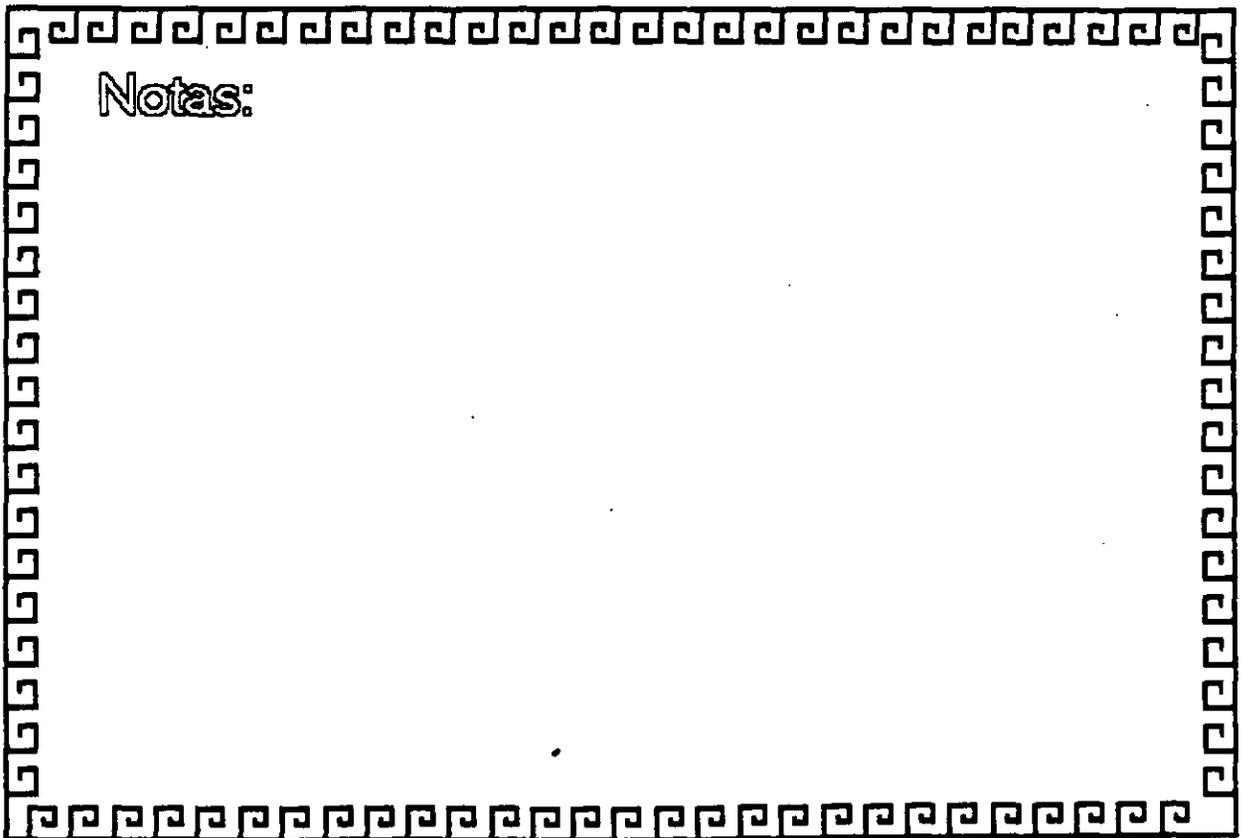
Lantastic Single Mode (1 usuario)

Lantastic for Netware

Lantastic for Macintosh



Notas:





Principales Sistemas Operativos de RED

SCO

Lan Manager for Work Groups (5,10,15 usuarios)

Lan Manager Enterprise Edition (15 usuarios)

Notas:

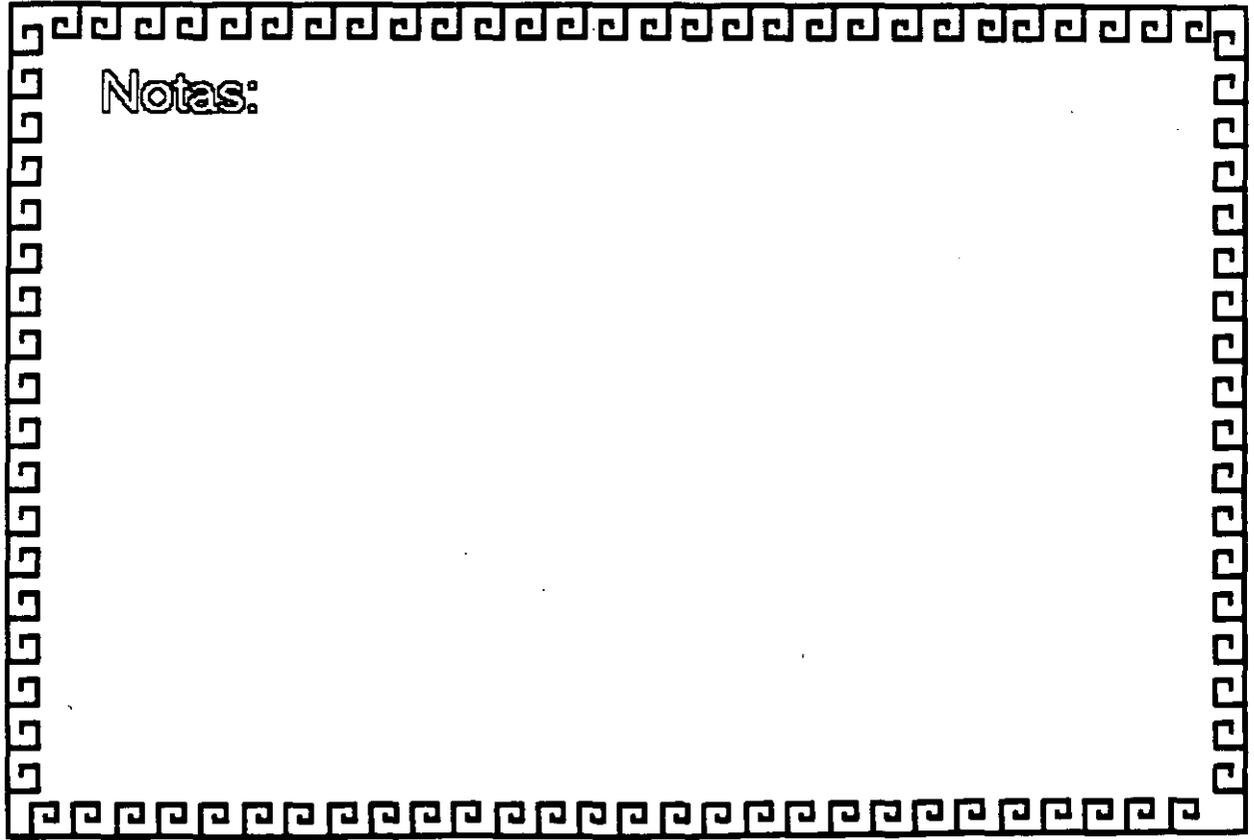


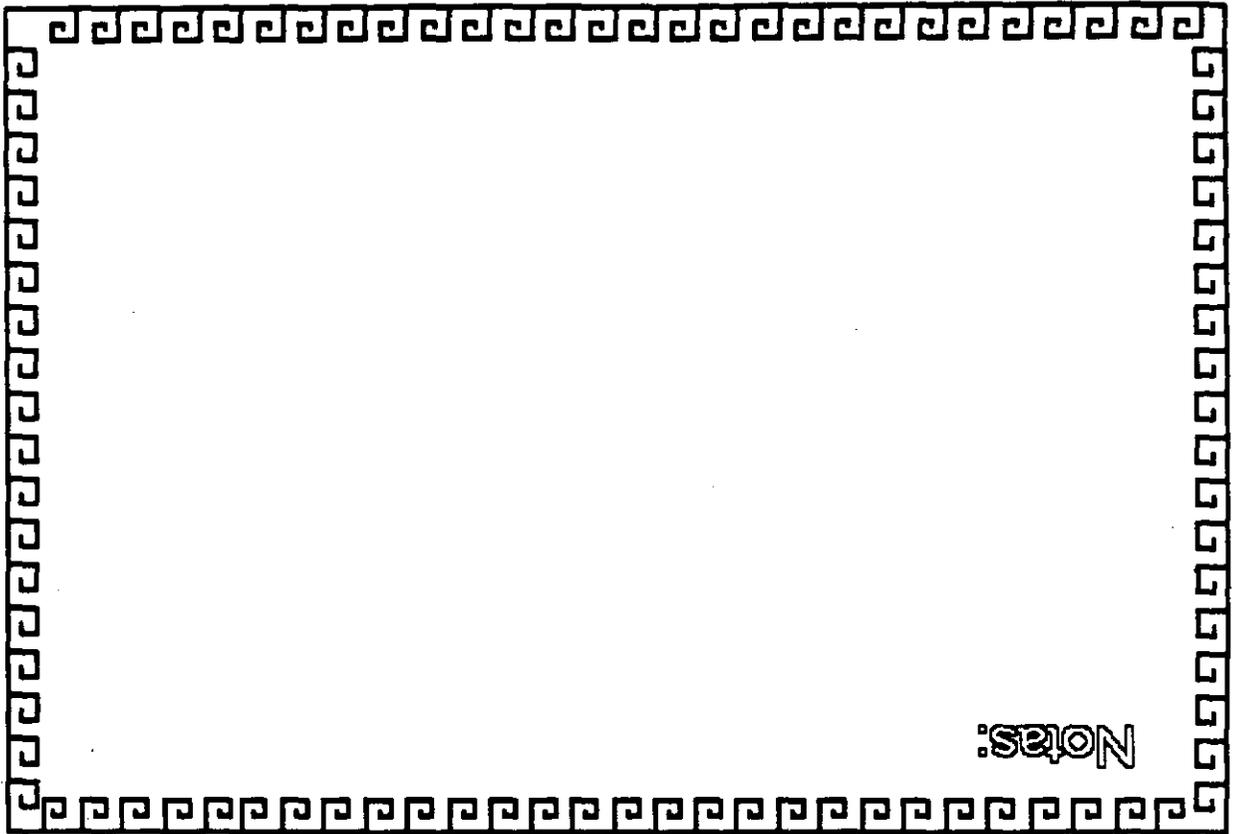
Soluciones para Comunicaciones

- Puentes de Red Local
- "Gateways" al computador central

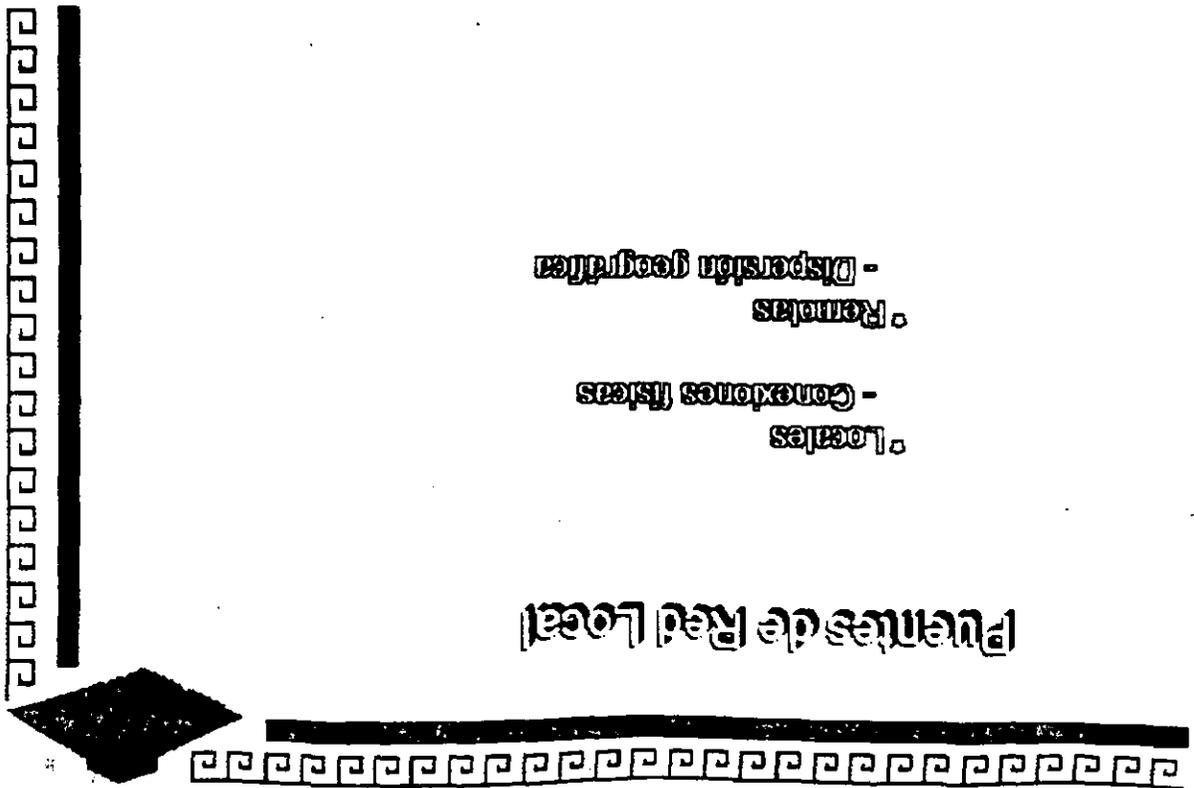


Notas:





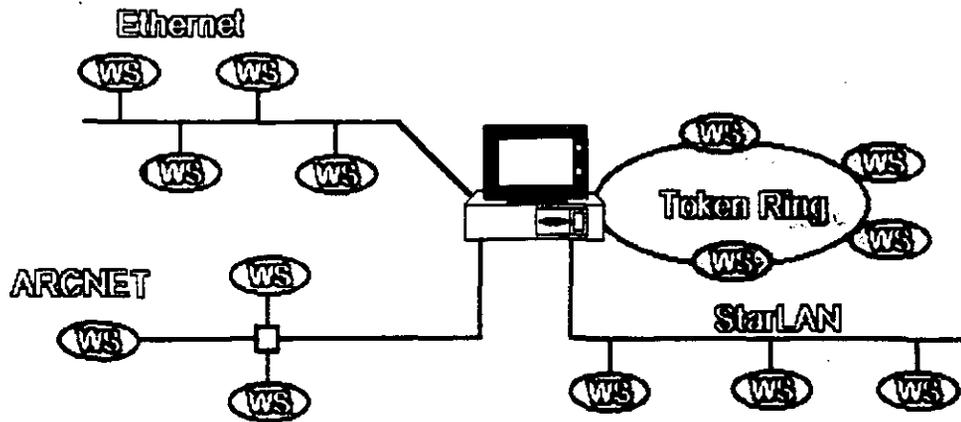
Notes:



Puentes de Red Local

- Locales
- Conexiones físicas
- Remotas
- Disponibilidad geográfica

PUENTE DE RED LOCAL



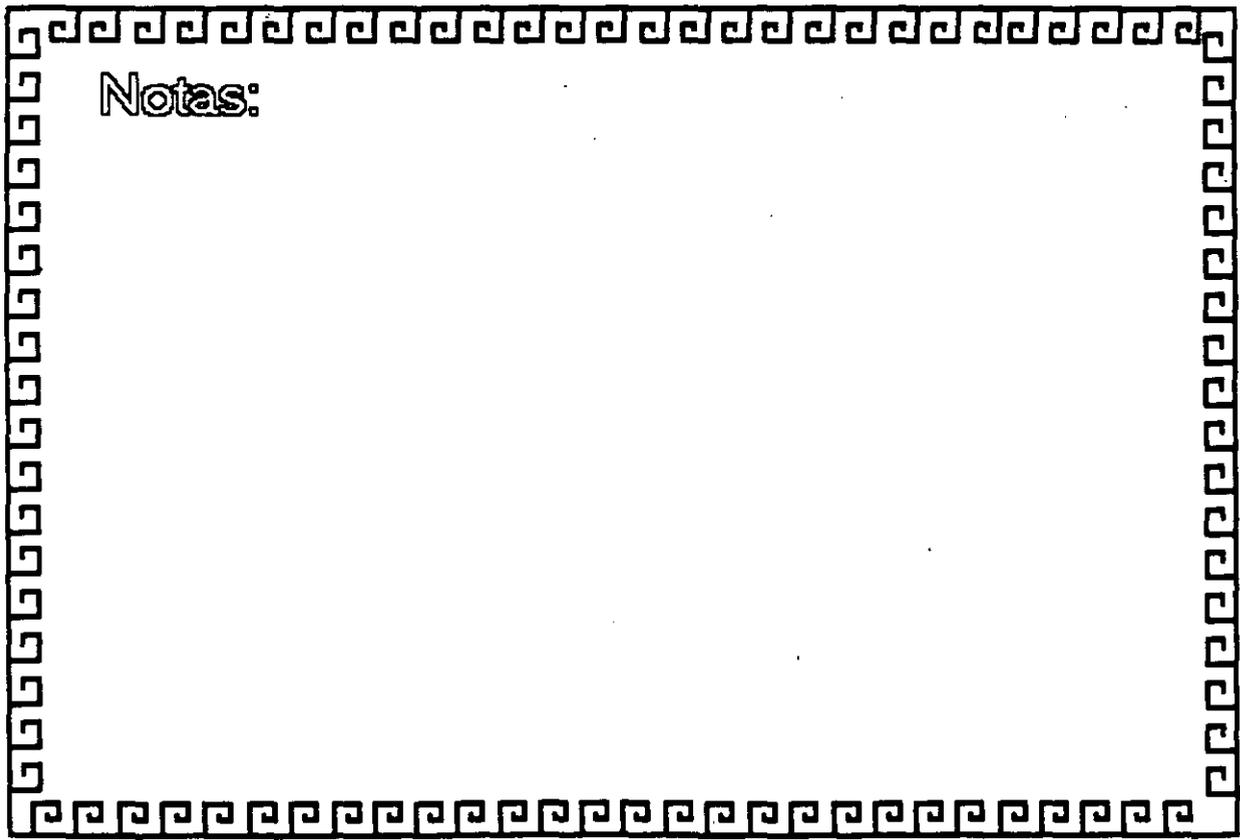
Notas:



Puentes LAN

Puentes para Comunicaciones a Distancia

- Punto a Punto
 - Una conexión
- Múltiples Puntos
 - Múltiples conexiones concurrentes



Notas:

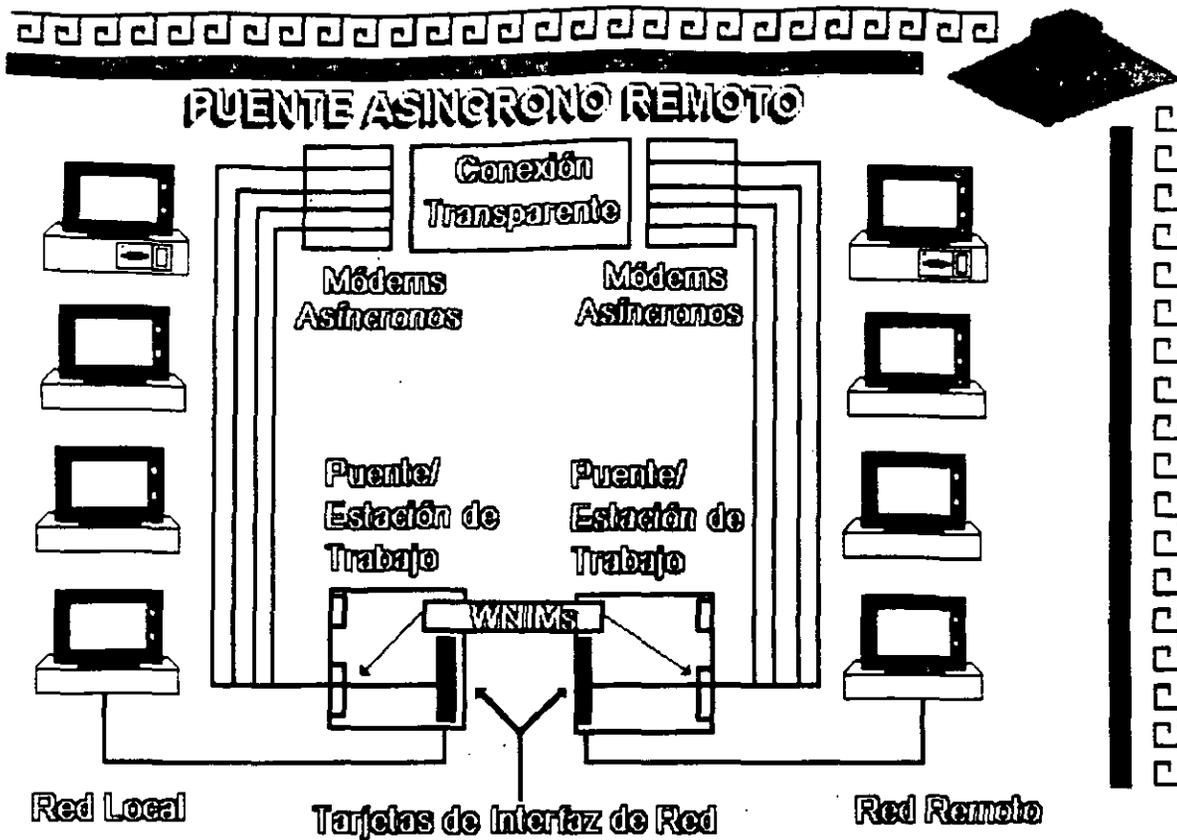


Puentes de Red Local

Puente Punto a Punto para Comunicaciones a Distancia

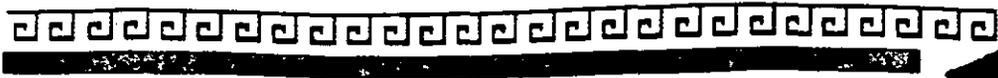
- °Asíncronos
-192 kbps
- °X25
-64 kbps

Notas:



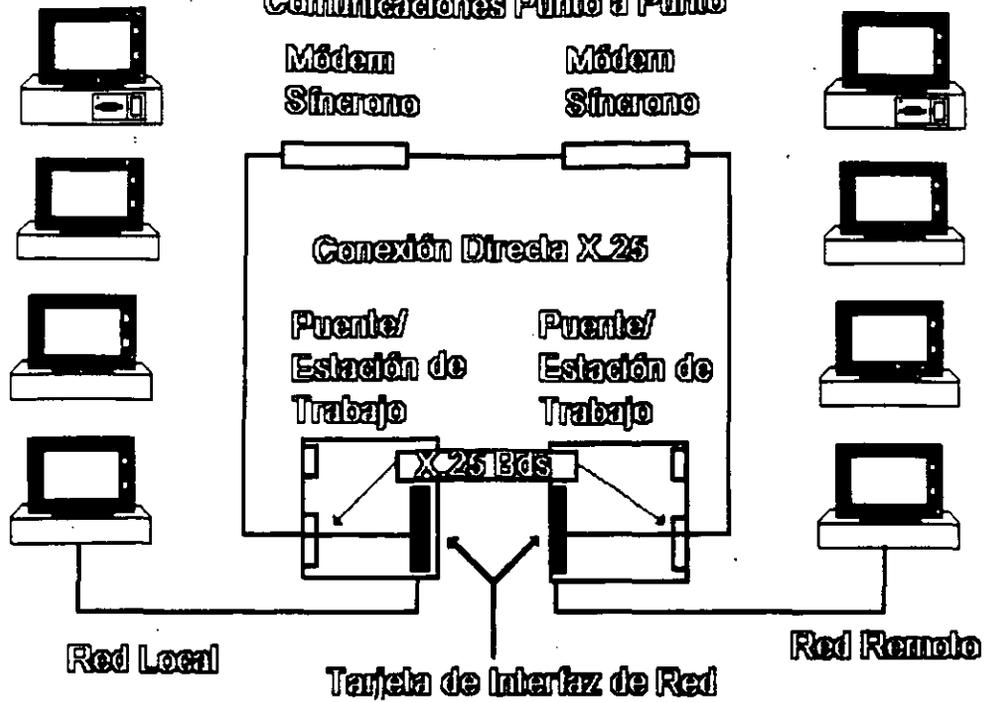
Notas:

Figura C- 6

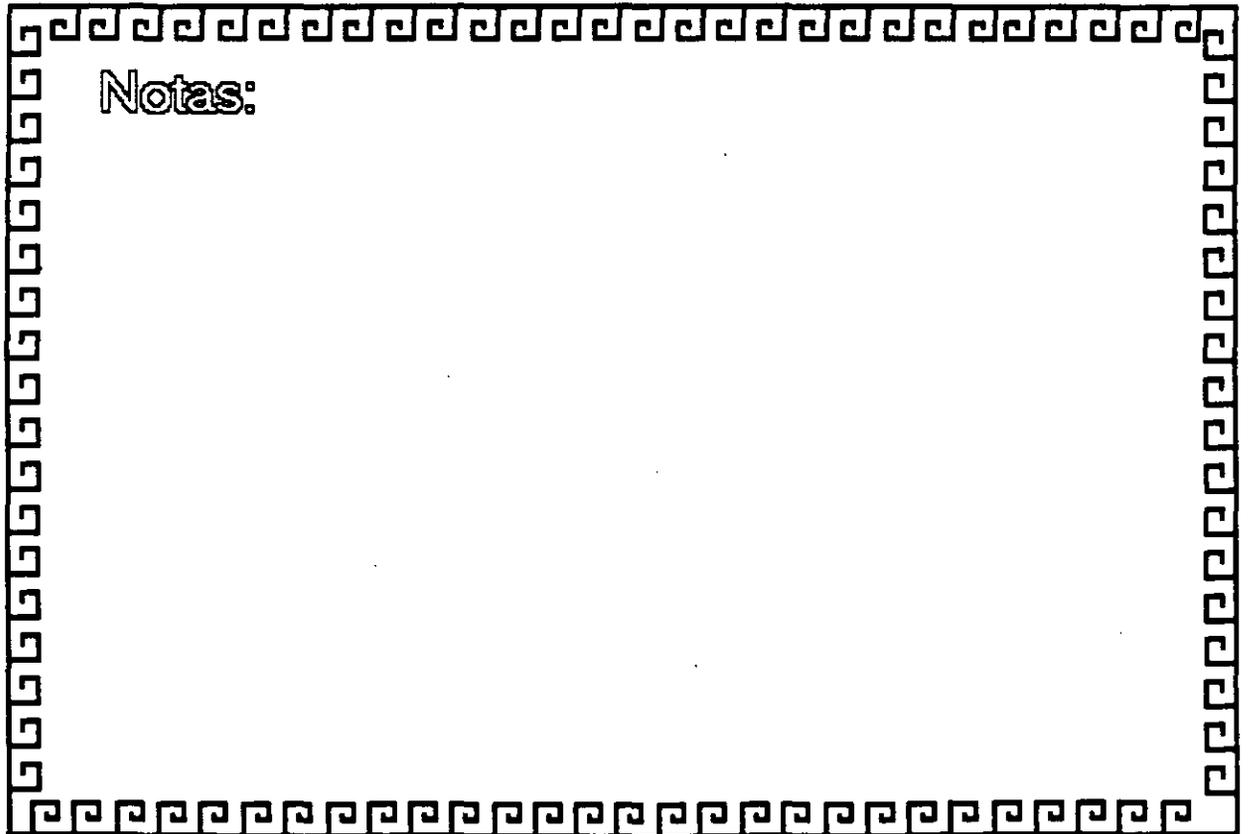


PUENTE REMOTO X.25

Comunicaciones Punto a Punto

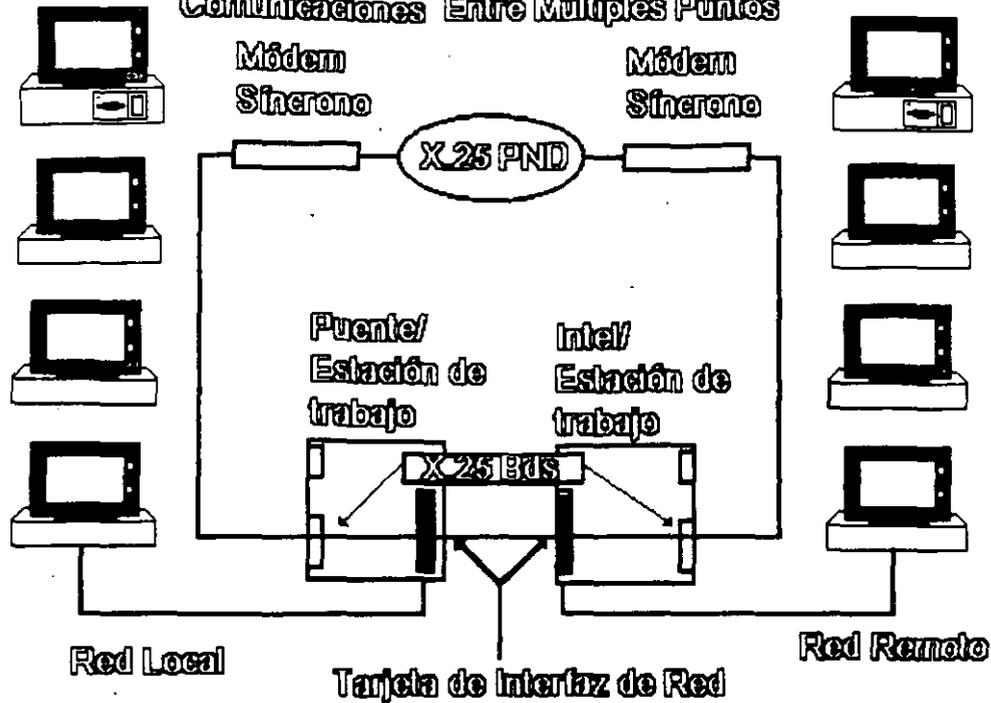


Notas:

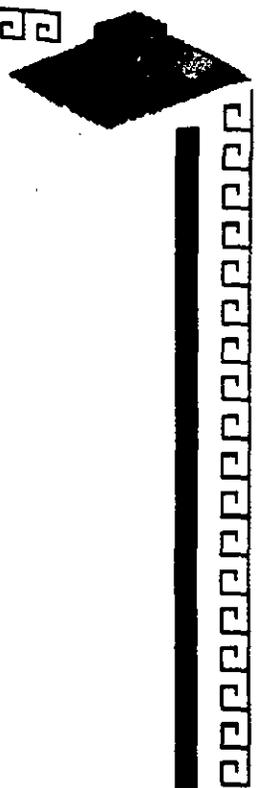


PUENTE REMOTO X.25

Comunicaciones Entre Múltiples Puntos



Notas:



"Gateways" del Computador Central

- Asfneronos
- SNA
- Sistema/3x
- X.25

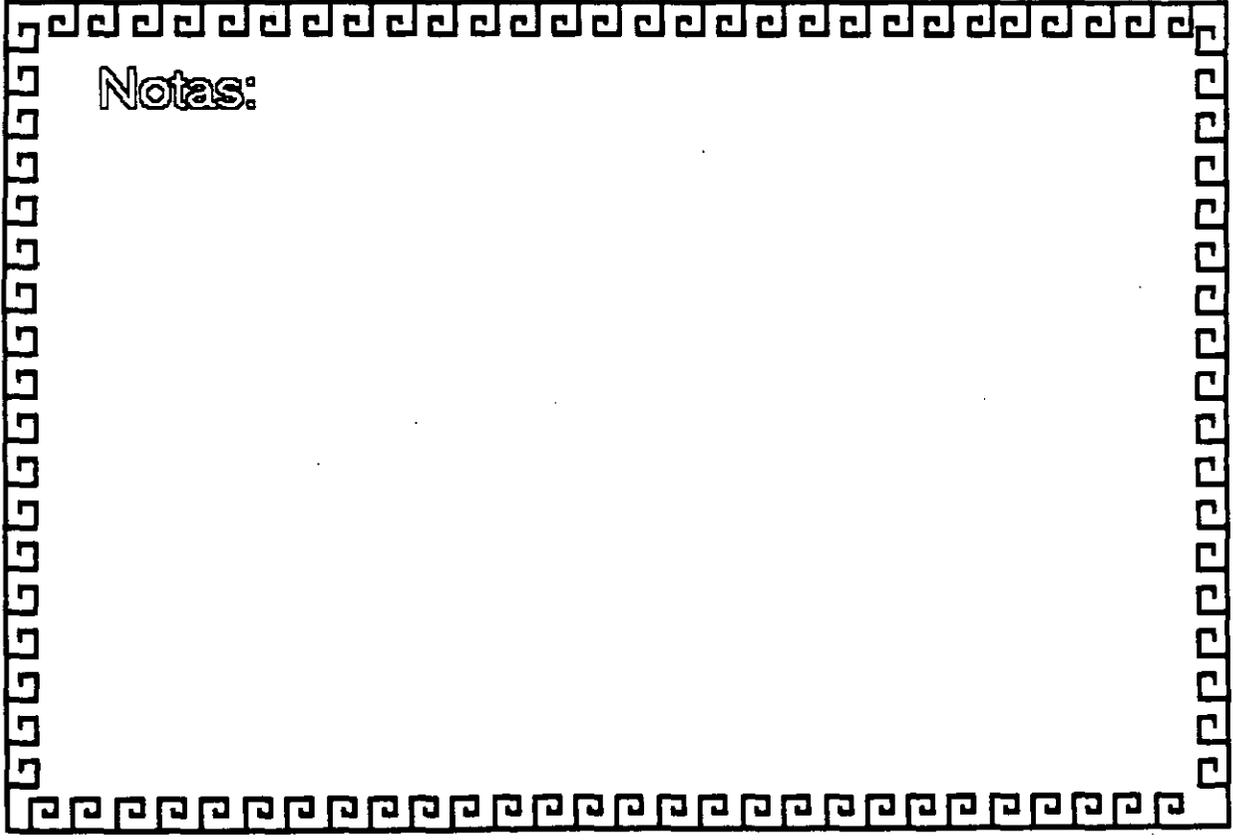


Notas:



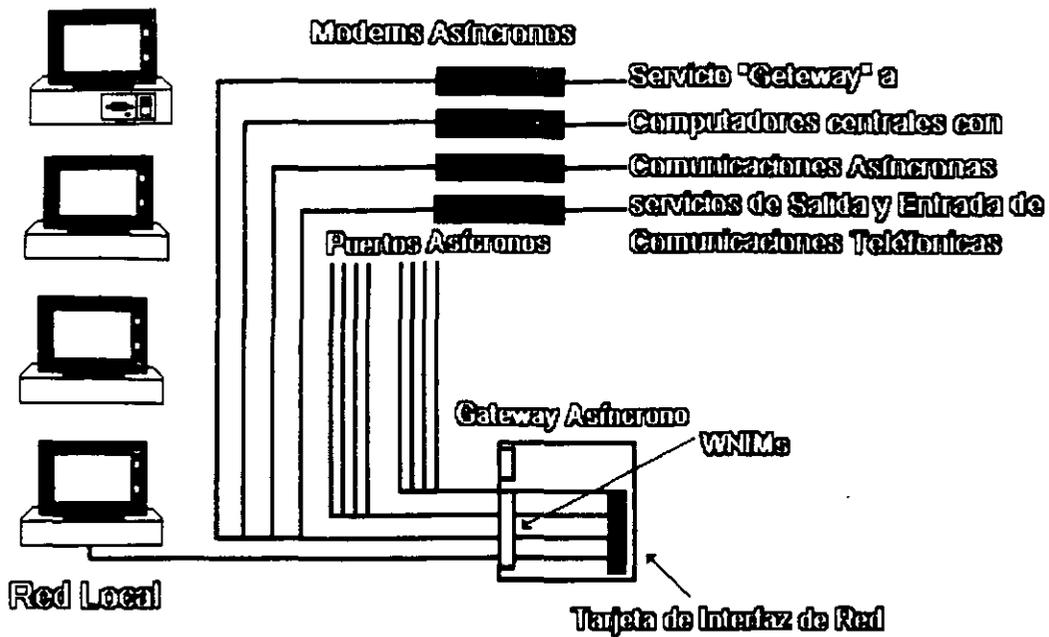
"Gateways" Asíncronos

- Uso compartido de los módems de la Red
 - "Gateway" a computadores centrales con comunicación es asíncronas
 - Servicios telefónicos de acceso remoto y de salida
- 



Notas:

GATEWAYS ASINCRONOS



Notas:

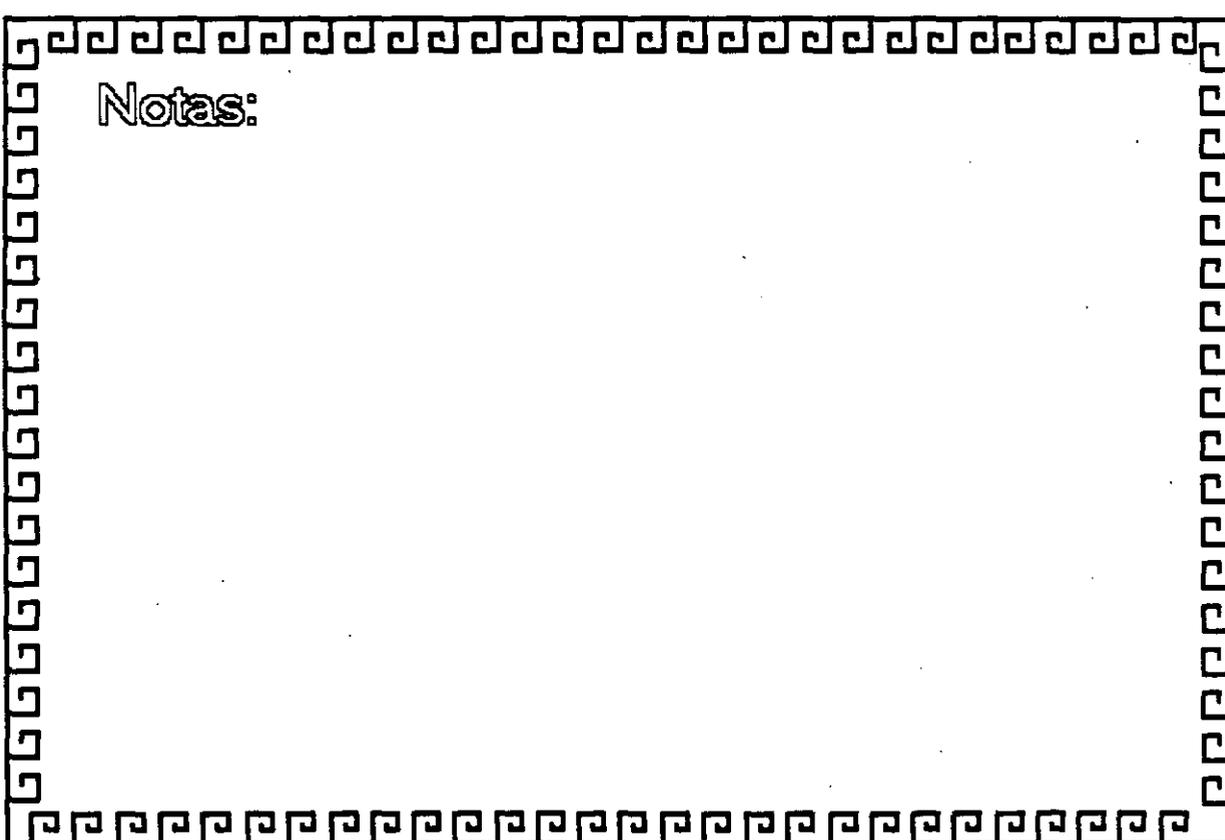


"Gateways" SNA

• Cable Coaxial

• SDLC

• "Token Ring"



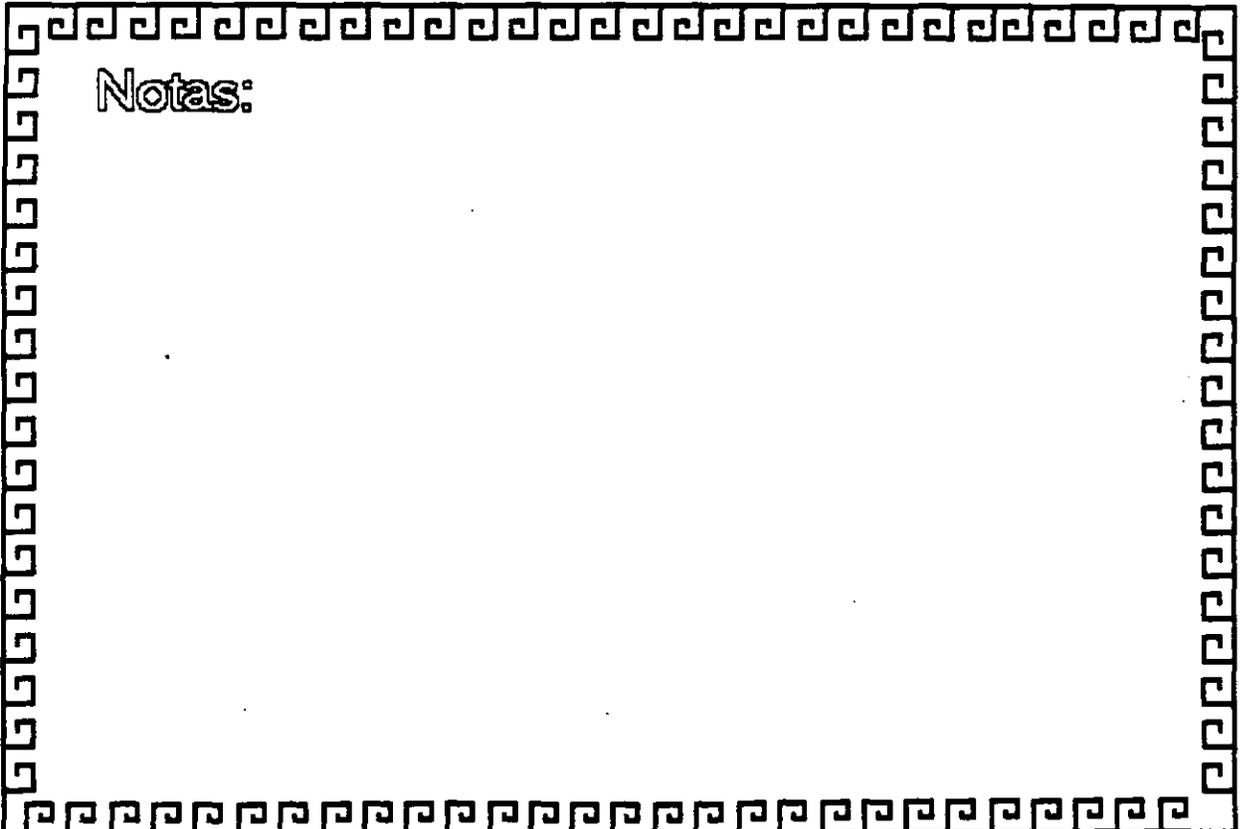
Notas:



"Gateways" SNA

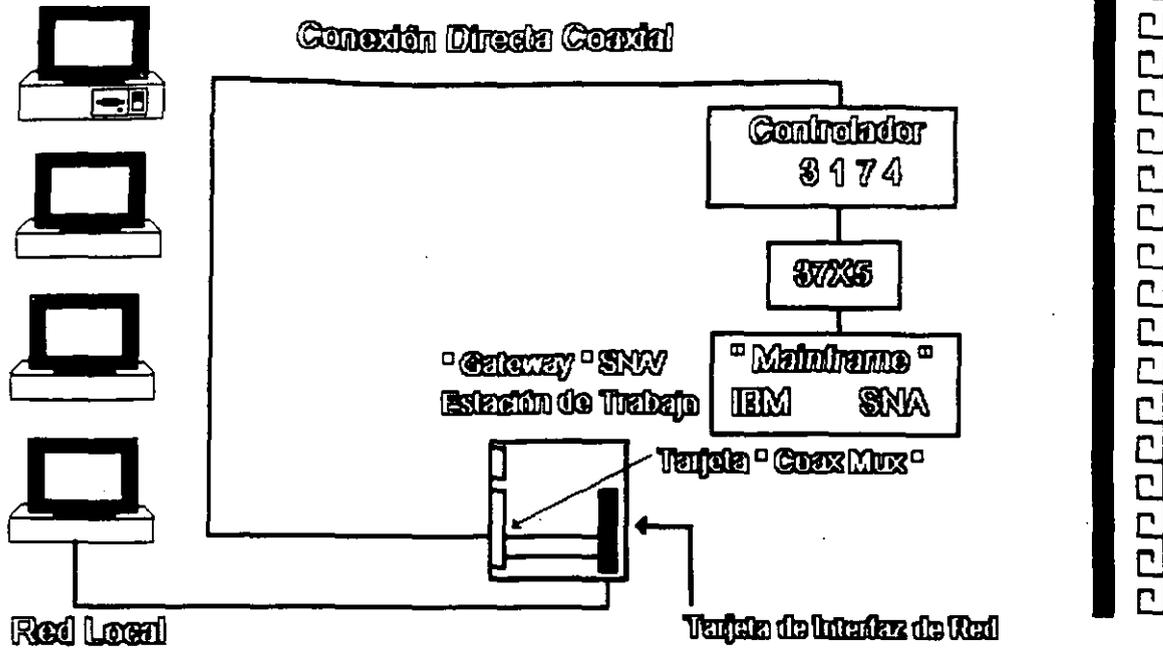
Cable Coaxial

- Provee hasta 40 sesiones
 - Conexión de 2,3 Mbit/s
 - Se conecta a un controlador 3174
o a un Multiplexor 3299
- 



Notas:

Conexión "Gateway" a través de Cable Coaxial



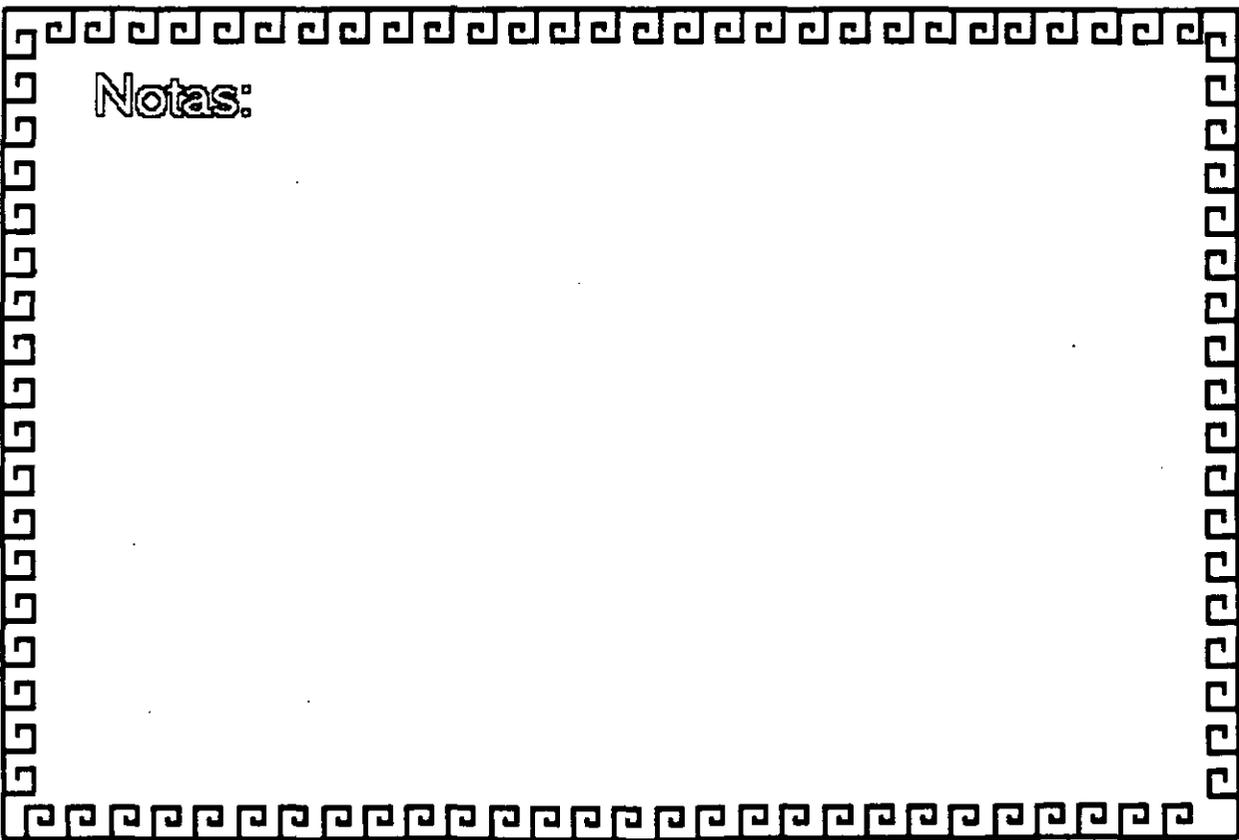
Notas:



"Gateways" SNA

SDLC

- Provee hasta 128 sesiones
 - Conexión de 64 Kbits (máximo)
 - Se conecta al controlador de comunicaciones 3705/3725 mediante un modem
 - Emulación del controlador principal 3174
- 



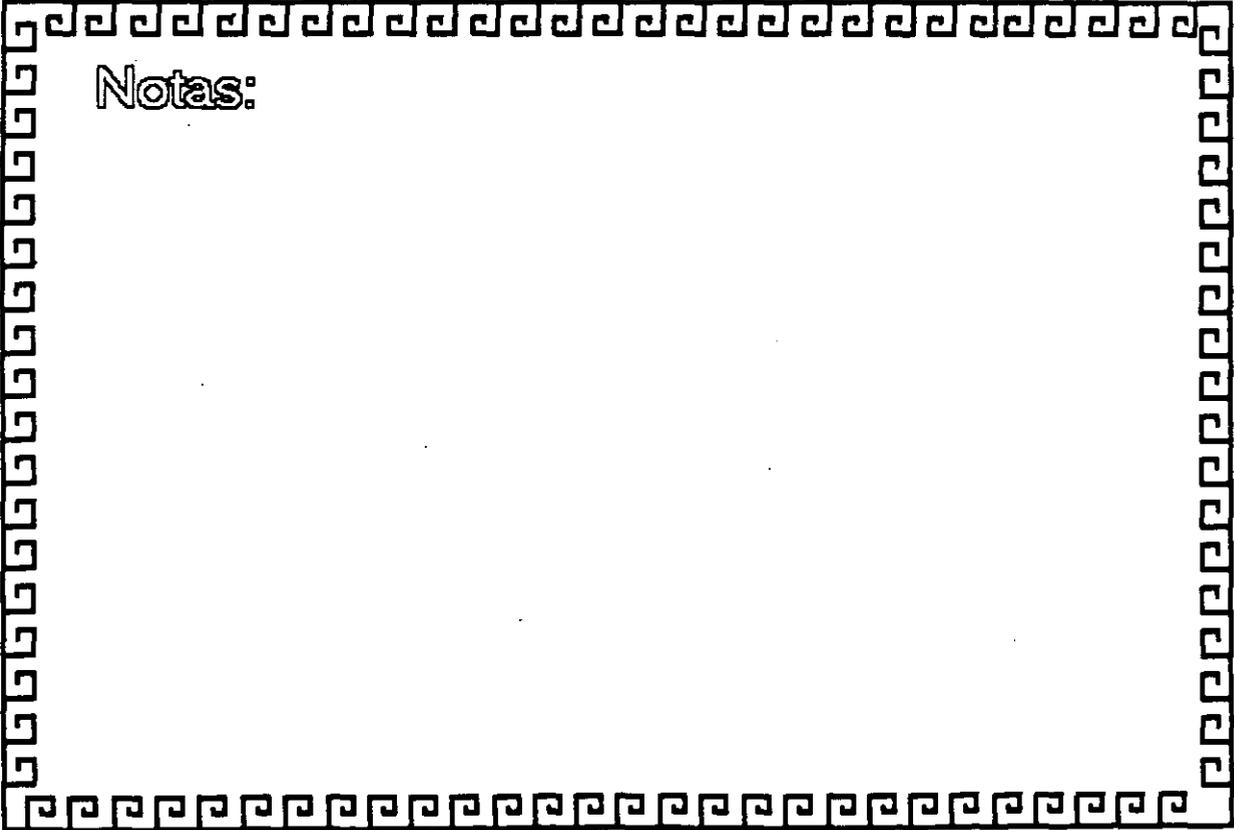
Notas:



"Gateways" SNA

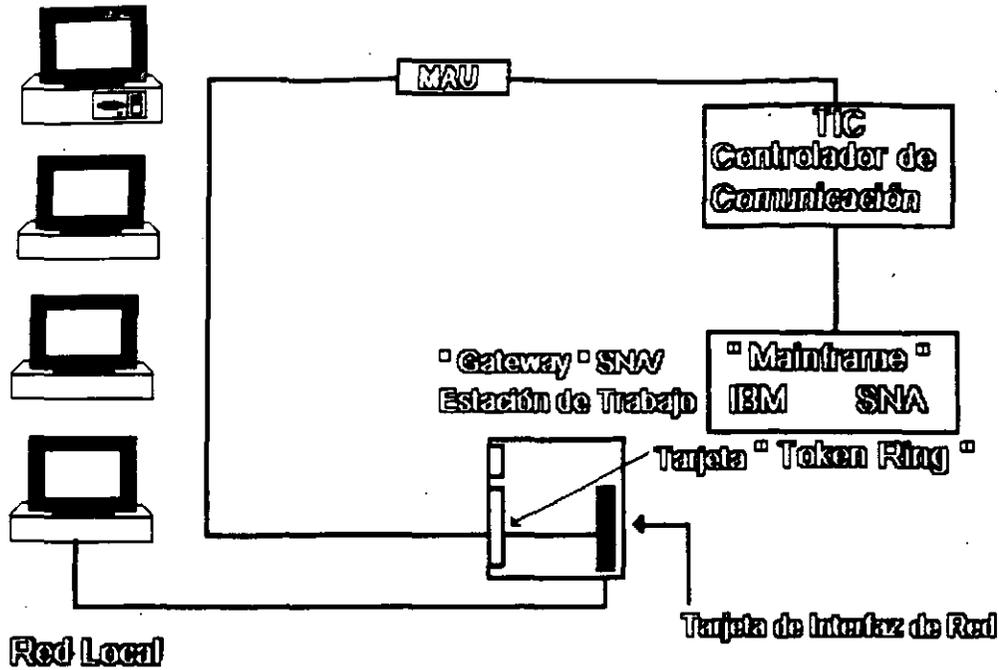
Token Ring

- Provee sesiones SNA distribuidas en una Red de tipo "Token Ring"
 - Utiliza opción "Token Ring" ofrecida por IBM en los controladores 3174 ó 3715
 - Hasta 128 sesiones
 - Ancho de Banda : 4 Mbit/s
- 



Notas:

Conexión "Gateway" Token Ring

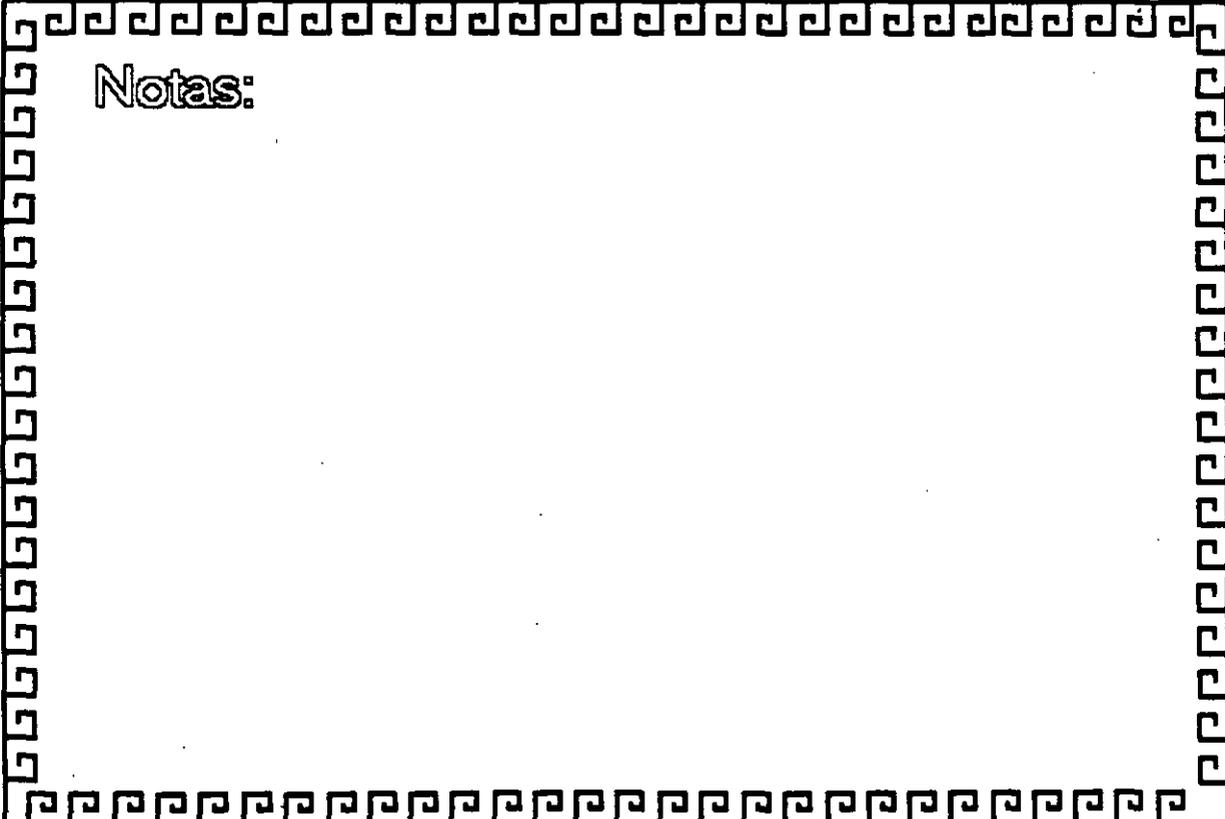


Notas:



"Gateways" X.25

- Provee sesiones con computadores centrales ASCII mediante servicios PDN
 - Conexión de 64 Kbit/s (como máximo)
- 

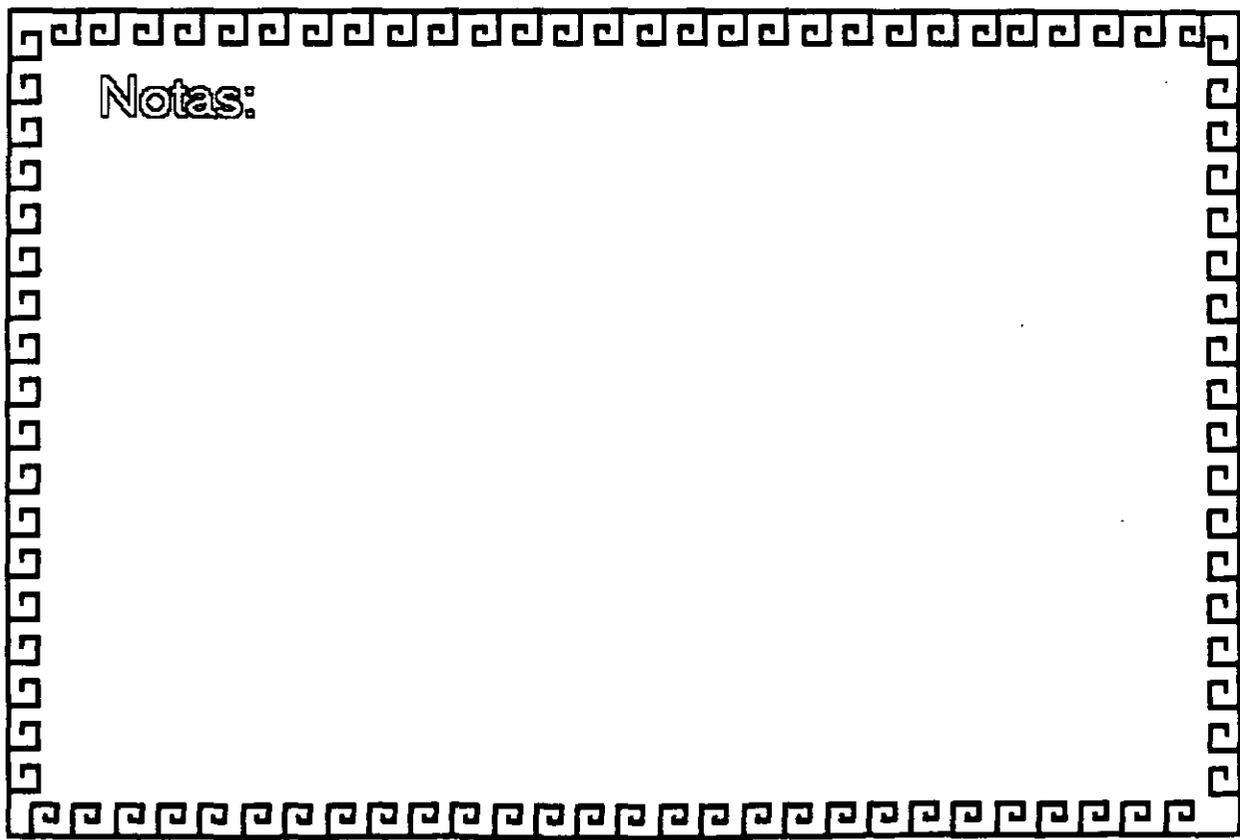


Notas:

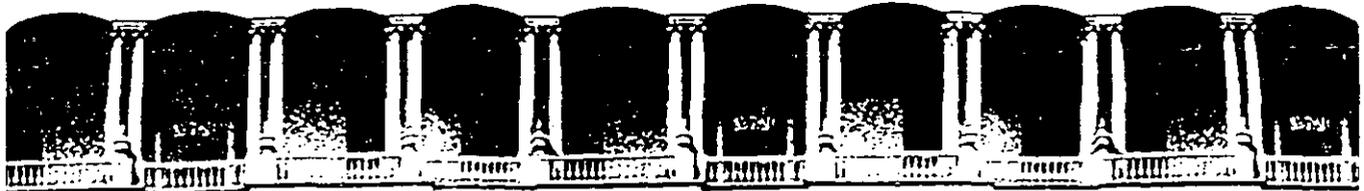


"Gateways" del Sistema / 3x

- Provee 9 sesiones con el minicomputador IBM Sistema / 3x
 - Conexión de 19,2 Kb/s (como máximo)
- 



Notas:



**FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA**

REDES (LAN) DE MICROS PARTE II

MODULO II DEL DIPLOMADO DE REDES

MATERIAL DE APOYO DIDACTICO

MARZO, 1994

CURSO : REDES LAN DE MICROS PARTE II MODULO II DEL DIPLOMADO DE REDES LOCALES

PRESENTACION

Bien se sabe que en 1985 se inició un movimiento tendencioso hacia las redes, ahora el uso de éstas como herramienta de la computación es toda una realidad y una necesidad de primer orden.

Este módulo II del curso será un apoyo a los profesionistas de la computación, que por sus necesidades de productividad estén involucrados con las redes de micros, ya que el enfoque teórico-técnico que tiene, será la base para que el participante se actualice e inicie como futuro especialista. Desde luego para aquellos que contemplen lograr el DIPLOMADO EN REDES (LAN) DE MICROS, este módulo será el siguiente peldaño en la cuesta hacia su objetivo, donde deberán cumplir con los requisitos académicos del caso.

OBJETIVOS

Reforzar y abundar en los tópicos del módulo I y ofrecer al participante una herramienta más potente en este campo, a efecto de consolidar con teoría y prácticas lo visto y aprendido en la parte anterior.

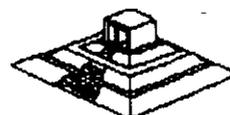
Lograr que los participantes puedan incursionar con éxito en otros niveles en este apasionante campo de LAS REDES (LAN).

A QUIEN VA DIRIGIDO

A profesionistas, ejecutivos, funcionarios, técnicos y personas que por sus requerimientos profesionales, tengan la necesidad de revisar, afirmar y abundar en esta herramienta de actualidad, tan indispensable en el mundo de la computación.

REQUISITOS

Que los participantes tengan buen nivel en microcomputación con amplio manejo de MS-DOS y haber tomado sin ser limitante, el módulo REDES (LAN) DE MICROS PARTE I.



TEMARIO

1.- INTRODUCCION

- 1.1 Esquema general
- 1.2 Revisión de conceptos

2.- TARJETAS PARA RED.- ANALISIS, COMPARACION Y NORMAS

- 2.1 Modelo de referencia ISO-OSI
- 2.2 Ethernet
- 2.3 Token-Ring
- 2.4 Arcnet
- 2.5 Normalización (IEEE, CCITT, etc)

3.- INSTALACION DE SISTEMAS OPERATIVOS PARA RED

- 3.1 Diseño conceptual
- 3.2 Requerimientos de hardware y software
- 3.3 Instalación física y lógica
- 3.4 Administración
- 3.5 Documentación

4.- SOFTWARE Y APLICACIONES VERTICALES

- 4.1 Servidores de base de datos
- 4.2 El estandar SQL
- 4.3 Manejadores de base de datos
- 4.4 Correo electrónico
- 4.5 Aplicaciones en general
- 4.6 El supervisor, diagnósticos y utilerías

5.- TECNOLOGIAS DE VANGUARDIA

- 5.1 Cableado estructurado
- 5.2 Puentes, ruteadores y concentradores
- 5.3 Fibra óptica, backbones, FDDI
- 5.4 Redes WAN y MAN
- 5.5 Enlaces TCP/IP
- 5.6 Administración vía SMNP
- 5.7 Nuevas tecnologías de impresión
- 5.8 El "downsizing"

6.- CONCLUSIONES

- 6.1 Planeación de una red
- 6.2 Fases para la implementación de una red

7.- SESIONES DE TALLER EN CADA PUNTO DEL TEMARIO



CURSO : REDES LAN DE MICROS PARTE II
MODULO II DEL DIPLOMADO DE REDES LOCALES

1.-) INTRODUCCION

INTRODUCCIÓN

ESQUEMA GENERAL.

Antes que nada se analizarán los conceptos más relevantes de una red, las partes que la conforman y la terminología adecuados para cada componente y la descripción de su función.

Después se profundizará en las diferentes topologías físicas de las redes más comunes y sus características, para después analizar y comprender cada uno de los protocolos de comunicación de las técnicas de **Token Passing** y de **Carrier Sense Multiple Access/ Collision Detection (CSMA/CD)** y en qué tipo de topología se utiliza cada uno.

También se verán cuales son los diferentes medios físicos existentes para establecer la comunicación y sus características. Y se finalizará con la explicación de los conceptos de banda base y banda ancha.



REVISION DE CONCEPTOS

TOPOLOGÍA DE REDES LOCALES.

La manera de interconectar los distintos elementos de una red da un primer acercamiento a la estructura y comportamiento de la misma. A la configuración geométrica resultante se le llama **topología** de la red.

Para el estudio de la topología se deben de considerar dos tipos:
(figura 1-1)

- * Física
- * Lógica

La topología física es determinada por la disposición de los elementos conectados a la red. (figura 1-2)

En la figura se puede apreciar que todos los nodos están conectados a un elemento central conformando una estrella física. La línea discontinua indica la topología lógica.

La topología lógica la determina el protocolo de comunicación operando en la red, no importando la disposición física de los elementos; en otros términos, se puede implementar un anillo lógico en una estrella física. (figura 1)

Un elemento que es determinante en el rendimiento de la red es el protocolo de comunicación, para el análisis de este no importará cual sea la topología física (figura 1-3)

En el mercado actual existe una gran variedad de topologías físicas, para entender como funcionan todas estas, es importante conocer cómo funcionan lógica y físicamente los tipos básicos antes mencionados; sobre todo su protocolo de comunicación, para que se puedan entender y conocer las características de cualquier topología que el mercado pueda ofrecer.

Los nodos que conforman la red, pueden representar tanto a elementos terminales de comunicación, servidores, estaciones de trabajo, nodos de impresión, así como también elementos de unión de las distintas ramas de la red. (figura 1-4)



La elección de la topología tiene un fuerte impacto sobre el comportamiento final que se va a obtener de la red. Como se verá más adelante, el eficaz aprovechamiento de la red depende de una serie de **protocolos** de comunicación entre sus distintos elementos, así como también la estructura topológica condiciona algunas características (figura 1-5), entre las más relevantes cabe citar:

- a) Protocolo de Comunicación Física.
- b) La flexibilidad de la red para añadir o eliminar nuevas estaciones de trabajo.
- c) La repercusión en el comportamiento de la red, considerando que se pueda tener una falla en una de las estaciones o nodos.
- d) El flujo de información que pueda transitar sobre la red sin que existan problemas asociados a retardos en la comunicación debido a una carga excesiva de transporte de información.
- e) Versatilidad en el diseño de cableado.
- f) Posibilidades de crecimiento.

Las múltiples configuraciones que pueden presentarse, obedecen básicamente a tres tipos:

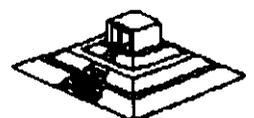
Estrella

Anillo

Bus (lineal o árbol)

(figura 1-6)

A continuación se verá con más detalle cada una de las configuraciones mencionadas.



CONFIGURACIÓN EN ESTRELLA.

Antes que nada cabe mencionar que la topología de estrella no es un estandar. El protocolo de el que hace uso es el *polling o poleo*.

En una red en estrella, todas las **estaciones de trabajo** se comunican entre sí a través de un dispositivo central.

El nodo central asume un papel muy importante, ya que todas las comunicaciones que se llevan a cabo en la red se realizan por medio de éste. Lo usual es que el nodo central ejerza todas las tareas de control y posea los recursos comunes de la red; para poder reducir su influencia se puede optar por localizar el control en alguno(s) de los nodos periféricos, de modo que el nodo central actúe como una unidad de conmutación de mensajes entre todos los nodos periféricos.

La configuración de estrella presenta buena flexibilidad para incrementar o decrementar el número de estaciones de trabajo, ya que las modificaciones necesarias no representan ninguna alteración de la estructura y están localizadas en el nodo central.

La repercusión en el comportamiento global de la red al presentarse una falla en uno de los nodos periféricos es muy baja y solo afectaría al tráfico relacionado con ese nodo. En caso contrario si la falla se presentara en el nodo central, el resultado podría ser catastrófico y afectaría a todas las estaciones de trabajo.

El flujo de información puede ser elevado y los retardos introducidos por la red son pequeños si la mayor parte de ese flujo ocurre entre el nodo central y los nodos periféricos.

En caso de que las comunicaciones se produzcan entre las estaciones, el sistema se vería restringido por la posible congestión del dispositivo central.

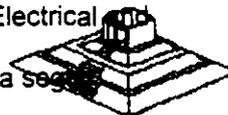
En caso de existir una falla en el medio de comunicación, sólo quedaría fuera de servicio la estación de trabajo afectada.

Por lo general, esta topología no es adoptada por la redes locales más importantes y no ha sido incluida dentro de las configuraciones normalizadas por la IEEE¹. No obstante, es de interés debido al auge que para la comunicación de voz y datos están teniendo las centrales telefónicas automáticas **PABX** (Private Automatic Branch Exchange).

El número de nodos afecta mucho al rendimiento del servidor, a mayor número de estaciones de trabajo, disminuye el tiempo de atención.

¹ La IEEE es una organización internacional, las siglas significan Institute of Electrical and Electronic Engineers.

Es uno de los organismos que presentan los estándares y recomendaciones a seguir.



La disposición física de los elementos ocasiona que sea una topología "costosa", porque no se puede aprovechar la cercanía de las máquinas para interconectarlas, sino que se deben conectar al *centro*.

CONFIGURACIÓN DE ANILLO.

En una configuración de anillo, los nodos de la red están colocados formando un anillo, de manera que cada estación tiene conexión con otras dos estaciones.

Los mensajes viajan por el anillo, de nodo en nodo, en una única dirección de manera que toda la información pase por todos los módulos de comunicación de la red.

Cada nodo tiene que ser capaz de reconocer los mensajes que van dirigidos a él y actuar como retransmisor de los mensajes que, pasando a través de él van dirigidos a otras estaciones que puedan existir dentro de la red.

Puede haber más de una línea de transmisión, aunque lo más habitual es la existencia de una sola.

El control de la red puede ser centralizado o distribuido entre varios nodos.

En caso de ser centralizado, uno de los nodos actúa como controlador de manera que, como todos los mensajes tienen que pasar a través de él, si no hay averías, puede verificarse el correcto funcionamiento de la red y en caso de una falla, adoptar las correspondientes medidas para solucionar el problema.

En caso de ser distribuido, el control se ejerce de manera conjunta entre diversos nodos.

El flujo de información se verá limitado por el ancho de banda del medio de comunicación.

Ya que cada estación de trabajo está obligada a retransmitir cada mensaje, en caso de existir un número elevado de estaciones, el retardo introducido por la red puede ser demasiado grande para ciertas aplicaciones.

En la estructura de anillo, una falla en cualquier parte del medio de comunicación, deja bloqueada a la red en su totalidad.

Si la falla se da en una de las estaciones de trabajo, la repercusión en el resto de la red dependerá de si la avería se encuentra o no en el módulo de retransmisión.



En caso de que el módulo de retransmisión continúe funcionando de manera adecuada, la avería no se propaga a la red, sino que solamente deshabilita a esa estación de trabajo en particular. En caso contrario, donde la falla también involucra a el módulo de comunicaciones, el anillo se "corta" y la red queda bloqueada.

Una manera de evitar estos riesgos consiste en el uso de **concentradores**.

El concentrador es un dispositivo, fabricado con una alta confiabilidad, al que se conectan las estaciones de trabajo de la red.

El anillo **lógico** ocurre dentro del concentrador y cuando un nodo deja de funcionar, se hace corto circuito con la entrada hacia la estación en el propio concentrador, reestableciéndose el anillo.

A simple vista, la topología **física** parecerá de estrella, más la topología **lógica** continúa siendo de anillo.

El concentrador acepta un número limitado de estaciones de trabajo, por lo que en caso de necesitar añadir alguna otra estación una vez agotado el espacio disponible para la conexión, se puede recurrir a concatenar varios concentradores para ampliar la red. En el ámbito comercial, a estos concentradores se les llama **MAU** (Multiple Access Unit).

CONFIGURACIÓN DE BUS.

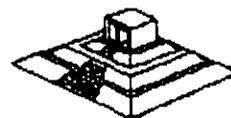
En la topología de *bus*, todos los nodos están conectados a un único canal de comunicación.

En las redes con esta configuración, a diferencia de las de anillo, cada nodo no necesita actuar como repetidor de los mensajes, sino que simplemente debe reconocer su propia dirección para poder tomar aquellos mensajes que viajan por el *bus* y se dirigen a él.

Cuando una estación de trabajo deposita un mensaje en la red, la información se difunde a través del *bus* y todas las estaciones de trabajo son capaces para recibirla.

Debido a que se comparte el medio de comunicación, antes de transmitir un mensaje, cada nodo debe averiguar si el bus está disponible.

Las redes en esta configuración son sencillas de instalar y pueden tener dificultades para adaptarse a las características del terreno o local.



Esta configuración además presenta gran flexibilidad en lo referente a incrementar o decrementar el número de estaciones de trabajo.

La falla en una de las estaciones de trabajo, sólo repercutirá a esa estación de trabajo en particular, pero una ruptura en el bus dejará a la red dividida en dos o inutilizada totalmente según esté implementado el control.

El hecho de que exista un bus común al que acceden todas las estaciones de trabajo tiene algunas ventajas ya mencionadas, pero nos obliga a que el control de acceso a la red sea más delicado que en el caso de las otras topologías.

Cabe señalar que dentro del mercado se reconoce una topología conocida como **árbol o estrella distribuida**, pero en terminos técnicos es un anillo lógico.

MEDIO DE COMUNICACION.

La interconexión de las estaciones de trabajo en una red local se realiza usando medios físicos muy diversos. La elección del medio apropiado se hace en base a (figura 1-7):

- * Cubrir el ancho de banda necesario
- * Cubrir las velocidades requeridas
- * Cubrir las distancias requeridas
- * Adaptacion al entorno físico-geográfico.
- * Minimizar posibilidades de fallas.
- * Posibilidades de crecimiento y modularidad.
- * Minimizar costos de instalación y mantenimiento.

De acuerdo a las características particulares de cada implementación de red se le dará énfasis a los factores mas determinantes de acuerdo a las necesidades de la misma.



Los principales medios de comunicación dentro del mercado son:
(figuras 1-8,1-9):

Par trenzado

El par trenzado es cable de cobre en dos hilos por los que fluye la información. Dentro de este tipo de cable es posible encontrar variantes como cable sin blindaje (**Unshielded Twisted Pair UTP**) y cable con blindaje (**Shielded Twisted Pair STP**), éste consiste en una capa de metal que protege al cable interior, es una malla tejida de hilos de metal.

Este medio es el que presenta más bajo costo pero también es el más vulnerable a el ruido, por lo que no se considera adecuado para altas velocidades o largas distancias.

Las instituciones encargadas de realizar las recomendaciones indican que para el cable UTP se deberá contemplar una distancia de 100 a 150m. como máximo y el cable STP 300 m. como máximo.

Cable coaxial

Este medio consiste en un conductor central de cobre, rodeado de otro conductor, generalmente una malla de hilos de metal, separados entre sí por un medio aislante, este apantallamiento evita interferencias.

El cable coaxial puede manejar un ancho de banda mayor al par trenzado. Además de clasificarse por su tamaño físico, también se clasifica por su impedancia.

Existen varios tipos de cable coaxial usados en redes locales:

- **Cable Ethernet**, que cumple con la especificaciones de este tipo de red y existen dos tipos:

Thin Ethernet.- RG-58U, distancia máxima por segmento 300 m.
impedancia de 58.5 ohms.

Thick Ethernet.-RG-11, distancia máxima por segmento
500 m. impedancia de 58.5 ohms.

- **Cable coaxial Arcnet**, RG-62, distancia máxima
de 600m. impedancia de 73 ohms.



Fibra óptica

Los cables anteriores deben colocarse en lugares libres de problemas ambientales evidentes, más el cable de fibras ópticas no tiene esa desventaja.

Este tipo de medio, novedoso, presenta excelentes características, desde el punto de vista eléctrico y mecánico, pero resulta muy costoso todavía.

Las fibras ópticas son hilos delgados de vidrio con un alto nivel de pureza, que se procesa desde silicatos a grandes temperaturas, para lograr un hilo fino y uniforme. Este medio tiene la ventaja de poder conducir información en forma de luz a velocidades mucho más altas que en el cobre y aún el oro.

Otra gran ventaja de este medio es que tiene un amplio ancho de banda, lo que nos permite transmitir información de diversa naturaleza, como voz, datos e imágenes con la misma facilidad.

Señales radioeléctricas

Este medio se basa en la transmisión vía ondas de radio u otros medios inalámbricos, haciendo uso de los diversos equipos necesarios para la adecuada transmisión de la información.

En la transmisión radioeléctrica se hace uso del aire como medio de transmisión, aprovechando el fenómeno electromagnético de las antenas tanto receptoras como transmisoras. Algunos ejemplos de lo anterior serían las comunicaciones vía microondas, vía rayos láser, hasta llegar a la transmisión vía satélite.

CONTROL DE ACCESO AL MEDIO DE COMUNICACION.

La forma en que las estaciones de la red accedan al uso del canal común de comunicación para depositar y recoger datos y los mecanismos existentes para controlar este acceso, representa una de las características más significativas de la planeación de cada red y condiciona el comportamiento global de ésta.

Los métodos aplicables en el control de acceso a las redes locales son múltiples y variados.



Los organismos de normalización² se han inclinado por adoptar sólo un número reducido de métodos de control de acceso, razón por la que solamente se comentarán dos técnicas (figura 1-10):

- 1.- Técnica de selección por **Token Passing**.
- 2.- Técnica de contienda. (**CSMA/CD**)

TECNICA DE TOKEN PASSING.

Esta técnica se conoce como "token passing" y consiste en que los usuarios deben esperar hasta ser seleccionados para poder depositar sus mensajes en la red.

Una variedad de las técnicas de selección es el método de acceso por sondeo, conocido como "polling"; que consiste en que una estación primaria (si el control es centralizado) selecciona al usuario enviando su dirección, que también es recibida por todos los demás usuarios.

El usuario seleccionado envía sus mensajes pendientes y posteriormente devuelve el control.

Una variedad de las técnicas por sondeo consiste en el uso de una clave o "token" que permita al dispositivo que lo posee hacer uso del canal de comunicación.

El testigo o "token" no es devuelto a una entidad sino que es pasado de un nodo a otro en un orden predeterminado, por lo que este método puede ser considerado como sondeo distribuido.

Dependiendo de la topología de la red, estas técnicas se subdividen en:

- 1.- Token Passing "token"en anillo (token ring).
- 2.- Token Passing en "bus"(token bus).

Token Passing "token"en anillo (token ring).

Esta técnica es usada en topologías de anillo. La descripción que se dará a continuación corresponde al estandar de IBM basado en la norma **802.5 de la IEEE**.

El funcionamiento básico consiste en una trama de bits, "token", que se transmite de nodo en nodo, cuando una estación lo recibe lo excluye de la circulación y comienza a transmitir el mensaje que tenía pendiente.

²Usualmente son IEEE y CCITT.



Al llegar a la estación destino, ésta reconoce su dirección y lo copia para después volverlo a transmitir pero con la información de "mensaje copiado" incluida.

La estación siguiente, al recibir el testigo, tiene la oportunidad de transmitir un nuevo mensaje pendiente.

De esta forma se asegura el uso de la red por parte de todos los usuarios siguiendo un orden prefijado por su posición relativa dentro del anillo.

Tal esquema puede ser refinado mediante la asignación de diferentes niveles de prioridad, esto es que al mismo tiempo que el mensaje circula, lleva una indicación de prioridad y reserva.

Cada estación examina la trama "token" y si su prioridad es mayor que la marcada y además, tiene mensajes pendientes por enviar, hace una reserva para que le sea enviado el testigo o "token".

La estación que envió el mensaje, antes de poner en circulación al testigo, analiza la petición de reserva que fué anotada durante la circulación del mensaje y marca el testigo para que le sea entregado a la estación con más alta prioridad.

Es posible que se presenten problemas cuando debido a alguna anomalía desaparece el testigo o se deteriora algún mensaje. Para resolver esto, se puede recurrir al control de la red por parte de alguna de las estaciones, que jugará el papel de monitorea del proceso.

Token Passing en "bus".

El principio de funcionamiento es muy similar al anterior, con la única diferencia de que la conexión al bus implica mayor flexibilidad a la hora de incrementar o decrementar el número de estaciones de trabajo.

Las redes locales para automatización industrial tienden a adoptar este método de acceso y el método se basa en la recomendación 802.4 de la IEEE.

El testigo o "token" controla el derecho de acceso al medio físico de manera que la estación que lo posee tiene momentáneamente el derecho de transmitir.

El testigo se pasa de estación en estación formando un anillo lógico. La trama de bits o "token" debe incluir por lo tanto, la dirección de la estación a la que le corresponde tomar el turno, lo que significa que cada estación debe conocer cuál es la siguiente dentro del anillo lógico.



Insertar una nueva estación o eliminar alguna ya existente, obliga a reestructurar las direcciones de encaminamiento de las estaciones afectadas.

La información transmitida por una estación es difundida por todo el bus, lo que hace posible que algunas estaciones puedan recibir mensajes aunque por estar fuera del anillo lógico por donde está circulando el testigo, nunca puedan tomar la iniciativa de transmitirlos, pero si pueden emitir respuestas.

Esta característica de difusión a lo largo del bus hace que el retardo de transmisión, una vez seleccionada la estación, dependa solamente de la velocidad de propagación en el medio y no del número de estaciones conectadas.

La asignación de prioridades en el uso del canal hace que se modifique el orden de entrega del testigo por parte de una estación.

Algunas de las características más importantes de este método son (figura 1-12):

- Eficiencia en situaciones de carga elevada ya que la coordinación entre las estaciones requiere sólo un pequeño porcentaje de la capacidad del medio.
- Proporciona un reparto equitativo de la capacidad del medio.
- Evita interferencias entre estaciones.
- Los módulos de conexión a la red son baratos debido a la sencillez del método de comunicación.
- Se pueden acotar el retardo máximo en el acceso al medio por parte de una estación, teniendo en cuenta las prioridades y la configuración de la red.
- El método presenta muy pocas restricciones frente a la manera en que una estación puede usar el medio durante el período de tiempo en que le corresponde acceder.
- Permite la presencia de estaciones de trabajo con jerarquías muy diferenciadas, por lo que pueden coexistir estaciones de bajo costo y reducidas funciones, junto con estaciones más complejas que además asumirán el control.



TECNICA DE CONTIENDA.

La técnica de contienda o CSMA/CD³ parte de la base de que, cuando una estación tenga que transmitir, deberá intentar competir con las restantes en el uso del canal.

Esto implica un riesgo de colisión entre los datos por lo que se hace necesario tener un árbitro.

Cuando una estación desea transmitir, "escucha" el canal antes de hacerlo para saber si está siendo usado por alguna otra transmisión. En caso de encontrarse ocupado el canal espera a que concluya y vuelve a intentarlo.

La estación seguirá en reposo siempre que no tenga mensajes que transmitir o si aún teniéndolos detecta la presencia de otra transmisión en el canal.

Ahora bien, si el canal está libre y la estación tiene mensajes, pasa a estado de transmisión, si termina su transmisión normalmente, regresa al estado de reposo.

Es posible que al empezar a transmitir otra estación esté en una situación similar y se genere una colisión, con la consecuencia de la pérdida de información, más esto sería suficiente para que los nodos transmisores detecten la situación y reinicien el proceso.

Para evitar la pérdida de tiempo ocasionada por los mecanismos antes mencionados, surge una mejora al método (es cuando se denomina CSMA/CD⁴).

Para lograr que se tenga una detección de colisiones se hace que las estaciones de trabajo continúen "escuchando" la línea aún después de transmitir.

Al detectar una colisión, deja de transmitir automáticamente.

Añadiendo además un tiempo de espera aleatorio se evita la posibilidad de una nueva colisión.

Este método es uno de los más populares en el campo de las redes locales.

³Las siglas significan Carrier Sense Multiple Access, o bien acceso múltiple con detección de portadora.

⁴Las siglas significan Carrier Sense Multiple Access, Collision Detect, lo que significa que se puede detectar las colisiones.



El trabajo conjunto de Digital, Xerox e Intel en el desarrollo de la red local Ethernet, en la que se usó la técnica de acceso CSMA/CD sentó un precedente que más tarde se afianzó con la normalización por parte de la IEEE en la norma 802.3.

BANDA ANCHA Y BANDA BASE.

Existen dos métodos principales de comunicación respecto al aprovechamiento

La diferencia entre redes de banda ancha (figura 1-13) y redes de banda base (figura 1-14); radica solamente en la forma en que se transmiten las señales por el canal.

Los diferentes medios para establecer la comunicación, tales como par trenzado, cable coaxial, etc, condicionan el tipo de señales eléctricas que pueden ser enviadas a través de ellos:

En las redes de banda base, las señales son transmitidas en forma de onda cuadrada directamente sobre el medio físico, aplicando dos niveles de voltaje diferenciados, cuyas transiciones representan los dos estados binarios.

En las redes de banda ancha es necesario modular una onda portadora con las señales digitales a transmitir.

La interfaz para acceder a una red en banda base es muy simple y de bajo costo, sin embargo en redes donde se usa la modulación es necesario incluir en la interfaz un *modem* o modulador/demodulador que actúe como intermediario entre las señales manejadas por la estación y las que fluyen por el canal.

La característica principal en las redes de banda ancha es la creación de múltiples canales paralelos con un único medio físico como soporte, para ello el espectro de frecuencias se divide en canales de un determinado ancho de banda por cada uno de los cuales va a circular información distinta.

Los distintos canales creados por multiplexación de frecuencia tienen entre sí diferentes anchos de banda, dependiendo de la misión específica a la que cada uno sea destinado; así se logra transmitir por un sólo medio simultáneamente información de voz, datos e imágenes.

En este tipo de redes las señales transmitidas han de serlo en una sola dirección, por lo que se debe establecer un canal para la recepción y otro para la transmisión, esto se puede lograr de dos formas:

- 1.-Dividiendo el ancho de banda de un sólo cable, o bien
- 2.-Usando un cable para la transmisión y otro para la recepción.



En caso de usar un sólo cable, el ancho de banda necesario es el doble que si se usan dos cables, aunque también se reduce el costo de instalación.

Además, en este caso habría que dotar a la red de un convertidor de frecuencia con el fin de trasladar la transmisión a la frecuencia de recepción en el cable.

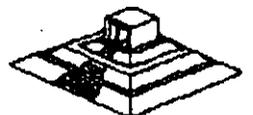
Un problema adicional que se presenta con la necesidad de instalar el convertidor de frecuencia es la posibilidad de que se averíe y toda la red quede fuera de uso.

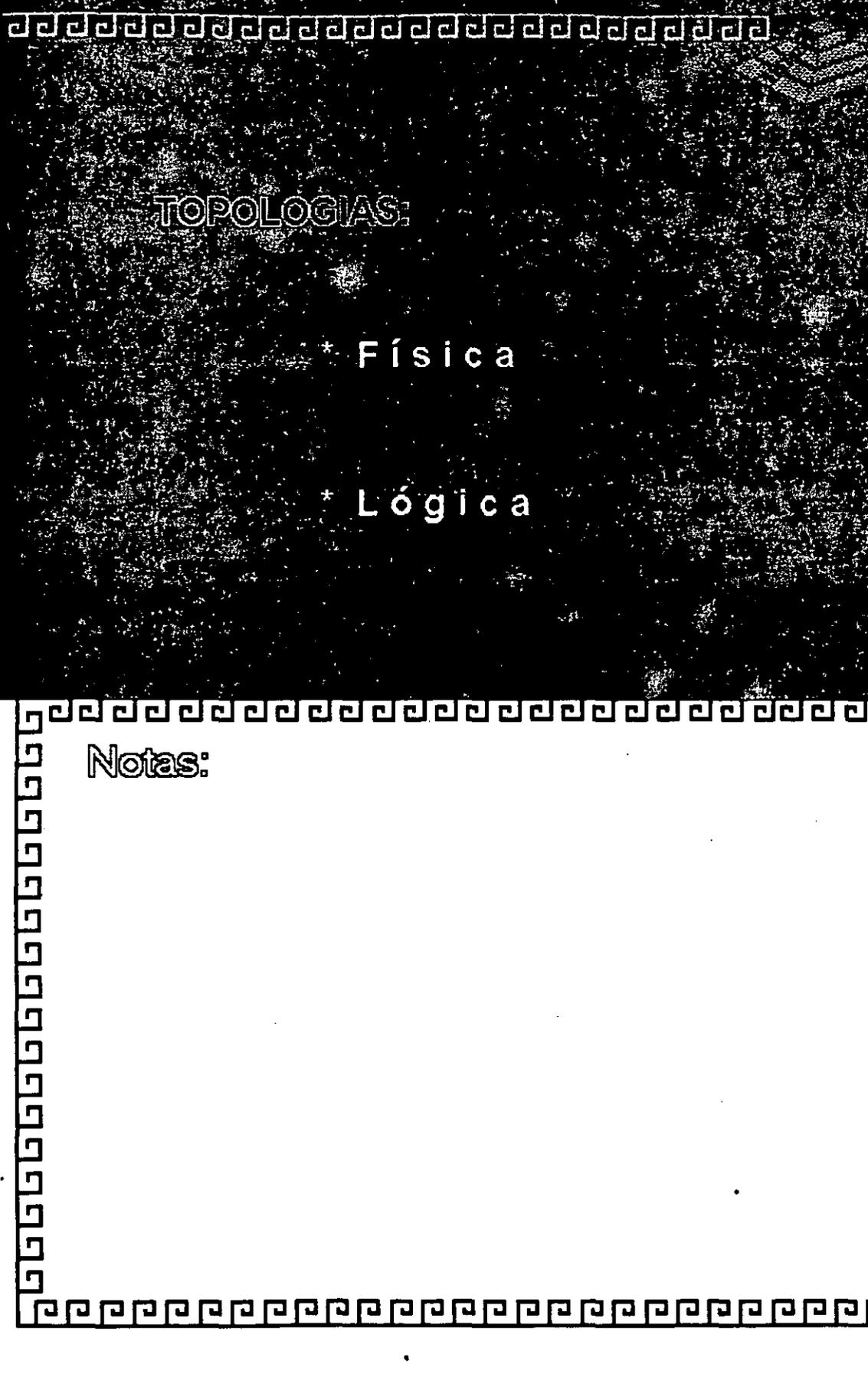
Si se usan dos cables disminuye la posibilidad de una falla y aumentaría en el doble la capacidad del canal de datos. Un elemento fundamental en las redes de banda ancha es el *modem* que, conectado a cada nodo se encarga de convertir las señales.

El modem debe tener algunas características muy especiales para poder adaptarse a las altas velocidades de transmisión de estas redes.

De todo lo anterior se puede inferir que las redes de banda ancha son de un alto costo debido a las singulares características que deben reunir sus componentes, al contrario de las redes de banda base, que resultan más económicas.

A cambio del alto costo, se tienen ventajas que las hacen muy atractivas, como las altas velocidades que son posibles de obtener para transmitir, además de su fiabilidad, lo que las hace ideales para el tratamiento integral de la información incluyendo en un mismo medio los datos, la voz y las imágenes.



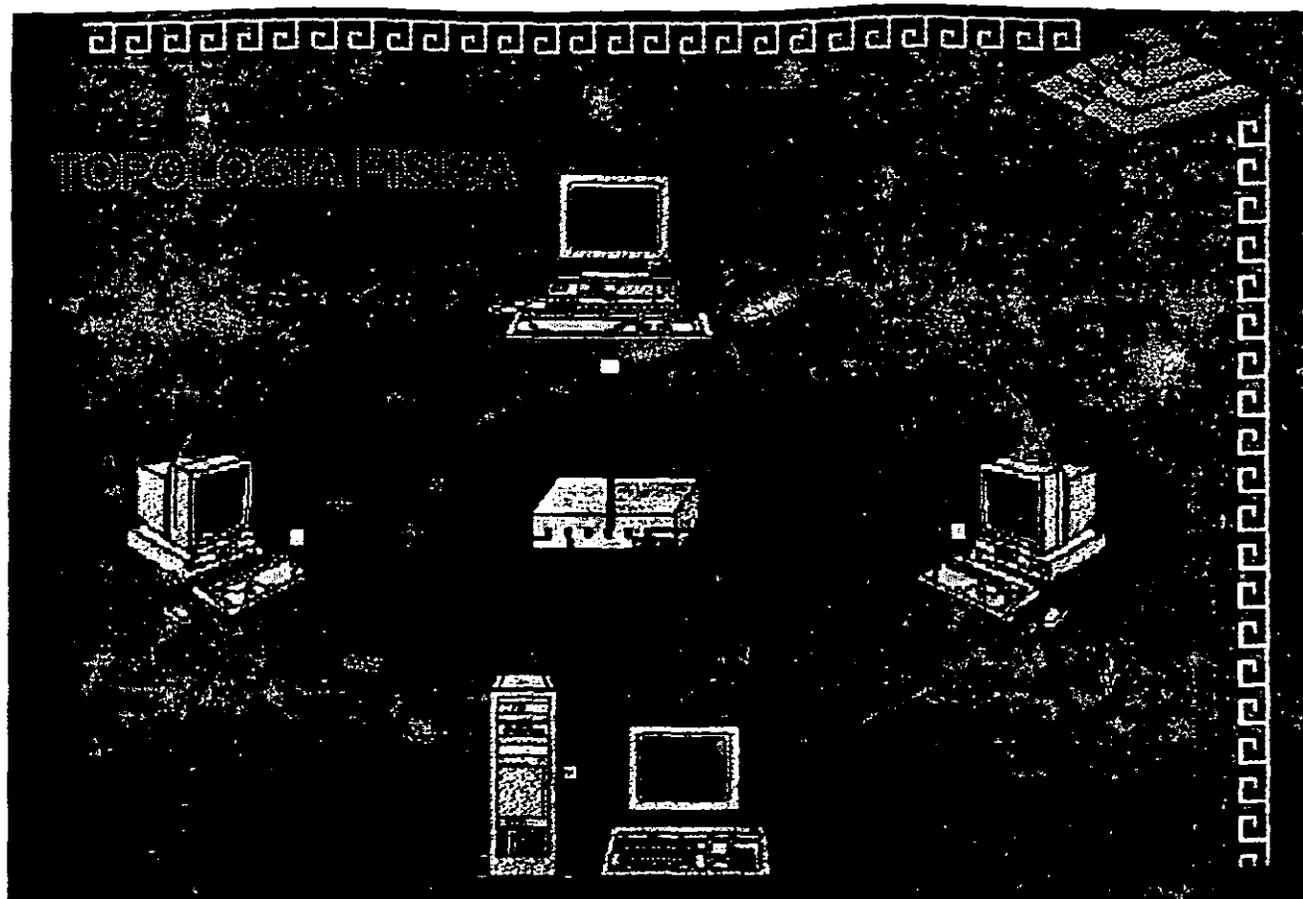


TOPOLOGIAS:

* Física

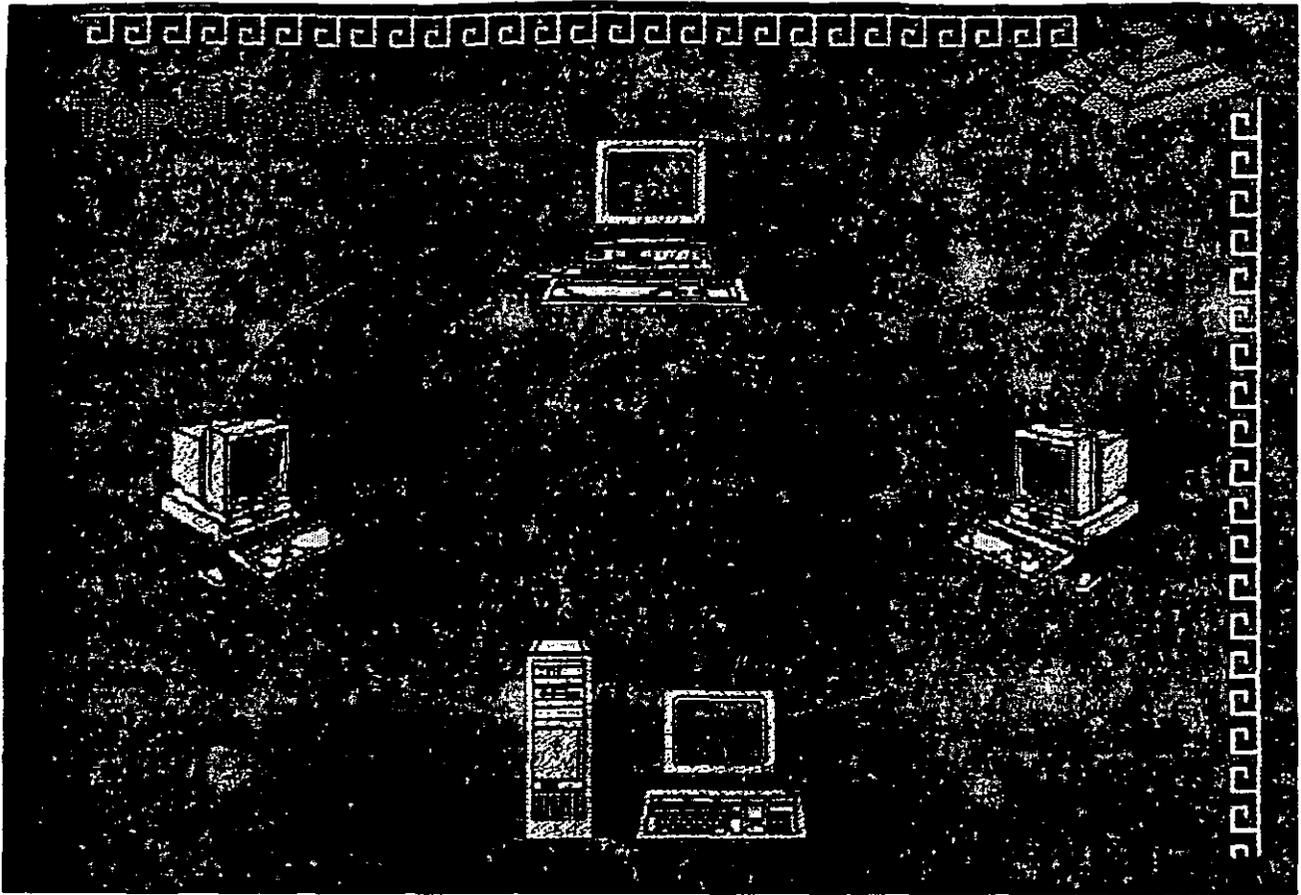
* Lógica

Notas:



Notas:

Figura 1-2



Notas:

Figura 1-3

NODOS:

- * Servidores
- * Estaciones de trabajo
- * Nodos de Impresión
- * Elementos de unión a otras Redes

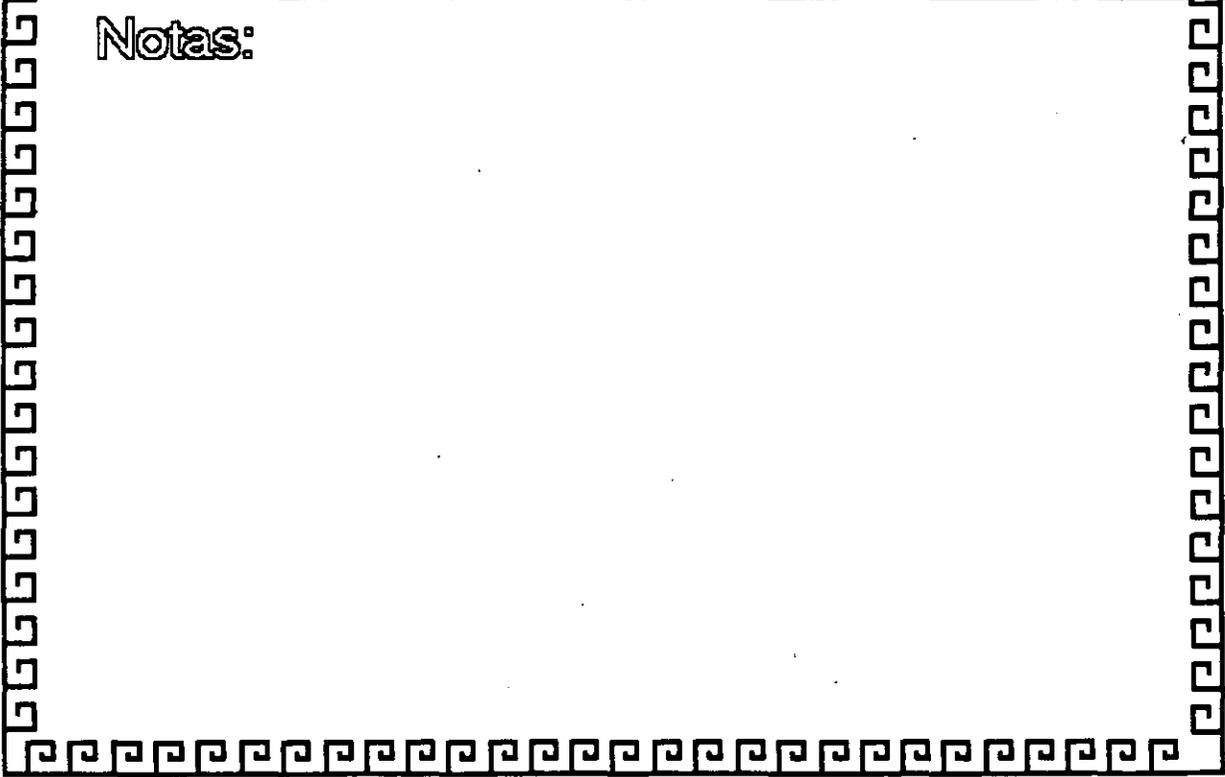
Notas:



ELECCION DEL MEDIO DE COMUNICACION

- * Cubrir ancho de Banda necesario
 - * Cubrir las velocidades requeridas
 - * Cubrir las distancias requeridas
 - * Adaptacion del entorno Físico-Geográfico
 - * Minimizar posibilidades de fallas
 - * Posibilidades de crecimiento y modularidad
 - * Minimizar costos de Instalación y Mantenimiento
- 

Notas:





PRINCIPALES MEDIOS FISICOS

Par
Trenzado



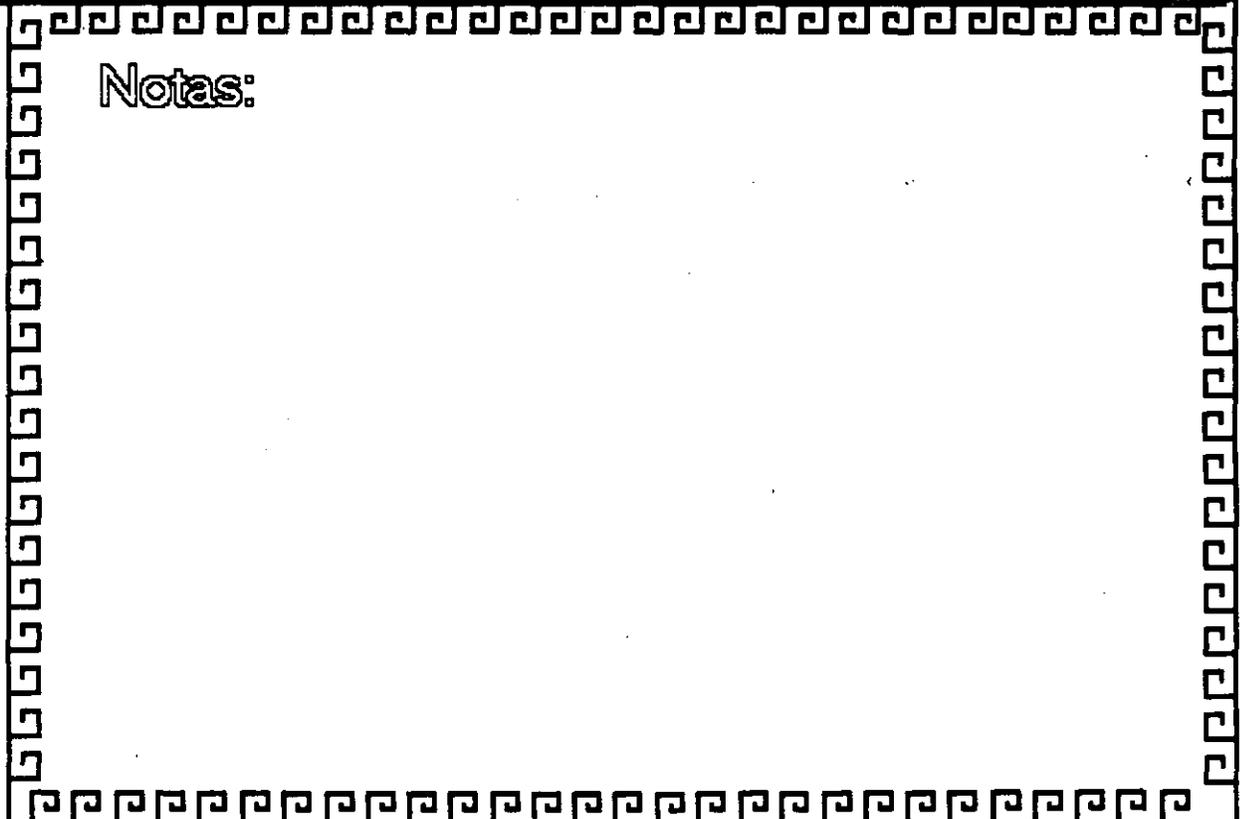
Coaxial



Fibra Optica



Señales Radioeléctricas



Notas:

Figura 1-8



PRINCIPALES MEDIOS FÍSICOS

Par
Trenzado { STP.- Shielded Twisted Pair
 { UTP.- Unshielded Twisted Pair

Coaxial { RG58U.- Thin (Ethernet)
 { RG11.- Thick (Ethernet)
 { RG62.- Arcnet

Fibra Optica

Señales Radioeléctricas



Notas:

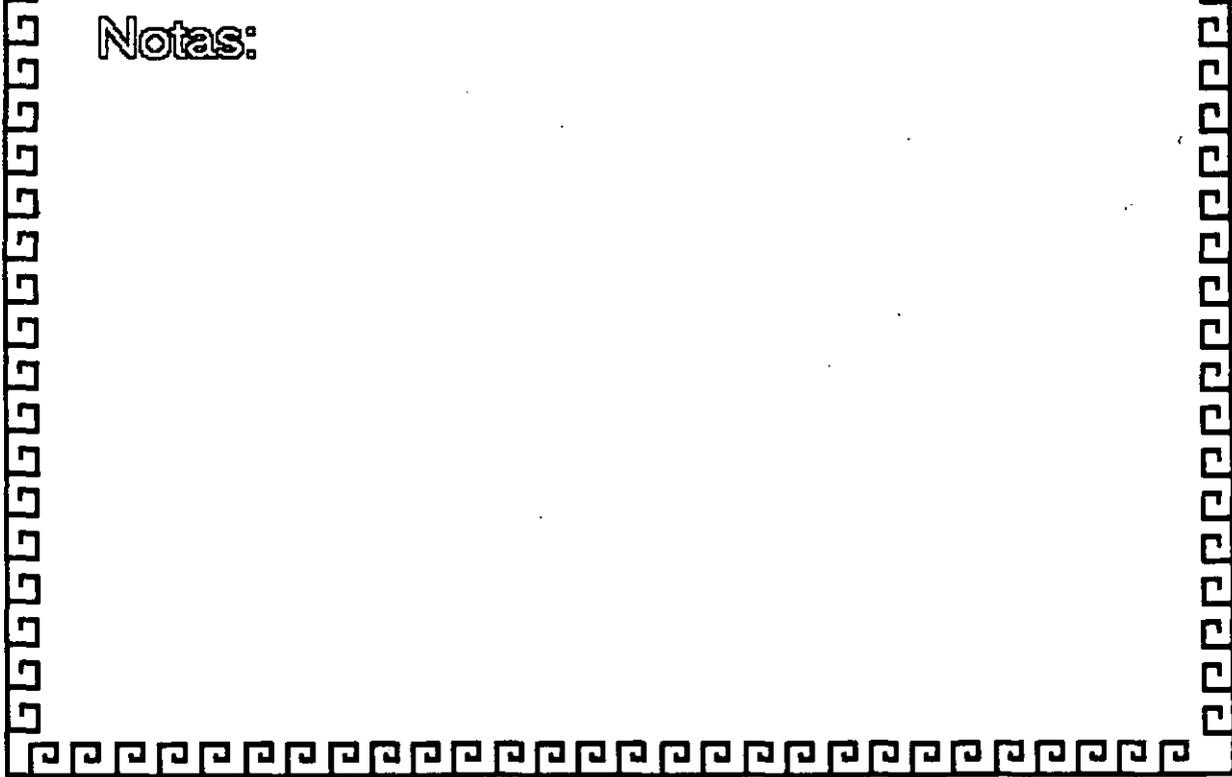
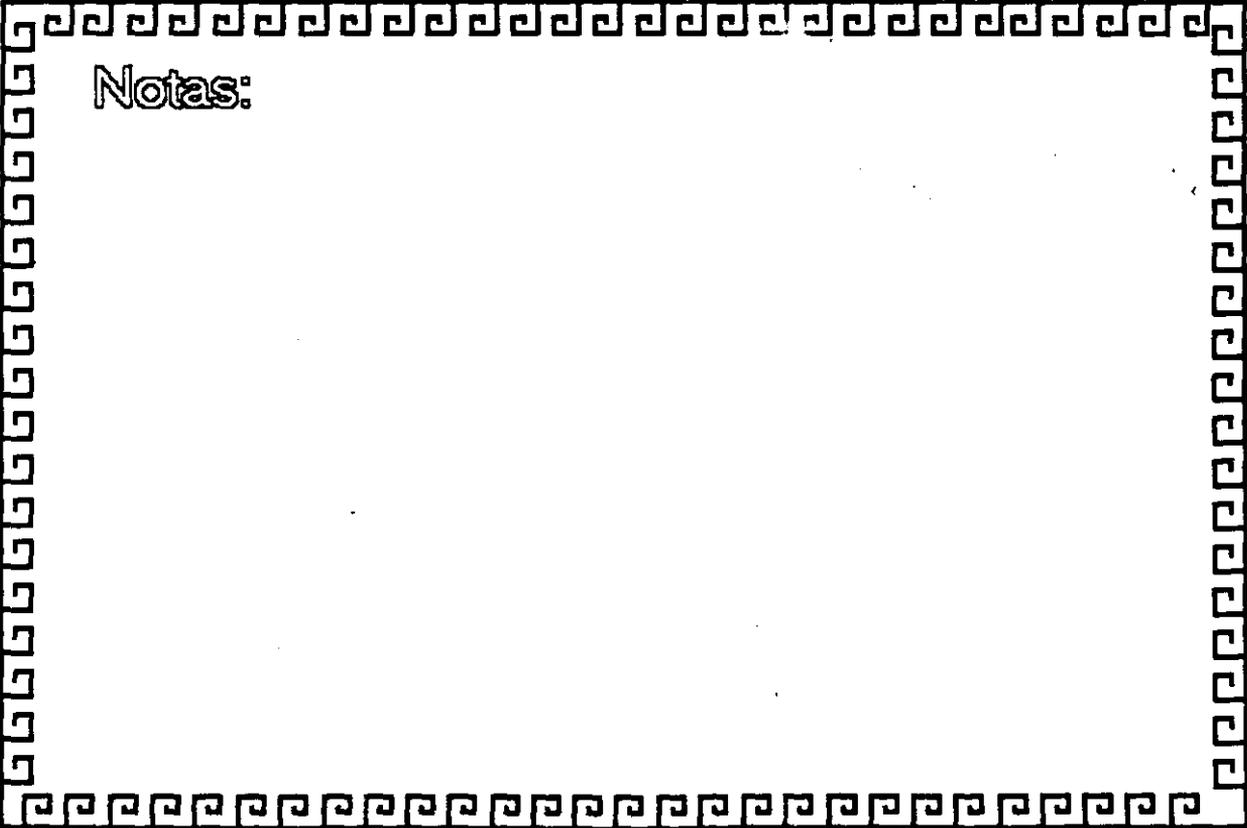


Figura 1-9



**CONTROL DE ACCESO AL MEDIO
DE COMUNICACION**

- * Técnica de Selección de Token Passing
- * Técnica de Contienda (CSMA/CD)



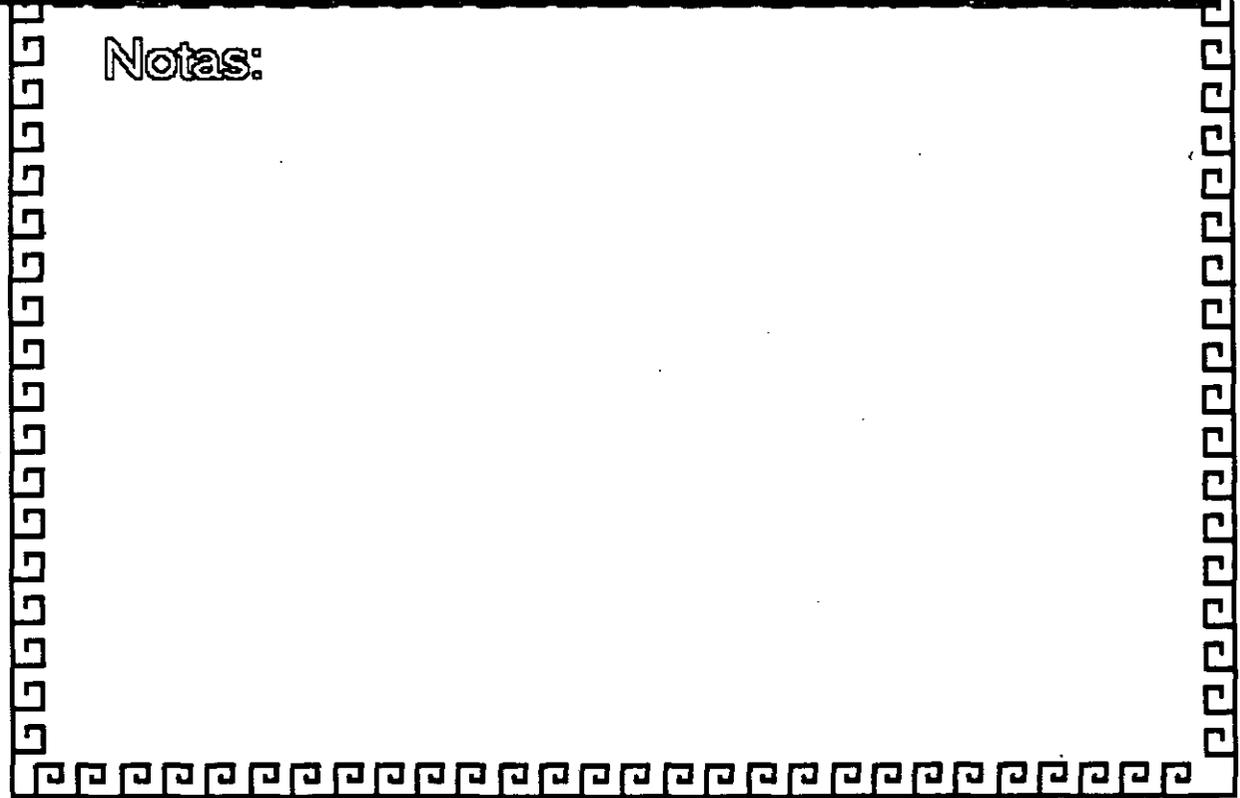
Notas:



TECNICAS DE SELECCION
TOKEN PASSING

* Token Passing en Anillo.- Token Ring
Norma IEEE 802.5

* Token Passing en Bus.- Token Bus
Norma IEEE 802.4



Notas:



PRINCIPALES TIPOS DE REDES

- Banda ANCHA
- Banda BASE



Notas:

Figura 1-12

CARACTERISTICAS TOKEN BUS

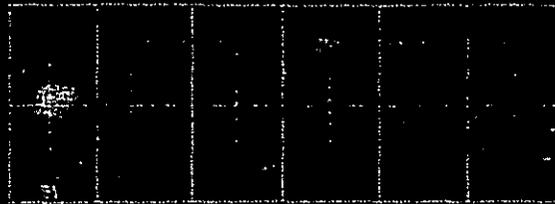
- * Uso Industrial
- * Eficiente con cargas elevadas
- * Reporte equitativo del medio
- * Evita interferencias entre Nodos
- * Económico
- * Permite jerarquización de Nodos
- * Permite conexión de Nodos sencillos o muy complejos

Notas:

BANDA BASE

Características

- * Un sólo canal
- * Bajo costo
- * Se modula y demodula la señal
- * Utilizada por los estándares actuales de REDES locales



Notas:

TOPOLOGIA

Factores de Análisis

- a) Protocolo de Comunicación Física
- b) Flexibilidad para agregar o eliminar nodos
- c) Repercusiones sobre falla en algún nodo
- d) Problemas en el flujo de Información
- e) Versatilidad en el diseño del cableado
- f) Posibilidad de crecimiento

Notas:

CURSO : REDES LAN DE MICROS PARTE II
MODULO II DEL DIPLOMADO DE REDES LOCALES

2.-)TARJETAS PARA RED
ANÁLISIS, COMPARACIÓN Y NORMAS.



TARJETAS PARA RED ANÁLISIS, COMPARACIÓN Y NORMAS.

MODELO DE REFERENCIA ISO-OSI

El modelo OSI⁵ estructura en siete niveles o capas el fenómeno global de la comunicación, es un marco hoy en día obligado y universalmente aceptado.

Las normalizaciones en redes locales tratan de encuadrarse dentro de este modelo. Además, las redes locales deberán acoplarse a las redes públicas de área extendida actualmente existentes y en permanente expansión.

El modelo para la interconexión de sistemas abiertos, ISA⁶ u OSI⁷ se ha convertido en una referencia obligada para todo lo relacionado con la intercomunicación de computadoras.

Frecuentemente, en artículos o descripciones relacionadas con este tema, se encuentra un dibujo de la "torre" de siete niveles y un enunciado somero, y habitualmente poco claro, de las funciones y cometidos de cada uno de ellos.

La estructura jerarquizada de este modelo se explica a continuación:

Por ejemplo, si se analiza una estructura humana de comunicación de mensajes, se puede describir ésta mediante un determinado número de niveles de abstracción de los distintos fenómenos y tareas que se producen.

Imagínese una comunicación donde el mensaje emitido tiene un nivel cognoscitivo relacionado con cualquier materia o asunto, de manera que para el receptor pueda entenderlo debe estar al corriente de la materia que se trate. (Figura 2-1)

Este mensaje ha de ser codificado en un lenguaje natural concreto, por ejemplo inglés o español.

Además para poder transferir el mensaje al receptor, será necesario utilizar algún medio físico concreto (ondas sonoras, papel, etc.) y elegir un método acorde con este medio.

En el lugar del receptor el proceso sería el mismo pero en orden inverso.

⁵ International Standards Organization

⁶ Siglas en español

⁷ Siglas en inglés, Open System Interconnection



En cada estación debe haber una comunicación interna entre niveles, de arriba a abajo en el emisor y de abajo hacia arriba en el receptor, lo que obliga a la existencia de una interface adecuada entre niveles consecutivos.

Por ejemplo:

Si para N1 se elige el método escrito en un determinado alfabeto será necesario en el emisor, alguien que sea capaz de escribirlo y en receptor alguien que sea capaz de interpretarlo.

La idea que se pretende hacer quedar clara es que, tiene que haber una coherencia entre cada par de niveles. Por lo tanto, si el lenguaje elegido es el castellano, éste debe ser el mismo en ambas estaciones.

Esto significa que existen entre niveles homólogos unos *protocolos de pares*, es decir, un conjunto de reglas que permiten relacionar horizontalmente a dos entidades de comunicación.

A nivel cognoscitivo, de nada sirve al oyente de un mensaje en castellano, tener un magnífico oído y un buen conocimiento de la lengua si no entiende el tema del que se está hablando.

En una comunicación estratificada en niveles, la comunicación real se hace en niveles consecutivos dentro de una misma estación y solamente a través del medio físico en la comunicación entre dos estaciones; aunque desde el punto de vista lógico es más interesante hablar de la comunicación entre niveles homólogos mediante protocolos de pares.

ESTRUCTURA GENERAL DEL MODELO.

Desde el punto de vista de ISO, un sistema abierto es el conjunto de una o más computadoras con su software, periféricos y terminales, capaces de procesar y transmitir información.

Es un modelo que está relacionado con las funciones que tienen que ser desarrolladas por el hardware y el software para obtener una comunicación fiable e independiente de las características específicas de la máquina. Es decir, está pensada para la interconexión de sistemas heterogéneos.

El sistema está compuesto por siete niveles, mediante los cuales dos sistemas informáticos se comunican entre sí.

Con frecuencia, quienes inician el estudio del modelo se preguntan la razón de que sean siete niveles en la arquitectura y no un número mayor o menor.



Si se volviera al ejemplo anterior(de la comunicación humana), se vería que los tres niveles mediante los que se describe, podrían ser ampliados pensando por ejemplo, en la naturaleza del medio de comunicación, si se han elegido tres es porque así queda suficientemente bien dividido y descrito el problema.

De la misma manera, el grupo de estudio que elaboró el modelo OSI pensó que la división en siete niveles era una buena propuesta, pero eso no significa que tenga que ser necesariamente así.

No obstante, este modelo ha sido plenamente aceptado tanto por fabricantes como por usuarios.

Las características del modelo podrían resumirse de la siguiente forma:

- Cada nivel está representado por una entidad de nivel. Los niveles equivalentes en dos sistemas diferentes se comunican de acuerdo con unas reglas y convenios denominados *protocolos de nivel o protocolos de pares*.

- Cada nivel proporciona un conjunto definido de servicios al nivel superior y a su vez utiliza los servicios que le proporciona el nivel inmediatamente inferior.

- La comunicación se realiza a través de los niveles inferiores, siendo el protocolo de pares una abstracción lógica de relación entre las dos entidades comunicantes.

- Si un nivel N desea transmitir una unidad de datos a otro nivel N homólogo en otro sistema informático, se la pasará al nivel inmediatamente inferior, el cual le añadirá información delimitadora propia y a su vez pasará esta información a su nivel inmediatamente inferior.

En el sistema receptor cada nivel separará la parte del mensaje que le corresponde y pasará el resto a su nivel inmediatamente superior, que hará lo propio. Así el mensaje del nivel N es como si viajara horizontalmente hasta su nivel homólogo en recepción.

LOS SIETE NIVELES.

Los tres primeros niveles tratan los protocolos asociados con la red de conmutación de paquetes utilizada para la conexión y pueden agruparse dentro del llamado bloque de transmisión.



El nivel cuatro enmascara a los niveles superiores los detalles de trabajo de los niveles inferiores dependientes de la red, y junto con ellos forma el bloque de transporte.

Los tres niveles superiores, del quinto al séptimo, son los usuarios del bloque de transporte y aíslan la comunicación de las características específicas del sistema informático.

A continuación se analizan uno por uno los diferentes niveles, estudiando sus funciones y características.

EL NIVEL SIETE: APLICACION

Este nivel se preocupa de proporcionar un conjunto de servicios distribuidos a los procesos de aplicación de los usuarios. El usuario se comunicará directamente con este nivel a través de la correspondiente interface o agente de usuario.

Actualmente se están desarrollando una serie de normas y recomendaciones tendientes a tipificar cada uno de estos servicios o aplicaciones distribuidas.

Entre los más conocidos podemos citar:

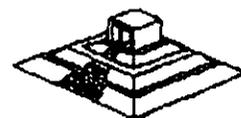
- Servicio de mensajería(correo electrónico), servicio de almacenamiento y recuperación de documentos, servicio de directorio, etc.

EL NIVEL SEIS : PRESENTACION.

Este nivel se ocupa de la representación de los datos usados por los procesos de aplicación del nivel siete. Por lo tanto, si es necesario, realizará la transformación de los datos que reciba de o para el nivel de aplicación.

Esto en el caso de que el proceso originador y el receptor tuvieran versiones de datos sintácticamente diferentes, pero también puede darse el caso de que para una determinada aplicación distribuida exista un conjunto de caracteres normalizados diferentes de los del originador y el receptor, en cuyo caso los niveles de presentación respectivos deberían de hacer las transformaciones necesarias.

Otra función que se puede encargar al nivel seis, es la de velar por la seguridad de los datos, siendo responsable de la encriptación de mensajes confidenciales antes de su transmisión. La función inversa será realizada por el nivel de presentación del sistema receptor.



NIVEL CINCO: SESION.

Su función es establecer y gestionar un camino de comunicación entre dos procesos del nivel de aplicación. Este nivel establece una sesión y se encarga de controlar la comunicación y sincronizar el diálogo.

La información que se envía se fracciona en pedazos y se generan unos puntos de sincronización. En caso de interrumpirse la sesión por alguna falla en la comunicación, los datos pueden ser recuperados y se conoce con precisión por ambos interlocutores hasta qué punto de sincronización la comunicación fue correcta.

Al reanudarse la sesión no será necesario transmitir de nuevo toda la información, sino solamente a partir del punto donde se quedó el último paquete de información válido.

En una sesión hay un diálogo entre máquinas, entre procesos y el protocolo debe regular quién "habla", cuándo y por cuánto tiempo.

Estas reglas necesitan ser acordadas cuando la sesión comienza. Este nivel también es responsable de dirigir el diálogo entre las entidades de nivel de presentación.

Para ello, cuando se establece una conexión de sesión, es necesario que ambos niveles cinco se pongan de acuerdo sobre el papel a desempeñar por cada uno de ellos en la comunicación.

NIVEL CUATRO: TRANSPORTE.

Este nivel es responsable de una transferencia de datos transparente entre dos entidades del nivel de sesión, liberando a dichas entidades de todo lo referente a la forma de llevar a cabo dicho transporte.

Los protocolos que maneja este nivel suelen llamarse *protocolos end-to-end*, o protocolos entre puntos finales, debido a que este nivel se encarga de realizar una conexión lógica entre dos estaciones de transporte de los sistemas informáticos que quieren comunicarse, independientemente de donde se encuentren estos.

Este nivel puede multiplexar varias conexiones de transporte dentro de una única conexión de red o puede, por el contrario, repartir una conexión de transporte entre varias conexiones de red.



NIVEL TRES: RED.

Este nivel enmascara todas las particularidades del medio real de transferencia. Es el responsable del encaminamiento de los paquetes de datos a través de la red. Cada vez que un paquete llega a un nodo, el nivel tres de ese nodo deberá seleccionar el mejor enlace de datos por el que envíe la información.

Las unidades de datos de este nivel son los paquetes de datos que deberán ir provistos de la dirección de destino. Por lo tanto, entre las funciones fundamentales del nivel de red se encuentran las de establecer, mantener y liberar las conexiones necesarias para la transferencia de los paquetes de datos.

Además son funciones de este nivel la definición de la estructura de datos de los paquetes, las técnicas de corrección de errores, la entrega en secuencia correcta al nivel de transporte de los paquetes recibidos, así como otras de reiniciación y control de flujo.

Para las redes públicas de transmisión de datos la CCITT ha definido la norma X.25 que describe los protocolos de comunicación para los niveles uno, dos y tres del modelo de referencia de ISO.

NIVEL DOS : ENLACE.

Un enlace de datos se establece siempre entre dos puntos físicos de conexión del sistema. En el caso de una red de datos de conmutación de paquetes, el nivel de enlace es responsable de la transferencia fiable de cada paquete al nivel de red.

La CCITT ha definido dentro de la recomendación X.25 un subconjunto del protocolo HDLC⁸ como protocolo del nivel de enlace.

NIVEL UNO: FISICO.

Este nivel engloba los medios mecánicos, eléctricos, funcionales y de procedimiento para acceder al medio físico. Es el encargado de la activación y desactivación física de la conexión. Ciertos protocolos estandar clásicos como el X.21 y V.24 son utilizados en el nivel físico.

Cada estación de trabajo y servidor, requieren de una tarjeta de red o interface, el propósito de esta tarjeta es para poder comunicarnos por medio de un conducto "inteligente" por el que estaremos moviendo los datos de un lugar a otro de la red.

⁸ High Level Data Link Control



Para ilustrar lo anterior, se verá cada uno de los estándares para tarjetas de interface.

ETHERNET

Es un estandar que se sustenta en los estratos fisico (uno) y de enlace de datos (dos) del modelo OSI. Corresponde a la recomendación 802.3 de la IEEE.

La parte del estandar que entra en el estrato de enlace de datos consta del subestrato de control de acceso a medios y del control del enlace lógico, en lugar de encomparar un protocolo de transmisión de datos completo.

Los servicios MAC para Ethernet incluyen CSMA/CD y el formato de cuadros básico. Existe flexibilidad en el formato de cuadros, en particular con respecto a las direcciones fuente y destino que pueden tener 16 o 48 bits de longitud.

Lo que en un principio fue un prototipo de Xerox Corporation, desarrollado durante los años 70 como un intento de aprovechamiento de recursos en su centro de investigación, se convirtió posteriormente en la primera red local comercial en 1980, año en que Xerox, Digital e Intel publicaron las especificaciones definitivas de Ethernet.

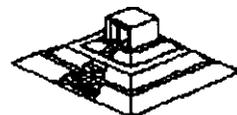
Las características generales son:

Topología	Configuración en bus o árbol
Medio físico	Cable coaxial de 50 ohms
Medio de transmisión	Banda base
Método de acceso	CSMA/CD
Número máximo de nodos	1024
Vel. máxima de transmisión	10 Mbps
Separación max. entre nodos	2.5 KM

Esta red constituye la especificación de los dos primeros niveles de una arquitectura telemática jerarquizada. Por lo tanto, lo único que resuelve la red Ethernet es la problemática de mantenimiento del enlace de datos activo entre dos nodos y libre de errores.

En el aspecto hardware, diversas marcas han provisto al mercado de varios dispositivos y tarjetas capaces de actuar como controladores de enlace Ethernet.

En cuanto al software, puede recurrirse a la adquisición de paquetes especialmente desarrollados, o bien optar por las ofertas que se adaptan a los niveles superiores.



Dado que han surgido implantaciones de la red Ethernet antes de la elaboración de las recomendaciones TOP, existe una amplia oferta de software comercial que puede dar solución a la mayoría de los requerimientos de comunicación y recursos compartidos.

La red local Ethernet típica consta básicamente de tres componentes: los nodos, los controladores y los sistemas de transmisión.

El sistema de transmisión incluye todos los componentes necesarios para establecer una comunicación entre controladores o, más propiamente, entre nodos. Esto incluye el medio de transmisión y recepción (transceivers o transreceptores) y opcionalmente, repetidores para extender la capacidad del medio.

El medio de transmisión acaba por ambos extremos en unos dispositivos denominados terminadores, cuya función es la de evitar la pérdida de la señal por reflexiones debido a desacoplos.

Los transreceptores contienen la electrónica necesaria para transmitir y recibir señales en el canal, además de conocer la presencia de señal cuando otro nodo está transmitiendo (carrier sense) también han de ser capaces de detectar una colisión cuando dos nodos envían mensajes simultáneamente.

Los repetidores son usados para extender la longitud del sistema de transmisión más allá de los límites impuestos por el medio. Un repetidor usa dos transreceptores para conectar dos segmentos de la red y combinarlos en un único canal lógico, amplificando y regenerando las señales que circulan en ambos sentidos.

Los repetidores son transparentes para el conjunto del sistema y los nodos situados en diferentes segmentos de la red pueden colisionar. Por consiguiente, el repetidor debe propagar la detección de colisión de un segmento a otro.

Controladores

El controlador posee el conjunto de funciones y algoritmos necesarios para dirigir el acceso al canal común. Aquí se realizan prácticamente todas las acciones a desarrollar por el nivel físico de esta arquitectura.

El controlador, normalmente, suele ser una tarjeta de circuito impreso que trabaja conjuntamente con la estación conectada a la red y que ejerce de interfaz con la conexión de la misma.

Actualmente, pueden encontrarse en el mercado circuitos integrados VLSI controladores de Ethernet que realizan la mayor parte de las tareas de conexión.

Las funciones propias del enlace a la red las realizan los dos niveles inferiores de la arquitectura: el nivel físico y el de enlace de datos, cada uno de ellos con unas funciones muy definidas que interactúan por medio de interfaces



El nivel de enlace de datos es independiente del medio sobre el cual se transmite y sus principales funciones son:

1. Encapsulado y desencapsulado de datos
2. Control de enlace de datos

A su vez, la función de encapsulamiento de datos tiene como misiones principales la generación de las tramas a ser enviadas, así como el direccionamiento de origen y destino de las mismas y la detección de errores producidos en la transmisión y recepción.

El nivel físico es el encargado del acceso al canal común en el aspecto más elemental, controlando los niveles de voltaje de las señales, la temporización, la codificación de los datos, etc.

La red local Ethernet usa como medio de transmisión el cable coaxial y como modo de transmisión la banda base, lo que provoca la existencia de ciertas limitaciones en cuanto a la distancia máxima. La configuración estandar posee una longitud máxima por segmento de 500 m. Cada nodo debe estar separado al menos 2.5 m. (Con cable grueso). Este tipo de red se recomienda cuando se necesita extender la red local por varias plantas de un edificio.

Cuando los requerimientos de distancia son menores, el estandar Ethernet soporta una opción más barata, denominada Thin Wire (cable delgado), que con un cable de inferior calidad (RG-58) y con conexiones más sencillas puede lograr una cobertura máxima de 300 m.

Para la necesidad de una cobertura mayor hay una oferta, denominada Broad Band. En realidad, esta opción usa un cable de banda ancha y las técnicas de cambio de frecuencia y doble cable son igualmente viables. Aquí la longitud del segmento de cable puede ser de hasta 3800 m., aunque el costo es lógicamente más alto.

En banda ancha, el controlador Ethernet situado en la computadora es conectado a un modem especial llamado DECOM, y éste a su vez, va conectado directamente al cable común. DECOM puede ser usado en los dos tipos de redes en banda ancha, simple o doble cable.

En las configuraciones de banda base, la forma de conexión es completamente distinta en las redes estandar que en las Thin Wire. En el primer caso, la conexión del controlador de comunicaciones al cable coaxial se hace por medio de un transreceptor, como ya se vió. En caso de usarse la configuración de Thin Wire, la forma de conexión es completamente distinta, más simple. Cada nodo es conectado a un adaptador terminado en un conector "T", al que va directamente unido el segmento de cable.

En cada segmento de cable el número máximo de transreceptores posibles es de 100. Un nodo insertado en la red es unido al transreceptor por un cable de cuatro pares de hilos cruzados. Este cable tiene una longitud máxima de



Repetidores

Los repetidores son dispositivos diseñados con el fin de extender la longitud de la red más allá de los 500 mts máximos de segmento de cable coaxial. Cada repetidor puede añadir un nuevo segmento al cual pueden ser conectados 99 transreceptores adicionales. Existen dos tipos de repetidor: local y remoto.

El repetidor local es usado para conectar dos segmentos de cable separados por una distancia máxima de 100 mts, mientras que el repetidor remoto (usando fibra óptica) conecta segmentos separados hasta 1000 mts y sólo se puede usar un repetidor remoto en una red.

Un servidor es cualquier nodo de la red que contiene recursos compartidos. Cada terminal conectada a un servidor puede acceder cualquier computadora que este conectada en la red. Es posible conectar terminales asincrónicas con velocidades de hasta 19,200 bps.

Gateways (Pasarelas)

Existe también la posibilidad de conectar redes Ethernet a otros tipos de redes, tanto locales como de área extendida , esto se puede conseguir por medio de gateways.

los principales tipos son:

- Ruteadores
- SNA
- X.25
- Para concentradores 3270

El Router tiene como misión principal permitir a los usuarios, hacer uso de las comunicaciones sobre la red telefónica conmutada, usando una amplia gama de productos de comunicaciones.

El SNA Gateway permite conectar la red con sistemas IBM que soporten SNA.

El X.25 Gateway es una extensión del Router que incluye además la posibilidad de usar redes de conmutación de paquetes que soporten protocolos X.25 para establecer el intercambio de información con otros procesadores.

La combinación de redes locales con Bridges y Gateways proporciona la posibilidad de crear conjuntos de redes cuya extensión geográfica es ilimitada, y cuya capacidad permite la coordinación de cientos, quizás miles de equipos de distintas características.



Existe software disponible, que permite realizar una serie de funciones sobre la red Ethernet, así como sobre la red extendida, usando la facilidad de comunicación vía redes de conmutación de paquetes existentes y conexiones punto a punto.

Este software proporciona todos los servicios necesarios para que las distintas computadoras puedan comunicarse, dichos servicios son:

Comunicación programa a programa.- Dos programas corriendo en nodos diferentes pueden intercambiar datos.

Terminal virtual de red.- Permite a terminales conectadas a un nodo cualquiera actuar como si físicamente estuvieran conectados a otro nodo.

Transferencia de archivos

Comando remoto.- (procesos batch) Un usuario de un nodo puede solicitar la ejecución de un archivo de comandos en otro nodo.

Acceso a recursos remotos.- Permite que sean compartidos recursos como dispositivos periféricos o archivos de base de datos.

Transferencia de software.- Permite la carga remota del software necesario para el funcionamiento de algunos servidores.

TOKEN-RING

Este estandar surgió en 1985 aproximadamente, su creador fue IBM y se apega al estandar 802.5 de IEEE. Como su nombre lo indica, emplea una topología de anillo y el método de acceso con transmisión de señales.

Comunmente, las estaciones de trabajo se conectan con par trenzado brindado o no brindado, hacia un concentrador de conexiones llamado unidad de acceso a multiestaciones o MAU.

Esto con el fin de no tener que depender de la confiabilidad del cableado para el correcto funcionamiento de la red. Los MAU son aparatos confiables que además facilitan la instalación de la red, así como su mantenimiento.



La red original Token Ring operaba a 4 Mb/s con un máximo de 100 metros del concentrador de conexiones a una computadora y 72 estaciones que usaban cable UTP especial de IBM. Más tarde en 1989, se extendió hasta 16 Mb/s. Cuando se usa par trenzado brindado (STP) se pueden construir LAN mayores de hasta 260 estaciones.

Una dificultad que compartían los fabricantes de hardware para redes Token Ring en común con IBM, era que el precio de lista de una tarjeta de interface ordinaria era aproximadamente el doble de una tarjeta de interface Ethernet, además, en la versión de 16 Mb/s se requiere cable dúplex trenzado aislado, lo que eleva aún más los costos de instalación.

Características

Topología	Configuración en anillo
Medio físico	Cable de par trenzado (UTP o STP)
Modo de transmisión	Banda base
Método de acceso	Token passing
Número máximo de nodos	260
Velocidad máxima de transmisión	4 Mbps o 16 Mbps

Formato de la trama

Hay dos formatos básicos de los mensajes que se intercambian los nodos para la transmisión de los datos y control: Token y tramas de datos.

Contiene campos delimitadores del principio y del final de la trama.

El otro campo está dividido en cuatro partes:

El bit T.- indica si la trama es el Token o es de datos.

El bit M.- se activa sólo por una estación privilegiada que lo usa para detectar tramas de datos de los cuales, con la dirección inadecuada, circulan indefinidamente por el anillo.

Los bits P.- indican la prioridad de la trama y del token.

Los bits R.- indican la reserva de prioridad pedida. Estos bits se usan para gestionar la asignación del token a las distintas estaciones.



El campo FC (frame control) consta de :

Bits F.- que definen el tipo de trama .

00	trama MAC
01	trama LLC
1x	reservado, no usado.

Bits z.- indican el tipo de trama en el caso de la trama MAC e información de control en el caso de trama LLC.

Los restantes campos tienen la siguiente información:

Campos DA y SA contienen las direcciones destino y fuente.

Campo INFO contiene los datos para LLC

Campo FCS es un campo de verificación de trama. Se usa para detectar errores de transmisión

Campo FS contiene los bits de estado de la comunicación indicativos de recepción y/o error en la trama.

El mecanismo que sigue el anillo de estaciones para llevar a cabo y controlar la comunicación es el que sigue:

El token circula continuamente de una estación a otra, esto sucede mientras no hay ninguna estación que desee emitir datos. En este caso, el campo de prioridad y el de respuesta están en cero.

En el momento en que una estación desea realizar el envío de datos, espera a que el token la visite y en ese momento lo retira y en su lugar emite una trama de datos. El campo de prioridad estará activo según la prioridad correspondiente a los datos que en ese momento se están transmitiendo. El campo de reserva tendrá el valor de cero.

La trama de datos circulará por el anillo, siendo retransmitida por cada estación hasta llegar a la estación destino. Dicha estación, reconocerá su dirección, recogerá la trama completa, la almacenará internamente y la volverá a retransmitir con la indicación de datos recibidos activa en el campo FS. La trama continuará circulando hasta alcanzar de nuevo al emisor, el cual la retirará y emitirá otra vez el token.

Si durante el viaje de la trama de datos ésta pasa por alguna estación que tenga datos que transmitir, la estación puede, mediante los bits R del campo AC, indicarlo.



Estos bits indican la prioridad de los datos que se desea enviar por alguna estación en sucesivos pasos del token, de manera que este campo siempre contiene la indicación de la máxima prioridad de datos en el anillo.

Cuando la trama de datos vuelve otra vez al emisor, éste analiza el campo de reserva y genera el token con los bits P reflejando esa prioridad. De esta manera, aquellos datos con mayor prioridad podrán ser transmitidos antes de los de menor prioridad.

Debido a que en el medio de comunicaciones pueden producirse errores y a que ciertas condiciones de funcionamiento anómalo de estaciones puede derivar en el funcionamiento inadecuado, existe un nodo especial denominado **monitor**, capaz de supervisar y en todo caso restablecer el funcionamiento correcto.

Hay dos casos básicos de mal funcionamiento:

1. La desaparición del testigo
2. La circulación indefinida de una trama de datos

En el primer caso, el nodo monitor es el encargado de restablecer de nuevo el token. Para ello dispone de un temporizador que inicializa cada vez que le atraviesa el token.

Si el token desaparece, el temporizador vencerá y como consecuencia el monitor reinsertará de nuevo el token, con lo que el funcionamiento quedará restablecido.

El segundo caso, el nodo monitor también toma medidas, en este caso usa el bit M del campo AC y cada vez que una trama de datos lo atraviesa, activa el citado bit a uno. Cuando una trama de datos da una segunda vuelta sin ser retirada, el nodo monitor lo detecta y sustituye por el token, reestableciendo la normalidad en el anillo.

A continuación se presenta la relación de las distintas tramas de control del MAC que existen:

- Claim token
- Duplicate Address test
- Active monitor present
- Standby monitor present
- Beacon (alarma)
- Purge (inicialización)

Las tramas de control del MAC tiene como misión establecer los mecanismos para asegurar el correcto funcionamiento del anillo. En particular existen procedimientos que permiten asegurar la presencia del nodo monitor, procurando si se da el caso, que otras estaciones que actúan de monitores de reserva se conviertan en monitores activos.



También existe un mecanismo que permite la detección de rupturas del anillo y su localización, basándose en el conocimiento por parte de cada estación de la dirección de su predecesora.

En los procesos de inicialización e incorporación de estaciones, se asegura de la unicidad de la dirección de todas las estaciones del anillo mediante la emisión por parte de éstas de una trama identificadora.

La configuración más sencilla de todas es aquella en la que existe un sólo anillo, como se dijo anteriormente se pueden conectar en cascada varios MAUs, con lo que resulta un anillo de mayor número de estaciones.

La solución se basa en conectar dos o más MAU, usando una toma de cada uno para conectarse al otro. Debido a que el número de estaciones está limitado en el anillo y a que el rendimiento puede ser pequeño cuando el número de estaciones es grande, existe una segunda opción: usar Bridges, estos se usan para interconectar dos o más redes de anillo. Cada red posee su propio token circulando, por lo que por el Bridge pasarán los dos.

El funcionamiento del puente es como sigue:

Una estación se desea comunicar con otra estación que se encuentra en la segunda red, para lo cual debe esperar a disponer del token, envía la trama habitual de datos colocando en ella la dirección del destinatario. Esta trama circula por el anillo hasta llegar al Bridge, éste determina que la dirección corresponde a una estación de la segunda red y por lo tanto, recoge la trama y activa el bit de recepción correspondiente.

Recogida la trama, ésta es manejada internamente por el puente, que esperará a disponer del token del segundo anillo. Entonces colocará la trama en el anillo segundo para hacerla llegar a su destino.

La trama una vez alcanzada la estación destino, continuará circulando hasta que llegue al puente, el cual la retirará reestableciendo de nuevo el token como es ya conocido.

Con el anterior mecanismo aumenta considerablemente la capacidad de la red, ya que aumenta el número de nodos factibles. Pero el hecho de tener varios token activos a la vez, ocasiona que los retardos naturales de circulación del token y los datos sean menores, ya que en cada anillo la transmisión se produce independientemente de los datos.

El software disponible para este tipo de red es suministrado por IBM, y cuenta con tres programas, el programa de instalación, el programa PC LAN y el NETbios.



El primero de ellos es un programa que guía al usuario paso a paso en la instalación de cada nodo, ayudándole en la definición de las funciones a realizar por cada uno de ellos.

PC LAN es el sistema operativo de la red, es el encargado de comunicar las PC entre sí y controlar todas las operaciones realizadas por los servidores de archivos y de impresión.

Por último, NETbios es una interface que proporciona una serie de rutinas básicas de entrada/salida.

Una computadora conectada a la red puede ser configurada por el programa PC LAN de cuatro posibles maneras:

Configuración redirectora.- permite compartir recursos y enviar mensajes a otros nodos. Puede usar recursos remotos.

Configuración receptora.- añade a la configuración anterior la posibilidad de recibir mensajes de otros usuarios.

Configuración mensajera.- realiza las mismas funciones que el anterior más la de reencaminar un mensaje recibido hacia otros nodos.

Configuración de archivo o impresora.- convierte a la PC en un servidor de archivos o de impresión.

ARCNET

Es un desarrollo de Datapoint, y es un esquema de bus de transmisión de señales codificadas.

Este sistema apareció en el mercado a mediados de los 70's .

Como ARCNET es anterior a la aparición de estándares de bus de señales, los sistemas basados en ARCNET observan algunas inconsistencias con el resto de los productos de la industria de las comunicaciones de datos, como otros esquemas con bus de señales que se desarrollaron antes de la promulgación del estandar 802.4 de la IEEE. Y no es un estandar.



NORMALIZACIÓN

RECOMENDACIONES IEEE 802

El mercado de las redes locales se debate en ofrecer soluciones normalizadas que permitan la comunicación de dispositivos de diferentes marcas, o bien ofrecer soluciones únicas para un solo producto, sacrificando la normalización en beneficio de un mejor rendimiento.

La normalización es la única vía que garantiza la compatibilidad de los equipos y la posibilidad de expandirse en un futuro evitando que queden obsoletos.

Así, se permite la independencia de los fabricantes, en el sentido de que si los productos están normalizados serán compatibles entre sí y en todo momento el comprador podrá evaluar las distintas ofertas.

Se cuenta además con la garantía de soportar un conjunto de servicios bien conocidos basados en métodos y técnicas bien probadas. Y se cuenta también con la facilidad de la expansión, permitiendo añadir en un futuro nuevos equipos y nuevos protocolos a la configuración existente.

Se citarán algunos de los organismos encargados de la normalización:

ISO

Es una organización internacional de normalización, que presenta entre otras, el modelo de referencia OSI.

CCITT

Es un comité consultivo internacional telegráfico y telefónico, este es un organismo de gran influencia en el entorno de las comunicaciones. Su recomendación para la conexión y cableado de interfaces son de aplicación común.

IEEE

Es el instituto de ingenieros eléctricos y electrónicos, este organismo ha tenido un especial protagonismo en el tema de redes locales. Las recomendaciones de la serie 802.1 a 802.6 prometen ser una norma estable para los niveles inferiores de las redes locales y han sido adoptadas por ANSP⁹ También ECMA¹⁰ ha puesto sus recomendaciones en consonancia con las de la IEEE.

⁹ American National Standard Institute

¹⁰ European Computer Manufacturers Association



En un principio el modelo de referencia OSI, fue concebido para normalizar las redes de área extendida en la que los niveles inferiores de la arquitectura quedan cubiertos por la red de conmutación de paquetes (IBERPAC en España).

Al aplicar las consideraciones generales del modelo OSI a las redes locales, los niveles cuyas características resultan más peculiares son los locales, los niveles uno y dos (nivel físico y nivel de enlace).

Como se mencionó con anterioridad, el organismo que ha conducido los estudios sobre normalización de estos niveles ha sido la IEEE y sus propuestas han sido aceptadas por los restantes organismos de normalización, ISO incluido.

La recomendación 801.1 corresponde a un documento de contextualización de estas normas y su relación con el modelo ISO.

La recomendación 802.2 trata de una parte del nivel dos denominada control de enlace lógico, mientras que la otra parte de este nivel, más el nivel físico no se ha normalizado de una manera única, sino que han optado por generar diversas recomendaciones dependiendo del tipo de configuración y del método de acceso al medio.

El nivel dos se ha subdividido en dos subniveles denominados control de enlace lógico¹¹ y control de acceso al medio¹².

El primero de ellos es común para redes locales, mientras que el segundo es específico para cada una de las configuraciones.

NORMA 802.2 SUBNIVEL LLC.

Esta recomendación describe las funcionalidades propias de este subnivel más las interfaces con el nivel superior (red) y con el subnivel inferior.

La especificación de la interface con el nivel de red describe los servicios que éste subnivel, más los restantes inferiores, ofrecen a los niveles superiores, independientemente de la topología y del medio físico sobre el que se apoyen.

Ofrece la transferencia de una unidad de datos a una dirección concreta pudiendo garantizar el control de flujo y errores.

La interface con el subnivel de control de acceso al medio, MAC, describe los servicios que ésta capa proporciona al subnivel LLC.

Según se ha dicho, existe una especificación MAC distinta para cada una de las configuraciones (CSMA/CD, paso de testigo en bus, etc.) pero el servicio que proporciona este nivel debe ser el mismo en todos los casos con independencia del nivel físico.

¹¹ Las siglas son LLC

¹² Las siglas son MAC



Debido a ello, el subnivel LLC se dice que controla el enlace desde un punto de vista lógico, permitiendo la comunicación entre dos puntos mediante un protocolo de pares.

Las unidades de datos de este protocolo contienen un campo para la dirección de la estación destino y otro para la dirección de la estación origen, además de los bits de información y control.

La dirección del emisor tiene que ser una concreta, pero la dirección del destinatario puede ser expresada de tres formas distintas:

- Dirección de una estación concreta. El destinatario es único.
- Dirección de grupo. Expresa que los destinatarios son un grupo de estaciones.
- Direccionamiento difundido (broadcast). Indica que todas las estaciones de la red son destinatarios del mensaje.

Dentro de una red local, este nivel se comporta como un protocolo end-to-end, es decir, relaciona dos puntos de ésta sin ayuda de intermediarios, siempre desde un punto de vista lógico.

En las redes de área extendida, el nivel end-to-end es el nivel cuatro o nivel de transporte debido a que actúa como intermediaria en las transacciones entre dos equipos terminales. En el caso de una red local aislada, la función del protocolo end-to-end puede ser cumplida por el subnivel superior del nivel dos.

Cuando existen varias redes locales concatenadas esta función la cumple el nivel cuatro, al igual que en los WAN.

La norma prevé la posibilidad de que este nivel proporcione dos clases de servicio. La clase uno ofrece un servicio no orientado a la conexión con un mínimo de complejidad en el protocolo y está previsto para dar servicio a niveles superiores que se encargan de la recuperación y secuenciamiento.

La clase dos proporciona un servicio orientado a la conexión que soporta el secuenciamiento de tramas entregadas y recuperación por errores, es del tipo de los protocolos HDLC.

NORMA 802.3 CSMA/CD.

Describe el subnivel de control de acceso al medio (MAC) y el nivel físico, incluidas las distintas interfaces, para redes locales con acceso al medio por el método de contienda en el que está basada la red Ethernet.



La recomendación 802.3 recoge una versión ya aceptada por ISO a 10 Mbits por segundo y sobre cable coaxial de impedancia de 58.5 ohms , aunque el grupo de trabajo está trabajando sobre versiones en banda ancha y versiones de prestaciones y costos reducidos.

NORMA 802.4 PASO DE TESTIGO EN BUS.

Regula el método de acceso por paso de testigo en bus (token passing bus) en sus dos versiones de banda base y banda ancha, norma que ya ha sido aceptada por ISO.

La opción en banda base usa cable coaxial de 75 ohms y transmite a 1.5, 10 ó 20 Mbits por segundo. La opción en banda ancha es más compleja y difícil de implantar.

Dentro del grupo de trabajo hay un comité, el 802.4B, que está trabajando en una versión más económica denominada *carrier-band*, o banda de portadora, pensada para dar soporte a redes locales para la automatización de plantas de fabricación con bajos requerimientos.

NORMA 802.5 PASO DE TESTIGO EN ANILLO.

Este método de acceso fue de los primeros en ser usados en redes locales por su simplicidad desde un punto de vista lógico, debido a lo que existen múltiples versiones en cuanto a formato de tramas, existencia o no de prioridades, etc. La norma 802.5 regula una de éstas versiones, que posteriormente fue adoptada por IBM para su red en anillo.

Anteriormente, cuando se estudiaron genéricamente los métodos de acceso, al describir el correspondiente a paso de testigo en anillo, se optó por referirse exactamente al método recogido en la recomendación 802.5 por entender que otros métodos alternativos carecen de perspectivas tecnológicas hoy en día, no porque sean intrínsecamente peores que el regulado en la norma, sino simplemente porque difieren de ésta.

NORMA 802.6

Se refiere a redes de área metropolitana, cuyo estudio no se abordará en este curso.



MODELOS PARA EL ENTORNO INDUSTRIAL MAP Y TOP

El modelo de referencia para la interconexión de sistemas abiertos OSI, se concibió originalmente para las redes de área extendida, por esta razón, la IEEE creó un grupo de trabajo para desarrollar los dos niveles inferiores a la arquitectura.

Para los niveles de aplicación surgieron dos iniciativas paralelas, una por parte de la General Motors que se interesaba por las aplicaciones de las redes locales en el entorno de la automatización industrial, y otra por parte de la Boing Computer Services, interesada en el entorno de oficinas. En ambos casos estos grupos de trabajo se basaban (y participaban) en los desarrollos de la IEEE para los niveles uno y dos.

Como resultado de estos estudios surgieron el MAP¹³ para la automatización de los procesos fabriles y el TOP¹⁴ para las aplicaciones de gestión en el entorno de oficinas. Actualmente, se tiende hacia la unificación de ambos en un único conjunto de definiciones desarrollado por el denominado MAP/TOP users group.

La especificación de estos protocolos se inscribe dentro del nivel de aplicación.

Además de desarrollar los protocolos del nivel de aplicación, el grupo MAP/TOP ha especificado también las particularidades de los niveles intermediarios (del tercero al sexto) aceptando para ello los principios de las normas ISO y seleccionando subconjuntos de ellas.

Respecto a los niveles inferiores normalizados por la IEEE , el MAP se apoya en la recomendación 802.4, que describe el método de token passing en bus, mientras que TOP utiliza el método CSMA/CD descrito en la norma 802.3.

La razón de esta diferenciación estriba en la diferente expectativa que se tiene respecto a los tiempos de respuesta y acceso de las estaciones a la red.

¹³ Manufacturing Automation Protocol

¹⁴ Technical and Office Protocol



ESTRUCTURA GENERAL

Modelo OSI

7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Data Link
1	Físico

Notas:

Figura 2-1

MODELO OSI

Nivel 2

NIVEL DE DATA LINK

Checa errores de transmisión a nivel de **FRAMES** y presenta al nivel tres una línea libre de errores.

Define métodos de acceso al medio físico

Notas:

Figura 2-3



MODELO OSI

Nivel 4

NIVEL DE TRANSPORTE

Verifica que los paquetes lleguen en el orden requerido (secuencial).



Notas:

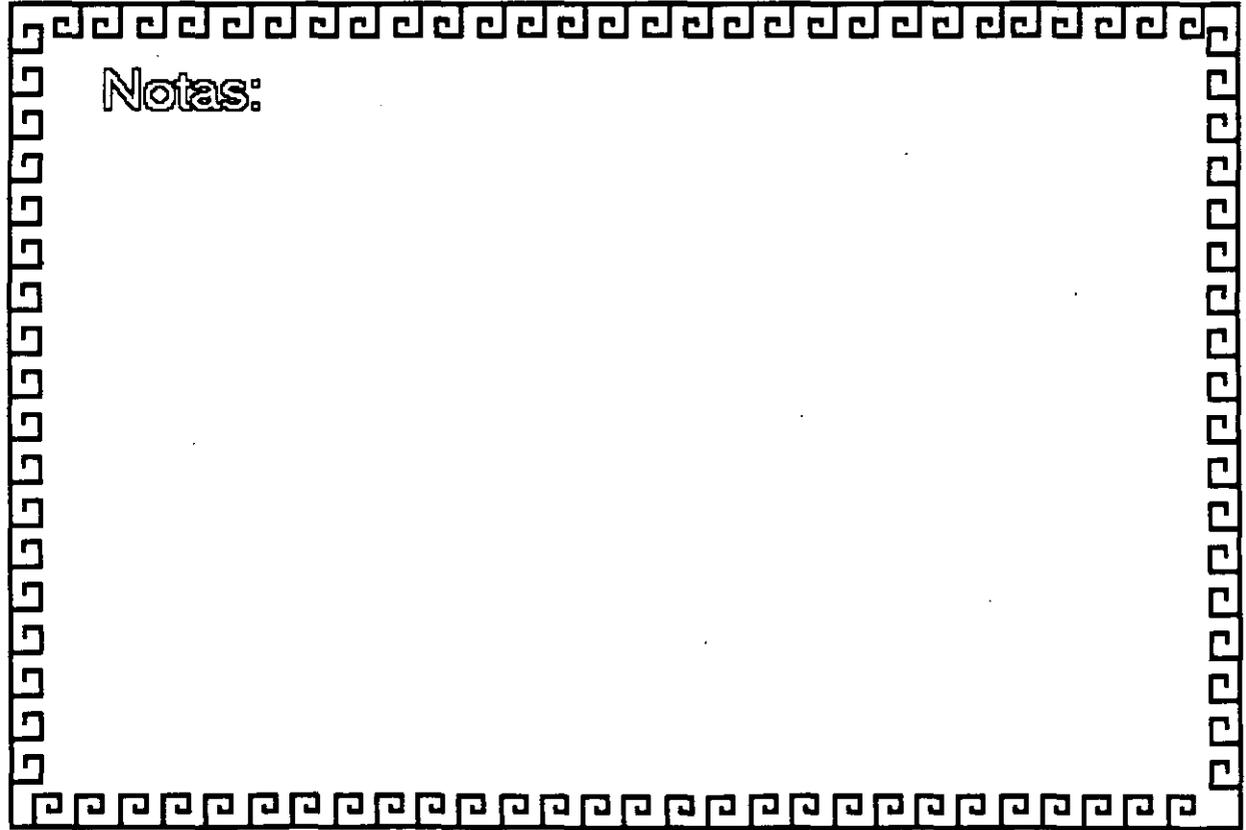


Figura 2-5

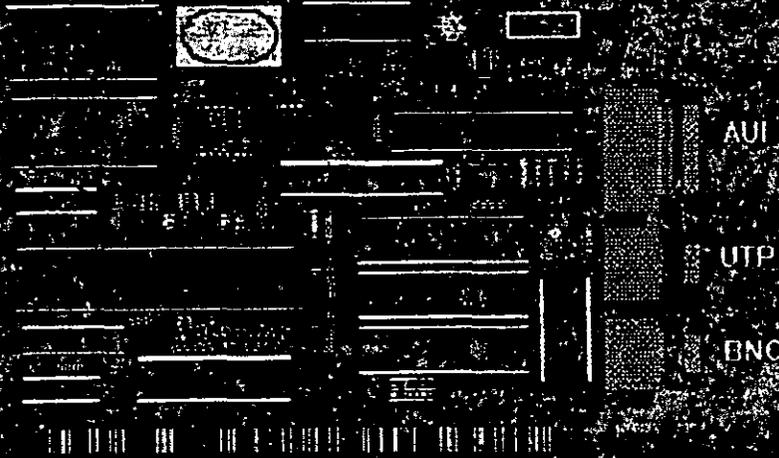
ETHERNET

Características

- 
- Creada por XEROX (1970)
 - Estándar más Estable
 - Versátil en distintos Ambientes
 - Instalación Compleja

Notas:

ETHERNET



Notas:

Figura 2-11

ETHERNET

ESPECIFICACIONES TECNICAS

Velocidad 10Mbits/seg
Protocolo CSMA/CD
Nodos 1 a 1023

Cableado

THICK (RG-11) 500m
THIN (RG-58) 300m
TWISTED PAIR 150m
FIBRA OPTICA

Máximo 3 segmentos

Notas:

ETHERNET

FABRICANTES MAS IMPORTANTES



Notas:

ETHERNET

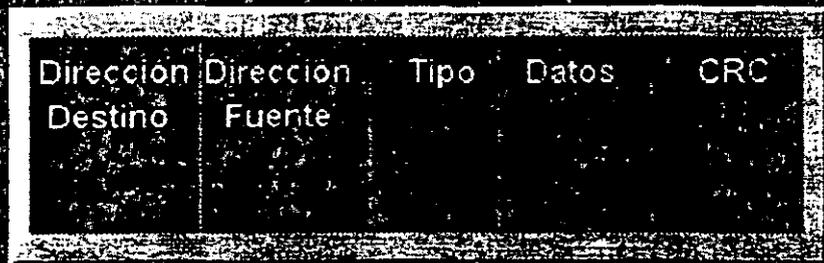
VARIANTES EN INTERFACES PARA PC's

- 
- Tamaño de BUFFER: 8, 16, 40, 64 Kbytes
 - Bus de 8, 16, 32 Bits o Microcanal
 - Uso de DMA
 - Procesador
 - Generación: 1ra, 2da, y 3ra.

Notas:

ETHERNET

FORMATO DEL FRAME

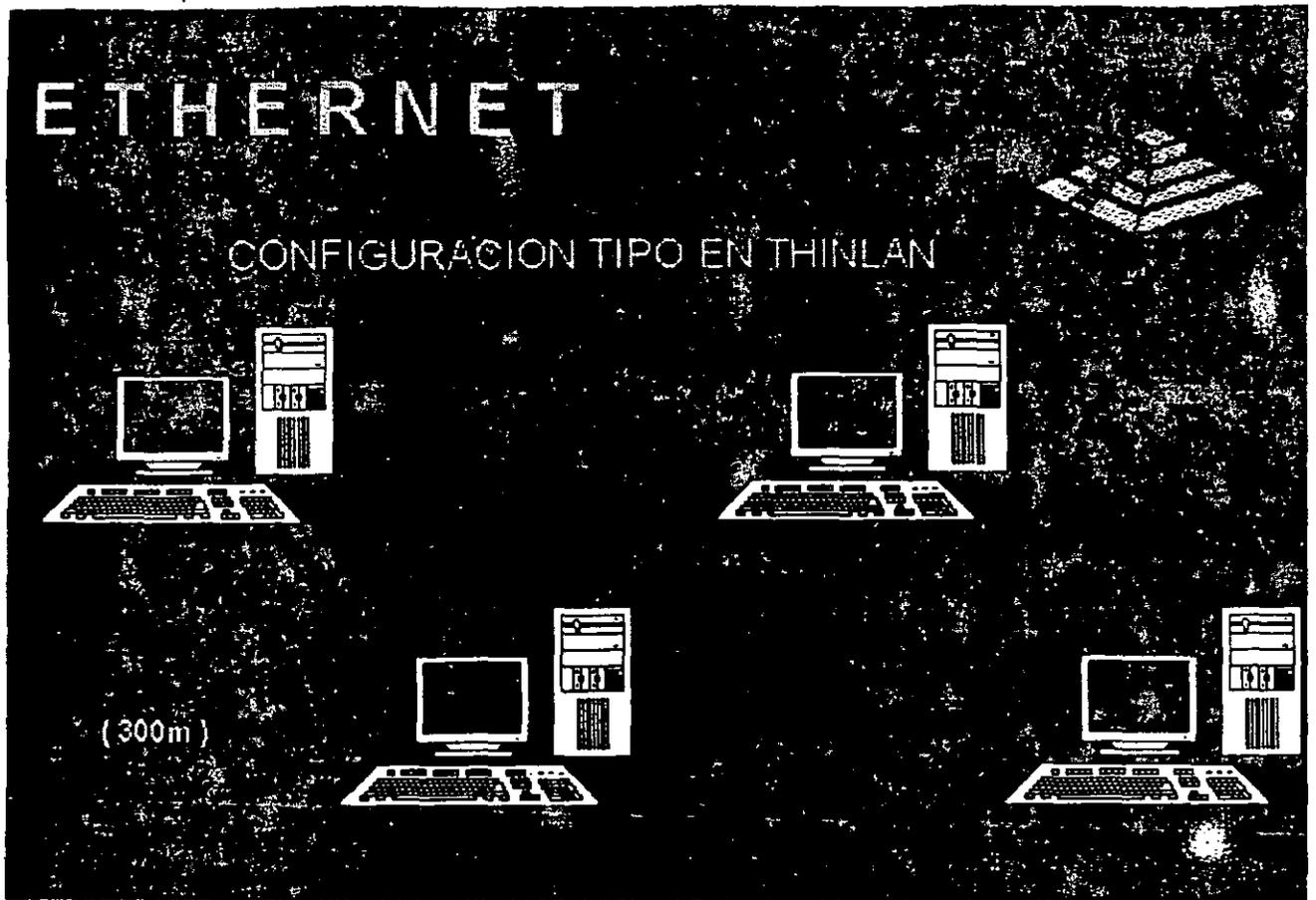


Notas:

Figura 2-15

ETHERNET

CONFIGURACION TIPO EN THINLAN



Notas:

Figura 2-16

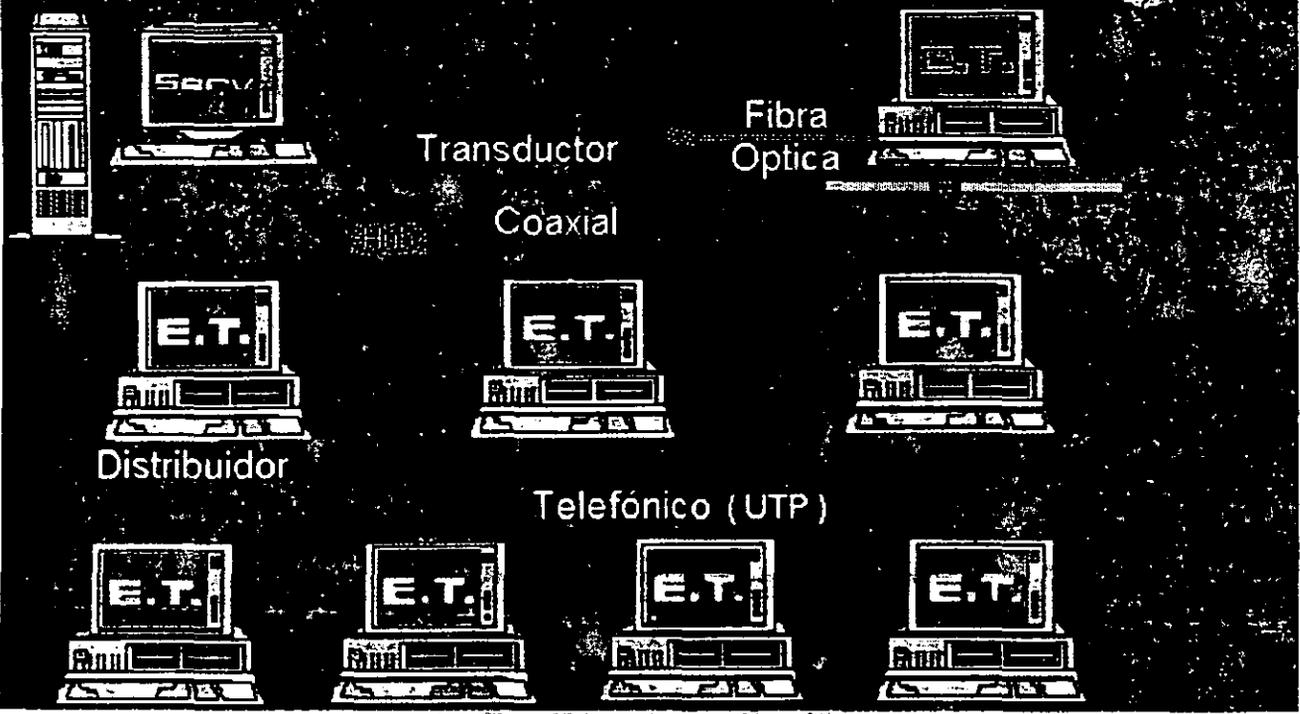
ETHERNET

Resumen Técnico

- Velocidad 10 Mbits/seg
- Estandar más utilizado en el orbe
- Más alto rendimiento (performance)
- Cableado
 - Coaxial Delgado (300 m/seg.)
 - Coaxial Grueso (500 m/seg.)
 - Paralelónico (150 m/seg.)
 - Fibra Óptica
- Conectividad hacia otros sistemas
- Norma 802.3 (IEEE)

Notas:

ETHERNET



Notas:

Figura 2-18

TOKEN RING

CARACTERISTICAS

- Creada por IBM
- Alta Conectividad en IBM
- Buen complejo
- Buen rendimiento
- Opción de 4 y 16 Mbits/seg.

Notas:

TOKEN RING



Notas:

TOKEN RING

Especificaciones Técnicas

Velocidad	4 o 16 Mbits/seg
Protocolo	Token Passing
Nodos	1023
Instalación	MAU's
Cableado	STP/IBM tipo 2 UTP FIBRA OPTICA

Notas:

TOKEN RING

FABRICANTES MAS IMPORTANTES

- 3 COM
- IBM
- MICRON
- UNGERMAN - BASS
- PROTEON

Notas:

TOKEN RING

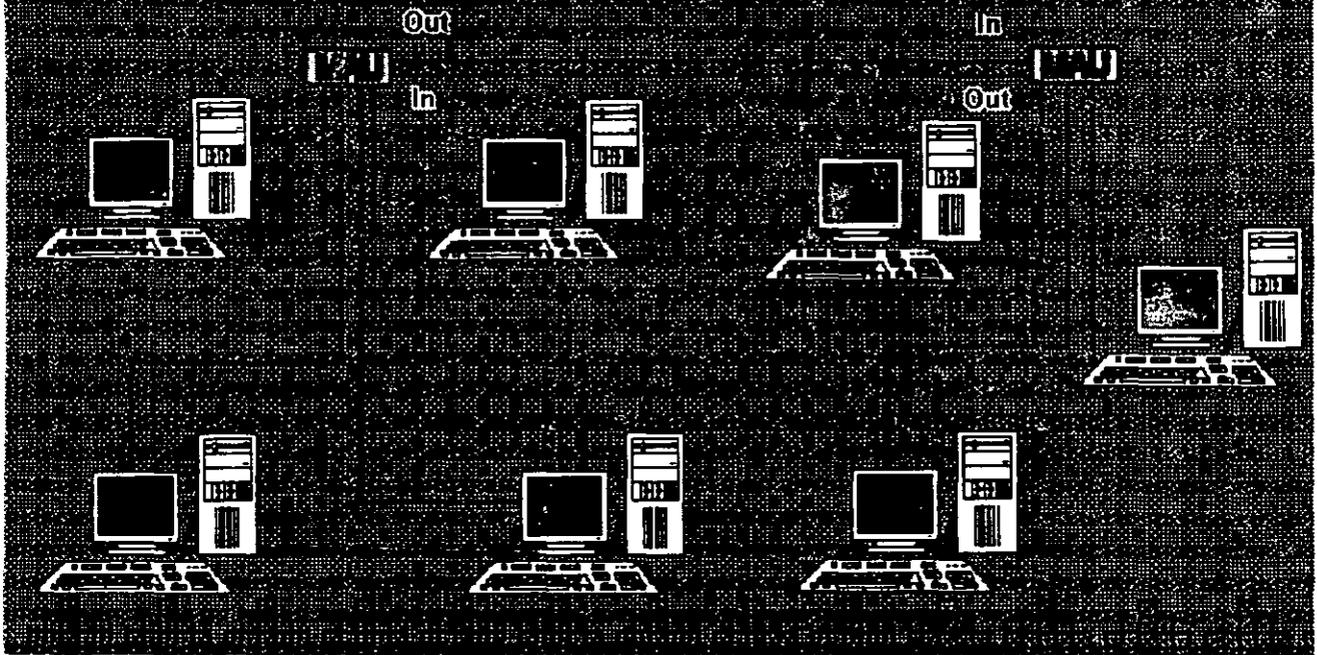
FABRICACION

El conjunto de Chips para Token Ring se desarrollo conjuntamente entre IBM y Texas Instruments. Casi todas las interfaces Token Ring se basan en el Chipset de T.I. (TMS380)

Notas:

TOKEN RING

CONFIGURACION TIPO TOKEN - RING



Notas:

TOKEN RING

Resumen Técnico

- 4 Mbits/seg.
- Topología de Estrella distribuida
- Norma 802.5 (IEEE)
- Protocolo Token Passing
- Cable IBM tipo 2
- conectividad hacia ambiente IBM

Notas:

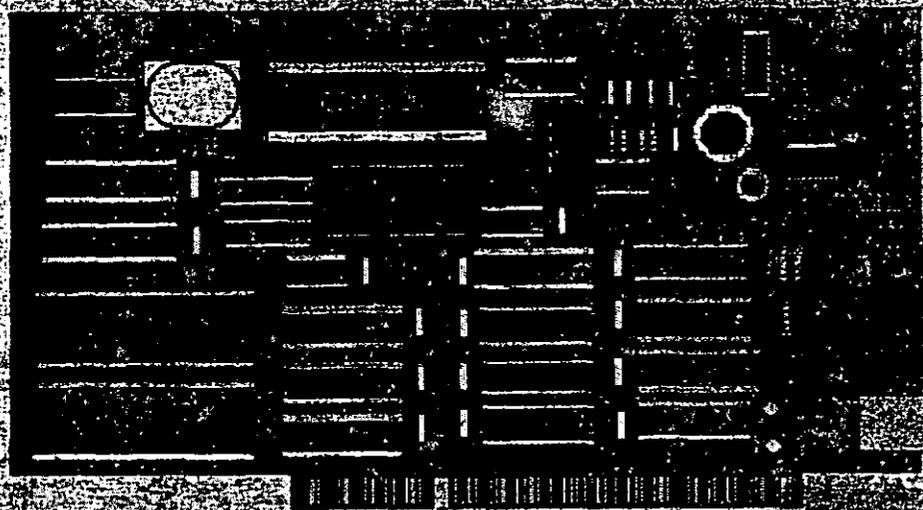
ARCNET

CARACTERISTICAS

- Creada por Datapoint
- Mejor precio/rendimiento
- Cableado muy versátil
- Fácil instalación
- Actualmente saliendo del mercado

Notas:

ARCNET



Notas:

Figura 2-27

ESPECIFICACIONES TÉCNICAS

Especificaciones Técnicas

Velocidad..... 2.5 Mbits/seg.

Protocolo Token - Passing

Nodos 1 a 255

Instalación ... repetidores [Activos - Pasivos]

Cableado	RG - 62
	Fibra Optica
	Twisted Pair

Notas:

ARCONE

Estructura General

SWITCHES

I/O Address

DMA

Node
Address

COM 9026

I/O

Notas:

ARCNET

FABRICANTES MAS IMPORTANTES



- MICRON
- DATAPOINT
- STANDAR MICROSISTEMS
- PURE DATA
- NOVELL
- THOMAS CONRAD

Notas:

A large rectangular frame with a Greek key border, intended for notes. The frame is empty, with the word "Notas:" written in the top left corner.

FORMATO DEL FRAME

Alerta SOH SID SID DID Cont Datos CRC CRC

Notas:

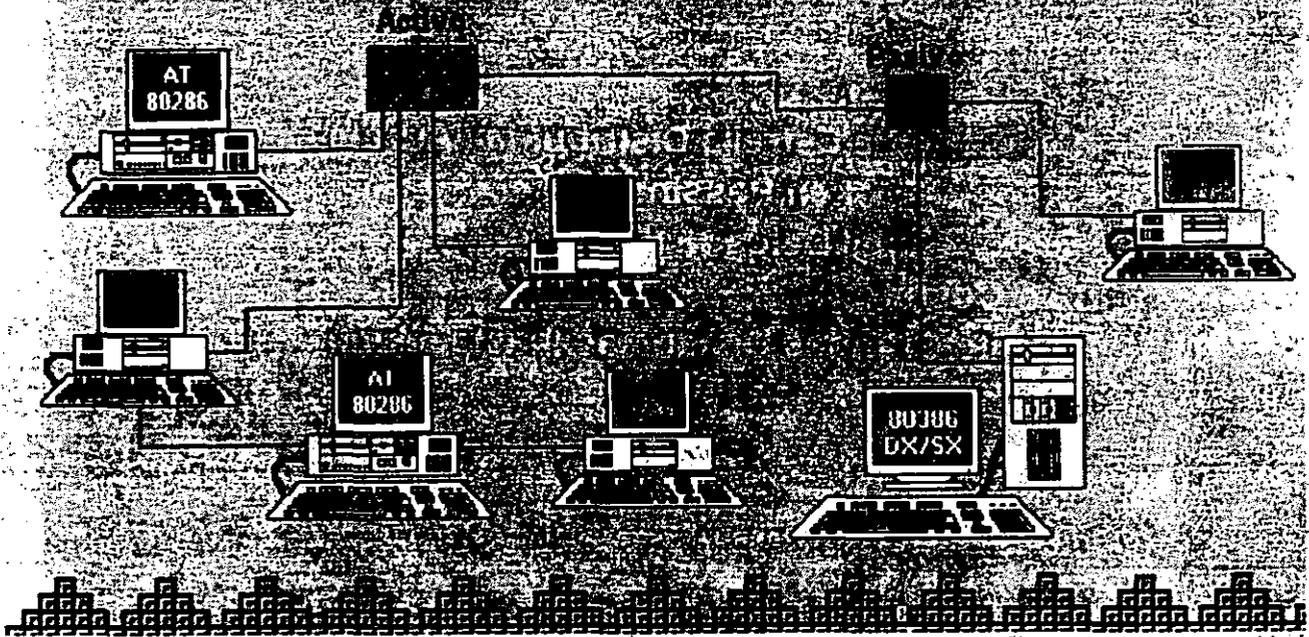


Notas:

Figura 2-32

ARCNET

CONFIGURACION TIPO EN ARCNET



Notas:

Figura 2-33

ARCNE

Resumen Técnico

- 2.5 MBits/s
- Topología de Estrella Distribuida (Arbol)
- Protocolo Token Passing
- Cable Coaxial Delgado (RG-62)
- Bajo Costo
- Permite Grandes Distancias (hasta 6 km)

Existen otros estándares
No muy comerciales

Notas: